Keeping Your Eyes Peeled: Sensing-Driven Feedback-Computing for Network Security

Bruce DeBruhl
PhD Candidate, ECE
Wireless Network & System Security Group
Carnegie Mellon University

November 14, 2014
CyLab Partners' Conference
What does it mean to be sensor-driven?

What do we do with the massive amount of data available?

We have new data that recently did not exist.

We have new data scales that recently did not exist.
Agent-Based Feedback-Computing

Network

Feedback & Observation

System Agent

Optimize & Adapt

Device Agent

Feedback & Observation

Infer / Learn

Analyze Costs + Benefits

Carnegie Mellon University
Sensor-Driven Systems

Vehicle Platooning

Inference-Based Adaptive Jamming
Traffic is Terrible

People Drive Horrible
Decreasing Traffic

- Increase the number of roads
  - Not possible
- Increase current road capacity
  - Not possible
- Increase the density of traffic
  - People drive terrible
  - .5s reaction speed
  - 2s recommended following speed
  - Actual following speed is much less
Platooning with DSRC

- Radar alone does not solve the problem
  - Brake lag can be considerable
- DSRC - Dedicated Short Range Communication

I'm slowing down!
I'm slowing down!
I'm slowing down!
Platooning with DSRC
Emergency Stopping
Platooning Attacks

[Diagram showing the interactions between DSRC, GPS, Controller, and Environment]
Suicide Attack
Attack Detection

Car 3’s model of Car 2 -> \( \hat{a}_2 \) -> Misbehavior Detector -> Attack

\( \bar{a}_1 \) -> \( \hat{a}_2 \) -> \( a_2 \) -> \( \bar{a}_2 \)

That's not right....

I'm speeding up!

I'm slowing down!

Carnegie Mellon University
Attack Detection Results

Desired Acceleration Based Misbehavior Detection

- No Attack
- Decreased Headway
- Accel Misreport
- No radar
- Added Signal

Carnegie Mellon University
Optimal Platooning Attack

• What is the worse case scenario

• Two scenarios
  – Microscopic
  – Macroscopic

Can I cause an accident without being involved?

Where do I cause traffic to create the biggest delays?
Microscopic Attack
Jamming

- Conceptually, jamming is a physical layer denial-of-service attack that aims to prevent wireless communication between parties.
Jamming Strategies

Time Domain

Link Traffic

\[
P_k \quad P_k \quad P_k \quad P_k \quad P
\]

- **Constant**
- **Random**
- **Periodic**
- **Reactive**
Jamming Strategies

Frequency Domain

Link Traffic

Broadband

Single Ch.

Single Sub-Ch.

Multiple Sub-Ch.
Modern SDR capabilities
+
Broad range in jamming attack strategies
=
New jamming attacks!
Adaptive Jamming

- More generally, the attacker can observe the opponent and tweak a number of parameters to meet a specific goal.
10%-PDR Adaptive Jamming
Anti-Jamming

• Too many options and parameters to be able to design a single strong defense

• Instead, design a family of specialized defenses, and learn which to use adaptively

• Take advantage of and build upon classical anti-jamming techniques
A Specialized Attack

- We designed an efficient and stealthy jamming signal to target 802.15.4
  - Time: periodic, period $\sim kT_s$, duty cycle $\sim 2$-10%
  - Frequency: single tone located randomly in each 5MHz channel
A Specialized Defense

Given that an attack has been detected at a known frequency, a software filter can eliminate the jamming signal while retaining enough valid signal to decode.
Adaptive Anti-Jam Filtering

Bob finds $PDR > \delta$

Of course, Mallory can adapt the attack as well...
Implementation
Some Results

- Jamming Frequency
- Time (seconds)
- Filter Number
- PDR
Jamming Games

What if both the attacker and defender are freely adapting in response to each other?
Full Knowledge Game

- Our game is...
  - Round based - players keep a strategy for a determined period known as a round
  - Full knowledge - Players know the energy levels and previous plays of both players
  - Solvable - optimal mixed strategies exist
  - Zero-sum - When one player wins the other loses
Full Knowledge Game
Simulation

- Utility is based on defender's throughput
- Use values from an SDR
Interesting Result - Bullying
Sensor-Driven Systems

Vehicle Platooning

Inference-Based Adaptive Jamming
Questions?

Contact:

debruhl@cmu.edu
tague@cmu.edu