Security Initiatives at WINLAB

Rutgers, The State University of New Jersey

www.winlab.rutgers.edu
WINLAB’s Security and Computing Initiatives

- WINLAB has a growing initiative in wireless network security and mobile/pervasive computing
- Currently the Security Group consists of
  - 3 Faculty Members:
    - Marco Gruteser (University of Colorado): Ubiquitous Computing, Secure Software Engineering, Privacy in Location Services
  - Many Students!!!
  - Collaboration: Princeton (H. Kobayashi), Columbia (H. Schulzrinne), Bell Labs (S. Paul), IBM Watson, UMD (KJR Liu, M. Wu), Rutgers CS (B. Nath, R. Martin), UColorado (Grunwald), URI (Y. Sun), UBC (Z. Wang), U. Texas (IAT), M. Kuroda (NICT)
  - Collaboration:
    - NICT Japan: Secure Future Wireless Networks (B3G)
    - NSF: ORBIT (joint with Princeton, Columbia, Bell Labs, IBM, Thomson), PARIS
    - Rutgers AEF (ICIS) Initiative
Results from Last Year’s Effort

- Wireless security papers accepted or under review:
Research Areas, Directions, and Tools

Focus Areas

- Wireless Network Security
- Sensor Network Security
- Multicast Security
- Multimedia Security

Research Initiatives

- Wireless and Sensor Privacy
- DoS Resistance (Jamming, Flooding, Identity Vulnerabilities)
- Location-based Security
- Measurement Security

Supporting Tools

- Cryptography
- Network Security Protocols
- Layer 1 and Layer 2 Methods
- Statistical Analysis
- Testbeds and Simulations
- Other Mathematical Tools
Wireless DoS Security
Denial of Service Threats

- Most work on wireless security has focused on access control and confidentiality
- Availability is the core feature of wireless networks!
- Denial of Service attacks prevent legitimate users from accessing network services.
- DoS threats are more pronounced for wireless than wired networks.

Issues:
  - Detecting DoS attack is often slow (network management/diagnosis tools are too young!)
  - There are many varieties: Jamming, MAC-layer misbehavior (e.g. Virtual Carrier Sense Attack in 802.11), De-Authentication/De-Association
  - Full strength countermeasures might require redesign of standard. We need light weight solutions that can be integrated with existing wireless networks!
Staggered TESLA: Authentication at the Receiver

- Receivers have a chained buffer
  - As keys arrive, MACs are verified
  - If matches, it puts the packet into the next layer. If not, the packet is dropped.
  - As the packets move to lower buffer layers, the trustworthiness of the packets increases

- Future Directions for Staggered TESLA and Reduced-delay Multicast Authentication:
  - Implementation and validation
  - Average authentication delay significantly reduced
  - Maximum authentication delay also reduced
DARWIN: Jamming Detection and Defense

DARWIN: Defenses for Attacks of Radio-interference on Wireless Networks
- Wireless networks may be subjected to “jamming” attacks that prevent wireless communication.

Detection:
- Challenge is to discriminate between legitimate causes of poor connectivity and jamming
- Jamming Detection (Mobihoc) paper will be presented in the Afternoon!

Defense Strategies: Channel Surfing and Spatial Retreats
- Channel Surfing Demonstration Later Today!
- Spatial Retreats Talk in the Afternoon!
Signal Strength Consistency Checks

- Build a (PDR, SS) look-up table empirically
  - Measure (PDR, SS) during a guaranteed time of non-interfered network.
  - Divide the data into PDR bins, calculate the mean and variance for the data within each bin.
  - Get the upper bound for the maximum SS that would have produced a particular PDR value during a normal case.
  - Partition the (PDR, SS) plane into a jammed-region and a non-jammed region.

- Experiment setup:
  - The sender power: -5dBm
  - Data rate: 20 packets/sec
  - Average PDR over 200 packets
  - SS were sampled every 1msec for 200msecs
  - Vary the $D_{SR}$
  - PDR bins: (0, 40) (40, 90) (90, 100)
  - PDR threshold 65%
  - 99% confidence bar
Jamming Defense: Channel Surfing

- **Adversary Model:**
  - We assume there is only one stationary adversary, who blasts on a single channel at any time.

**Adversary Model:** There is one stationary adversary, who continuously blasts on a single channel at a time.

- If we are blocked at a particular channel, we can resume our communication by switching to a different (and hopefully safe) channel that does not overlap current channel.
- Inspired by frequency hopping techniques, but operates at the link layer

- **System Issues:**
  - Must have ability to choose multiple “orthogonal” channels:
    - Prevents Interference
    - Practical Issue: PHY specs do not necessarily translate into correct “orthogonal” channels
    - Examples:
      - MICA2 Radio recommends: “choose separate channels with a minimum spacing of 150KHz” but this is incorrect
      - 11 channels in 802.11b, but only 3 orthogonal channels
  - Can the adversary follow?
Channel Surf: Two Party Prototype

- Prototype:
  - Two Berkeley motes A and B
  - A sends out a packet to B every 200msecs
  - Measure the packet delivery rate = #recv/#sent
  - Used waveform generator as jammer X
  - A and B try to detect the DoS attack periodically

- Code:
  ```c
  task void checkDos() {
    sent = call SendMsg.send(
      TOS_BCAST_ADDR,
      sizeof(uint16_t),
      &beacon_packet);
    if(!sent){
      if(++failures< thresh)
        post checkDos();
      else post changeChan();
    } else {
      failures = 0;
    }
  }
  ```

Question: How to extend this idea to WLANs?
The Attack is a form of session hijacking:

- Attacker armed with a laptop having 2 wireless cards.
- One card monitors all TCP traffic on the AP channel.
- Second card sends back TCP replies to select TCP requests (e.g. all requests for a particular web page). These are sent as if appearing from the server the user was connecting to.
- At the MAC layer the attacker spoofs AP by injecting custom 802.11x frames with AP’s source MAC address.

Result: The user session is hijacked, and service can be DoSed.
Sequence Number Filtering Strategy

- Wireless NICs typically have MAC-layer packet sequencing in firmware
  - Difficult to bypass without significant engineering

- Sequence Numbering increases monotonically

- During a spoofing attack, the observed sequence numbering will not behave monotonically

- We are designing MAC-layer filtering strategies that look for consistent sequencing
Privacy in Wireless Networks
Privacy Issues in Wireless Networks

- **Content-Oriented Security and Privacy:**
  - Issues that arise because an adversary can observe and manipulate the *exact* content in a sensor message.
  - Best addressed through cryptography and network security.

- **Context-Oriented Privacy:**
  - Issues that arise because an adversary observes the *context* surrounding creation and transmission of a sensor message.
  - Examples:
    - **Source-Location Privacy:** The physical location of communication participants may be sensitive.
    - **Traffic Privacy:** The size and amount of messages originating from a sensor may be sensitive.

- For wireless networks, **Source-Location Privacy** focuses on protecting the client from being followed and traced due to association and handoffs.

- For wireless networks, **Traffic Privacy** focuses on protecting the context of the application from being inferred by watching the size of data packets!

---

Privacy in Sensor Networks

**PARIS**: Privacy Augmented Relaying of Information from Sensors:

- Issues that arise because an adversary observes the context surrounding creation/transmission of wireless message.
- For sensor networks, Source-Location Privacy focuses on protecting the networked entity from traceback attacks by adversaries!

- New Strategies we developed:
  - Fake Sources
  - Phantom Routing

*Game Over!*
Phantom routing

• The source message is sent out on a **directed random walk** for “h” hops before being flooded or sent down to shortest path.

• Thus a **phantom source** is created for every “new” message that’s sent out.

• Combines the best of flooding and shortest path strategies but without any of the problems.
Privacy-observant Location Tracking

- Location Information useful for
  - Calibrating the tracking system
  - Location-based applications
- Can we perturb time-series information?
  - Individual paths are not identifiable
  - Aggregate information from multiple users is useful
- Afternoon talk by Baik Hoh on privacy for location services
Secure Localization
Location-based Security in Wireless Networks

- Already, many techniques have emerged to localize a wireless device.
- Enforcement of location-aware security policies will become a new application for wireless networks:
  - A laptop should not be taken out of a particular building
  - A file should not be opened outside of a secure room
- As more of these location-dependent services get deployed, the very mechanisms that provide location information will become the target of misuse and attacks.
- Trusted location information is critical to the success of these new services!
- Two efforts to address this problem:
  - Integrate resilience into localization methods (Z. Li)
  - Intrusion detection via verifiable localization algorithms (Y. Zhang)
Intrusion Detection and Location-Authentication in Wireless Networks

- **Idea:** Set up different power configurations and alternate between them randomly.

- **Result:** Wireless devices will change their association as they can no longer hear a BS/AP
  - We may use this to locate a wireless device
  - Intruders in a wireless network will not be able to fake a location

- **Question:**
  - How to modulate the power configurations to best isolate a mobile device?
Wireless Localization Security

- Location information will facilitate new computing services
  - Location-based file access control
- **Problem**: Localization methods are not secure!
- Traditional cryptography and network security can address cryptographic attacks (Is this beacon really from the AP?)

**Is cryptography alone enough?**

**No!**

The localization algorithms depend on measurements that are susceptible to attack!!
## Possible Attacks vs. Localization Algorithms

<table>
<thead>
<tr>
<th>Property</th>
<th>Example Algorithms</th>
<th>Attack Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time of Flight</td>
<td>Cricket</td>
<td>➢ Remove direct path and force radio transmission to employ a multipath; ➢ Delay transmission of a response message; ➢ Exploit difference in propagation speeds (speedup attack, transmission through a different medium).</td>
</tr>
<tr>
<td>Signal Strength</td>
<td>RADAR, SpotON, Nibble</td>
<td>➢ Remove direct path and force radio transmission to employ a multipath; ➢ Introduce different microwave or acoustic propagation loss model; ➢ Transmit at a different power than specified by protocol; ➢ Locally elevate ambient channel noise</td>
</tr>
<tr>
<td>Region Inclusion</td>
<td>APIT, SerLoc</td>
<td>➢ Enlarge neighborhood by wormholes; ➢ Manipulate the one-hop distance measurements; ➢ Alter neighborhood by jamming along certain directions</td>
</tr>
<tr>
<td>Property</td>
<td>Example Algorithms</td>
<td>Attack Threats</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Angle of Arrival</td>
<td>APS</td>
<td>➢ Remove direct path and force radio transmission to employ a multipath;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>➢ Change the signal arrival angel by using reflective objects, e.g., mirrors;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>➢ Alter clockwise/counter-clockwise orientation of receiver (up-down attack)</td>
</tr>
<tr>
<td>Hop Count</td>
<td>DV-Hop</td>
<td>➢ Shorten the routing path between two nodes through wormholes;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>➢ Lengthen the routing path between two nodes by jamming;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>➢ Alter the hop count by manipulating the radio range;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>➢ Vary per-hop distance by physically removing/displacing nodes</td>
</tr>
<tr>
<td>Neighbor Location</td>
<td>Centroid, SerLoc</td>
<td>➢ Shrink radio region (jamming); Enlarge radio region (transmit at higher power, wormhole);</td>
</tr>
<tr>
<td></td>
<td></td>
<td>➢ Replay; Modify the message; Physically move locators;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>➢ Change antenna receive pattern</td>
</tr>
</tbody>
</table>
Attacks on Signal Strength

- Distance is measured using the relationship between received signal strength and distance.
- Adversary may affect the receive signal power by:
  - Alter transmit power of nodes
  - Remove direct path by introducing obstacles
  - Introduce absorbing or attenuating material
  - Introduce ambient channel noise
Attacks on Hop-Count

- DV-hop localization algorithm:
  - Obtain the hop counts between a sensor node and several locators.
  - Translate hop counts to actual distance.
  - Localize using triangulation.

It is critical to obtain the correct hop counts between sensor nodes and every locator.
Defenses for Wireless Localization

Strategy: Two-tier approach to defending wireless localization…

Add Security and Robustness!

Add Authentication, Entity Verification, Etc…
See SerLoc, SPINE, ROPE
Switched LMS-LS Algorithm

- Directly applying robust statistical methods (LMS) is computationally prohibitive.
- We have devised an adaptive algorithm that switches between LS and LMS based upon the likelihood the localization algorithm is under attack.