Towards Ultra Light-weight Solutions for IMD Security

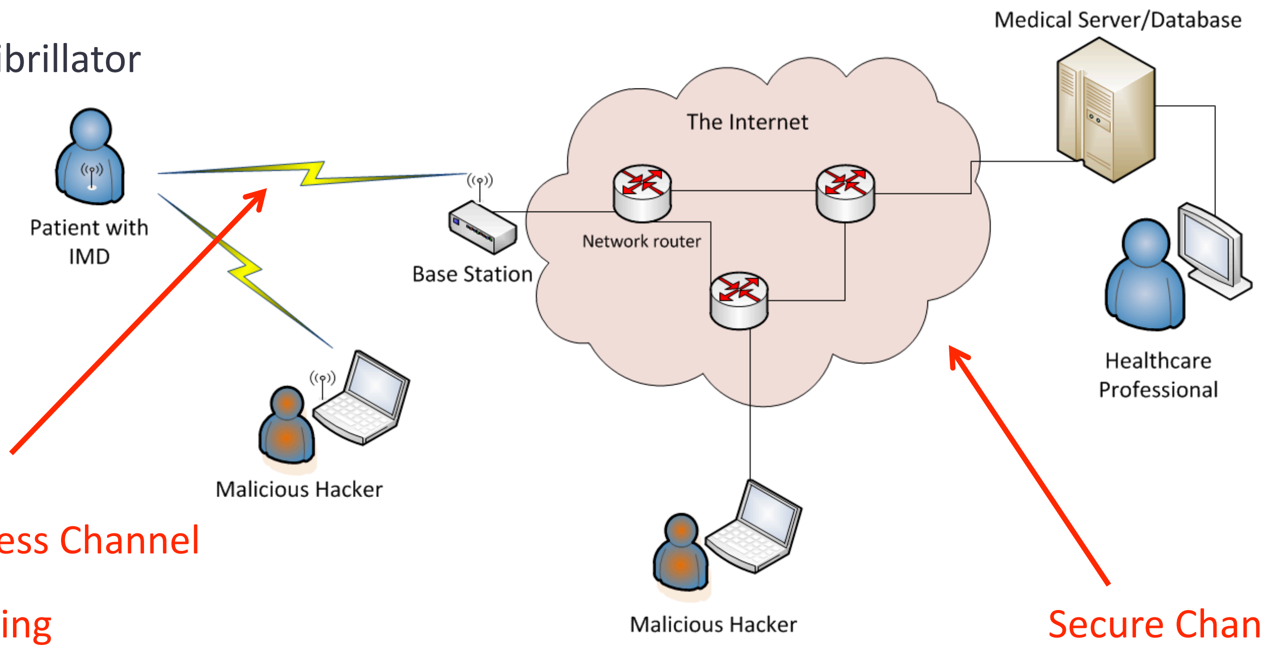
Saied Hosseini Khayat, *PhD*
Assistant Professor
Digital Systems Lab
Electrical Engineering Department
Ferdowsi University of Mashhad, Iran

Workshop on Security and Privacy in Implantable Medical Devices, EPFL, April 2011

Motivation

- Wireless + IMD → Convenience - Security

Pacemaker
Cardiac defibrillator



Insecure Wireless Channel

Eavesdropping
Masquerading
Denial of service

Secure Channel
standard protocols
e.g. IPSEC

Motivation

- Kevin Fu, "**Reducing the risks of implantable medical devices: A prescription to improve security and privacy of pervasive health care**" Inside Risk 218, *Communications of the ACM*, 52(6):25–27, June 2009.

- D. Halperin, *et al.*, "**Security and Privacy for Implantable Medical Devices**," *IEEE Pervasive Computing*, Jan-March 2008.

- K. Malasri, L. Wang, "**Securing Wireless Implantable Devices for Healthcare: Ideas and Challenges**," *IEEE Communications Magazine*, July 2009.

- D. Halperin, *et al.*, "**Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses**," *IEEE Symposium on Security and Privacy*, 2008.

Vision

- IMD security is **vitally important**.
  - No one buys a house, car lacking a door-lock.

