BEYOND PKI: ENHANCED AUTHENTICATION IN VEHICULAR NETWORKS VIA MIMO

C. EMRE KOKSAL

Electrical and Computer Engineering
The Ohio State University
CONNECTED VEHICLES

- 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?
CONNECTED BUT SECURE?

The Map of Cybersecurity Domains (v1.0)
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?

• 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
WHAT DOES MIMO BRING ON THE TABLE?

- **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.

![Diagram showing main lobe and side lobes in MIMO systems.](image-url)
PROBLEM

Attack:

GPS spoofing + false message injection

 claimed location

true location

Road Side Unit

1 2 3 ... M
**SOLUTION**

**Attack:**

GPS spoofing + false message injection

**Road Side Unit**

**Claimed location**

**True location**

**Road Side Unit**

**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:

\[
\frac{|\hat{\theta} - \theta_b|}{\sqrt{\text{CRB}}} \geq H_1 \quad \alpha
\]

where CRB is the Cramer Rao bound for AoA estimation and \( \alpha \) is the decision threshold
Area Security

- Physically Secure Area
- Physically Vulnerable Area

Distance = d
**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.
IMPLEMENTATION – RADIO SOFTWARE

System Components

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

IEEE 802.11p Waveform Parameters

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

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
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”
• 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:
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:
3. Abdelaziz A. and Koksal C. E. “Fundamental Limits of Covert Communication over MIMO AWGN Channel,” submitted to *IEEE Transactions on Information Theory*
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 $\alpha$. (a) Ricean $k$ factor of 10. (b) Ricean $k$ factor of 10.

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