Security and Privacy at WINLAB

Wade Trappe

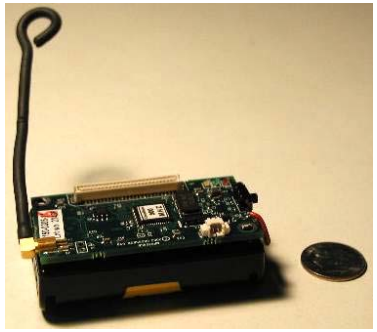
WINLAB
WIRELESS INFORMATION NETWORK LABORATORY

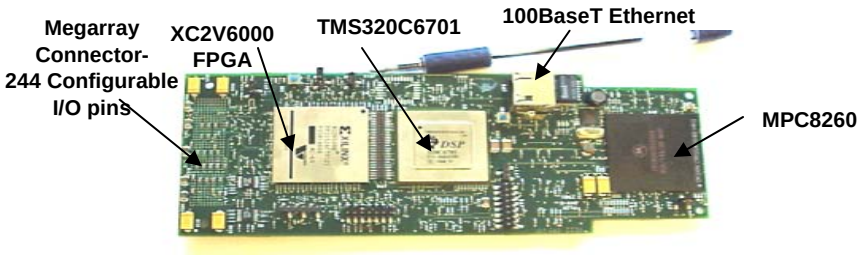
Overview and Lead-In…

- Security has been one of the great detractors for wireless technologies
- WINLAB's security initiatives:
  - Non-traditional
  - Leverage existing strengths
  - Wireless networks are **different** from standard networks!
- Today, think about the questions:
  - Should we reevaluate the definition of security?
  - Is there more to protect than e-commerce?
  - Is there more to security than cryptography and network security?
  - Should security be considered separately from the network/system?
  - What benefits are there if we integrate security into the network?
  - How private do we really want our lives?

Through the Looking Glass, the Wireless World

- Key properties and differentiators that make wireless security **different**
  - Physical Layer
  - Ubiquity
  - Mobility
  - Resource adaptability
  - Location
  - Affordability
  - Platform heterogeneity
  - Programmability
- Many threats are easier to conduct against wireless networks:
  - Eavesdropping
  - Spoofing/Masquerade
  - Denial of Service





WINLAB's Security and Privacy Initiatives

- WINLAB has a grown a large and unique initiative in wireless security and privacy:
  - Faculty Members:
    - *Originally: Wade Trappe, Yanyong Zhang, Marco Gruteser*
    - *New Additions: Larry Greenstein, Narayan Mandayam, Roy Yates, Predrag Spasojevic*
  - Many Students!!!
  - Collaboration:
    - *NICT Japan: Security for Future Wireless Networks (B3G)*
    - *CMU/UIUC/Intel: Secure Routing for MANETs and Mesh Networks*
    - *Interdigital: Physical Layer Security*
  - Our Strategy:
    - *Security at many different layers*
    - *Blend theory and systems investigation*
    - *Work with industry*

WINLAB's Security Research Areas and Tools

Focus Areas

- Wireless Network Security
- Sensor Network Security
- Privacy in Wireless Networks
- MANET Security
- Securing Vehicular Networks

Research Initiatives

- Physical Layer Security
- Wireless and Sensor Privacy
- Availability (Jamming/Flooding)
- Location-centric Security
- Secure Routing
- Securing Wireless Resources
- Privacy in Vehicular Networks
- Malcode in Wireless Networks

