Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Selected Topics in Physical Layer Security

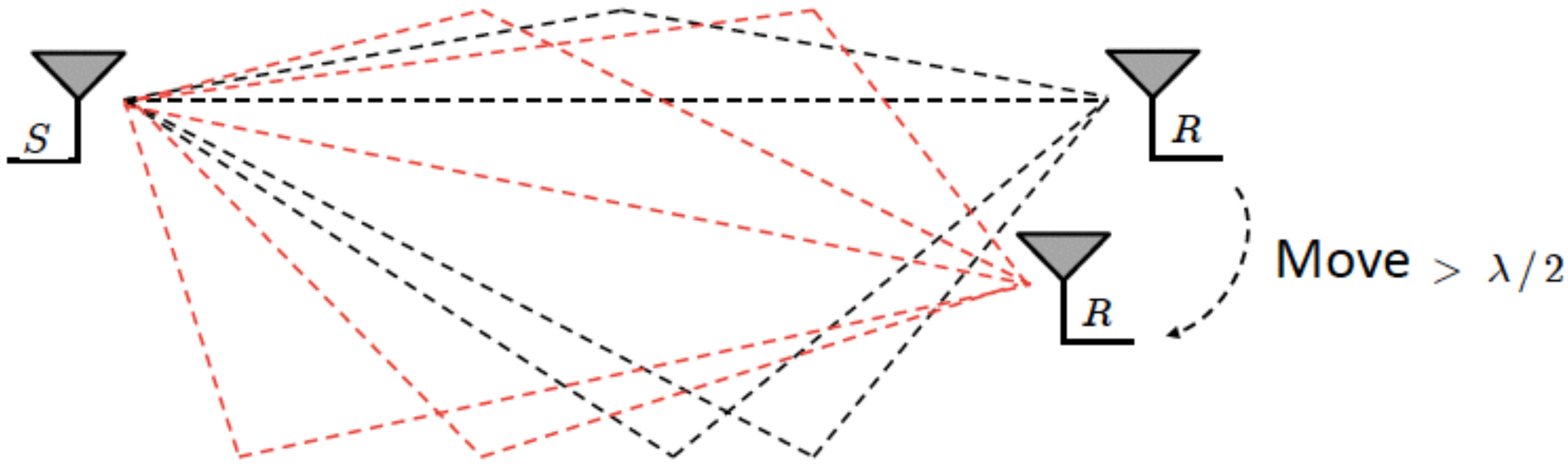
Srdjan Čapkun
Department of Computer Science
ETH Zurich

Content of this slide:
“Wireless is everywhere and important”

Can we leverage the Physical Layer for Confidentiality? Authentication? Access Control?

Channel-based Key Establishment

Wireless Channel

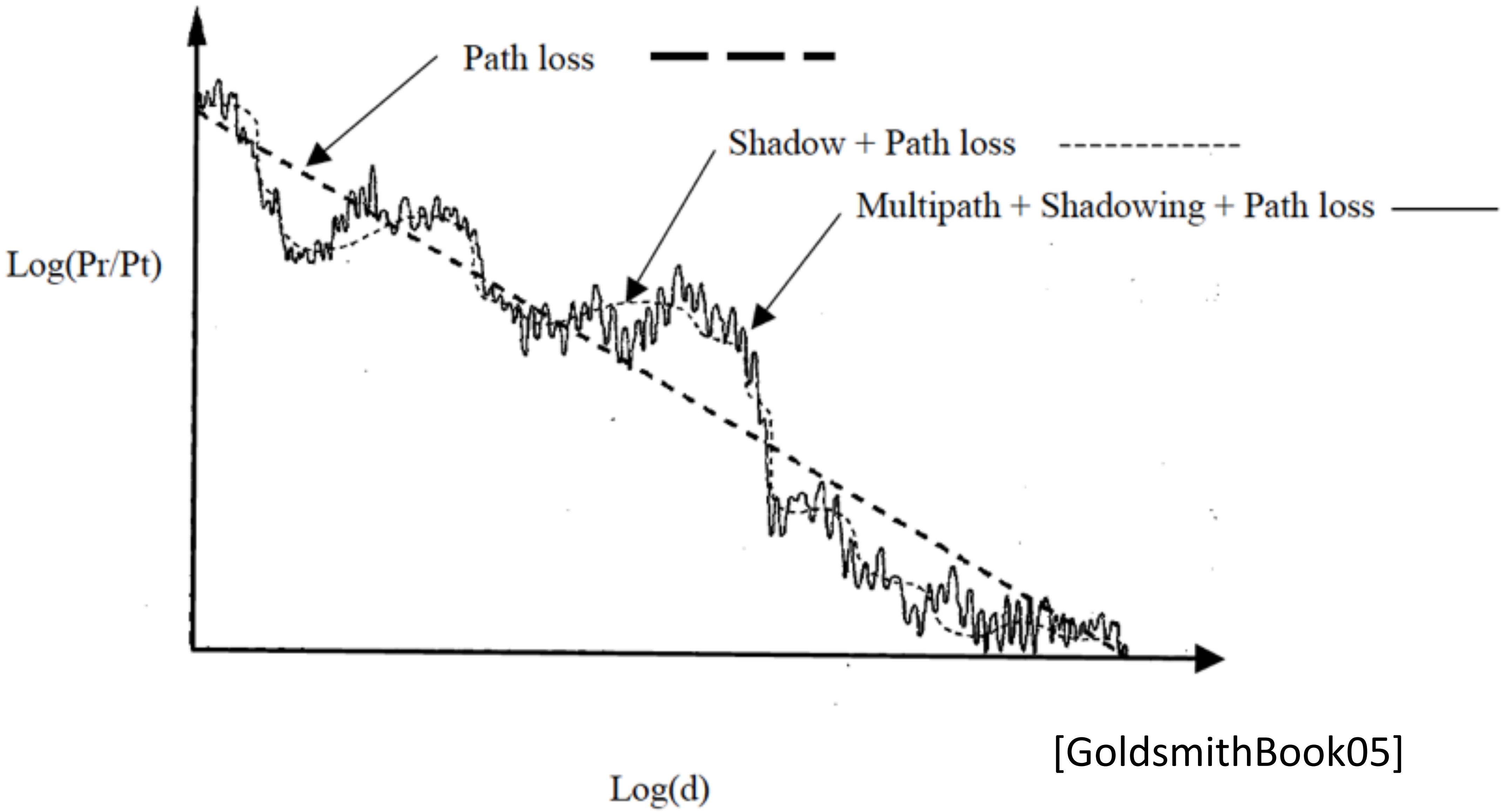


- In a complex, multipath-rich environment, channels exhibit ***time-varying, stochastic and reciprocal*** fading.
- For receivers that are > λ/2 away, channels are not correlated.

=> the channel between S and R will be ‘random’ and will not be known to the attacker

=> a natural wiretap channel

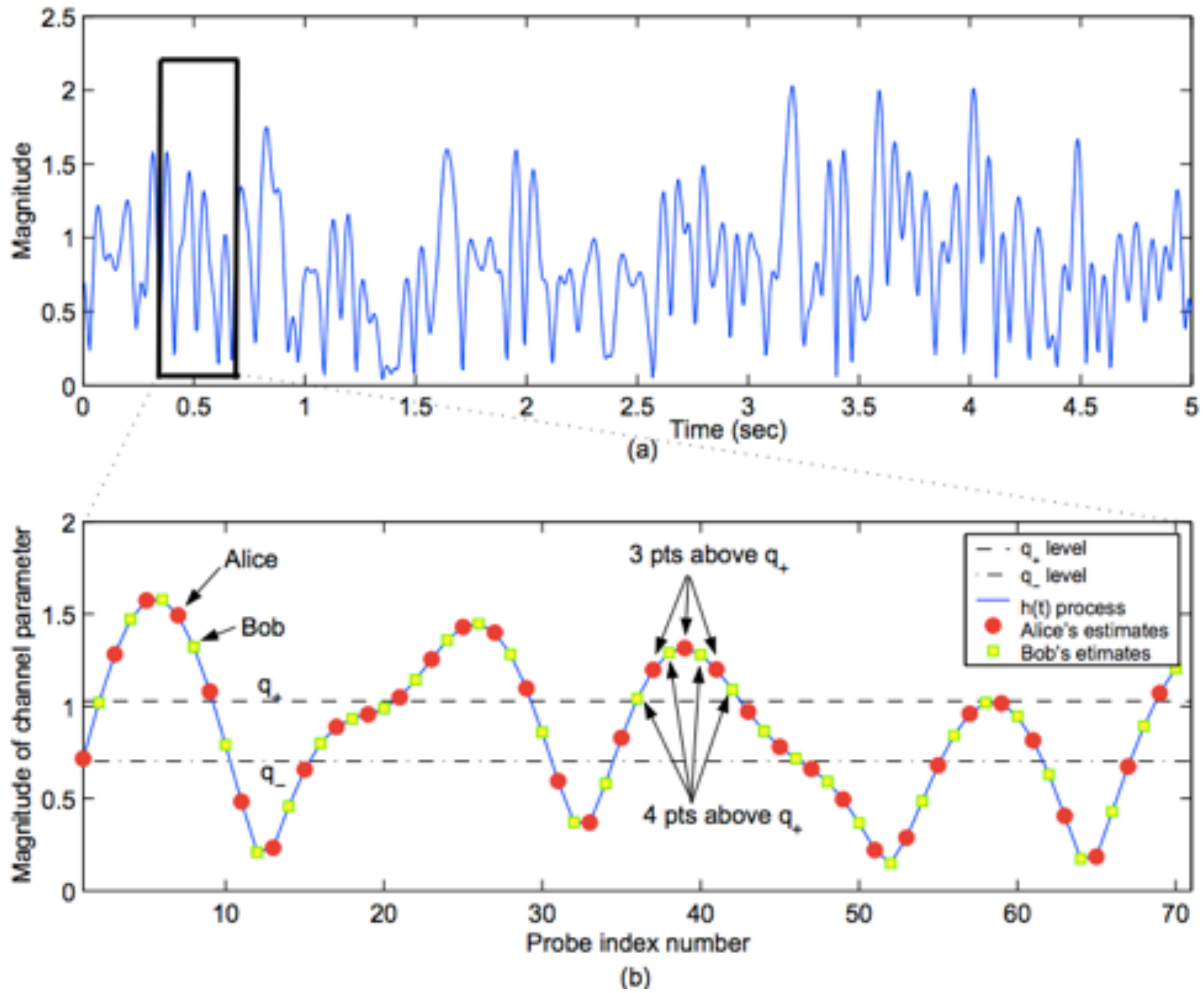
Wireless Channel



[GoldsmithBook05]

- the attacker does not know and cannot remotely measure multipath fading components

Key Agreement: RSSI [MathurMobiCom08]



1. Signal acquisition and Quantization
2. Reconciliation (error correction, privacy amplification)
3. Key confirmation

Key Agreement

Channel property[a]	RSSI [17,18,10,19,1,16,13]	CIR [12,1,13,14]	Phase [15]
Entropy source	Movement [17,10,19,12,11,1,13,14]	Channel-selective fading [16]	Angle of arrival [18]
Hardware	802.15.4 [17,18,19,11,16]	UWB [10,12]	802.11a [1,13]
Quantization	1-threshold [18,10]	2-thresholds [17,12,1,13]	Dynamic multi-threshold [19,11,15,16,14]
Error correction	Block-based parity [17]	Quantization-dependent [18,10,19,12,1,16]	Error correction codes [13,14]
Attacker model	Passive [17,18,10,19,12,15,16,14]	Active [11,1,13]	—

[a] Some protocols use multiple channel properties.

[EberzESORICS12]

- A broad range of HW assumptions.

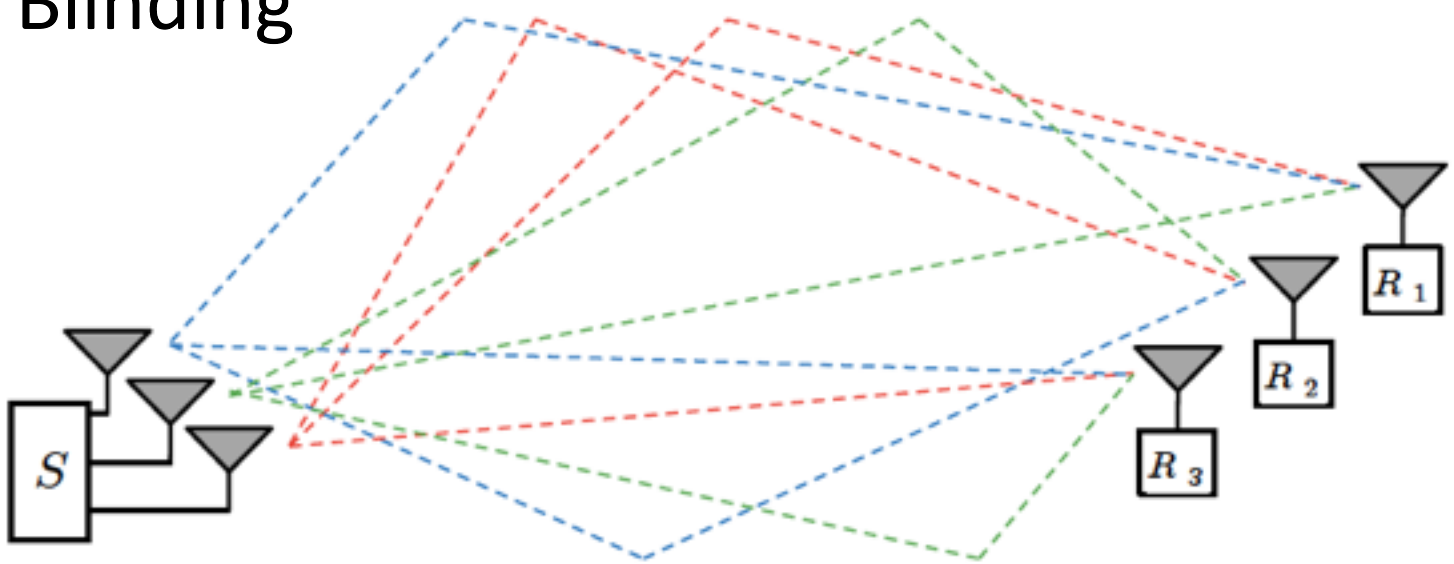
Analysis

- No authentication!
  - secret key established but with which device?
  - cannot use channel information to authenticate
- No guarantees on the environment
  - is the environment multipath-rich?
  - can attacker pre-measure environment [TmarPhD2012]?
  - can attacker be verified to be > $\lambda/2$ away?
- Questionable benefits over existing PK/SK schemes
  - Information-theoretic guarantees claimed in some papers but unclear how these hold

