Abstract:
This work is targeting a solid security improvement in the wireless communication between existing and possibly future implantable medical devices (IMDs) and Programmer Monitor Device (PMD). A public medical server acting as a trusted Authority is introduced. A dedicated Pacemaker Proxy Device (PPD) is proposed to serve as a security mediator between PMD and IMD taking care of all medical security, liability and responsibility issues. The key idea is based on embedding low-complexity and resilient digital physical identities based on a new concept in the system devices to prohibit physical substitution/cloning attacks. A biometric identity extracted from the patient's ECG (electrocardiogram) is supporting the security system by adding rather hard-to-clone patient personal health profile. A machine learning algorithm is deployed to extract such biometric identity (key). The initial results of the proposed approach showed practical accuracy in extracting the biometric identity approaching 95%. The whole resulting system ensures solid, resilient and high level of protection for future smart medical environment.