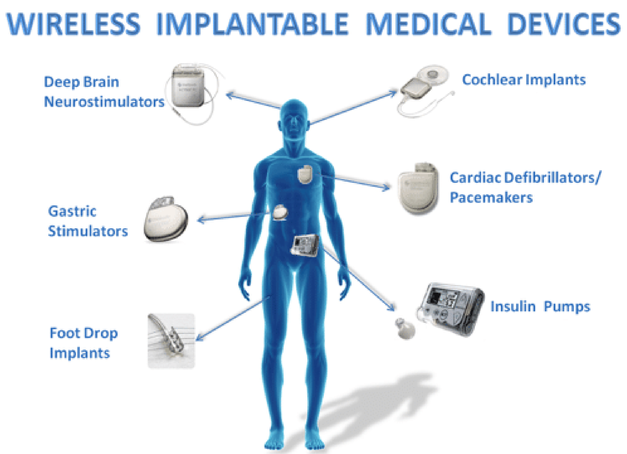
Dynamic and Lightweight Encryption towards Data Confidentiality in Medical IoT Devices (MIoT)

MIoT SECURITY

Medical IoT is growing at an exponential rate because of its promises to help advance patient engagement and improve delivery of health care. However, it also incurs a range of security concerns. As medical IoT devices may gather hosts' geographical information, monitor patients' privacy activities, and record clients' biometric features, one of the critical concerns is how to preserve the confidentiality of such sensitive data. Specifically, because of the broadcast nature of wireless signal, the communication and data transmission with Medical IoT devices are usually vulnerable to eavesdropping attacks.

Intuitively, cryptography encryption methods can be applied to encrypt all the conversation from medical IoT devices. However, as medical IoT devices, such as Implantable medical devices (IMDs), are usually featured with limited computational capacity and limited power, they may not afford expensive cryptography operations by conventional encryption methods like AES or RSA. To cope with the limited resources of medical IoT devices, we propose a novel encryption scheme, named Dynamic Wireless Channel Pad (DyWCP), that takes advantage of dynamic signal variation in wireless context to achieve the confidentiality of sensitive data.

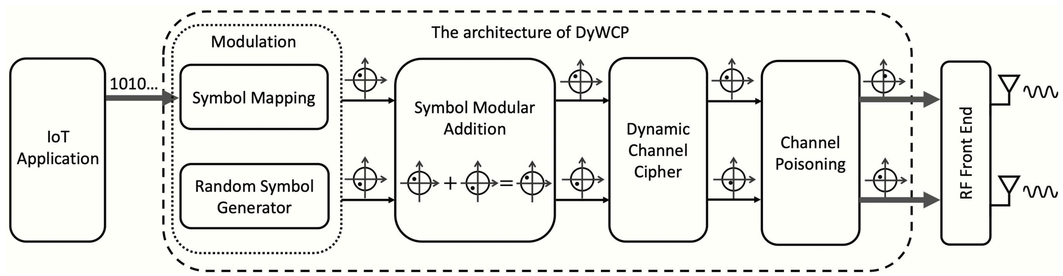


SYSTEM DESIGN

It is essential to secure the communication between medical IoT devices. We develop a dynamic and lightweight encryption scheme named DyWCP to protect sensitive data. DyWCP is inspired by one-time pad encryption which is lightweight and simple but has been proven of the perfect secrecy property. Nevertheless, one-time pad encryption has been rarely used in practice since it was invented several decades ago. The key negotiation creates the essential hurdle of applying one-time pad encryption. In our design, we aims to address this hurdle by completely removing the step of key negotiation to enable the practical use of one-time pad encryption for medical IoT devices.

We incorporate DyWCP into physical layer processing in wireless context to achieve the goal. As shown in the figure, it consists of four modules:

1) **Modulation:** it converts incoming bit sequence into continuous wireless symbols, and produces arbitrary keys for symbol encryption.
2) **Symbol modular addition:** it performs symbol wise modular addition to encrypt incoming messages by the random generated keys.
3) **Dynamic channel cipher:** it calibrates encrypted symbols to accommodate channel variation ensuring that the key always cancels at receiver but remains at an eavesdropper.
4) **Channel poisoning:** it disables the capability of the eavesdroppers to estimate the wireless channel from the predefined information.



FEATURES

1. **Light-weight:** DyWCP is designed to only consumes few computational resources. It works along with the baseband equalization processing, while decryption is hassle-free without any computational consumption.
2. **Secure:** The scheme is inspired by the one-time pad encryption, simple but with high secrecy.
3. **Compatible:** DyWCP can work independently from application layer. It is complementary to traditional cryptography scheme and can work together to further improve the security.
4. **Ubiquitous:** DyWCP can be applied to most medical IoT applications with wireless connectivity

CONTRIBUTIONS

In this research, we propose a lightweight encryption scheme named DyWCP to protect sensitive data in medical IoT devices. Towards the proposed scheme, we create a dynamic channel cipher design to utilize wireless channel features for basic encryption, a symbol-level modular addition method to enables the incorporation of the proposed scheme into practical wireless systems, and a channel poisoning method to address the known plaintext attack for improved information security.

We implement the proposed scheme using USRPs and conduct a suite of experiments to evaluate the performance of the proposed scheme. The evaluation results show that DyWCP can effectively and efficiently defend against the potential eavesdropping attacks and preserve the data confidentiality of medical IoT devices

AUTHORS: [1]Tao Hou and [2]Tao Wang

[1]Department of Computer Science, Texas State University, Email: taohou@txstate.edu, Homepage: https://tao-hou.com

[2]Department of Computer Science, New Mexico State University Email: taow@nmsu.edu, Homepage: https://tao-wang.com

*This work is published in ACM WiSec 2022