CAREER: Enhancing the Security of Pervasive Wireless Networks by Exploiting Location

PI: Yingying (Jennifer) Chen
Stevens Institute of Technology
http://personal.stevens.edu/~ychen6/


PI Yingying Chen

This project aims to use location-oriented information as a promising new dimension to complement conventional security solutions and enhance wireless security.

Motivation

- Wireless systems become more pervasive
  - anytime-anywhere service model
- Wireless security
  - a major technical barrier for wide-deployment
- Traditional approaches
  - case-by-case basis in an ad-hoc manner
  - Infrastructural and management overhead
- New and rapidly evolving adversaries
  - Due to ubiquity of wireless systems

Objective

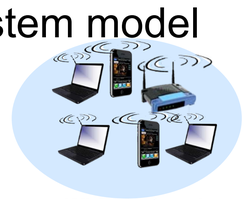
- Location-oriented information is powerful
  - describe current location of wireless device
  - cornerstone of new wireless services
  - hard to falsify, not reliant on cryptography
- Location should be integrated into any wireless network stack as a true partner to cope with attacks
- Security solutions can leverage the knowledge provided by spatial invariants across different network layers

Research Thrusts

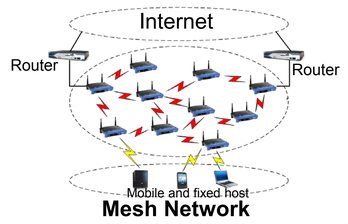
- Location enabled attack detection
  - Address fundamental network threats that involve identity-compromise - first step to launch a variety of attacks
- Robust localization of adversaries
  - Coping with the localization infrastructure attacks
  - Jammer location identification for reliable communication
- Attack resistant location aware secure access

Attack Model and System Model

- Attack model
  - Identity based attacks: spoofing & Sybil
  - Localization infrastructure attacks: signal strength or Access Points (APs)
  - Jamming attacks and radio interference
- System model


Wi-Fi Network

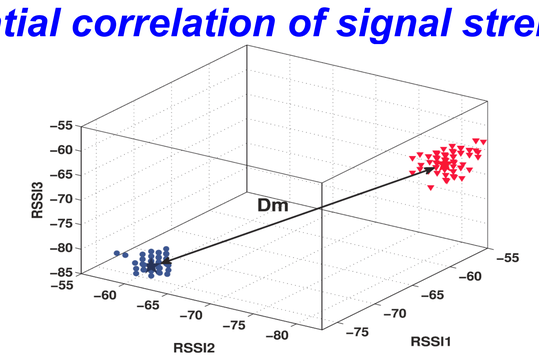

Cellular Network



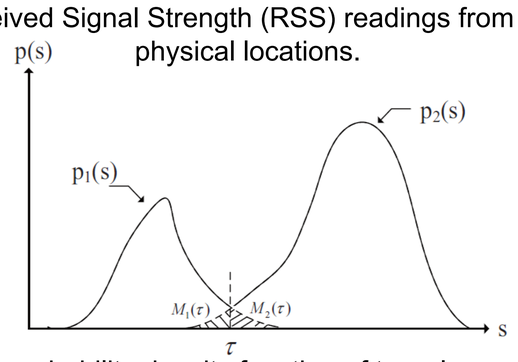
Mesh Network

Approaches

Spatial correlation of signal strength

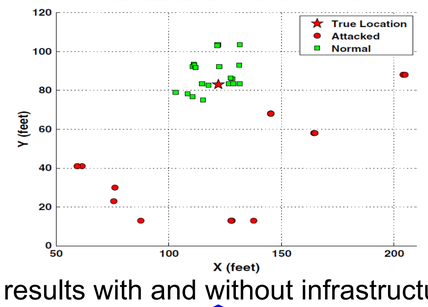


Received Signal Strength (RSS) readings from two physical locations.



RSS probability density function of two classes.

