Network Security (NetSec)

TECHNISCHE UNIVERSITÄT DARMSTADT

Summer 2015
Physical Layer Security

CASED

Learning Objectives

- Get a basic idea about the physical layer
- Get to know some approaches how the physical layer can be used to enhance security of a system
- Understand attacks against physical layer security

SECURE MOBILE NETWORKING

Motivation

Security in the ISO-OSI Model

Application Layer	SSH, HTTPS, FTPS, PGP	End-to-End
Transport Layer	SSL, TLS	
Network Layer	IPSec	Machine-to-Machine
Data Link Layer	WEP, WPA(2), 802.1X	Device-to-Device
Physical Layer	?	

Security in a wired setup

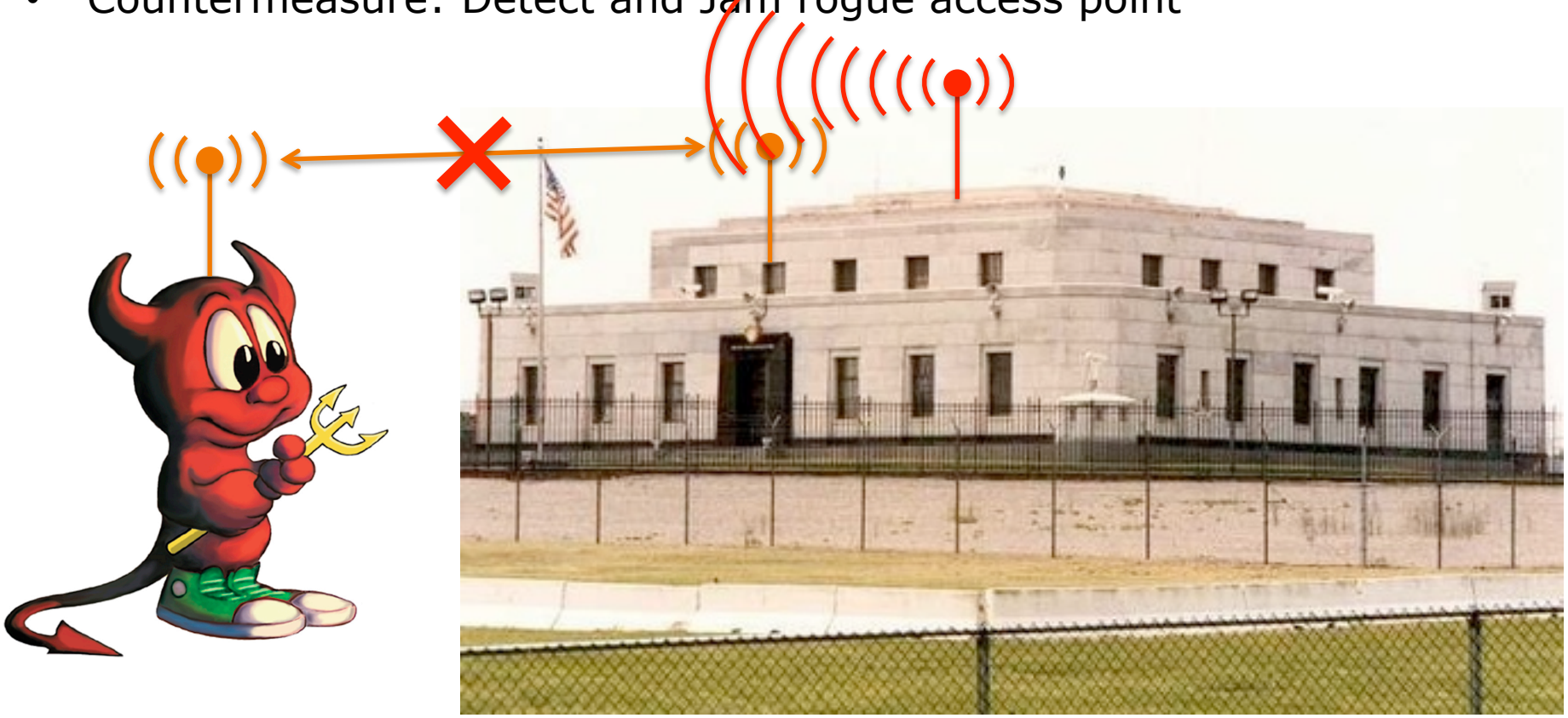
- Attacker needs physical access to network equipment

Security in a wired setup

- Attacker needs physical access to network equipment
- Rogue Access Points attached to the network are a security thread

Security in a wired setup

- Attacker needs physical access to network equipment
- Rogue access points attached to the network are a security thread
- Countermeasure: Detect and Jam rogue access point

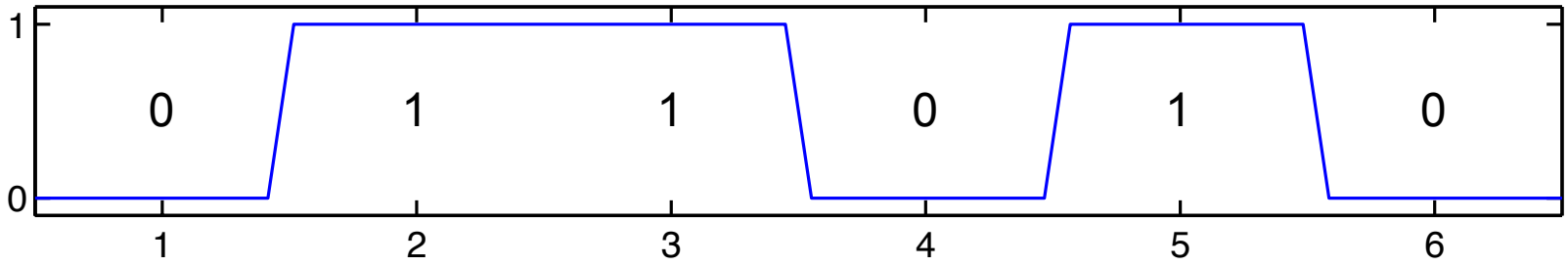


SECURE MOBILE NETWORKING

Physical Layer 101

How signals get transmitted

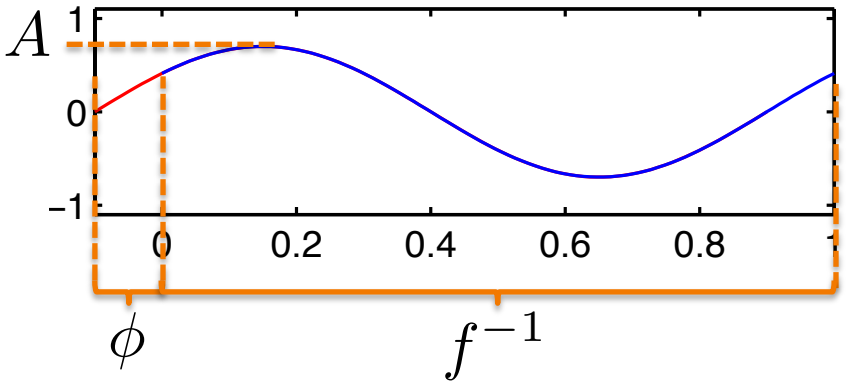
- In a computer, data is represented as bits (0 or 1)



- In the physical layer data is mapped to analog signals, represented as a sum of sine waves

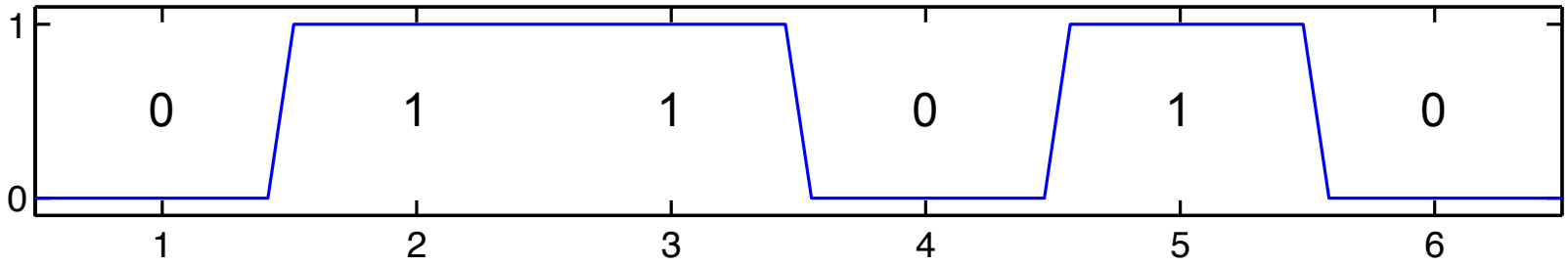
$$A \cdot \sin(2\pi f t + \phi)$$

Amplitude Frequency Phase



How signals get transmitted

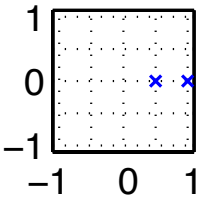
- In a computer, data is represented as bits (0 or 1)

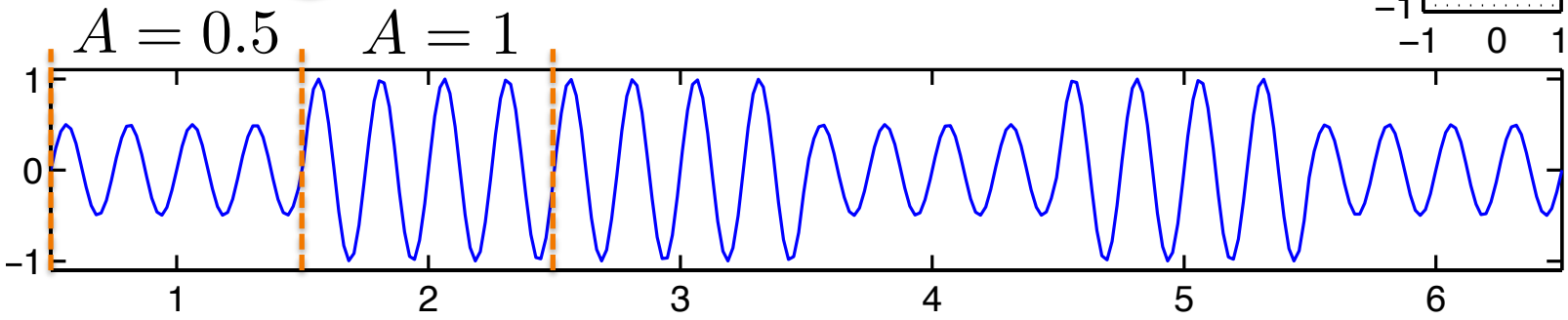


- Amplitude Shift Keying (ASK) modifies the signal's amplitude

$$A \cdot \sin(2\pi f t + \phi)$$

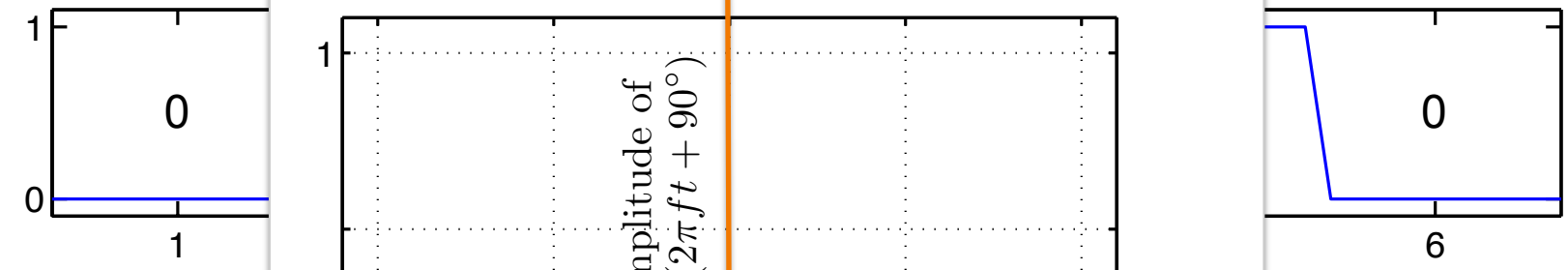
Constellation Diagram:



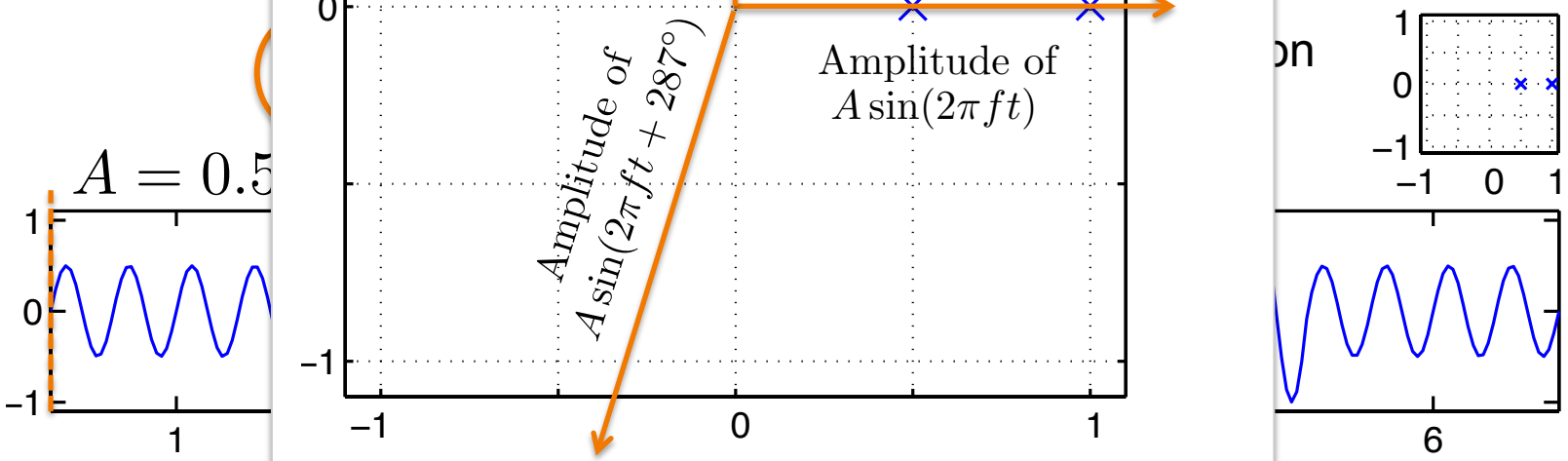


How signals get transmitted

- In a com … 1)

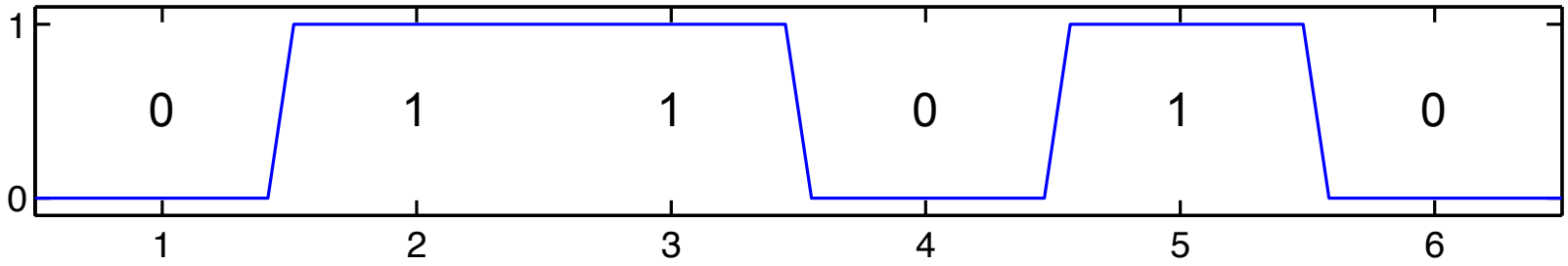


- Amplitud … al's amplitude



How signals get transmitted

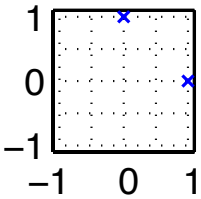
- In a computer, data is represented as bits (0 or 1)

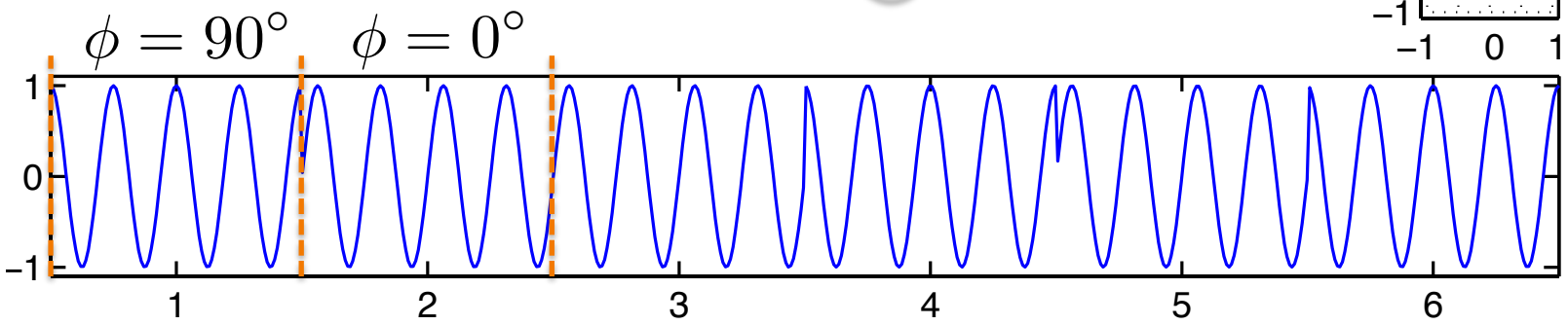


- Phase Shift Keying (PSK) modifies the signal's phase

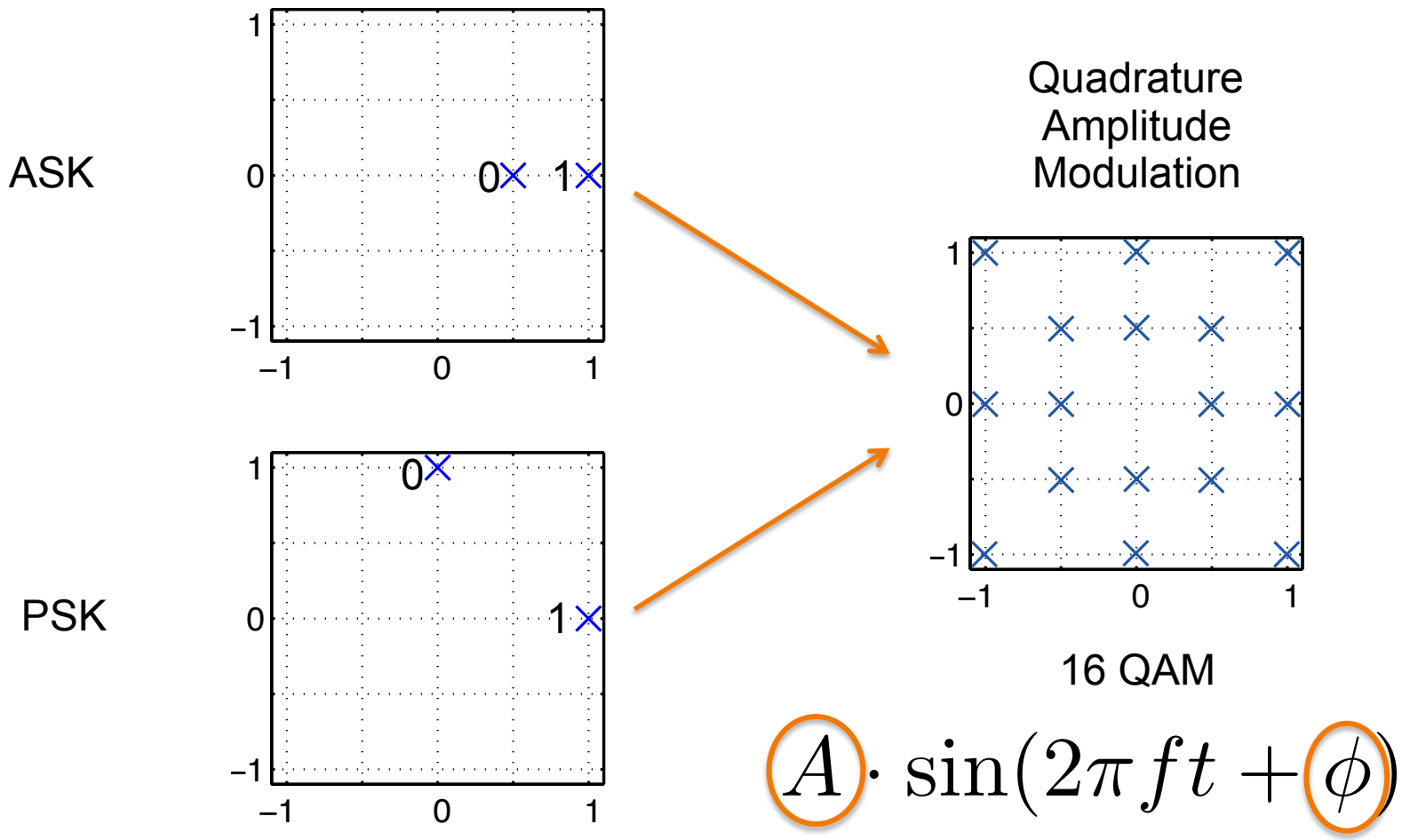
$$A \cdot \sin(2\pi f t + \phi)$$

Constellation Diagram:



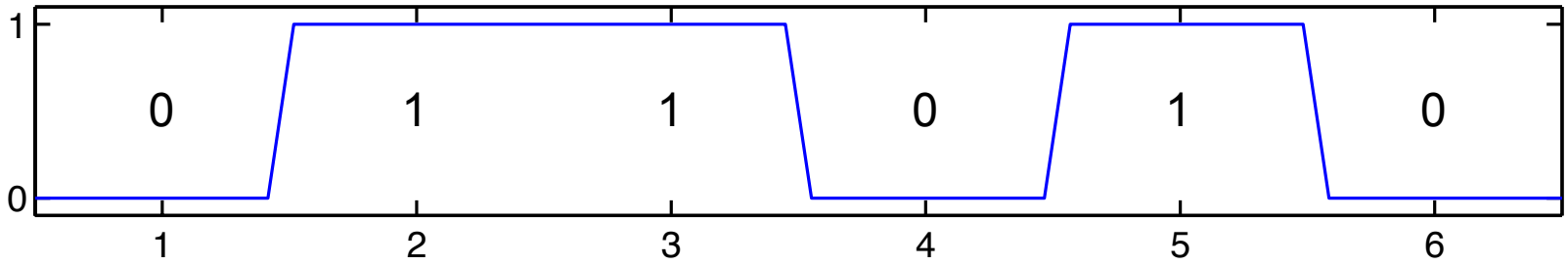


How signals get transmitted



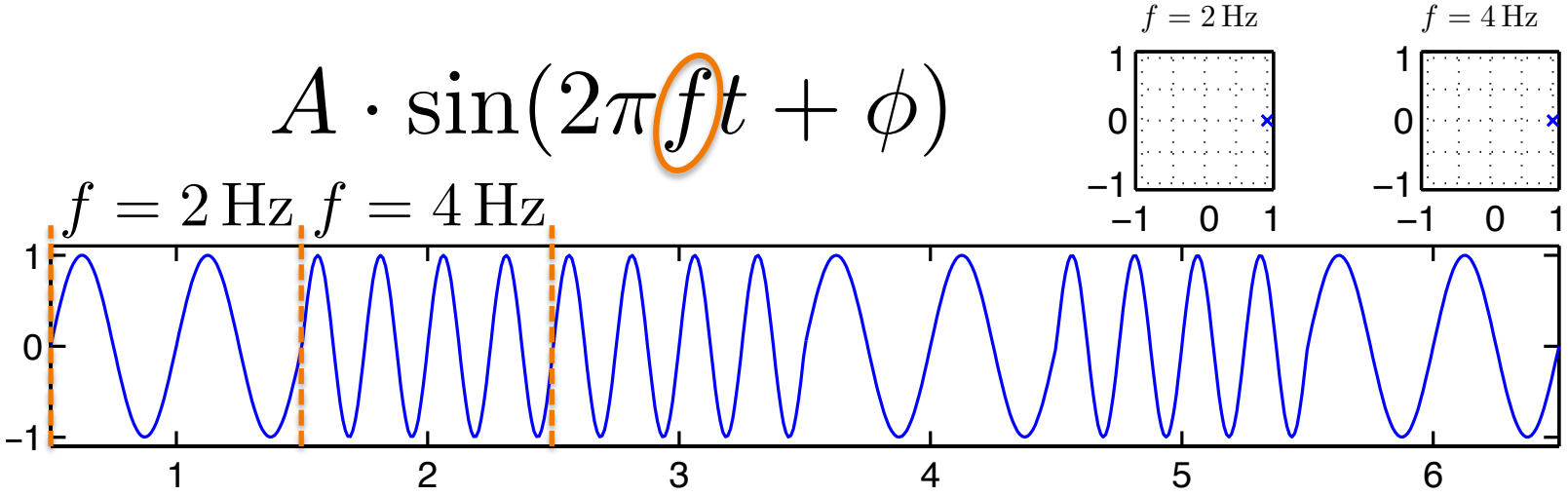
How signals get transmitted

- In a computer, data is represented as bits (0 or 1)



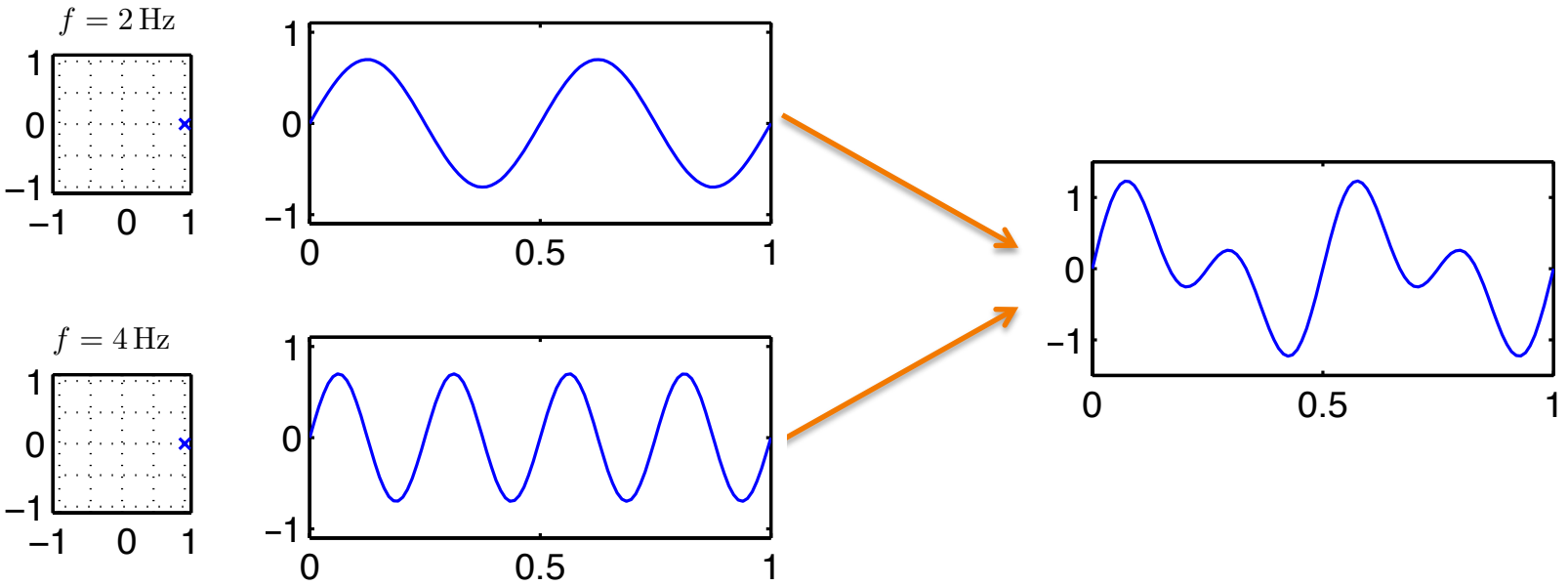
- Frequency Shift Keying (FSK) modifies the signal's frequency

$$A \cdot \sin(2\pi f t + \phi)$$

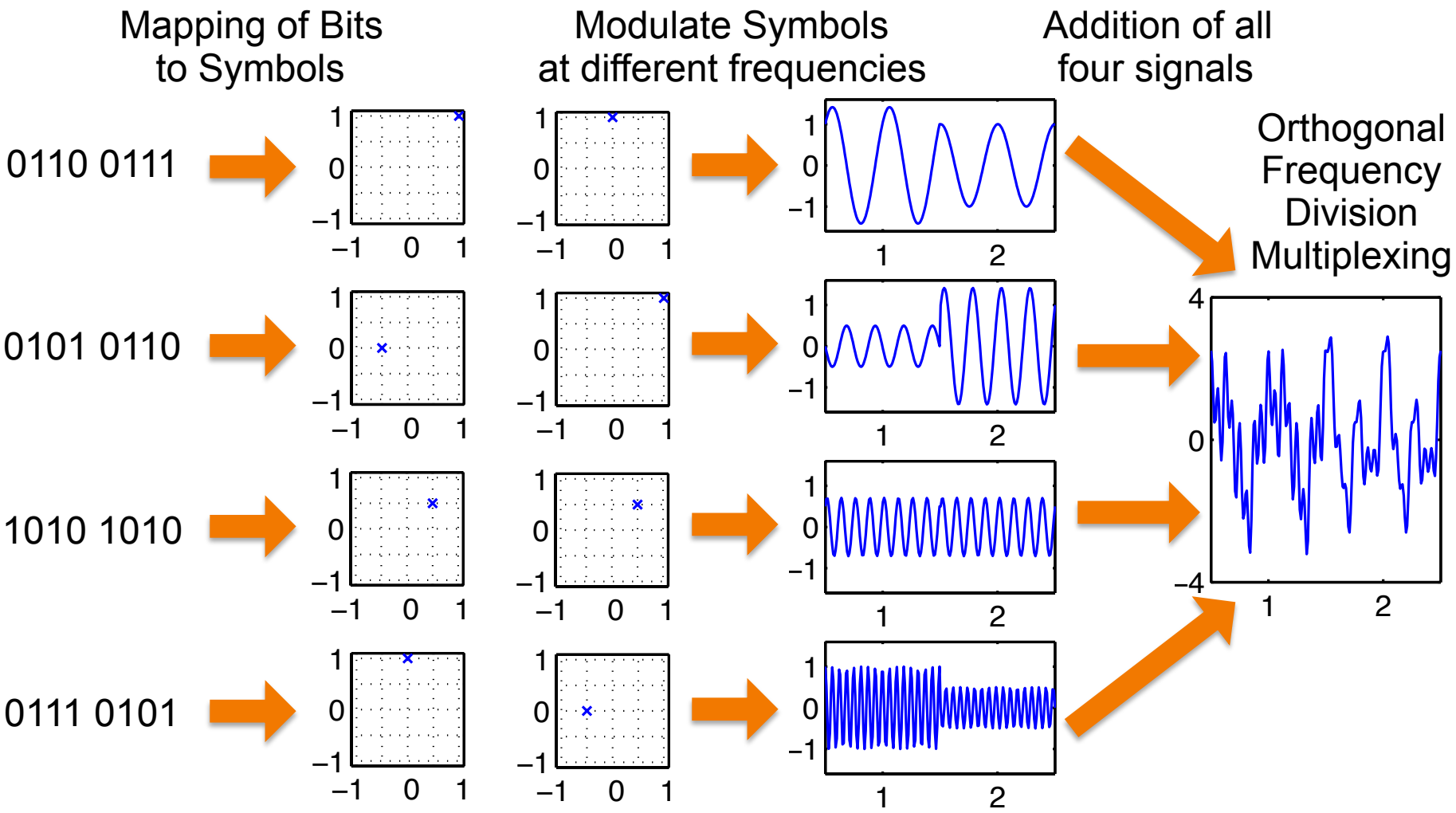


How signals get transmitted

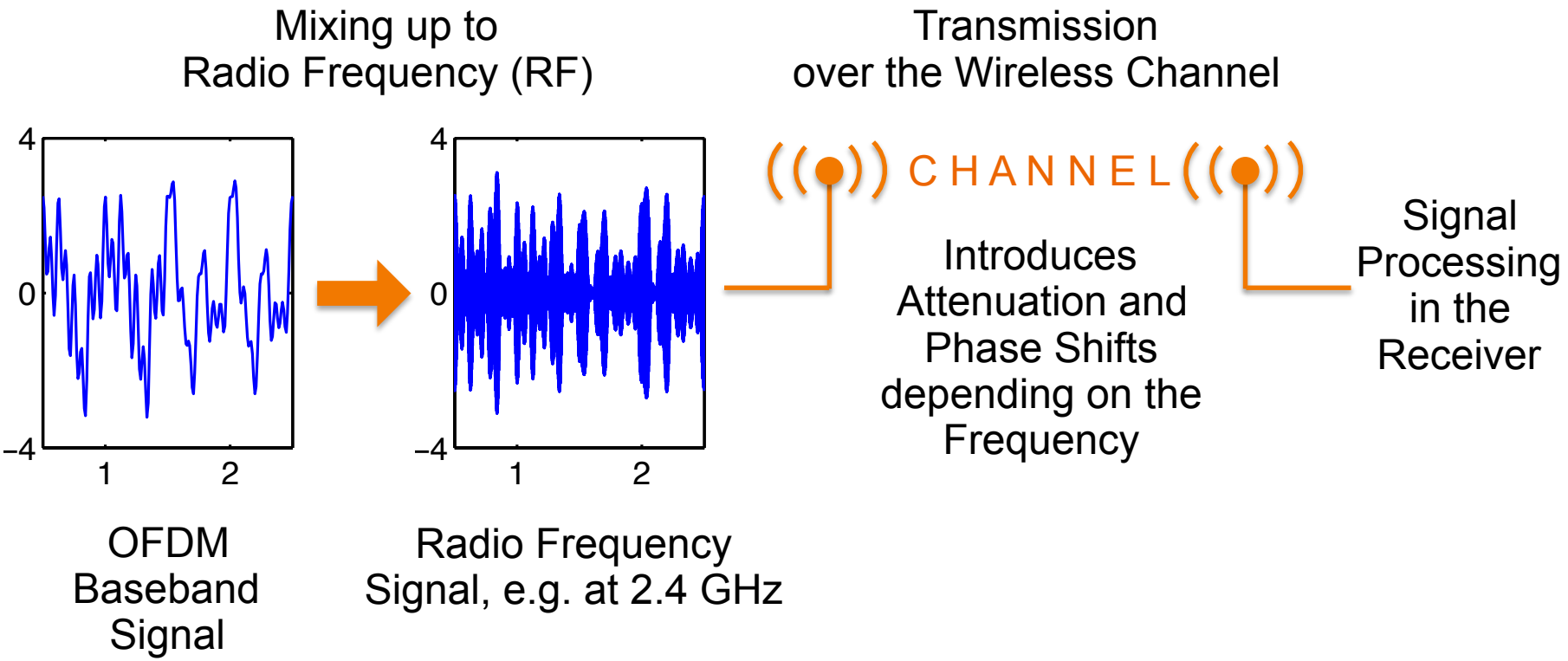
- Sine functions at different frequencies are independent (orthogonal) → we can transmit them at the same time and separate them at the receiver again



How signals get transmitted

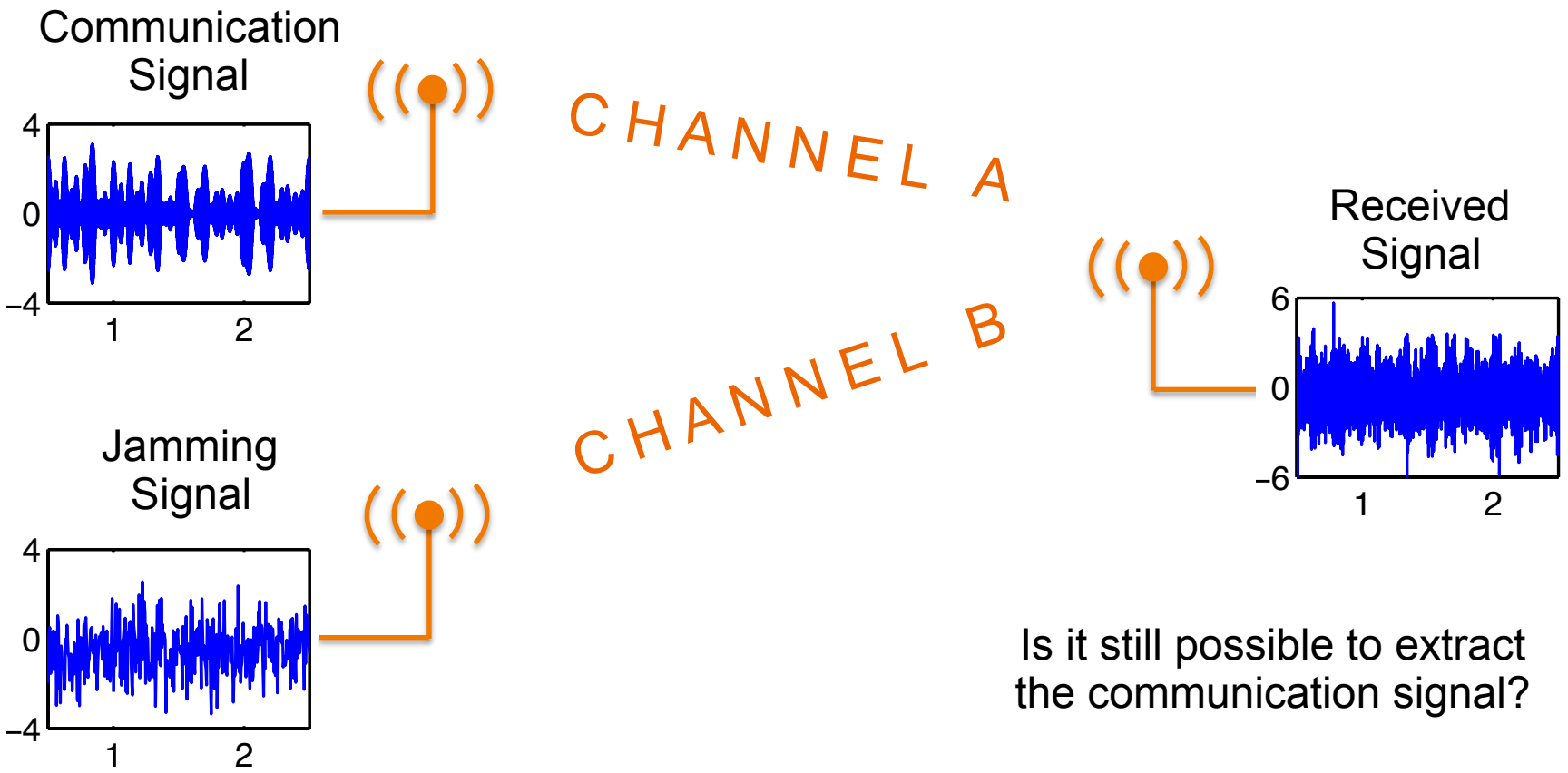


How signals get transmitted



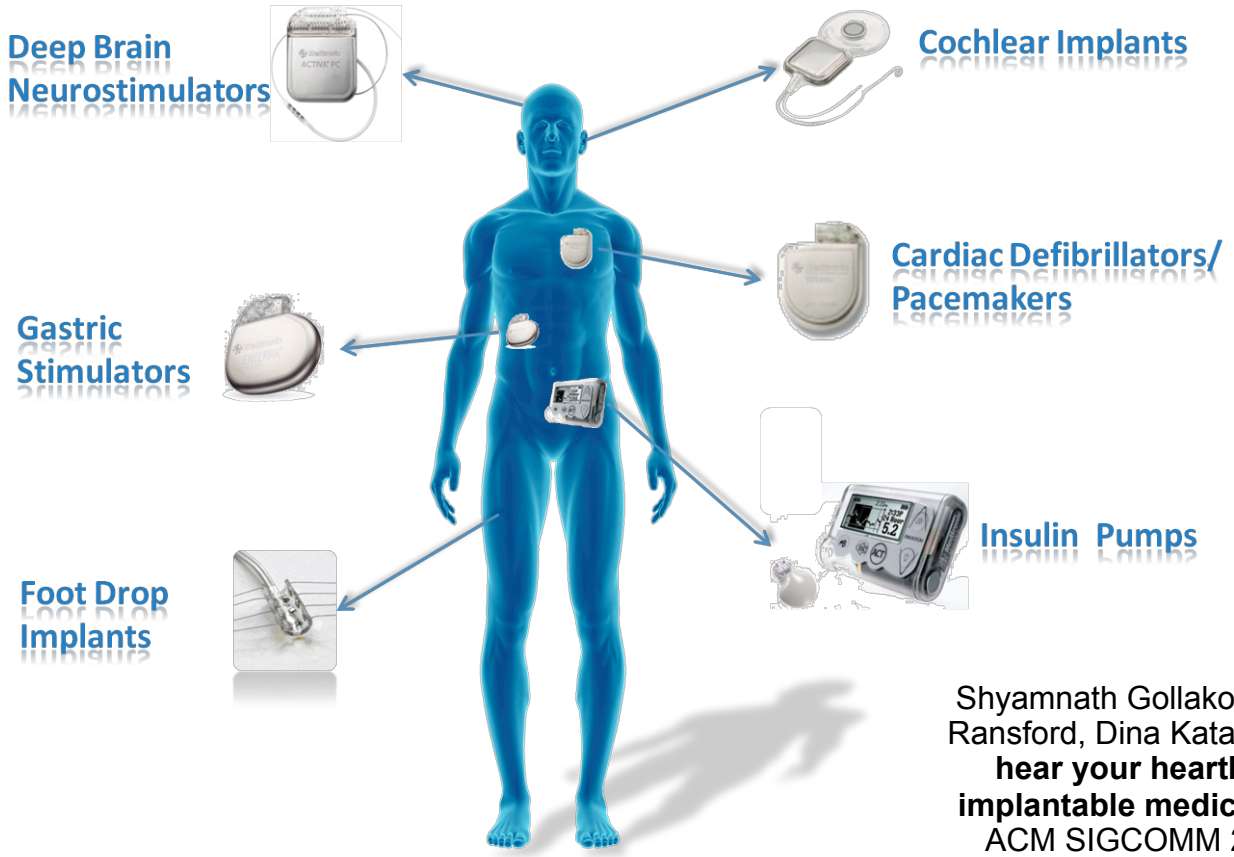
Jamming

Jamming



Is it still possible to extract the communication signal?

IMD Shield: Securing Implantable Medical Devices



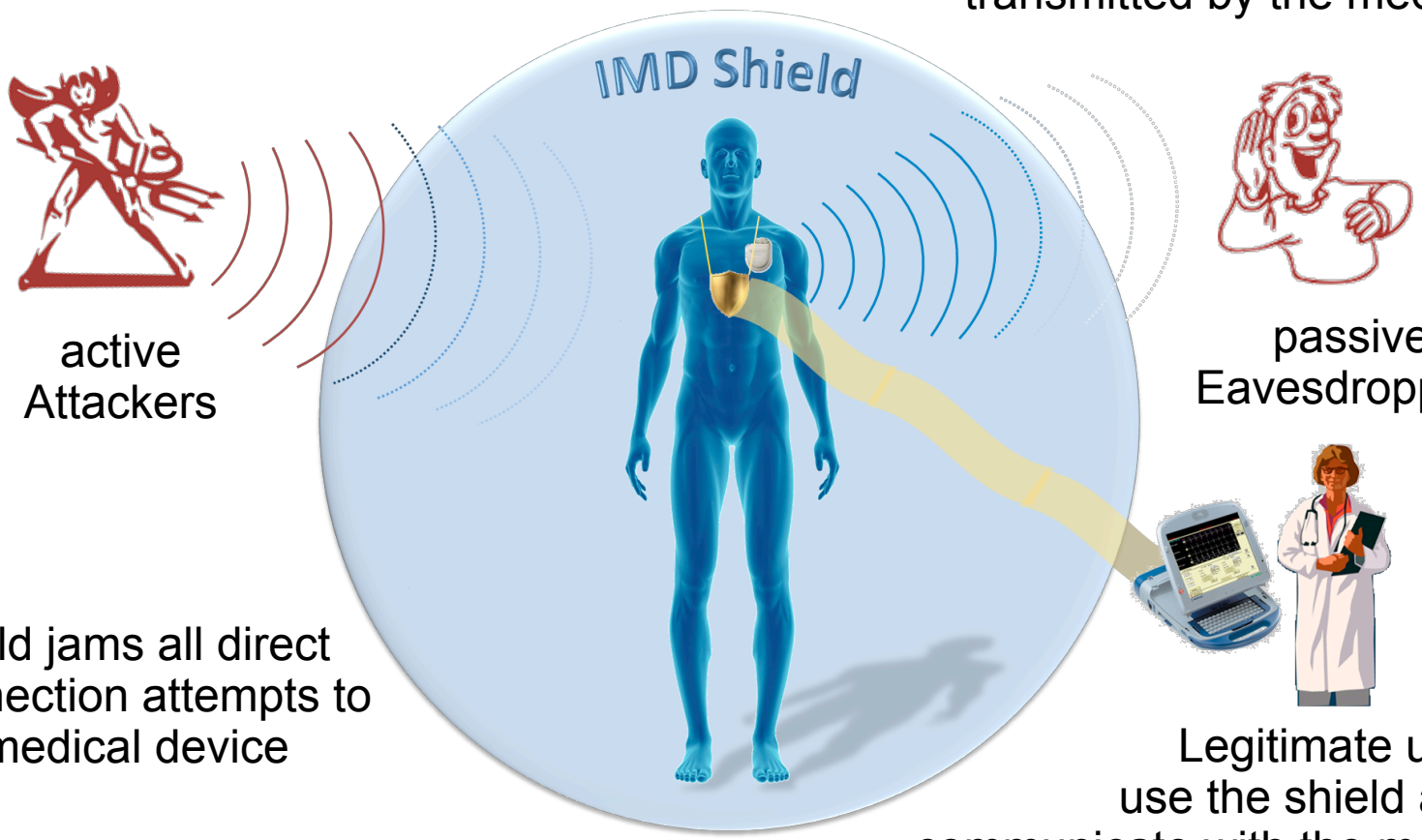
Communication is often not encrypted:

Eavesdropping and malicious reprogramming is possible

Updates for implanted are not feasible

Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. 2011. **They can hear your heartbeats: non-invasive security for implantable medical devices**. In Proceedings of the ACM SIGCOMM 2011 conference (SIGCOMM '11).

IMD Shield: Securing Implantable Medical Devices



Shield jams all responses transmitted by the medical device

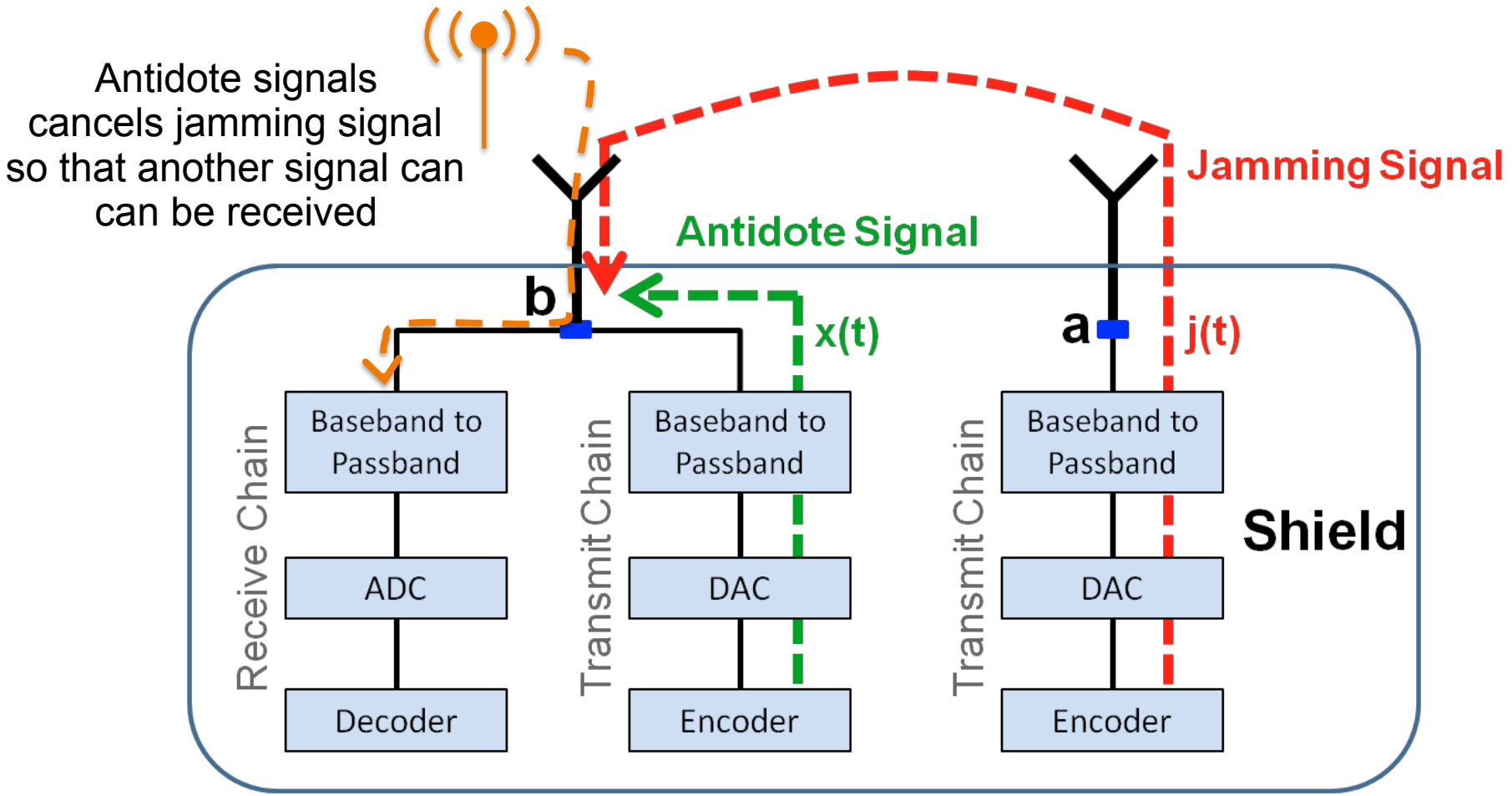
active Attackers

passive Eavesdroppers

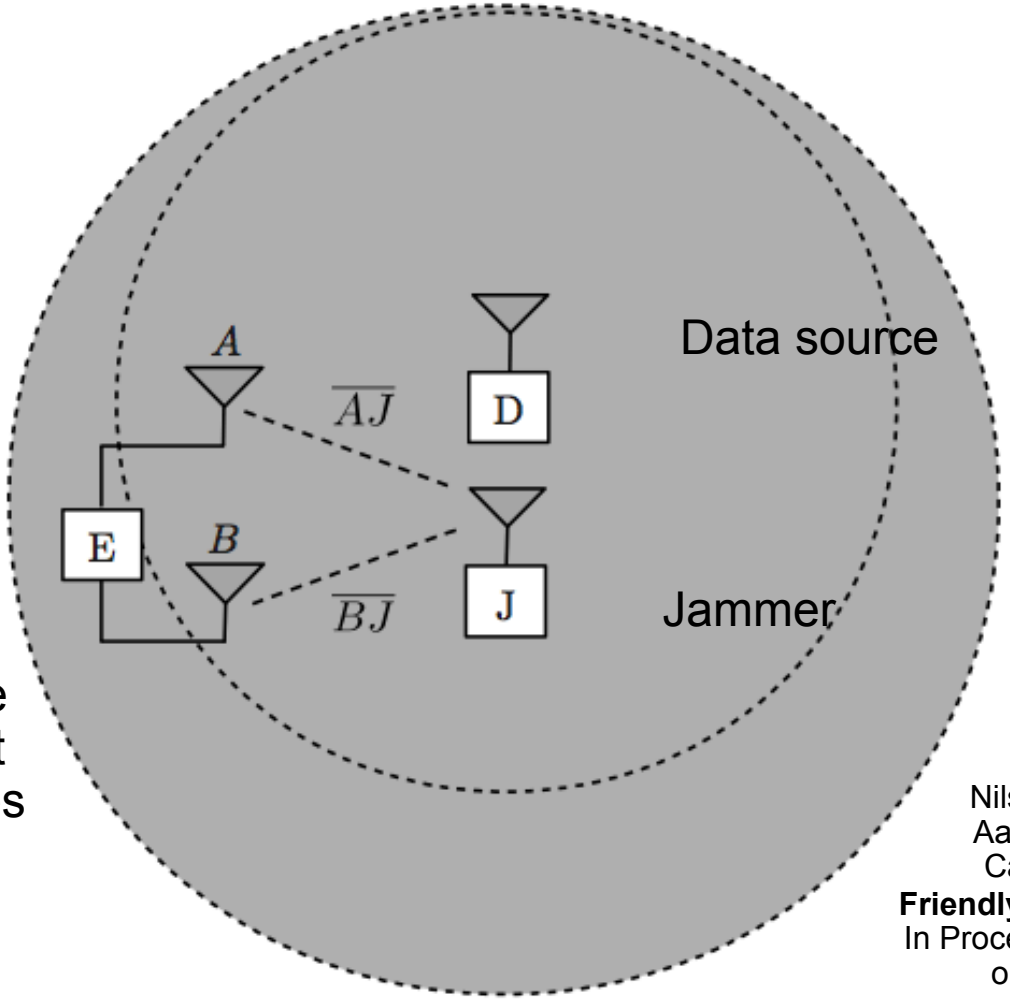
Shield jams all direct connection attempts to the medical device

Legitimate users have to use the shield as a proxy to communicate with the medical device

Jammer-cum-Receiver



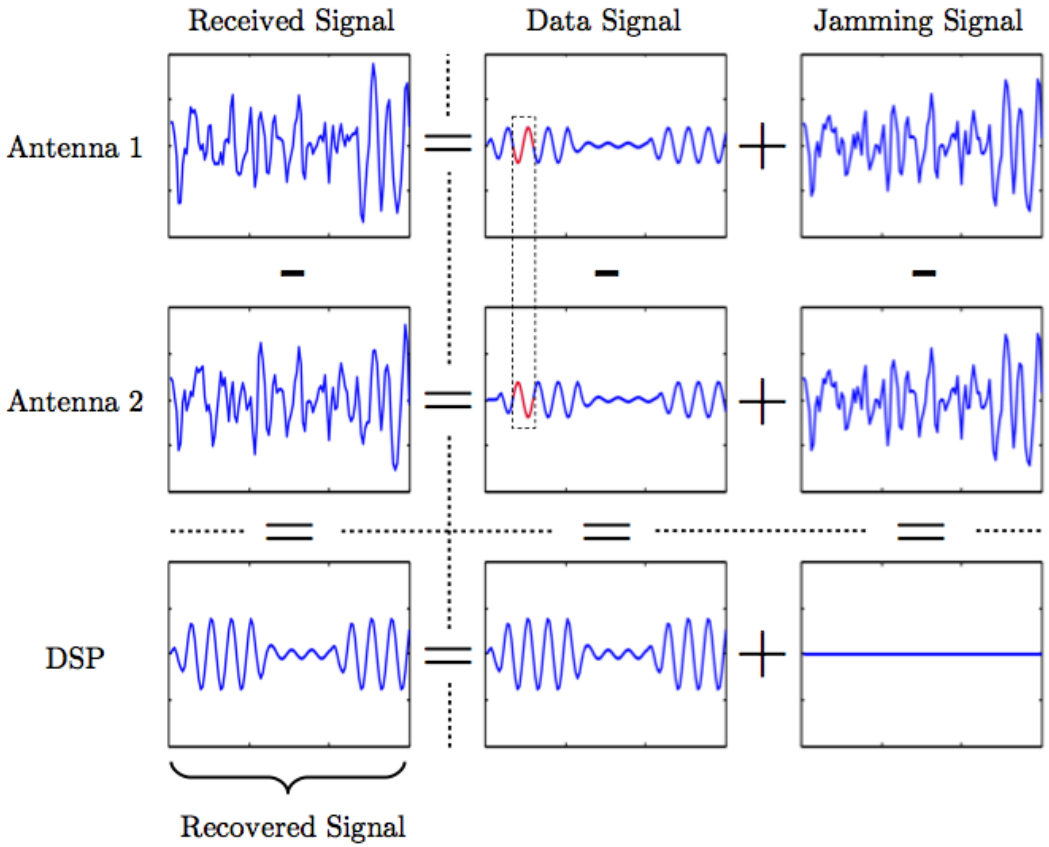
On Limitations of Friendly Jamming for Confidentiality

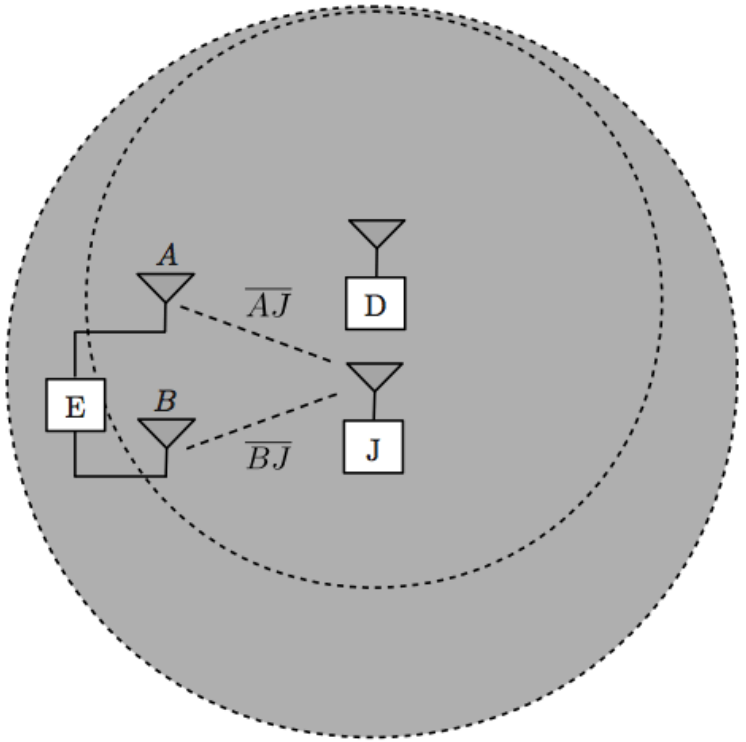


Eavesdropper with two antennas, both having the same distance to J but different distances to D.

Nils Ole Tippenhauer, Luka Malisa, Aanjhan Ranganathan, and Srdjan Capkun. 2013. **On Limitations of Friendly Jamming for Confidentiality**. In Proceedings of the IEEE Symposium on Security and Privacy (S&P'13)

On Limitations of Friendly Jamming for Confidentiality





Interested in Physical Layer Experiments?

SEEMOO
SECURE MOBILE NETWORKING

NATIONAL INSTRUMENTS LabVIEW

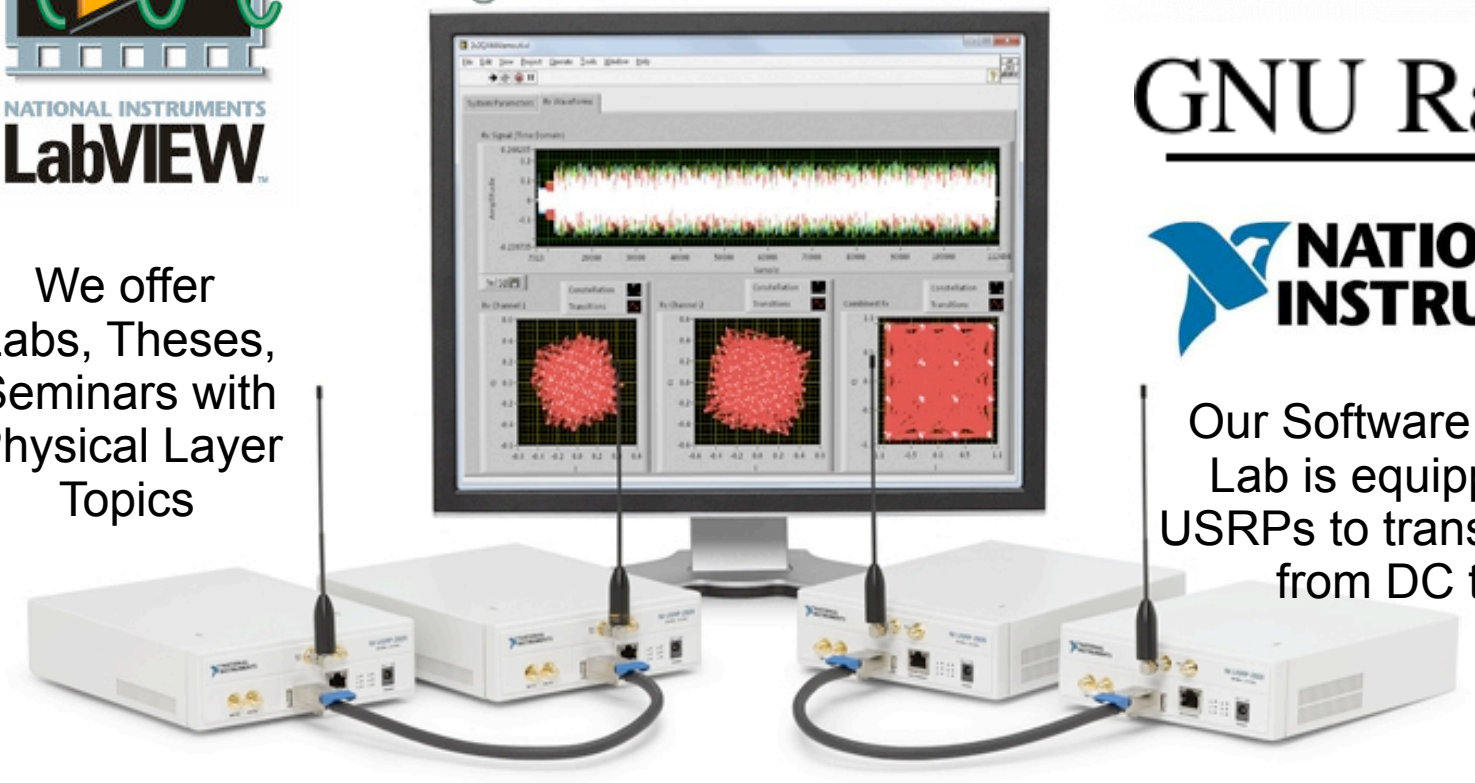
Ettus Research

MATLAB SIMULINK

GNU Radio

NATIONAL INSTRUMENTS

We offer Labs, Theses, Seminars with Physical Layer Topics

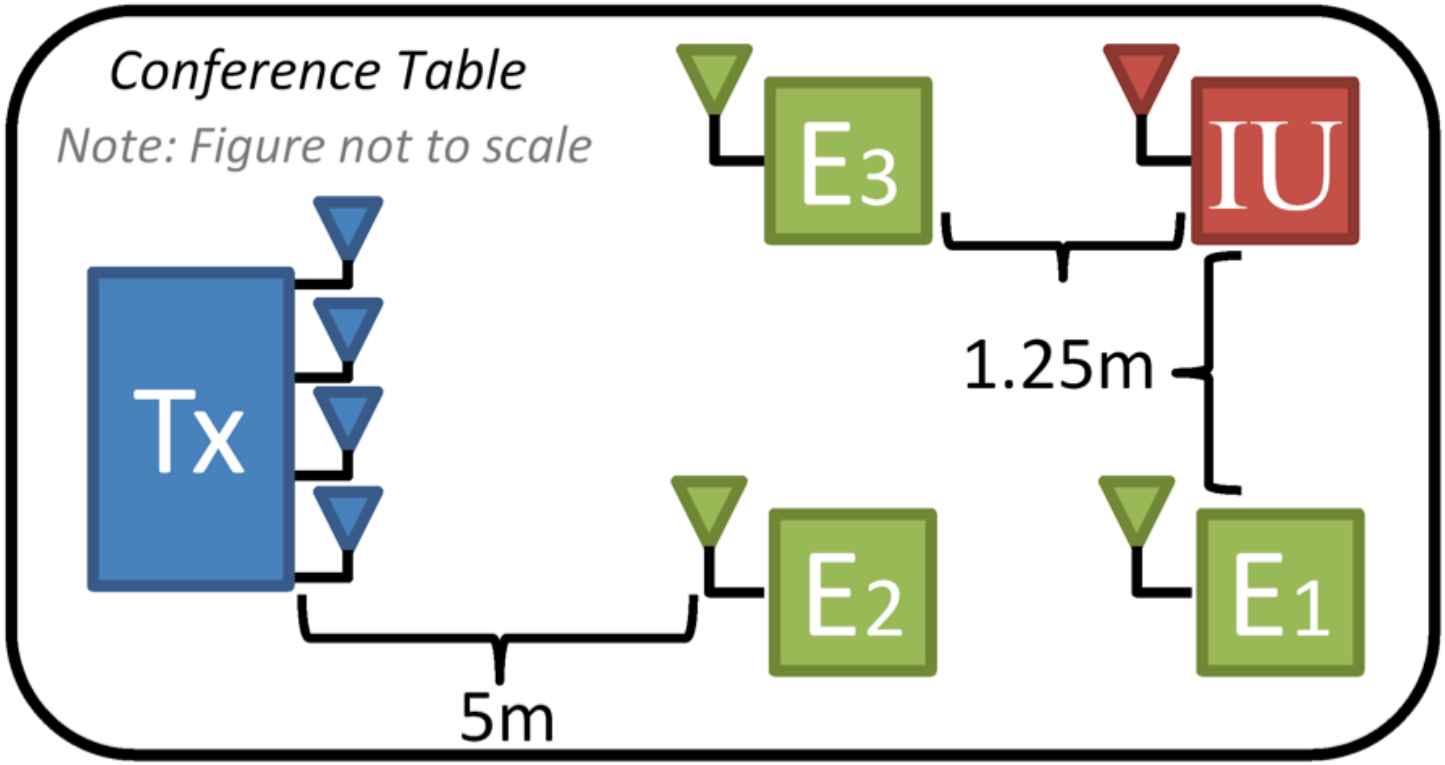


Our Software Defined Radio Lab is equipped with eight USRPs to transmit and receive from DC to 4.4 GHz

STROBE: Actively Securing Wireless Communications using Zero-Forcing Beamforming

Transmitter with four antennas (MIMO) can send signals into four spatial dimensions

Three eavesdroppers and one intended receiver each equipped with one antenna

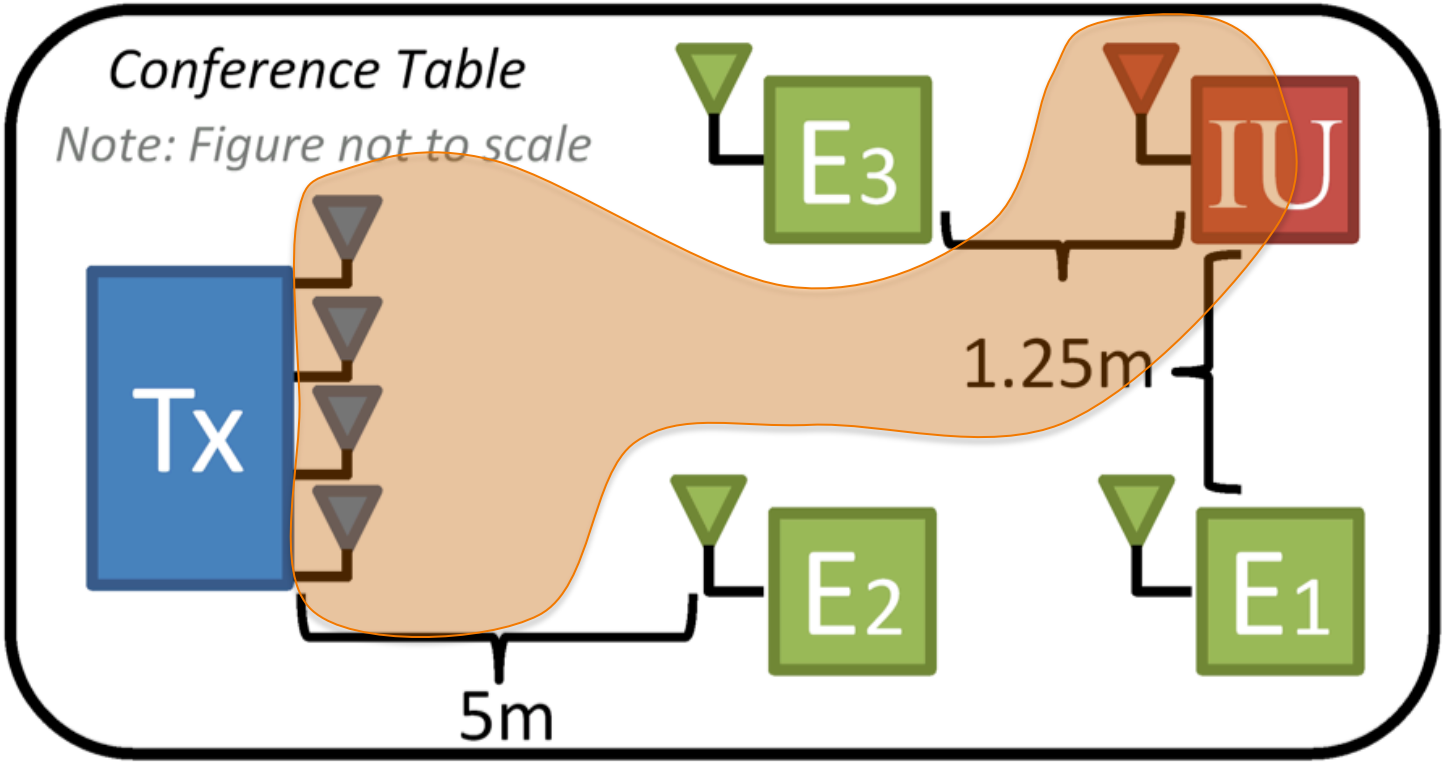


N. Anand, Sung-Ju Lee, E.W. Knightly. 2012. **STROBE: Actively securing wireless communications using Zero-Forcing Beamforming.** In Proceedings of the INFOCOM 2012

STROBE: Actively Securing Wireless Communications using Zero-Forcing Beamforming

Transmitter with four antennas can send signals into four spatial dimensions

Three eavesdroppers and one intended receiver each equipped with one antenna



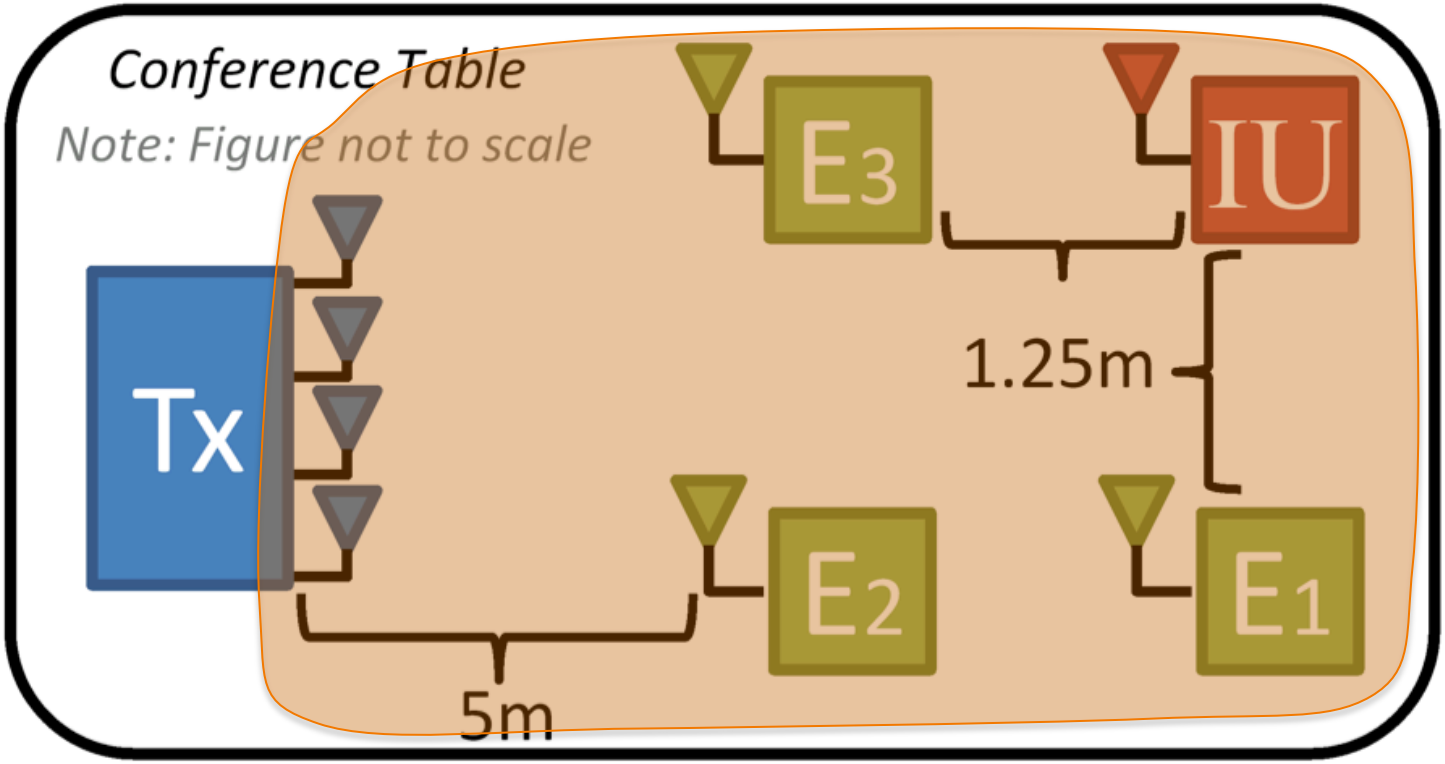
If channels from transmitter to eavesdroppers are known at the transmitter, it can be avoided to transmit to the eavesdroppers.

N. Anand, Sung-Ju Lee, E.W. Knightly. 2012. **STROBE: Actively securing wireless communications using Zero-Forcing Beamforming.** In Proceedings of the INFOCOM 2012

STROBE: Actively Securing Wireless Communications using Zero-Forcing Beamforming

Transmitter with four antennas can send signals into four spatial dimensions

Three eavesdroppers and one intended receiver each equipped with one antenna



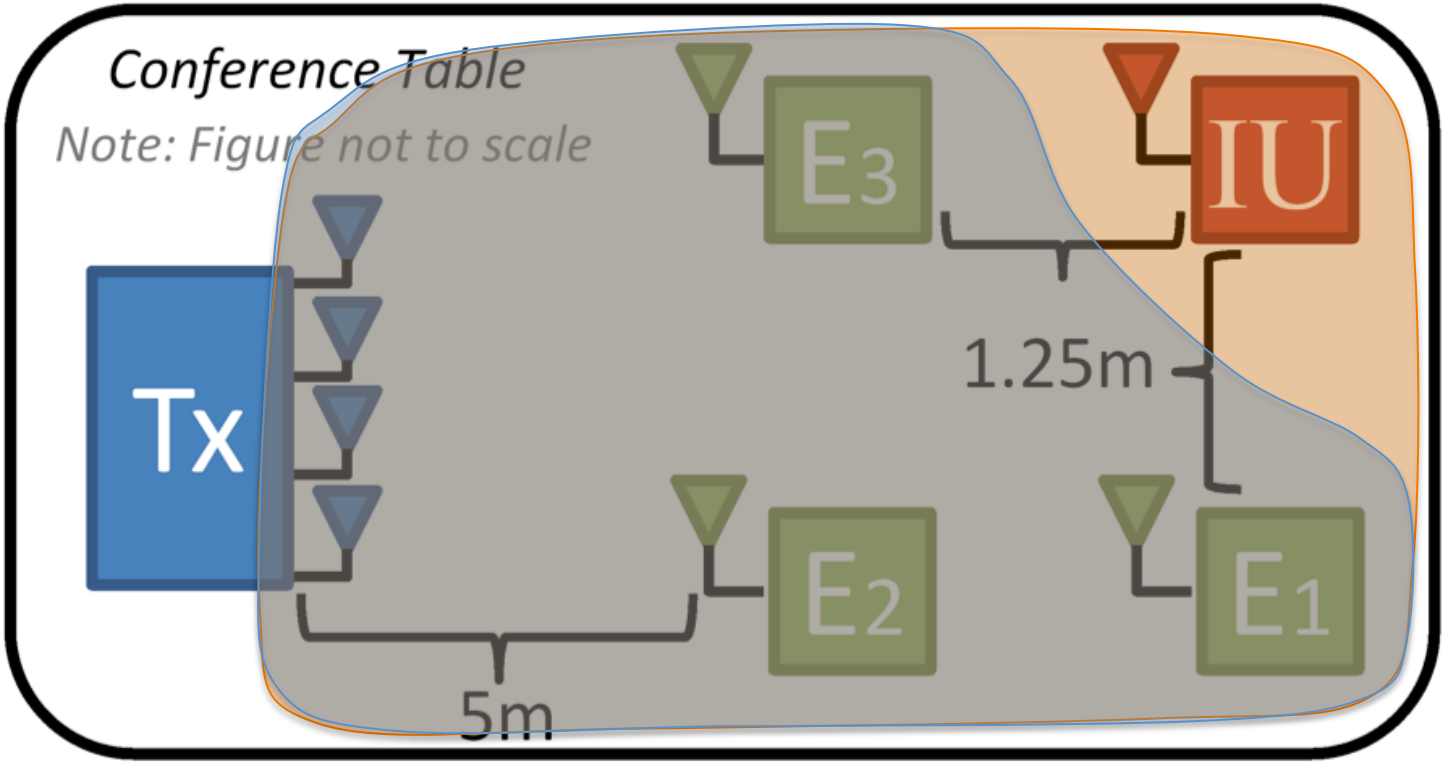
If channels from transmitter to eavesdroppers are NOT known at the transmitter, the signal can be received by the eavesdroppers.

N. Anand, Sung-Ju Lee, E.W. Knightly. 2012. **STROBE: Actively securing wireless communications using Zero-Forcing Beamforming.** In Proceedings of the INFOCOM 2012

STROBE: Actively Securing Wireless Communications using Zero-Forcing Beamforming

Transmitter with four antennas can send signals into four spatial dimensions

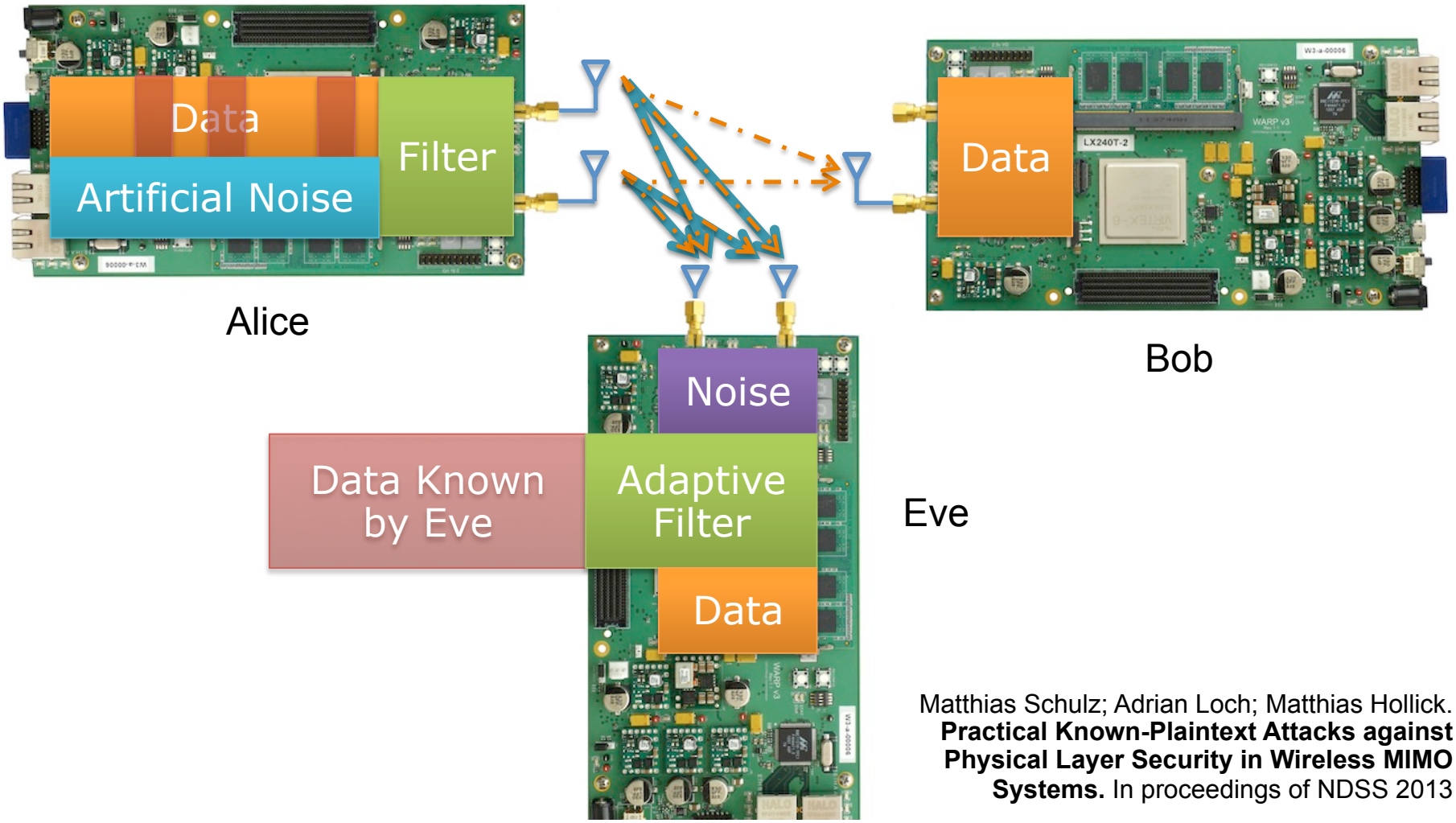
Three eavesdroppers and one intended receiver each equipped with one antenna



As only one spatial dimension is required to transmit to the receiver, the transmitter can use its additional three spatial dimensions to transmit artificial noise orthogonal to the receivers channel

N. Anand, Sung-Ju Lee, E.W. Knightly. 2012. **STROBE: Actively securing wireless communications using Zero-Forcing Beamforming.** In Proceedings of the INFOCOM 2012

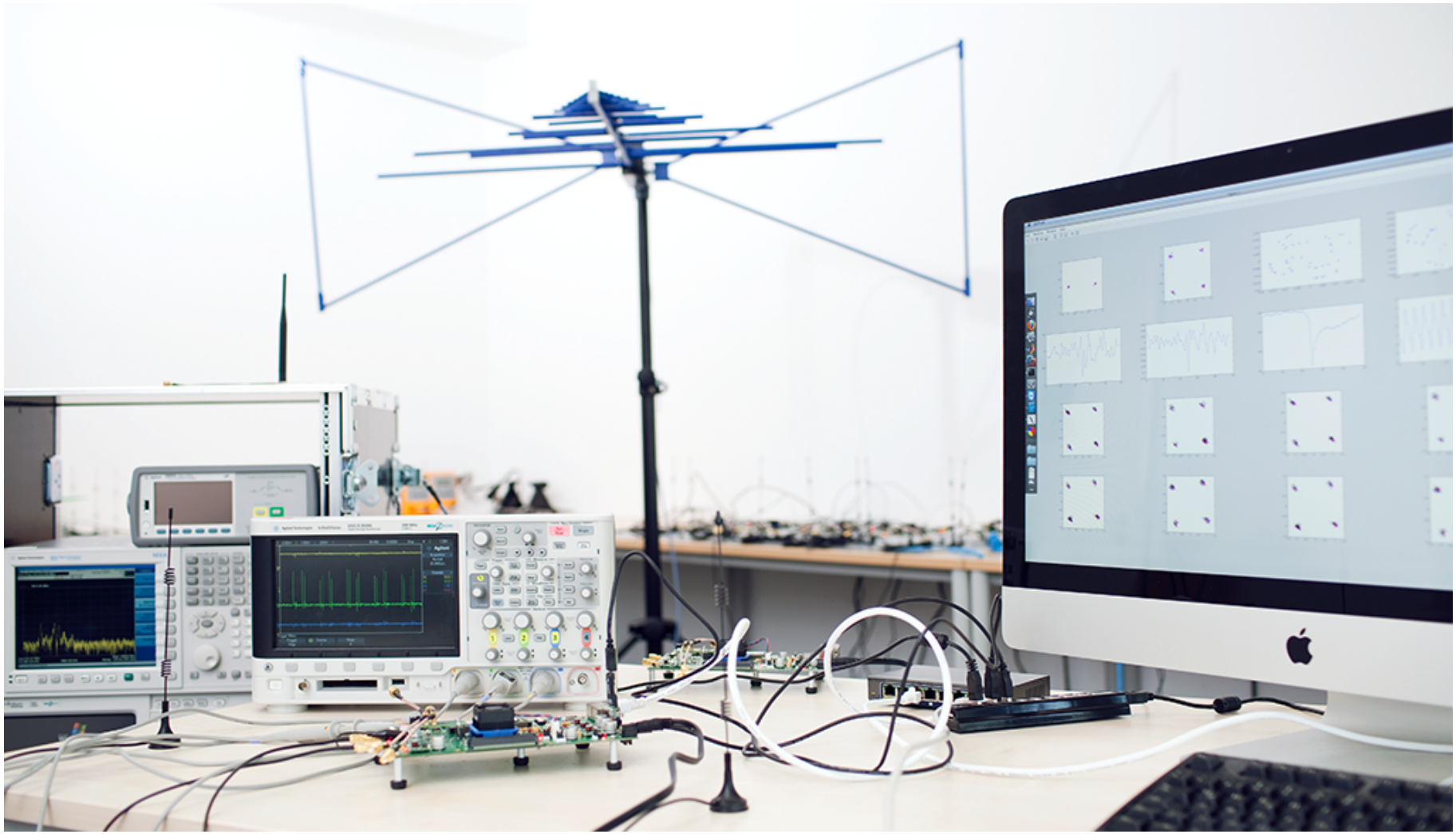
Known Plaintext Attacks against Physical Layer Security in Wireless MIMO Systems



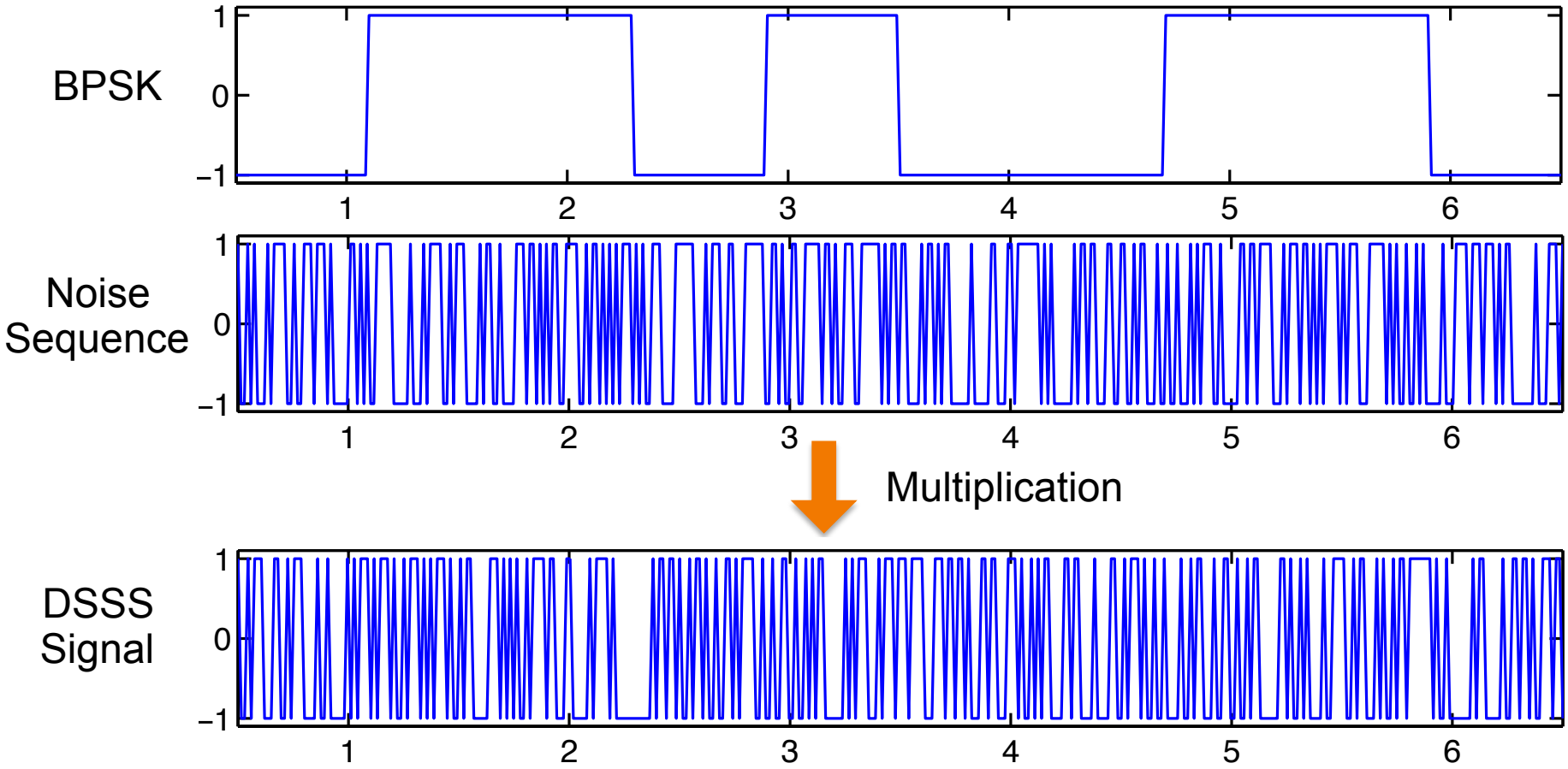
Matthias Schulz; Adrian Loch; Matthias Hollick. **Practical Known-Plaintext Attacks against Physical Layer Security in Wireless MIMO Systems.** In proceedings of NDSS 2013

Interested in Advanced Physical Layer Experiments with MIMO Systems?

SEEMO
SECURE MOBILE NETWORKING

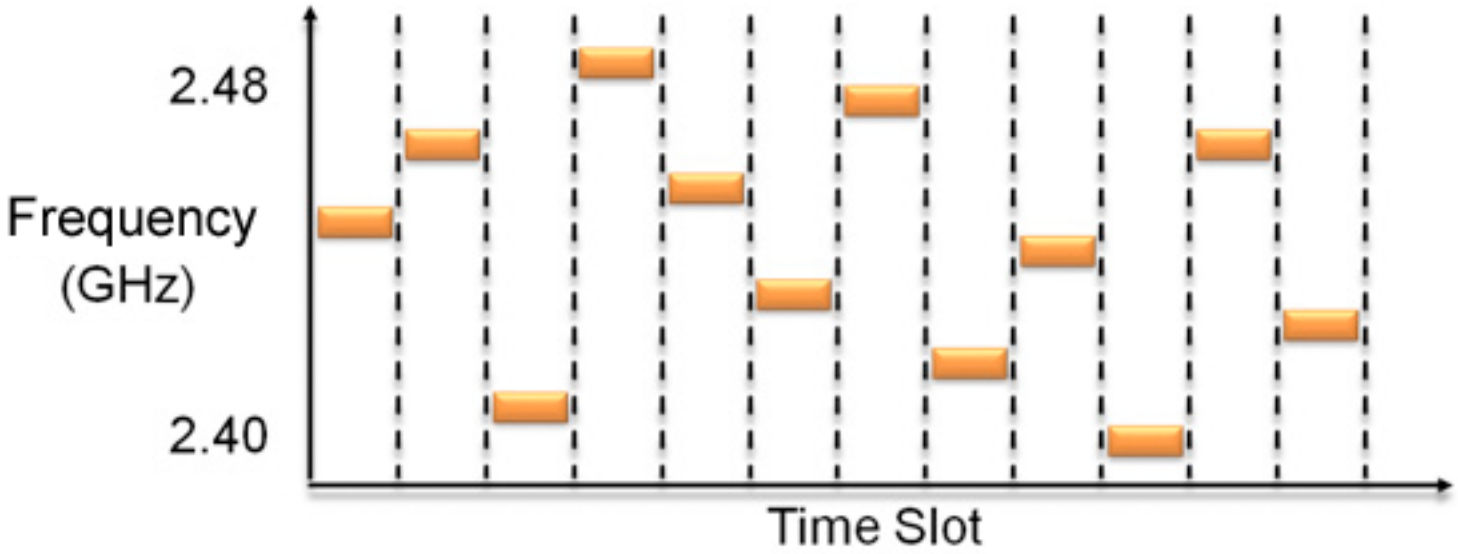


Direct Sequence Spread Spectrum (DSSS)



The noise sequence is required to extract the information signal, this can be used like a one-time pad.

Frequency Hopping



The Radio Frequency is constantly changing. Only if the hopping sequence is known the transmitted information can be reconstructed.

Downside: If there is only one transmitter an eavesdropper can observe the whole frequency spectrum and record the complete transmission to reconstruct the hopping sequence.

Read the article about our Lab in the hoch³ FORSCHEN

SECURE MOBILE NETWORKING

hoch³ FORSCHEN
Das Medium für Wissenschaft

TECHNISCHE UNIVERSITÄT DARMSTADT

__ 1 Sicher in die Kurve: Neue Technik für Motorräder __ 2 Versteckte Schätze bergen: Wertvolle Rohstoffe in Altgebäuden __ 3 Immer auf Empfang und Sendung: Mobile Kommunikationsnetzwerke werden robuster __ 4 Das Interview: Signale für die Smart City

hoch³FORSCHEN / Jahrgang 2 / Juni 2013

INFORMATIONS SYSTEM TECHNIK

et:t

Fachbereich Informatik

http://seemoo.de/physec

Drahtlose Netze zur Krisenbewältigung: Grundlagen, Entwurf und Aufbau von Null

20-00-0780-iv

How to survive the ZOMBIE APOCALYPS

SEEMOO
SECURE MOBILE NETWORKING

Integrated Course

5 CP

INFORMATIONS SYSTEM TECHNIK

et:t

Fachbereich Informatik

http://seemoo.de/zombie

Copyright Notice