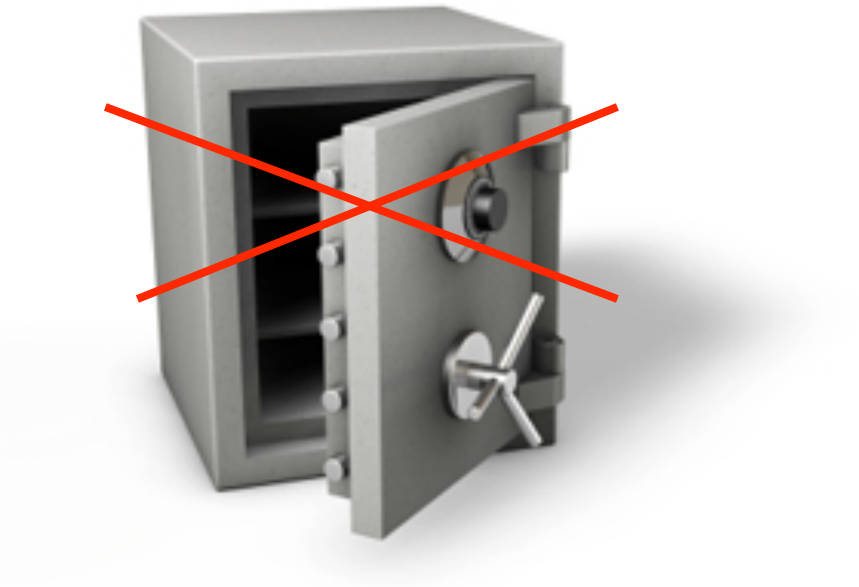
- ~~Security is expensive.~~
- ~~IMD has no room (cost, area, power) for security.~~

- Security can be **transparent** and **low-cost**.
  - Should not get in the way of functionality, performance.
  - Should not increase cost, power consumption.

- Protect the "**common patient**" against the "**common bad guy**."

Equip a normal house with a normal door-lock.

Heavy-weight security



Light-weight security

Our (Partial) Solution

- Employ a lightweight 64-bit block cipher.
  - 128-bit block ciphers too heavy
  - Stream ciphers require bit-level synchronization of sender and receiver. Hard to maintain.
- Create a lightweight protocol around cipher.
  - Existing protocols (e.g. IPSEC) too heavy
- Implement protocol in dedicated hardware.
  - Software implementation wasteful of power
- Use subthreshold logic to minimize power.
  - Goal: Minimum power for a decent level of security

Broad Taxonomy of Medical Sensors

- **Function**
  - Sensing
  - Sense and actuate
- **Life-time**
  - Short-term (days)
  - Medium-term (months)
  - Long-term (years)
- **Location**
  - On body
  - In body
- **Energy source**
  - Battery
  - Harvesting
  - Induction
- **Connectivity**
  - Wired
  - Wireless
  - No connection
- **Data rate**
  - Low
  - High

My Focus

IMD Requirements

- Sensing and digital signal processing (e.g. ECG)
- Actuating (e.g. defibrillation shock)
- Radio communication
- High reliability
- Minimal device size
- Small nonrechargeable battery (~5000 Joules)
- Very long operational life-time (~10 years)

→ 10-20 μW average power for the entire device!

Demands ultra low-power electronics

Any room left for crypto processing ??

Goal in the rest of this talk

- To present a lightweight protocol that protects against
  - Breach of privacy (i.e., eavesdropping)
  - Malicious control, reprogramming of IMD (i.e., masquerading)

Assumptions

- A secret key is shared between IMD and BaseStation.
- The employed block cipher is not “broken.”
- Long data blocks are segmented into 64-bit blocks.
- Each IMD has a unique ID (serial number).
- No guaranteed delivery of packets
- No specific assumption about MAC layer

Attack Model

- Attacker does not have:
  - Physical access to IMD
  - Physical access to Base Station
  - Secret keys
- Attacker can:
  - Listen to messages
  - Transmit fake messages
  - Save and replay messages

Covers most of common attacks

- Above model differs from RFID and sensor network.

Lightweight Block Ciphers

My favorite

- DES, DESXL, HIGHT, PRESENT, KATAN, AES

2309 GE

2168 GE

3048 GE

1570 GE
5 uW @ 100 KHz

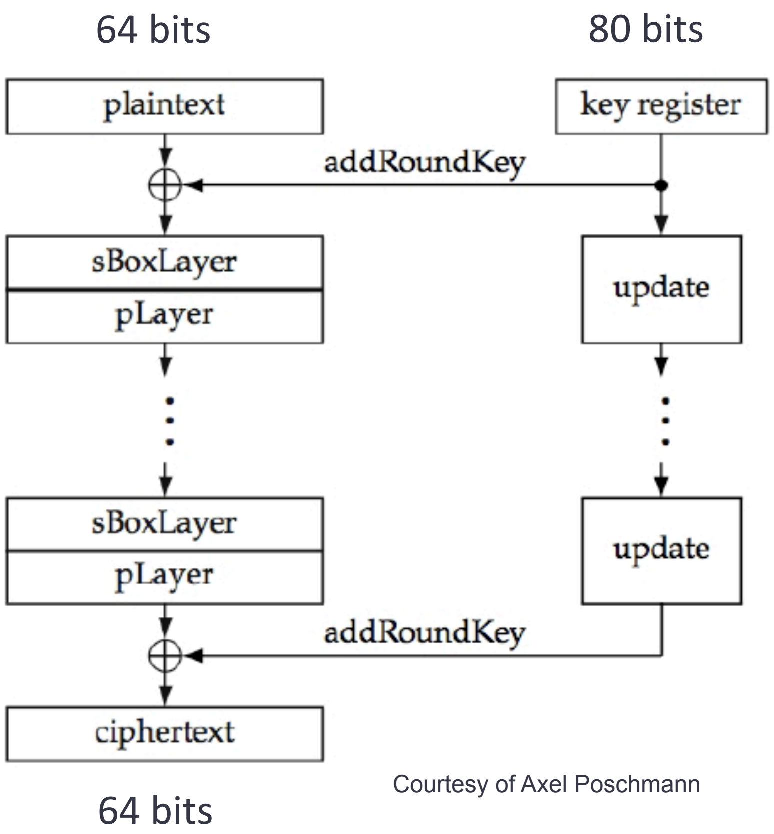
1054 GE

3400 GE

Bogdanov, *et al*, 2007

PRESENT Block Cipher

2007. Bogdanov, et al



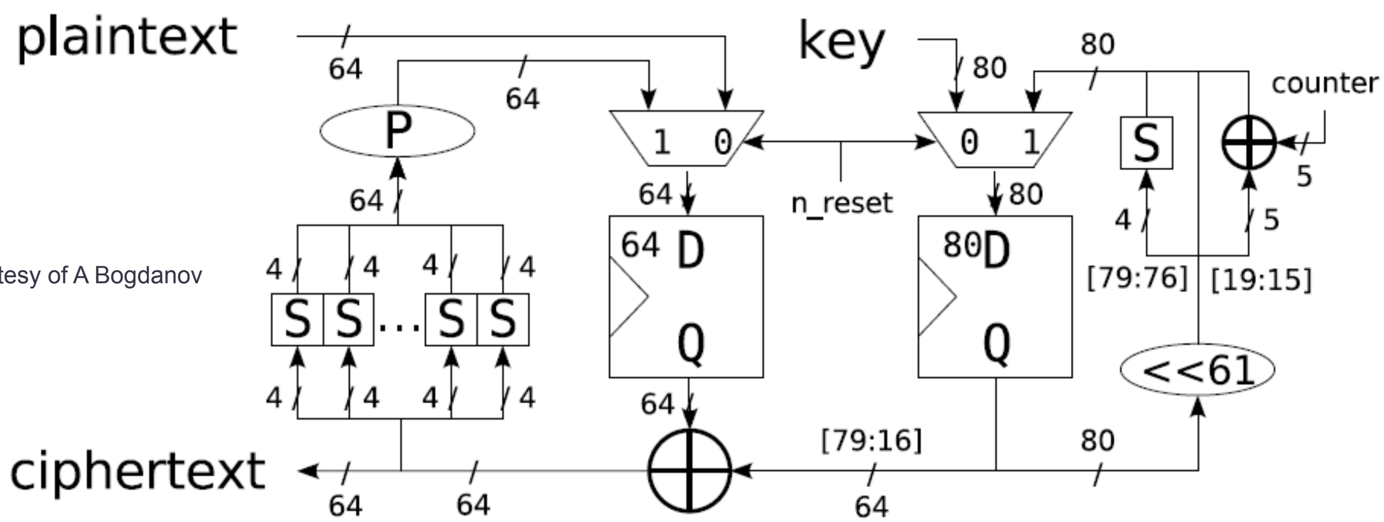
Courtesy of Axel Poschmann

Features

- Symmetric block cipher
- 64-bit block
- 80-bit key
- 31 rounds
- Simple S-P network
- 16 identical 4x4 Sboxes
- On-the-fly key schedule
- Resistance to differential and linear attacks

PRESENT Block Cipher

2007. Bogdanov, et al



Courtesy of A Bogdanov

For AES

Our implementation
Of PRESENT

Resources:
MUX21: 144
XOR2: 69
DFF: 149
Sbox: 17

Vdd=0.35v, f=25KHz
~41 nW, 0.8 pJ/bit

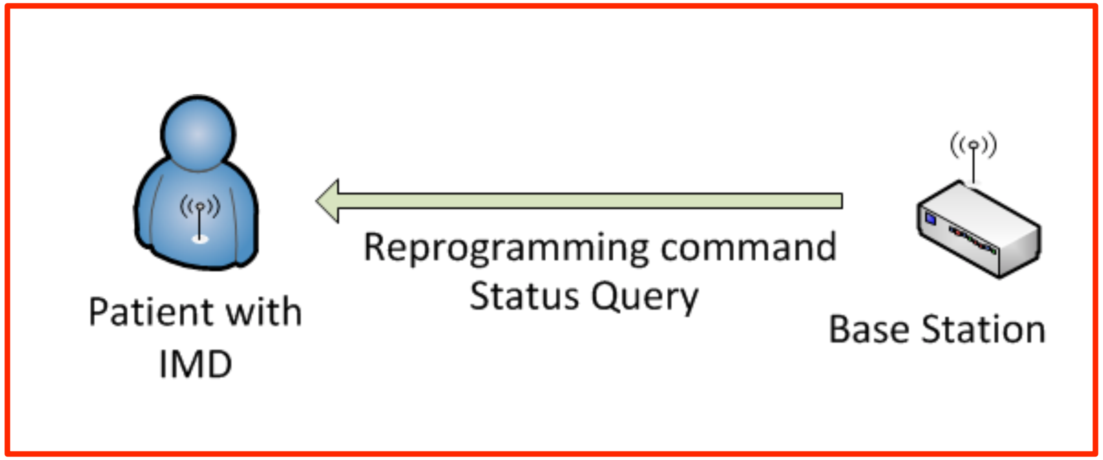
(Simulated 0.18 um TSMC)

65nm, Vdd=0.35v, f=30 KHz
210 nW, 5.8 pJ/bit

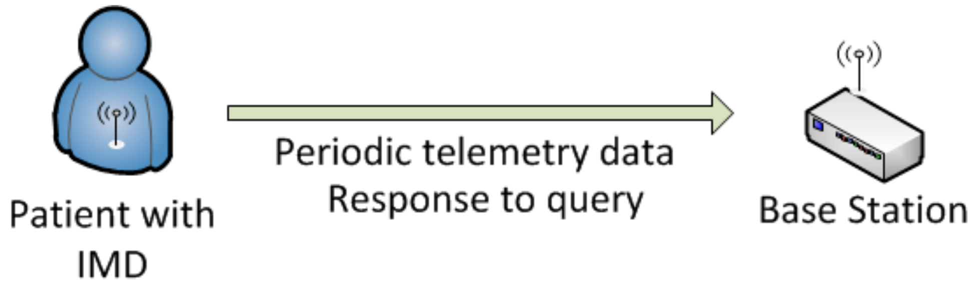
C´edric Hocquet, et al,
JOURNAL OF CRYPTOGRAPHIC ENGINEERING , Feb 2011

Communication Modes

Receive Mode

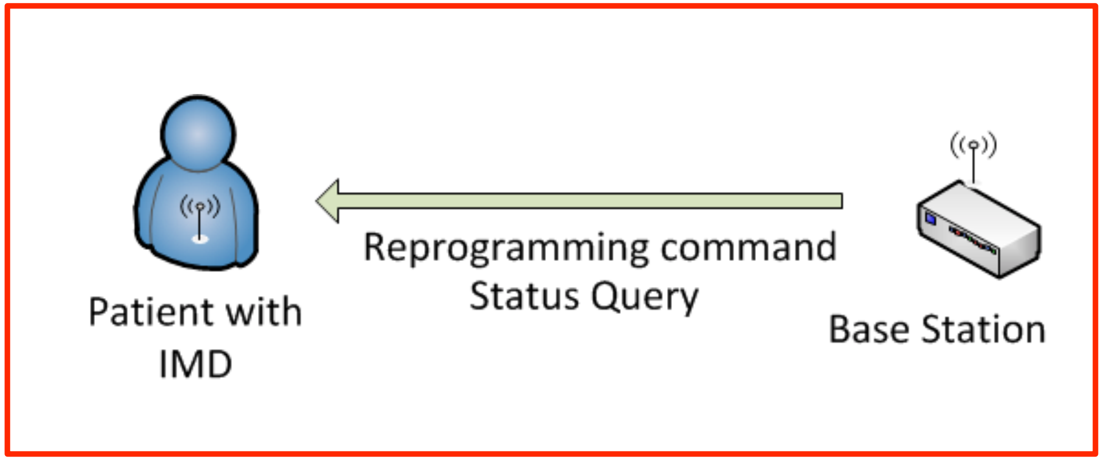


Transmit Mode



Lightweight Protocol

Receive Mode



Registers

IMD Serial number: S (32 bits)

Anti-replay counter: A

Secret Key: K (80 bits)

Received message: X (64 bits)

IMD Serial number: S (32 bits)

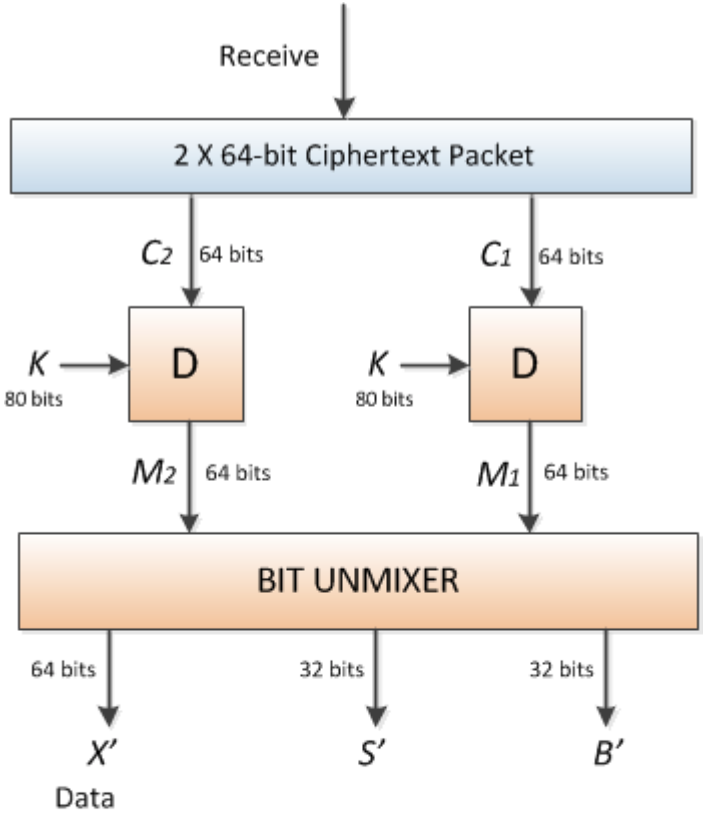
Anti-replay counter: B

Secret Key: K (80 bits)

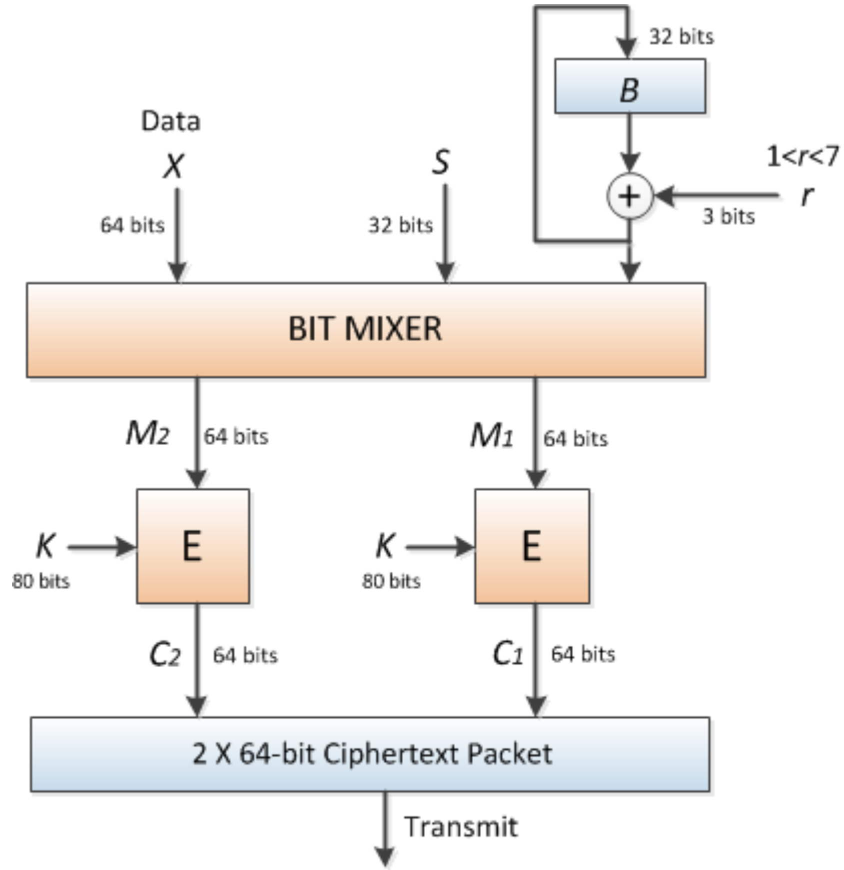
Sent message: X (64 bits)

Lightweight Protocol

Receive Side



Transmit Side



Validity condition: $X=X'$ if ($S=S'$) AND ($B'>A$)

Counter Advancement: If valid then A = B’

Lightweight Protocol

BIT MIXER does the following:

$\{ B_O, B_E \} \leftarrow \text{deInterleave}(B)$

$\{ S_H, S_L \} \leftarrow \text{split}(S)$

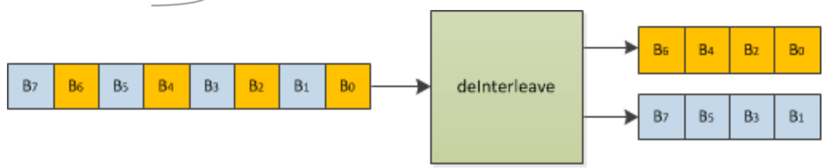
$\{ X_H, X_L \} \leftarrow \text{split}(X)$

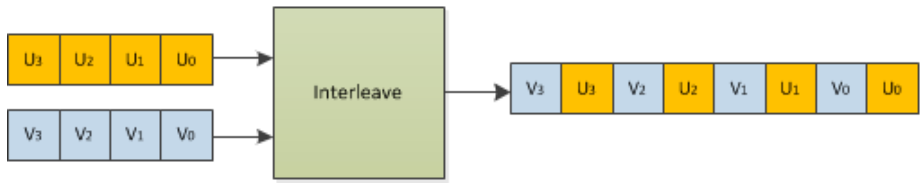
$M_1 \leftarrow \text{Interleave}(X_L, \{ S_L, B_E \})$

$M_2 \leftarrow \text{Interleave}(X_H, \{ S_H, B_O \})$

Only bit permutations

No logic gates required





Required Resources

When Tx and Rx designed as separate modules

Module	Rx	Tx
Cipher module	1 Decryption	1 Encryption
Key register	80 DFF	80 DFF
A/B counter	32 DFF	32 DFF
S register	32 DFF	32 DFF
Data register	64 DFF	64 DFF
32-bit binary comparator	2	0
32- bit adder	0	1
Mux2-1	64	64
Memory	0	0
Total Power (nW)	**~83**	**~77**

Sum = ~160 nW

Subkeys are generated on the fly, so no memory is needed. Otherwise 2560 bits of memory would be needed.

Good

Other Security Challenges

- Denial of Service Attacks:
  - **Jamming**: Adversary blocks communications by transmitting strong signal (noise).
    - Solution: Lightweight UWB? Lightweight Spread Spectrum?
  - **Battery drain**: Adversary keeps IMD receiver frequently busy by sending fake packets.
    - Solution: Energy harvesting for IMD receiver?

Conclusion

- IMD security is vitally important.
- Lightweight IMD security is feasible.
- An example protocol was presented.

Thank you.