Security in Wireless Ecosystems

Wade Trappe
Wireless Ecosystems represent the next generation of pervasive computing systems

- Integrating the physical world with the Internet
  - Ability to view, search and interact with the physical world
  - Pervasively deployed mobile and embedded computing devices

- A set of evolving "wireless ecosystems" emerge
  - Weaving information into the fabric of human lives

- Characteristics of pervasive ecosystems
  - 10s of billions of wireless devices connected to the global network
  - Scale is 2 orders of magnitude greater than today’s internet
  - Licensed and Unlicensed Spectrum
  - New challenges in enabling technologies, system architecture and human-centric design

- Communications/Networking with Cognitive Radios
  - Design of hierarchical, distributed, decentralized and adaptive protocols
  - Spectrum Coexistence in dense wireless networks
  - Efficient integration with the future internet

- Security and Privacy
  - Personal nature of use of technologies
  - Ubiquitous nature of use of technologies
Wireless Ecosystems represent the next generation of pervasive computing systems

“Human in the Loop”

Application Management & Control Software

Control Module

Autonomous software agents

Cognitive Intelligence Module

Global Pervasive Network (Future Internet)

Content & Location Aware Routers

Protocol module

To Actuators

Smart Public Space

Autonomous Wireless Clusters ("ecosystems")

From Sensors

Hospital with Embedded Monitoring

Virtualized physical world object

Physical World with Embedded Wireless

Network Connectivity & Computation

Vehicles with Sensors & Wireless

Multiple radio standards, Cognitive radios

Content & Location Aware Routers

Computation & Storage

Rutgers

WINLAB
Wireless Ecosystems are a multi-dimensional activity at WINLAB

"Wireless Ecosystems"

- **Platforms/Prototypes**
  - WiNC2R Programmable agile radios
  - GNU platforms
  - Cognitive Radio Network Testbeds

- **Cooperative Communications**
  - Information & Coding Theory
  - Statistical Signal Processing
  - Game Theory/Microeconomics
  - MAC & Networking Algorithms

- **Spectrum Policy**
  - Economics
  - Regulation
  - Legal
  - Business
**WINLAB has a holistic approach to addressing security issues in emerging wireless systems**

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Wireless is easy to sniff. We still need encryption services and key management. Key freshness is an issue.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Wireless hardware/equipment need to be safe from modification. Data/control info should not be modified before or during transit.</td>
</tr>
<tr>
<td>Forensics</td>
<td>Wireless networks will be the platform of choice for attacks. Should the network keep track of forensic evidence?</td>
</tr>
<tr>
<td>Privacy</td>
<td>Perpetual connectivity can mean constant surveillance! With snooping one can monitor mobility and handoffs between networks.</td>
</tr>
<tr>
<td>Location</td>
<td>Location is a new form of information provided by wireless systems that will facilitate new services. Location information needs to be trusted.</td>
</tr>
<tr>
<td>Intrusion</td>
<td>The pervasiveness of the wireless networks should not mean that just anyone can participate! Example: Rogue APs</td>
</tr>
<tr>
<td>Availability</td>
<td>The value of a wireless network is its promise of ubiquitous connectivity. Unfortunately, wireless networks are easy to “break” (e.g. jam, denial of service)</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>RF energy radiates, and wireless entities within the radio coverage pattern may serve as witnesses for the actions of the transmitter.</td>
</tr>
</tbody>
</table>
Security can be achieved by exploiting unique properties of the wireless physical layer (SEVILLE)

- Wireless channels are “open” and hence more susceptible to eavesdropping, intrusion and spoofing…
- Interestingly, wireless channel properties (“RF signatures”) can be exploited for authentication and to identify attackers
- Project on protocols and algorithms for security functions; also experimental validation
SEVILLE exploits the physical layer to achieve new forms of key establishment

- Use channel reciprocity to build highly correlated data sets
  - Probe the channel in each direction
  - Estimate channel using recd. probe
- Eve receives only uncorrelated information as she is more than $\lambda/2$ away
- Level crossings are used to generate bits
- Alice and Bob must exchange msgs over public channel to create identical bits
- What if channel is not already authenticated?
  - Requires additional sophistry to prevent man-in-the-middle attack.
  - It is possible using the correlated data collected from received probes.

