On Limitations of Friendly Jamming for Confidentiality

Nils Ole Tippenhauer, Luka Malisa, Aanjhan Ranganathan, Srdjan Capkun
ETH Zurich

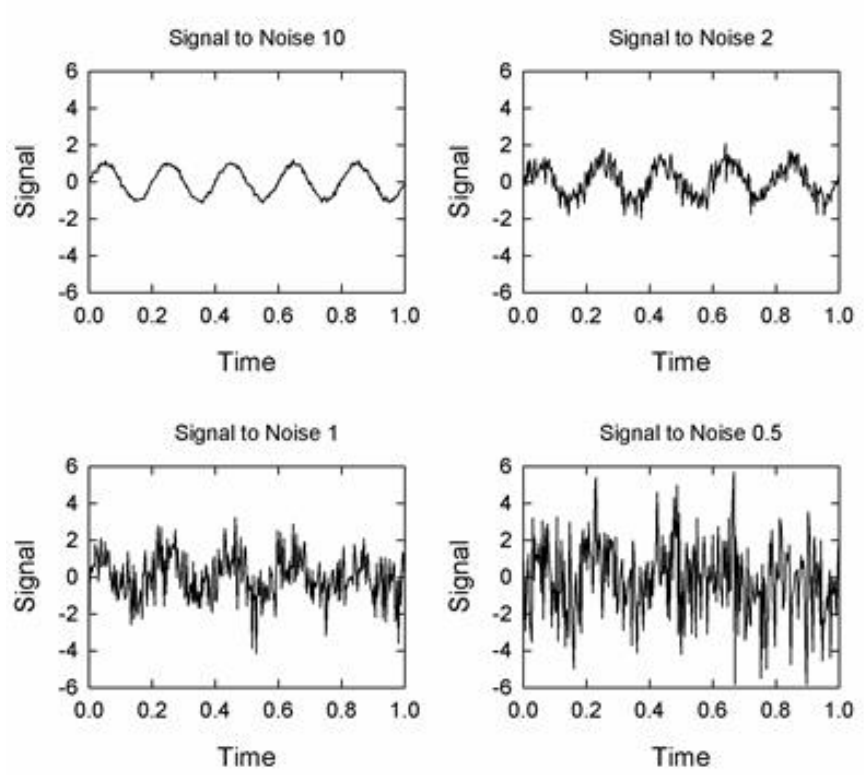
IEEE Symposium on Security and Privacy, 2013

Presenter Junghan Yoon

PPT by Sangmi Noh

INTRODUCTION

- Jamming?



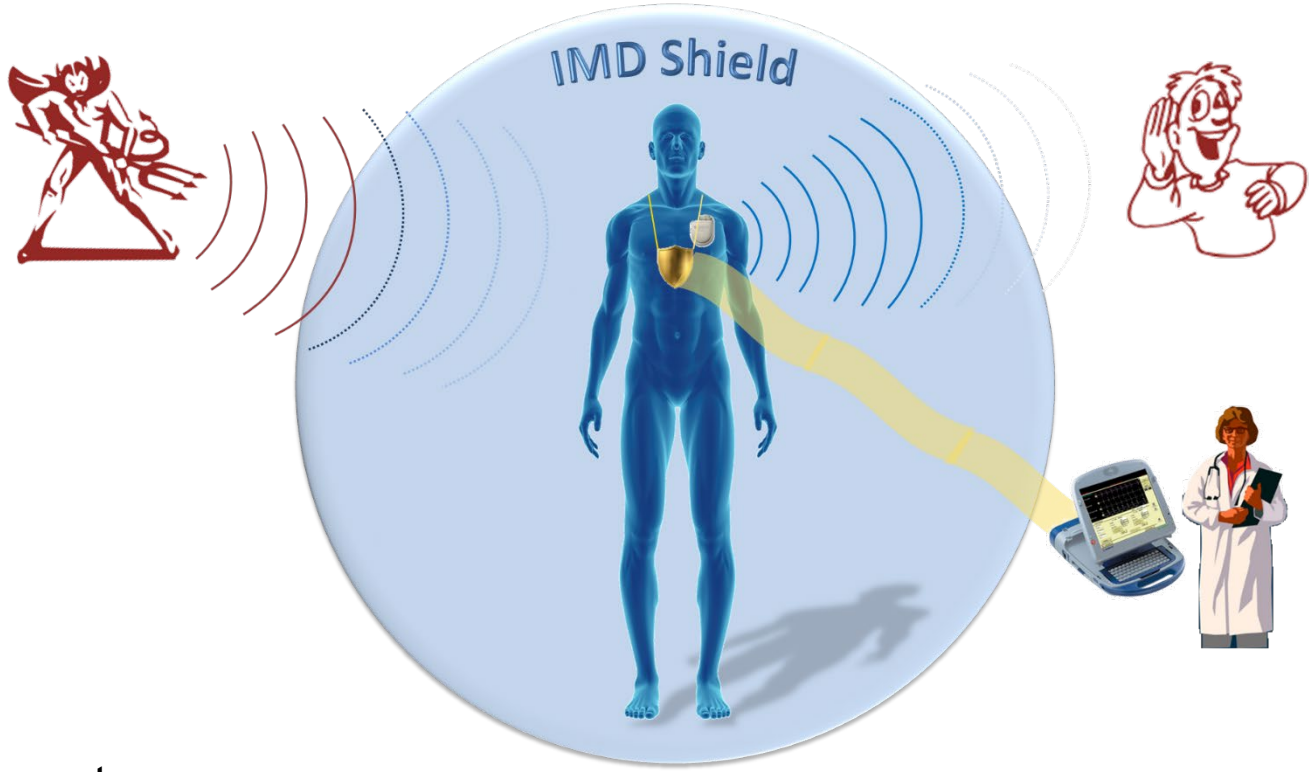
INTRODUCTION

- Target System : Friendly Jamming on IMD (Implatable Medical Device)

"They Can Hear Your Heartbeats: Non-Invasive Security for Implanted Medical Devices", -

SIGCOMM'11 Best Paper Award

- No communication with IMD
- No eavesdropping on IMD's message
- No need to re-implant
- No encryption



- Unfortunately,

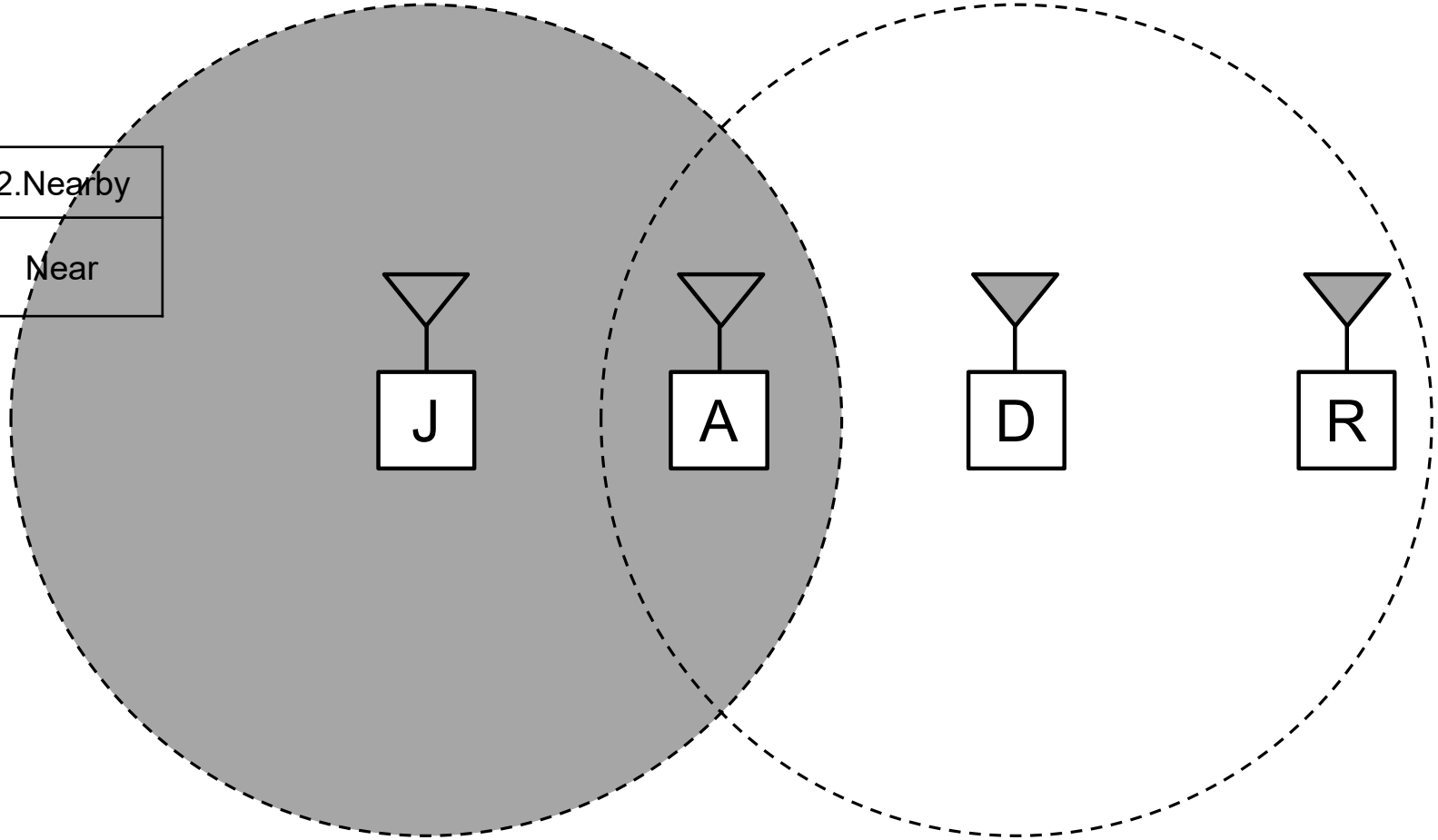
  today's paper showed the limitation of the target paper.

BACKGROUND

- Friendly Jamming Scenario

1. Remote jammer system
2. Nearby jammer system

Jamming type	1.Remote	2.Nearby
Distance Device-Jammer	Far	Near



BACKGROUND

- Previous Work
  - R. Negi and S.Goel, "Secret communication using artificial noise," VTC 2005
  - S.Goel and R.Negi, "Guaranteeing secrecy using artificial noise," IEEE Trans. Wireless Commun., 2008
  - L. Dong, et al., "Cooperative jamming for wireless physical layer security," SSP 2009
  - J. Vilela, et al., "Friendly jamming for wireless security," ICC 2010
  - J. Vilela, et al. "Wireless secrecy regions with friendly jamming," *IEEE Trans. Info. Forensics and Security,* 2011

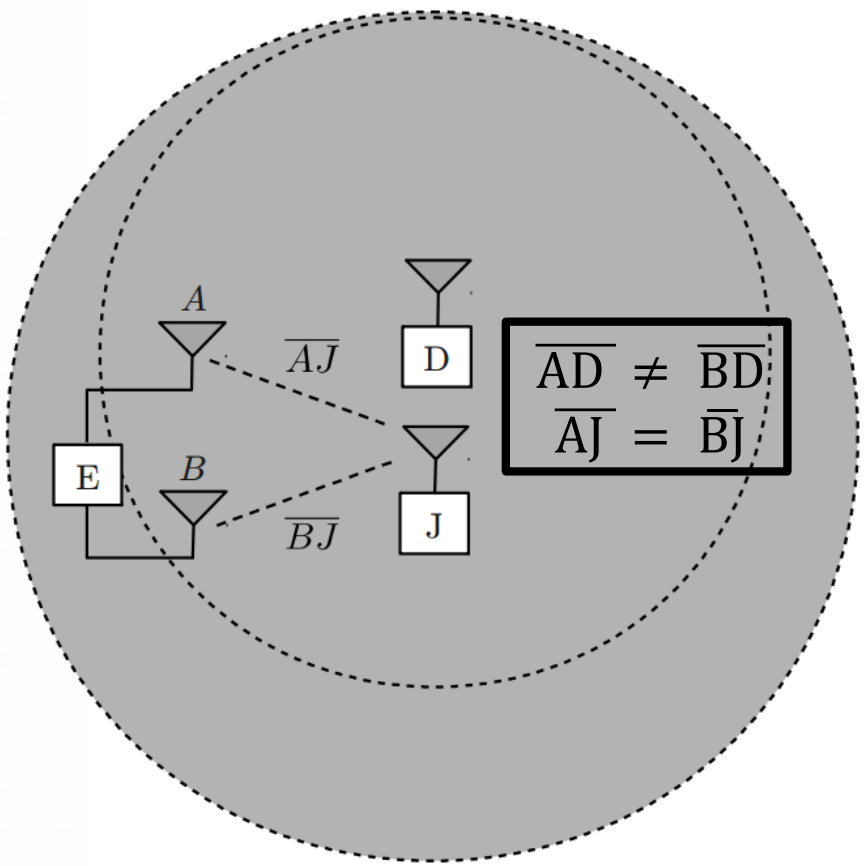
→ Considered only remote jamming, single antenna, passive eavesdropper