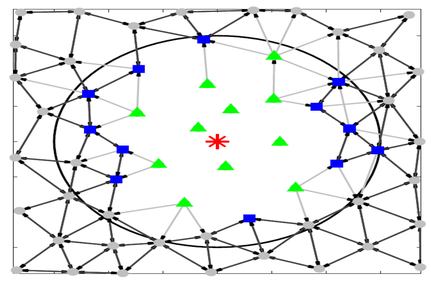
Correlation among benign localization results



Localization results with and without infrastructure attacks.

- Geometric relationship: Localization results under normal situations are clustered together, whereas they are scattered under infrastructure attacks.
- Spatial correlation of received signal strength is exploited to discriminate identify fraud attack scenarios from normal situations.
- Automatic network topology partitioning under jamming: multiple jammers may have overlapping jamming regions and form only one connected jammed area.

Topology change under jamming


The topology change due to jamming.

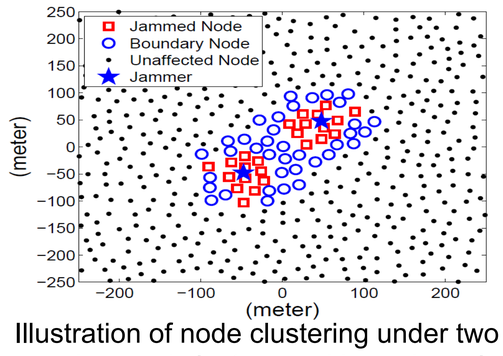
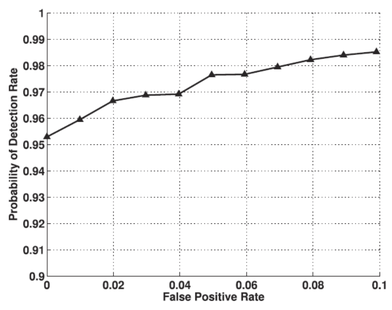


Illustration of node clustering under two jammers: jammed clusters and boundary clusters

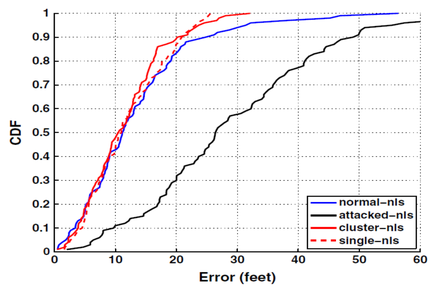
Results

Spoofing attack detection



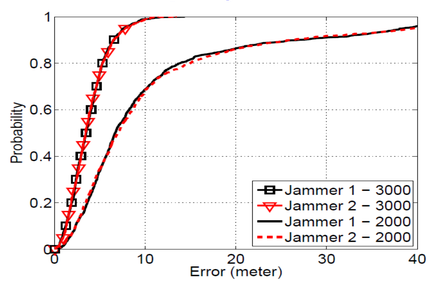
Spoofing attack detection using spatial correlation of RSS.

Attack resistant attacker localization



Attacker localization error CDF under Infrastructure attacks.

Localization of multiple jammers



Error CDF when localizing two jammers.

More Aspects

Secret key extraction using RSS

- Secret key generation using physical layer information can complement conventional security methods without requiring a fixed key management infrastructure.
- Channel reciprocity: Radio propagation of the wireless channel is identical on both directions of a link.
- Two wireless devices can extract identical secret bits independently by using the sampled physical layer information.

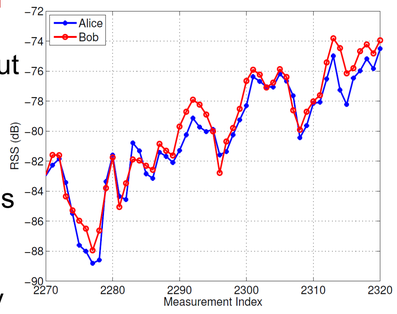


Illustration of Channel Reciprocity

Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

National Science Foundation
WHERE DISCOVERIES BEGIN

STEVENS INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY