Physical Layer Security for Cyber-Physical Systems: Friendly Jammers

GUNES KARABULUT KURT

gkurt@itu.edu.tr

Wireless Communications and Research Laboratory (WCRL)

ISTANBUL TECHNICAL UNIVERSITY

OUTLINE

Introduction

- Cyber-Physical Systems
- Main Components
- Physical Topology

Requirements

- Operational
- Security

Security View

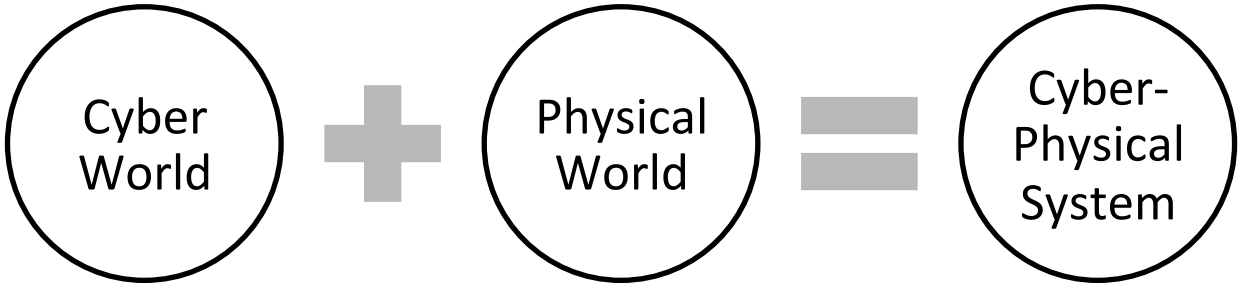
- Classical View
- Physical Layer Security
- Cross-Layer Security

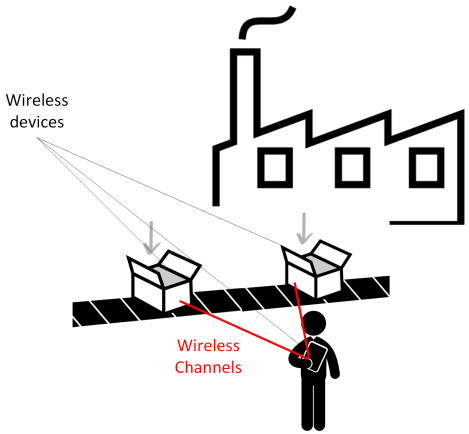
Measurement Results

Summary

Cyber-Physical Systems

"Cyber-Physical Systems are co-engineered interacting networks of physical and computational components."
https://www.nist.gov/el/cyber-physical-systems

