BEYOND PKI: ENHANCED AUTHENTICATION IN VEHICULAR NETWORKS VIA MIMO

C. EMRE KOKSAL

Electrical and Computer Engineering

The Ohio State University

- OnStar (employed in GM cars):
  - Automatic crash response
  - Emergency services
  - Stolen Vehicle Assistance
  - Navigation

- Ford:
  - Navigation, weather, etc.
  - IoT - interaction with a data center

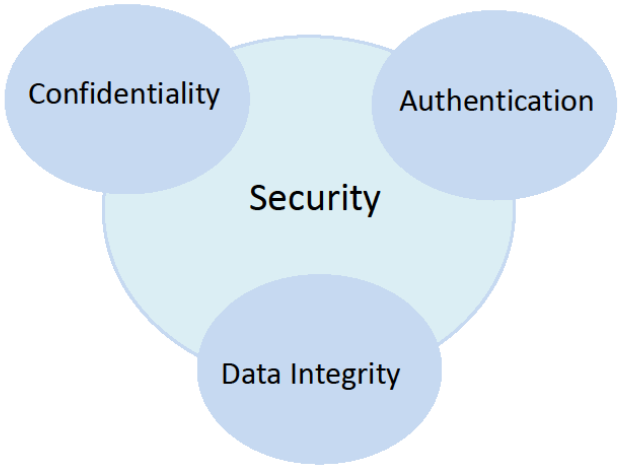
- Connections to **outside** world
  - **cellular:** 3G-4G LTE
  - **V2X:** 802.11p, DSRC
  - major application is the exchange of safety messages for intelligent transportation systems

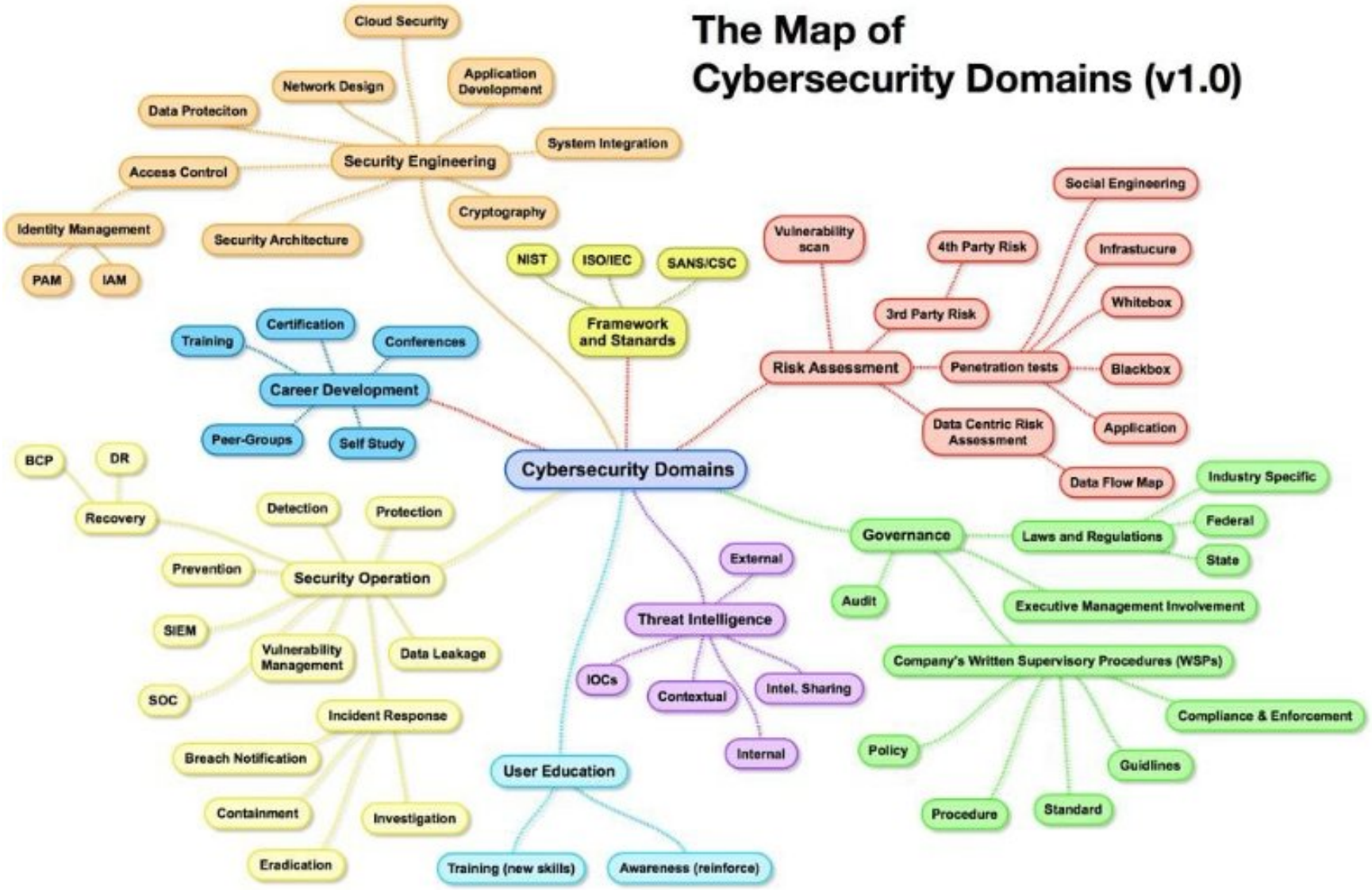
- Connections **internal** to the vehicle
  - **WiFi:** Hotspot - 50 feet in radius
  - **Bluetooth:** Multi-device support
  - major application is to replace internal wiring with wireless

