Dependable Middleware for Wireless Sensor and Mesh Networks

Saurabh Bagchi
Dependable Computing Systems Lab (DCSL)
& Center for Wireless Systems and Applications (CWSA)
School of Electrical and Computer Engineering
Purdue University
sbagchi@purdue.edu

http://www.ece.purdue.edu/~dcsl

Work supported by:
NSF, Indiana 21st Century Fund, Motorola, Purdue Research Foundation

PURDUE UNIVERSITY

Challenges to Providing Dependability

- Open communication media
  - Snooping is easy
- Hostile environment
  - Attackers everywhere
- Limited resources
  - Bandwidth and energy resources are constrained
  - Can not tolerate high overhead measures
  - Easy to launch attacks (cheap devices, no tamper-proof)
- Lack of infrastructure and difficult-to-reach deployments
  - Difficult to manage and control
  - Nodes are easy to access and capture by attackers
- Mobility
  - Dynamic topology
  - Frequent link failures

PURDUE UNIVERSITY

Security Attacks

- Two classes of attacks
  1. Attacks that can be defeated by crypto mechanisms
     - Eavesdropping: Solved by encryption
     - Message tampering: Solved by authentication
  2. Attacks that subvert the functionality of the network
     - Control attacks: Manipulating control traffic (e.g., routing traffic) to disrupt data traffic
       - Examples: ID spoofing and Sybil, sinkhole, rushing, wormhole
     - Data Attacks: Directly manipulate data traffic
       - Examples: Blackhole, grayhole
     - This class cannot be prevented by cryptographic mechanisms alone
- We focus on the second class

PURDUE UNIVERSITY

Overview of Our Completed Work

- Overall goal: Design, develop, and deploy practical solutions to provide end-to-end reliability in sensor and mesh networks

1. Detection of Malicious Nodes through Local Overhearing
   - No need for trusted entity in the middle of the network
   - Leverage the ability to overhear neighbor communication to detect misbehaving nodes
   - Nodes are isolated based on quorum
   - We have a solution for mobile networks using few secure nodes distributed through the network
2. Detection in multi-channel mesh networks
   - Different nodes communicating on different channels
   - Dynamically determine which channels to monitor
   - Incremental operation when some nodes change their channel assignments

PURDUE UNIVERSITY

Overview of Our Completed Work

3. Reputation system in wireless networks
   - Limit the capacity for malicious nodes to cause continued harm in network
   - Reputation of a node maintained in a distributed manner
   - Reputation built through normal node actions (data sensing, forwarding, …)
   - Each node's interaction determined by its view of reputation of another node
   - Reputation also computed from second-hand information
4. Secure middleware for core network functions
   - *Remote code upload*: Network can be reprogrammed *in situ*
   - We have optimized the bandwidth, energy, and time required for reprogramming
   - *Synchronization*: Network-wide synchronization needed due to low duty cycle operation
   - We have a scheme for on-demand synchronization
   - All the middleware is robust to external adversary nodes

PURDUE UNIVERSITY

Ongoing Work

1. Design of protocols that will guarantee communication between two network nodes even if the adversary can selectively compromise node. (Joint work with Prof. Xiaojun Lin)
2. Use reputation in a multi-hop network for common network operations, such as data gathering and data storage. (Joint work with Prof. Xiaojun Lin)
3. Interactions between heterogeneous networks – mobile ad-hoc and sensor, or mesh and sensor networks.

- All publications on the topic are on the publications page of our research group – Dependable Computing Systems Lab (DCSL)
  - Look under "Intelligent Ad-Hoc Wireless Networks"

PURDUE UNIVERSITY