- Most schemes consider only passive adversary
- Active attacks
  - influence and discover the established key [EberzESORICS12]
  - abuse the lack of authentication

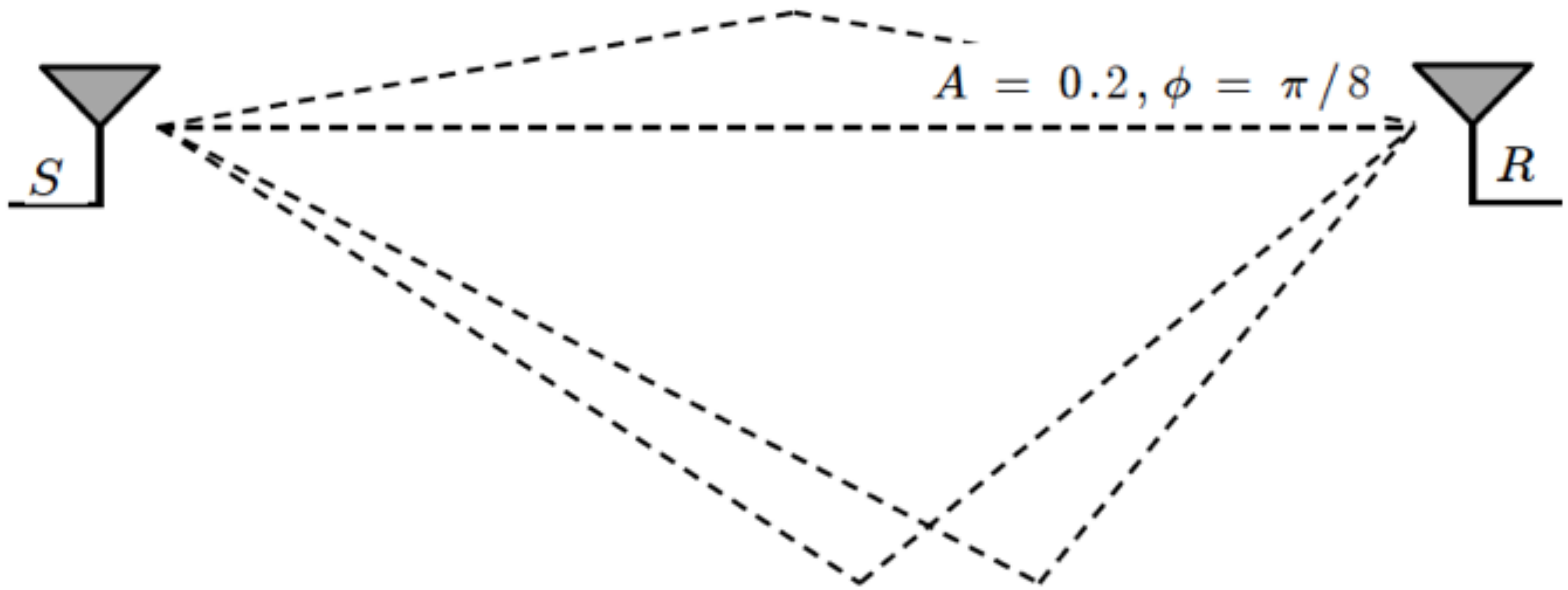
Ensuring Secrecy with MIMO

- Approaches:
  - Zero Forcing
  - Orthogonal Blinding



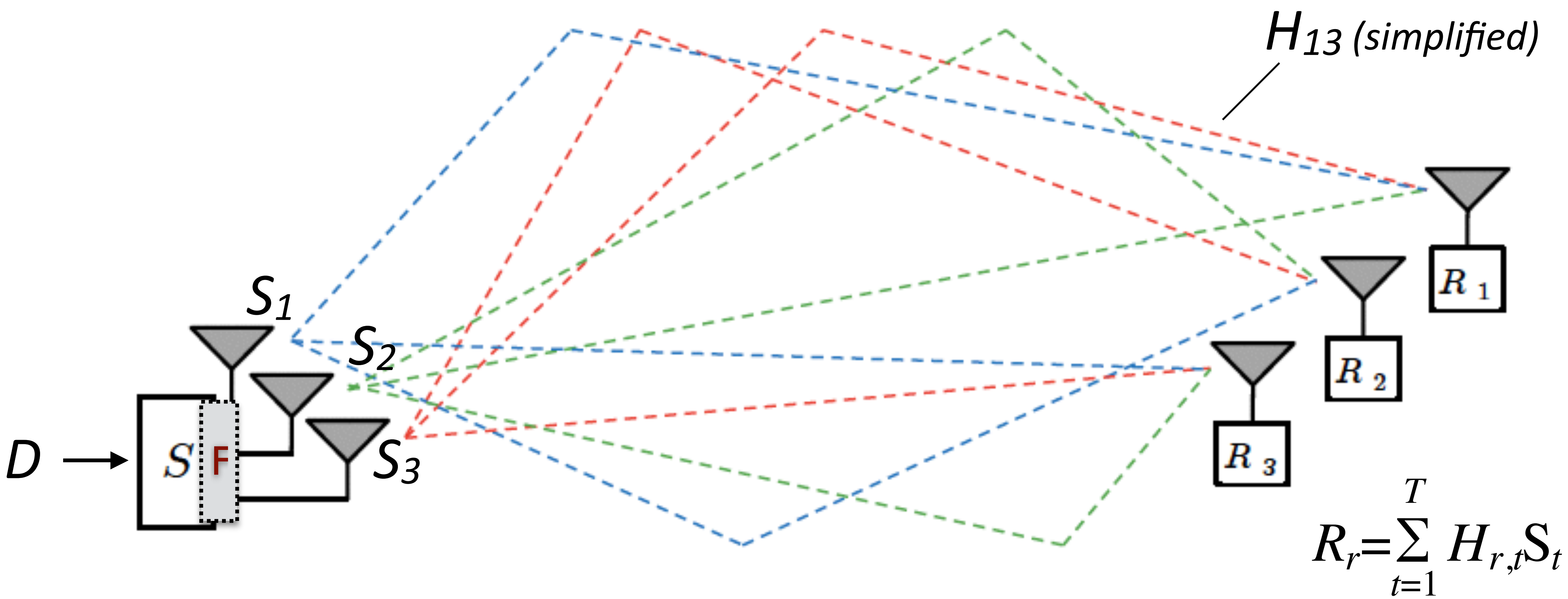
- Main ideas:
  - *Steer the signals towards the receiver and away from the attacker.*
  - *Use jamming to interfere with the attacker, but not with the receiver.*

Modeling the Channel



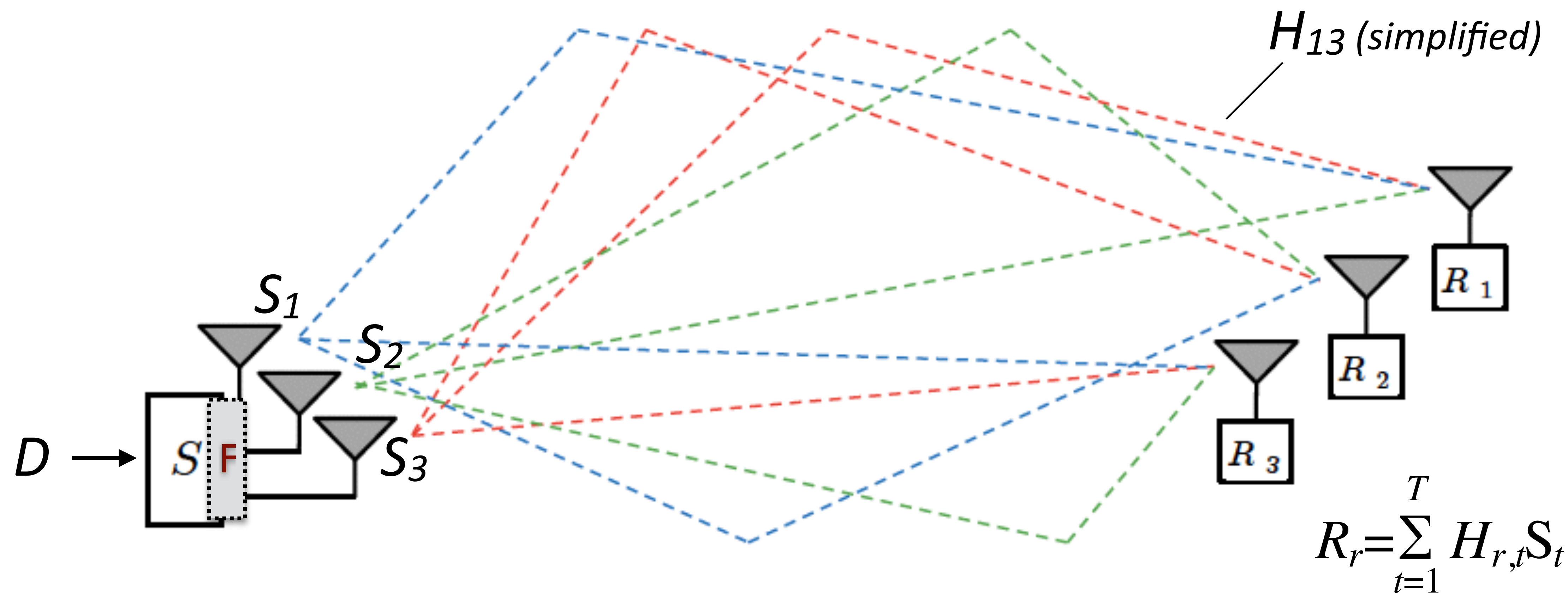
- At the receiver, signal has different phase and amplitude
- Channel is modeled as a single complex number
  - Captures both change in amplitude (real part) and phase (imaginary part)
  - Represents cumulative effects of all multipath components

Zero Forcing



- S knows the channels to R_1 and to attackers R_2,R_3
- *R = H* ***F*** *D = H S*
- *H: channel matrix*
  D: data matrix (conf. data)
- ***F*** is a transmission filter, constructed given ***H****, s.t.*:
  - R_1 = confidential data
  - R_2,R_3 = no (useful) data

Orthogonal Blinding



- S knows the channels to R_1 ***but not to attackers***
- *R = H* ***F*** *D = H S*
- *H: channel matrix (part randomly generated)*
  D: data matrix (conf. data and noise)
- ***F*** is a transmission filter, constructed given ***H**, s.t.*:
  - R_1 = confidential data
  - R_2,R_3 *(attackers)* = ***data + jamming signal (noise)***

Analysis

- Stronger guarantees than SISO schemes:
  - beamforming focuses the energy to the receiver
  - jamming interferes with the attacker

- No authentication!
- No guarantees on the environment
- Questionable benefits over existing PK/SK schemes

- Passive attacks: known plaintext attack **[SchulzNDSS2013-to appear]**
  - *attacker trains a filter until it finds a plaintext and thus discovers the channel between S and R*
- Active attacks:
  - abuse the lack of authentication

Can we use Friendly Jamming for Confidentiality and Access Control

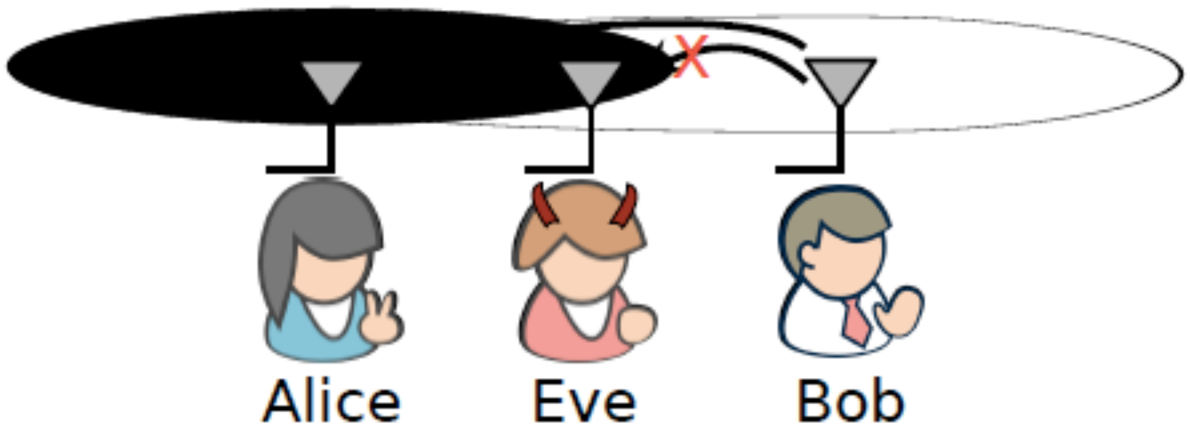
Jamming for Confidentiality

- The use of jamming for
  - *confidentiality*
  - authentication / access control
  - S.Goel, R.Negi, “Guaranteeing secrecy using artificial noise,” IEEE T. on Wireless 2008
  - A. Araujo, J. Blesa, E. Romero, and O. Nieto-Taladriz, “Cooperative jam technique to increase physical-layer security in CWSN 2012
  - L. Dong, Z. Han, A. Petropulu, and H. Poor, “Cooperative jamming for wireless physical layer security,” in Proc. of IEEE Workshop on Statistical Signal Processing (SSP), 2009
  - X. Tang, R. Liu, P. Spasojevic and, and H. Poor, “Interference assisted secret communication,” IEEE Transactions on Information Theory, vol. 57, no. 5, pp. 3153 –3167, May 2011.
  - J. Vilela, M. Bloch, J. Barros, and S. McLaughlin, “Friendly jamming for wireless secrecy,” in Proceedings of the IEEE ICC 2010
  - M. R. Rieback, B. Crispo, and A. S. Tanenbaum, “Keep on blockin’ in the free world: Personal access control for lowcost RFID tags,” in Proc. 13th International Workshop on Security Protocols. LNCS, Apr 2005.
  - I. Martinovic, P. Pichota, and J. Schmitt, “Jamming for good: A fresh approach to authentic communication in wsns,” in Proceedings ACM WiSec. 2009,
  - C. Kuo, M. Luk, R. Negi, and A. Perrig, “Message-in-a-bottle: user-friendly and secure key deployment for sensor nodes,” in Proceedings of SenSys 2007.
  - ...