Supporting Tools

Cryptography

Network Security Protocols

Layer 1 and Layer 2 Methods

Statistical Analysis

Testbeds and Simulations

Other Mathematical Tools

WINLAB's Security Success Stories

- Over the past two years there have been several notable success stories
- Funding:
  - NSF NeTS-NOSS: PARIS: Privacy Augmented Relaying of Information from Sensors
  - NSF NeTS-ProWIN: Fingerprints in the Ether: Exploiting the Radio Channel to Enhance Wireless Security
  - NSF CT-ISG: Multi-Layer Anonymity Techniques for Time-Series Location Information in Wireless Systems
  - DARPA SEVILLE: Security Via Lower Layer Enforcements (Joint with Interdigital)
- Some Key Research Results:
  - Jamming Attacks and Defense: Mobihoc05, Sensys07, IPSN07
  - Physical Layer Security: WiSe07, Allerton07, ISIT07, Globecom07
  - Location-oriented Security: SECON06, SASN06, Infocom07, SECON07
  - Privacy: SecureComm05, ICDCS05, ICDCS07
  - Secure Routing (SEAR): Only viable secure AODV protocol (under review)
- A Growing Alumni:
  - Wenyuan Xu has tenure-track faculty positions
  - Ruoheng Liu: Post-Doc under Vince Poor (Princeton)
  - Industrial appointments: Qing Li (Hitachi), Pandurang Kamat (Ask.com)

Roadmap for Today

Morning

- Fingerprints in the Ether
- Secrecy via Multi-Antenna
- Multi-Antenna Secret Broadcasts
- Service Discovery and Ident.
- Attack Detection in Localization
- LGI: Establishing Order

- Lunch!!!
- Demonstrations

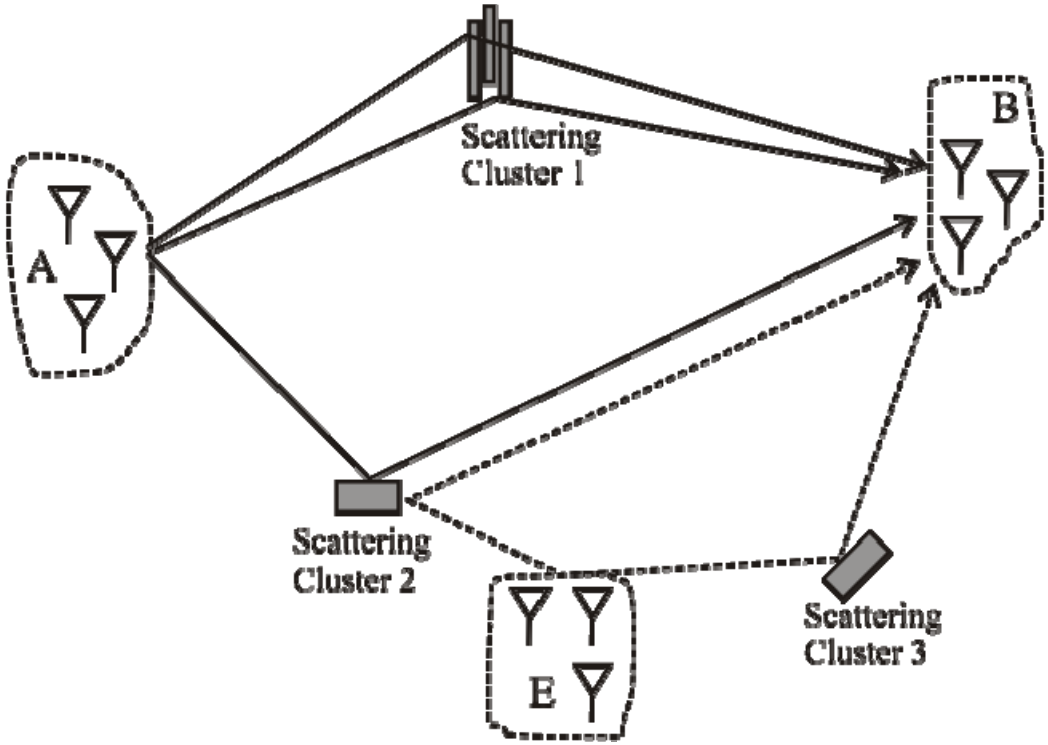
Afternoon

- Formalizing Trust
- Privacy in Vehicular Networks
- Temporal Privacy
- TRIESTE: CogRadio Security
- Spatio Temporal Access Control
- Channel Surfing: Anti-Jamming
- Panel: Wireless Security

Starting with PHY-layer Security

- Wireless networks have repeatedly been a source of “bad news” when it comes to security
- Although conventional cryptographic and network security techniques are essential to securing wireless networks, they are not a complete solution
- We believe lower-layer information associated with the wireless channel can be used to enhance wireless security
  - The typical wireless multipath transmit-receive channel is *frequency-selective* (or in the time domain, *dispersive*) in a way that is *location-specific* with rapid *decorrelation* properties
  - The channel response between a transmitter and a receiver can be a unique, shared, non-predictable source of *secret* information
- This secret information is a “fingerprint in the ether” we propose to use to develop cross-layer *Authentication Services* and *Confidentiality Services*

Alice, Bob and Eve get Physical !!!

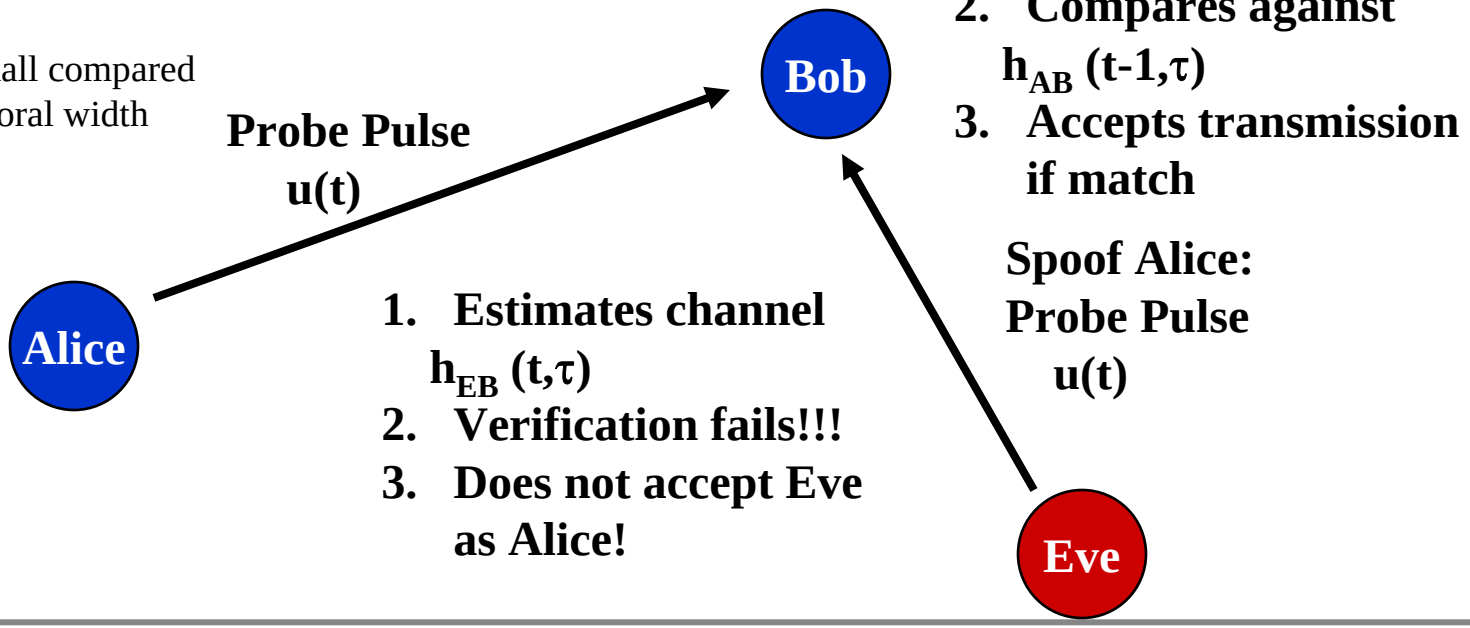


- All security problems need actors:
  - Alice (A): The transmitter
  - Bob (B): The receiver
  - Eve (E): The evil adversary
- Their roles depend on the type of security objective we have

PHY-Layer: Authentication

- Authentication in the PHY-sense is about verifying a transmission came from a particular transmitter– useful for spoofing detection!!!
- Wireless devices can authenticate themselves based upon
  - Ability to produce an appropriate received signal/channel estimate at the recipient
  - Location information can be extracted to authenticate a transmitter relative to its previous location

Bandwidth W of Probe Pulse is critical!
1/W must be small compared to channel temporal width

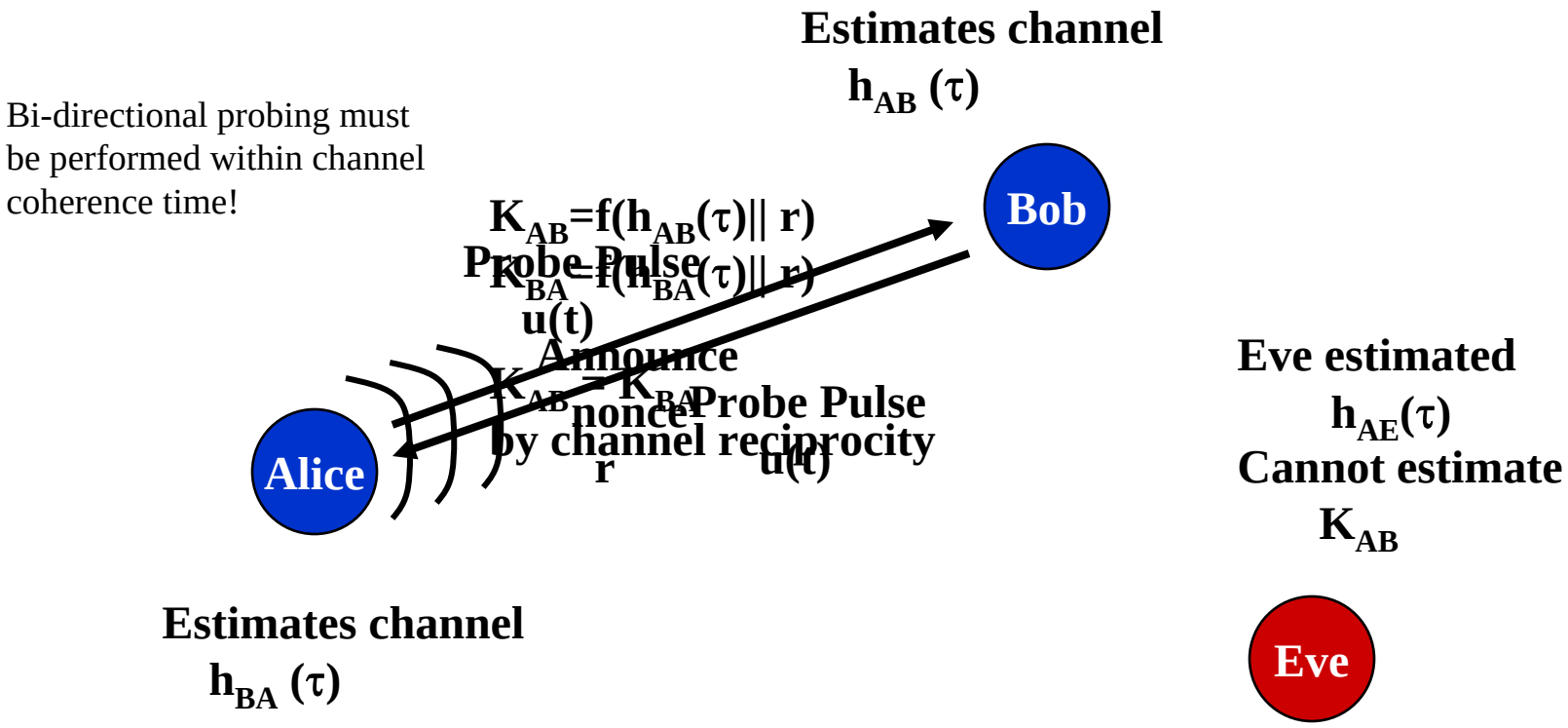


PHY-Layer Confidentiality: Types

- We also would like to use the PHY-Layer to support confidential communications
  - For higher-rate secret communications, we suggest that the PHY-layer be used to form higher-layer cryptographic keys
- There are two types of PHY-Layer Confidentiality Services:
  - Extraction: Use the channel estimate itself to form key bits
  - Dissemination: Use channel variations to opportunistically, and secretly convey communications/key bits…
- Note: There is a distinction between secret communication and LPI/LPD communications!
- Today, you will hear two talks that focus on "Secret Dissemination" using MIMO systems

Fingerprints: Confidentiality

- The uniqueness and non-predictability of the channel can be used to establish a shared secret key for encryption services



- Practical issues arise: quantization of channel estimates, channel reciprocity, temporal coherence, fast channel estimation.

Without Further Delay…
Onto the Excitement…