Securing Wireless Medical Implants

Shyamnath Gollakota

Haitham Hassanieh
Benjamin Ransford
Dina Katabi
Kevin Fu

Modern Implants Have Wireless

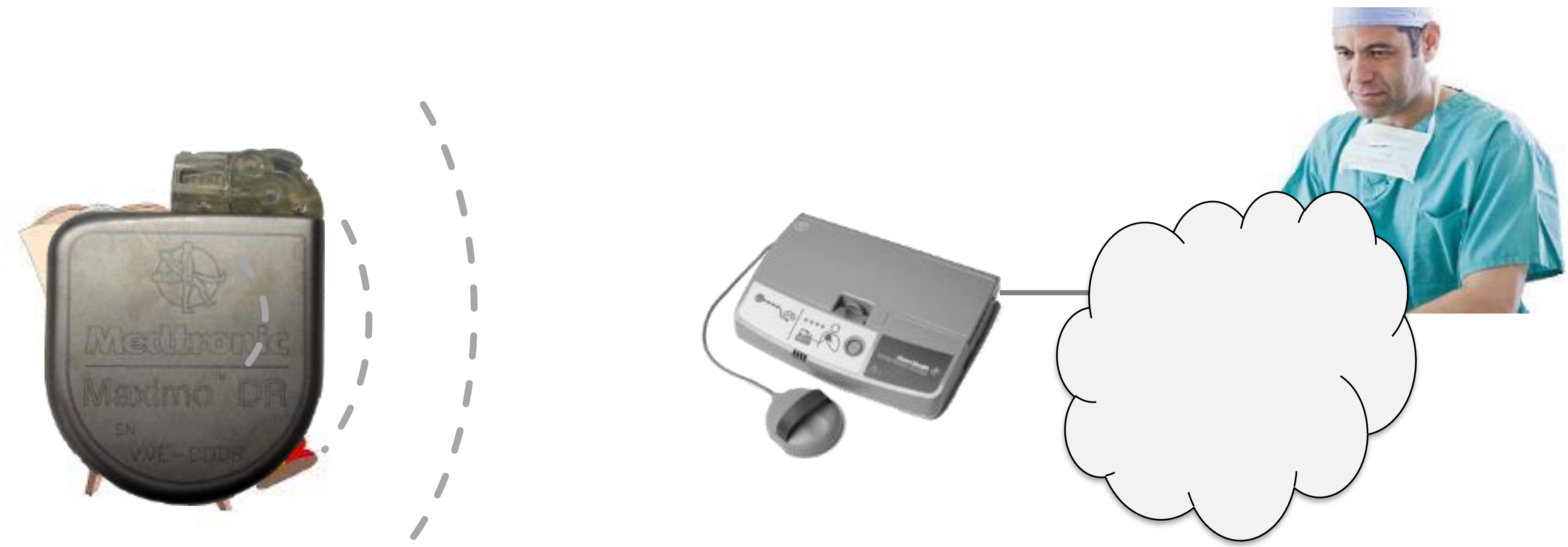
Cardiac Defibrillators

Neurostimulators

Cochlear Implants

Benefits of Wireless

- Easier communication with implant
- Remote monitoring



Benefits of Wireless

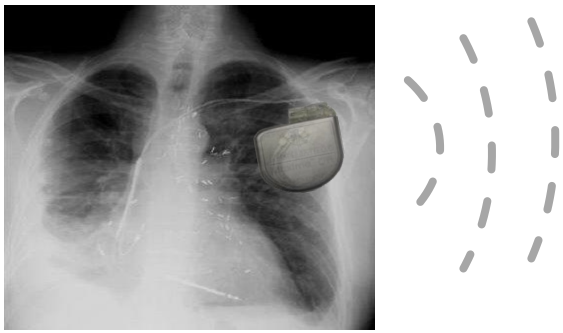
- Easier communication with implant
- Remote monitoring
  - ➢ Reduces hospital visits by 40% and cost per visit by $1800

    [Journal of the American College of Cardiology, 2011]

What about security?

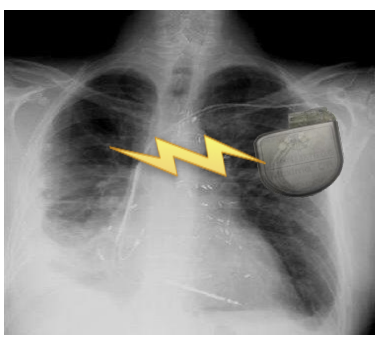
Security Attacks

1) Passive attack: Eavesdrop on private data



Patient diagnosis,
vital signs

2) Active attack: Send unauthorized commands



Turn off therapies,
deliver electric shock

[Halperin'08] demonstrated attacks using software radios

How Do We Protect Against Such Attacks?

Cryptography?

Problems with Adding Cryptography on Implants

- In emergencies, patient may be taken to a foreign hospital where doctors don’t have the secret key

- Millions of patients already have implants with no crypto; would require surgery to replace

Ideally,

Ideally, secure implants **without modifying them**

Delegate security to an **external device**

- In emergencies, doctor turns external device off
- Helps people who already have implants

Solution Idea

Wireless Device

Shield Protects from Active Attacks

Shield Protects from Active Attacks

- Shield listens on medium
- Shield jams unauthorized commands

Implant protected from active attacks

But How to Protect from Passive Attacks?

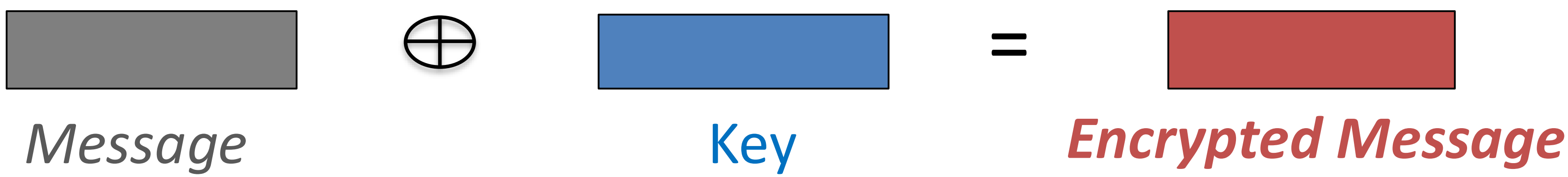
Naïve Sol: Shield jams implant tx so attacker can't decode

How can we prevent eavesdropper from getting data while delivering data to doctor?