Jamming for Confidentiality

- Orthogonal blinding / Zero forcing:
  transmit noise into the null-space of the receiver's channel
  - no pre-established secrets
  - used for key establishment

- ***Friendly Jamming:***
  transmit noise which the receiver subtracts
  - Receiver knows the seed used to generate the noise
  - Eavesdropper cannot separate signal and noise

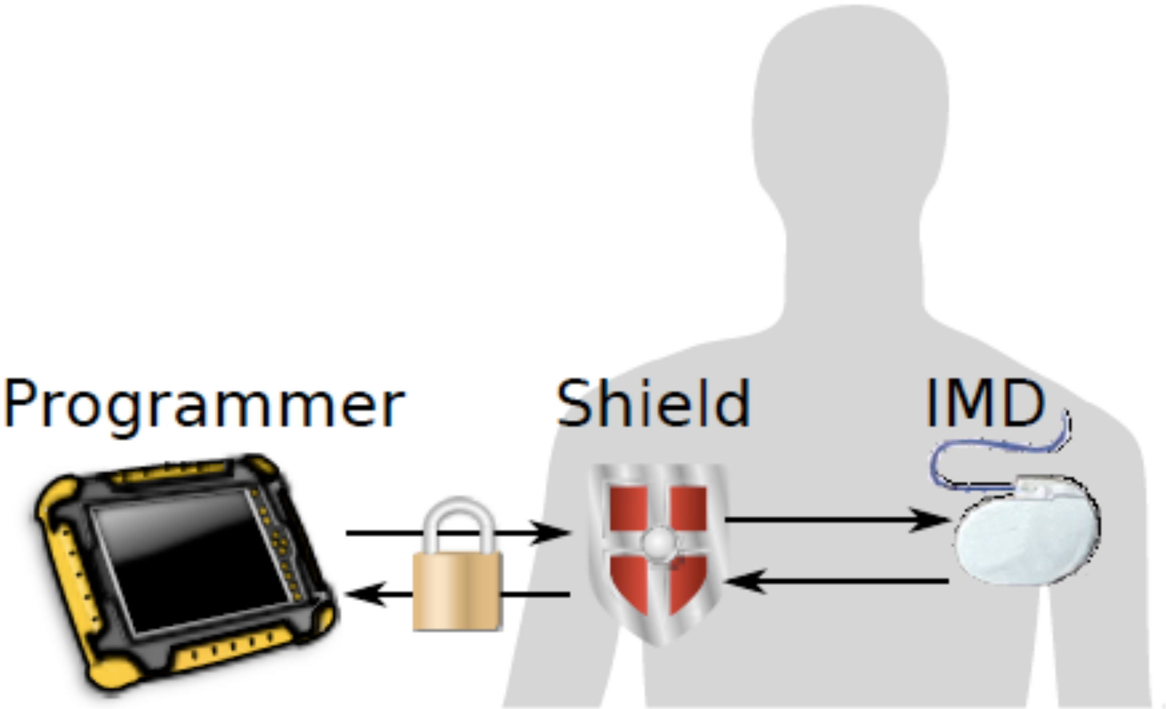


Friendly Jamming

- Jamming signal is much stronger and covers the spectrum of the data signal.
- If DJ > λ/2, attacker equipped with two antennas can separate signals from J and D (different channels).
- If DJ >> λ/2 attacker can use directional antennas to separate the signals.
- => the only “safe” case seems to be when DJ < λ/2

Example: “IMD Shield”

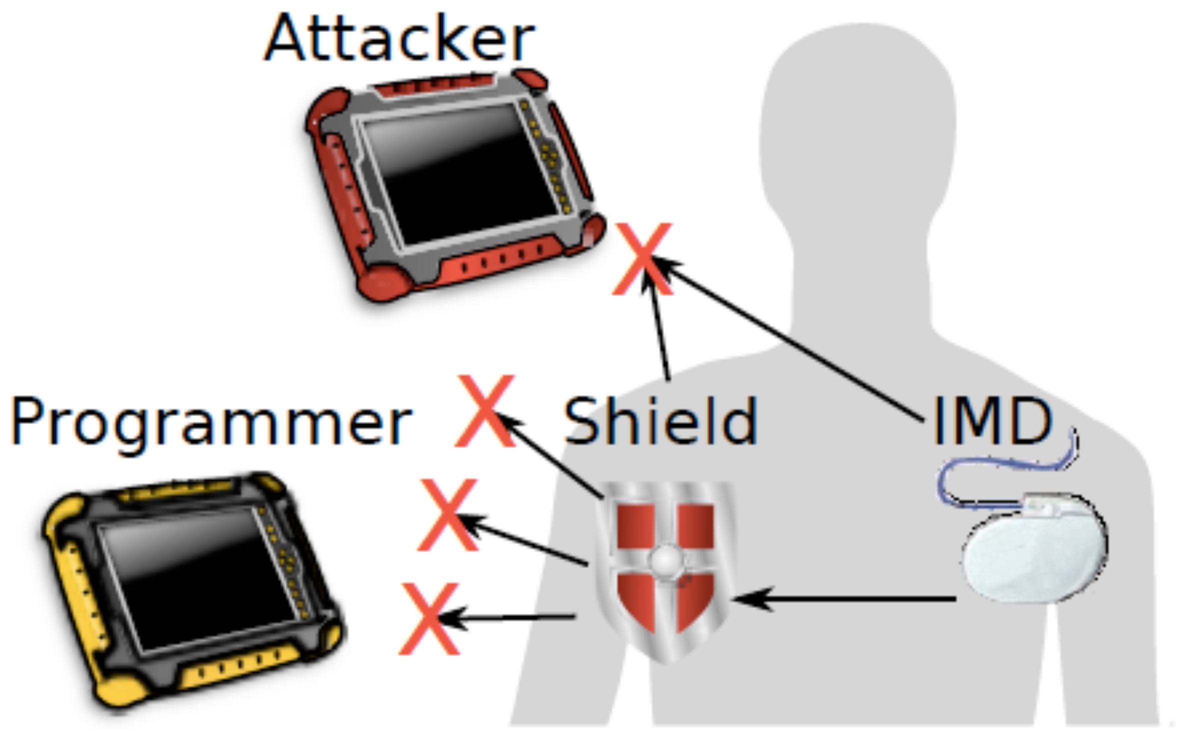
- *S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, K. Fu, “They can hear your heartbeats: Non-invasive security for implanted medical devices,” in Proceedings of the ACM SIGCOMM, 2011.*



- ***Confidentiality:***
  - IMD Shield jamms the eavesdropper.
  - Legitimate reader jammed but can remove jamming signal (shared key with the Shield).

Example: "IMD Shield"

- *S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, K. Fu, "They can hear your heartbeats: Non-invasive security for implanted medical devices," in Proceedings of the ACM SIGCOMM, 2011.*



- ***Confidentiality:***
  - IMD Shield jamms the eavesdropper.
  - Legitimate reader jammed but can remove jamming signal (shared key with the Shield).

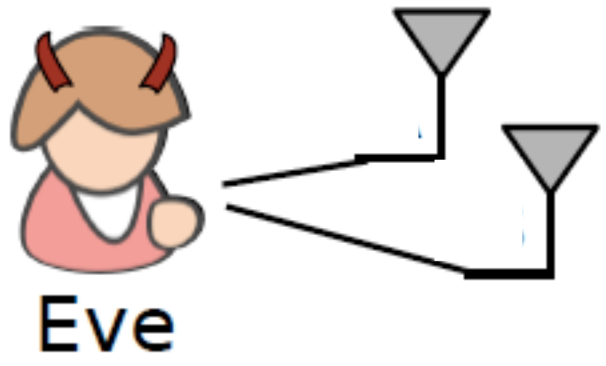
ETH Zürich

Friendly Jamming Security Arguments

- One of the main security assumptions:
  - If DJ < λ/2, *the attacker cannot separate signals from J and D irrespective of the number of antennas or their directionality.*

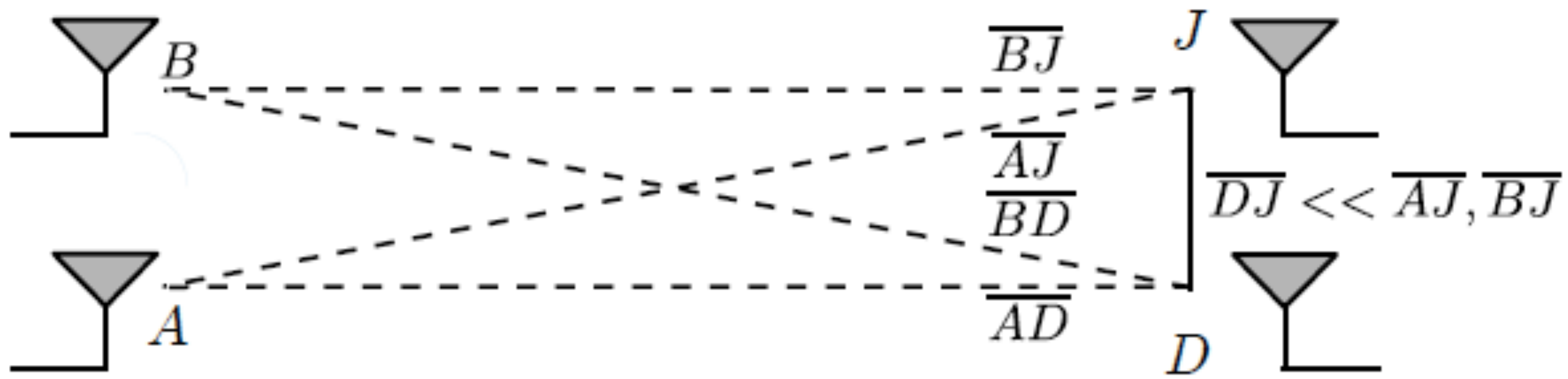
- However, we show that:
  - Confidentiality holds only for a single-antenna attacker.
  - *A MIMO-like attacker CAN separate the signals and recover the confidential message, from a number of locations.*

Attacker Model



- Passive attacker
  - Two antennas, free placement
  - IMD send private data in plain text
  - Attacker's goal is to break confidentiality i.e., recover data with BER< 50%

LoS Model of the System



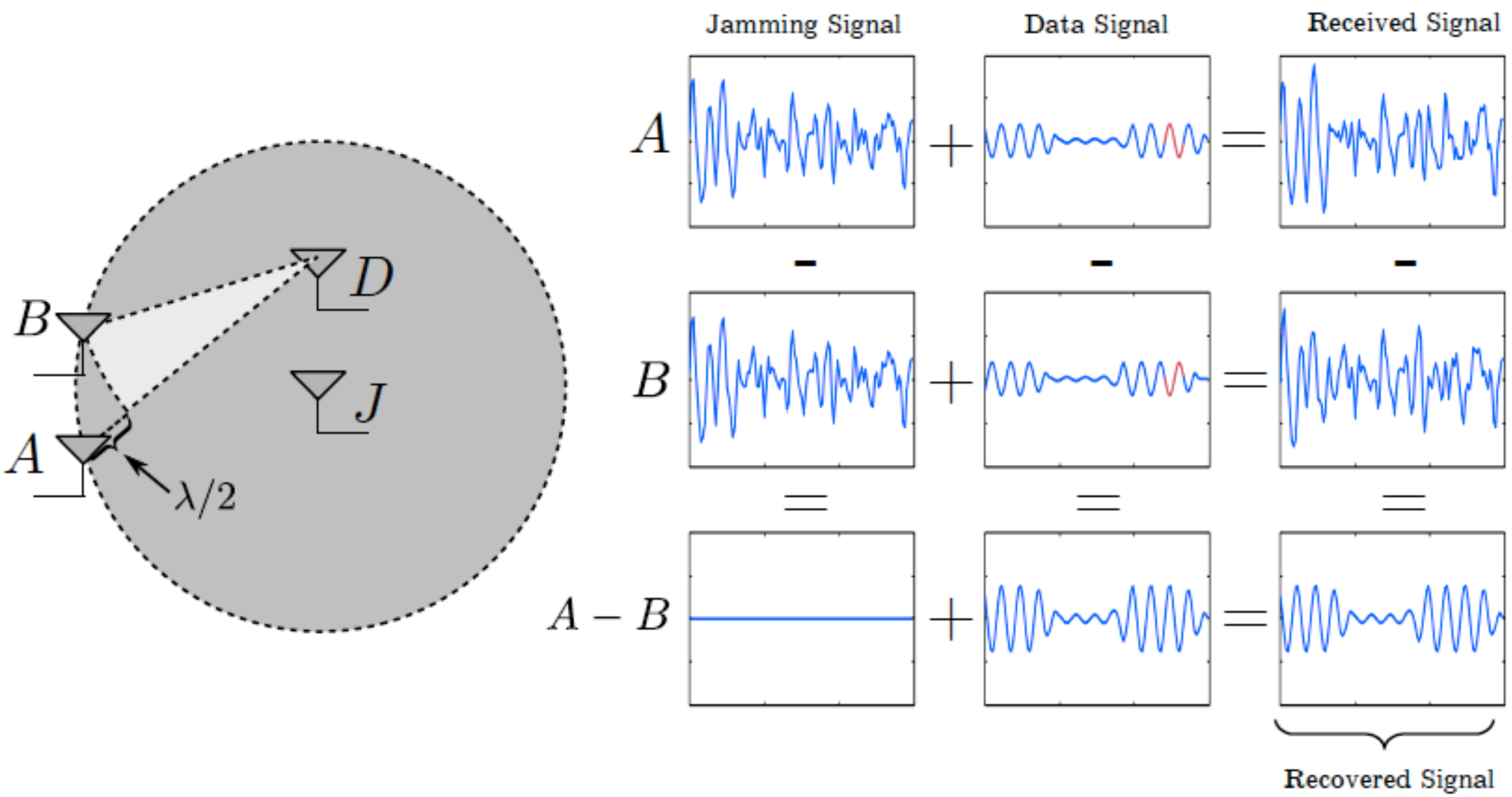
- A and B receive data and jamming signals with different relative offsets
- ToAs of signals are given by the geometry.
  In LOS settings:

$$Y_A(t) = X_D(t - \overline{AD}/c) + X_J(t - \overline{AJ}/c) \text{ and}$$
$$Y_B(t) = X_D(t - \overline{BD}/c) + X_J(t - \overline{BJ}/c)$$

- Each attacker's antenna (A and B) are still jammed.

