

2012 DHS S&T/ASD(R&E) CYBER SECURITY SBIR WORKSHOP



Homeland
Security
Science and Technology



Techniques for Physical Layer Security

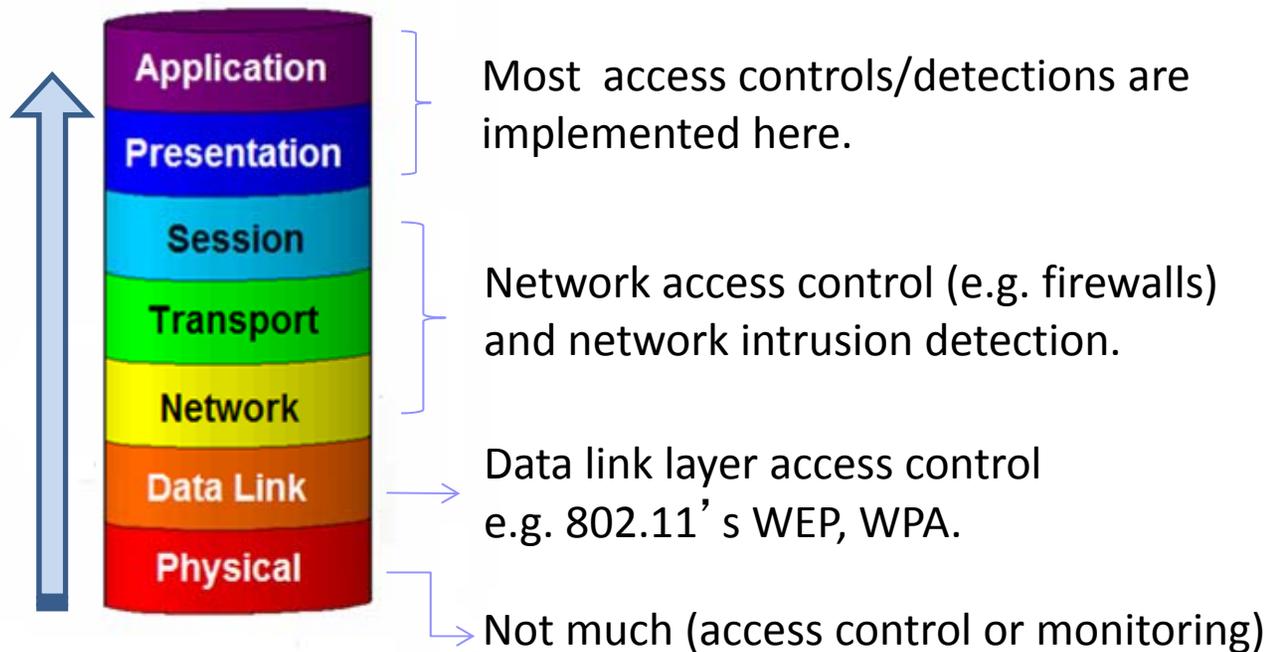
ANDRO Computational Solutions, LLC

Andrew L. Drozd

26 July 2012



Security in Network Stack

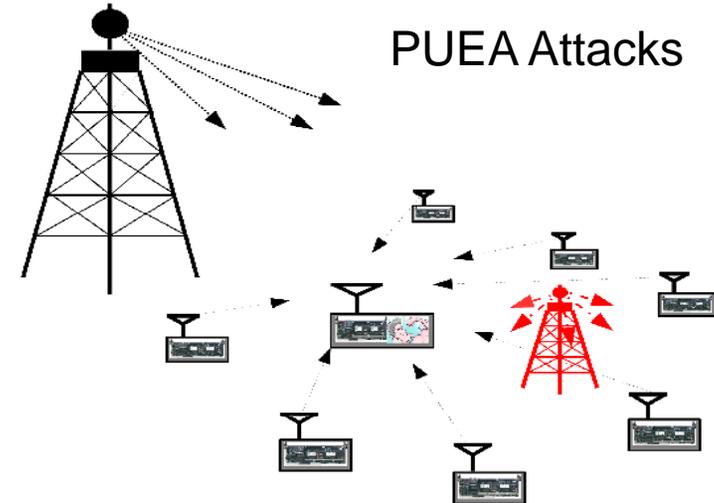
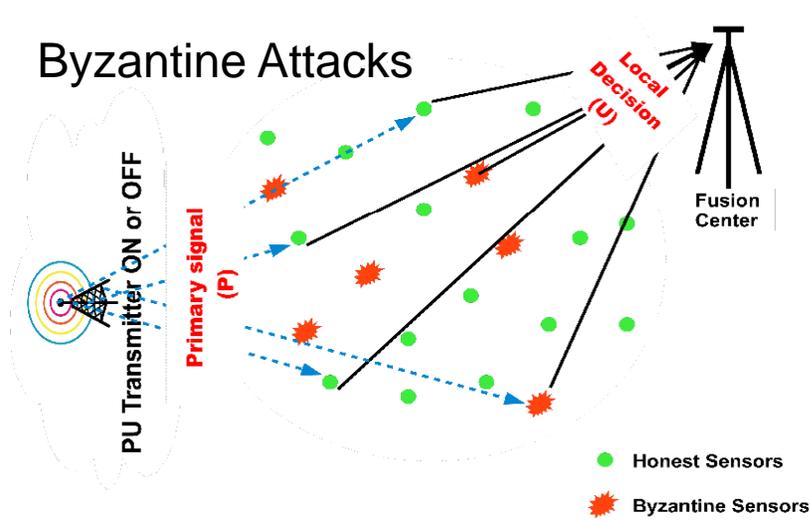


Focus: Cognitive Radio Networks (CRNs) & RF Cyber Attack.

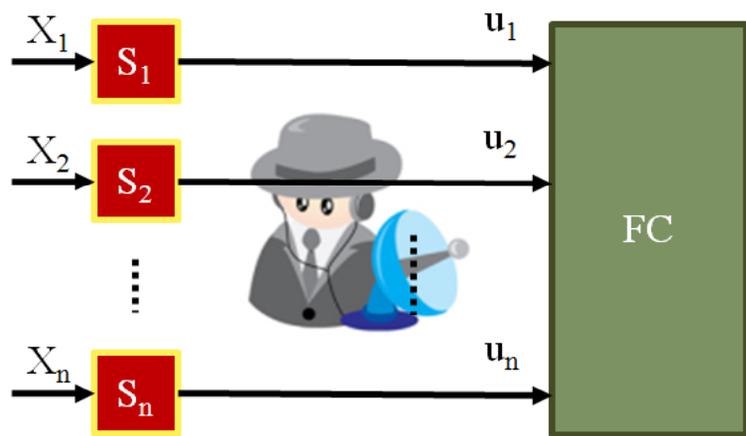
Goal: Build a secure physical layer as part of a multi-layer security approach!



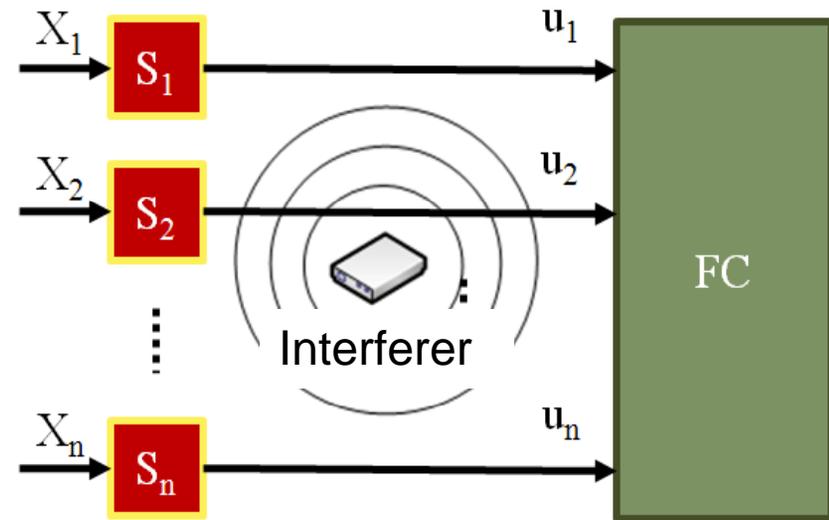
Security Issues in CRNs (RF Cyber Attack Strategies)



Eavesdropping Attacks



Interference Attacks/Disruption



Functions of CRNs

- Spectrum Sensing: Detection of white-spaces
- Spectrum Management: Capturing the best available spectrum to meet user requirements
 - Spectrum Sharing: Providing fair scheduling among coexisting CRs.
- Spectrum Mobility: Maintaining smooth handoffs while transitioning from one spectral band to another.



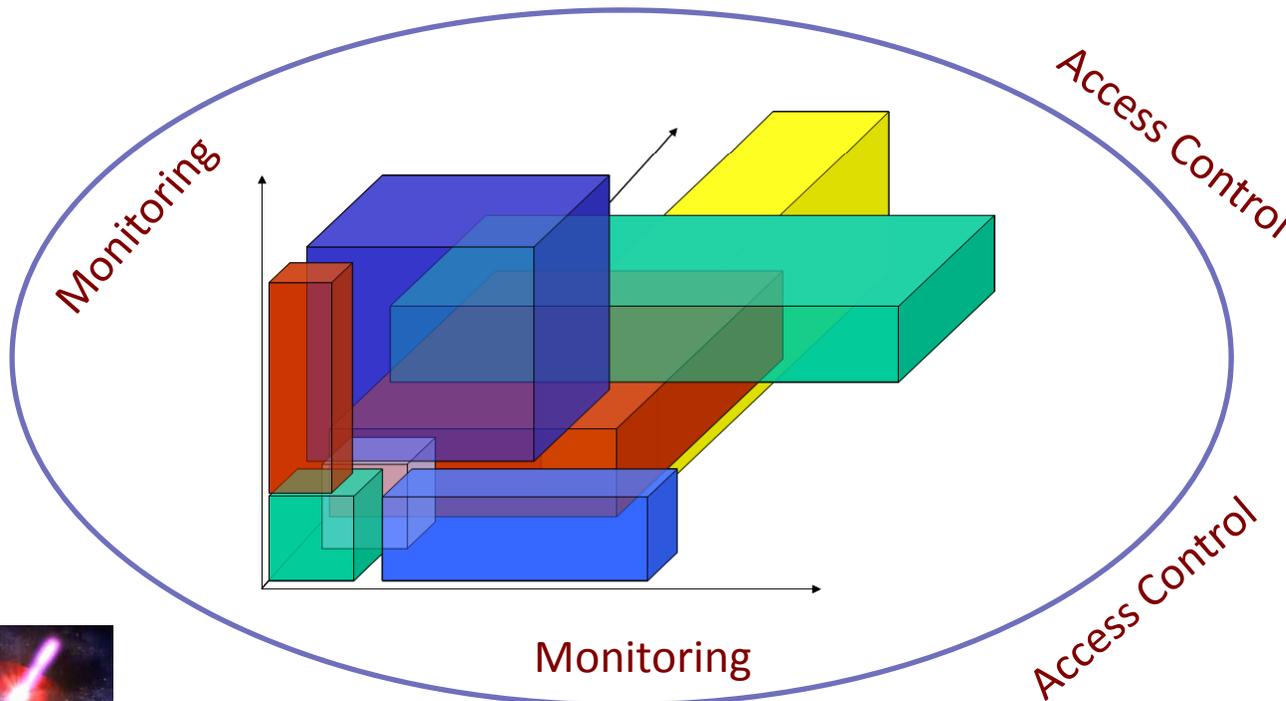
ANDRO's Approach

■ Transmission Hyperspace™ Concept

- Utilize multiple transmit resources and optimize jointly to maximize multiple communication objectives.

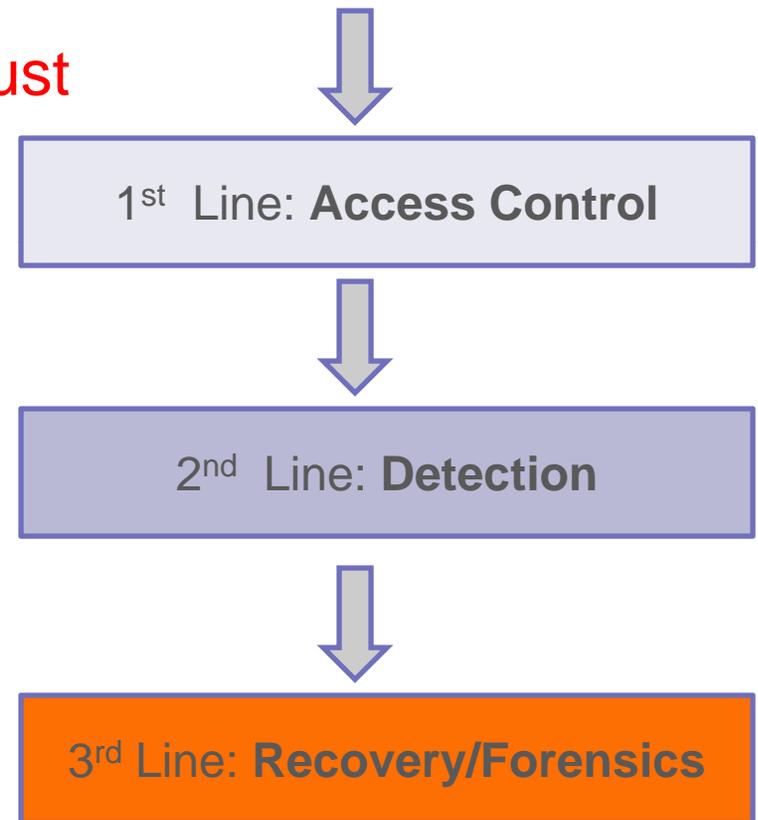
- Dynamic assignment
- Centrally managed
- On-demand
- Open access
- Priority/preemption enabled
- Decentralized local management nodes

Protected *Transmission Hyperspace™*



Capability-Based Access Control

- To use a coordinate in the *Transmission Hyperspace*, a user **must show it is authorized**.
 - Rejection at the physical layer
 - Detection at the physical layer.
- Capability-based access control (or token based)
 - Widely used in upper layers
 - Design capability for physical layer.



Cross-Layer Intrusion Detection

- What access control mechanisms are suitable for the physical layer?
 - Principles of access control
 - Issues: Coding, capability, granularity of control, isolation, privileges, etc.
- Intrusion Detection
 - Sensor deployment
 - Data fusion for intrusion detection
 - Cross-layer cooperation
- Combine network-layer intrusion detection with the information from the physical layer, such as frequency, signal power, direction of arrival, and estimated geo-location.
- Exploration of various data mining approaches, including the pattern matching approach.

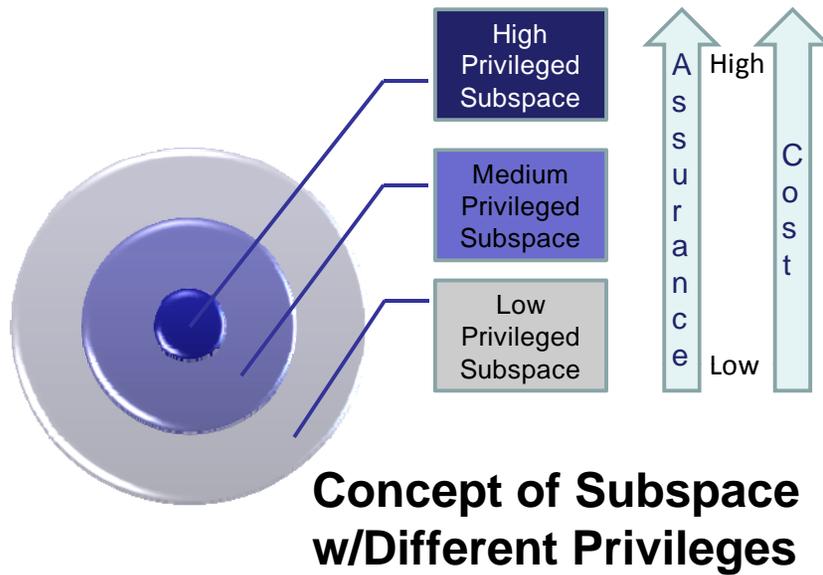


Technical Areas and Accomplishments

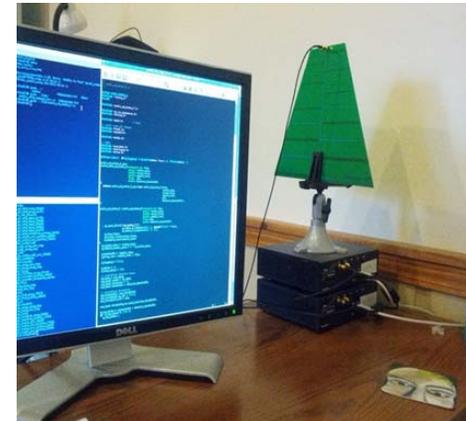
- Collaborative Spectrum Sensing in the Presence of Byzantines, Eavesdroppers and Interference Attacks
 - Carried out theoretical analyses using distributed detection, data fusion, and game theory.
 - Adaptive Spectrum Sensing by Learning Byzantines' Behavior
 - Developed Mitigation Strategies
- Detection of PUEAs using localization and data fusion
- Detection of PUEAs attacks in the presence of Byzantines
 - Game Theoretic Analyses
 - Developed Mitigation Strategies
- Physical Layer Authentication
 - Developed two novel authentication schemes
 - One based on digital modulation scheme
 - One based error correction scheme



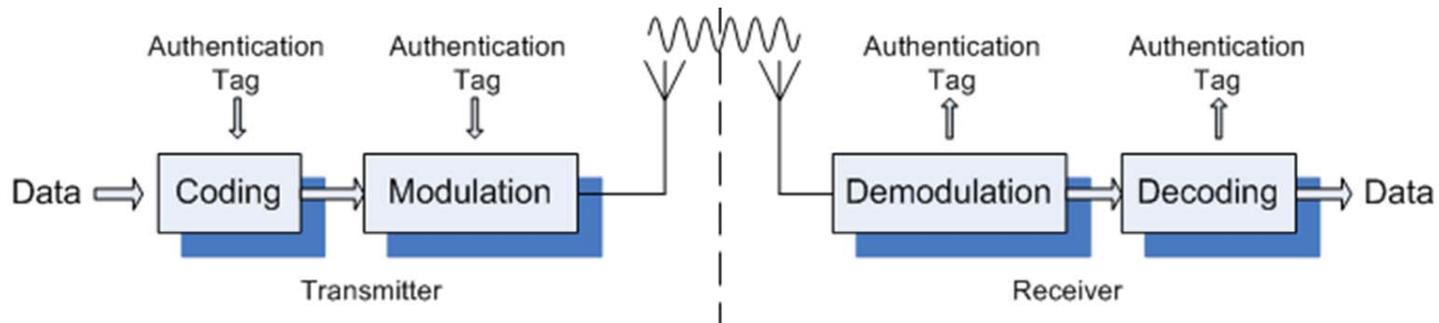
PHY Layer Assurance



GNU Radio Testbed

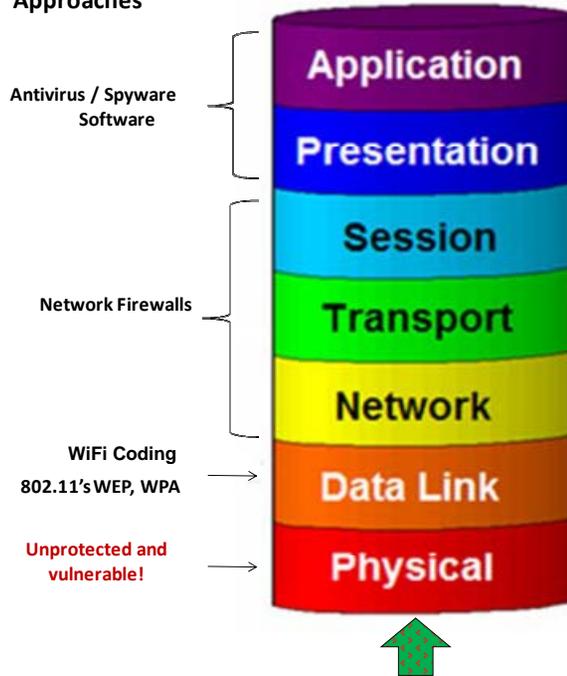


PHY Layer Authentication Coding/Tagging



Defense Strategy

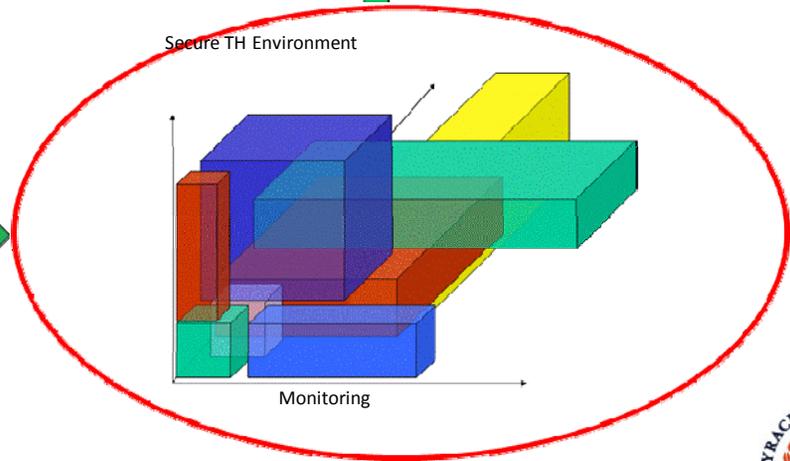
Traditional Security Approaches



Traditional Security Systems attempt to identify and defeat the attacker after they are already in the system.

Only Authorized Users enter the system

Authorized Users
& Attackers



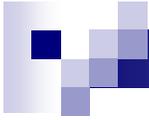
ANDRO's *CyberSE* technology blocks attackers from entering the system at the physical layer entrance!



About ANDRO

- Founded 1994.
- Core expertise:
 - Software systems development and hardware experimentation
 - Cognitive radio networks (GNU radio platforms)
 - Spectrum management & dynamic spectrum access
 - Electromagnetic Environment Effects (E³) on large systems
 - E3Expert toolkit – used by >40 organizations
 - Cyber security and spectrum exploitation
 - Multi-sensor exploitation.
- Nationally recognized expertise via IEEE, university and industry partnerships.





Thank you!