CONNECTED BUT SECURE?

- Connectedness has consequences
  - control of the vehicle
  - 1.4M vehicles recalled recently

- What are the major issues in security?

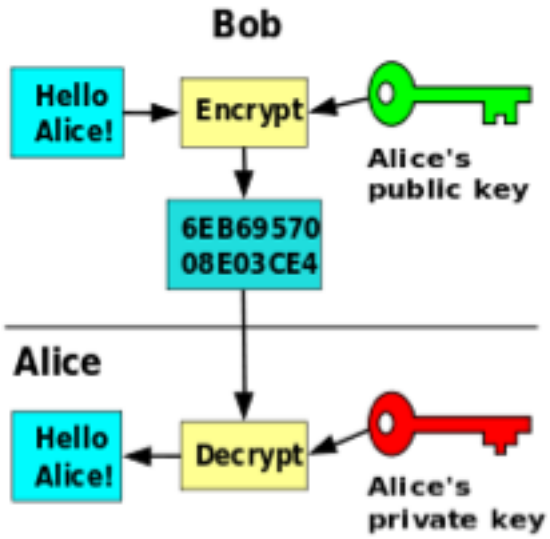



The Map of
Cybersecurity Domains (v1.0)
Cybersecurity Domains
Security Engineering
Cloud Security
Network Design
Application Development
Data Proteciton
System Integration
Access Control
Cryptography
Identity Management
Security Architecture
PAM
IAM
Framework and Stanards
NIST
ISO/IEC
SANS/CSC
Career Development
Training
Certification
Conferences
Peer-Groups
Self Study
Risk Assessment
Vulnerability scan
4th Party Risk
3rd Party Risk
Penetration tests
Social Engineering
Infrastucure
Whitebox
Blackbox
Application
Data Centric Risk Assessment
Data Flow Map
Governance
Laws and Regulations
Industry Specific
Federal
State
Audit
Executive Management Involvement
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
Policy
Guidlines
Procedure
Standard
Threat Intelligence
External
Internal
IOCs
Contextual
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforce)
Security Operation
Detection
Protection
Prevention
SIEM
Vulnerability Management
Data Leakage
SOC
Incident Response
Breach Notification
Containment
Investigation
Eradication
Recovery
BCP
DR

HOW DO WE APPROACH THESE PROBLEMS?

- Establishing connection leads to significant consequences
  - control of the vehicle
  - 1.4M vehicles recalled recently

- What are the major issues in security?
- These issues are addressed at the application layer via computational cryptography
  - **information confidentiality:** public/private key encryption
  - **authentication:** key-based, managed by trusted certificate authorities



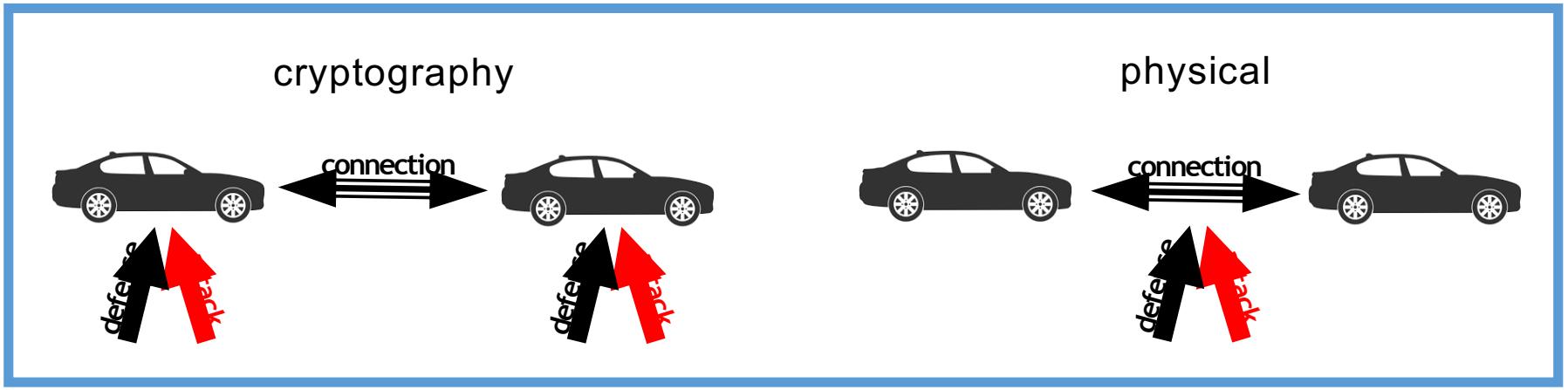
WHAT IS PHYSICAL-LAYER SECURITY?