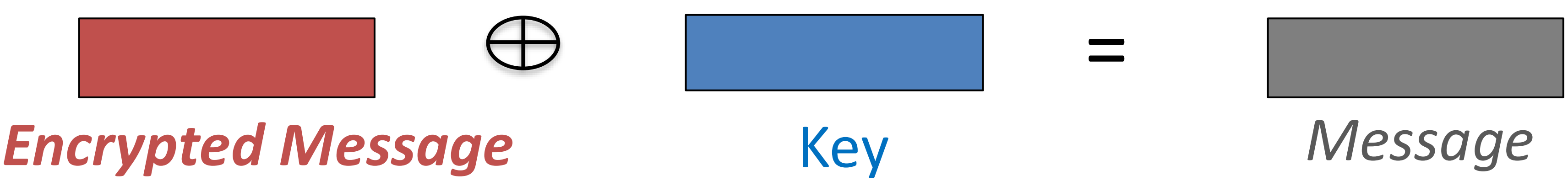
Analog one-time pad

Classic Approach: One-Time Pad

Encryption

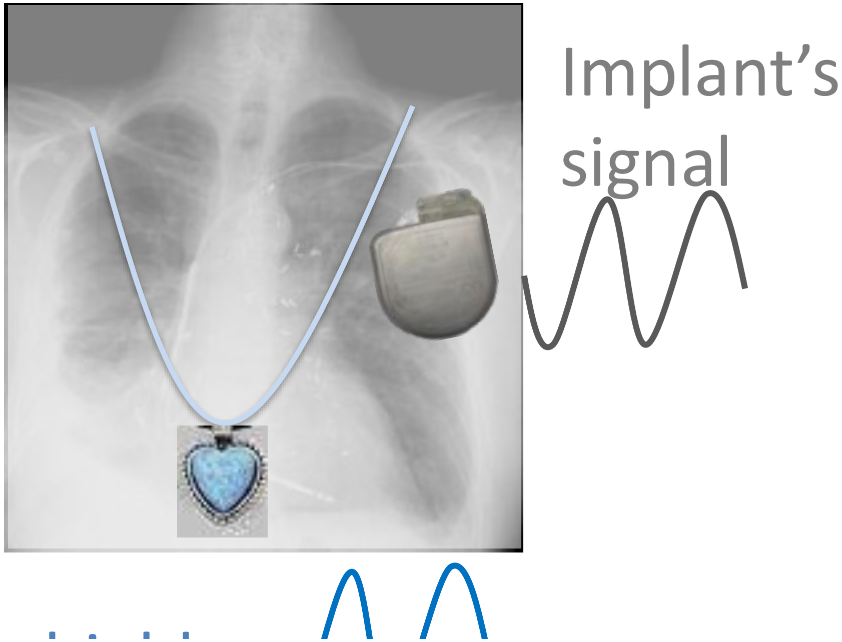


Decryption



Only a node that has the key can decrypt

Protect from Passive Attacks: Analog One-Time Pad

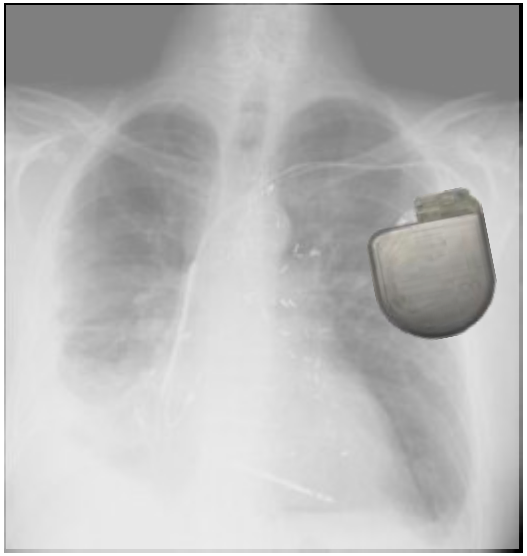


Random
Sum

Jamming signal acts like the key in one-time pad

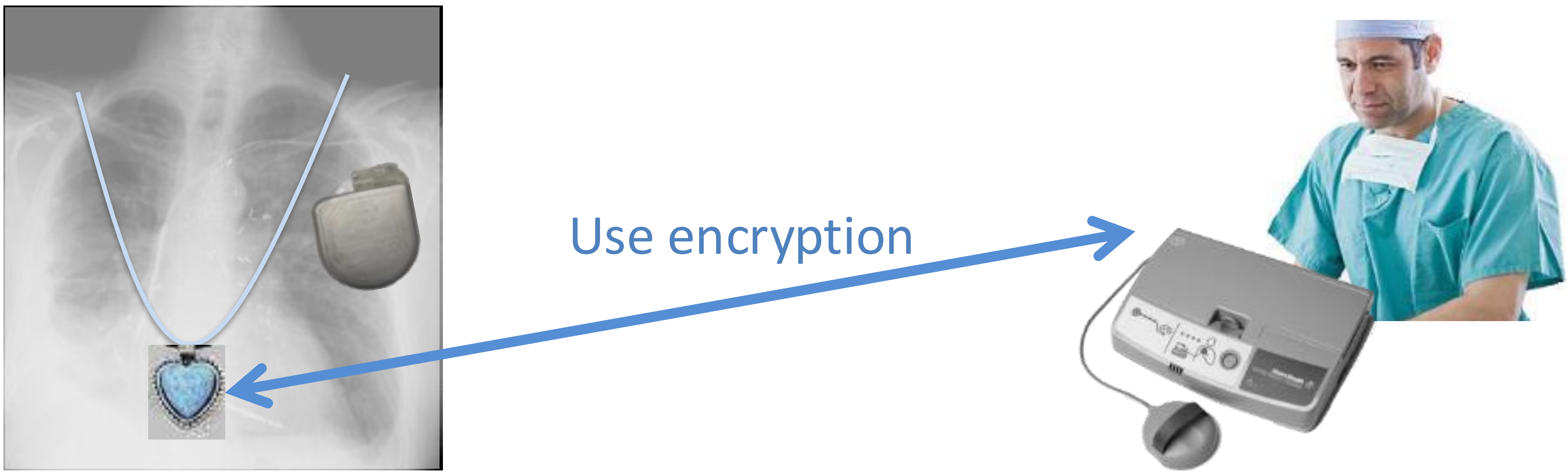
Putting it together

Traditional System



Putting it together

<u>Our System</u>



Shield encrypts the implant data and forwards it to doctor

→ **Shield acts as proxy**

Contributions

- First system that secures wireless implants without modifying them

- Design that simultaneously jams and decodes medical implant transmissions

- Implemented and evaluated using commercial cardiac defibrillators
  - Effective at protecting the implants

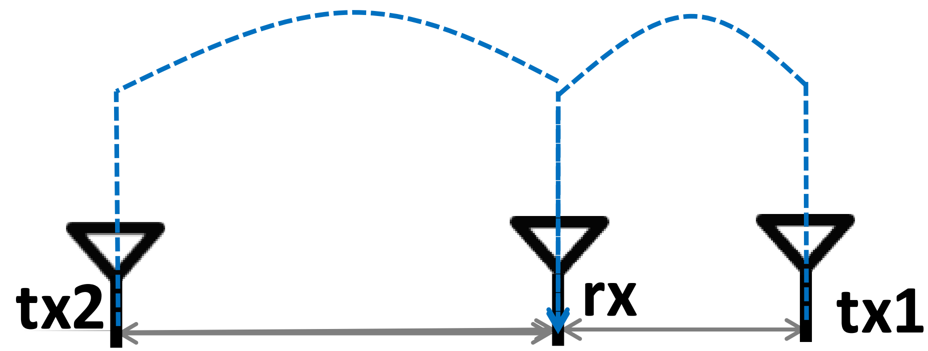
Shield simultaneously:

- Jams the implant's signal
- Decodes the implant's signal

Need radio that transmits and receives simultaneously, i.e., a full-duplex radio

How to Design Full-Duplex for Medical Implants?

Mobicom'2010



$d + \frac{wavelength}{2}$ $d + \frac{wavelength}{2}$ d

Cancel out

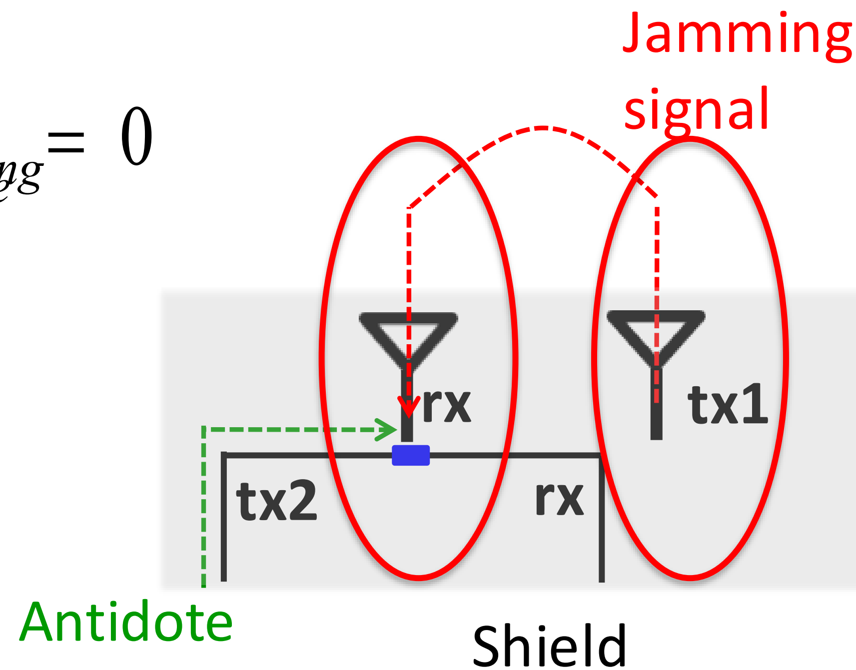
Too large for portable devices

2

Full-Duplex Without Antenna Separation

$$h_{cross} S_{antidote} + h_{self} S_{jamming} = 0$$

$$S_{antidote} = -\frac{h_{self}}{h_{cross}} S_{jamming}$$



- Shield can simultaneously jam and receive
- Design is small and portable

But, Full-Duplex Needs 60–80 dB Cancellation

Reduce signal power by 100 million times

- Requires highly linear components
- Expensive

Can we build shield with significantly less cancellation?

30–40 dB is sufficient!

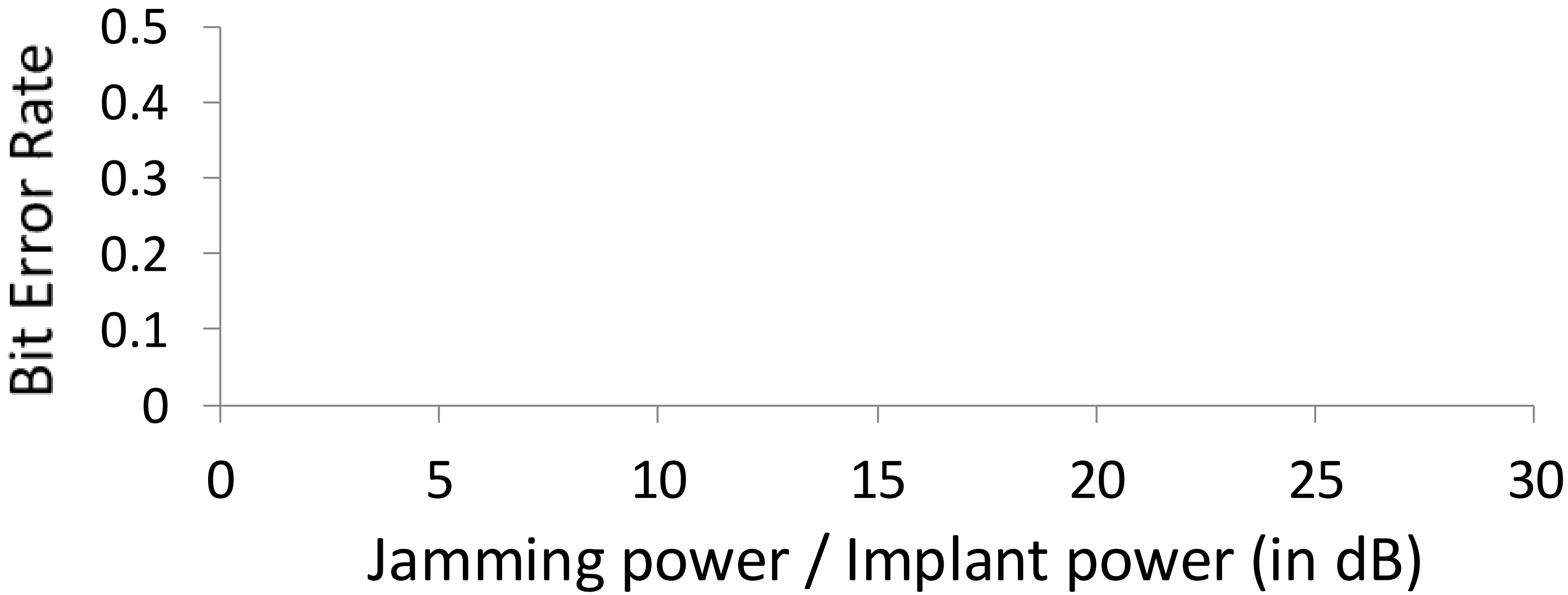
Shield Requirements

Decode Implant's signal

- FSK signal
- Implant signal has a 10 dB SNR

Jam eavesdropper

- 50% bit error rate



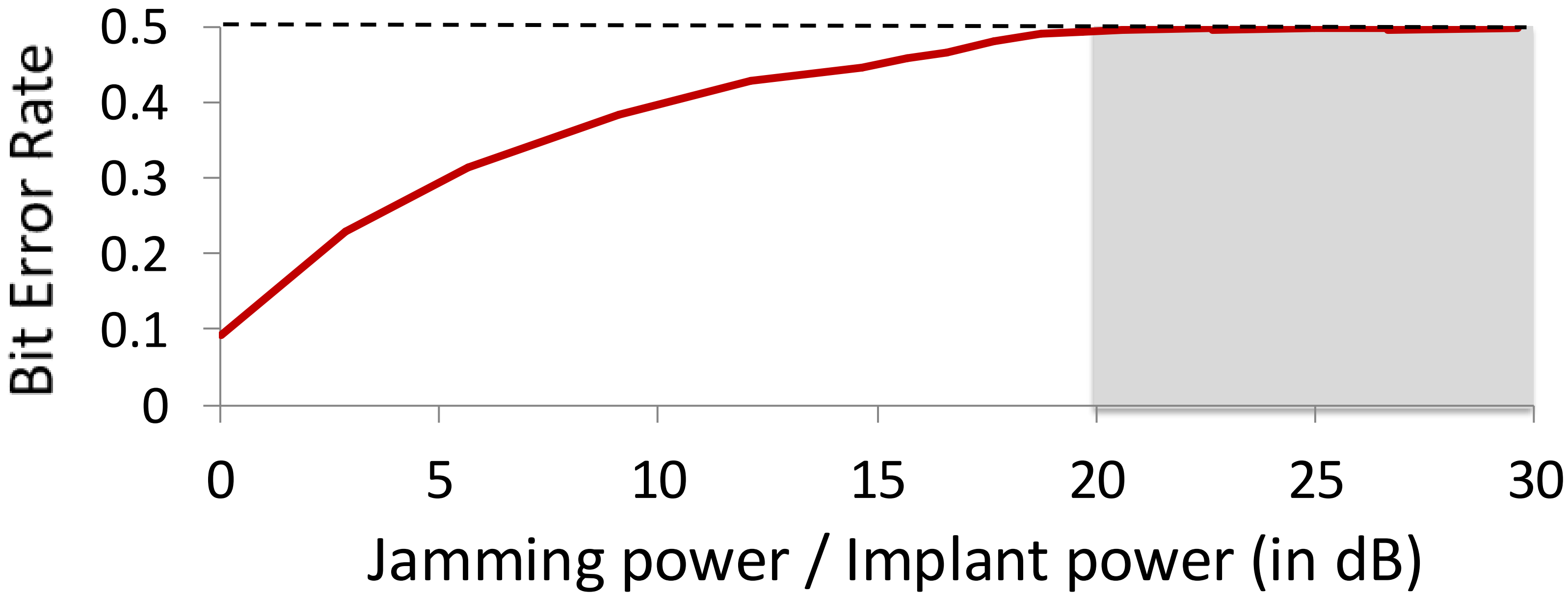
Shield Requirements

Decode Implant's signal

- FSK signal
- Implant signal has a 10 dB SNR

Jam eavesdropper

- 50% bit error rate
- Jamming power 20 dB higher than implant's power



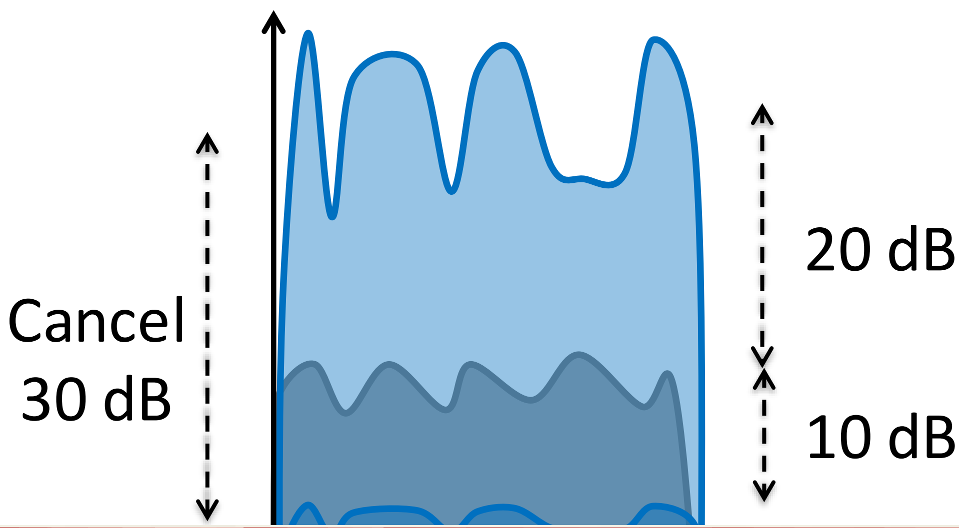
Shield Requirements

Decode Implant's signal

- FSK signal
- Implant signal has a 10 dB SNR

Jam eavesdropper

- 50% bit error rate
- Jamming power 20 dB higher than implant's power



Shield requires only 30 dB cancellation

Empirical Results

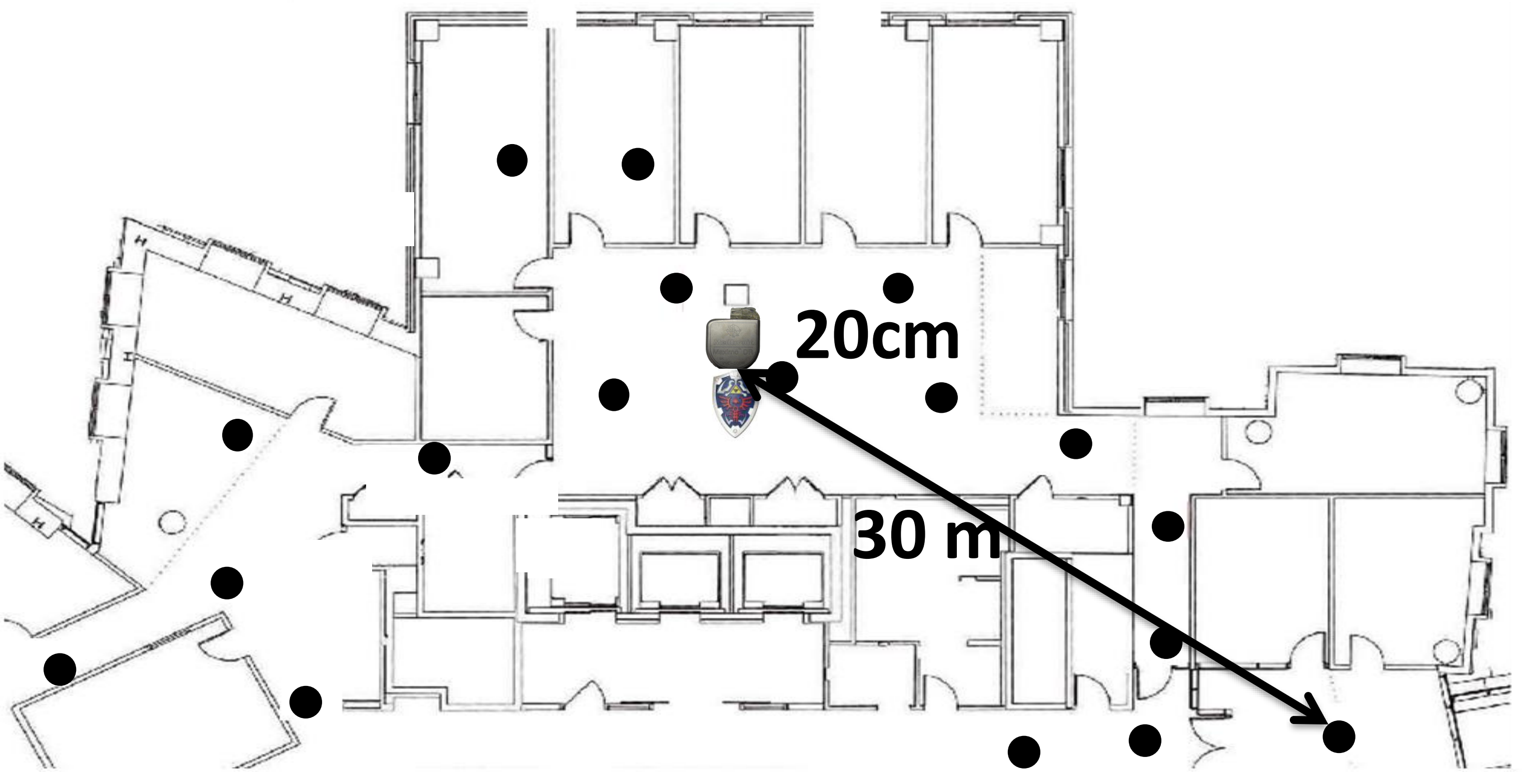
Evaluation

- Medtronic cardiac implants

- Medtronic programmer
- Implement attacker and shield on USRP2s
- Simulate human implantation: bacon & beef

Testbed

- 20-location test bed
- Fix locations of implant and shield
- Node at every other location acts as adversary