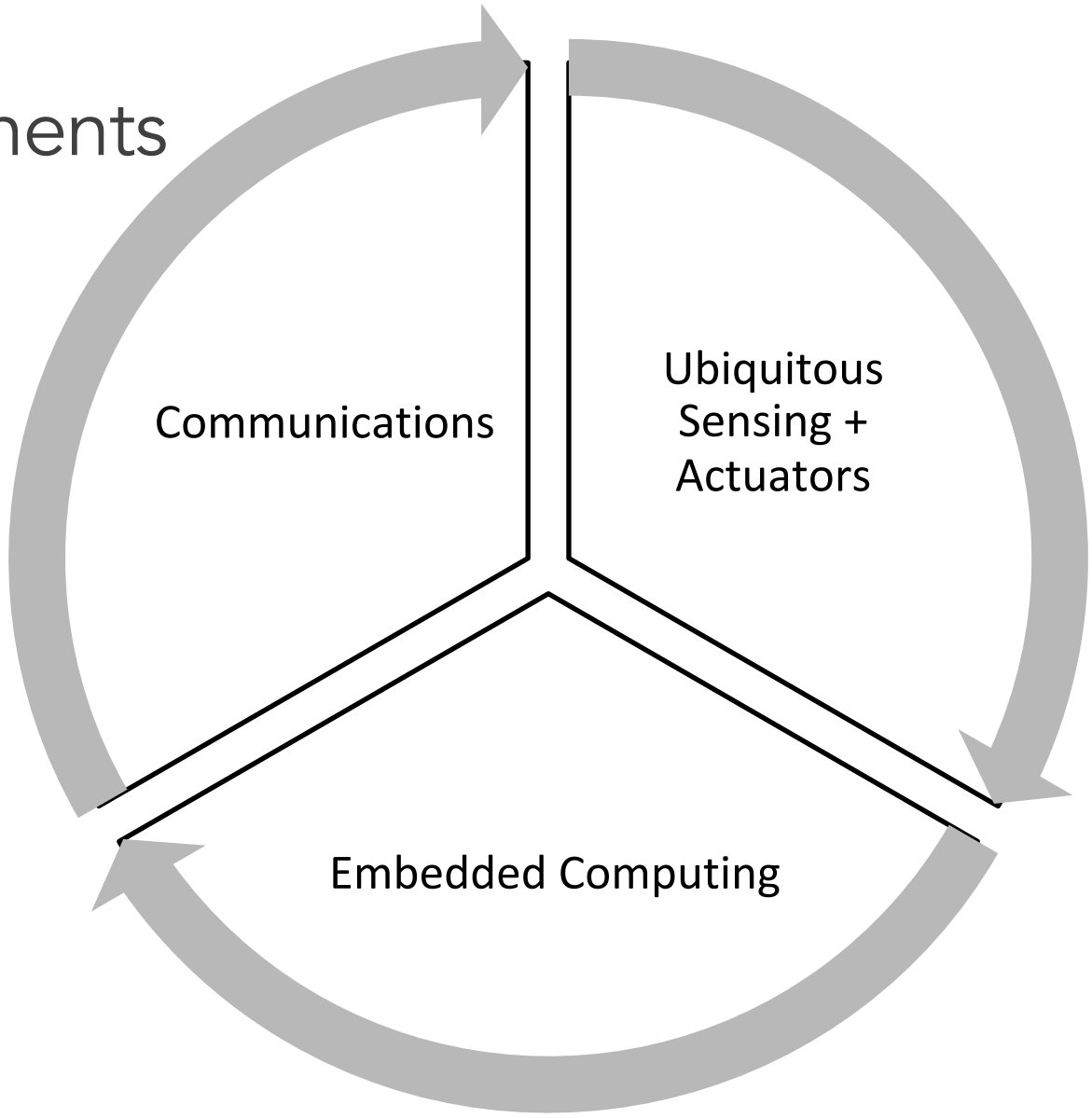


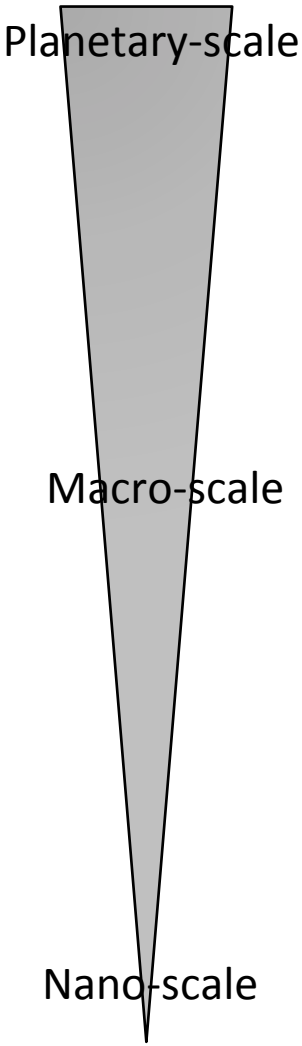


Target Industries:

- Energy
- Manufacturing
- Healthcare
- Smart cities
- Transportation
- …

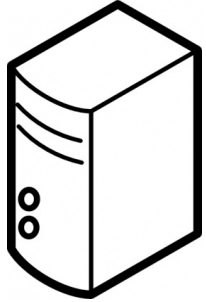
Main Components

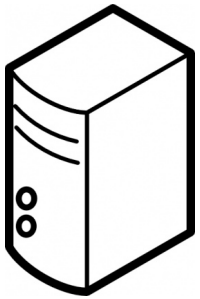




Physical Topology

Users





Distributed Controllers

INTERNET

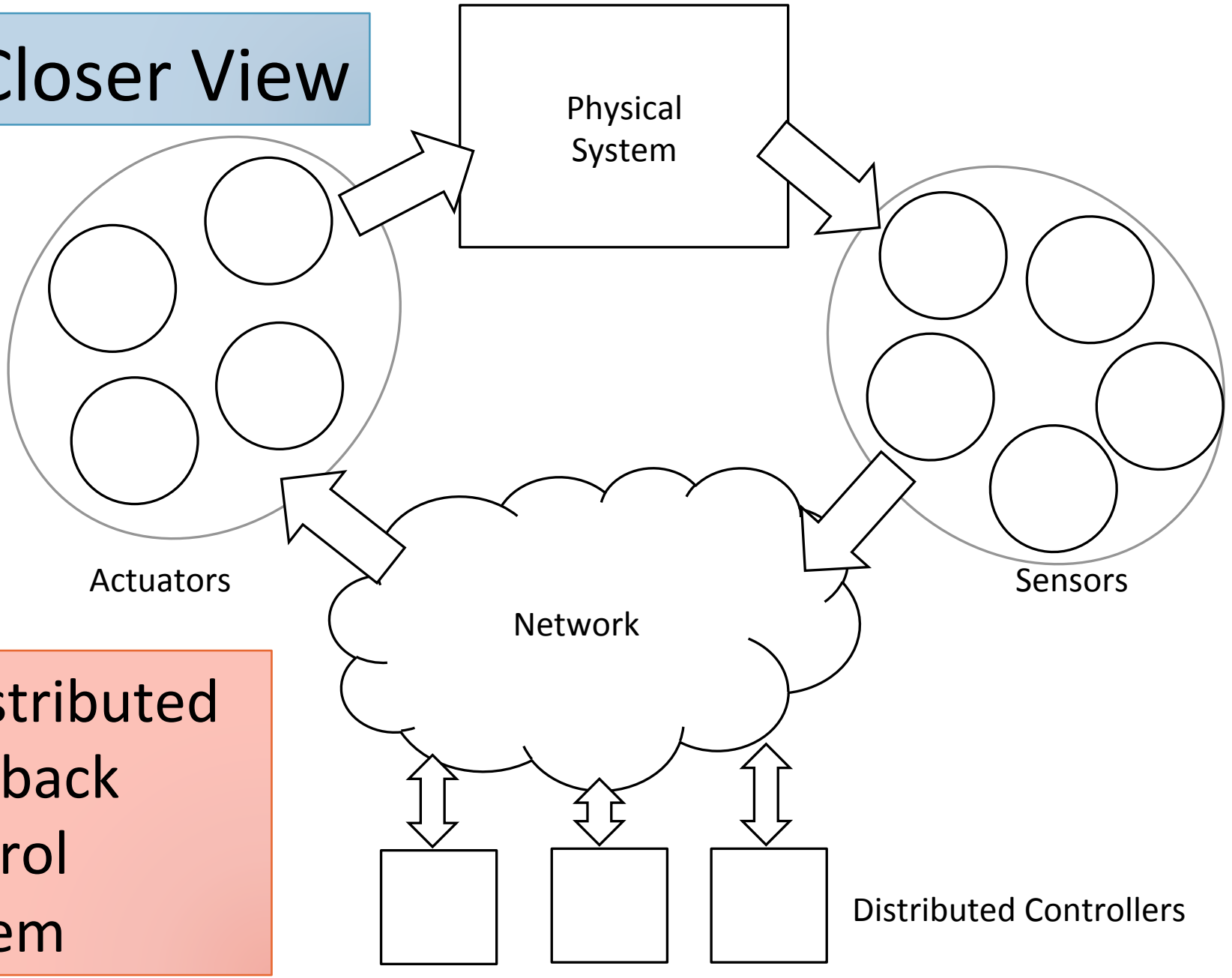
APPLICATION - 1

APPLICATION - 2

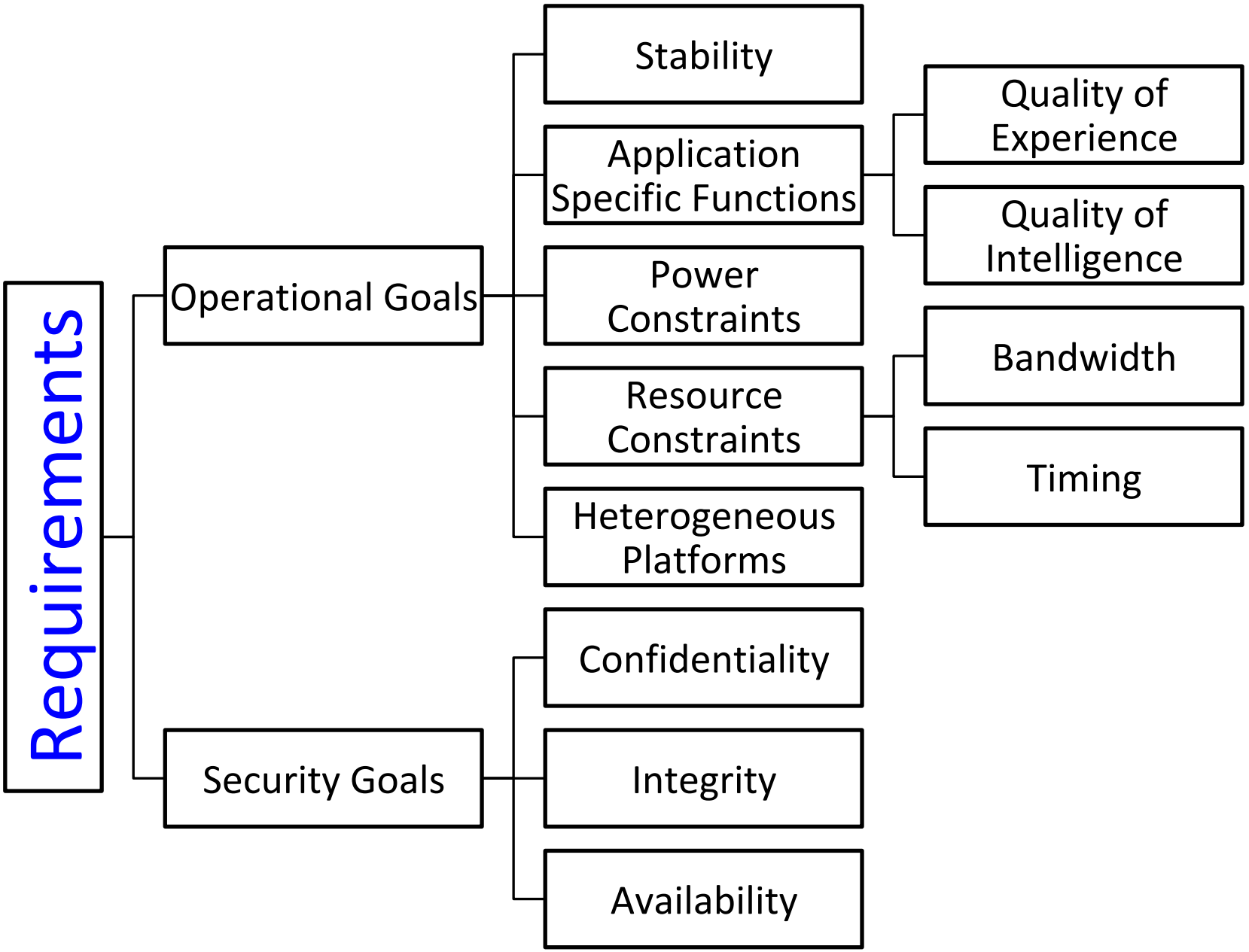
APPLICATION - 3

Applications

A Closer View



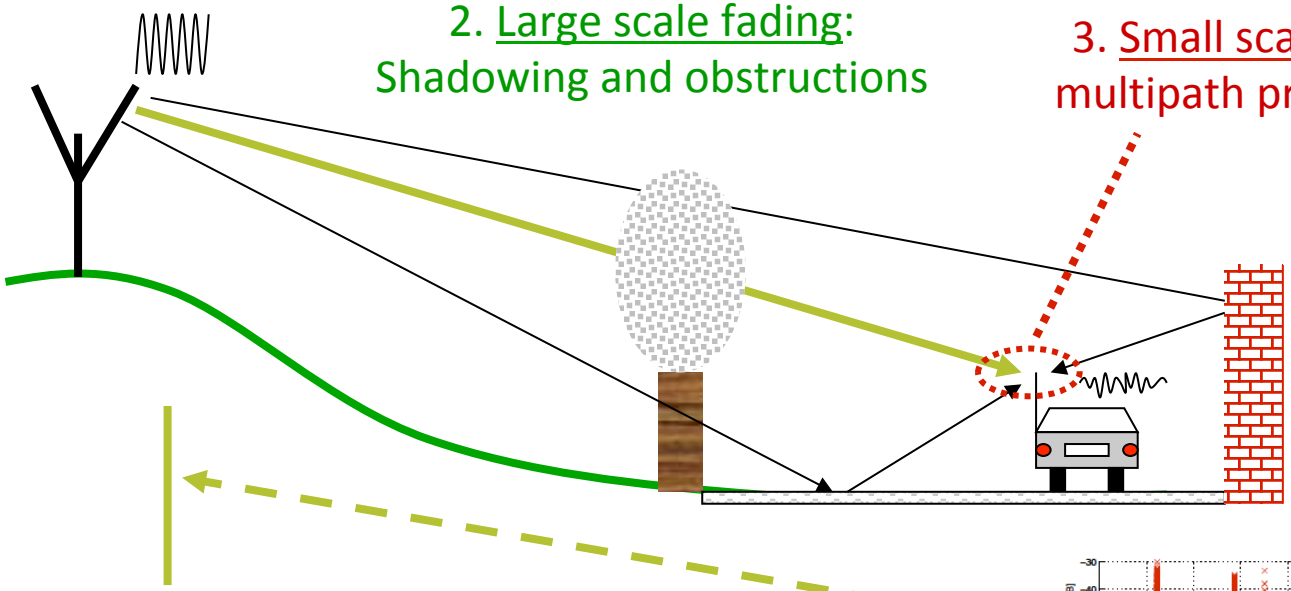
A distributed feedback control system


Requirements
Operational Goals
Security Goals
Stability
Application Specific Functions
Power Constraints
Resource Constraints
Heterogeneous Platforms
Quality of Experience
Quality of Intelligence
Bandwidth
Timing
Confidentiality
Integrity
Availability

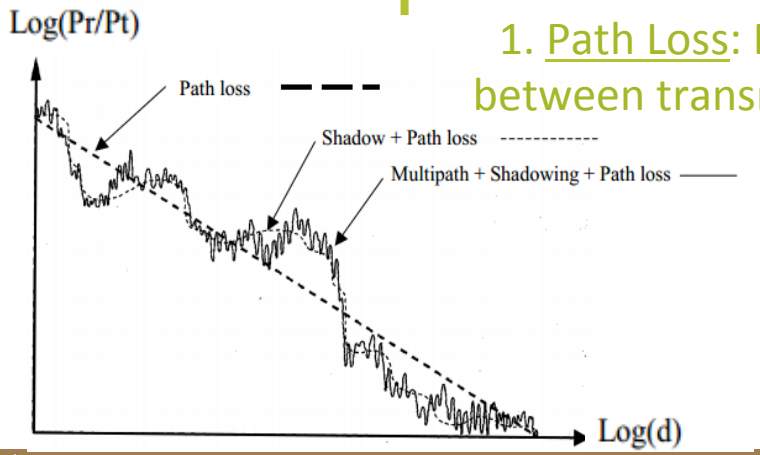
Wireless Channels: Broadcast Environment

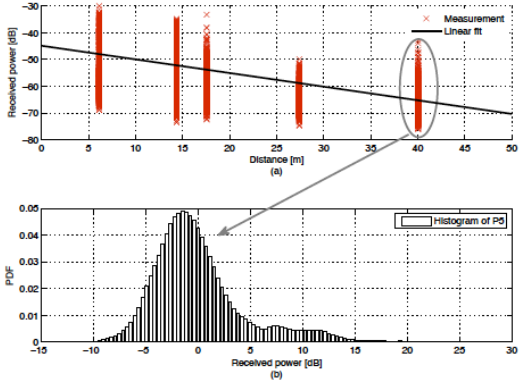
2. Large scale fading: Shadowing and obstructions

3. Small scale fading: multipath propagation



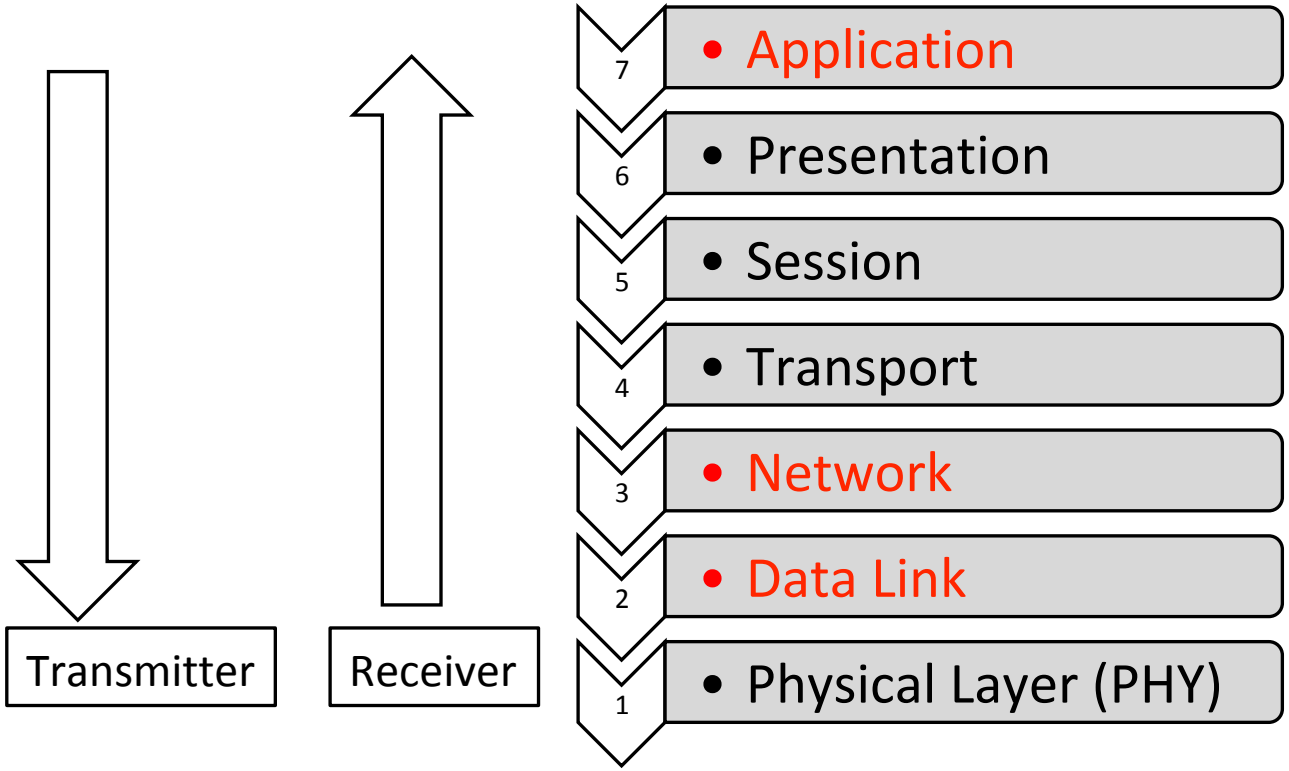
1. Path Loss: Based on distance between transmitter and receiver





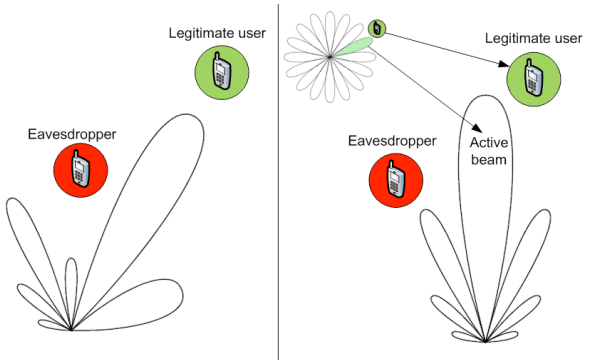
OSI Reference Model- Security Perspective

- Functionalities of a communication system can be characterized in terms of 7 abstraction layers



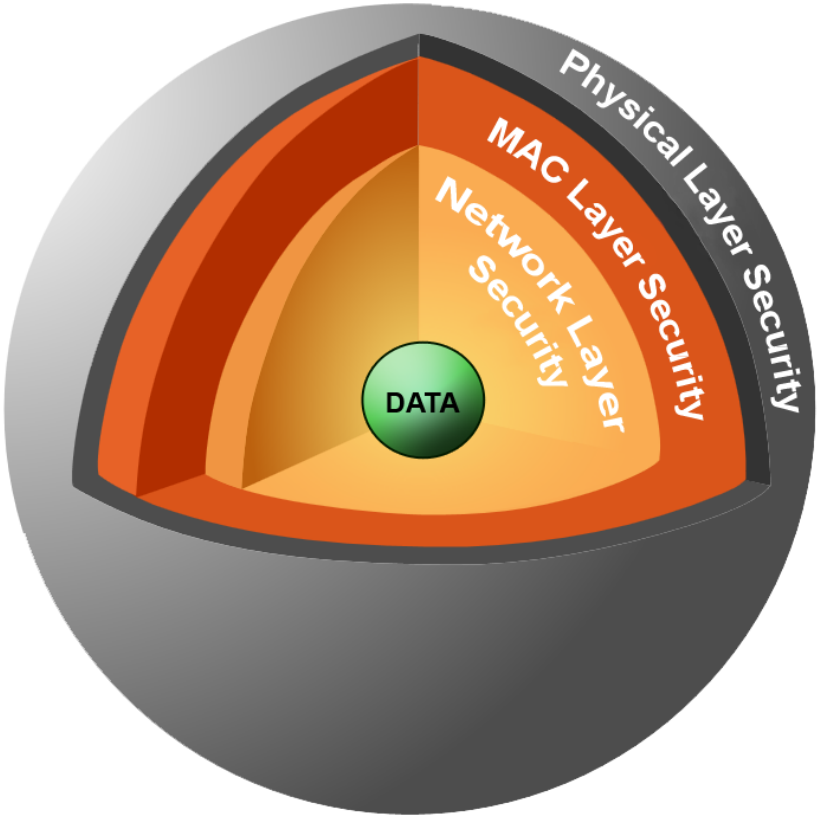
PHY Security - Improving Secrecy

Beamforming: A multi-antenna technique that enables the transmitter to focus signals spatially.



Artificial noise/ artificial interference: Making eavesdroppers' channel worse, by sending irrelavant signals.

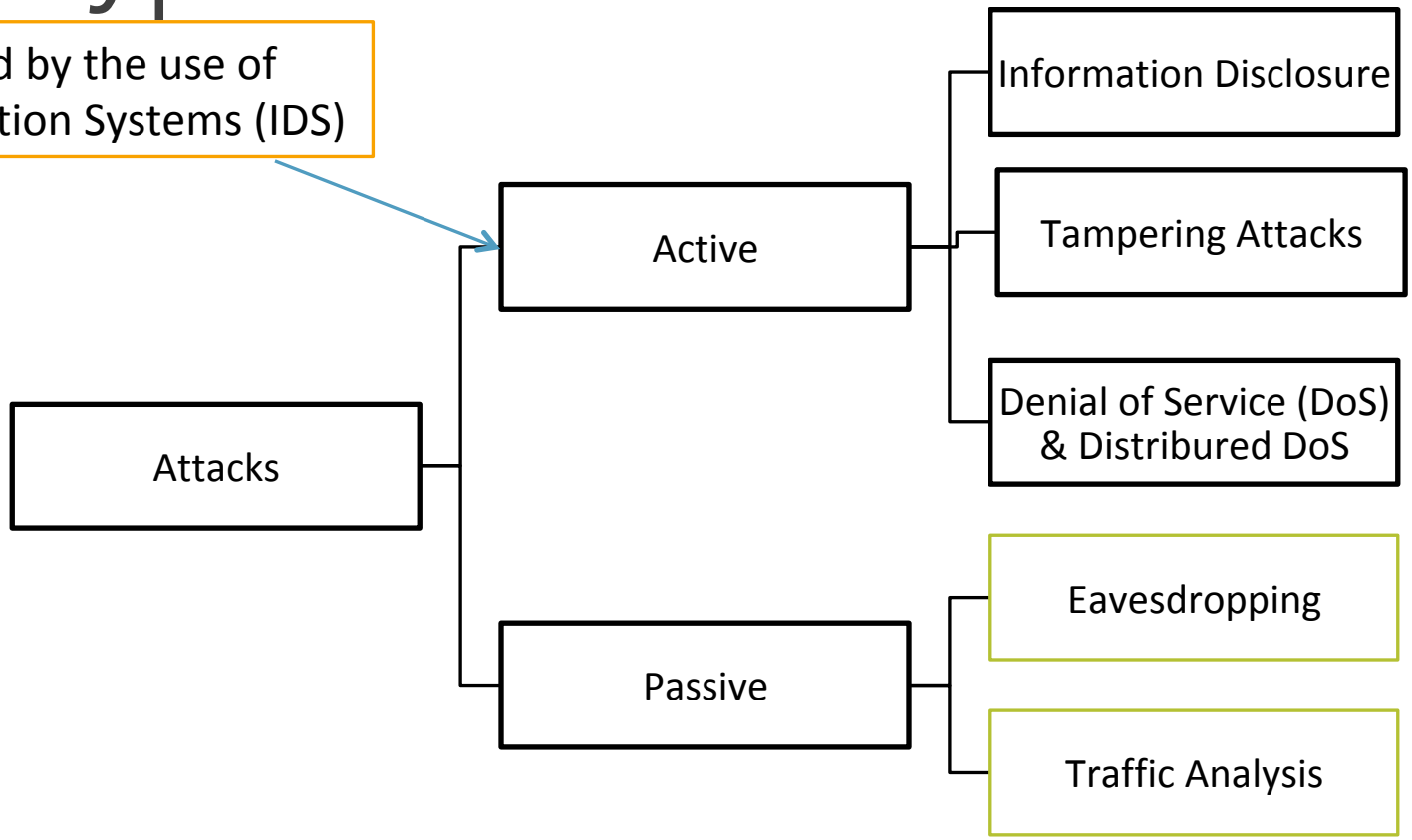
Cross-Layer Security



- Data should pass through all the layers.
- Physical layer (PHY) security becomes inevitably important, as it forms the first step of the security system.

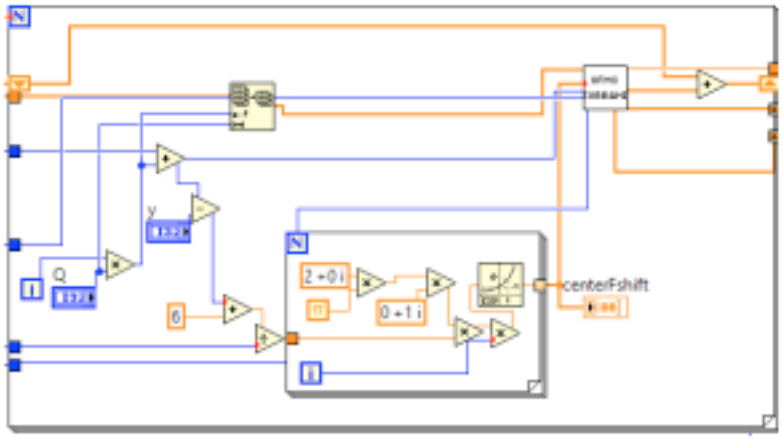
Attack Types

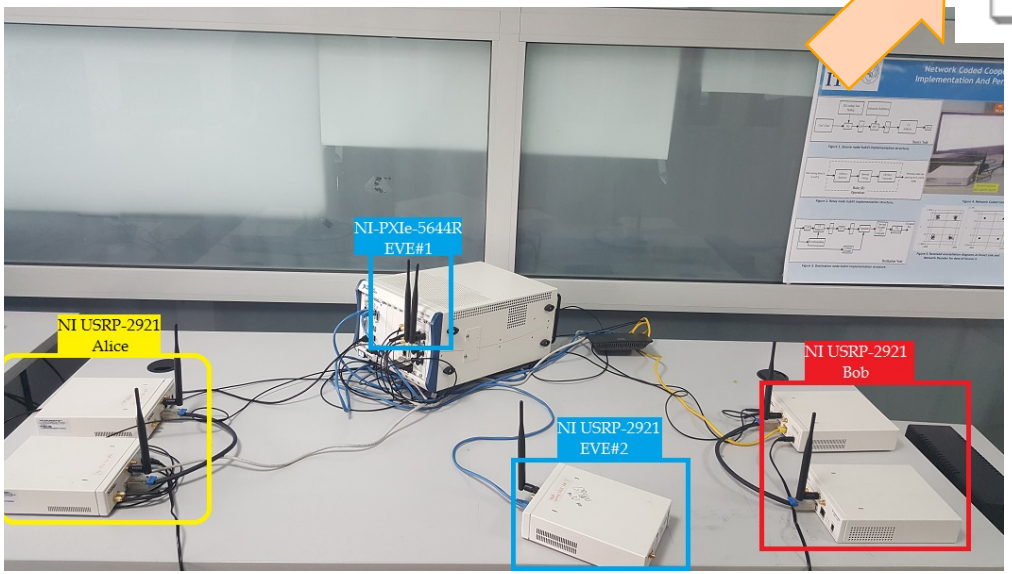
Can be detected by the use of Intrusion Detection Systems (IDS)



A multi-layer approach is required for improved security

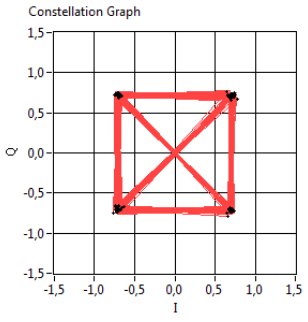
SDR Testbed



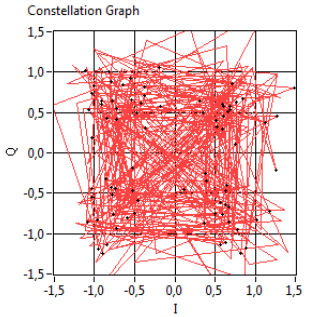


Jammers are co-located at Alice and Bob

Eavesdropper perspective



no Jammer

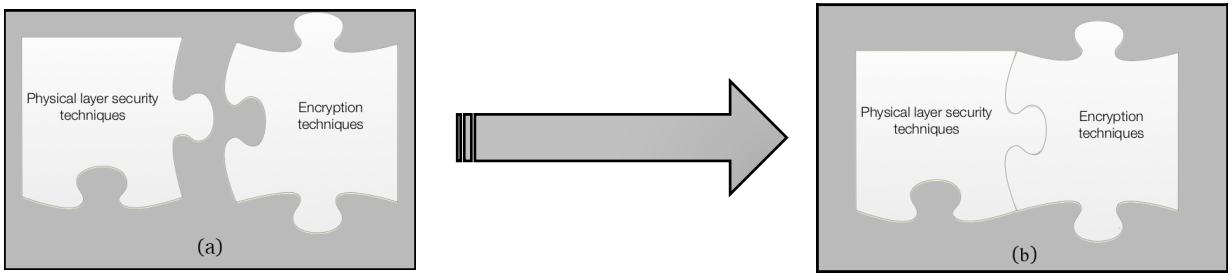


with Jammer

Summary

- Cyber-physical systems have tighter operational requirements than wireless networks
- Security is even more critical

A cross level security is will be necessary



Selected References:

- O. Cepheli, G. Karabulut Kurt, G. Dartmann, and G. Ascheid, “A Joint Optimization Scheme for Artificial Noise and Transmit Filter for Half and Full Duplex Wireless Cyber Physical Systems,” *accepted for publication* in *IEEE Transactions on Sustainable Computing.*
- G. Dartmann, E. Modarresi, M. Barhoush, N. Bajcinca, G. Karabulut Kurt, V. Lucken, E. Zhandi, G. Ascheid, *Adaptive Control in Cyber-Physical Systems: Distributed Consensus Control for Wireless Cyber-Physical Systems*, in Cyber-Physical Systems: Foundations, Principles and Applications 2017 (Elsevier).
- S. Gokceli, O. Cepheli, S. Tedik Basaran, G. Karabulut Kurt, G. Dartmann, and G. Ascheid, “How Effective is the Artificial Noise? Real-time Analysis of a PHY Security Scenario,” in *5th IEEE GLOBECOM Workshop on Trusted Communications with Physical Layer Security*, Singapore, Dec. 4-8, 2017.
- O. Cepheli, G. Dartmann, G. Karabulut Kurt, and G. Ascheid, “An Encryption Aware Physical Layer Security System,” in *IEEE International Conference on Communications (ICC) Workshop*, Paris, France, 21-25 May, 2017.


Thank you ...
Questions?
gkurt@itu.edu.tr