THE OHIO STATE UNIVERSITY

- Cryptographic approaches address critical problems, avoiding “hacking” upon connection establishment

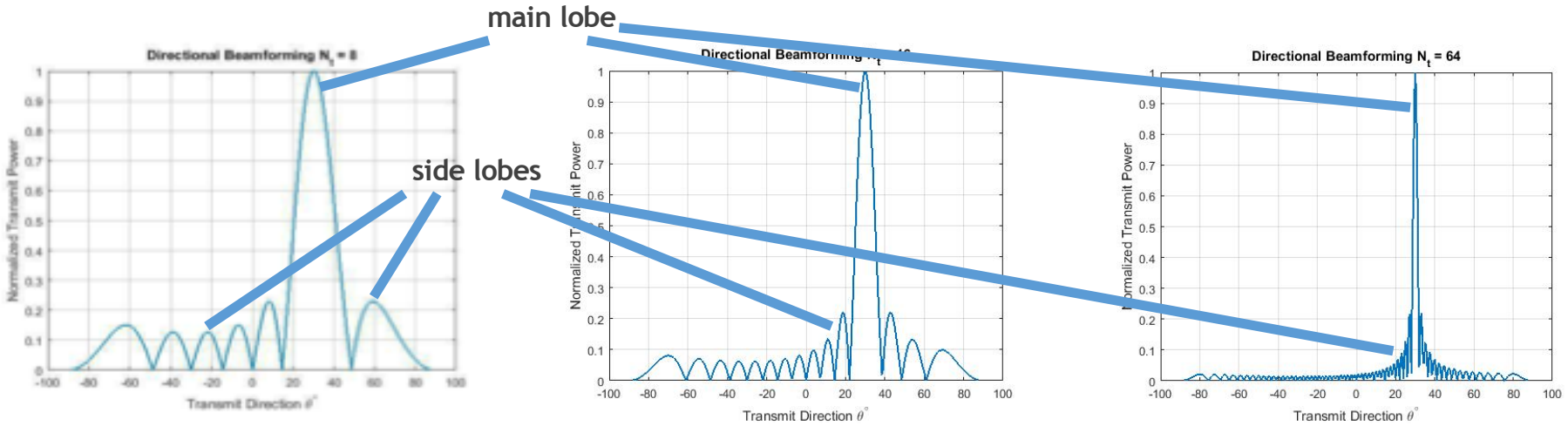
- **Question:** What about the connection itself? Is it secure?

- **Contribution:** Developing active phy-layer defense mechanisms to mitigate attacks at higher layers.



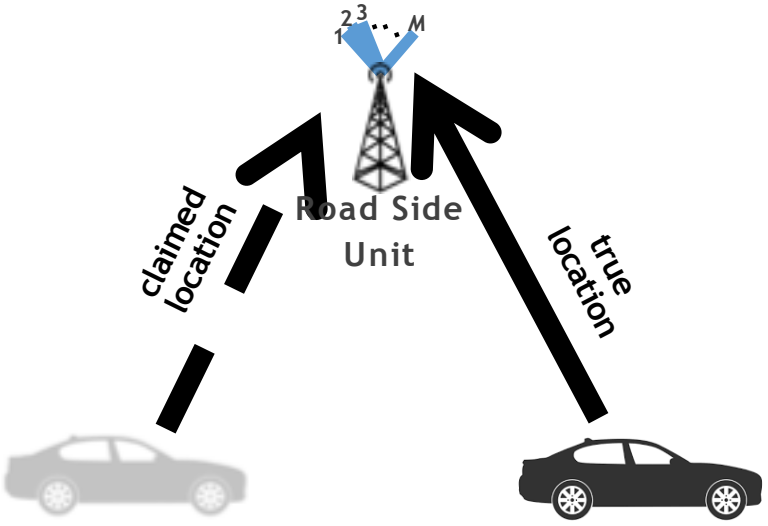
- This project develops solutions that utilize **Multiple Input Multiple Output (MIMO)** against impersonation attack with location spoofing

- MIMO channel and beamforming:
  - Unlike SISO, channel gains have directionality.
  - Receive array allows for Angle of Arrival (AoA) estimation
  - Transmit array allows for beamforming and spatial selection



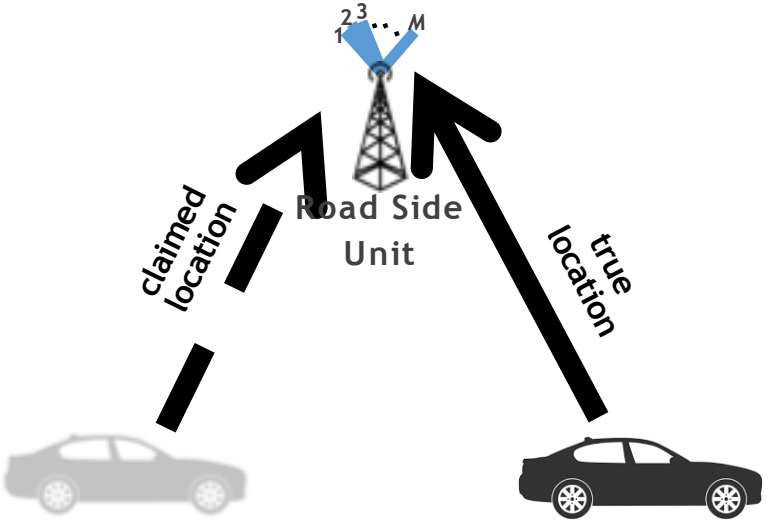
Attack:

GPS spoofing +
false message injection



Attack:

GPS spoofing +
false message injection



Defense:

- Use a multi-antenna roadside unit
- Use the array act as a **radar** as well as a data receiver
- Verify *true* location

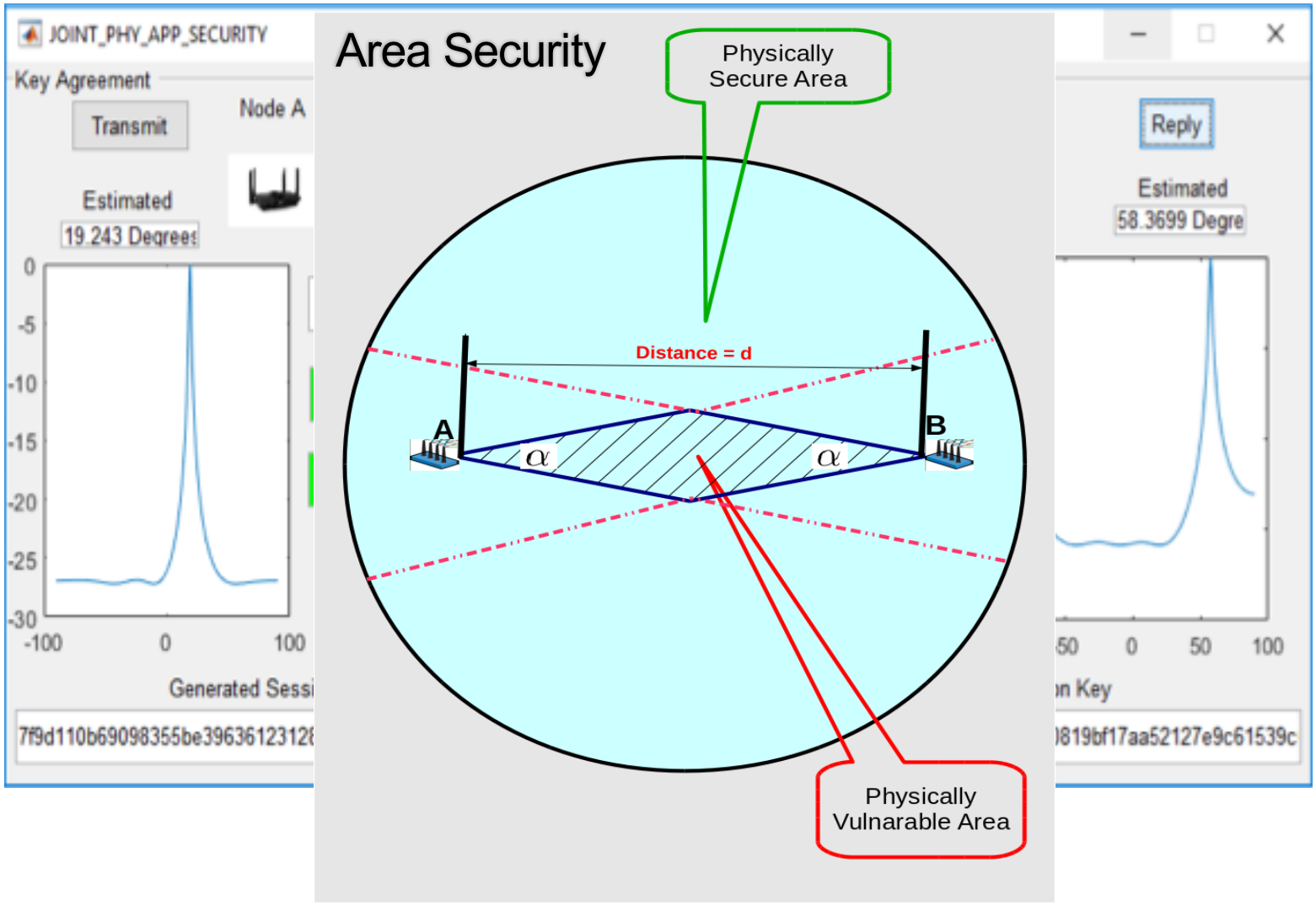
Techniques:

- The problem of deciding the authenticity of true transmission direction is a hypotheses testing problem
- The solution is Wald test statistics:

$$\frac{\left|\hat{\theta} - \theta_b\right|}{\sqrt{CRB}} \underset{<_{H0}}{\overset{\geq^{H1}}{}} \alpha$$

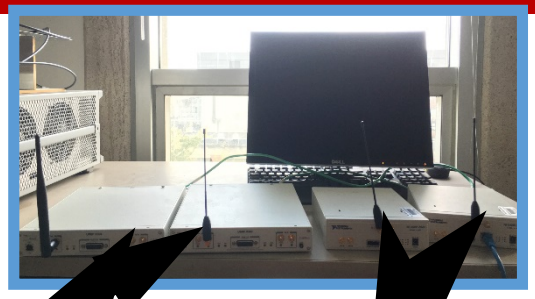
where CRB is the Cramer Rao bound for AoA estimation and α is the decision threshold

DEMONSTRATION



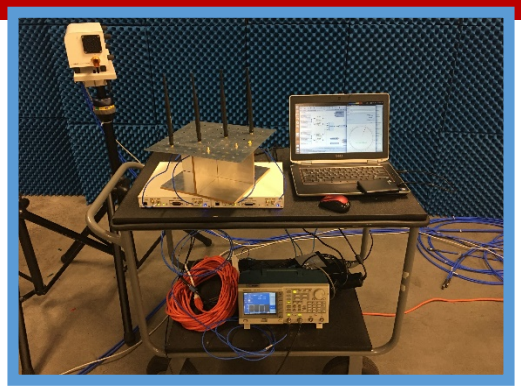
IMPLEMENTATION

THE OHIO STATE UNIVERSITY

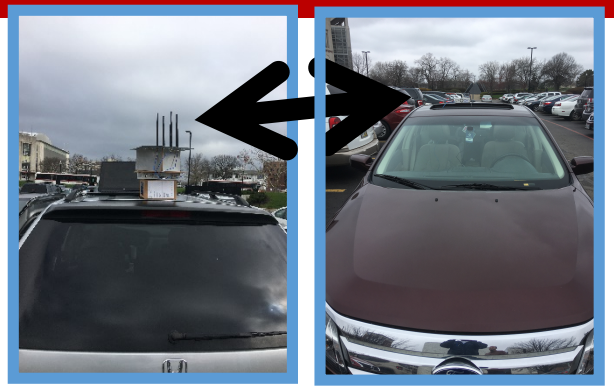


multi-channel SDRs, enabling secure 4-antenna MIMO transceiver

single-antenna transceiver units to emulate users in multiuser settings



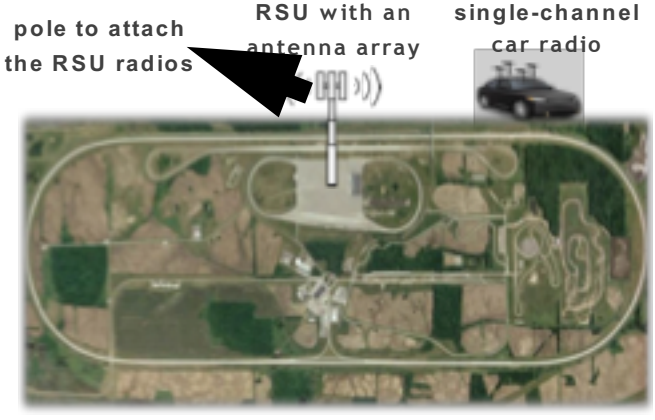
indoor setup for low-mobility security experiments



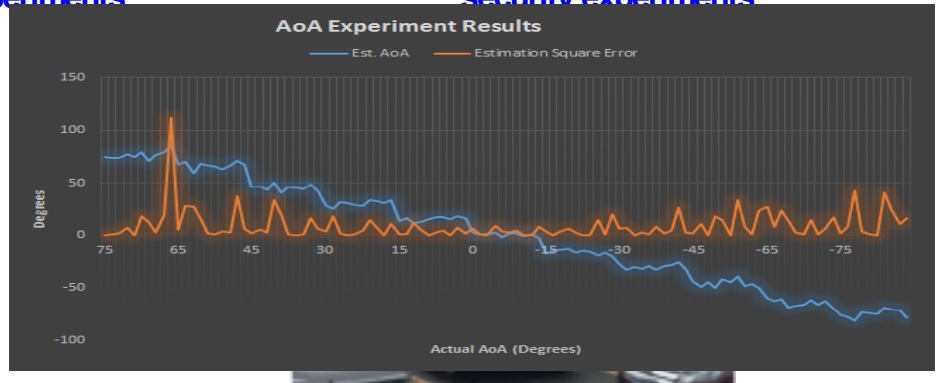
outdoor setup for low-mobility security experiments

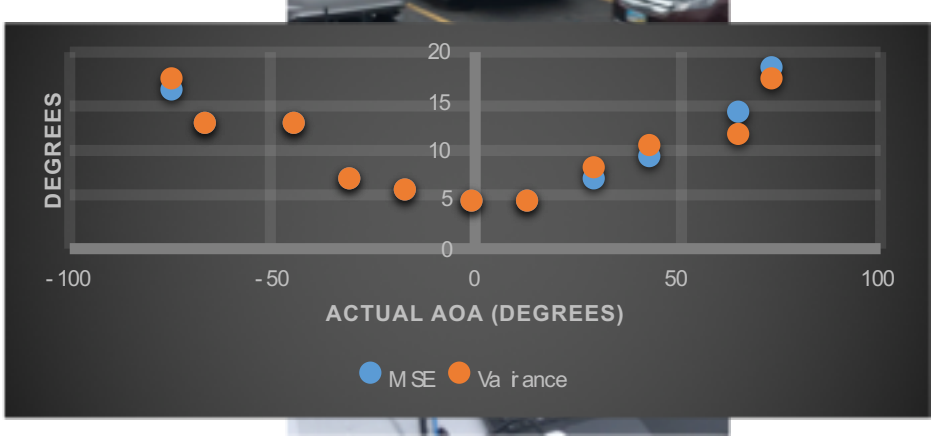
Experimental Setups

- We have implemented DSRC in full using X300 USRPs.
- We have successfully evaluated low-mobility indoor and outdoor settings.
- We have conducted high-speed experiments at TRC testing infrastructure at East Liberty, OH.



TRC test track





IMPLEMENTATION – RADIO SOFTWARE

THE OHIO STATE UNIVERSITY

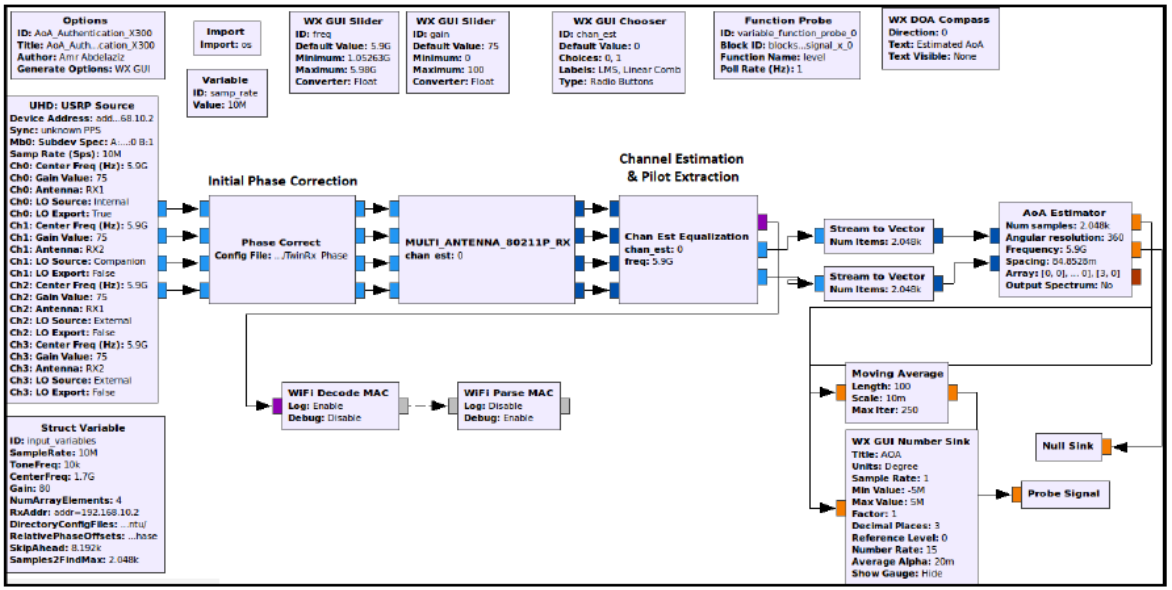
System Components

Component	Type	Role in Experiment
CPU	Intel Core i5-3200 CPU 3.40GHz × 2	Hosts for signal processing
Operating System	Ubuntu 16.04 LTS, 64 bits	—
GNU Radio	Version 3.7.10	Signal Processing Environment
USRP	Ettus X300 × 2	Transmitter and Receiver
RF Daughter Board	Ettus TwinRx × 2	Installed in one of the X300 USRP to form four channel Receiver
RF Daughter Board	Ettus CBX	Installed in one of the X300 USRP to form a single channel Transmitter
RF Antenna	VERT2450 × 5	—

IEEE 802.11p Waveform Parameters

Parameter	Typical Value
Center Frequency	5.9 GHz
Bandwidth	10 MHz
FFT Length	64
Occupied Subcarrires	52
Data Subcarriers	48
Pilot Subcarriers	4
Beacon Size	200 Bytes
Beacon Interval	100 ms
Modulation	BPSK
Encoding	Convolutional
Encoding Rate	1/2
Transmit Power	+20 dBm
Array Configuration	ULA
Array Spacing	25 mm

GNU Radio Setup Block Diagram

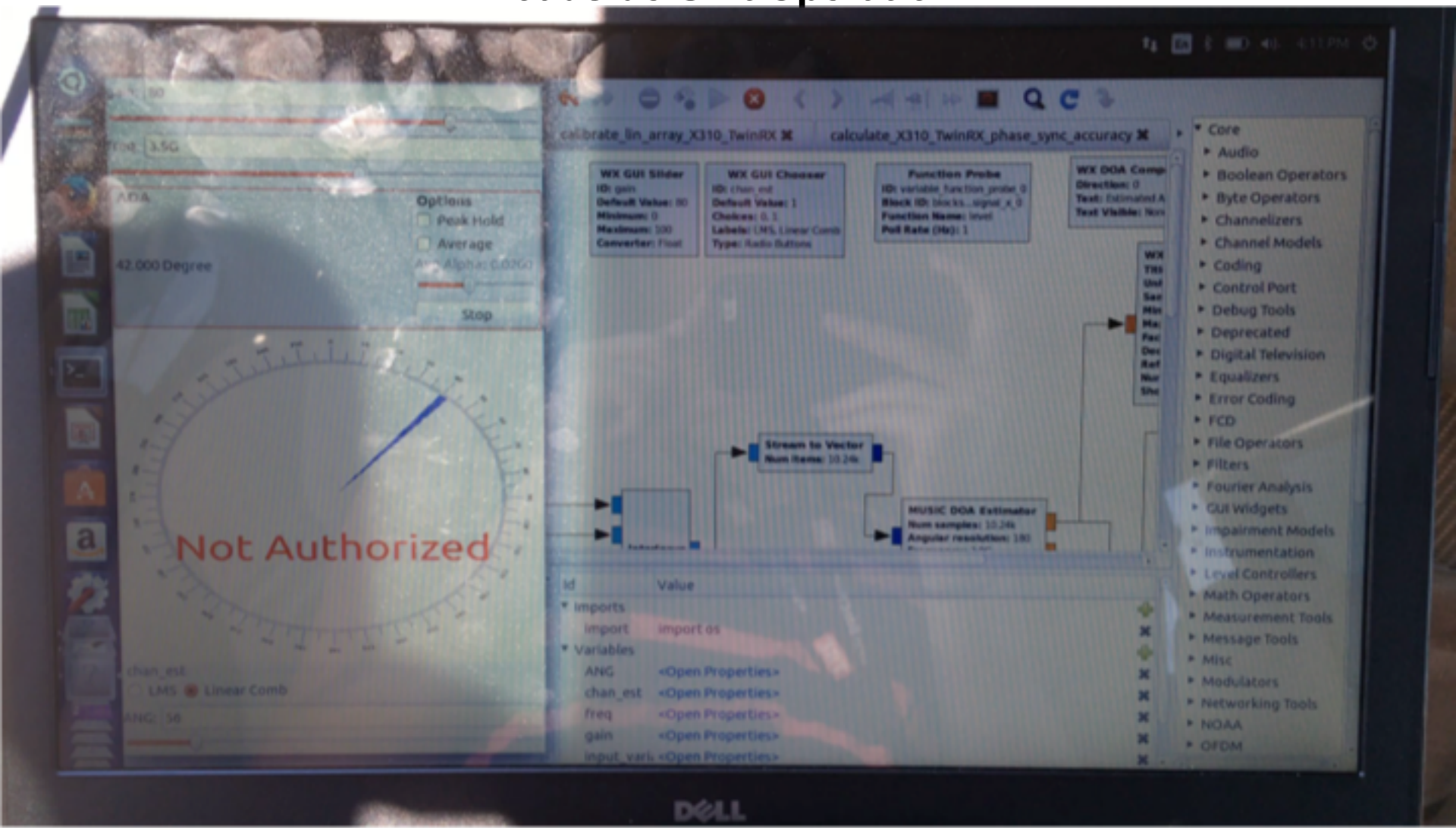


- **Transmitter:**
  - We have implemented a single-antenna DSRC beacon transmitter over a 2910 USRP
  - Transmits a beacon every 100ms

- **Access point:**
  - We have implemented a 4-channel DSRC receiver over two X300 USRPs
  - We have realized both ML and MUSIC AoA estimators over DSRC beacons
  - Unlike MUSIC, ML estimator takes the advantage of the known preamble/pilot sequence. We have shown that ML estimator is resilient to jamming attacks

Transmitter Operation

Roadside Unit Operation



SUMMARY OF OUR CONTRIBUTION AND ACTIVITIES

THE OHIO STATE UNIVERSITY

- Many attacks on the Vehicular Networking Systems can be addressed at the Physical Layer
- We developed new wireless defense mechanisms that exploit MIMO at RSUs to address attacks at Physical Layer as well as Higher Layers
- Our technique directly address the insider attack on PKI and enhance its security.
- News coverage:

R and D Magazine – "*Could your car be hacked?*"

Boston.com – "Why your car might be the latest target for hackers"

Dayton Daily News – "*The newest frontier for hackers: your car*"

Newswise – "*Cybersecurity for your car*"

ACM Tech News – ``*Cybersecurity for your car*"

SUMMARY OF OUR CONTRIBUTION AND ACTIVITIES

THE OHIO STATE UNIVERSITY

- Many attacks on the Vehicular Networking Systems can be addressed at the Physical Layer
- We developed new wireless defense mechanisms that exploit MIMO at RSUs to address attacks at Physical Layer as well as Higher Layers
- Our technique directly address the insider attack on PKI and enhance its security.
- Testified on Capitol Hill:

SUMMARY OF OUR CONTRIBUTION AND ACTIVITIES

THE OHIO STATE UNIVERSITY

- Many attacks on the Vehicular Networking Systems can be addressed at the Physical Layer
- We developed new wireless defense mechanisms that exploit MIMO at RSUs to address attacks at Physical Layer as well as Higher Layers
- Our technique directly address the insider attack on PKI and enhance its security.
- Papers:
  1. Gungor O. and Koksal C. E., "On the Basic Limits of RF-Fingerprint Based Authentication," ***IEEE Transactions on Information Theory**, Aug. 2016*
  2. Basciftci O., Koksal C. E., Ashikmin A., "Physical-Layer Security in Massive MIMO," ***IEEE Transactions on Information Theory** – revised and resubmitted*
  3. Abdelaziz A. and Koksal C. E, "Fundamental Limits of Covert Communication over MIMO AWGN Channel," submitted to ***IEEE Transactions on Information Theory***
  4. Abdelaziz A., Koksal C. E., Barickman F., Burton R., Martin J., and Weston J. *"*Mitigating Location Spoofing in Vehicular Networks using Angle of Arrival: Theory and Practice,*" submitted to **IEEE Transactions on Vehicular Technology***
  5. Abdelaziz A., Elbayoumy A., Koksal C. E, and El Gamal H., "*Delay Limited and Ergodic Secrecy Capacity of MIMO Wiretap Channel," submitted to **IEEE Journal on Selected Areas in Communication***
  6. Abdelaziz A. and Koksal C. E., "Fundamental Limits of Covert Communication over MIMO AWGN Channel," ***IEEE CNS 2017***
  7. Abdelaziz A., Elbayoumy A., Koksal C. E, and El Gamal H., "On the Compound MIMO Wiretap Channel with Mean Feedback," ***IEEE ISIT 2017***
  8. Abdelaziz A., Koksal C. E, and Burton R., "Message Authentication and Secret Key Agreement in VANETs Via Angle of Arrival," ***IEEE VNC 2016***
  9. Abdelaziz A., Koksal C. E, and El Gamal H., "On the Security of Angle of Arrival Estimation," ***IEEE CNS 2016***

THE OHIO STATE UNIVERSITY

CONTACT

car.osu.edu

C. Emre Koksal
Professor
koksal.2@osu.edu
614-598-1466

Correct decision probability as a function of SNR for different values of α. (a) Ricean k-factor of 10. (b) Ricean k-factor of 10.

False Alarm probability as a function of SNR for different values of α. Claimed and true angles are 2.5° apart. (a) Ricean k-factor of 10. (b) Ricean k-factor of 10.