Condition

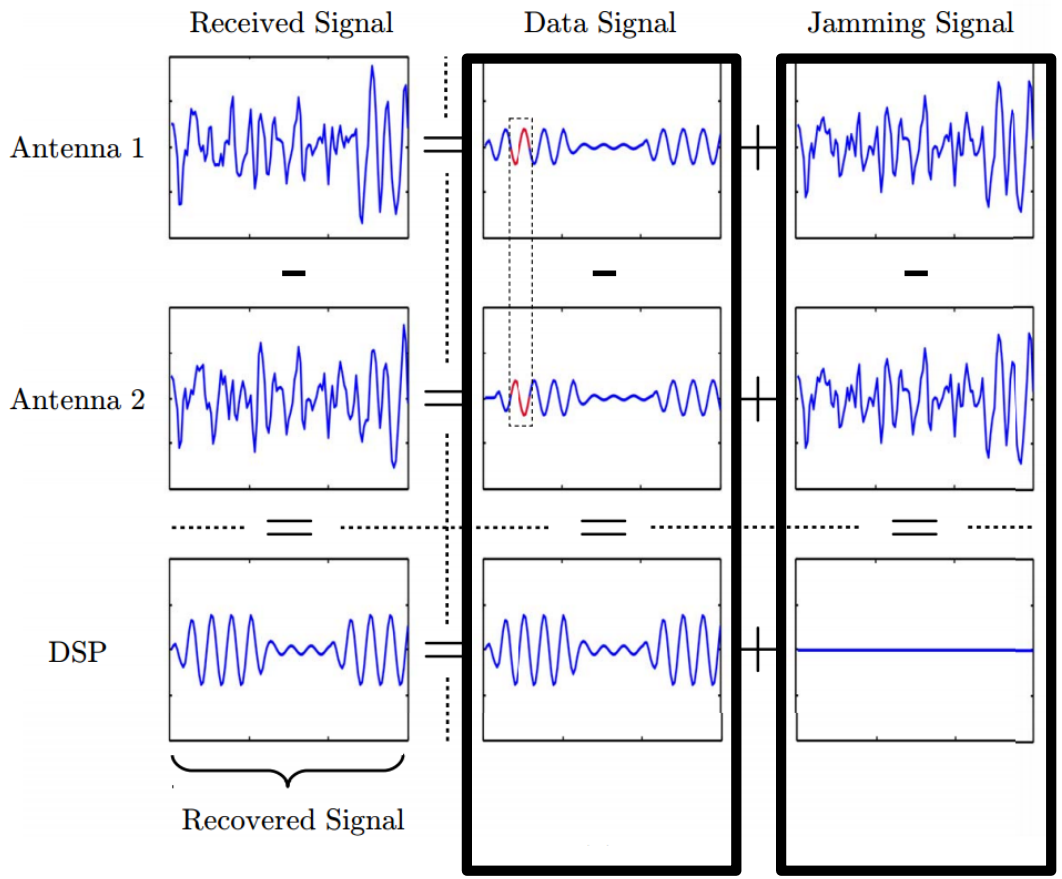
- Nearby Jamming
- 402-405 MHz MICS band (λ =75cm)
→ Strong Attacker

JAMMING MITIGATION USING CHANNEL RESOLUTION

- Friendly Jamming Scenario



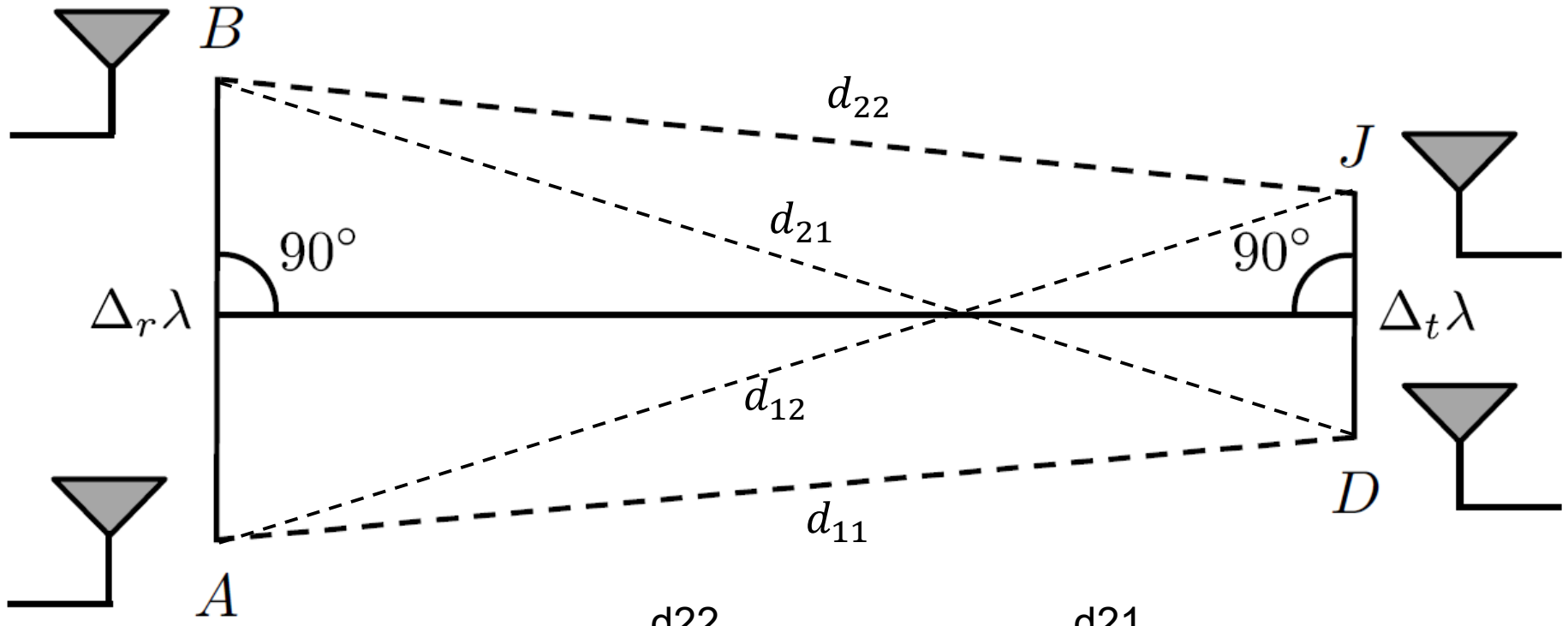
A simplified scenario of our attack



Waveform of signal on antenna A,B

JAMMING MITIGATION USING CHANNEL RESOLUTION

- Geometry of the simulations: isosceles trapezoid



d22 d21

$$H^g = H^m = a \begin{bmatrix} e^{-j2\pi d/\lambda} & e^{-j2\pi d/\lambda} \\ e^{-j2\pi d/\lambda} & e^{-j2\pi d/\lambda} \end{bmatrix} /\lambda$$

Le √ ` ~ ´ e √ ` ~ ´ /λ

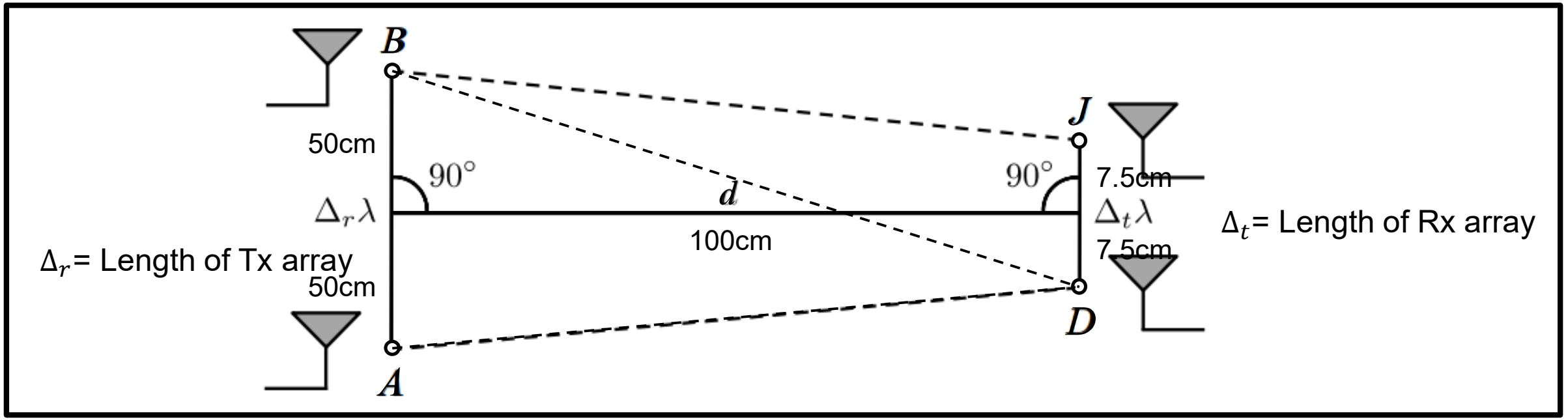
d12 d11

JAMMING MITIGATION USING CHANNEL RESOLUTION

- Geometry of the simulations: isosceles trapezoid

→ Investigated the performance for

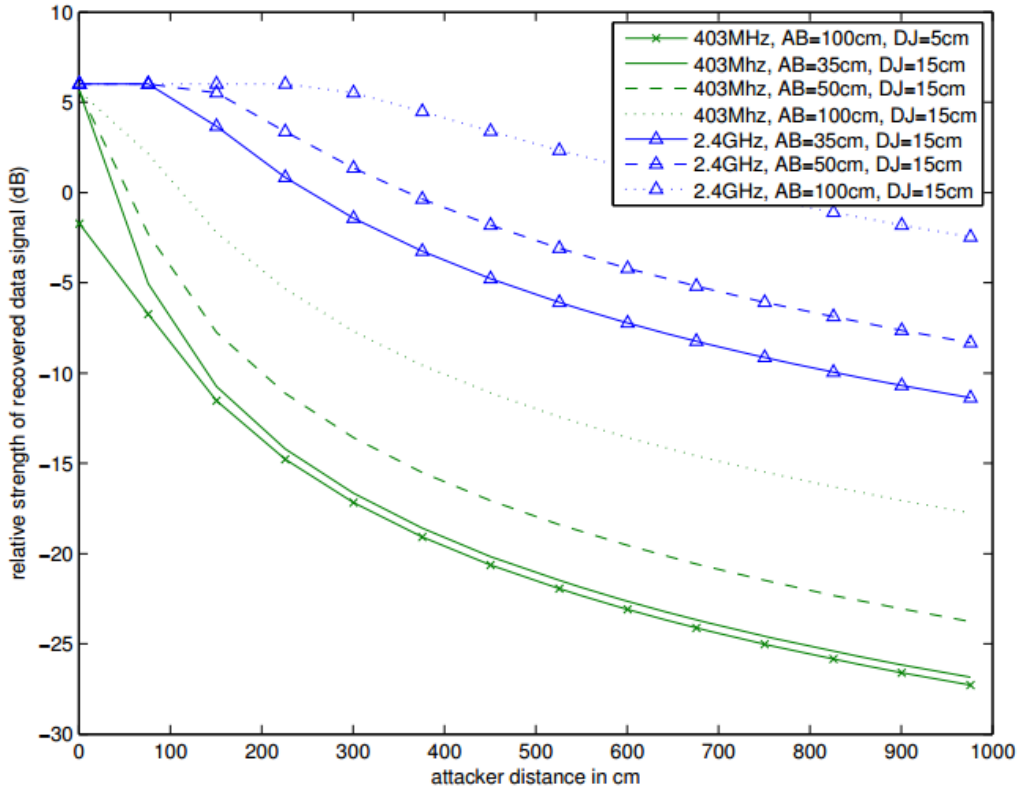
DJ : 5cm, 15cm, 30cm
AB : 35cm, 50cm, 100cm
Band : MICS, ISM



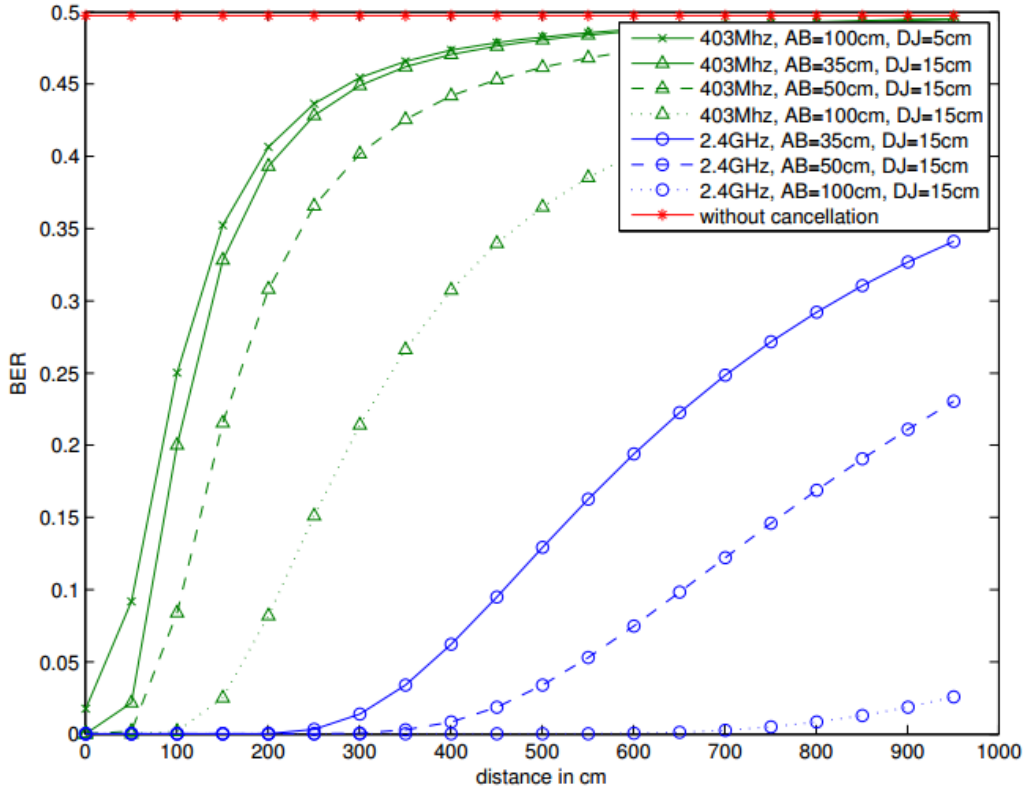
$$\delta = \overline{DB} - \overline{DA} = \sqrt{(50+7.5)^2 + 100^2} - \sqrt{(50-7.5)^2 + 100^2} = 6.7cm(\sim\frac{\lambda}{10})$$

JAMMING MITIGATION USING CHANNEL RESOLUTION

- Simulations result



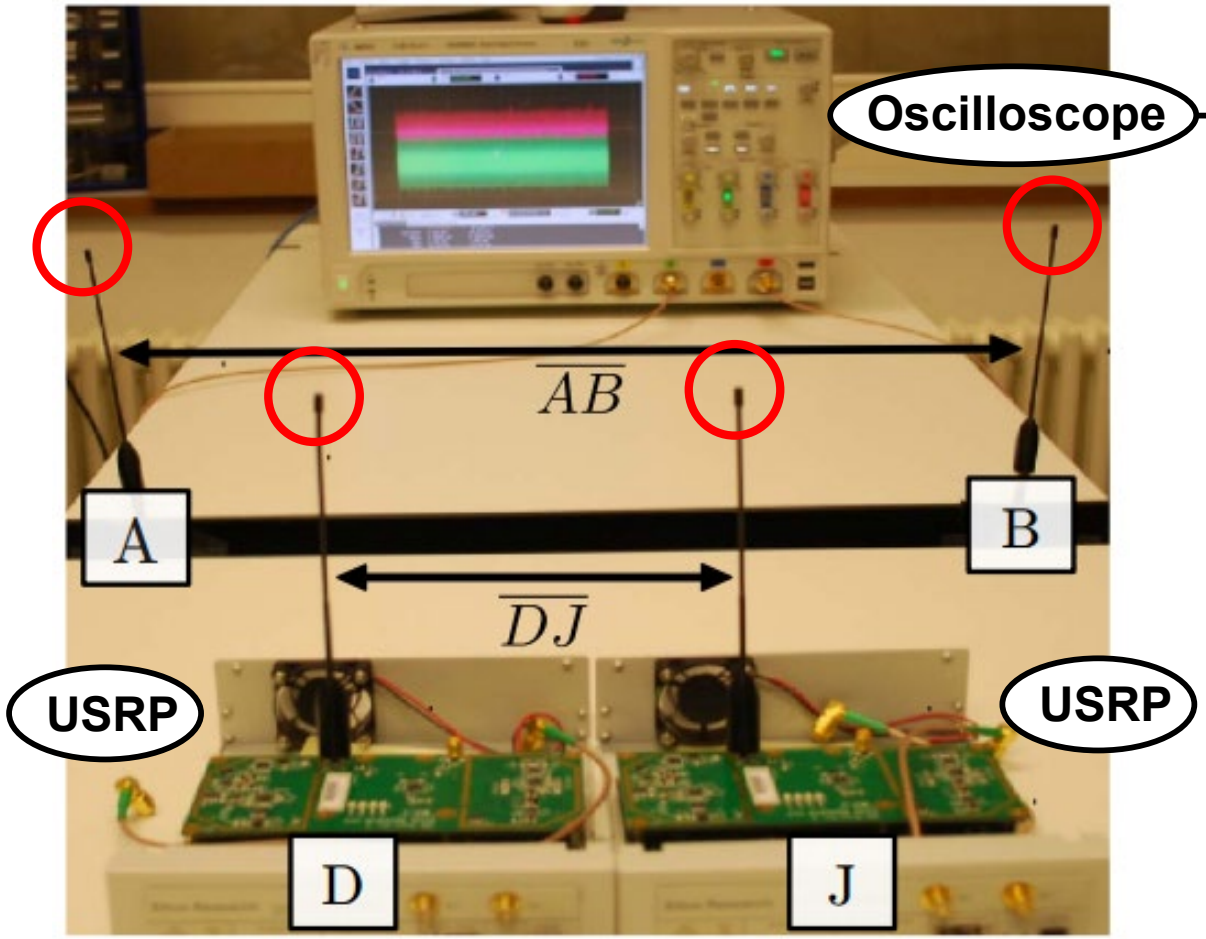
Theoretical limits for relative strength of recovered data signal

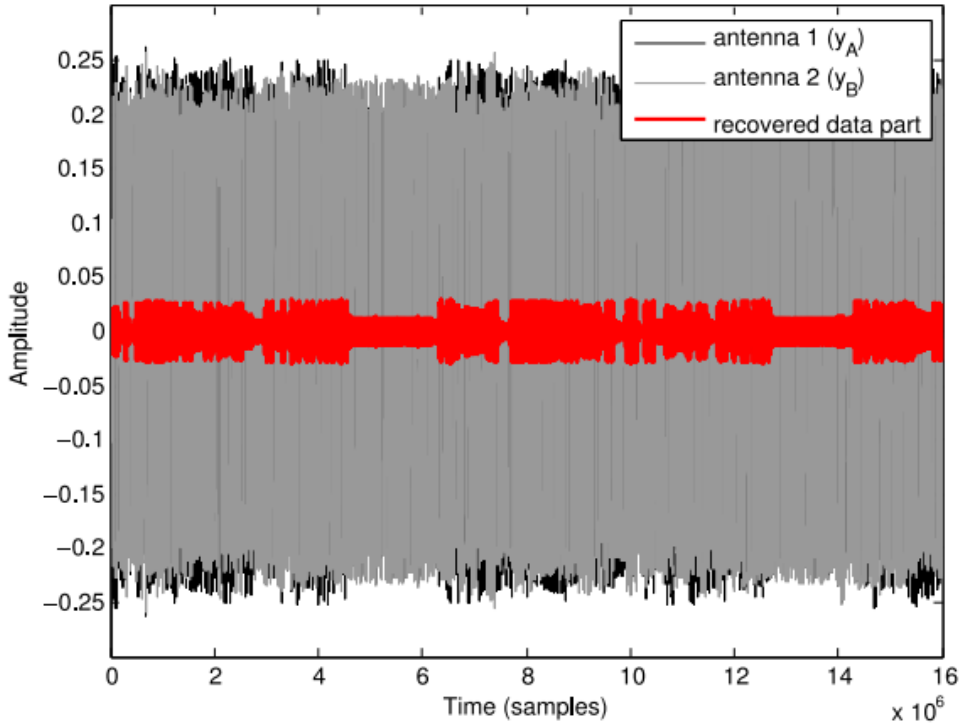


Expected Bit Error Rate at attacker

EXPERIMENTAL ANALYSIS

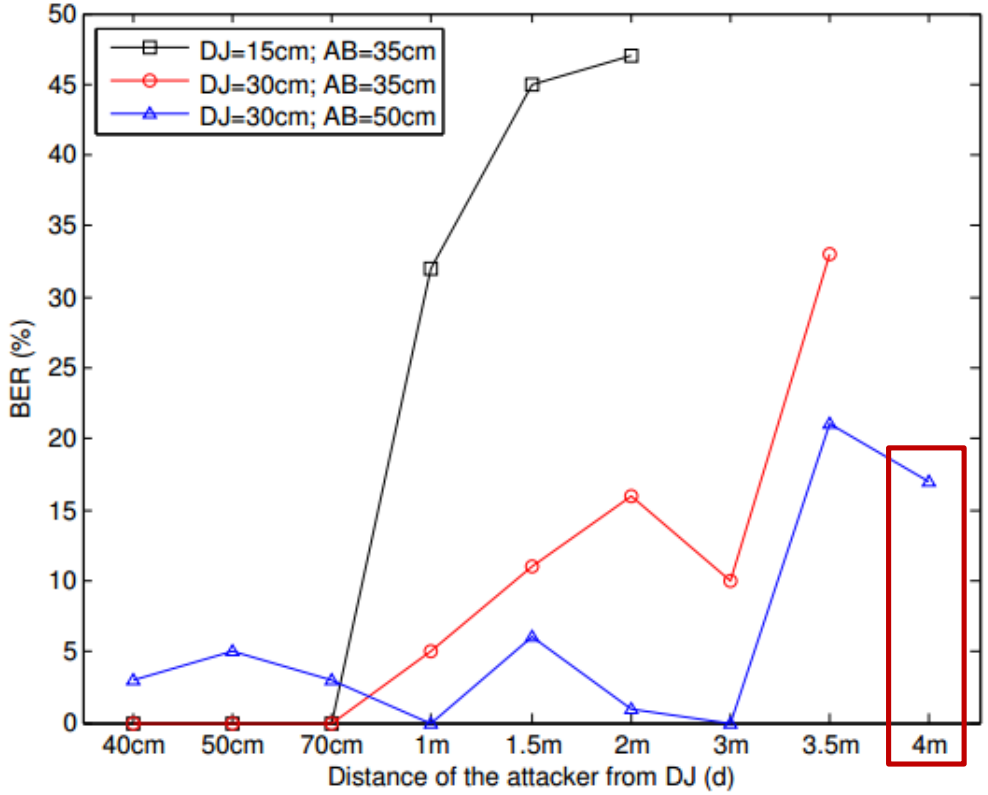
- Experimental Setup



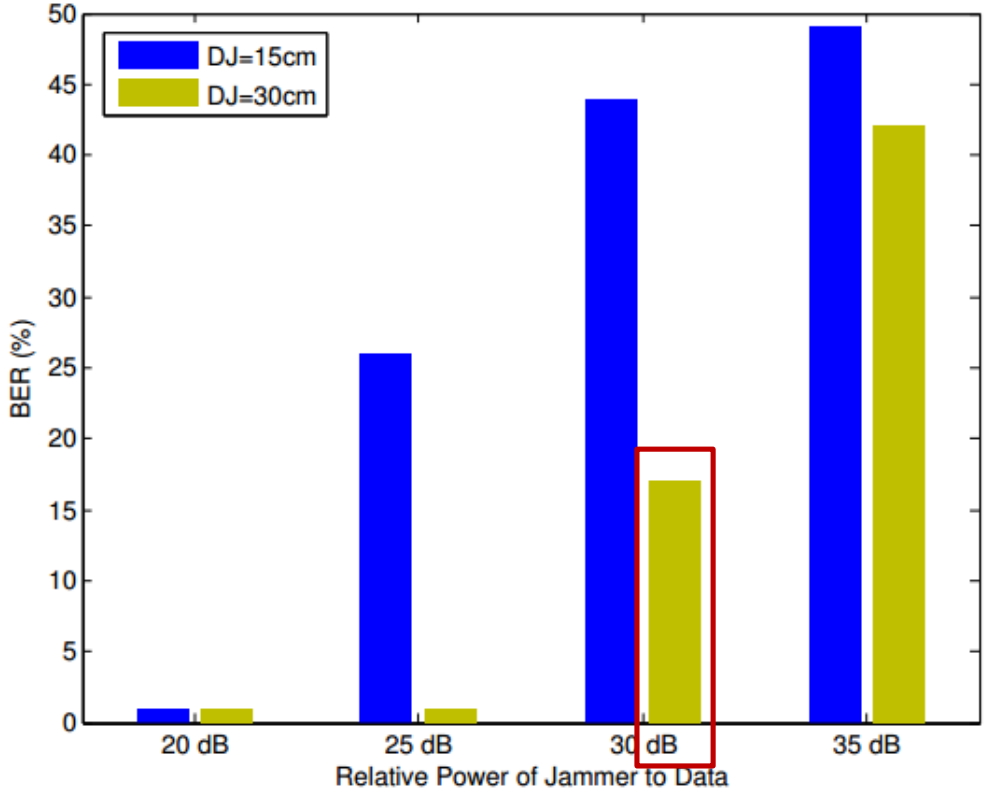


EXPERIMENTAL ANALYSIS

- Measurement & Analysis



Effect of Attacker's distance

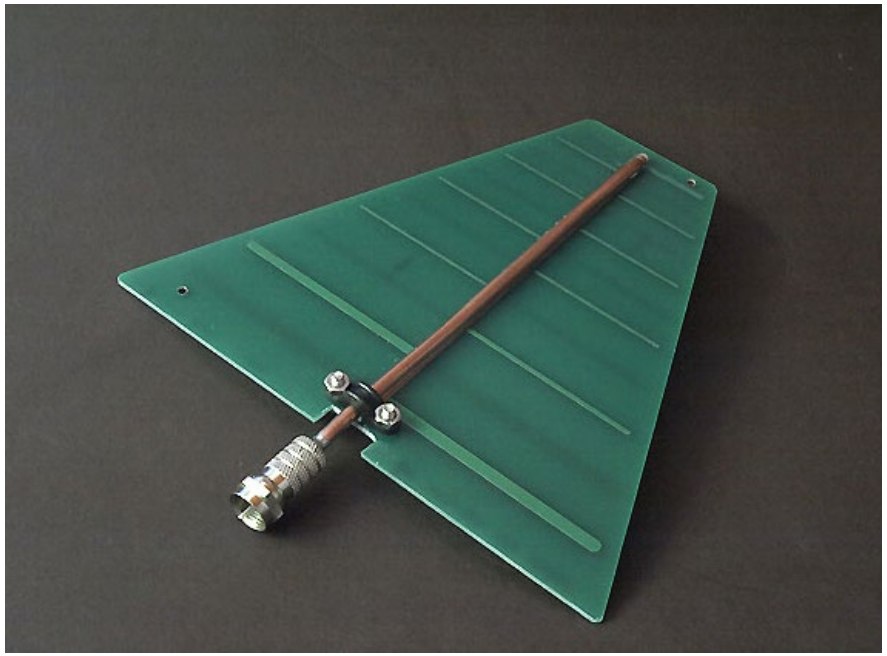


Effect of Jammer signal power

EXPERIMENTAL ANALYSIS

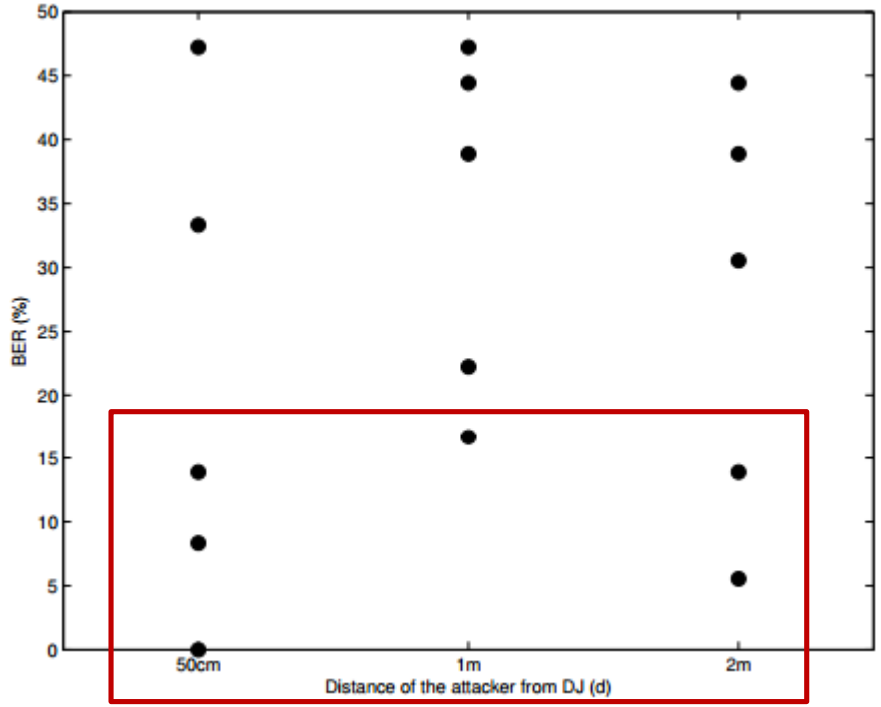
- Measurement & Analysis

400 MHz to 1 GHz
5-6dBi Gain



Directional log-periodic antennas

NLOS condition



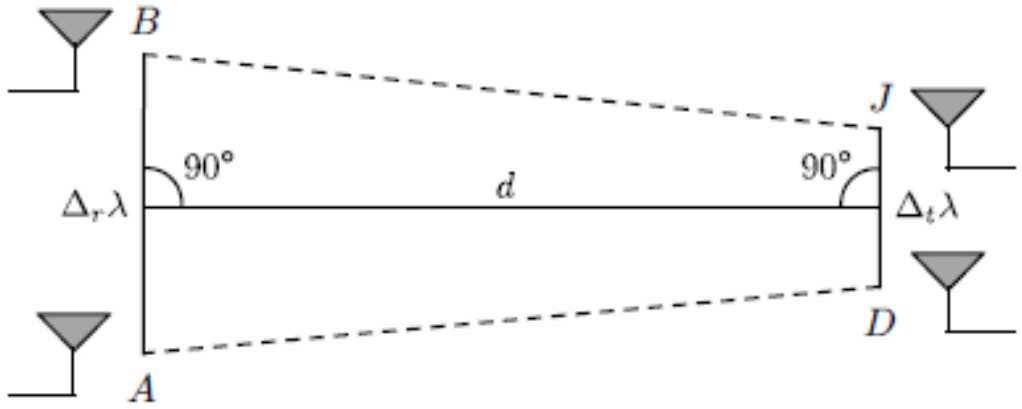
BER with ground beef and bacon

DISCUSSION

- Partial information leakage (feasibility)
  - BER of 0.2 at the attacker ⇒ successfully recover 80% of the bits
    ⇒ break confidentiality
- Placement of attacker antennas (feasibility)
  - Attacker can find good enough placements for the antennas
- Precise modeling of attacker's capability is important.

DISCUSSION

- Countermeasures:



  - Reduce the distance between device (D) and jammer (J). ($\overline{DJ} \ll \frac{\lambda}{2}$)
  - Use multiple jammers.

- FYI, there was no more friendly jamming paper after this paper.

QUESTIONS

- Best Question: (Seong-Joong Kim) Is this attack feasible when an IMD device has MIMO antenna?

  MIMO antenna consumes more battery on the IMD.

  Not much different from multiple jammers case.

  Useful, but still under attack from more powerful attackers.

- (Tae Hyeon Lee) Is there any additional advantage in security aspect, to friendly jamming rather than frequency hopping?

  Frequency hopping is for availability. It cannot defend attacks.

  Also, existing IMDs do not use it.

  Additional advantage: Friendly jamming does not need any surgery.

- (Wooyoung Go) I thought that it is not difficult to find the jammer antenna by bodyguard or security guard. To hide attacker's antenna, is there any way?

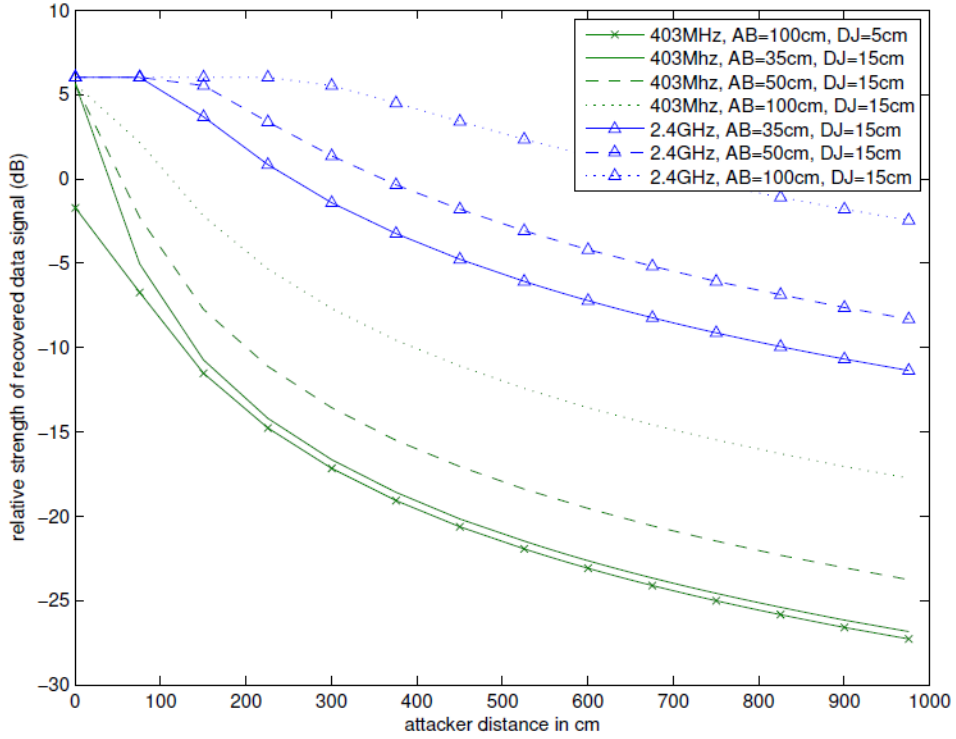
  (Not related to this paper.)

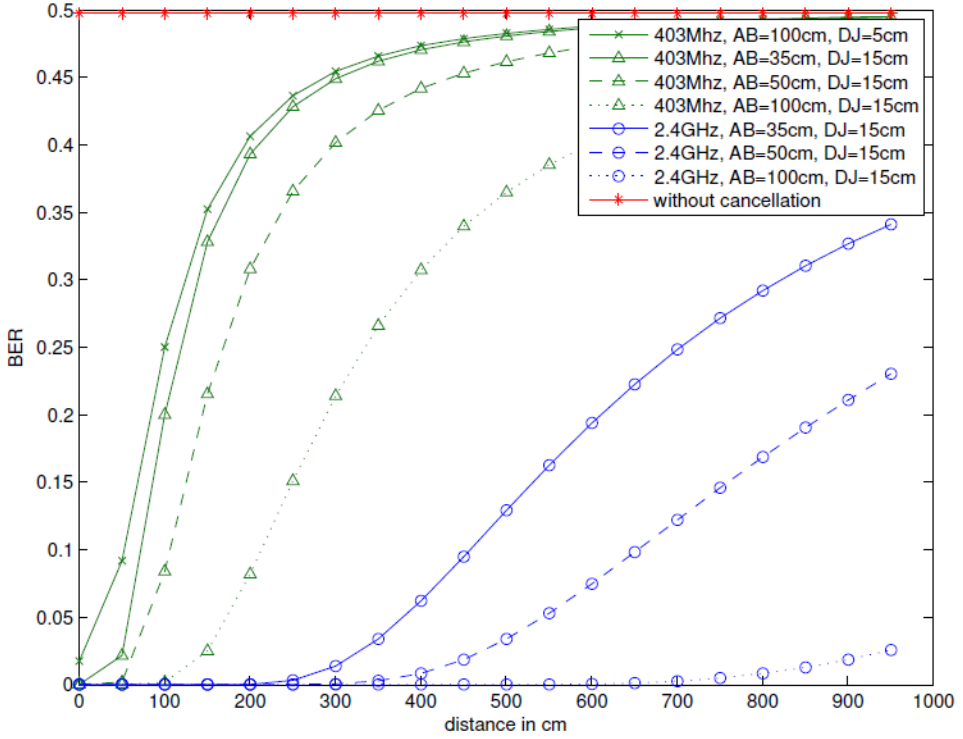
  We cannot find location of passive attackers.

Thank you.

APPENDIX - DISCUSSIONS

- Distance normalization



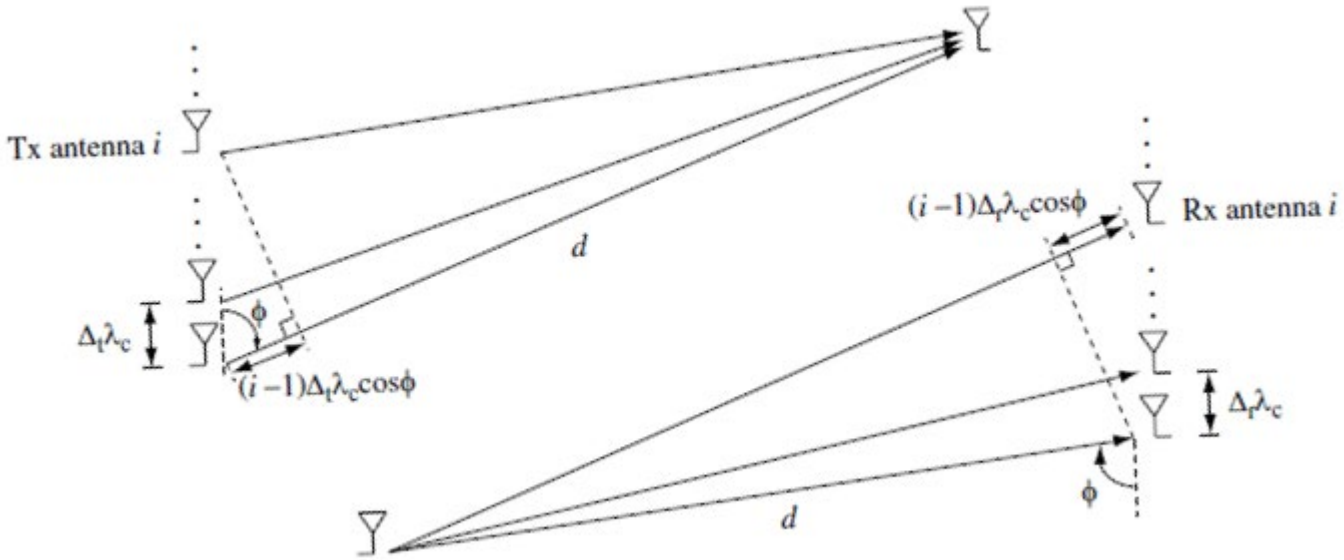


- 2.4 GHz ($\lambda/2 = 6.25$ cm)

  $\overline{DJ} = 15\ cm > \lambda/2$!!!

APPENDIX - JAMMING MITIGATION USING CHANNEL RESOLUTION

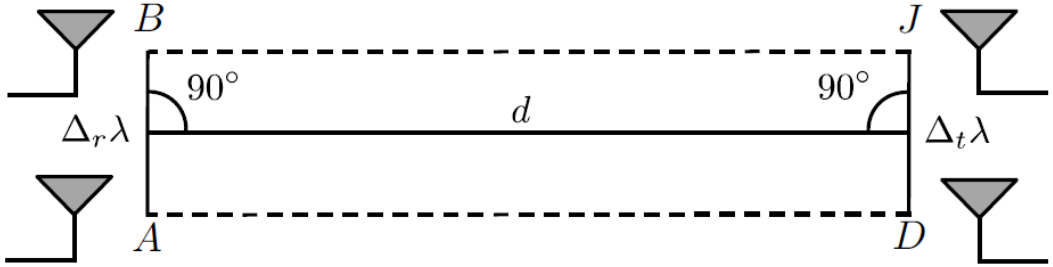
- Geometry of the simulations: isosceles trapezoid



$$h_{ik} = a\exp\left(-\frac{\mathrm{j}2\pi f_c d_{ik}}{c}\right) = a\exp\left(-\frac{\mathrm{j}2\pi d_{ik}}{\lambda_c}\right),$$

$$d_{ik} = d + (i-1)\Delta_r\lambda_c\cos\phi_r - (k-1)\Delta_t\lambda_c\cos\phi_t.$$

General LOS channel model



$$H^m = a\begin{bmatrix} e^{-j2\pi d/\lambda} & e^{-j2\pi d/\lambda} \\ e^{-j2\pi d/\lambda} & e^{-j2\pi d/\lambda} \end{bmatrix}$$

Geometry of the simulations

REFERENCES

- [7] J. Vilela, et al. "Wireless secrecy regions with friendly jamming," *IEEE Transactions on Information Forensics and Security, vol.* 6, no. 2, pp. 256-266, 2011
- [11] S. Gollakota, et al. "They can hear your heartbeats: non-invasive security for implantable medical devices," *ACM SIGCOMM vol.* 41, no. 4, pp. 2-13, 2011
- [21] S. Goel, and R. Negi. "Secret communication in presence of colluding eavesdroppers," *MILCOM 2005*
- [22] P. Pinto, J. Barros, and M. Win. "Wireless physical-layer security: The case of colluding eavesdroppers," *IEEE International Symposium on Information Theory (ISIT)*, 2009
- W. Shen, et al. "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time,"*IEEE Symposium on Security and Privacy (SP), 2013*