**Paper summary -   
They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices**

**Summary**

The main goal of the paper is to address the challenges of the security of implantable devices, considering the fact that the IMD device implanted in the patient **cannot** be changed or modified easily without being operated. The authors of the paper come up with a novel idea of a base station called *shield* which is responsible for the security of the IMD. The shield can be used as a jammer-cum-reciever that jams all the messages thereby preventing attackers from decoding the IMD messages while being able to decode them itself. It is a full duplex radio that can be worn as a necklace and jams signal only at the receiver's antenna. It can be used to provide confidentiality to sensitive data and protects IMD from unauthorized commands that can be dangerous to the safety of the patient. This shield is evaluated against commercially available IMDs and found to be successful.

**Strengths**

* Security analysis of attacks such as eavesdropping and replay attacks is done really well. It is also shown how the proposed solution can prevent such attacks and thereby ensure confidentiality and valid authorization of data and commands respectively.
* The proposed solution is also non-invasive and doesn't need any modifications to the IMDs present in the patient's body already, thereby making it scalable and usable with already existing devices.
* Considering the fact that the shield acts as a jammer, it is important to study its coexistence with other devices and the paper does that and states that there is no effect of jamming on any of the cross-traffic packets.

**Weaknesses**

* The *shield* technique proposed is still a research project and is evaluated against only two IMDs listed in the paper. It needs more evaluation in terms of the number of devices and real-world scenarios.
* The shield should also be worn as a necklace around the patient's neck which is debatable in terms of security vs usability. I am not sure if patients would really agree to wear a necklace all the time.
* There are also other assumptions that IMDs use protocols authorized by FCC and that programmers follow all the best practices. Although it's a reasonable assumption, it can only be verified when the product is tested across more devices.