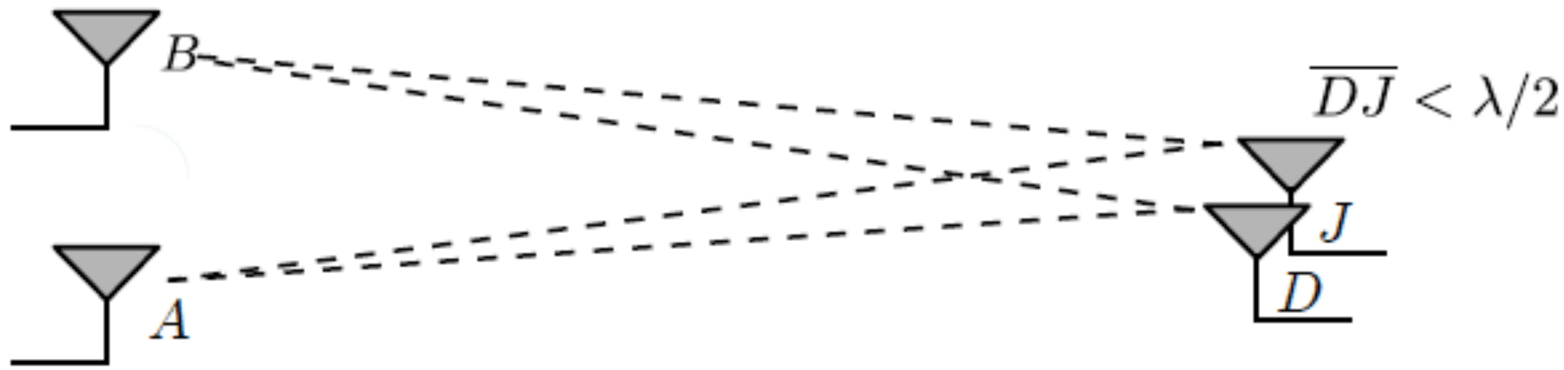
Ideal Placement of the Attacker's Antennas

- *N.Tippenhauer, L. Malisa, A. Ranganathan, S. Capkun, On Limitations of Friendly Jamming for Confidentiality, in Proceedings of the IEEE Symposium on Security and Privacy (S&P), 2013*



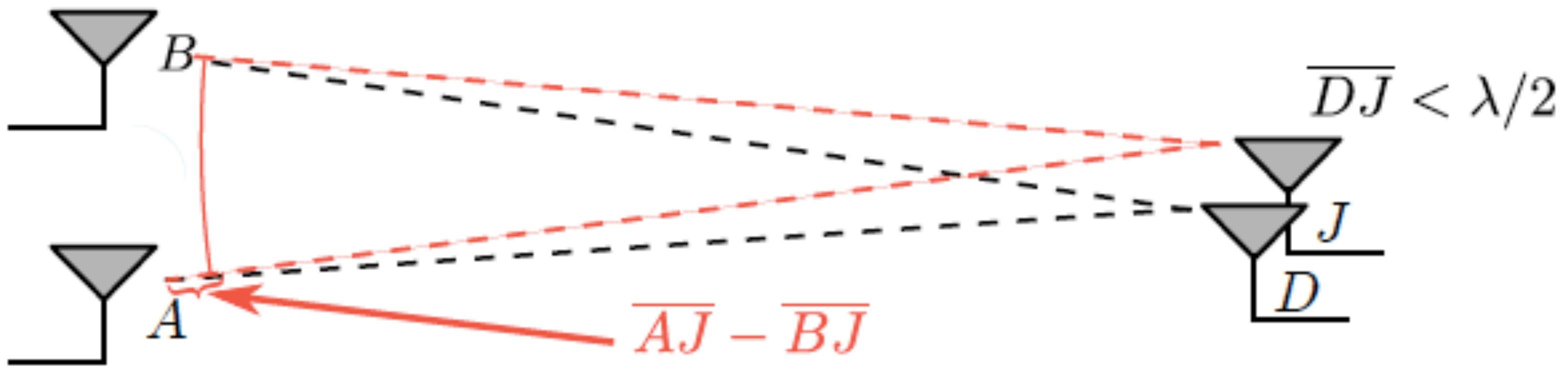
- jamming signals arrive simultaneously at A and B, whereas the data signals are shifted by λ/2 ...

Impact of Imperfect Attacker Placement



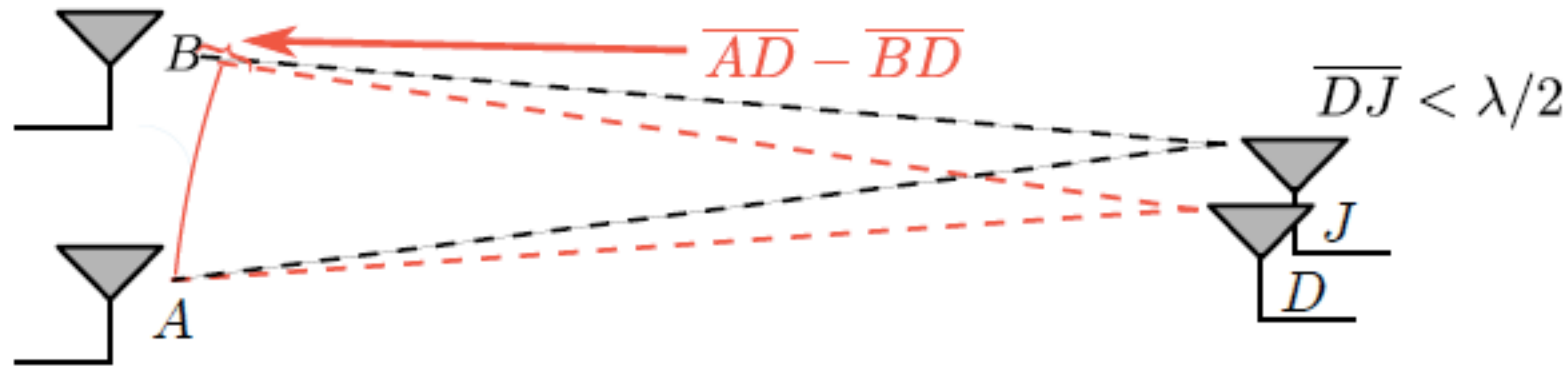
- Ideal cancellation of jamming signal relies on
  $\delta = |(\overline{AJ} - \overline{BJ}) - (\overline{AD} - \overline{BD})| = \lambda/2$
- For 2.4 GHz WLAN, λ/2 = 6.25cm, for 400MHz, λ/2 = 37.5cm
- Is data content recovery still possible with imperfect δ ?

Impact of Imperfect Attacker Placement



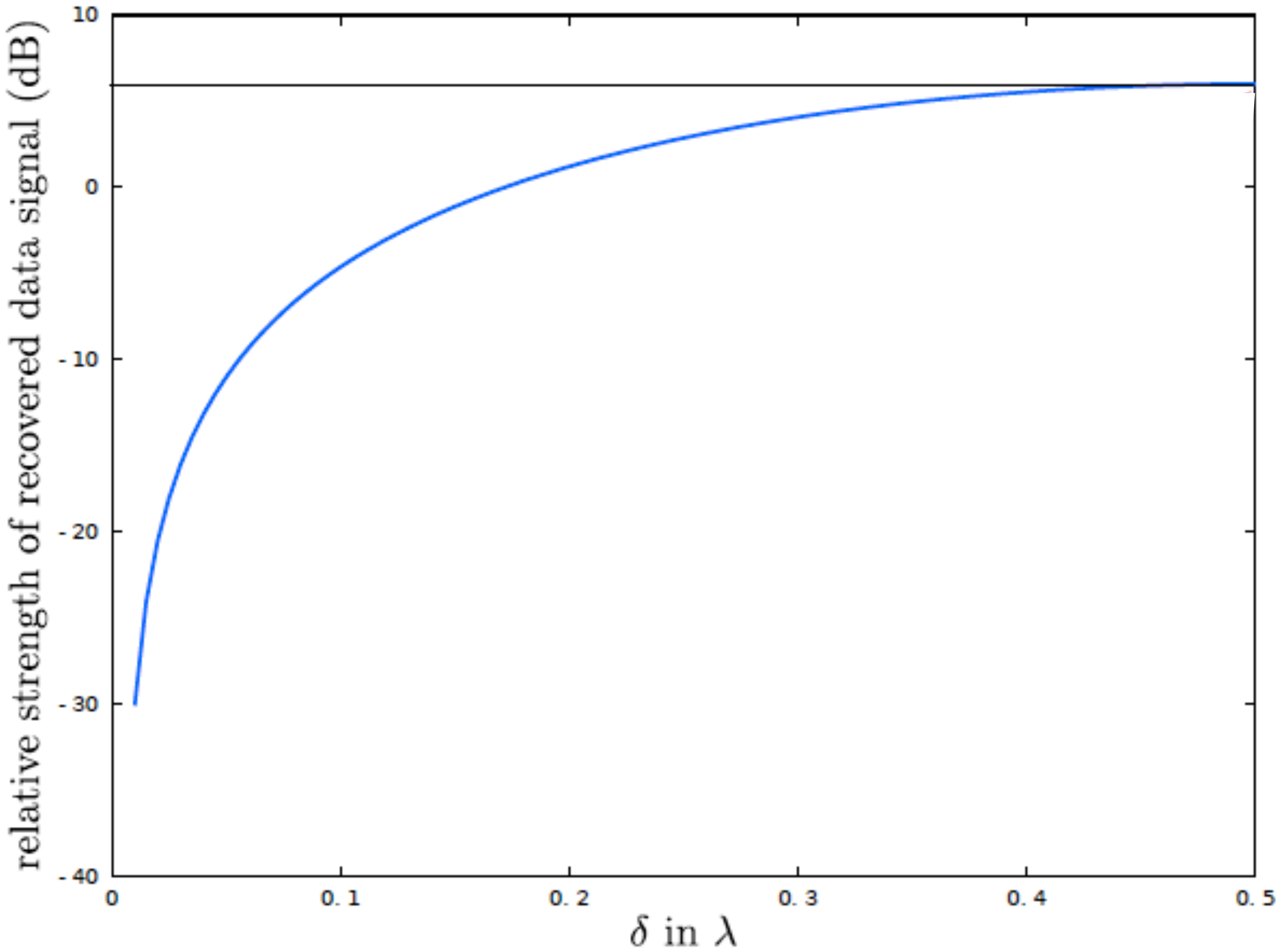
- Ideal cancellation of jamming signal relies on
  $\delta = |(\overline{AJ} - \overline{BJ}) - (\overline{AD} - \overline{BD})| = \lambda/2$
- For 2.4 GHz WLAN, λ/2 = 6.25cm, for 400MHz, λ/2 = 37.5cm
- Is data content recovery still possible with imperfect δ ?

Impact of Imperfect Attacker Placement



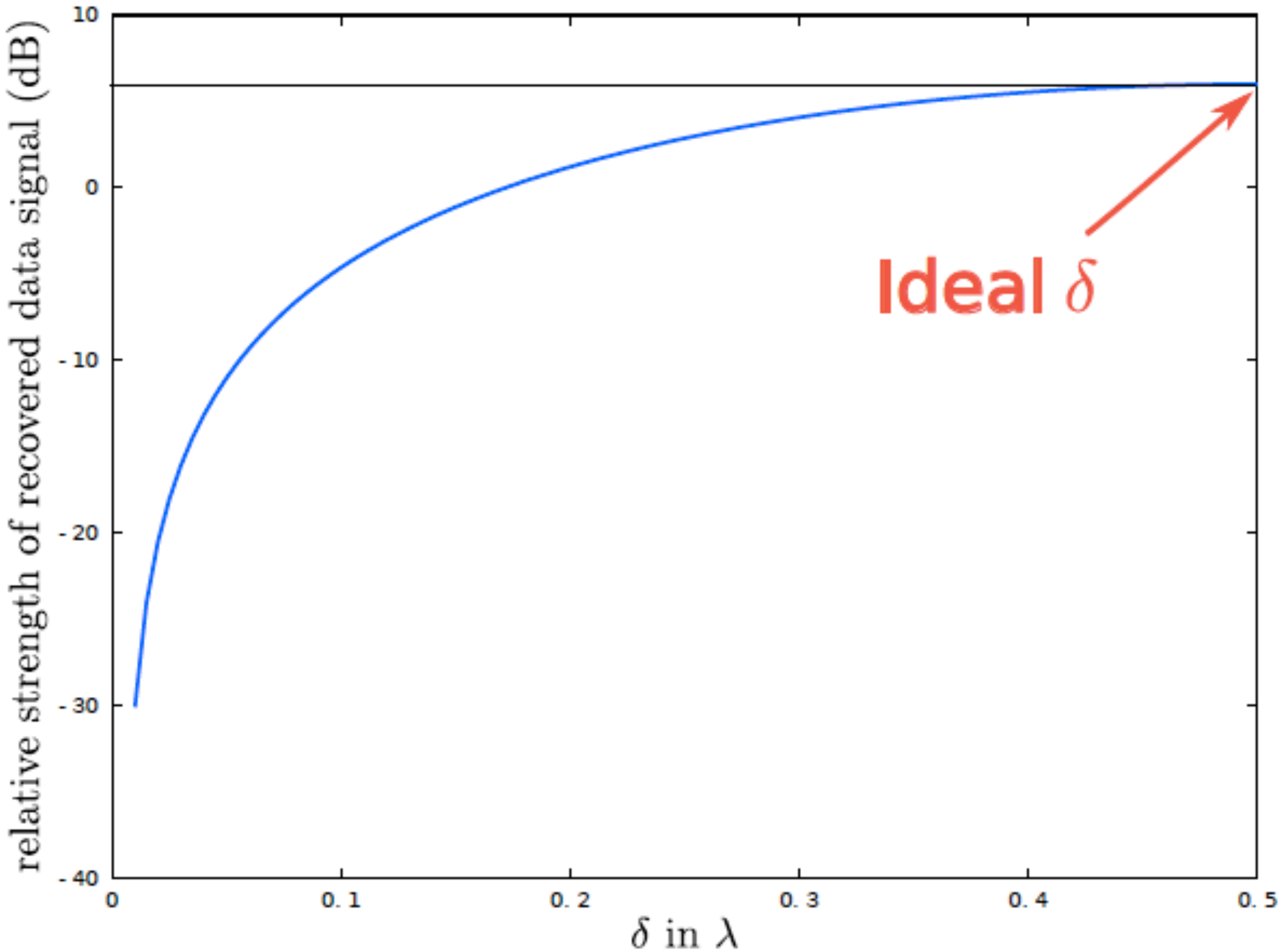
- Ideal cancellation of jamming signal relies on
  $\delta = |(\overline{AJ} - \overline{BJ}) - (\overline{AD} - \overline{BD})| = \lambda/2$
- For 2.4 GHz WLAN, L/2 = 6.25cm, for 400MHz, λ/2 = 37.5cm
- Is data content recovery still possible with imperfect δ ?

Impact of Imperfect Attacker Placement



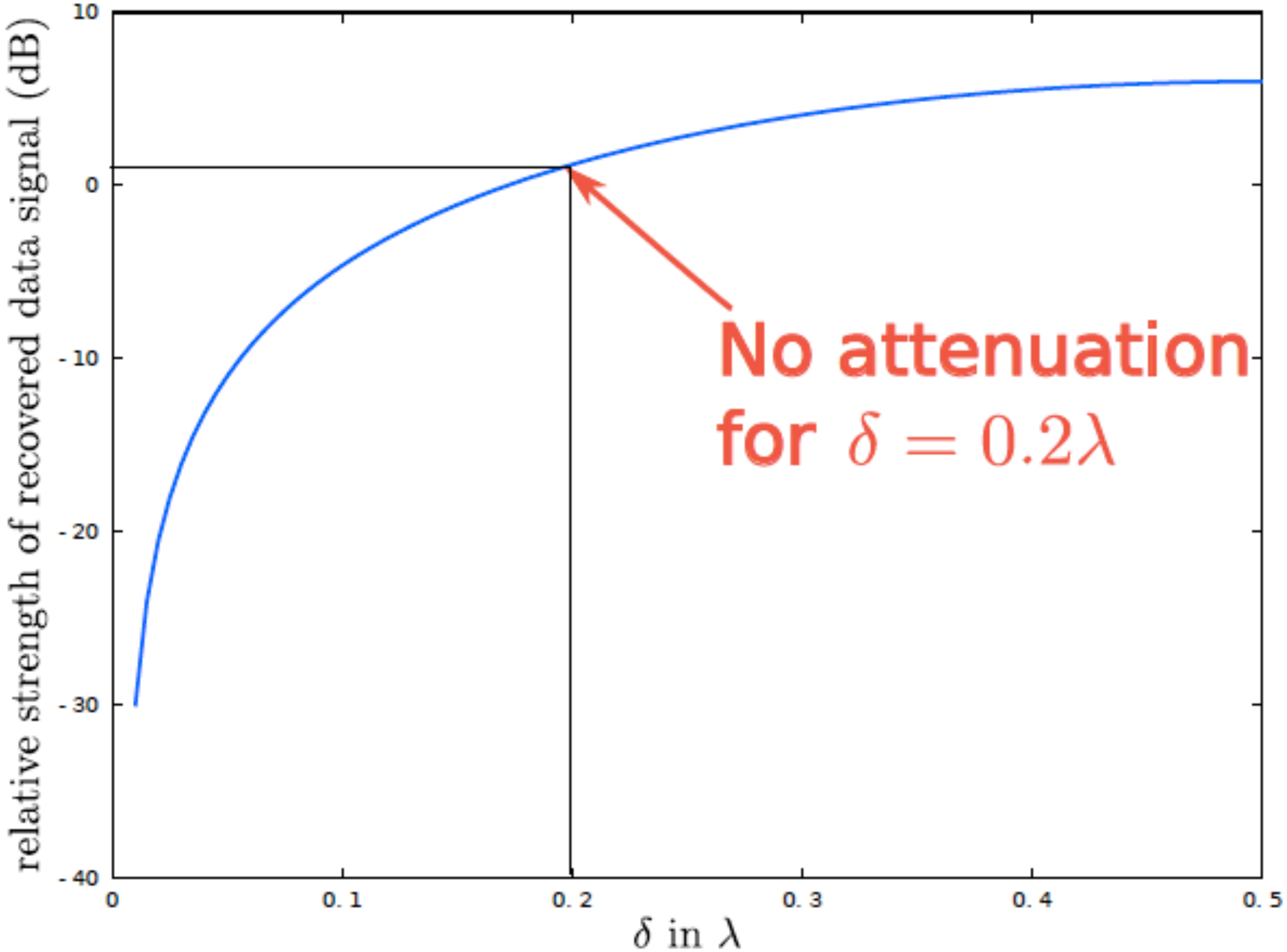
For $\delta = |\overline{AJ} - \overline{AD} - \overline{BJ} + \overline{BD}| > \lambda/5$, the attacker can recover the data signal with amplification (attenuation $< 0dB$).

Impact of Imperfect Attacker Placement



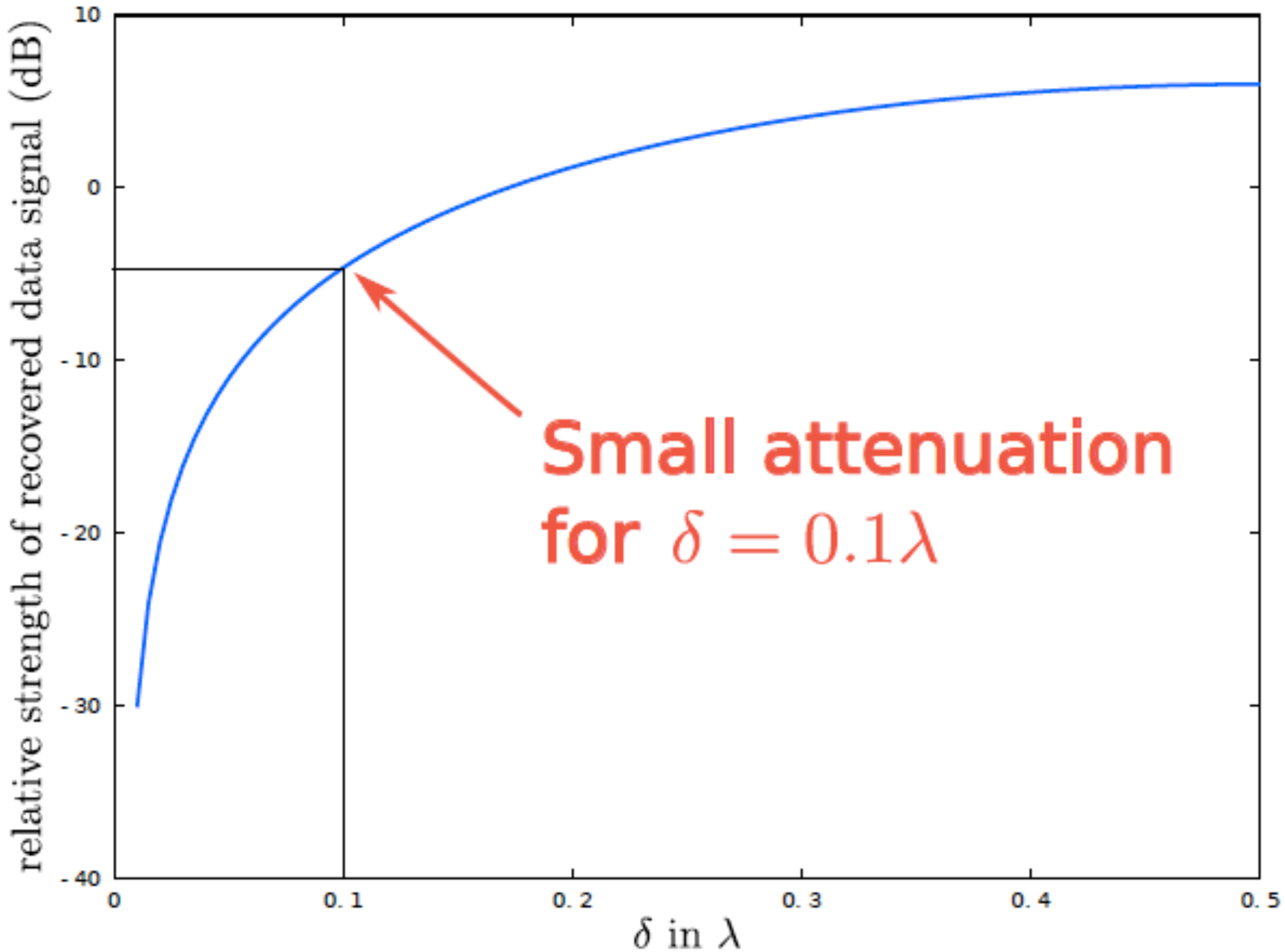
For $\delta = |\overline{AJ} - \overline{AD} - \overline{BJ} + \overline{BD}| > \lambda/5$, the attacker can recover the data signal with amplification (attenuation $< 0dB$).

Impact of Imperfect Attacker Placement



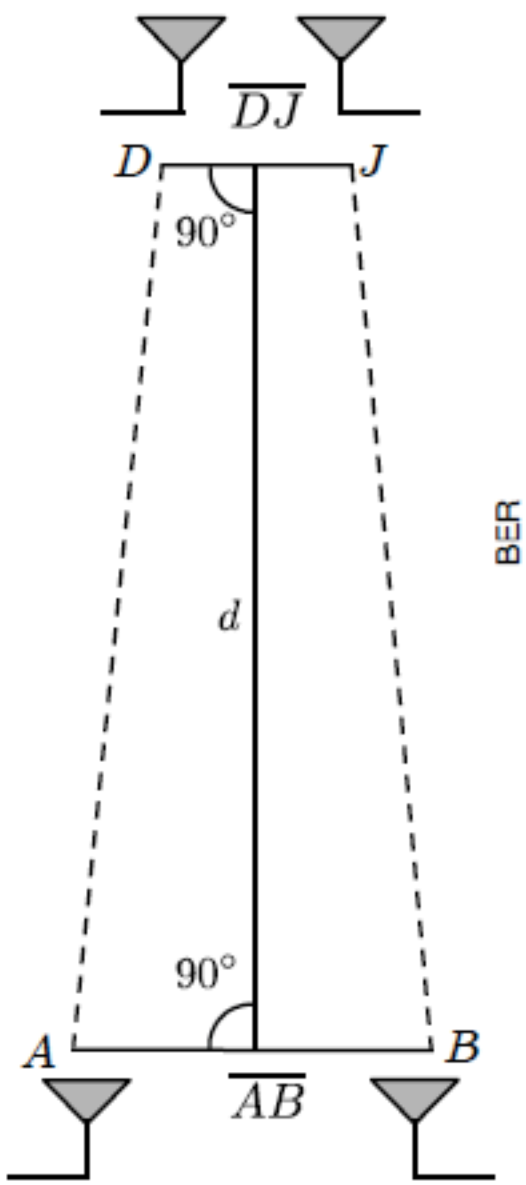
For $\delta = |\overline{AJ} - \overline{AD} - \overline{BJ} + \overline{BD}| > \lambda/5$, the attacker can recover the data signal with amplification (attenuation $< 0dB$).

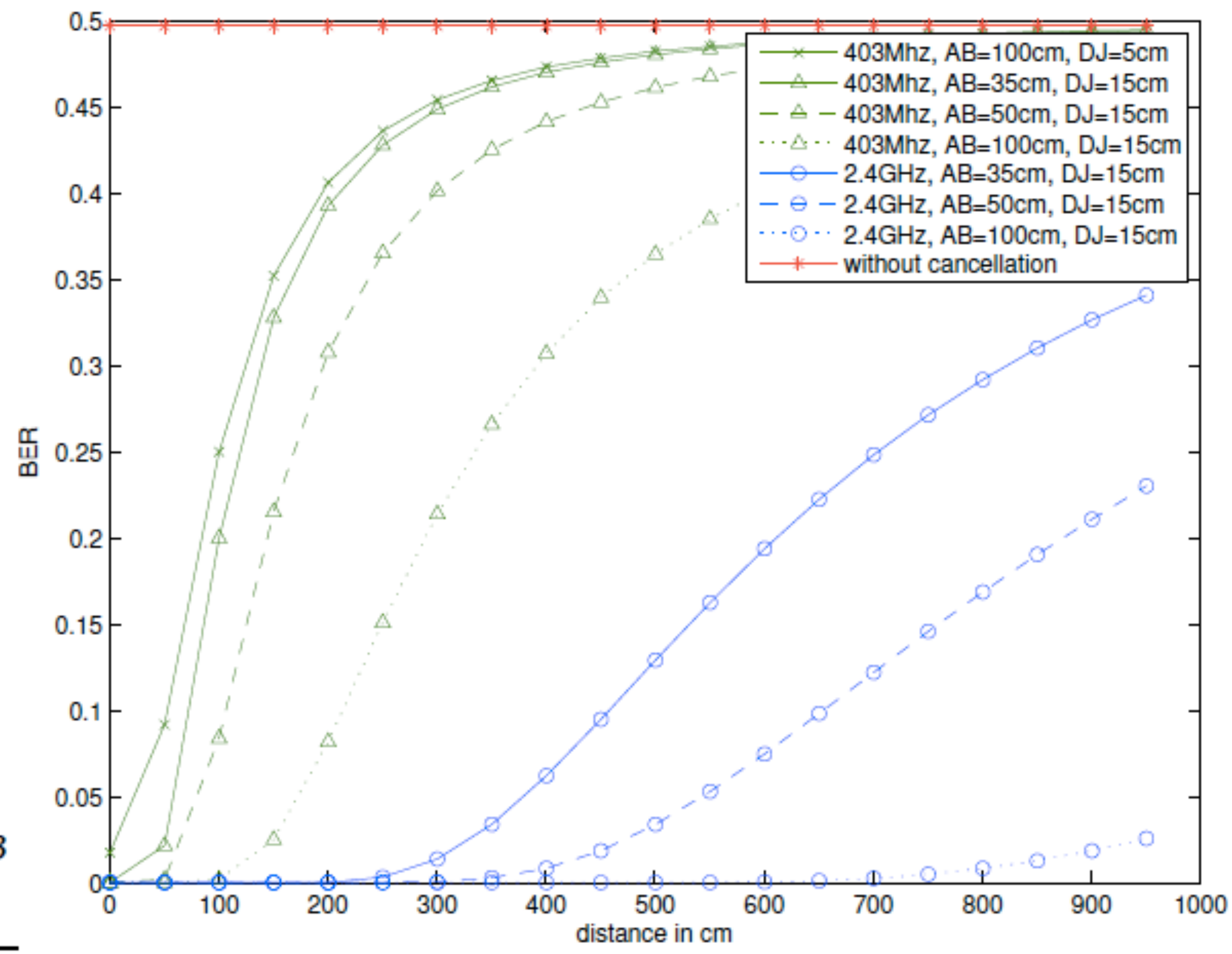
Impact of Imperfect Attacker Placement



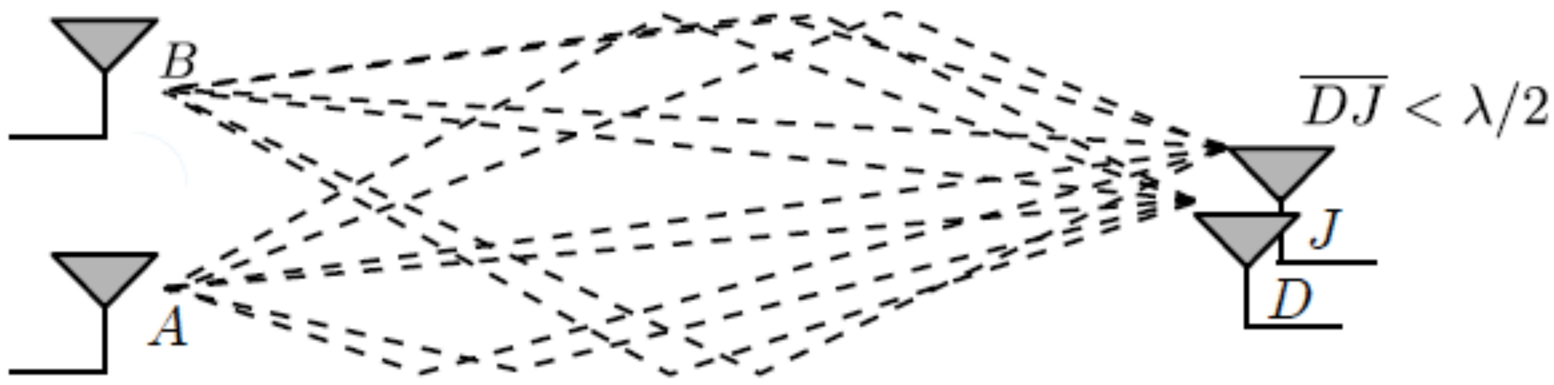
For $\delta = |\overline{AJ} - \overline{AD} - \overline{BJ} + \overline{BD}| > \lambda/5$, the attacker can recover the data signal with amplification (attenuation $< 0dB$).

Simulation Results



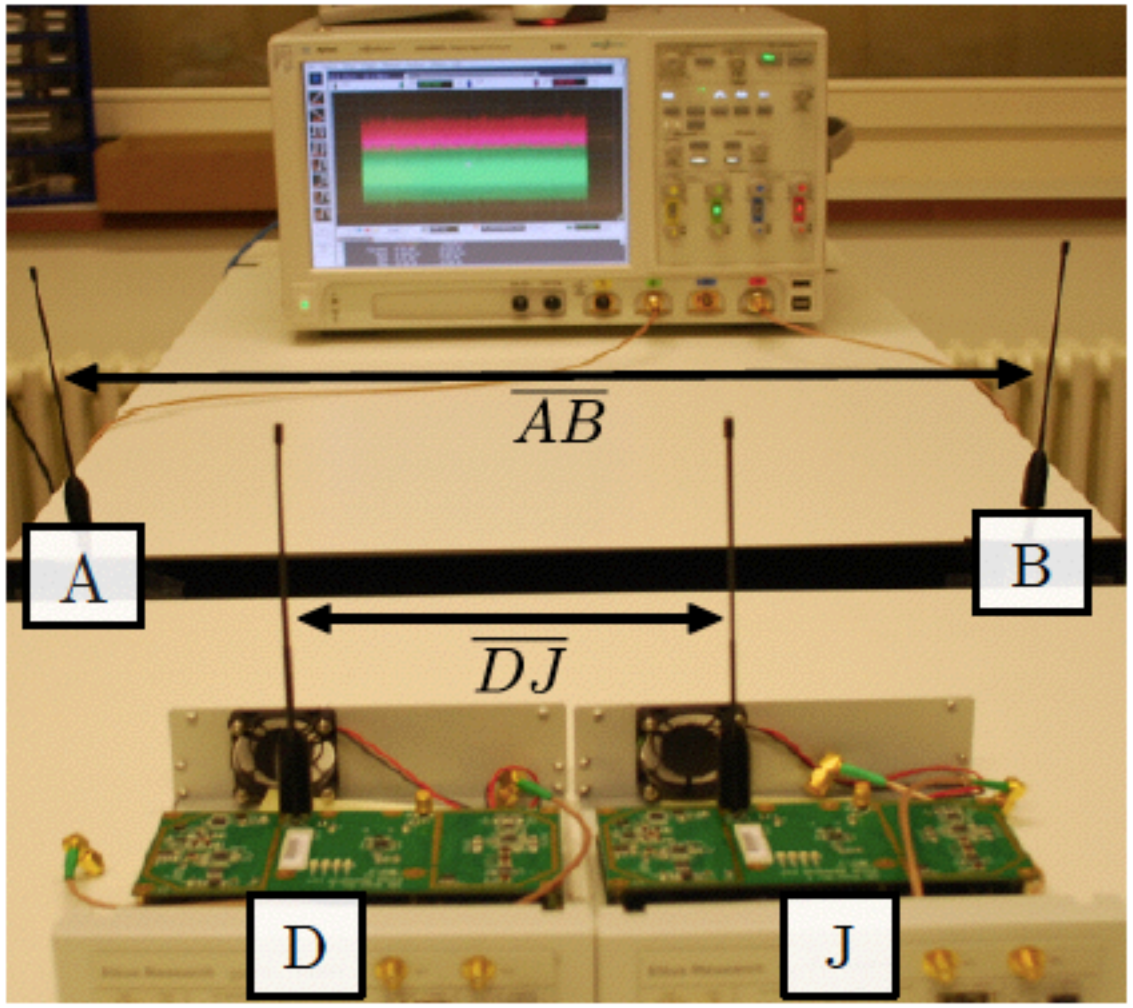


Multipath



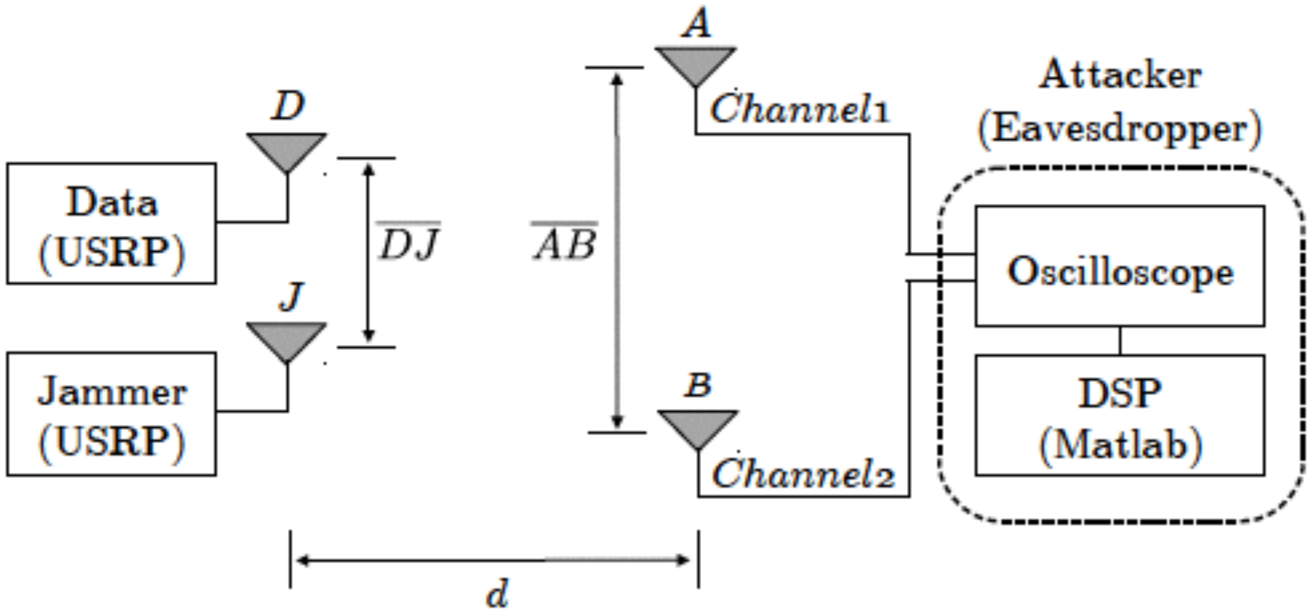
- So far, we looked at LOS channels, no reflections.
  - Multipath will Introduce more variation of amplitudes of components
  - Change the phase offsets of the signals
  - Potentially prevent us from canceling the jamming signals
  - We explore this with our experiments

Experimental Results



Parameter	Value
Attacker	
Antenna type	Omni-directional vertical
No. of antennas	2
Sampling rate	10 GSa/s
Data transmitter	
Antenna type	Omni-directional vertical
Carrier frequency	403 MHz
Bandwidth (D_{bw})	300 KHz
Packet length	67 bits
Data rate	150 Kbps
Jammer	
Antenna type	Omni-directional vertical
Jamming bandwidth	300 kHz
Noise type	Spectrum shaped random noise
Relative Power of Jammer	$\{20, 25, 30, 35\}$ dB

Table II
SUMMARY OF THE SYSTEM PARAMETERS IN EXPERIMENTAL SETUP.



ETH Zürich

Example Result

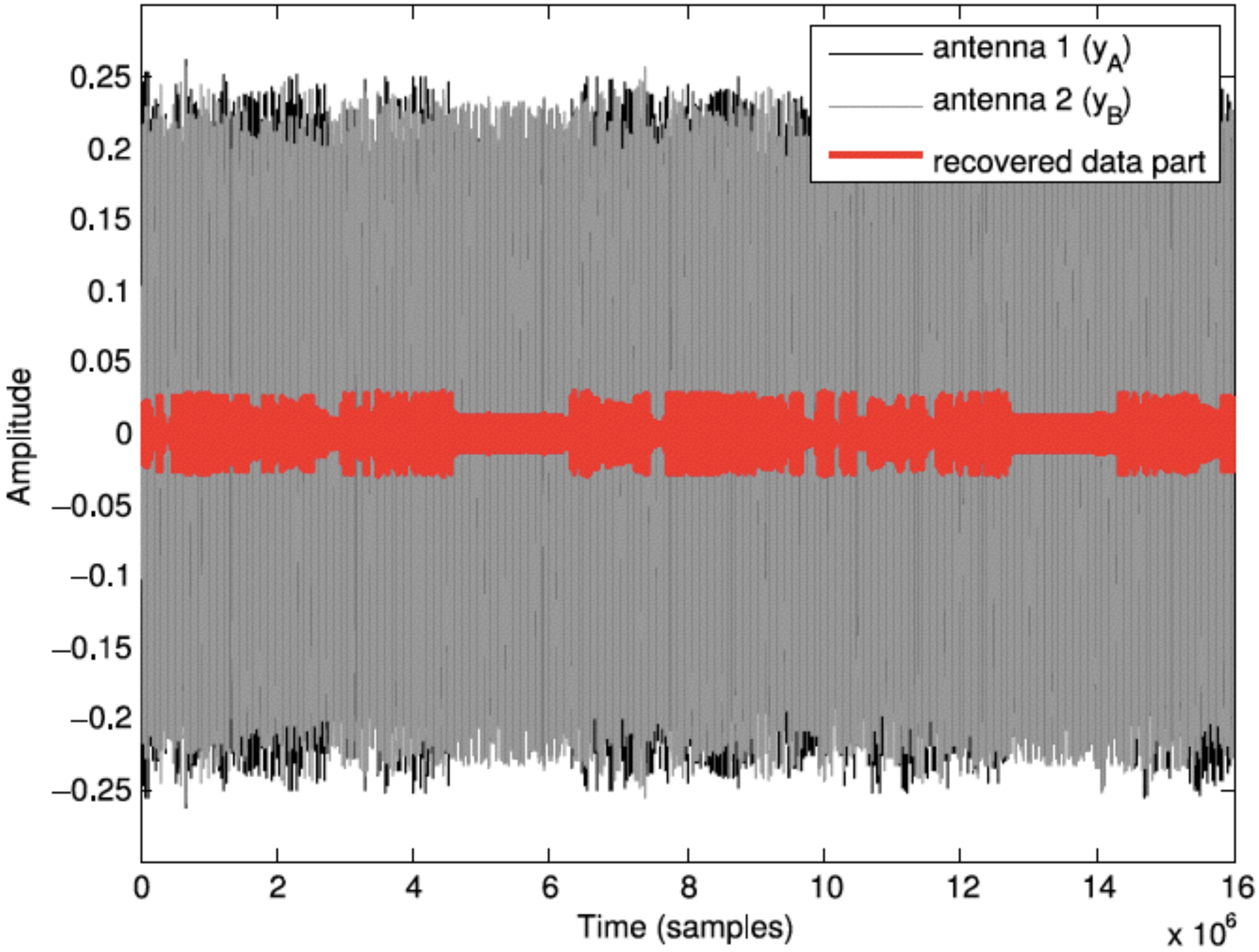
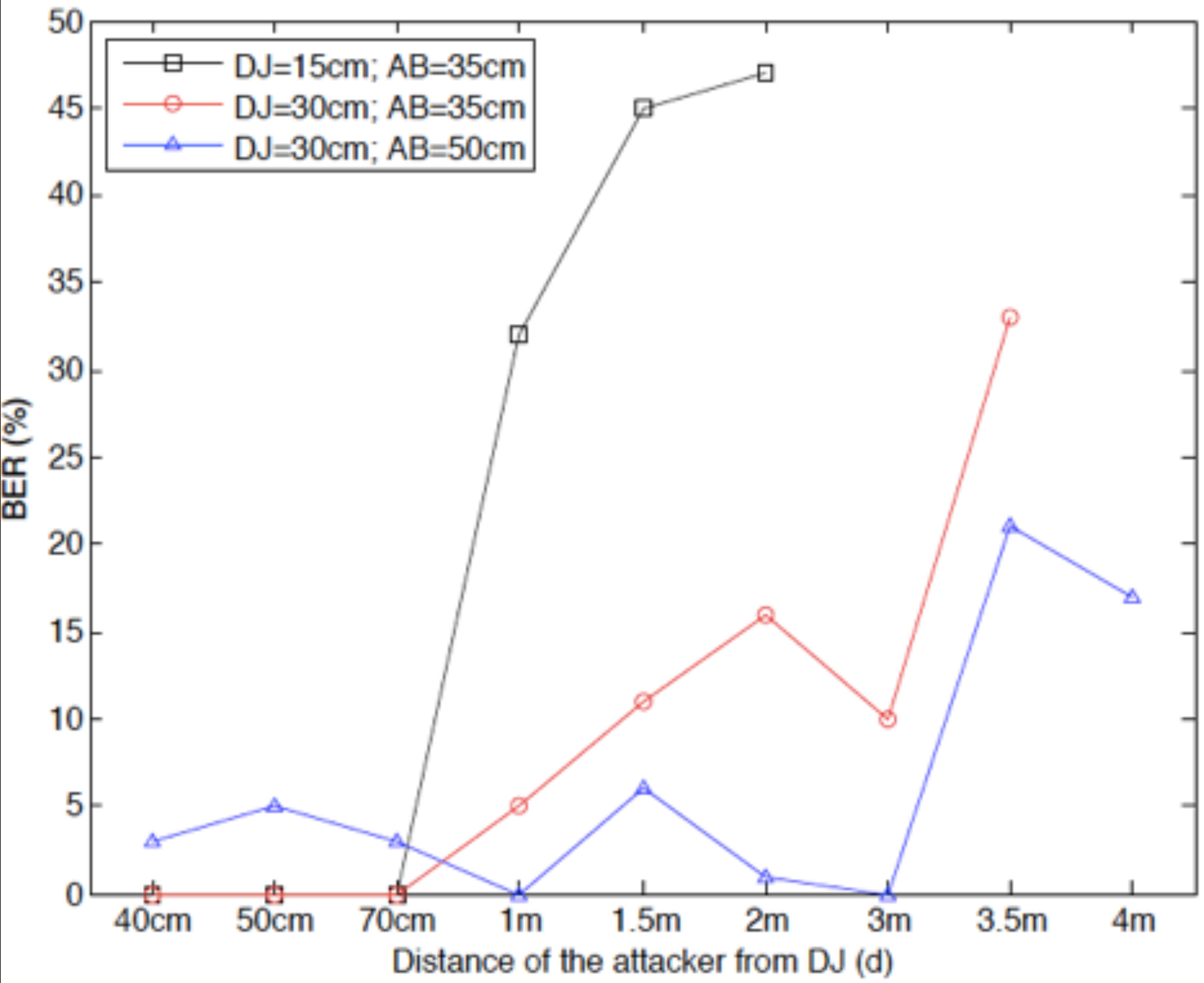
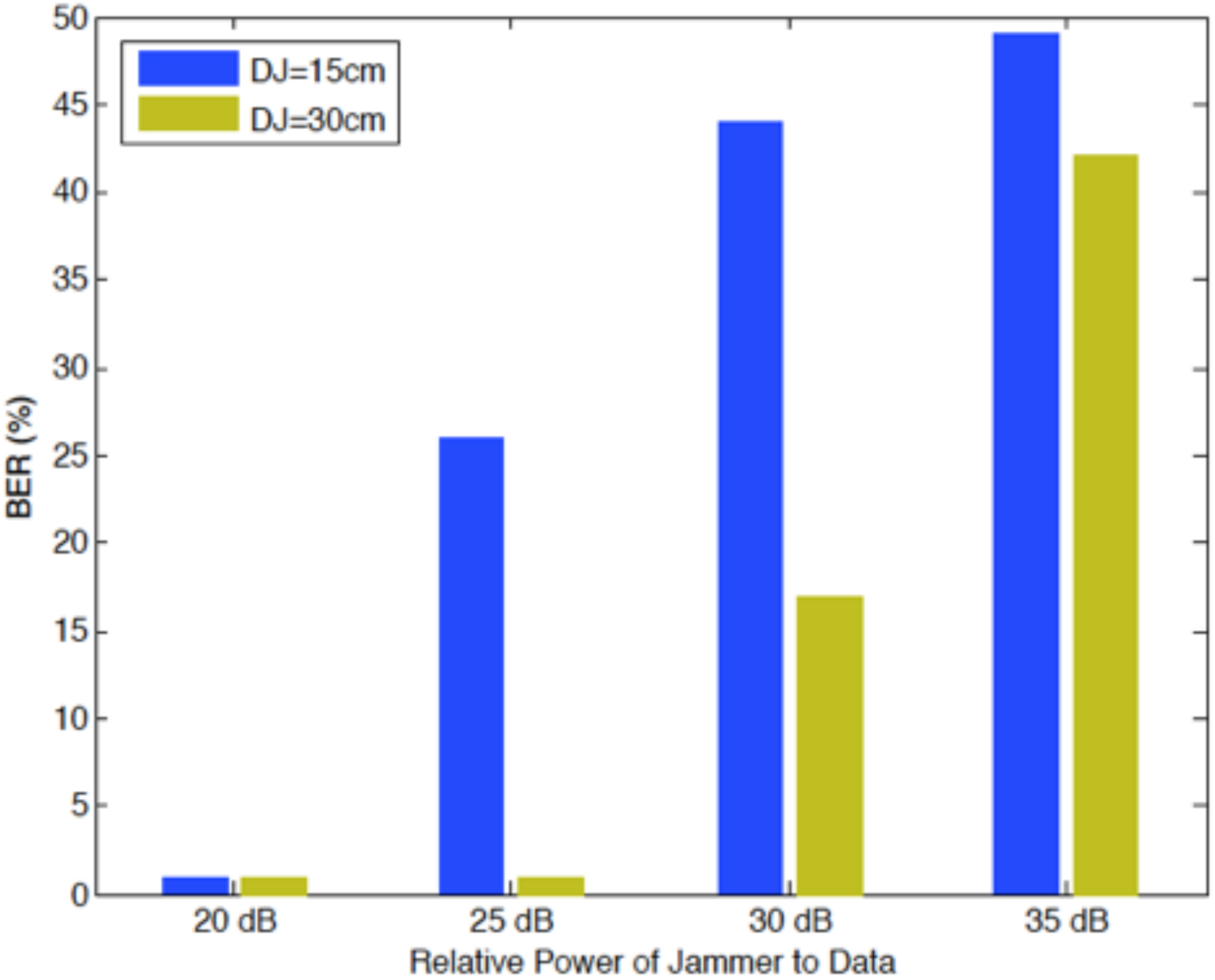
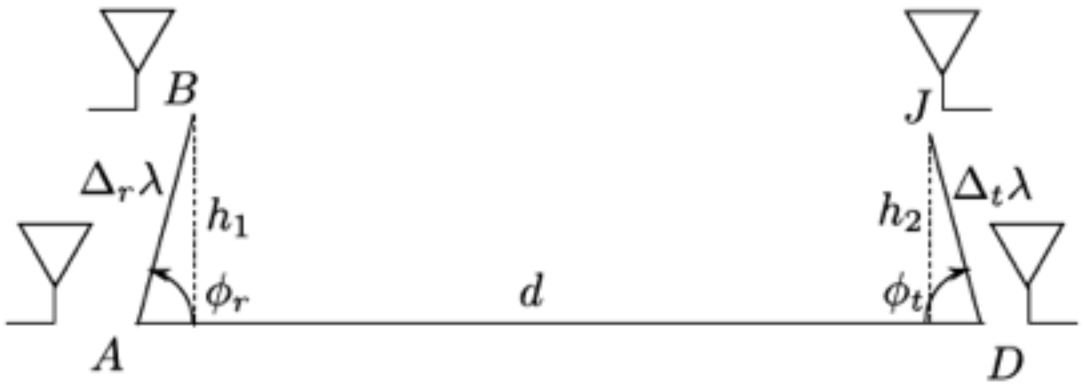


Figure 11. Black and gray waveforms correspond to signals acquired from two receiver antennas. Once the signals were aligned and subtracted, in red we can see the clearly visible, remaining data signal component.

Example Experimental Result







Lessons learned

- Using Jamming for confidentiality is not without risk
  - MIMO-like attacker can retrieve data despite DJ < $\lambda/2$.
  - The attack works from many locations (with some post-processing).
  - The attack can be effective even when jammer and source are mobile.

- Note: Friendly Jamming works well for access control.

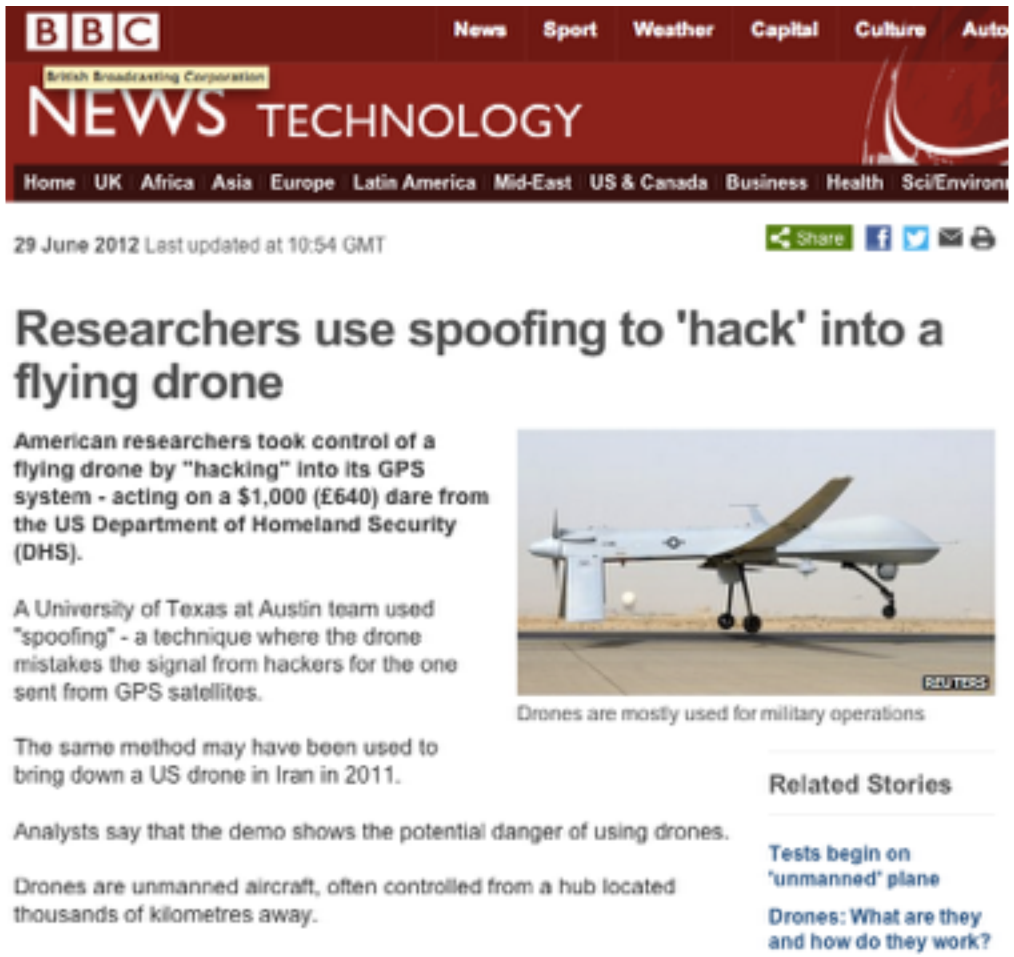
Summary

- Using channel characteristics and jamming for confidentiality is secure only in selected scenarios.
- There are many open questions about the utility and the security of the use of physical-layer schemes ***for confidentiality.***
- Given their guarantees, they are likely to be used not as sole but as complementary measures.
- The use of physical-layer schemes for access control seems more realistic and more robust to attacks.

Some other physical layer security topics

(that I believe are relevant and I enjoy working on)

(GPS) spoofing


BBC

News Sport Weather Capital Culture Auto

British Broadcasting Corporation

NEWS TECHNOLOGY

Home UK Africa Asia Europe Latin America Mid-East US & Canada Business Health Sci/Environ

29 June 2012 Last updated at 10:54 GMT

Share

Researchers use spoofing to 'hack' into a flying drone

American researchers took control of a flying drone by "hacking" into its GPS system - acting on a $1,000 (£640) dare from the US Department of Homeland Security (DHS).

A University of Texas at Austin team used "spoofing" - a technique where the drone mistakes the signal from hackers for the one sent from GPS satellites.

REUTERS

Drones are mostly used for military operations

The same method may have been used to bring down a US drone in Iran in 2011.

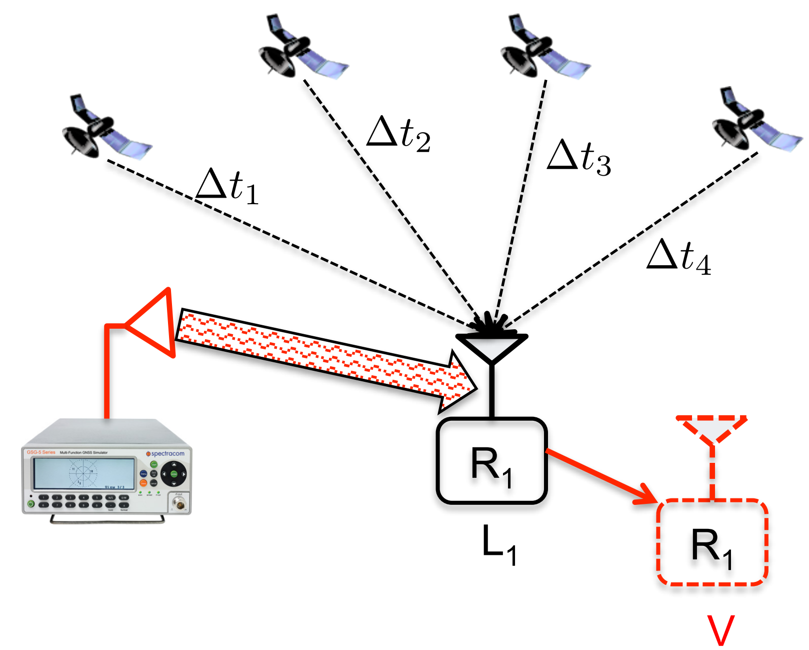
Analysts say that the demo shows the potential danger of using drones.

Drones are unmanned aircraft, often controlled from a hub located thousands of kilometres away.

Related Stories

Tests begin on 'unmanned' plane

Drones: What are they and how do they work?

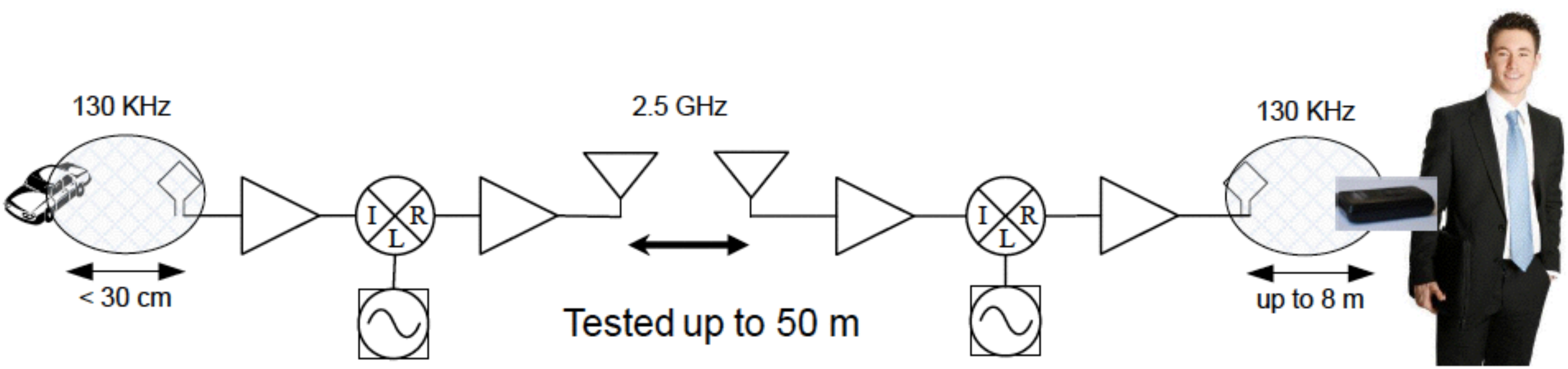


Relay Attacks (cars, payment systems)

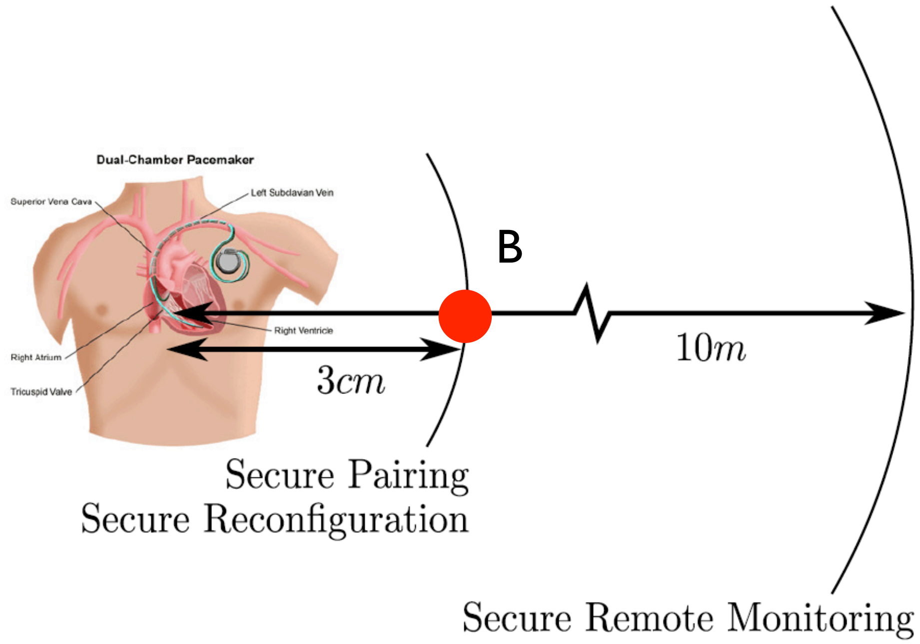
Hacking Cars with Keyless Systems Feasible and Practical, Swiss Researchers Say

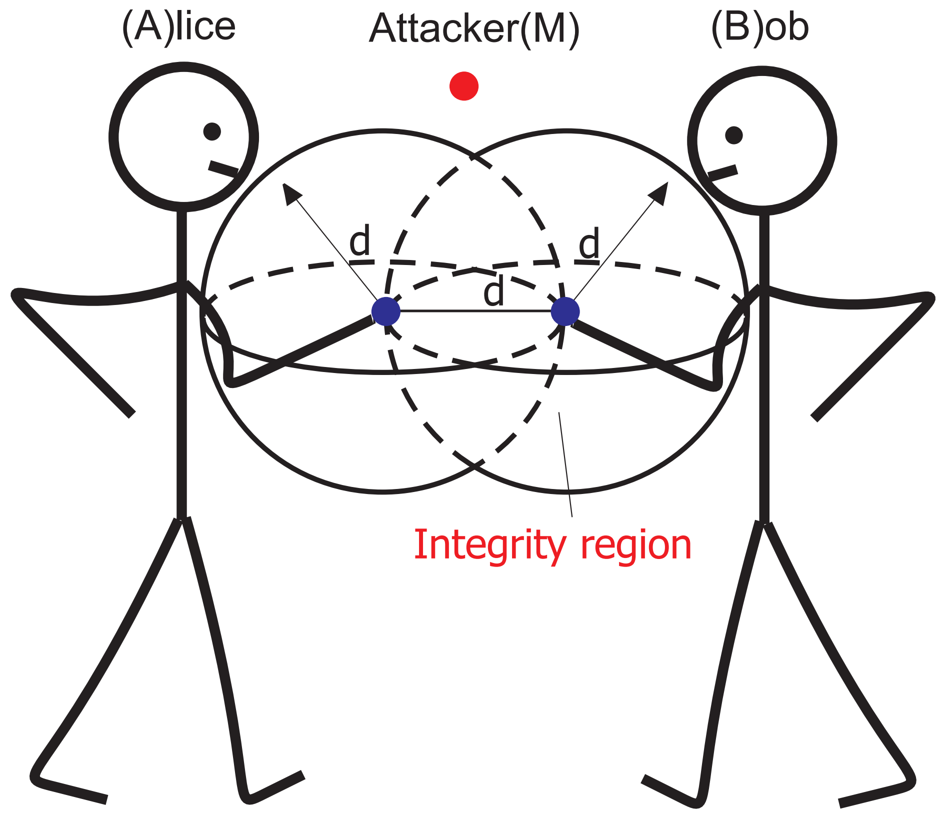
By Robert Charette
Posted 19 Jan 2011 | 16:15 GMT

Share | Email | Print



Distance Bounding



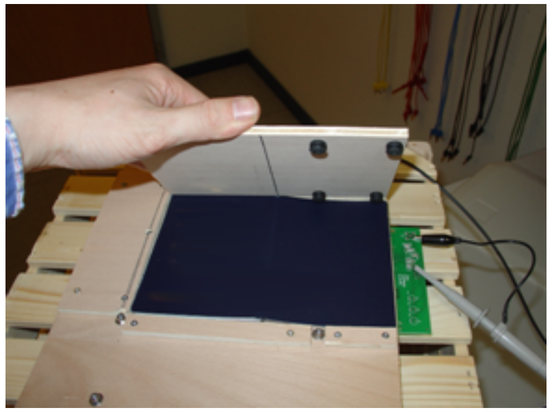


- Really stringent processing requirements (<1ns)
- We have many implementations of distance bounding radios and systems, based on Chirp, UWB … in analog and digital.

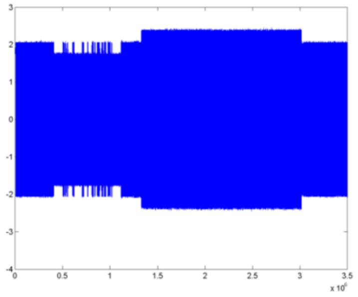
Device Fingerprinting / Physical Layer Identification

- RFID, WiFi, GSM/UMTS, UWB, …
- Tracking, access control, cloning detection …

Purpose-built HF (13.56MHz)
RFID Reader
ISO 14433 Type A and Type B



Acquisition antenna setup

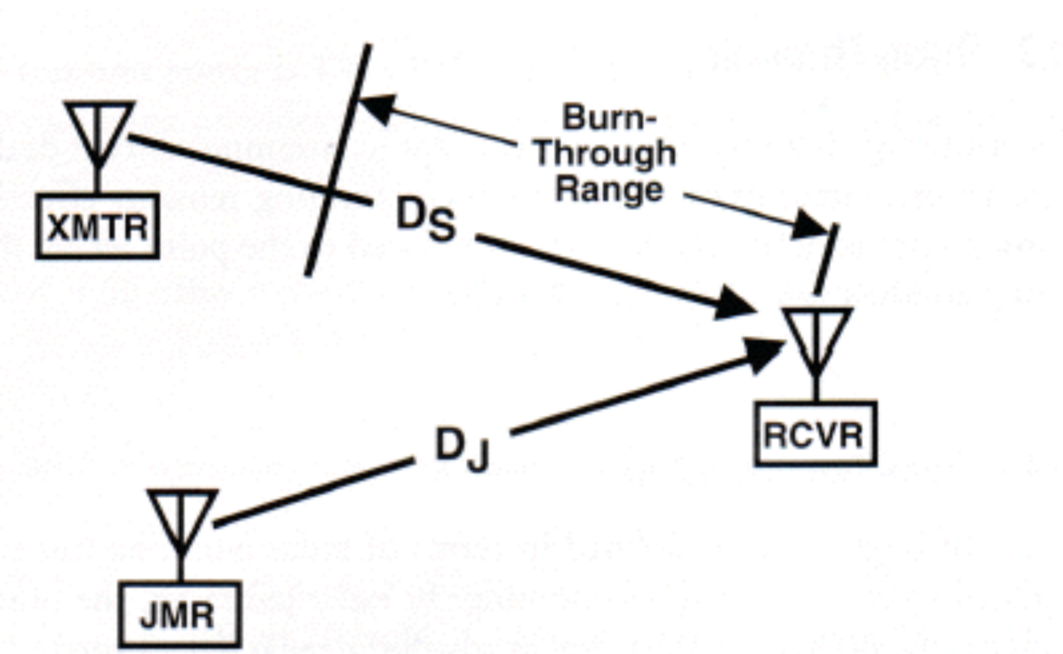


Captured signal transmission

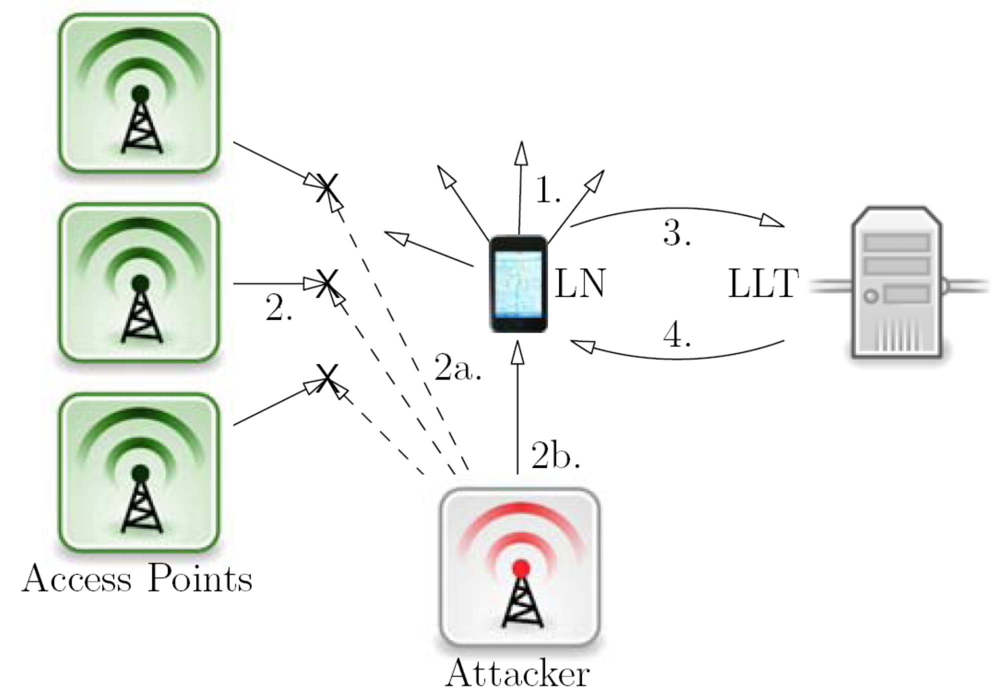
ETH Zürich

Jamming Resilience

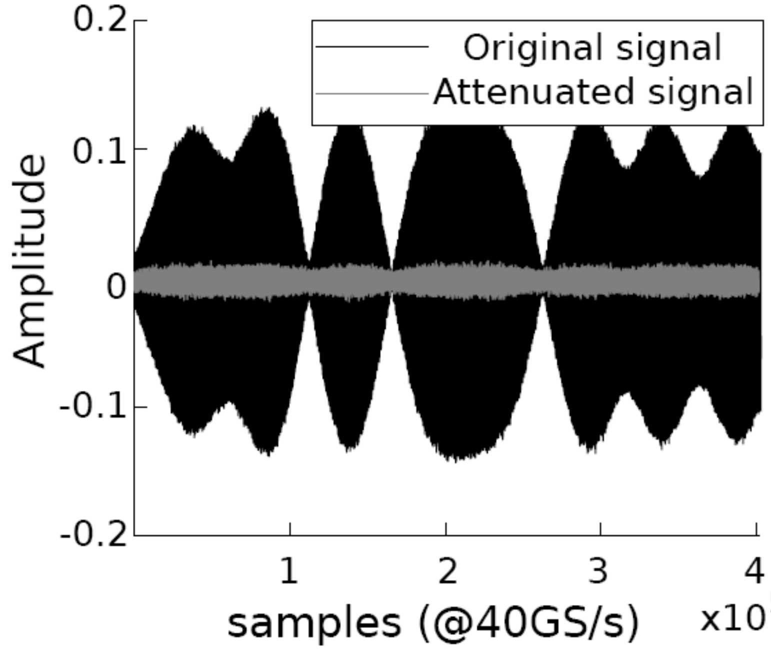
- Building jamming-resilient systems
- Detection of jamming
- Use of jamming for attacks



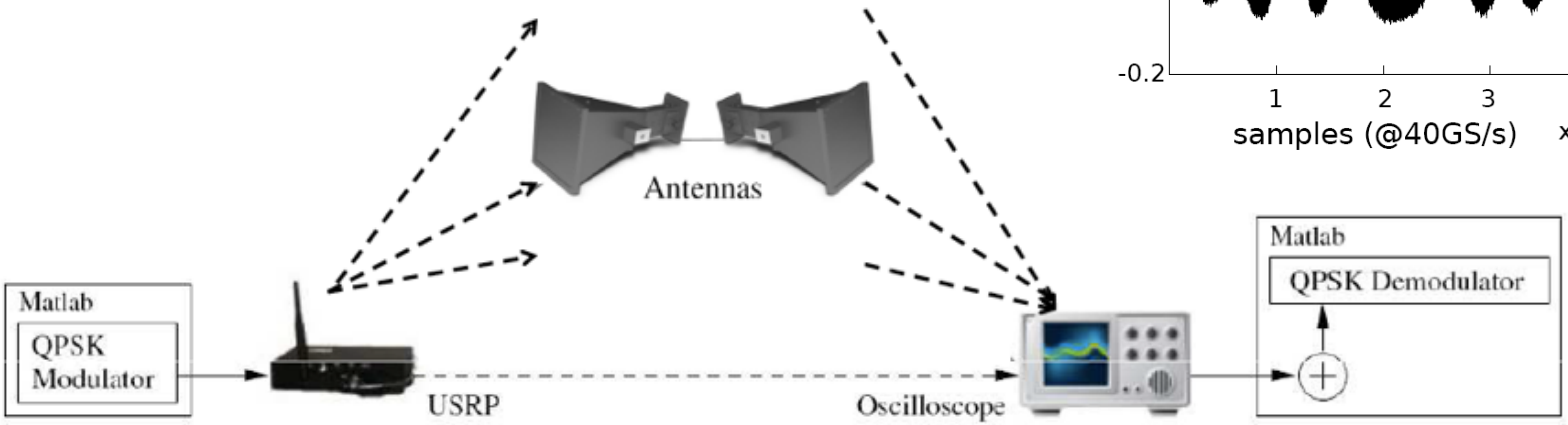
. Adamy, A First Course on Electronic Warfare



Signal Manipulation



- e.g., Signal Annihilation



- Simple setup creates artificial multi path that suppresses the transmitted signal at the receiver.
- The receiver does not know that any message was even sent by the transmitter.

- http://www.syssec.ethz.ch
- capkuns@inf.ethz.ch

FNSNF
Swiss National Science Foundation

ZISC Zurich Information Security & Privacy Center

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich