



Berkeley  
STANFORD UNIVERSITY  
CORNELL  
Carnegie Mellon

**TROST**  
Trust For Resilience In the Ubiquitous Systems Technology

# Security in Sensor Networks

Tanya Roosta  
Chris Karlof  
Professor S. Sastry



 June 26-28, 2005 All Hands Meeting

Berkeley  
STANFORD UNIVERSITY  
CORNELL  
Carnegie Mellon

**TROST**  
Trust For Resilience In the Ubiquitous Systems Technology

## Overview



- Sensor Networks
- Motivation
- Security Requirements
- Limitations
- Threat Models
- Previous Work
- Research Problems

 TRUST All Hands Meeting June 26-28, 2005

## Background on Sensor Network

- ❑ Wireless networks consisting of a large number of nodes
  - self-organizing
  - highly integrated with changing environment and network
- ❑ Highly Constrained resources
  - processing, storage, bandwidth, power
- ❑ Facilitate large scale deployment
  - Health care monitoring
  - Surveillance
  - Traffic monitoring
  - Military application



## Sensor Network Security

- ❑ Design time security
- ❑ Privacy of collected data
- ❑ New research challenges arising from new applications



## Basic Security Requirements

- Confidentiality
- Authentication
- Integrity
- Freshness
- Secure Group Management
- Availability



## Limitations in Sensor Networks

- Deployed in Hostile Environment
  - Vulnerability to physical capture
- Random Topology
  - No prior knowledge of post-deployment topology
- Limited Resources
  - Energy Restrictions
  - Limited Communication and Computational Power (10 KB RAM, 250 kbps data rate)
  - Storage Restrictions



## Attacker Models for Sensor Networks

- ❑ Mote-class Attacker
  - Controls a few ordinary sensor nodes
- ❑ Laptop-class Attacker
  - Greater battery & processing power, memory, high-power radio transmitter, low-latency communication



## Threat Models in Sensor Networks

- ❑ Outsider Attacks
  - Passive eavesdropping
  - Denial of service attacks
  - Replay attacks
- ❑ Insider Attacks: compromised node
  - Node runs malicious code
  - The node has access to the secret keys and can participate in the authenticated communication.



## Previous Work

- ❑ **Secure communication**
  - SPINS: Security Protocols for Sensor Networks (Perrig)
  - TinySec: Link Layer encryption for tiny devices (Karlof)
- ❑ **Robust aggregation**
  - SIA: Secure Information Aggregation for Sensor Networks (Przydatek)
  - Resilient Aggregation in Sensor Networks (Wagner)
- ❑ **Secure routing**
  - Countermeasures for Sybil attack (Perrig)
  - Countermeasures for Worm hole attack (Y. Hu, Capkun)



## Previous Work (cont.)

- ❑ **Secure location verification**
  - Verification of Location Claims (N. Sastry)
- ❑ **Robust localization**
  - Statistical Methods for Robust Localization (Z. Li)
  - SeRLoc (Lazos)
- ❑ **Key distribution protocols**
  - Random Key Distribution Protocol (Perrig, Eschenauer)



## Future Research

- ❑ Clock synchronization
- ❑ Secure location discovery & verification of location claims
- ❑ Privacy
  - Location
  - Collected data
- ❑ Secure aggregation & in-network processing
- ❑ Cluster formation/Cluster-head election
- ❑ Differentiating between node failure & security attack



## Research at Berkeley

- ❑ Time synchronization security
  - Attacks on time sync protocols
  - Designing secure time sync protocols
- ❑ Secure Tracking
  - MCMCDA tracking
- ❑ Statistical modeling for intrusion detection
  - Reputation system framework
- ❑ Wireless mobile systems
  - Data security/privacy



## Participants at Berkeley

- Shankar Sastry
- Doug Tygar
- David Wagner
- Chris Karlof
- Tanya Roosta
- Prabal Dutta
- Jonathan Hui
- Umesh Shankar
- Deirdre Mulligan
- Jack Lerner

