EPIDERMAL RFID-BASED PROGRAMMABLE SMART SHIELD FOR ENHANCING SECURITY OF IMPLANTABLE CARDIAC DEVICES

F. Lestini(1), G. Marrocco(1), C. Occhiuzzi(1)

(1) DICII, University of Rome Tor Vergata, Via del Politecnico 1, 00133 Rome, Italy. *name.surname@uniroma2.it*

Abstract

In recent years, Implantable Medical Devices (IMDs) have advanced with wireless connectivity, enhancing diagnostic and therapeutic capabilities while introducing cyber and physical vulnerabilities that could threaten patient safety. This paper proposes an epidermal RFID-based wireless programmable smart shield to protect Implantable Cardiac Devices (ICDs) from physical attacks. Positioned on the patient's skin, the shield blocks untrusted electromagnetic fields in the 401-406 MHz band and can be wirelessly reconfigured at 900 MHz to enable communication with a trusted external programmer for medical assistance. The smart shield is designed as a programmable Frequency Selective Surface (FSS). Preliminary simulations of the unit cell, featuring an RFID IC and PIN diodes for wireless reconfiguration, confirm the concept's feasibility.

Index Terms *– Frequency Selective Surfaces, Implantable Medical Devices, RFID, Wireless Programmability.*

I. INTRODUCTION

Implantable Medical Devices (IMDs) provide essential diagnostic, therapeutic, and monitoring functions, often incorporating wireless connectivity for remote monitoring and programming via the Medical Implant Communication Service (MICS) band (401-406 MHz). Despite enhancing IMDs' capabilities, this connectivity introduces cyber and physical security risks, leaving devices vulnerable to attacks [1], [2]. Although various protection mechanisms have been proposed over the years [3], IMDs are still vulnerable to physical attacks and cannot prevent cyber attacks if a vulnerability in the communication protocol is found [4]. Thus, finding an alternative solution for increasing the cyber/physical security of IMDs is essential, especially for high-risk devices like pacemakers, where *security* directly impacts patient *safety*.

This paper introduces a *wireless programmable smart-shield* designed to protect Implantable Cardiac Devices (ICDs) from unwanted electromagnetic

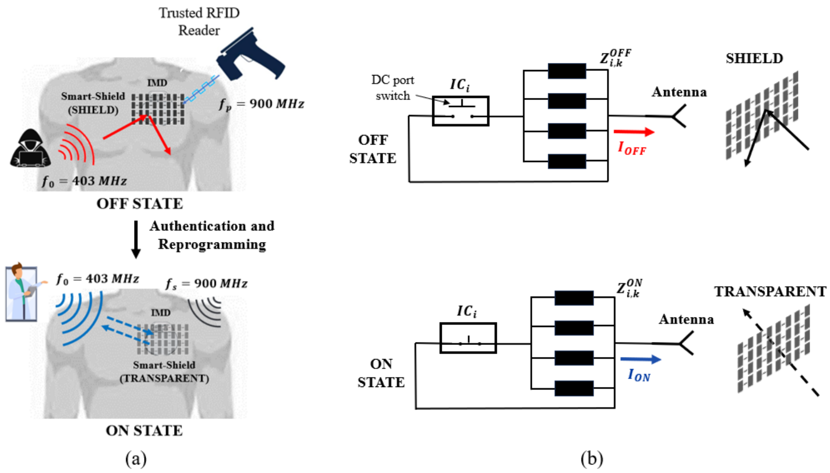

Figure 1: (a) Concept of Reprogrammable FSS for ICDs protection. (b) Schematic representation of the unit cell layout in both states.

fields in the MICS band. Positioned on the patient's skin, the shield blocks untrusted signals and enables secure communication with the ICD after successful authentication (Fig. 1a). Leveraging RFID wireless programmability [5], [6], the system uses RFID ICs and RF switches for reconfiguration. Authentication and reprogramming occur in the UHF band (860-960 MHz), while smart shielding operates in the MICS band, utilizing a programmable Frequency Selective Surface (FSS) [7] to dynamically adjust its stop-band for enhanced security.

II. Rationale

The proposed RFID-based wireless programmable Frequency Selective Surface (FSS) comprises an $N = n \times m$ grid of unit cells, each featuring 4 RF switches connected in parallel and a passive RFID IC for wireless reprogramming [6]. In the *OFF* state (Fig. 1.b), diodes are set to impedance $Z^{\text{OFF}}_{i,k}$, enforcing the FSS to reflect incoming fields at $f_o = 403\ MHz$, blocking unauthorized communications and preventing EMI attacks on the IMD. Reprogramming is performed by sending EPC Gen2 commands to the RFID ICs via a trusted reader at $f_p = 900\ MHz$, switching the tunable element impedance to $Z^{\text{ON}}_{i,k}$ (Fig. 1.b), making the FSS electromagnetically transparent at f_o. The necessary switching energy is supplied by an RF field at $f_s = 900\ MHz$ from the reader antenna. The FSS must ensure shielding in the *OFF* state, only becoming transparent in controlled environments to prevent unauthorized activation and security breaches.

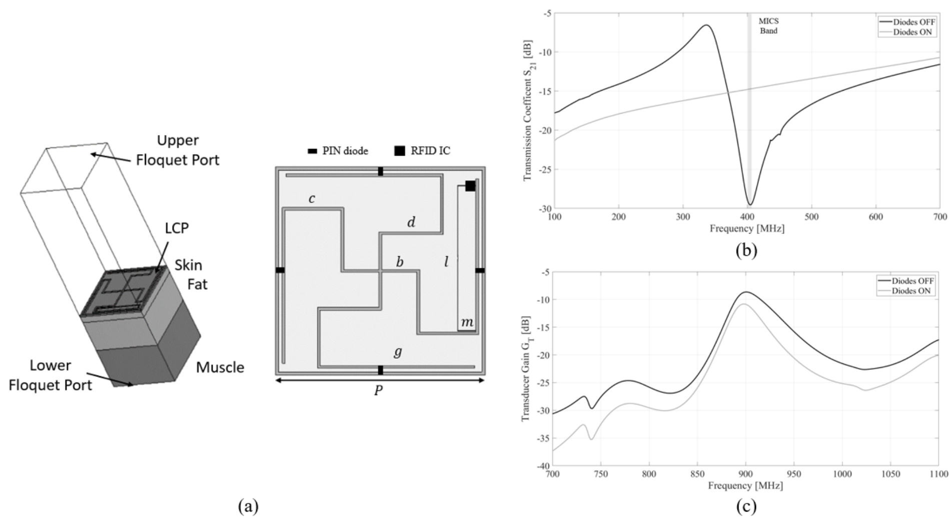

Figure 2: Unit cell simulations setup. Simulated (b) transmission coefficient and (c) transducer power gain in both states.

III. Numerical Analysis

The FSS was designed using CST Microwave Studio 2024, employing a square unit cell based on a layered human body phantom consisting of skin ($t_{skin} = 5\ mm$), fat ($t_{fat} = 20\ mm$), and muscle ($t_{muscle} = 26\ mm$), with periodic boundary conditions (Fig. 2a). The tissue dielectric properties were calculated using the Cole-Cole model. The conductive element is a meandered cross-shaped resonator surrounded by an inductive wire loop, placed on a flexible, biocompatible Liquid Crystal Polymer (LCP) substrate (0.4 mm thick, $\varepsilon_r = 3.3$, $tan\delta = 0.002$). Floquet ports were positioned 50 cm above the FSS and 26 mm deep in the muscle (the typical ICD implantation depth) to evaluate the scattering parameters between them. The RFID IC (EM4152, $Z_{IC} = 17.6 - j271.9\ \Omega$) was integrated into the layout via a Γ-Match for impedance matching [8], and 4 PIN diodes (modeled through their .s2p files) were placed across the resonator and external loop for reconfiguration ((Fig. 2a)). The unit cell's geometric parameters were optimized to center the FSS stop-band in the MICS band and maximize the transducer power gain G_T between the upper Floquet port and the RFID IC [9].
Simulation results for the transmission coefficient (S_{21}) and transducer power gain (G_T) confirm the reconfigurable capabilities of the FSS. In the OFF state, S_{21} is approximately -30 dB within the MICS band, while in the ON state, the S_{21} increases to -15 dB. The G_T values are approximately -9 dB in the OFF state and -11 dB in the ON state at 900 MHz, ensuring a reliable communication link [9].

IV. Conclusions

This paper introduces an epidermal RFID-based smart shield for ICD protection against physical and cyber attacks in the MICS band, with wireless programmability in the UHF band. The system, designed as a programmable FSS, blocks communications with the ICD until reprogrammed by a trusted RFID reader. Preliminary simulations of the unit cell's transmission coefficient and RFID IC transducer gain demonstrated the idea's feasibility. However, further optimization is needed for unit cell size and power consumption, e.g., using varactors or RF switches. Indeed, the unit cell is too large, challenging the final device's comparability to a typical epidermal patch, while the power required by the PIN diodes must be significantly reduced to allow passive reconfiguration. Future work will also focus on analyzing the finite array's performance and conducting experimental measurements to validate and refine the design.

References

[1] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem," *Medical Devices: Evidence and Research*, pp. 305–316, 2015.

[2] M. A. Siddiqi, W. A. Serdijn, and C. Strydis, "Zero-power defense done right: Shielding imds from battery-depletion attacks," *Journal of Signal Processing Systems*, vol. 93, pp. 421–437, 2021.

[3] S. Jacob, et al., "Clinical applications of magnets on cardiac rhythm management devices," *Europace*, vol. 13, no. 9, pp. 1222–1230, 2011.

[4] *Medtronic Conexus Radio Frequency Telemetry Protocol Vulnerability*, 2021. [Online]. Available: `https://www.cisa.gov/news-events/ics-medical-advisories/icsma-19-080-01`.

[5] Z. X. Wang, et al., "A long-range and nearly passive rfid-controlled information metasurface," *Advanced Optical Materials*, p. 2 203 114, 2023.

[6] F. Lestini, G. Marrocco, and C. Occhiuzzi, "Rfid-based reconfigurable electromagnetic devices," *IEEE Journal of Radio Frequency Identification*, vol. 8, pp. 226–234, 2024.

[7] M. Abdollahvand, et al., "Reconfigurable fss based on pin diodes for shared-aperture x/ka-band antennas," in *2021 15th European Conference on Antennas and Propagation (EuCAP)*, IEEE, 2021, pp. 1–4.

[8] G. Marrocco, "The art of uhf rfid antenna design: Impedance-matching and size-reduction techniques," *IEEE antennas and propagation magazine*, vol. 50, no. 1, pp. 66–79, 2008.

[9] F. Lestini, N. Panunzio, G. Marrocco, and C. Occhiuzzi, "Epidermal RFID-Based Thermal Monitoring Sheet (R-TMS) for Microwave Hyperthermia," *IEEE Journal of Electromagnetics, RF and Microwaves in Medicine and Biology*, vol. 7, no. 4, pp. 365–374, 2023.