

# DESIGNING SECURE SENSOR NETWORKS

ELAINE SHI AND ADRIAN PERRIG  
CARNEGIE MELLON UNIVERSITY  
Presented by  
Yuttasart Nitipaichit

TeleNet@Pitt

## Introduction

- Sensor network plays major role
- Limitation in WSN made it a challenge
  - Computation
  - Memory
  - Power resources
  - Susceptibility to physical capture
- Scalability
- Trade-off among various security measures
- Mechanism to achieve secure communication

TeleNet@Pitt

## Outline of paper

- THREAT AND TRUST MODEL
- SECURITY REQUIREMENTS
- ATTACKS AND COUNTERMEASURES
- RESEARCH DIRECTIONS

TeleNet@Pitt

## THREAT AND TRUST MODEL

- OUTSIDER ATTACKS
  - Eavesdrop, steal information
  - Alter or spoof packet
  - DoS: Injecting/Jamming
- INSIDER ATTACKS/NODE COMPROMISE
  - Subverted nodes/powerful devices with following properties
    - Running malicious code
    - Radio compatible
    - Authorized to participate
- THE BASE STATION AS A POINT OF TRUST
  - Physically protected, tamper-robust hardware?
  - Scalability?

TeleNet@Pitt

## SECURITY REQUIREMENTS

- DESIRED PROPERTIES
  - **Robustness against Outsider Attacks**
    - Primitive cryptography -> authenticity, secrecy
    - Large quantity of nodes -> redundancy
  - **Resilience to Insider Attacks, Graceful Degradation with Respect to Node Compromise**
    - mechanism to deal with compromised node
  - **Realistic Levels of Security**
- AUTHENTICATION
- SECRECY: secret key
- AVAILABILITY: DoS attack
- SERVICE INTEGRITY: data aggregation


TeleNet@Pitt

## ATTACKS AND COUNTERMEASURES

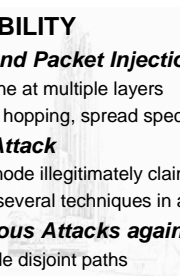
- ON SECRECY AND AUTHENTICATION
  - **Key Establishment and Management**
    - Study how to setup secret key btw nodes
    - Use global key: vulnerable to node compromised
    - Public key is popular but costly
    - Random key predistribution: need improve scalability
  - **Broadcast/Multicast Authentication**
    - Important for many WSN protocols
    - One approach is to use public key
    - uTesla introduces asymmetric into symmetric

TeleNet@Pitt

## ATTACKS AND COUNTERMEASURES




- **ON AVAILABILITY**
  - *Jamming and Packet Injection*
    - Can be done at multiple layers
    - Frequency hopping, spread spectrum
  - *The Sybil Attack*
    - Malicious node illegitimately claims multiple IDs
    - Proposed several techniques in another paper
  - *Miscellaneous Attacks against Routing*
    - Use multiple disjoint paths




TeleNet@Pitt 7

## ATTACKS AND COUNTERMEASURES




- **STEALTHY ATTACKS AGAINST SERVICE INTEGRITY**
  - **Make network accept false data**
  - **False synchronization message**
  - **Time synchronization protocols assume a trusted environment**

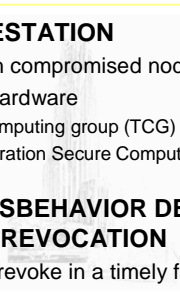


TeleNet@Pitt 8

## RESEARCH DIRECTIONS




- **CODE ATTESTATION**
  - Dealing with compromised nodes
  - Software/Hardware
    - Trusted computing group (TCG)
    - Next Generation Secure Computing Base (NGSCB)
- **SECURE MISBEHAVIOR DETECTION AND NODE REVOCATION**
  - Detect and revoke in a timely fashion
  - Voting system

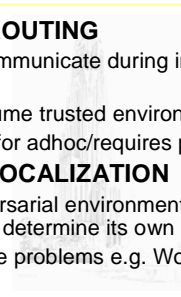


TeleNet@Pitt 9

## RESEARCH DIRECTIONS




- **SECURE ROUTING**
  - Able to communicate during in progress attack
  - Many assume trusted environment
  - Designed for adhoc/requires powerful node
- **SECURE LOCALIZATION**
  - In an adversarial environment, node must accurately determine its own coordinate
  - Might solve problems e.g. Wormhole, Sybil attack
- **EFFICIENT CRYPTOGRAPHIC PRIMITIVES**

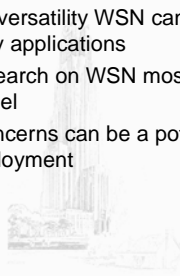


TeleNet@Pitt 10

## CONCLUSION



- Given their versatility WSN can play major role in many applications
- Current research on WSN mostly built on trusted model
- Security concerns can be a potential obstacle to wide deployment



TeleNet@Pitt 11





TeleNet@Pitt 12