![Diagram of channel reciprocity and key establishment](image-url)
SEVILLE’s key establishment has been validated in real customized and COTS systems

- Experimental setup:
  - Alice = AP
  - Bob = Client
  - Eve = Client on same channel
- Alice → Bob: PING REQUEST  Bob → Alice: PING REPLY
- 20 packets per second
- Eve overhears packets from both legitimate users
- (RSSI, timestamp) from recd. packet headers are pulled out by each user
- Msg. exchange protocol uses the locations of excursions to distil identical identical bits
- ~1 bit/sec in typical indoor environments with no errors.
DARWIN seeks to defend wireless networks from adversarial wireless interference

- Goal: to maintain wireless network connectivity in the presence of wireless interference (i.e. jamming)
- Strategies:
  - Channel Surfing: Adapt network channel allocations in an on-demand manner
  - Spatial Retreats: Use mobility to evade interference sources and re-establish network connectivity
  - Anti-jamming Timing Channels: Failed packet reception events may be modulated to establish a low-rate jamming resistant communication channel
  - Radio Teaming: A team of transmitters exploits multipath environments to perturb angular receiver patterns, in spite of SINR levels of -10dB or worse.

(Effect of a jammer on a network of Chipcon 1100 Radios)
A non-jammable timing channel remains when the physical layer is being jammed

- **Objective:**
  - Create a *low bit-rate overlay* that exists on the conventional physical/link-layers *in spite of* a broadband interferer.

- **Approach:** Modulate the interarrival time between packet transmissions to convey information
  - Jammed packets are detectable
Motivation:

- Units moving through “urban canyons” experience complex link quality conditions
- Adversarial scenarios, involving jammers, further complicate conditions

Increasing transmit power may not be an option... Team solutions are needed

- Can we do beamforming or cooperative communications?
- Can we utilize the “RF Clutter” to convey information?
**MIAMI: Mobile Infrastructures for Advancing Military Information Technologies involves security analysis of MIMO**

- DoD is reliant on wireless networks to support critical communications
  - Mobile Ad Hoc Networks
  - Pervasive monitoring of valuable military assets (such as artillery or food supplies)

- MIAMI seeks to address issues of performance, adaptability and reliability for three different wireless scenarios
  - *Design of Active RFID Systems for Inventory Management.*
  - *Design and Evaluation of Military MIMO Systems.*

- Task-1 emphasis is on tactical MIMO systems
  - Modeling of MIMO channels
  - Integrating ray-tracing and MIMO channel models with ns-2
  - Threat analysis of tactical MIMO radios

MIMO tactical scenarios will be integrated into a custom ns-2 simulator tool.
Cognitive Radios are an emerging wireless system with many potential security threats

- Expose the lower-layers of the protocol stack to researchers, developers and the “public”
  - scan the available spectrum, select from a wide range of operating frequencies
  - adjust modulation waveforms, perform adaptive resource allocation
- An ideal platform for abuse since the lowest layers of the wireless protocol stack are accessible to programmers.
  1. Poor programming:
    1. CR protocols will be complex, it will be easy to write buggy implementations
    2. Runaway software processes…
  2. Greedy exploitation:
    ■ Decrease back-off window in an 802.11 (or comparable) implementation
    ■ Ignore fairness in spectrum etiquette (many co-existence protocols assume honest participants, or honest data)
  3. Simply Ignoring Etiquette
    ■ Primary user returns… so-what???
  4. Economic/Game-theoretic Models
    ■ Standard economic models for spectrum sharing seek to support cooperation— but cooperation does not ensure trusted operation!
    ■ Security is an anti-social topic!
WINLAB is developing AUSTIN: Assuring Software Radios have Trusted Interactions

- Goal: to regulate the future radio environment, ensure trustworthy cognitive radio operation (Team: Rutgers, Virginia Tech, UMass)

- How — two complementary mechanisms
  - On-board enforcement – restrict any violation attempt from accessing the radio:
    - Each CR runs its own suite of spectrum etiquette protocols
    - Onboard policy checking verifies actions occur according to “spectrum laws”
  - An external monitoring infrastructure:
    - Distributed Spectrum Authority (DSA) — police agent observes the radio environment
    - DSA will punish CRs if violations are detected via authenticated kill commands.

Research
**CARMEN: A Collaborative, Assurable, and Reliable Mobile Network for Tactical Operations addresses MANET security**

**Approach:**

To address threats across all of the separate and interacting layers in the MANET, CARMEN involves a holistic suite of security mechanisms to assure proper operation of each layer. Some components that will be developed include:

- **PHY/Link-Layer Assurance:** Anti-jamming Channel Adaptation Methods will reconstruct network link connectivity to recover the network in the presence of interference.

- **Routing-Layer Assurance:** Multipath “Security Control” for Byzantine-Robust Forwarding will automatically re-allocate traffic around Byzantine nodes.

- **Transport and Resource Assurance:** Byzantine-Secure Accounting and Pin-pointing of Malicious Insiders will recognize when nodes utilize an unfair portion of system-wide network resources.

**Innovative Technology:**

- The CARMEN effort is centered on a novel architecture, involving a Secure Management Plane (SMP) that will support consistent and observable security control information across the entire MANET.

- **Advantages of CARMEN-SMP:**
  1. may utilize a separate radio link, optimized for reliability and radio range (not bandwidth).
  2. provides a common method/framework for exchanging security audit information;
  3. separate out signaling from the normal traffic/data plane;
  4. can be fed directly into trusted computing components;
  5. Reduction in hops on control plane increases provability of security for protocols.

**Implementation:**

The SMP is possible through a separate radio link optimized for reliability not bandwidth:

- Possible on dual-radio nodes (e.g., multiple 802.11 interfaces, with SMP using low-rate, more resilient modulation)

- For single-radio nodes it is possible to implement as a TDMA-overlay on 802.11

- Forward-looking vision: JTRS and other software radios can easily support multiple radio interfaces.
SEAR addresses known security weaknesses in secure AODV protocols (SAODV, ARAN)

- Characteristics
  - Authenticate RREQs/RREPs/RERRs
  - Based on symmetric key cryptography
  - Public key cryptography is only used in initial bootstrap phase
  - Sequence #'s and hop counts are protected through the use of a one-way function
  - Route errors are protected through a variation of TESLA

- Each node maintains 2 hash chains for itself to use
  - Authenticator hash chain
  - TESLA key chain

- Authenticator Hash Chain: What basically happens is…
  - Each individual hop for each even sequence number should have a corresponding hash value
  - Odd sequence number only needs one hash value
  - Nodes who have an even sequence number have the corresponding next higher odd sequence number
  - Intermediate nodes cannot increase the sequence number or decrease the hop count
New Active RFID technology targets advancing state-of-the-art in inventory management with unique security issues

- Rethink the RFID problem from bottom up using state-of-art technology
  - Simple (cheap!) tags, sophisticated readers
  - Continuous inventory, not portals
  - Route to extreme miniaturization—works for items of all sizes

- NSF STTR support and strong industry connections.
  - Initial target: jewelry supply/sales chain (Retail only: ~$50B/yr)

---

**RFID: Radio Frequency IDentification**
- RFID tags only respond when queried.
  - Easily shielded intentionally or by environment.
  - Only “seen” when pass a portal
- RFID tags are complex.
  - Many have processors, memory, and other features.
- Long life tags are passive
  - Short range, poor link quality
  - High power base stations (~5W each!)

**MRT: MicroRadio Tag™**
- MRTs announce their status continuously.
  - User knows immediately when/where they are moved.
  - Network connectivity allows remote access.
- MRTs only announce serial number
  - All other complexity is in the network and database.
- Long life with active radio
  - Long range, good link quality
  - Passive Basestations