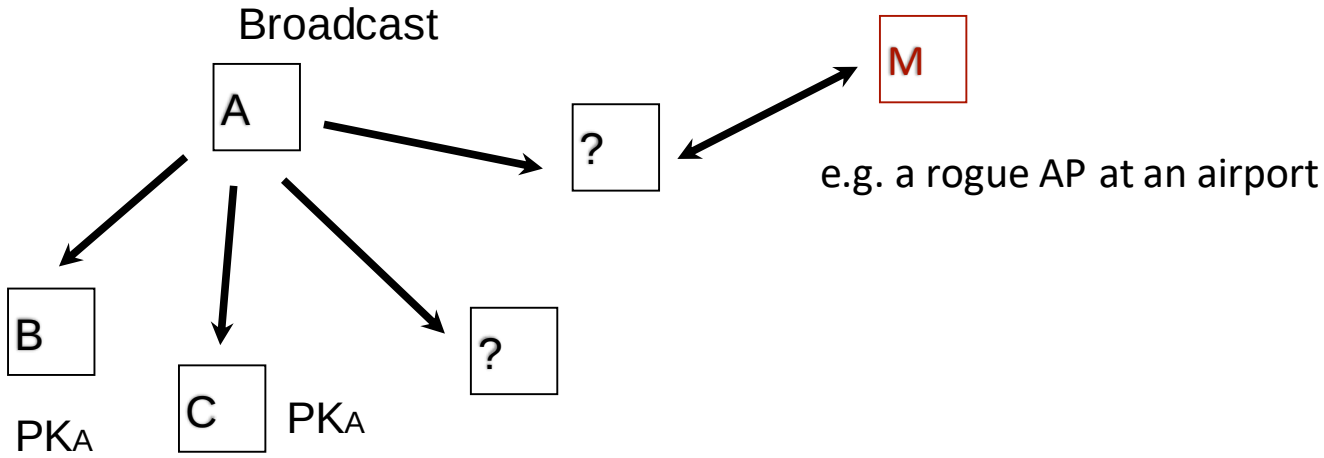

Physical-Layer
Based Security

Broadcast Authentication

Integrity Codes: Broadcast Authentication based on Presence Awareness

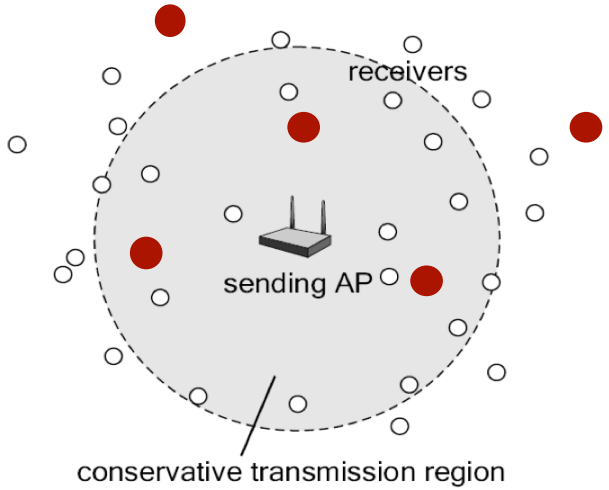
Broadcast Authentication

- Can we enable broadcast authentication without any pre-shared information?
  - *No pre-shared secret keys*
  - *No distributed credentials (e.g., certificates/public keys)*



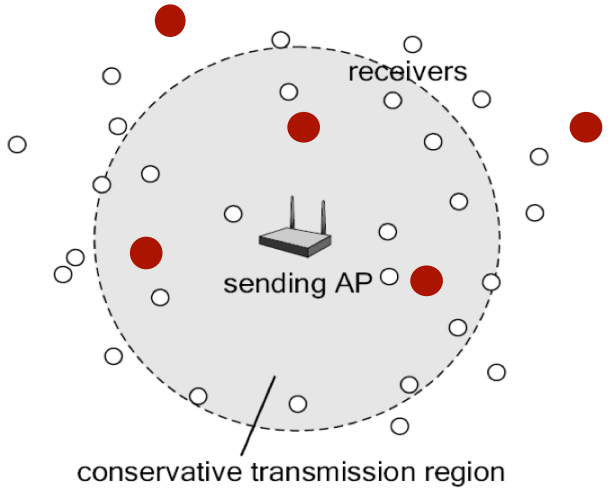
Integrity Codes

- Scenario:
  - The receiver is in direct power range of the sender, *and it knows it!*
  - E.g., a user walks into a university building equipped with university access points.
  - The attacker is not restricted in terms of location or number of devices that it has/deploys.



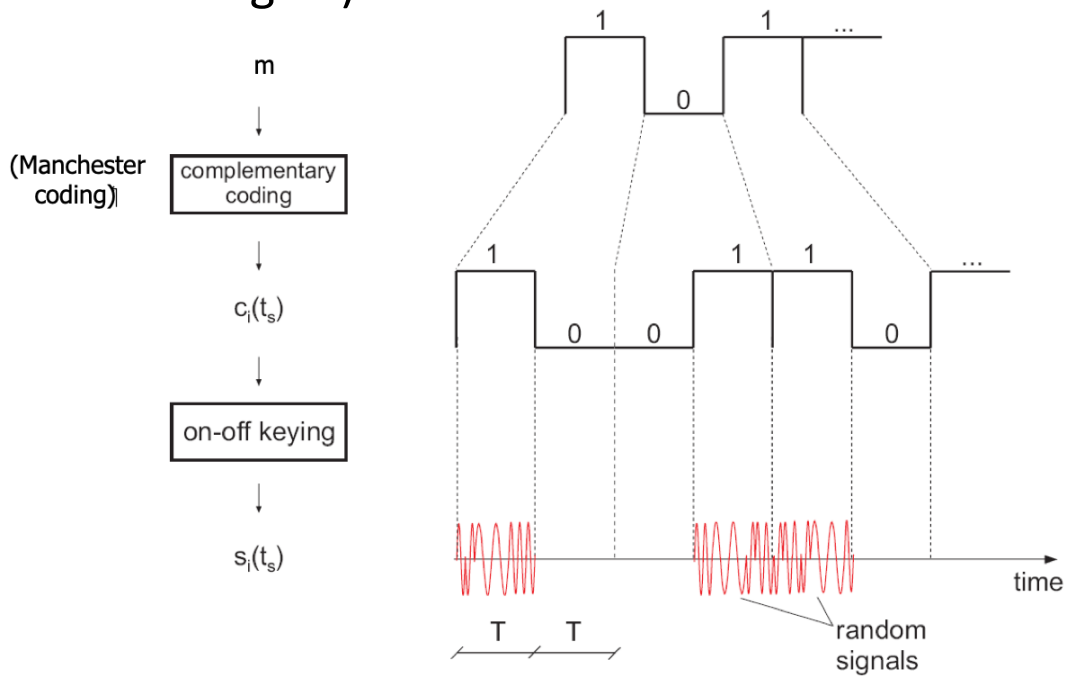
Integrity Codes

- Scenario:
  - The receiver is in direct power range of the sender, *and it knows it!*
  - The receiver *knows a communication channel* (e.g., channel 5)
  - The sender is *always on and transmitting*



Integrity Codes: Protocol

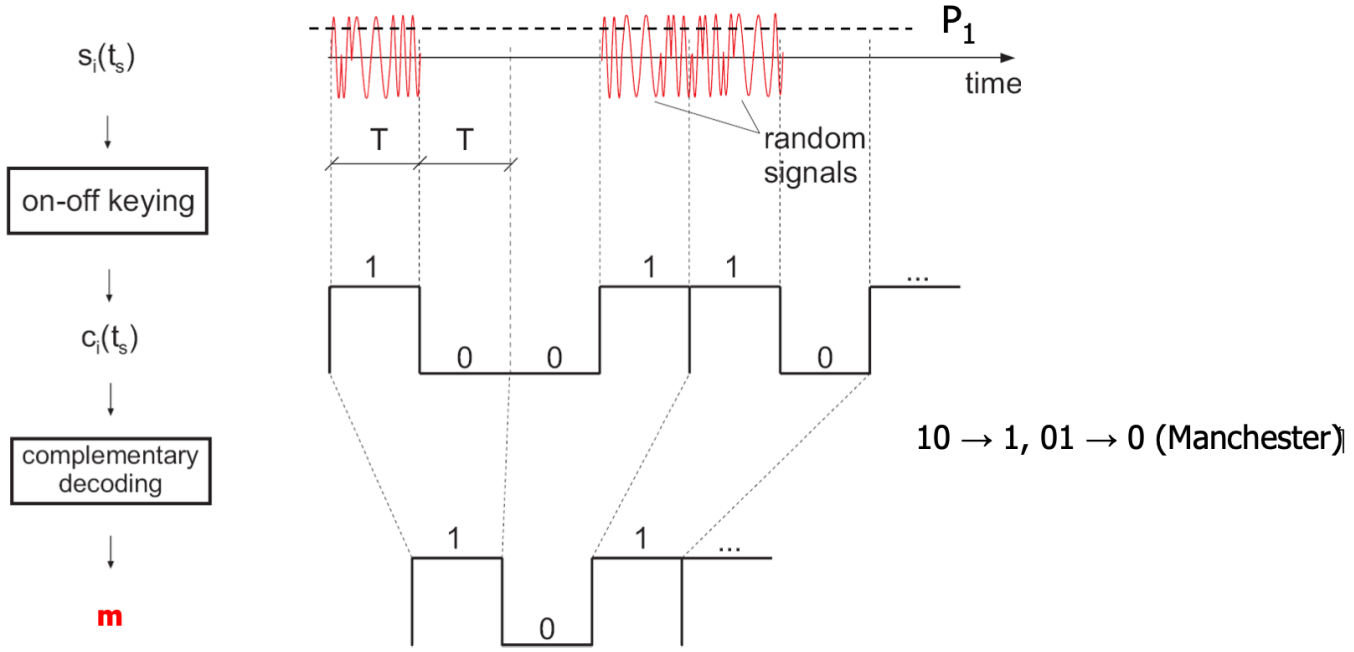
- *Transmission (**S**ender):*
  - *m* spread from k bits to 2·k bits (1→10, 0→01), H(m) = k
  - each resulting bit is then transmitted using on-off keying (each "1" is a freshly generated random signal)



H(m) = the number of bits "1" in m (Hamming weight)

Integrity Codes: Protocol

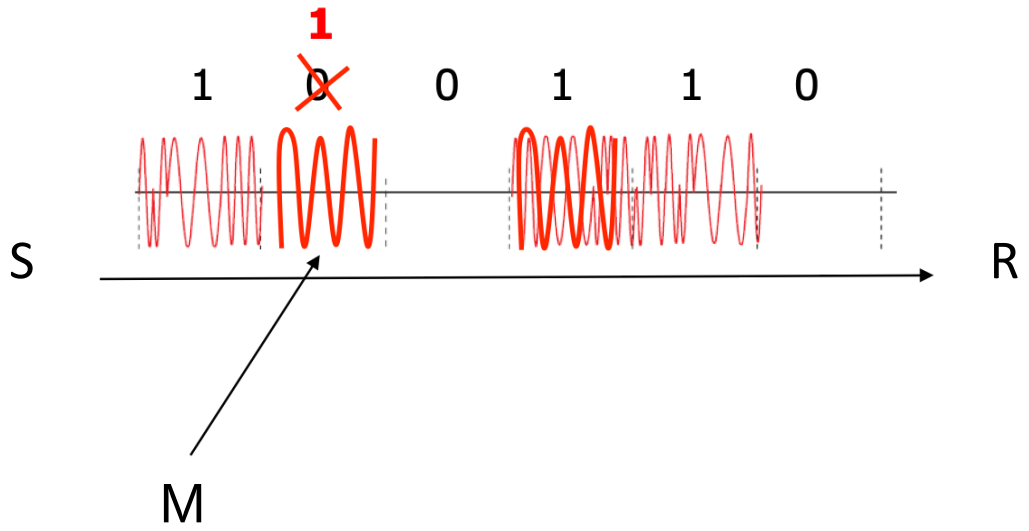
- *Reception (**R**eceiver):*
  - Presence of *any signal* (>P1) during T interpreted as “1” Absence of signal (<P0) during T interpreted as “0”
- *Integrity Verification*
  - IF H(m)=|m|/2 THEN “m” was not modified in transmission



Integrity Codes: Analysis

- Message Hamming weight is a public parameter H(m)=2
- Attacker can change 0 → 1 and NOT 1 → 0 (except with ε)
- The sender is permanently transmitting

=> The receiver can therefore detect all modifications of the message

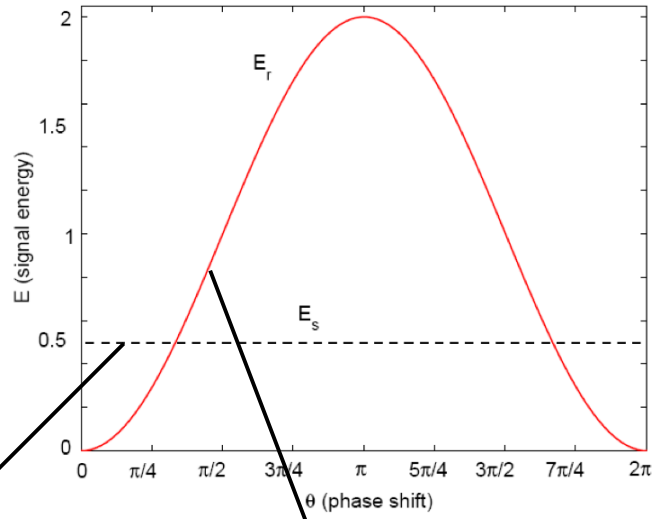


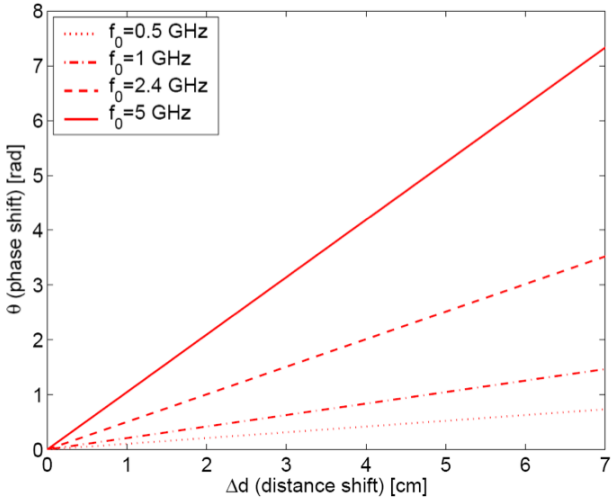
Integrity Codes: Analysis

- Probability of signal annihilation 1→0

$$\underbrace{r(t)}_{\text{receiver}} = \underbrace{\cos(\omega_0 t)}_{\text{sender}} - \underbrace{\cos(\omega_0 t - \theta)}_{\text{adversary}}, \text{ where } \theta \in [0, 2\pi)$$

$$E_r = \int_0^{T_s} r^2(t)dt \approx 2T_s \sin^2\left(\frac{\theta}{2}\right)$$





Error in attacker's distance estimation

Energy of the sender's signal.

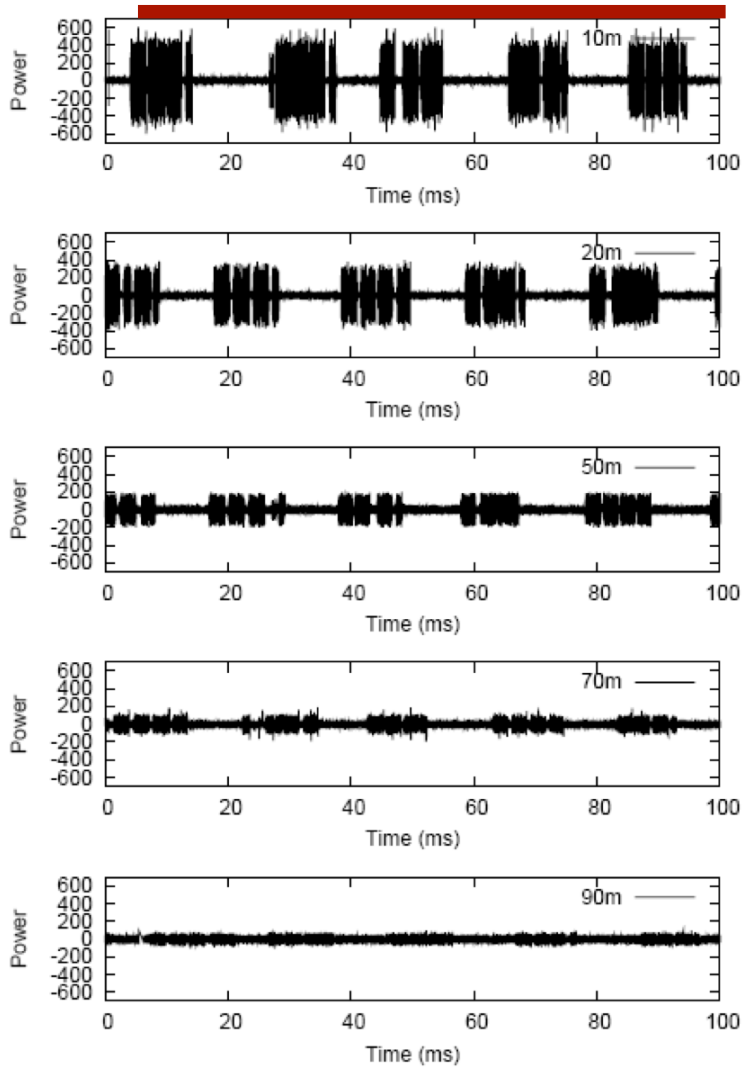
Energy of the combined sender's and adversary's signal.

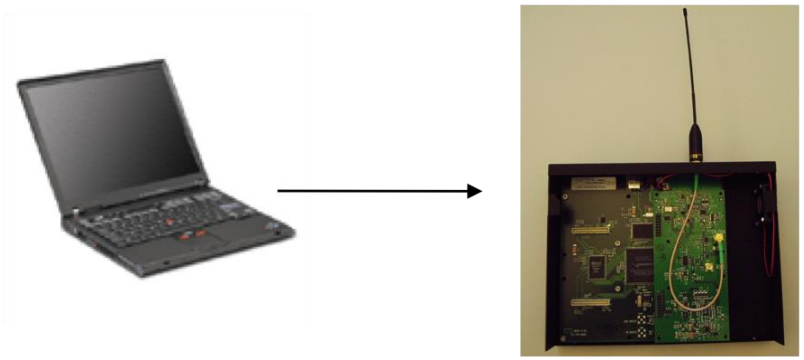
Integrity Codes: Analysis

- How can one handle messages of arbitrary sizes?
  - Receiver does not have to know the length of the message in advance
  - A valid message received between two subsequent i-delimiters is authentic.
  - For Manchester coding, an optimal integrity-delimiter is simply *111000*

  - *"111000"* cannot be a part of any codeword

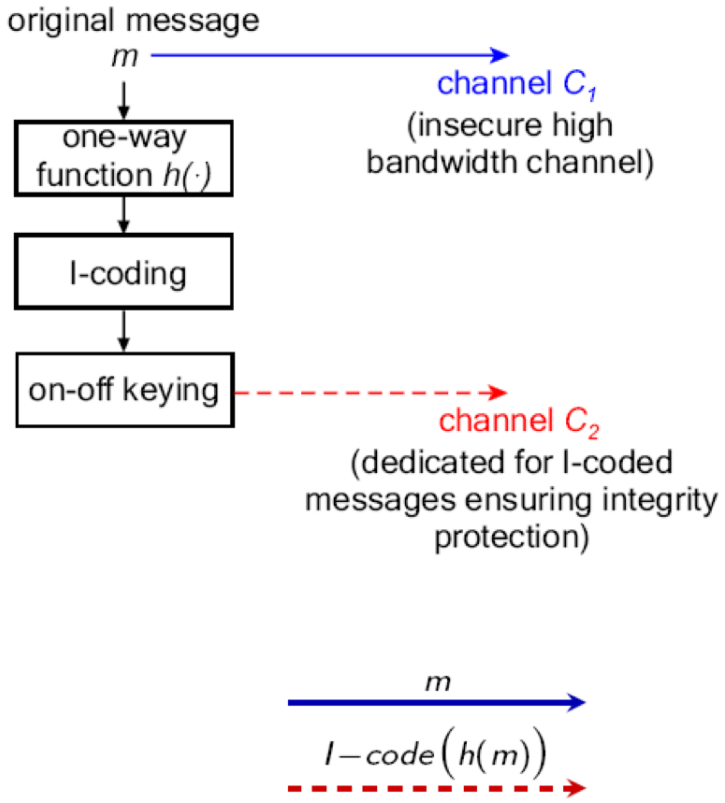
Integrity Codes: Implementation





Integrity Codes: Optimizations

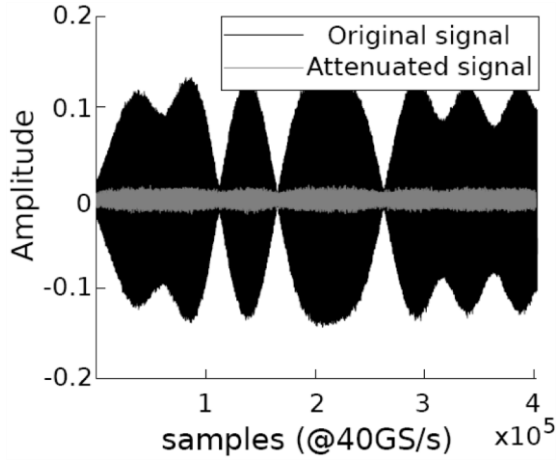
- Integrity Coded channel is slow

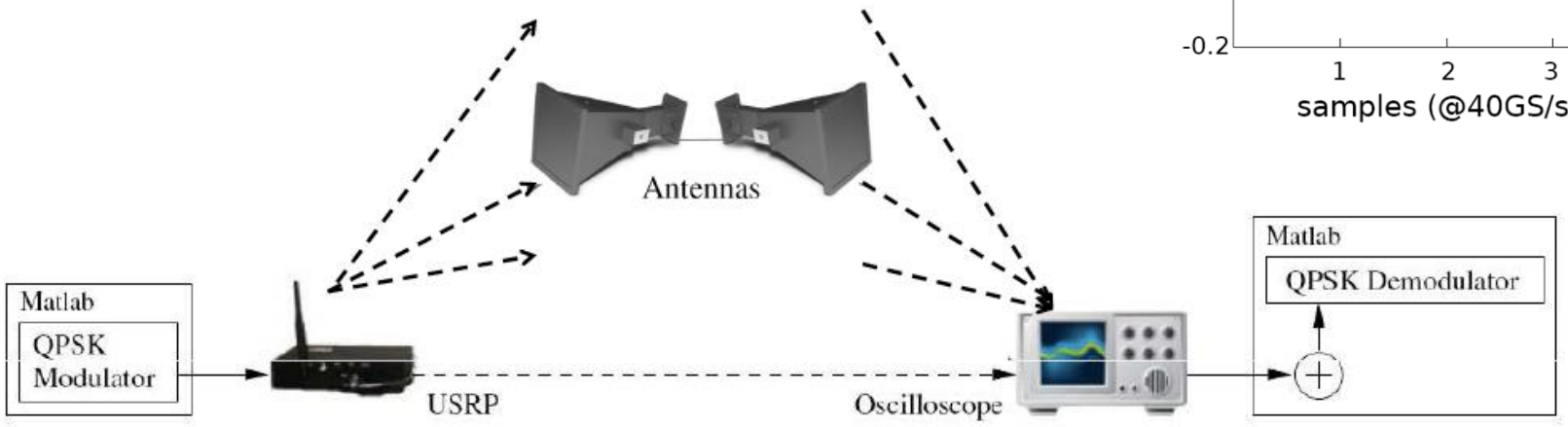


Can the attacker influence the channel?

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.

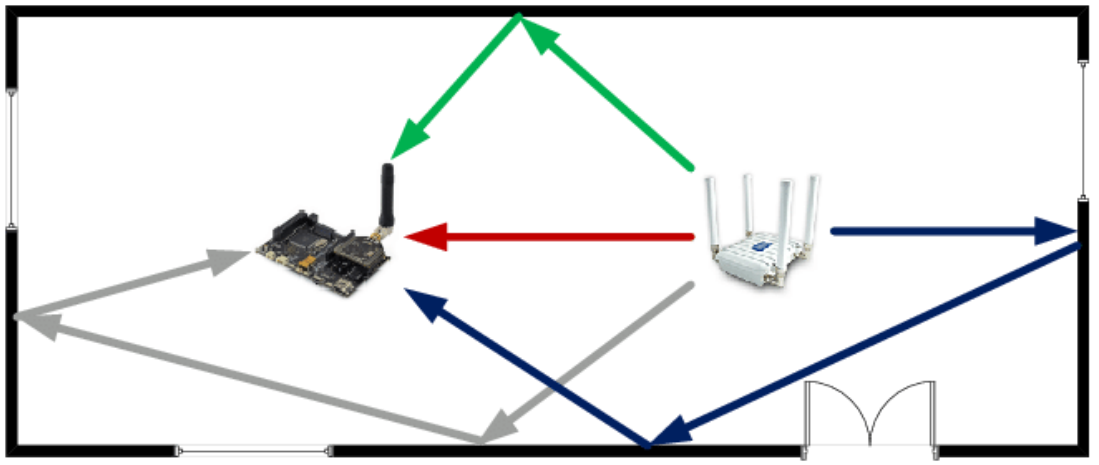
2- Physical-Layer Based Security

References / Recommended Readings

- On the Limitations of Friendly Jamming for Confidentiality. Nils Ole Tippenhauer, Luka Malisa, Aanjhan Ranganathan, Srdjan Capkun (IEEE Symposium on Security and Privacy 2013)
- Fundamentals of Wireless Communication, David Tse, Cambrige University Press, Chapter 7: "MIMO 1 : Spatial Multiplexing and Channel Modeling"
- Fundamentals of Wireless communication, David Tse, Cambridge University Press, Chapter 2: “The wireless channel”, https://web.stanford.edu/~dntse/Chapters_PDF/Fundamentals_Wireless_Communication_chapter2.pdf
- Physical Layer & Telecommunications Security Knowledge Area Version 1.0.1, Srdjan Čapkun, ETH Zurich, Chapter 1: “Physical Layer Schemes for Confidentiality, Integrity and Access Control” https://www.cybok.org/media/downloads/Physical_Layer_v1.0.1.pdf

Securing Wireless Networks is challenging...

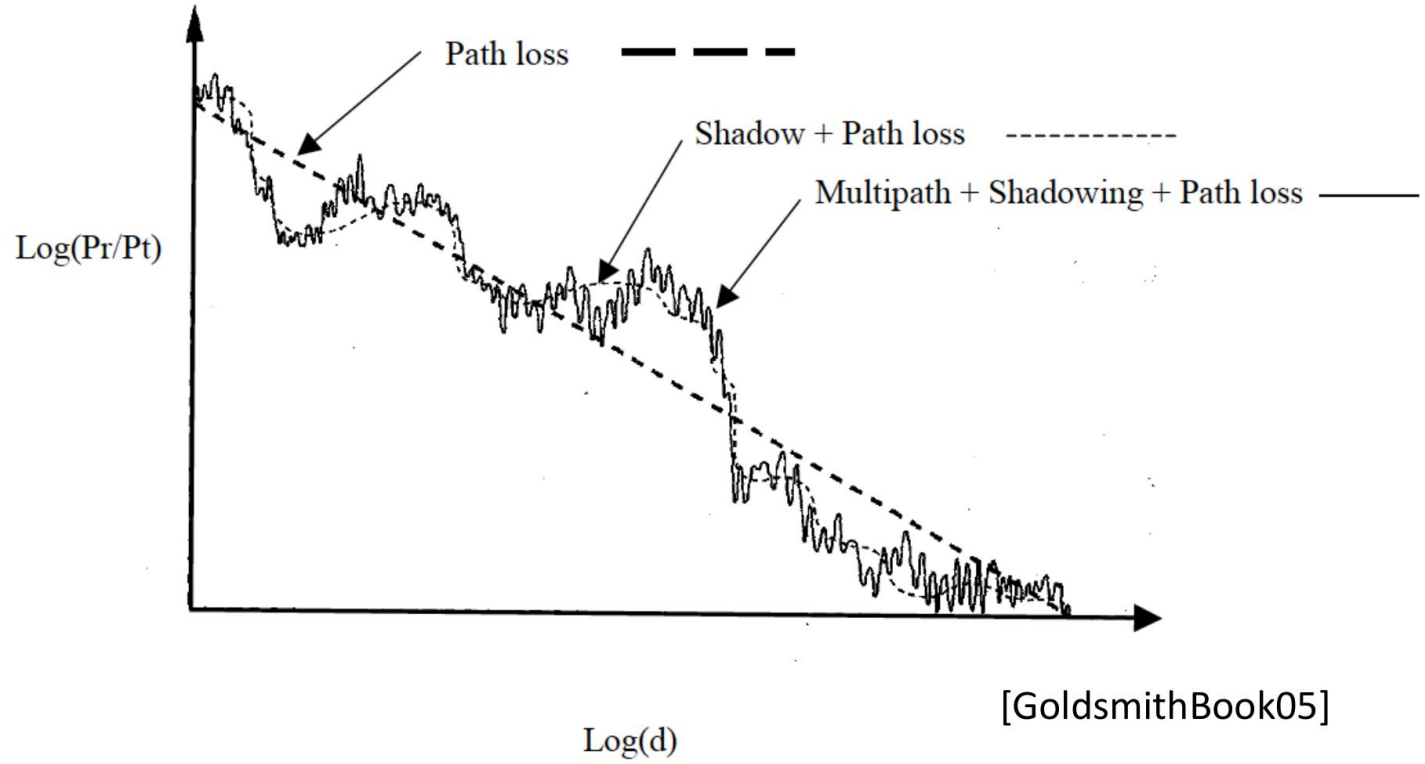
- Medium is shared
- Broadcast nature
- Eavesdropping, Modification, Blocking of messages



However...

- Radio signals are affected by reflection, diffraction, scattering
- Complex multi-path behavior
  - Frequency and position dependent random components

Uncertainty of the Wireless Channel II

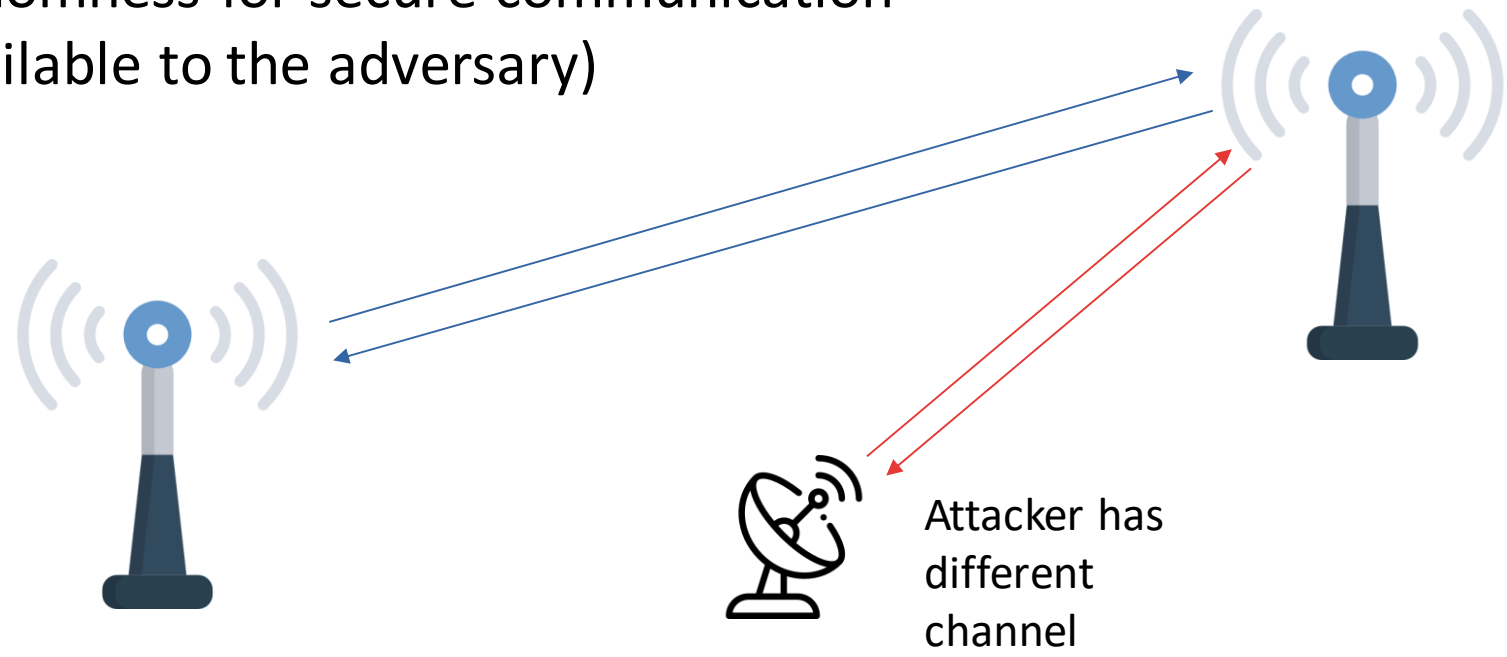


[GoldsmithBook05]

- Attacker does not know and cannot remotely measure multipath fading components

We would like to exploit these physical phenomena

- Within a short time span, communicating parties can measure highly correlated channels
  - Channel reciprocity
  - Establish shared randomness for secure communication (information is unavailable to the adversary)

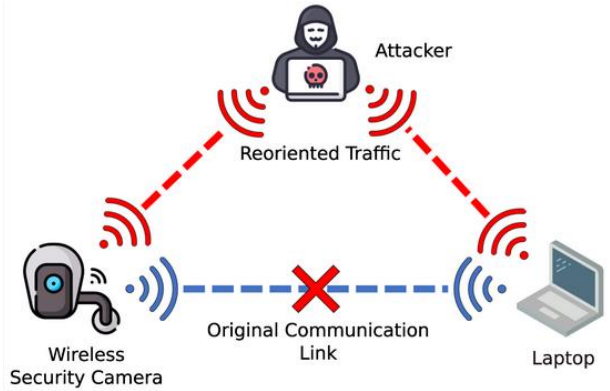


Physical-Layer Schemes for

Confidentiality
Eavesdropping messages in the air should be prevented

Integrity
Modifying messages in the air should not be possible

Access Control
Physical-layer properties as an authentication factor, e.g. closeness implies access granted (NFC)



https://www.mdpi.com/2076-3417/11/16/7228/htm
https://www.logicfireandsecurity.com/security/access-control/
https://www.softwaretestinghelp.com/best-wifi-packet-sniffer-review/

Important Note

- Modern-day cryptography provides many protocols to assure confidentiality, integrity and authenticity of data transmitted using radio signals
  (when parties are associated with each other / share a secret)

- If no pre-shared secrets are available, cryptographic protocols operating at higher layers of the protocol stack are not sufficient and physical-layer constructs can be viable solutions
  - Especially true if information exchange is not the only goal, e.g., in a positioning system

Types of Physical-Layer Schemes

Number of Endpoints:

SISO
Single input – single output.
Generally, communicating parties have one endpoint / antenna each

MIMO
Mulitiple output – multiple input.
Devices have multiple front-ends / antennas

Exploited Phenomenon:

Channel Reciprocity

Secrecy of Channel + Channel Dependence

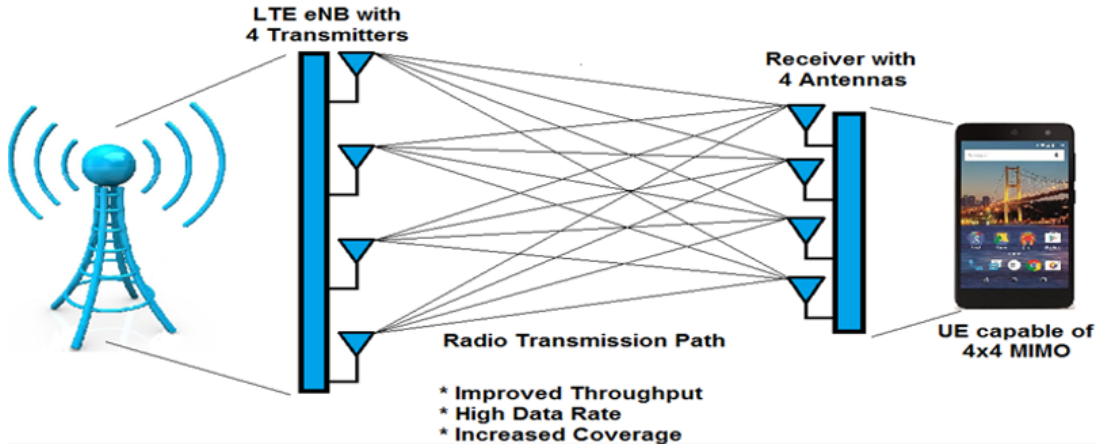
Beam-forming / Beam-steering

Interference + Noise-based

Types of Physical-Layer Schemes

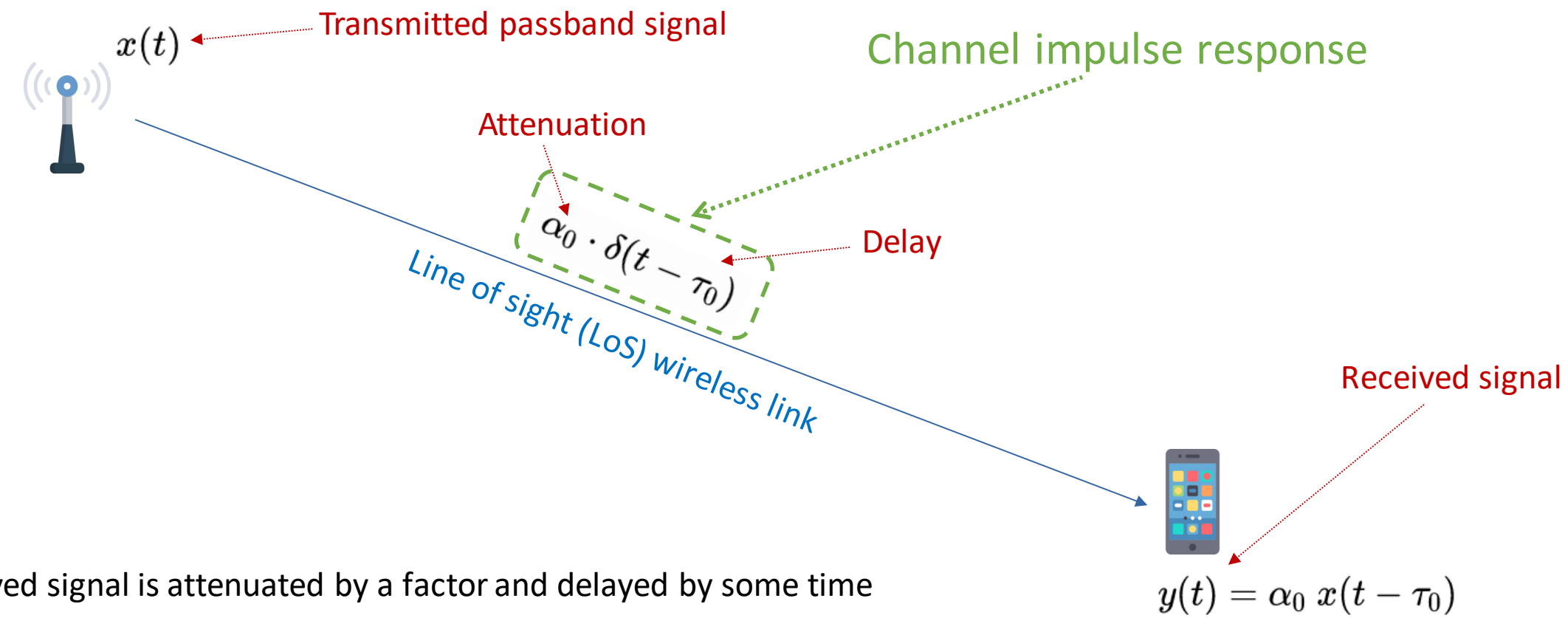
SISO:

MIMO:



https://www.4gmobiletech.com/multiple-input-multiple-output

Wireless Channel: Single Path Model



Received signal is attenuated by a factor and delayed by some time

Wireless Channel: Input/Output

If $x(t)$ is the transmitted passband signal, we can compute the received signal by convolving the transmitted signal with the channel impulse response:

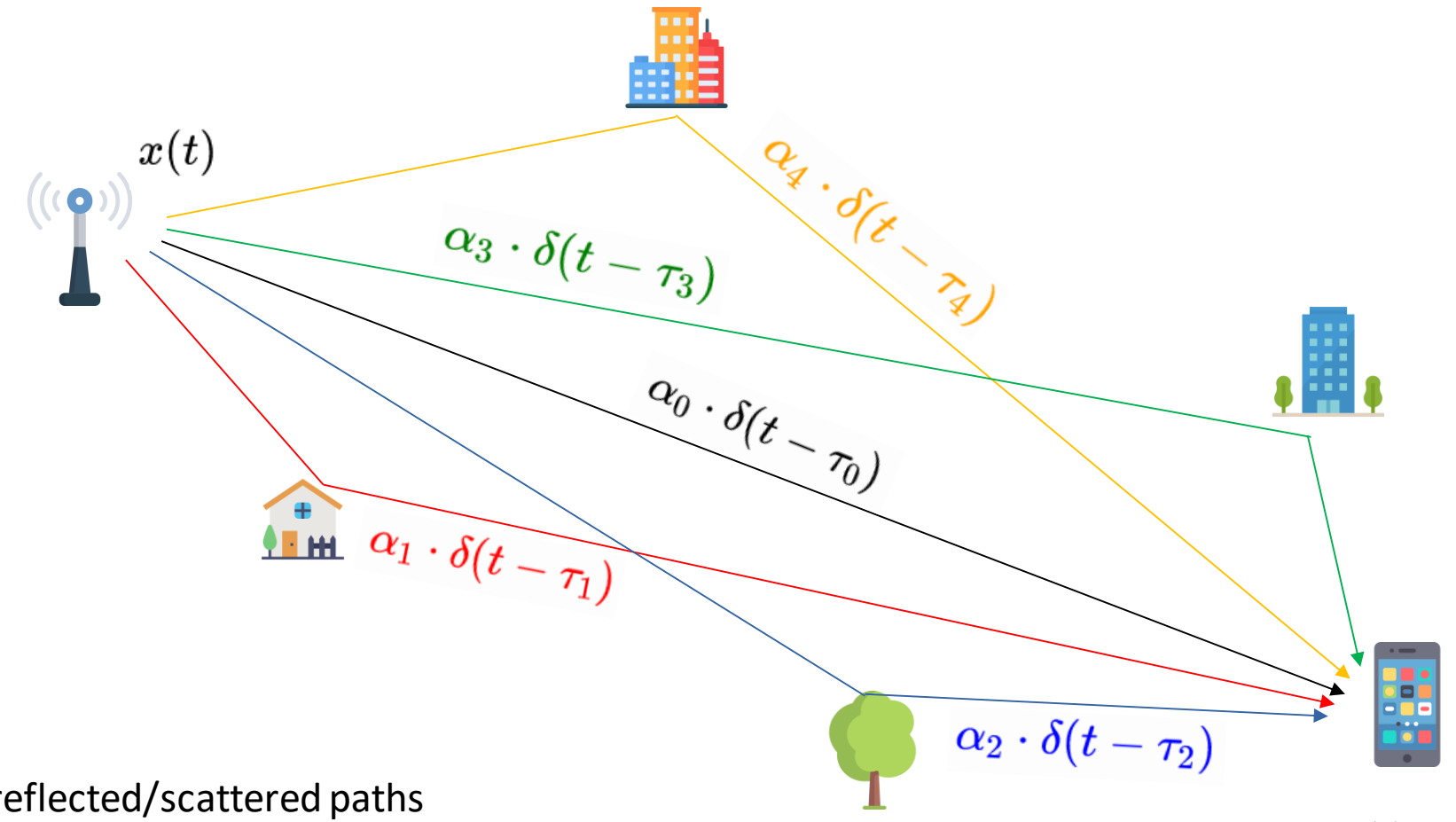
$$
\begin{aligned}
y(t) = (x \star h_0)(t) &= \int_{-\infty}^{\infty} x(t-\tau) \cdot h_0(\tau)\, d\tau \\
&= \int_{-\infty}^{\infty} x(t-\tau) \cdot \alpha_0\, \delta(\tau - \tau_0)\, d\tau \\
&= \int_{-\infty}^{\infty} x(u) \cdot \alpha_0\, \delta(t-u-\tau_0)\, du \\
&= \int_{-\infty}^{\infty} x(u) \cdot \alpha_0\, \delta(u-(t-\tau_0))\, du \\
&= \alpha_0 \cdot x(t-\tau_0)
\end{aligned}
$$

where we have used the channel impulse response from before, i.e.,

$$h_0(\tau) = \alpha_0 \cdot x(\tau - \tau_0)$$

as an example.

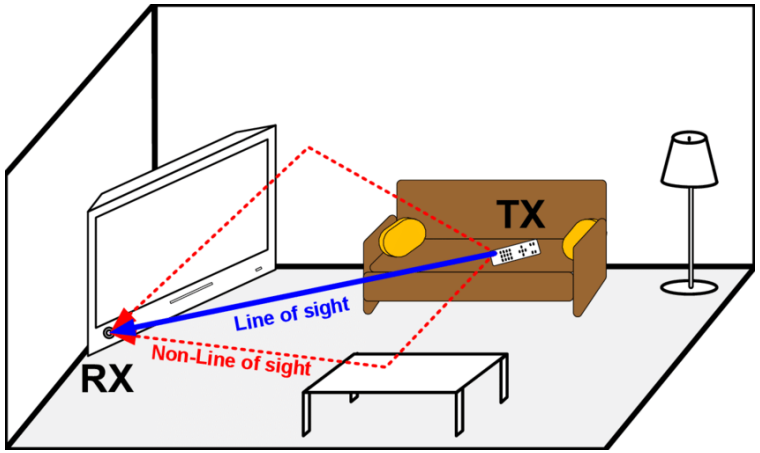
Wireless Channel: Multipath Model



- Several reflected/scattered paths
- Each path has different attenuation and delays
- Received signal is composed of multiple paths

$$y(t) = \sum_{l=0}^{L} \alpha_l \, x(t - \tau_l)$$

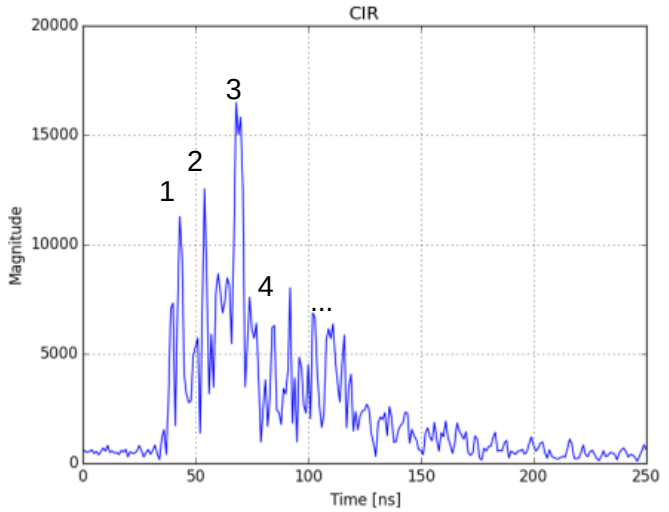
Wireless Channel: Multipath and Channel



© Measurement and characterization of ultra-wideband wireless interconnects within active computing systems

Multipath

Signal travels along different paths. Every path experiences different attenuation, reflection, diffraction



© NLOS Channel Detection with Multilayer Perceptron in Low-Rate Personal Area Networks for Indoor Localization Accuracy Improvement

Assuming there is a discrete number of paths:

For every path i, we measure attenuation and delay: $\alpha_i(t,f)$ and $\tau_i(t,f)$.

If channel is time-invariant and we only consider a narrow band, we simplify to α_i and τ_i.

Channel impulse response

First path is not always strongest (non line-of-sight, constructive interference)

Wireless Channel: Impulse Response

- We can model the wireless channel as a linear time-varying system
- The impulse response is

$$h(\tau, t) = \sum_i a_i(t)\delta(\tau - \tau_i(t))$$

  where we defined the overall attenuation and the propagation delay at time *t* for every path *i*.
- The relationship between the input *x* of the channel and the output *y* is then

$$y(t) = \int_{-\infty}^{\infty} h(\tau, t)x(t - \tau)\,\mathrm{d}\tau$$

Wireless Channel: Frequency Response

$$y(t) = \int_{-\infty}^{\infty} h(\tau, t)x(t-\tau)\,\mathrm{d}\tau$$

- *h* is the impulse response, i.e., the inverse Fourier transform of the system function *H*.
- We can therefore define the time-varying frequency response as follows

$$H(f;t) := \int_{-\infty}^{\infty} h(\tau, t)\mathrm{e}^{-\mathrm{j}2\pi f\tau}\,\mathrm{d}\tau = \sum_i a_i(t)\mathrm{e}^{-\mathrm{j}2\pi f\tau_i(t)}$$

- If the channel is time-invariant *H(f; t)* reduces to *H(f)*
- Using *H(f), we* can reason about many multipath fading channels, as the time-scale at which the channel varies is typically longer than the delay spread (i.e., the amount of memory) of the impulse response

Wireless Channel: Channel Estimation

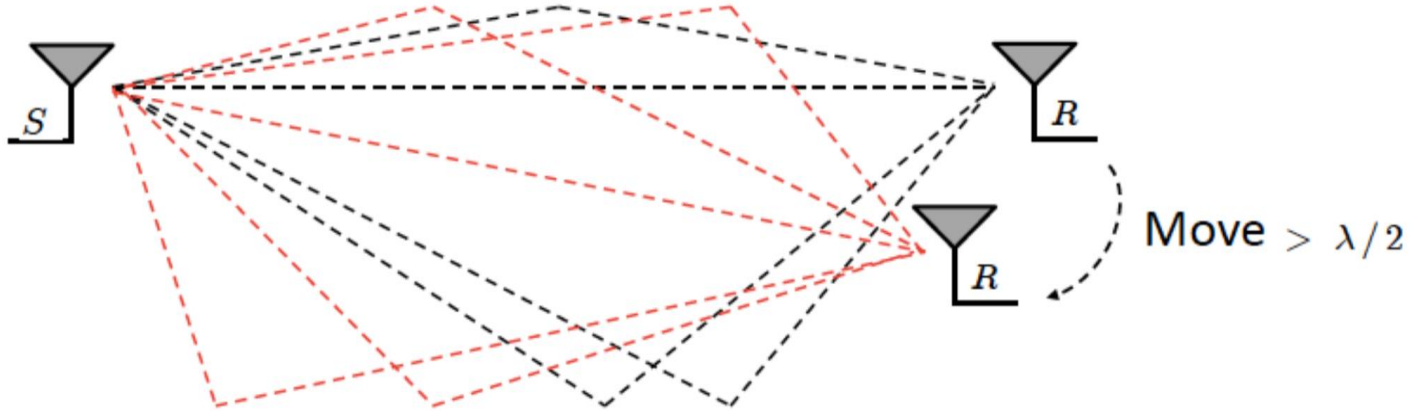
- Communicating parties can estimate *H* and/or *h* empirically to try to "understand" the (current) channel they are transmitting on

$$y(t) = (x * h)(t) \overset{\text{def}}{=} \int_{-\infty}^{\infty} x(t-\tau) \cdot h(\tau)\, \mathrm{d}\tau$$

- Channel estimation is the basis of many physical-layer security schemes in wireless communication
- The channel varies due to change in position, time and environment
- Uncertainty and variability of the channel can be extracted

Uncertainty of the 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
  - Channel between sender (S) and receiver (R) will be ‘random’ and will not be known to the attacker
  - Natural wiretap channel



Channel-based Key Establishment

- Physical-layer randomness of a wireless channel can be used to derive a shared secret
- Main assumption: Attacker located at least half a wavelength away from communicating parties
  - Attacker's channel measurements are de-correlated from those computed by the other parties
  - Therefore likely no have access to the measured secret randomness

  - If the attacker injects signals/interference during the key generation, the attacker signal is measured differently at the benign devices due to channel distortions and the result is key disagreement

Process:

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

Key Establishment Process

1. Signal Acquisition and Quantization

Record a time series of channel properties, measured over received packets, e.g., RSSI, channel impulse response. Time series is then quantised by both parties independently. This quantisation is typically based on fixed or dynamic thresholds

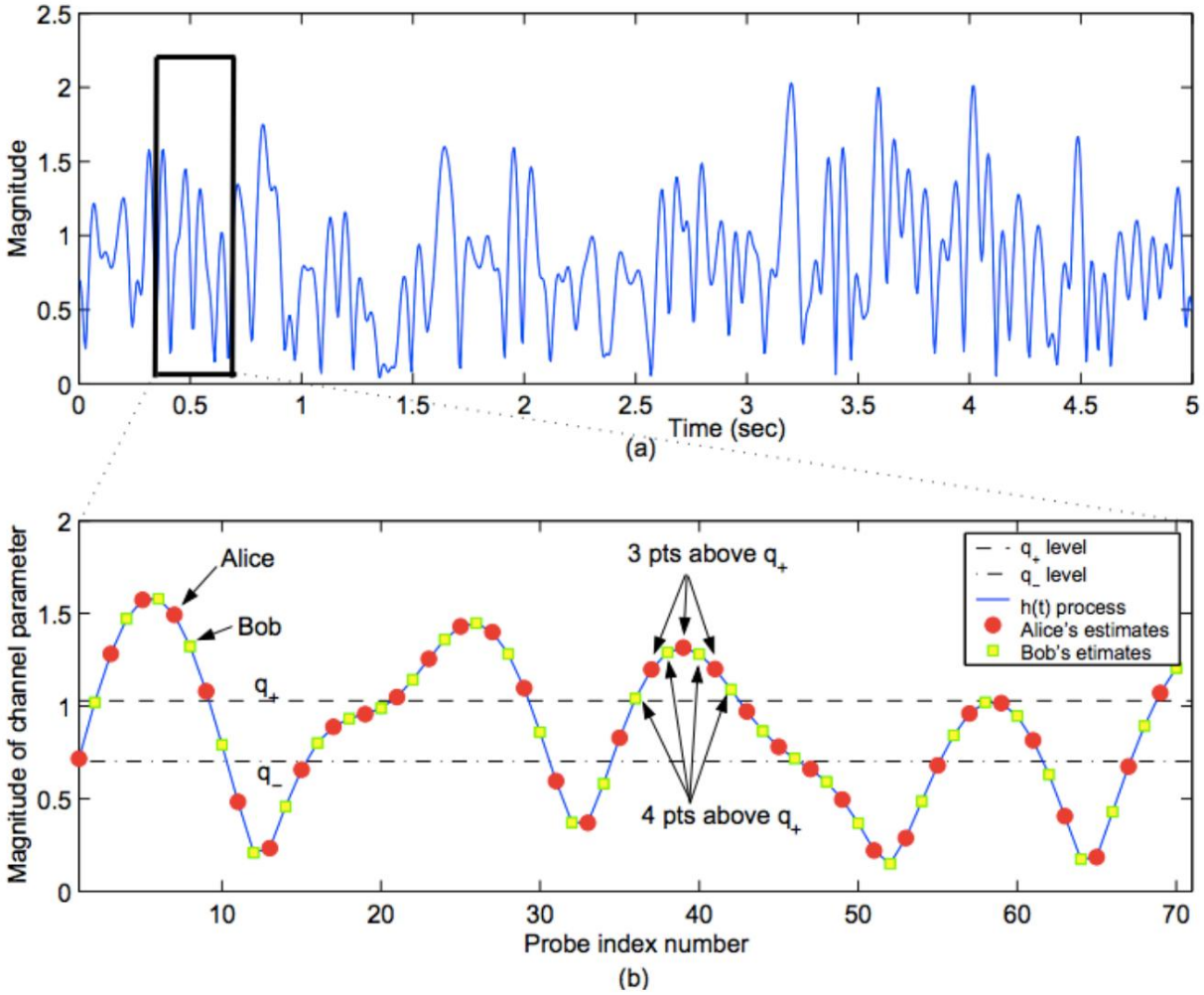
2. Reconciliation (error correction, privacy amplification)

Quantization likely to result in disagreeing sequences. Leverage error correcting codes and privacy amplification techniques

3. Key confirmation / verification

In this last phase, communicating parties confirm that they established the same secret key, e.g., by exchanging a hash value

Example: RSSI-based Key Agreement



©Suhas Mathur, et al. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. MobiCom '08.

Measure the received signal strength to derive a mutual key

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]

Broad range of HW assumptions!

Security 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

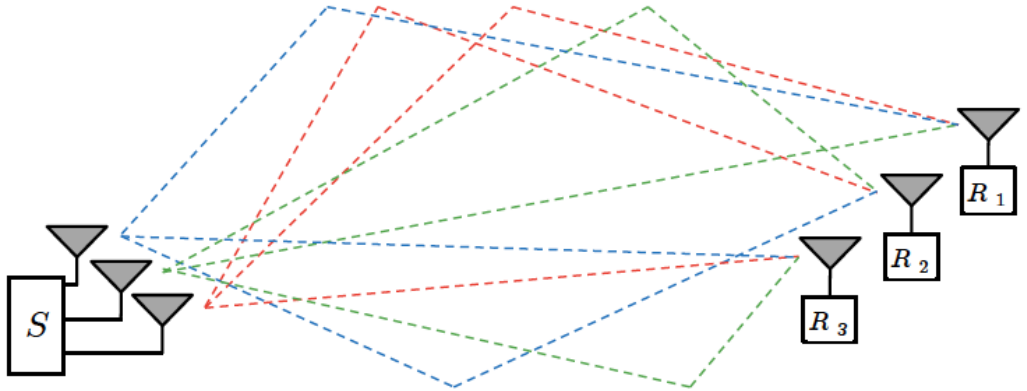
References

- An Adaptive Quantization Algorithm for Secret Key Generation Using Radio Channel Measurements. Sana Tmar - Ben Hamida et. al., New Technologies, Mobility and Security (NTMS), 2009.

- A Practical Man-In-The-Middle Attack on Signal-Based Key Generation Protocols. Simon Eberz et. al., ESORICS, 2012.

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.*

Simplified Modeling of the Channel I

Recall

$$H(f;t) := \int_{-\infty}^{\infty} h(\tau,t)\mathrm{e}^{-\mathrm{j}2\pi f\tau}\,\mathrm{d}\tau = \sum_i a_i(t)\mathrm{e}^{-\mathrm{j}2\pi f\tau_i(t)}$$

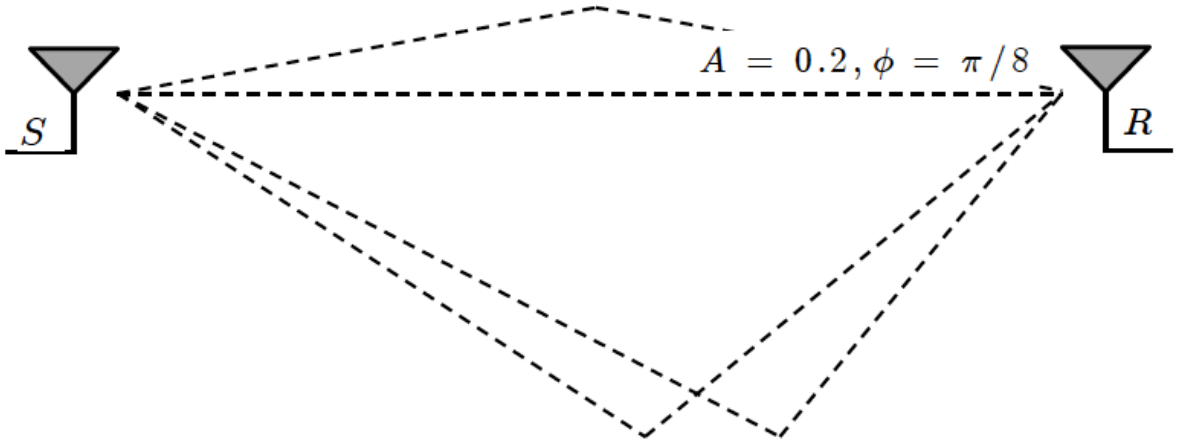
If there is no time-dependence, impulse/frequency response turns into

$$h(\tau) = \sum_i a_i\delta(\tau-\tau_i) \qquad \text{and} \qquad H(f) = \sum_i a_i\, e^{-j2\pi f\tau_i}$$

Moreover, if we set the frequency to a fixed value, we can express *H* as a simple complex number.

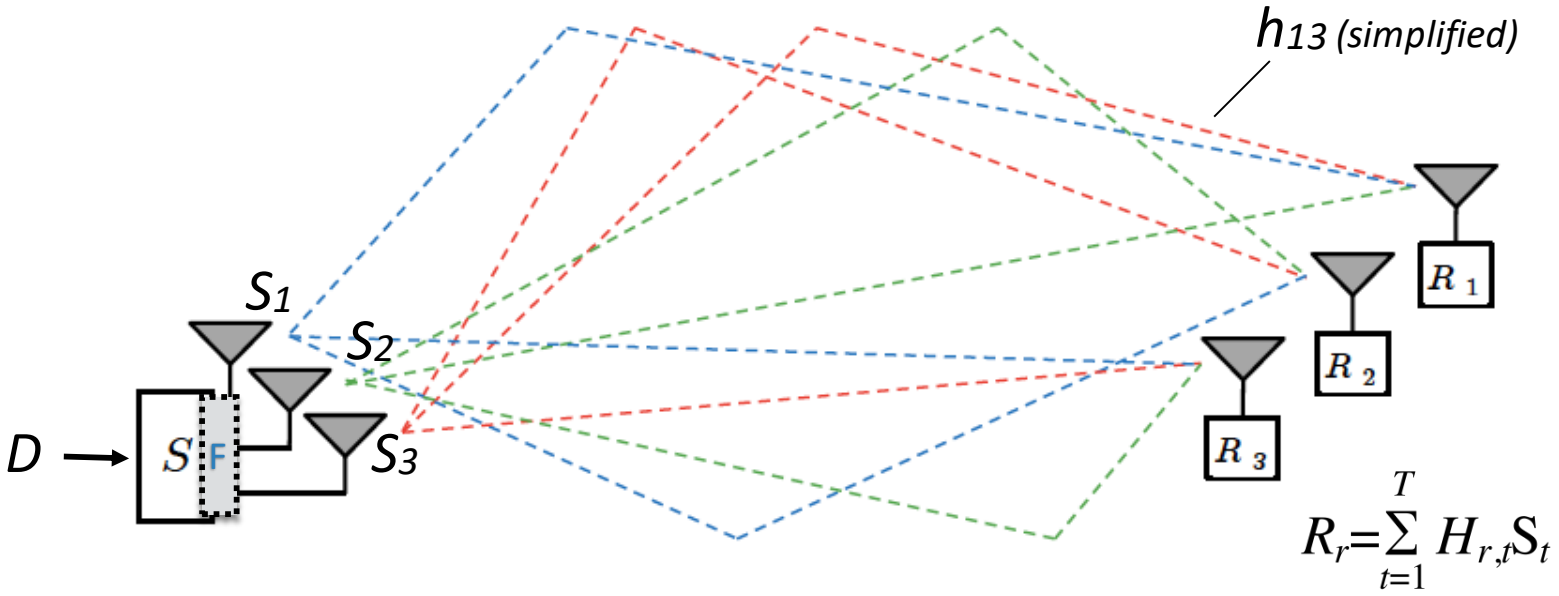
This simplified model forms the basis for MIMO techniques discussed in this lecture

Simplified Modeling of the Channel II



- 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 (confidential data)
- ***F*** is a transmission filter, constructed given ***H**, such that*
  - R_1 = confidential data
  - R_2,R_3 = no (useful) data

Zero Forcing: Filter (Weights)

- Zero forcing beam forming is implemented with pre-coding
  - Data is pre-coded with weights, i.e., filtered with a transmission filter
- If we have *N* transmit antennas and *M* single-antenna receivers, we get the channel matrix $H = [h_1; h_2; \ldots; h_M]$
- h_i is a row vector with *N* elements where elements correspond to the complex exponential gain between one of the transmitter's antenna and receiver
- We can define the steering weight matrix *W* as

$$W = [w_1\ w_2\ \ldots\ w_m]$$

- w_i is a column vector corresponding to the complex steering weights for user *i*

Zero Forcing: Optimal Weights

- Optimal selection of weights is the pseudo-inverse of H:

$$W = H^{\dagger} = H^{*}(HH^{*})^{-1}$$

- We achieve zero-interference condition: $h_i w_j = 0 \text{ for } i \neq j$

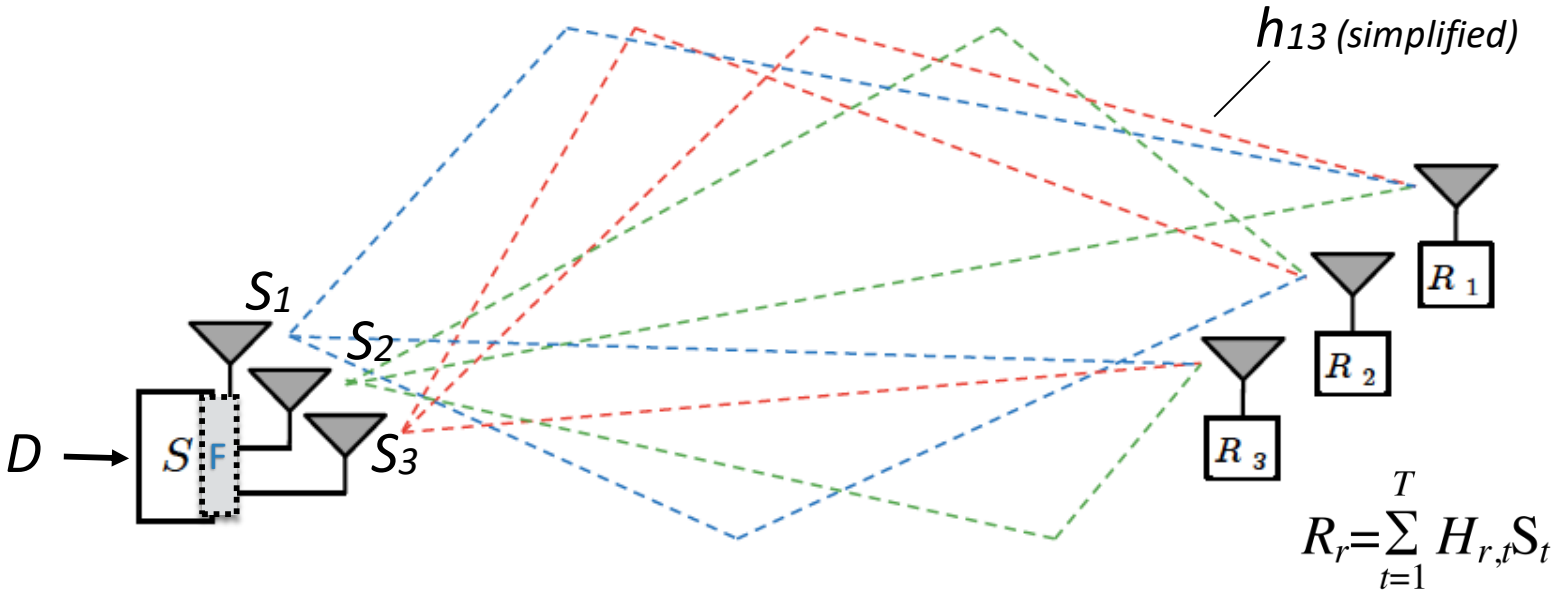
- It can be show that pseudo-inverse is optimal, but:

We might not know the channels to the eavesdroppers/attackers

- "Cooperating eavesdroppers" are a theoretical construct
- Even if we know their position, computing the channel is hard (compare with key generation)

Possible solution: Actively "blind" eavesdroppers by emitting (orthogonal) interference

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**, such that*
  - R_1 = confidential data
  - R_2,R_3 *(attackers)* = ***data + jamming signal (noise)***

Orthogonal Blinding: Possible Approach

Assume we don't know channels between transmitter and eavesdroppers

- Conceal the intended receiver's signal by overwhelming eavesdroppers with noise
- Transmit "blinding" streams concurrently with the intended receiver's stream
- Select h_1 that belongs to targeted receiver, then construct new channel matrix $\widehat{H}$ using Gram-Schmidt algorithm to construct M orthogonal *h* vectors

$$\widehat{h_k} = h_k - \sum_{j=1}^{k-1} \frac{\langle h_k, \widehat{h_j} \rangle}{\|\widehat{h_j}\|^2} \widehat{h_j}, \quad 1 \leq k \leq M$$

- We arrive at the new steering weight matrix $W = \widehat{H}^{\dagger} = \widehat{H}^{*}$ (constructed matrix is unitary)

Use the new weight matrix to transmit confidential stream and "blinding" streams in parallel

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*
  - *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

* Practical Known-Plaintext Attacks against Physical Layer Security in Wireless MIMO Systems. Mathias Schulz. NDSS 2014

References / Recommended Readings

- On the Optimality of Multiantenna Broadcast Scheduling Using Zero-Forcing Beamforming.
- STROBE: Actively Securing Wireless Communications using Zero-Forcing Beamforming. Narendra Anand et al., 2012 Proceedings IEEE INFOCOM.
- Fundamentals of Wireless Communication, David Tse, Cambrige University Press, Chapter 7: "MIMO 1 : Spatial Multiplexing and Channel Modeling"

Can we use Friendly Jamming for Confidentiality and Access Control?

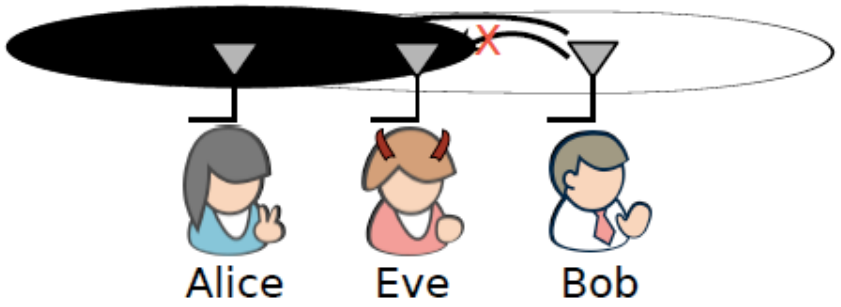
Jamming for Confidentiality

- 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 / confidential communication

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



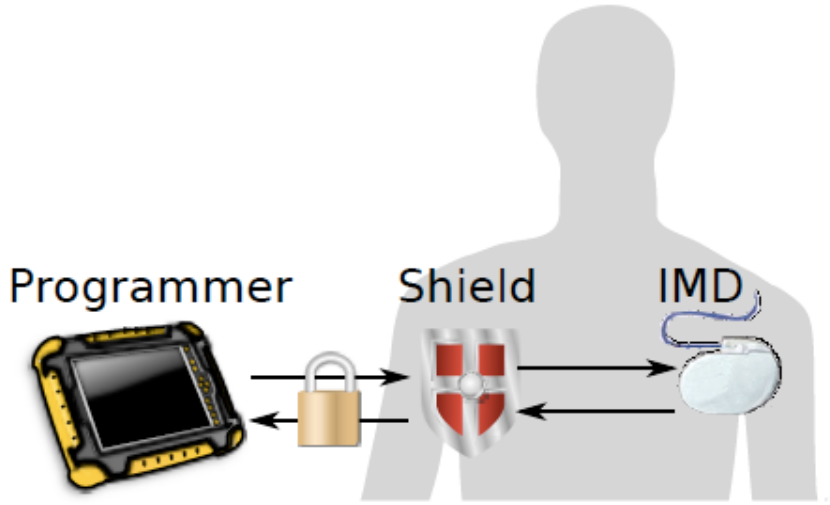
Friendly Jamming

- 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”

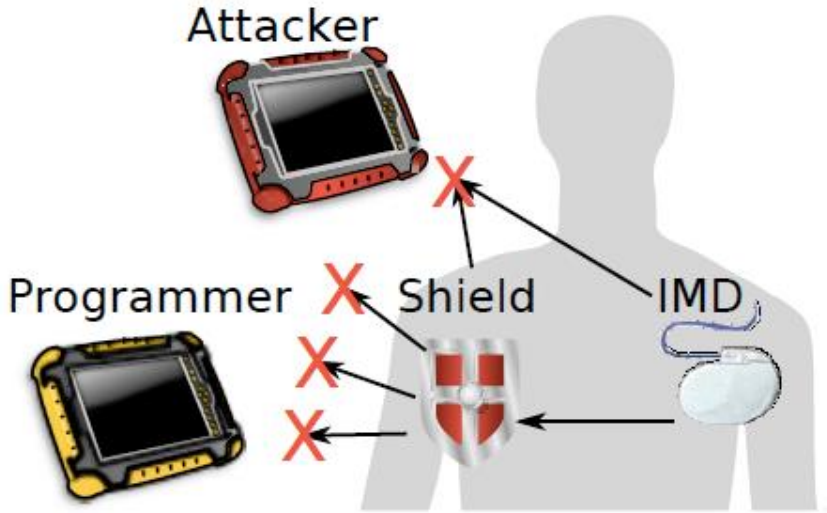
- *S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, K. Fu, “They can hear your heartbeats: Non-invasive security for implanted medical devices,” in Proceedings of the ACM SIGCOMM, 2011.*



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

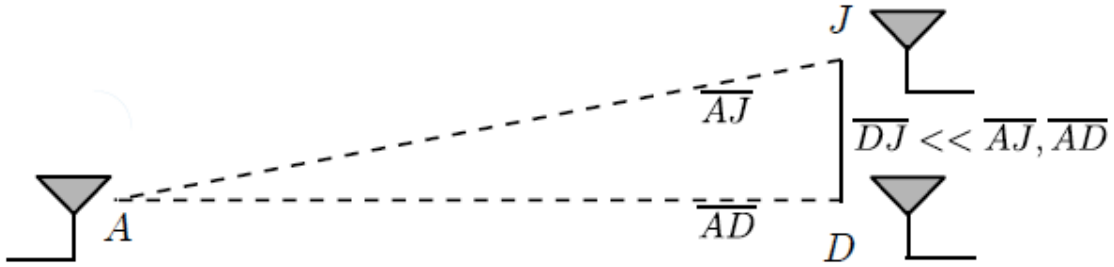
Example: “IMD Shield”

- *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 jams the eavesdropper.
  - Legitimate reader jammed but can remove jamming signal (shared key with the Shield).

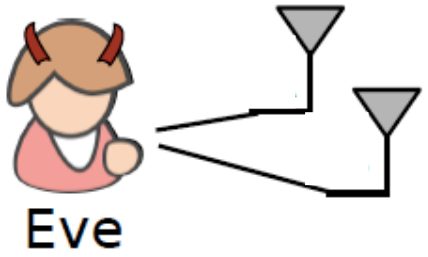
Friendly Jamming Security Arguments



- 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.*

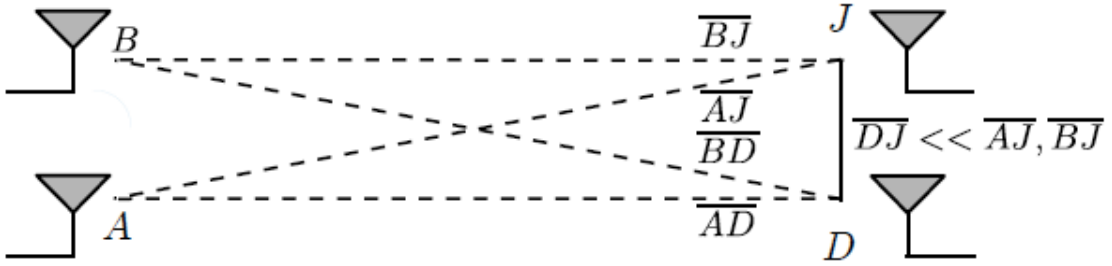
- However,
  - Confidentiality holds only for a single-antenna attacker.
  - *A MIMO-like attacker CAN separate the signals and recover the confidential message, from a number of locations.*

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



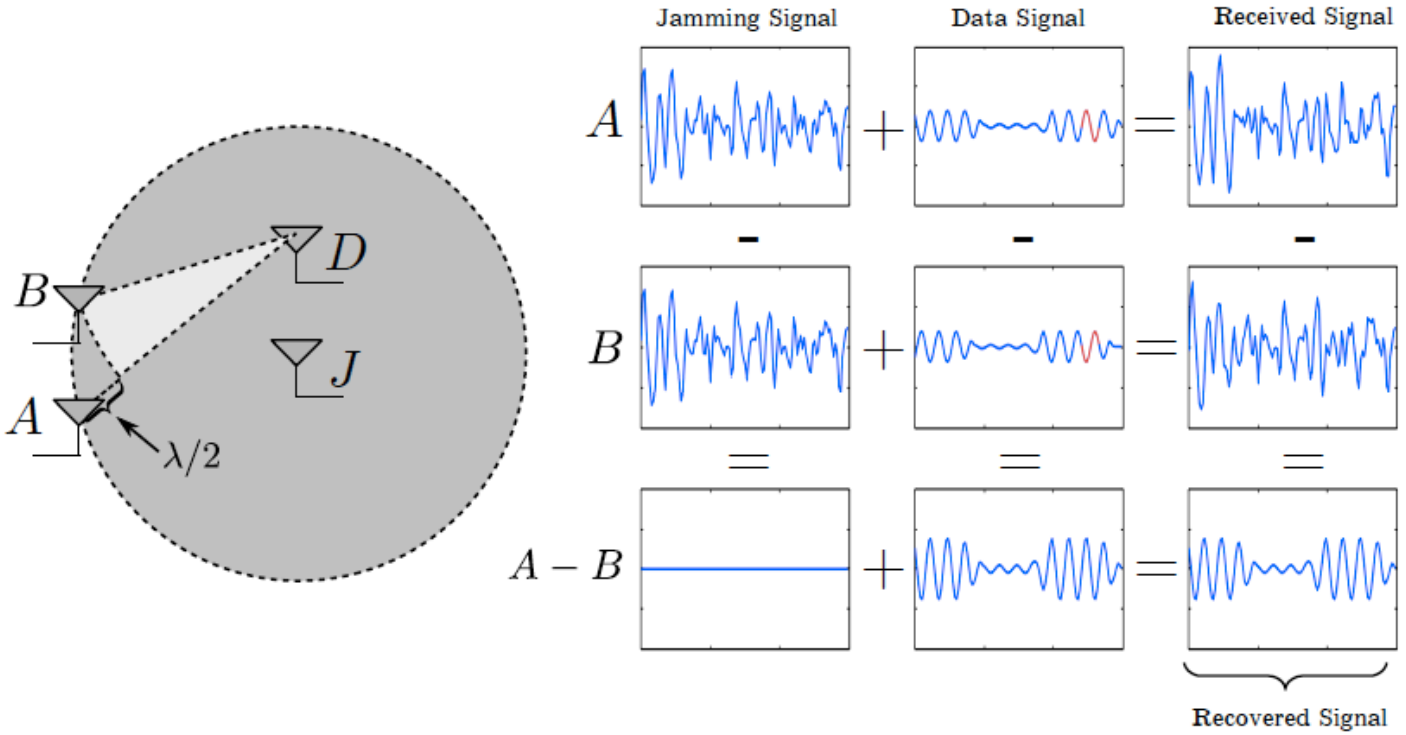
- A and B receive data and jamming signals with different relative offsets.
- Time of arrival of signals are given by the geometry.
  In LOS settings:

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

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

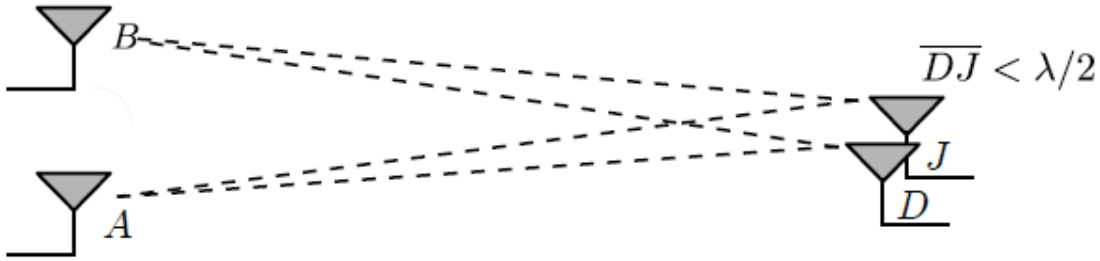
Ideal Placement of the Attacker's Antennas

- *N.Tippenhauer, et. al., 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, data signals are shifted by λ/2.

Impact of Imperfect Attacker Placement

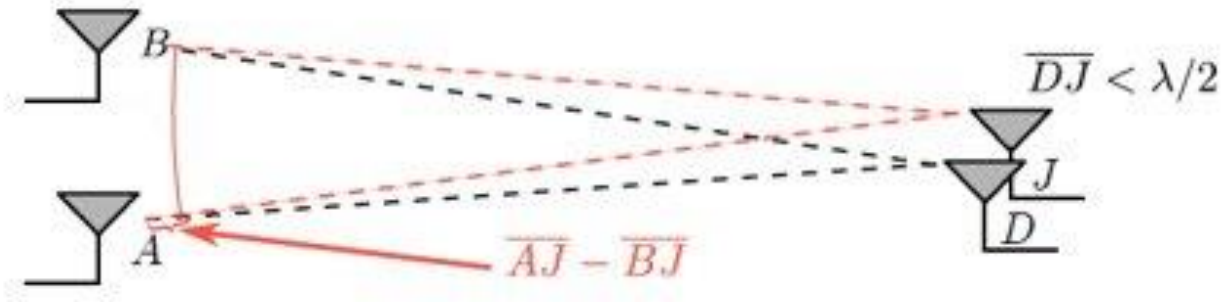


- Ideal cancellation of jamming signal relies on

$$\delta = |(\overline{AJ} - \overline{BJ}) - (\overline{AD} - \overline{BD})| = \lambda/2$$

- 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

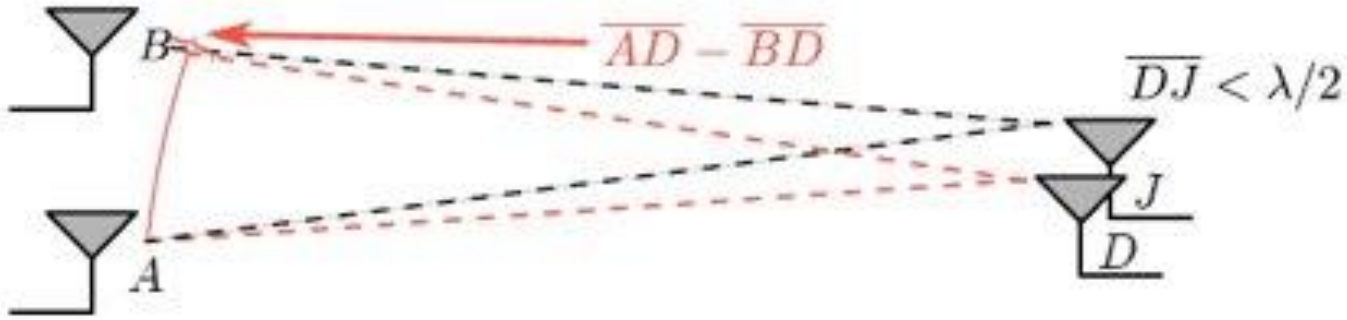


- Ideal cancellation of jamming signal relies on

$$\delta = |(\overline{AJ} - \overline{BJ}) - (\overline{AD} - \overline{BD})| = \lambda/2$$

- 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

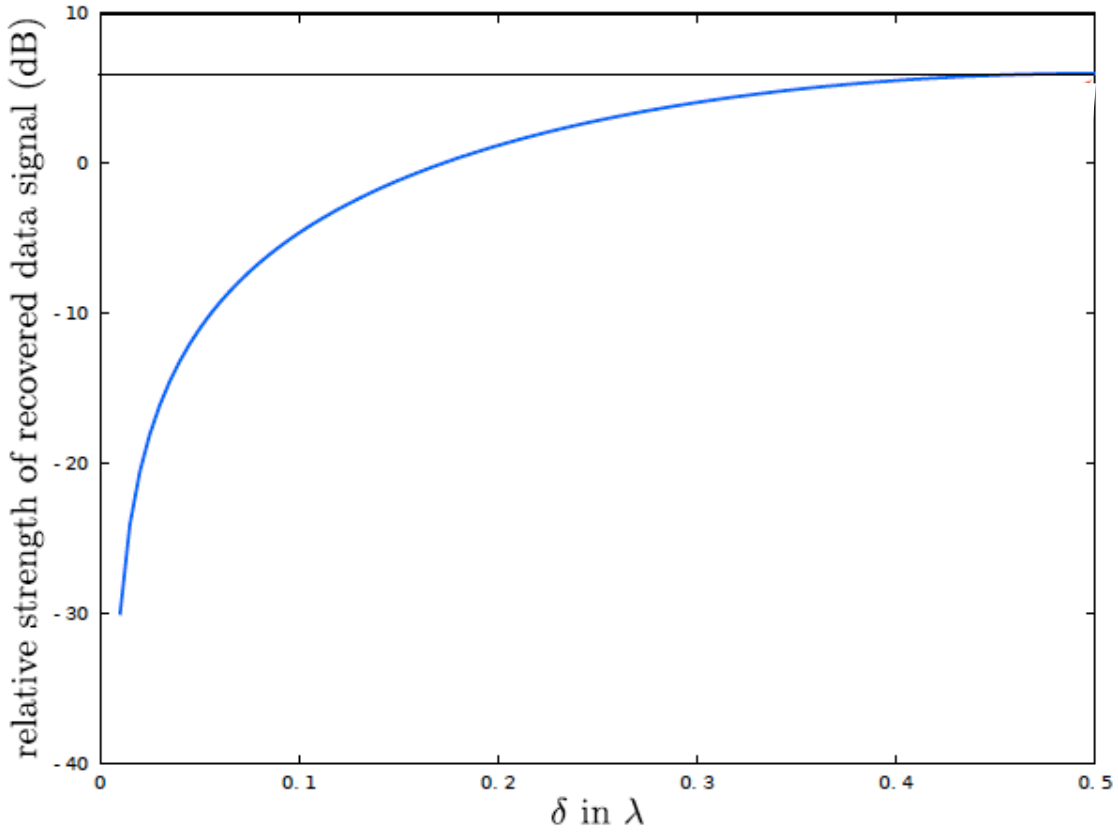


- Ideal cancellation of jamming signal relies on

$$\delta = |(\overline{AJ} - \overline{BJ}) - (\overline{AD} - \overline{BD})| = \lambda/2$$

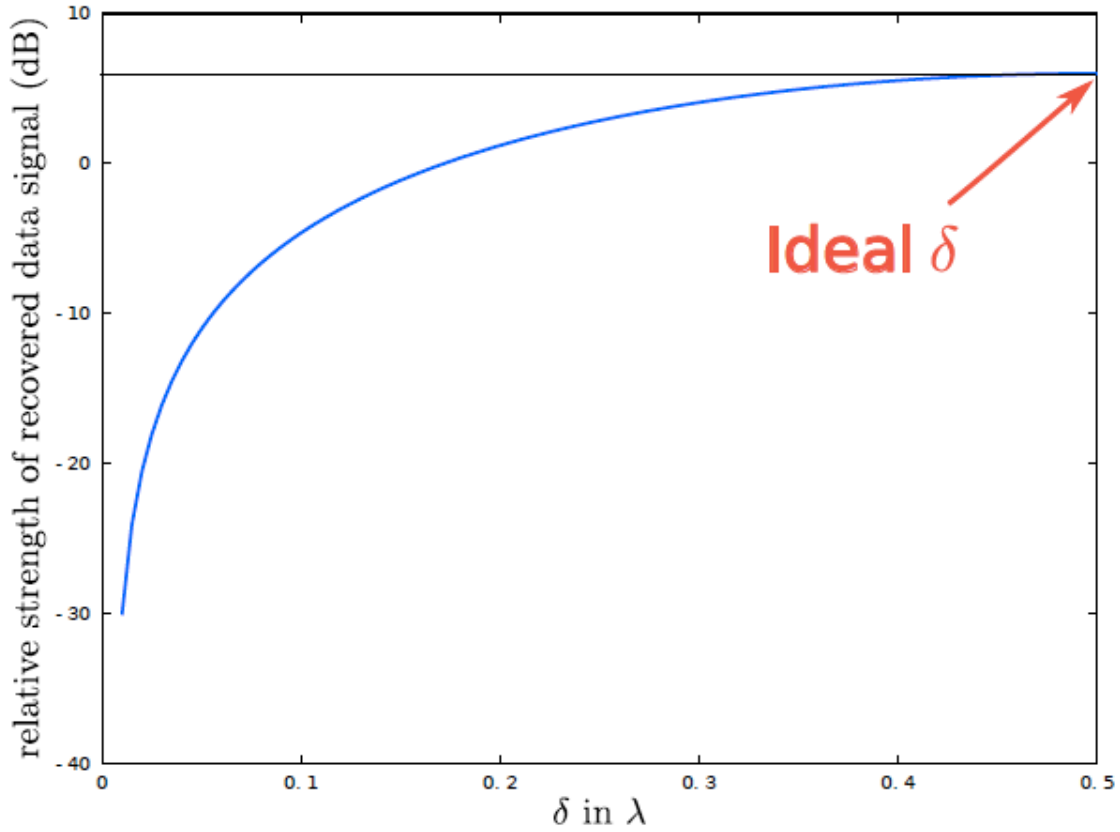
- For 2.4 GHz WLAN, λ/2 = 6.25cm, for 400MHz, λ/2 = 37.5cm
- Is data content recovery still possible with imperfect δ ?

Impact of Imperfect Attacker Placement



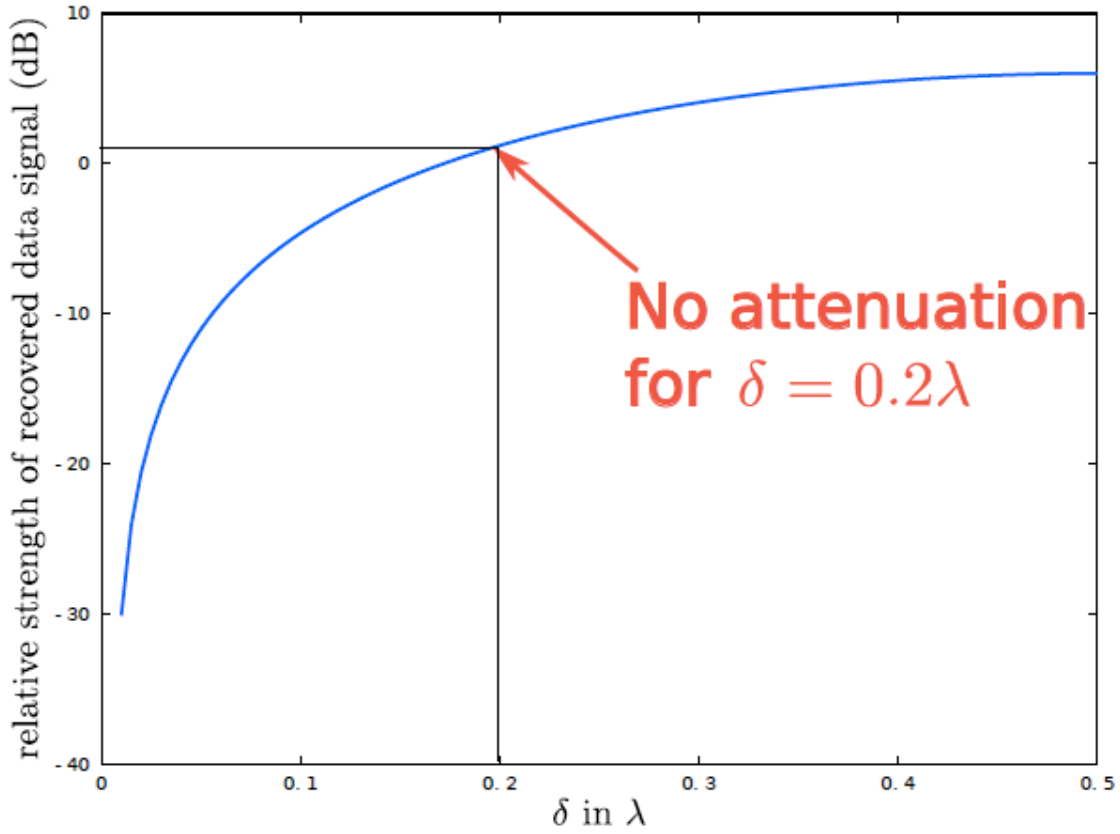
For $\delta = |\overline{AJ} - \overline{AD} - \overline{BJ} + \overline{BD}| > \lambda/5$, the attacker can recover the data signal with amplification (attenuation $< 0dB$).

Impact of Imperfect Attacker Placement



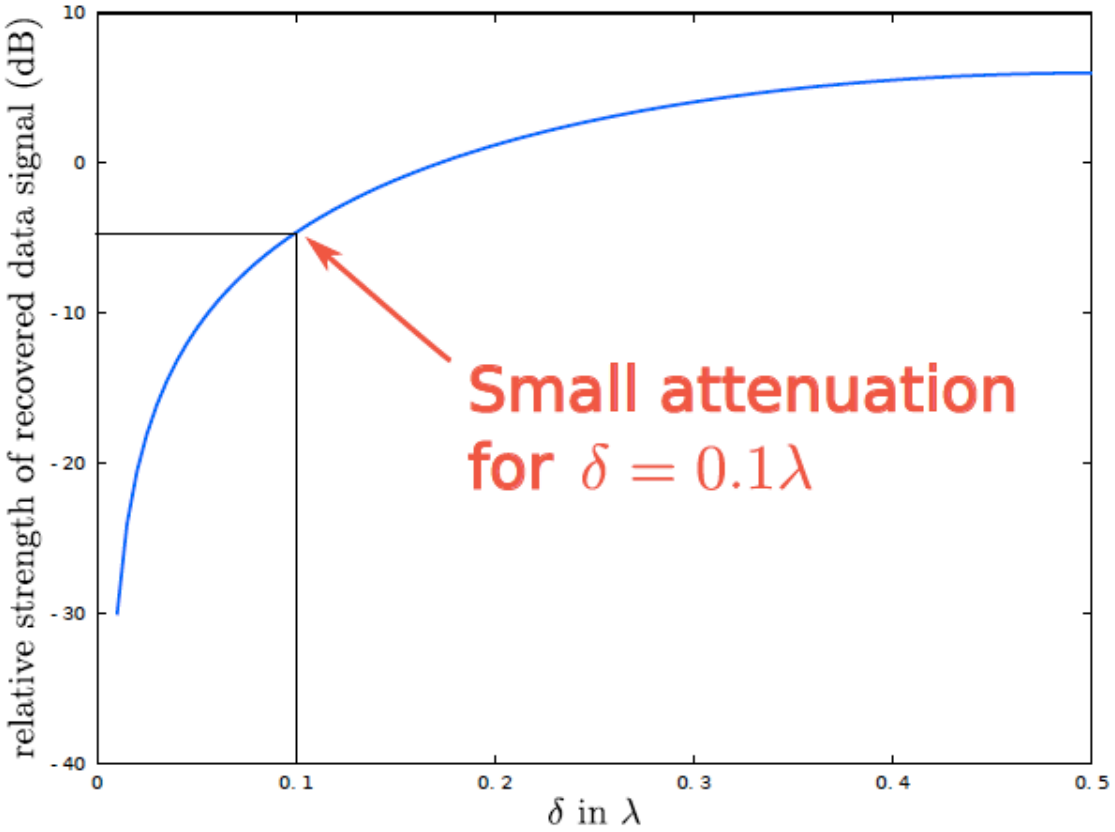
For $\delta = |\overline{AJ} - \overline{AD} - \overline{BJ} + \overline{BD}| > \lambda/5$, the attacker can recover the data signal with amplification (attenuation $< 0dB$).

Impact of Imperfect Attacker Placement



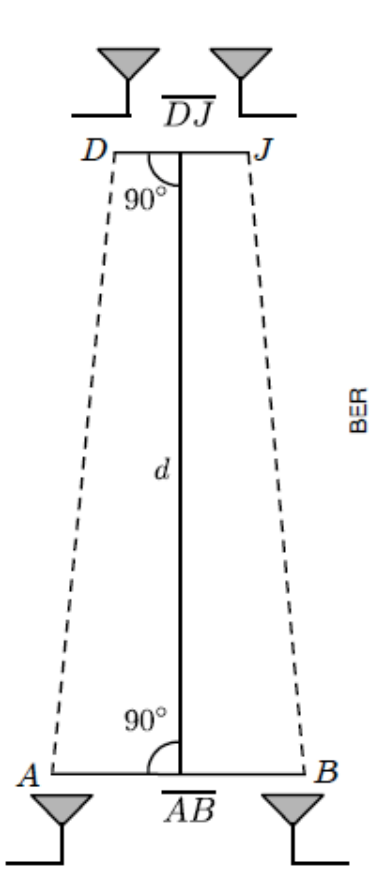
For $\delta = |\overline{AJ} - \overline{AD} - \overline{BJ} + \overline{BD}| > \lambda/5$, the attacker can recover the data signal with amplification (attenuation $< 0dB$).

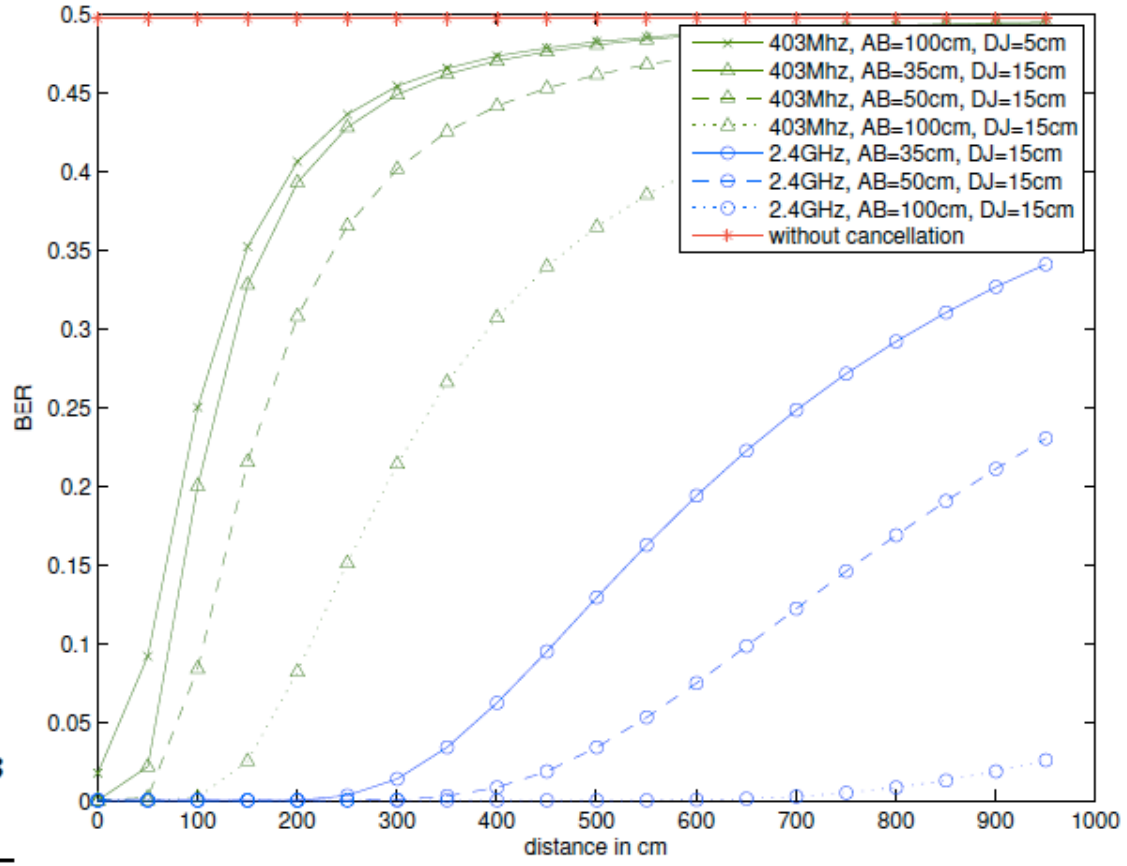
Impact of Imperfect Attacker Placement



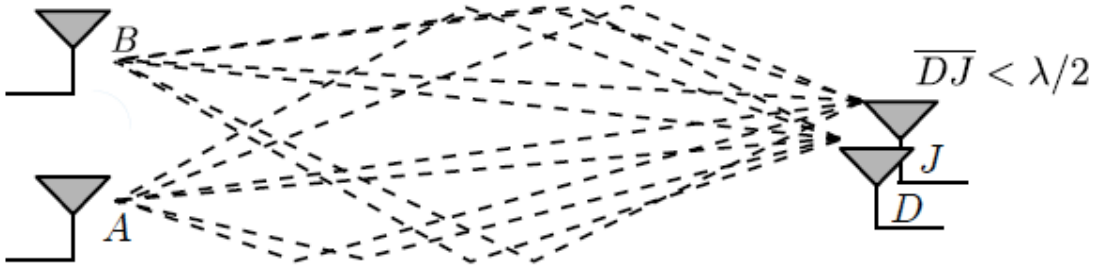
For $\delta = |\overline{AJ} - \overline{AD} - \overline{BJ} + \overline{BD}| > \lambda/5$, the attacker can recover the data signal with amplification (attenuation $< 0dB$).

Simulation Results



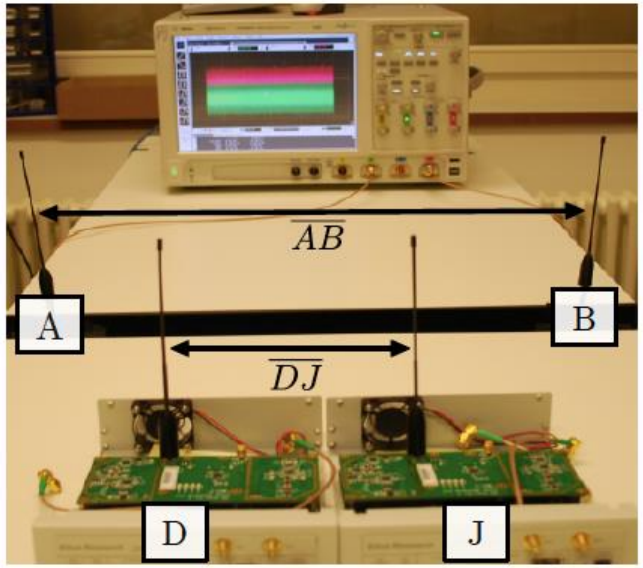


Multipath in (Friendly) Jamming



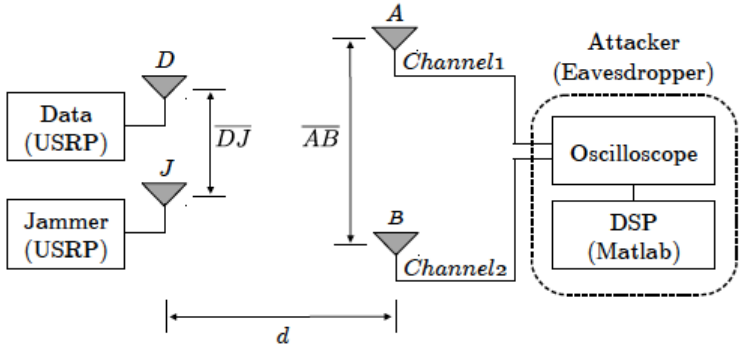
- So far, we looked at LOS channels, no reflections.
  - Multipath will Introduce more variation of amplitudes of components.
  - Change the phase offsets of the signals.
  - Potentially prevent us from canceling the jamming signals.

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.



Example Result

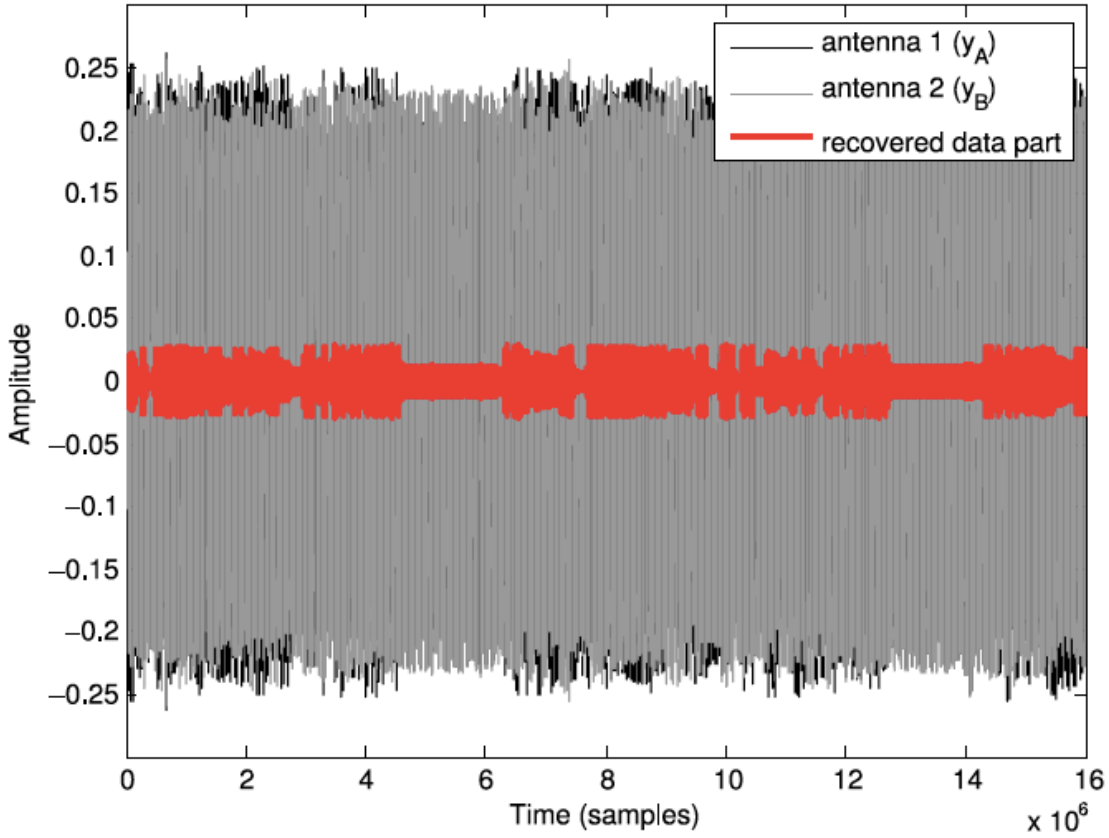
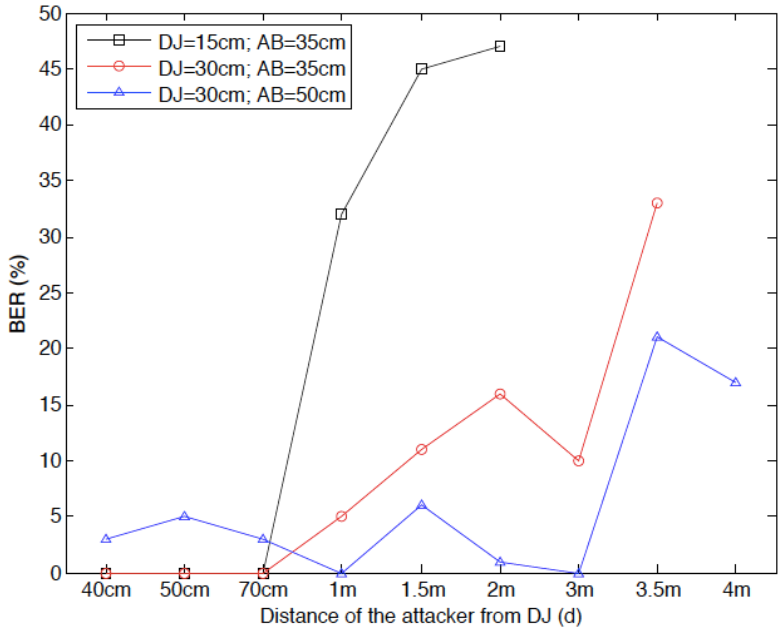
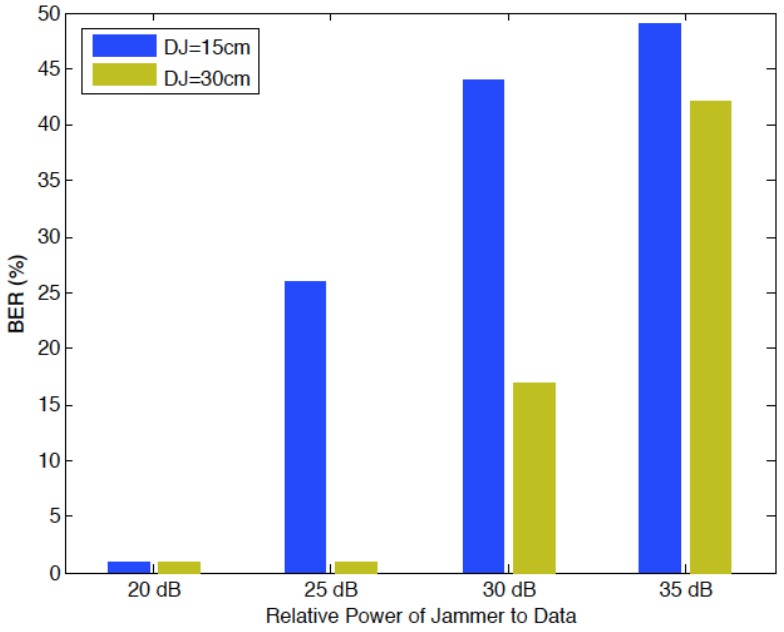
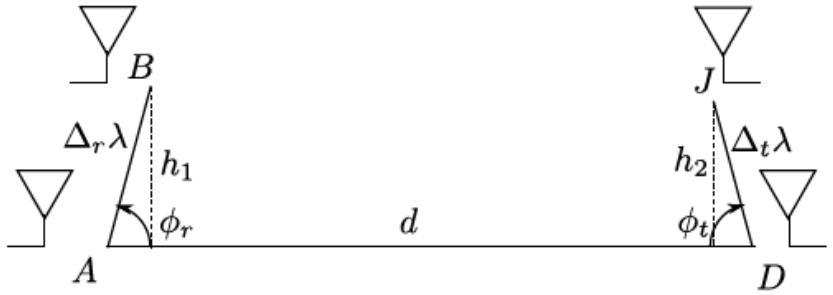


Figure 11. Black and gray waveforms correspond to signals acquired from two receiver antennas. Once the signals were aligned and subtracted, in red we can see the clearly visible, remaining data signal component.

Example Experimental Result







Lessons learned

- Using Jamming for confidentiality is not without risk
  - MIMO-like attacker can retrieve data despite DJ < λ/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.