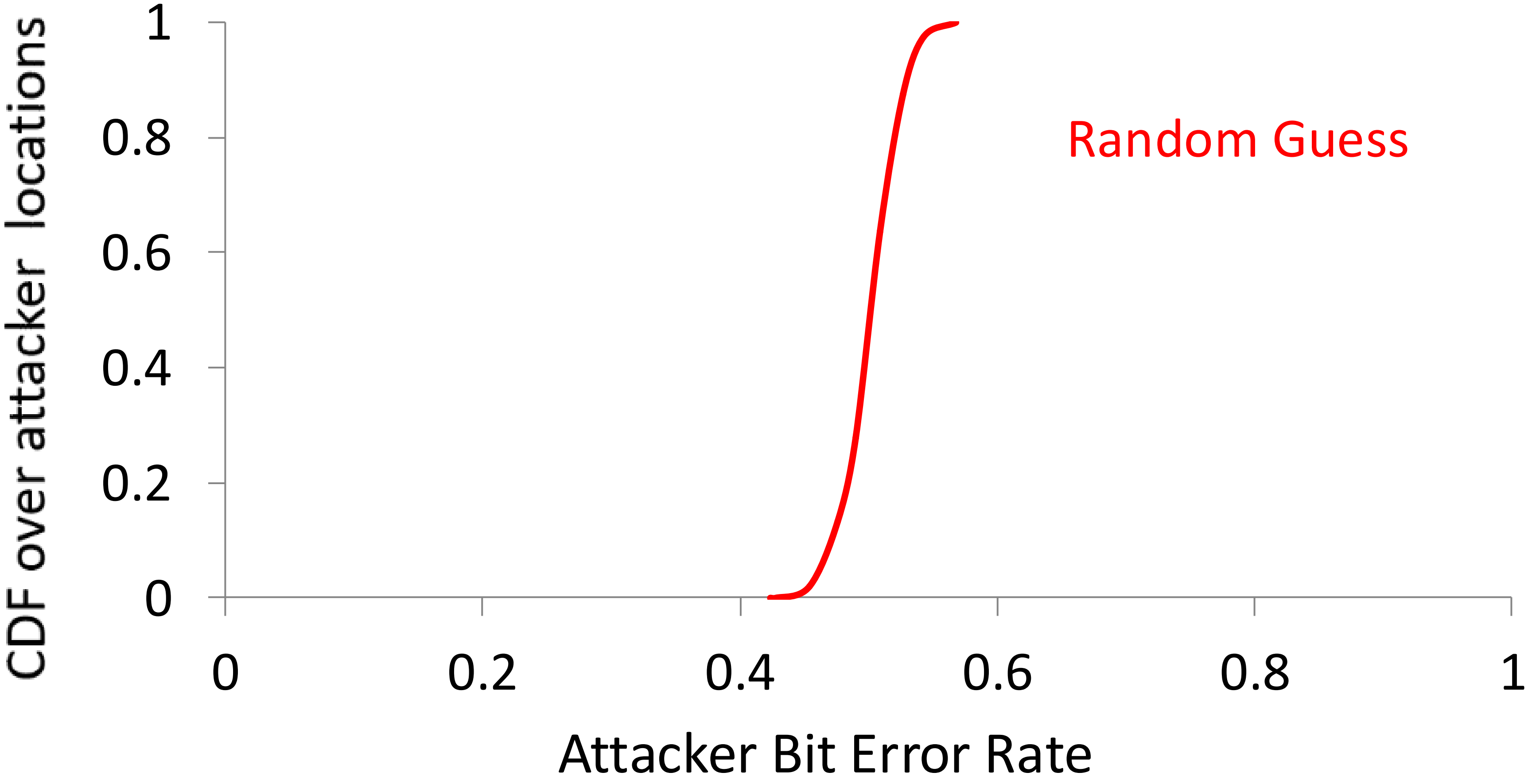
Passive Attacks

Eavesdrop on private data

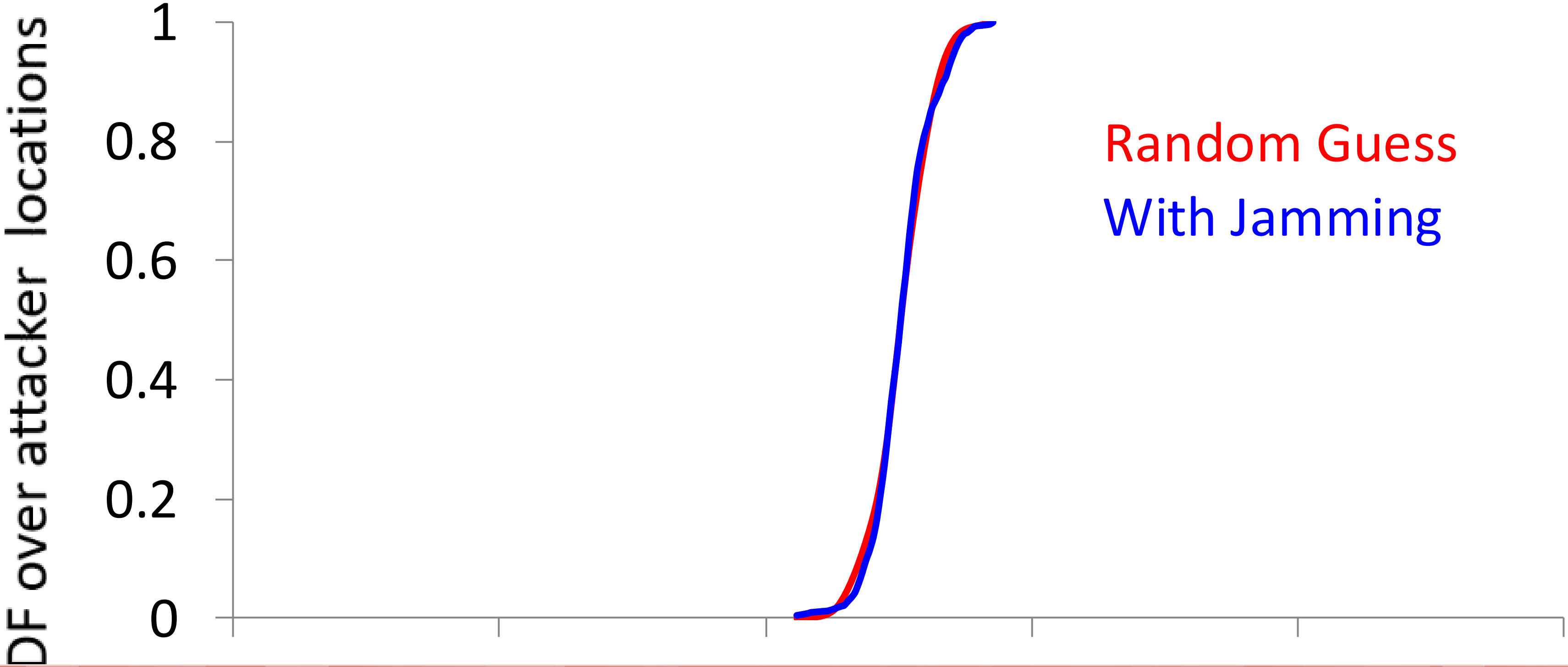
- Decode implant’s transmissions
- Use optimal FSK decoder

Can Eavesdropper do Better Than Random Guess?

Can Eavesdropper do Better Than Random Guess?

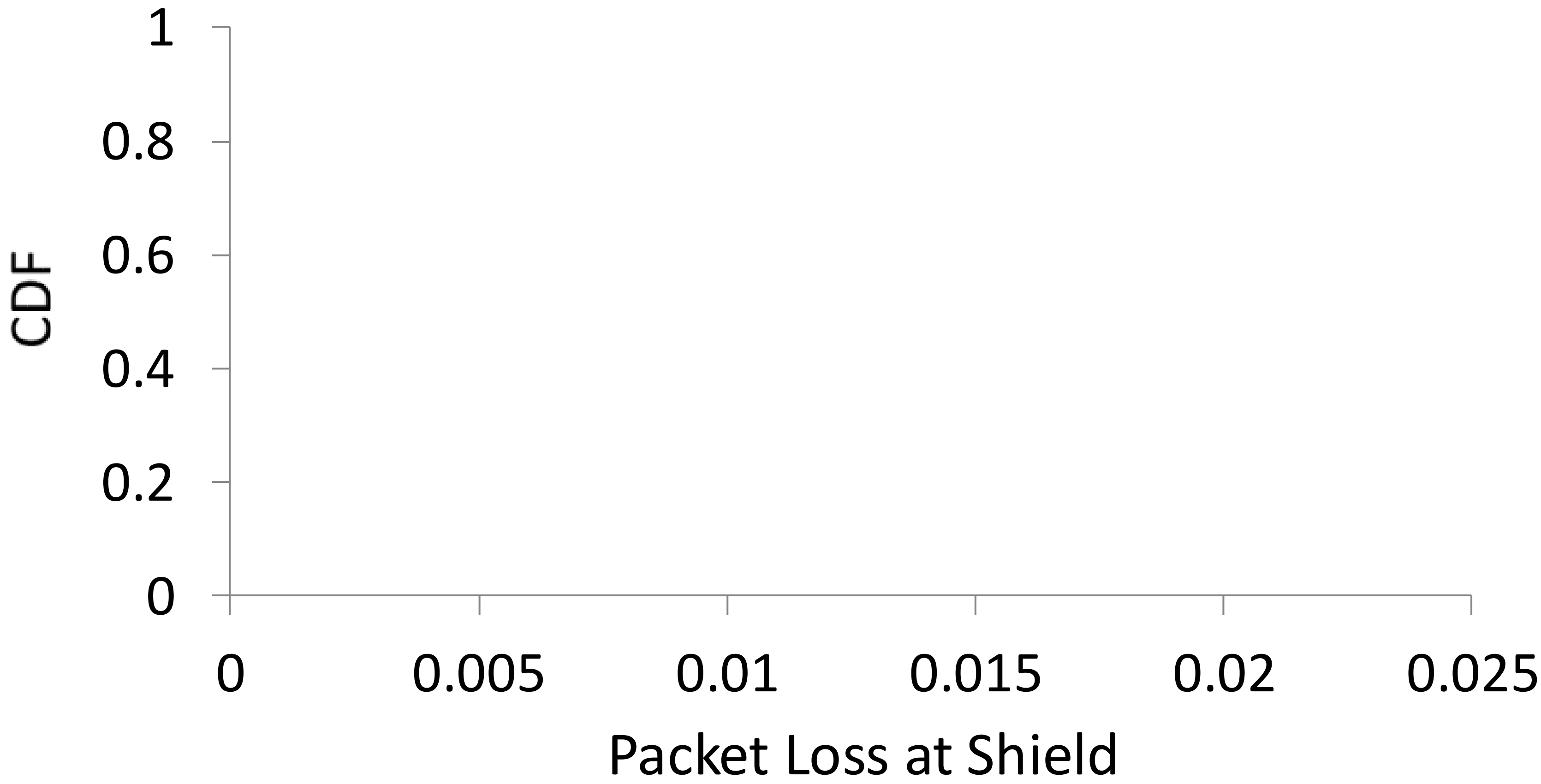


Can Eavesdropper do Better Than Random Guess?

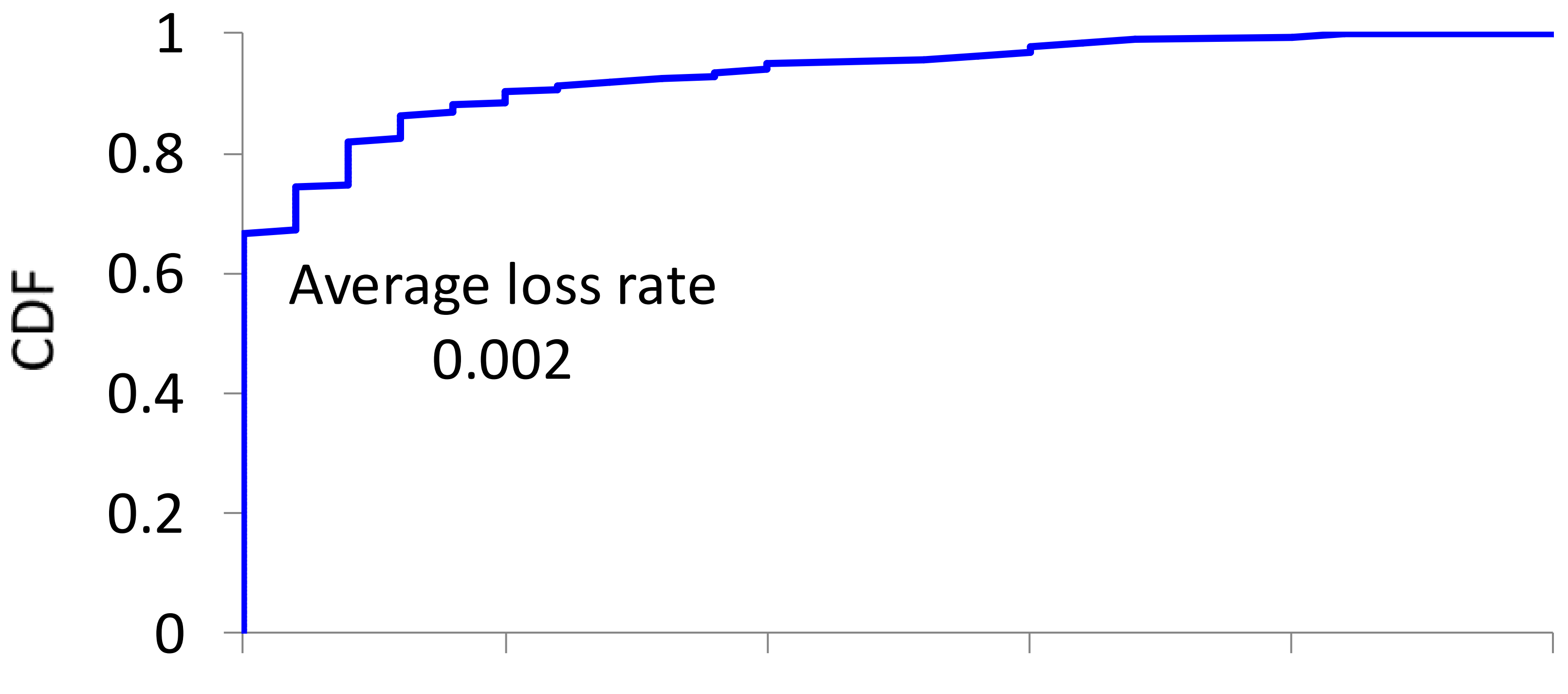


Independent of location, eavesdropper can do no better than a random guess

Can Shield Decode Implant's Messages?



Can Shield Decode Implant's Messages?



Shield can reliably decode the implant's messages, despite jamming

Active Attacks

Send unauthorized commands

- Attacker sends “change therapy”
- Shield jams
- Read implant to check if therapy has changed

Two Types of Active Attacks

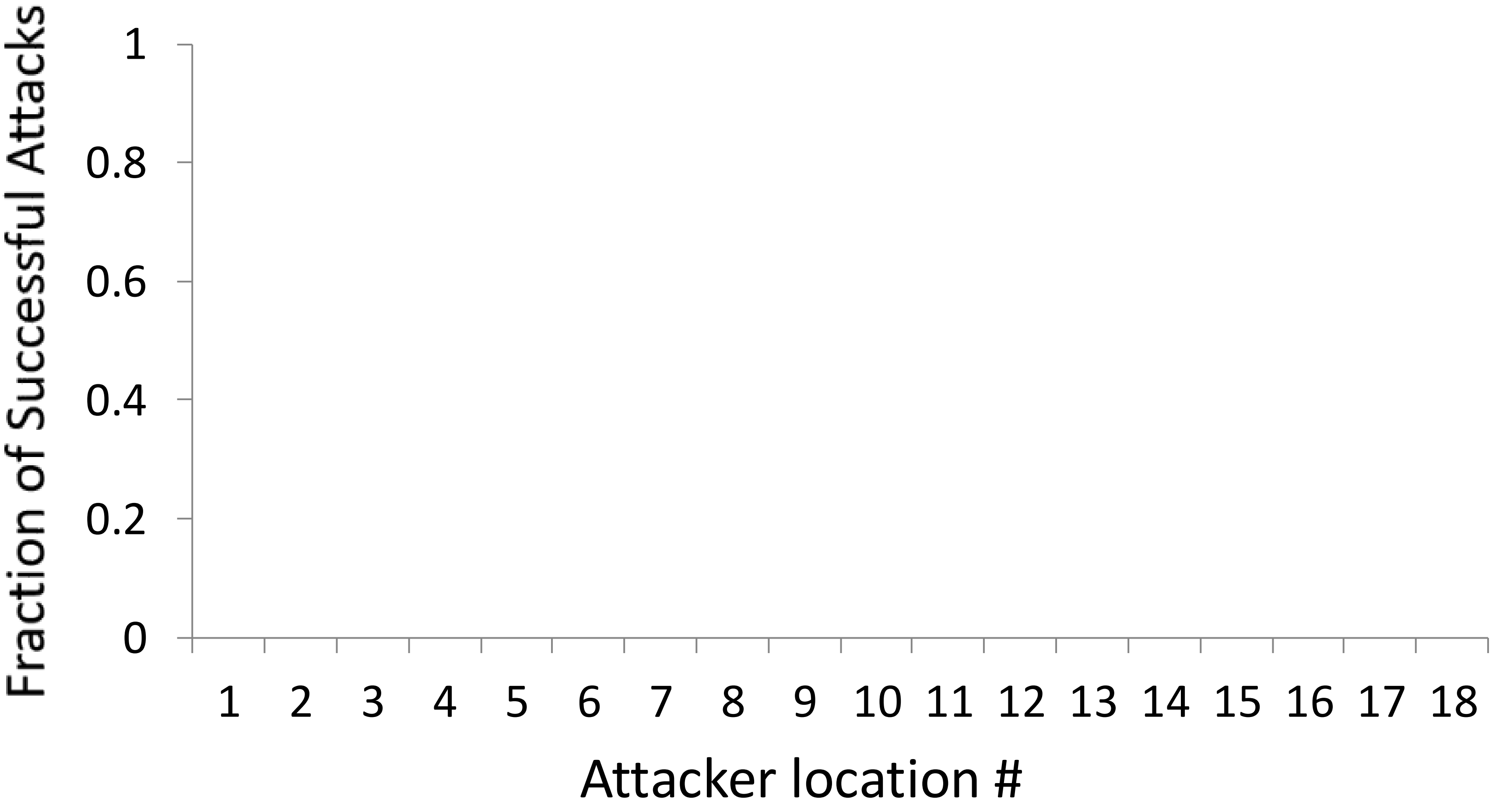
- Off-the-shelf implant programmers

→Same power as our shield

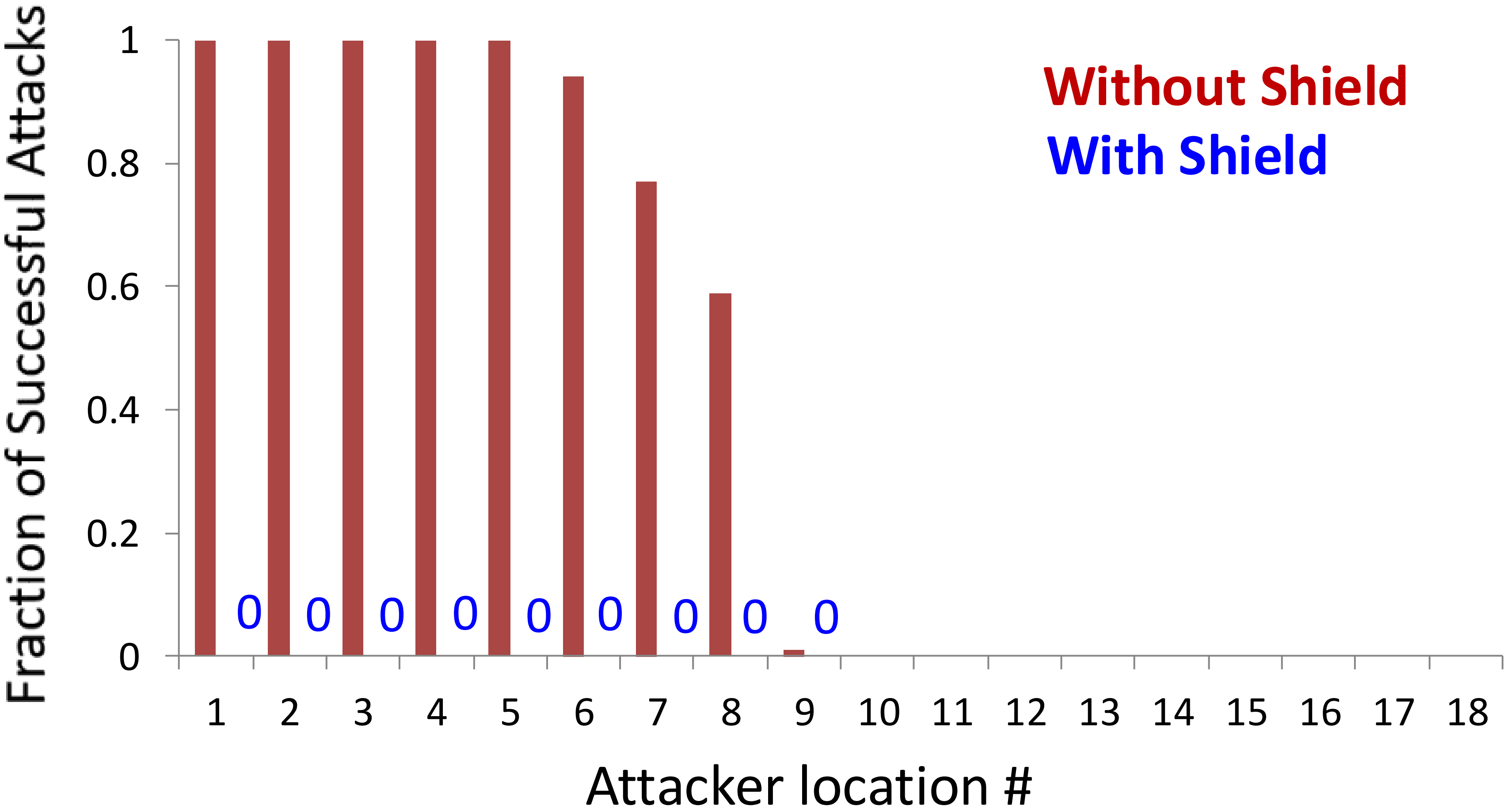
- Customized hardware

→ 100 times the power of our shield

Can Shield Protect Against Unauthorized Programmers?

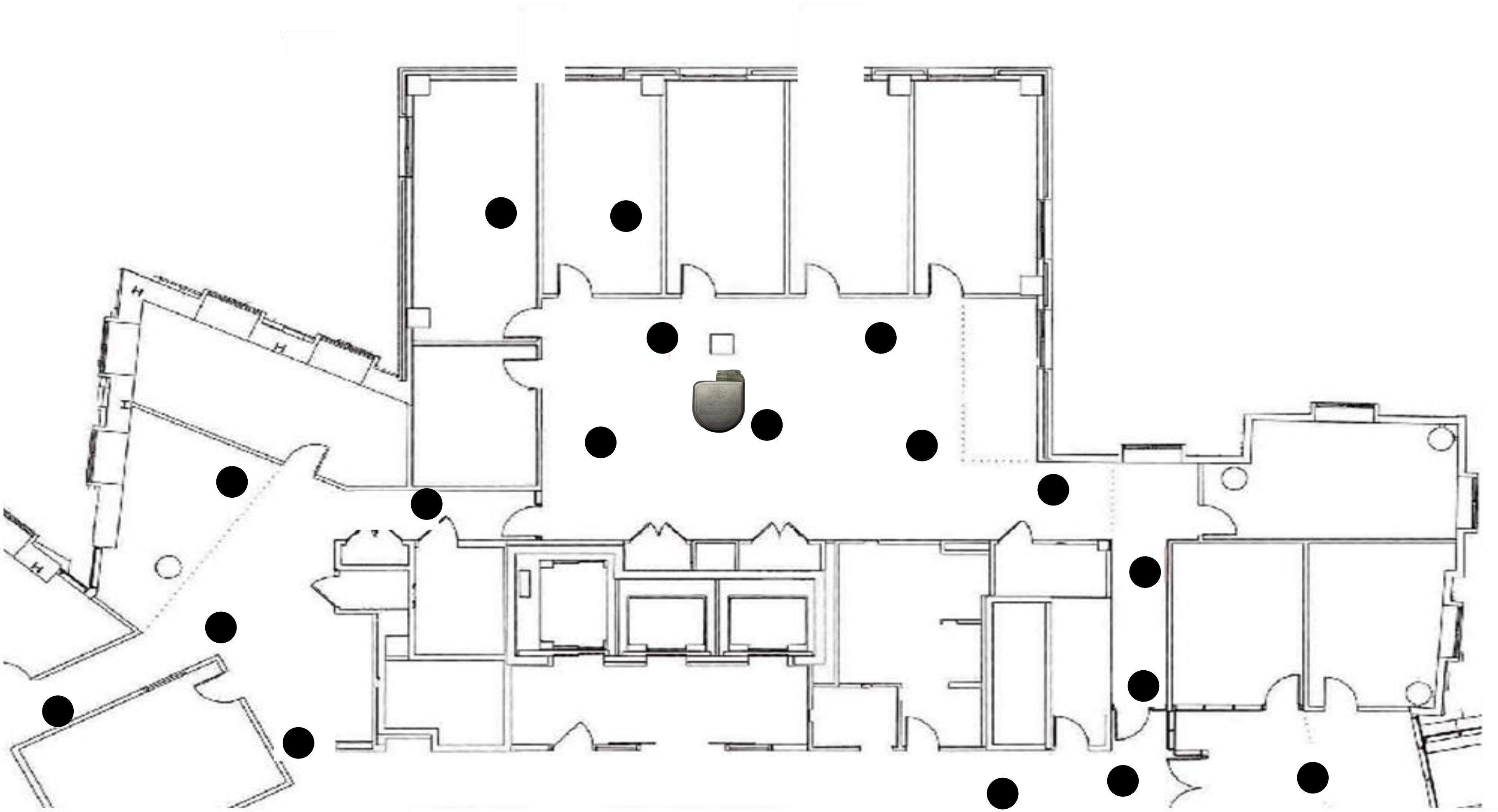


Can Shield Protect Against Unauthorized Programmers?



Can Shield Protect Against Unauthorized Programmers?

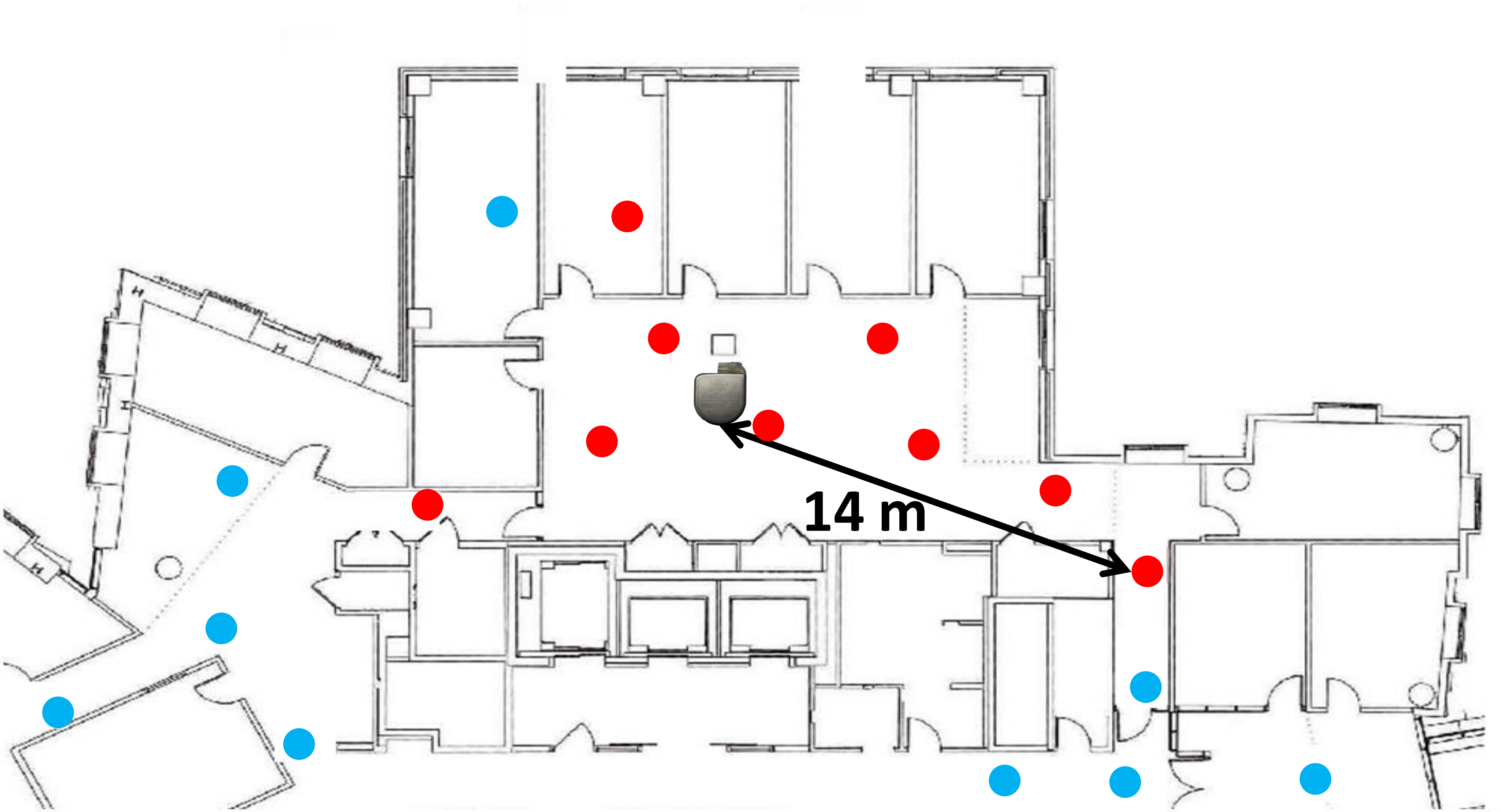
- ● – Any attack successful
- ● – No attack successful



Can Shield Protect Against Unauthorized Programmers?

- – Any attack successful
- – No attack successful

Without the Shield

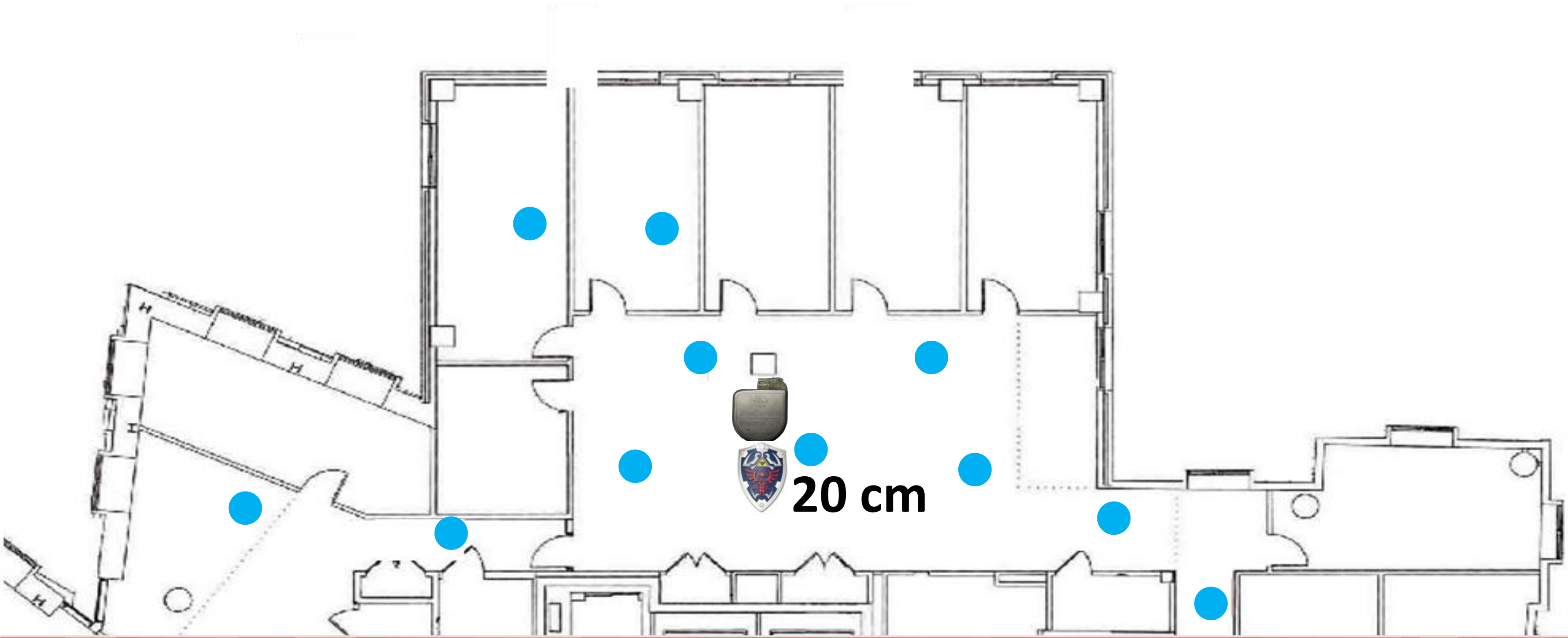


Can Shield Protect Against Unauthorized Programmers?

● – Any attack successful

● – No attack successful

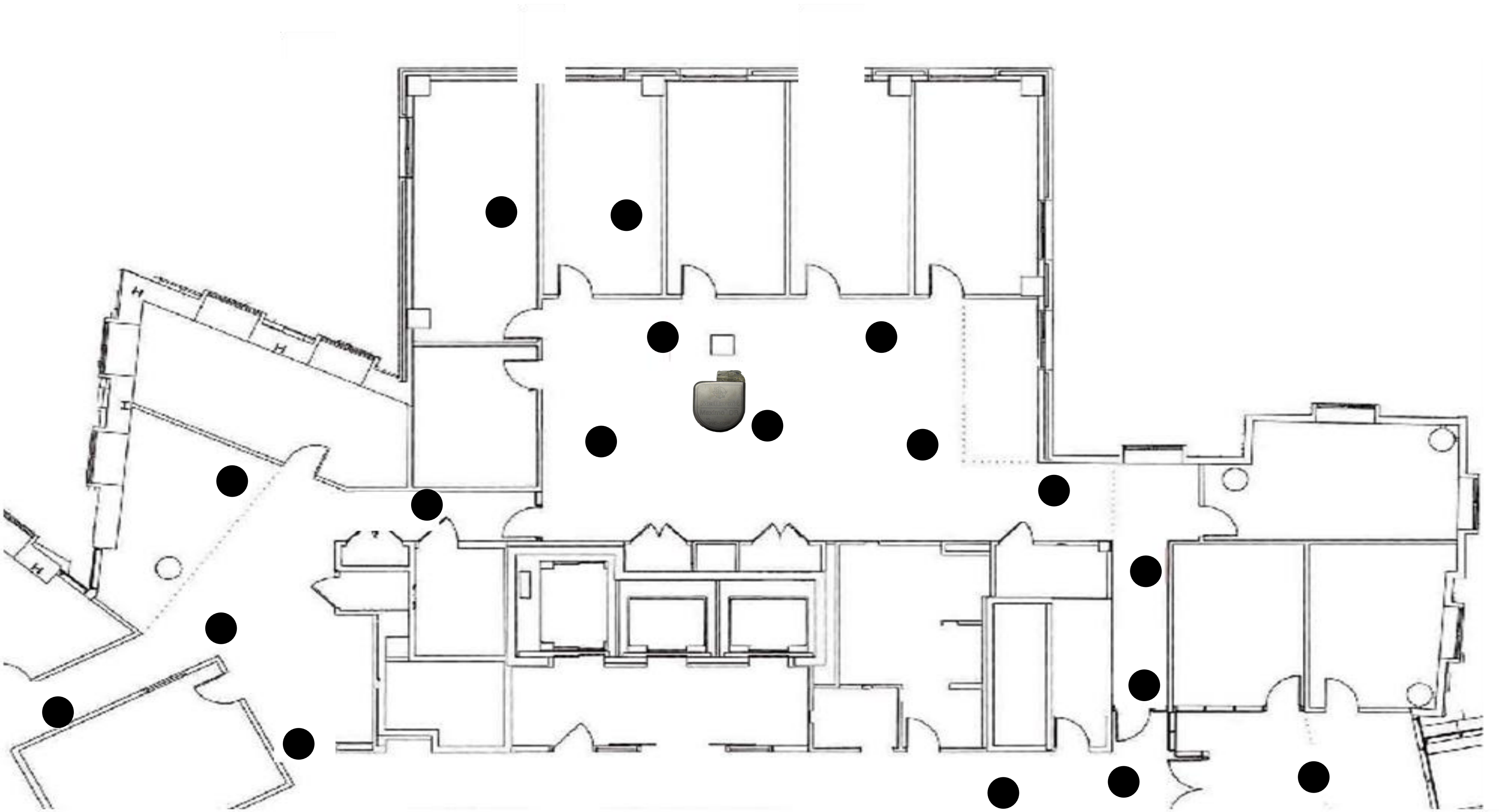
With the Shield



Independent of the location, shield protects from unauthorized programmers

Can Shield Protect Against High-Power Attacks?

- – Any attack successful
- – No attack successful

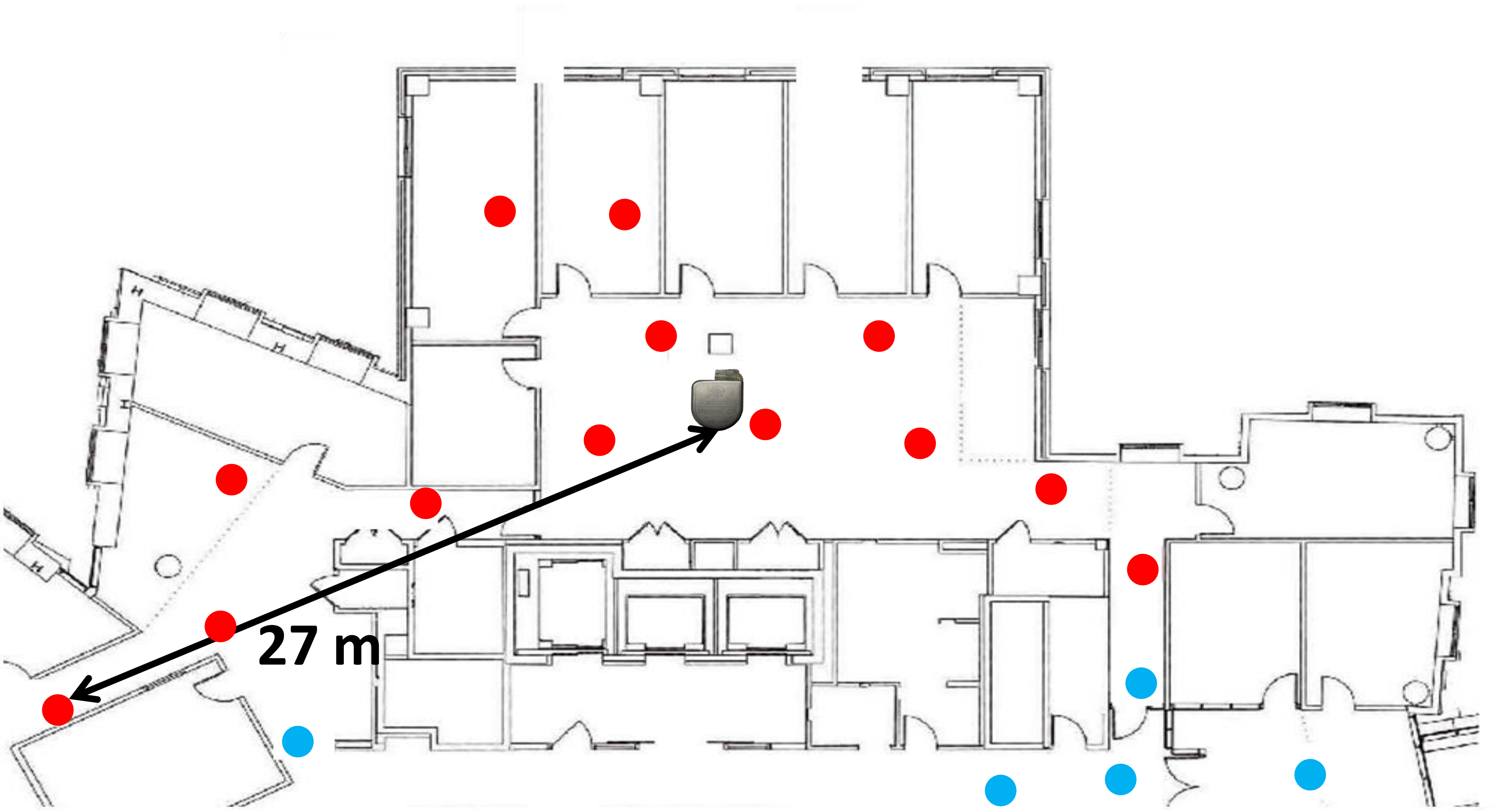


Can Shield Protect Against High-Power Attacks?

- Any attack successful

- No attack successful

Without the Shield

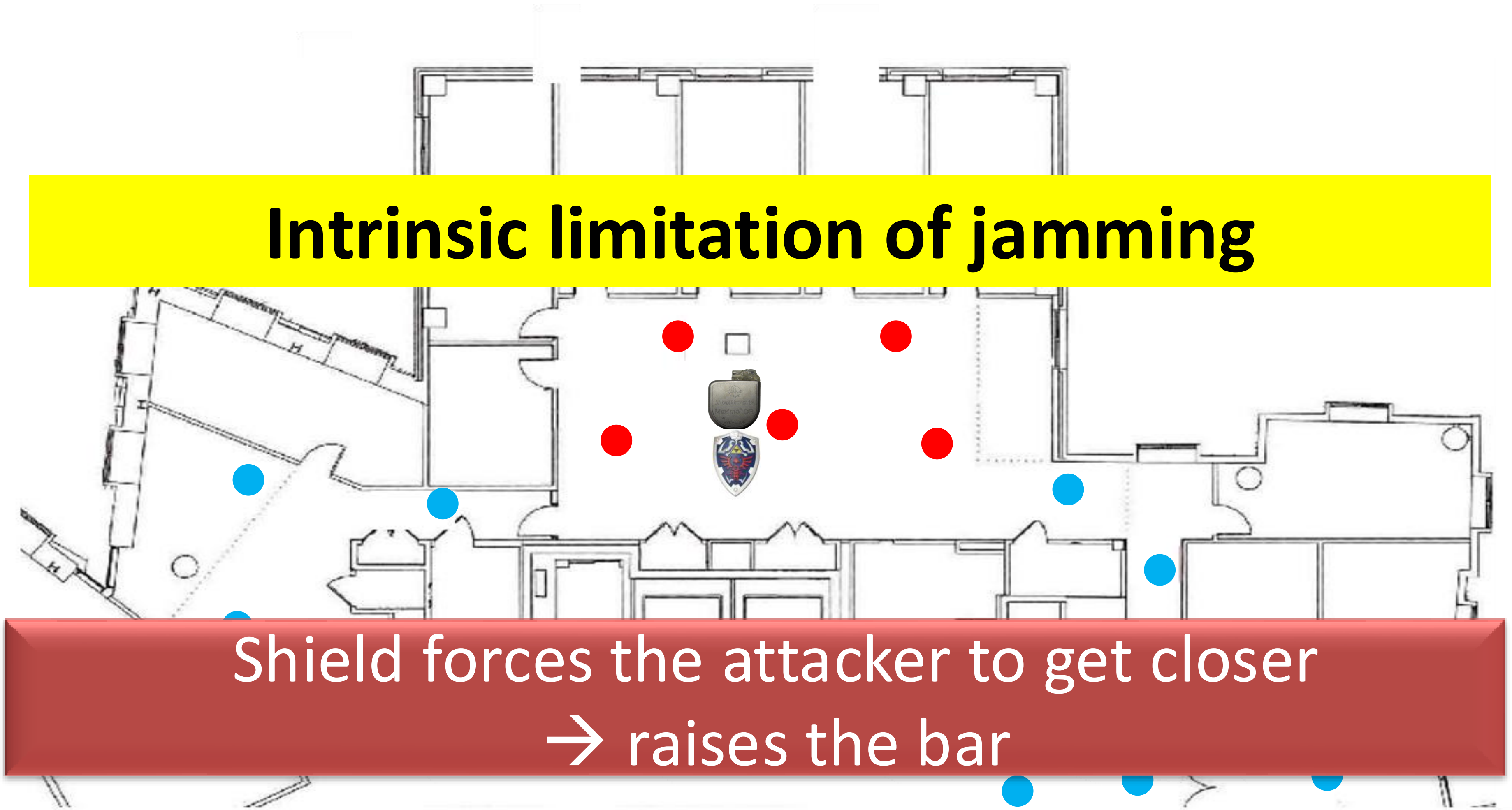


Can Shield Protect Against High-Power Attacks?

- Any attack successful

- No attack successful

With the Shield



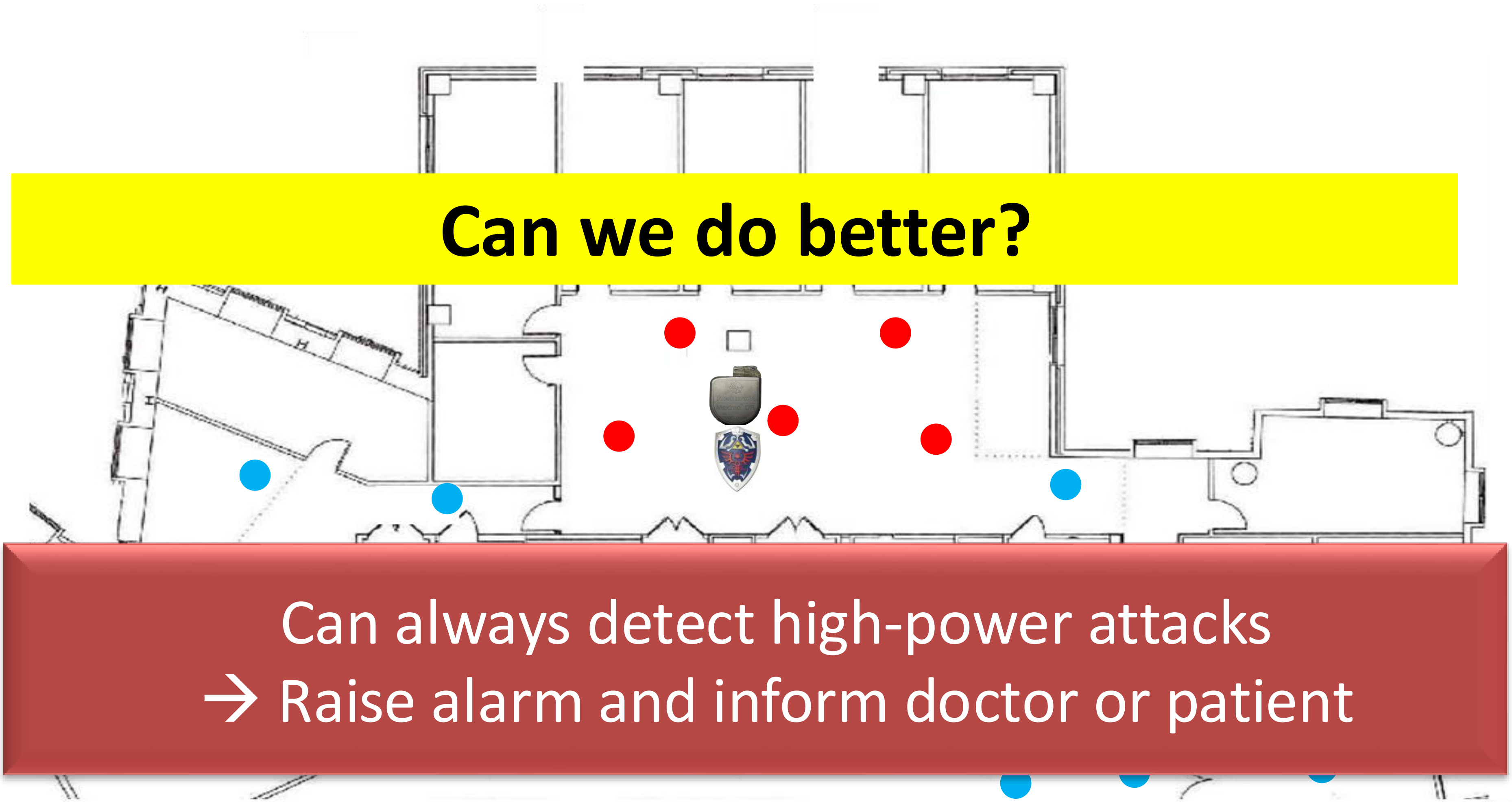
Intrinsic limitation of jamming

Shield forces the attacker to get closer
→ raises the bar

Can Shield Protect Against High-Power Attacks?

- – Any attack successful
- – No attack successful

With the Shield



Can we do better?

Can always detect high-power attacks
→ Raise alarm and inform doctor or patient

Conclusion

- First to secure medical implants without modifying them
- Other applications in RFIDs, small low-power sensors, legacy devices
- Convergence of wireless and medical devices open up new research problems

OPEN MEDICAL DEVICE RESEARCH LIBRARY

www.omdrl.org