UCLA
Posters

Title
SIP2: High integrity in Sensor Networks: Models, Techniques, and System Support

Permalink
https://escholarship.org/uc/item/85186154

Authors
Laura Balzano
Saurabh Ganeriwal
Mani Srivastava

Publication Date
2005

eScholarship.org
Powered by the California Digital Library
University of California

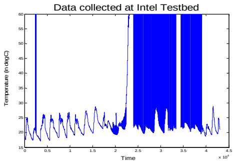
CENS Center for Embedded Networked Sensing

High Integrity in Sensor Networks

Saurabh Ganeriwal, Laura Balzano, and Mani Srivastava
Networked and Embedded Systems Laboratory

Introduction: Impact of integrity compromise

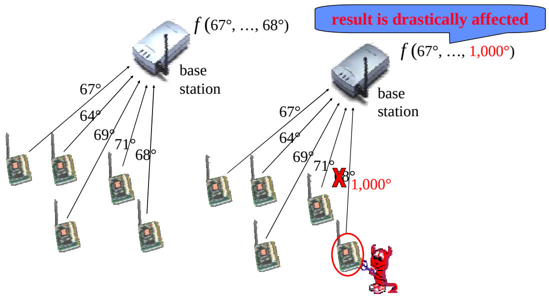
Data integrity is vulnerable to faulty and malicious behavior in all sensor network systems. In data aggregation systems, the system output is easily affected by faulty values.



Obvious solution: make devices tamper proof and robust to failures.

Our goals:

- Analyze the integrity of existing sensor systems.
- Propose algorithms and infrastructure for low-cost high-integrity sensor networks.



Problem Description: Three areas in need of integrity improvement

Models

- **Fault Modeling**
  - Model potential faults so that they can be identified
- **Analysis**
  - Using fault models we can identify potential weaknesses of data fusion algorithms

Techniques

- **Detection**
  - Nodes maintain a reputation to detect nodes that are not cooperating
  - Assess collected data with statistical fault models
- **Resilience**
  - Robust algorithms that can handle misbehavior in networking, sensing as well as data processing.

Systems Support

- **Assist in ease of use**
  - Provide an emulation framework for users to test there protocols in presence of fault
  - Reconfigurable support modules through SOS
  - Provide a user-level interface for customizing the behavior of RFSN

Proposed Solution: Reputation-based detection and Remote testing ability

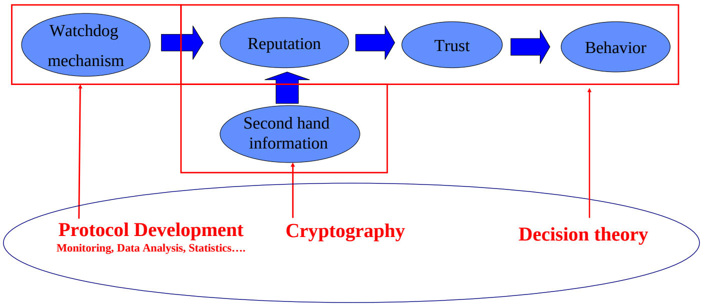
How do nodes trust each other?

- **Embedded in every social network is a web of trust**
  - When faced with uncertainty, trust those whom you think are trustworthy
- **Similar approach**
  - Nodes maintain reputation for each other.
  - Help them to differentiate between good and bad/faulty nodes.

Why take this approach?

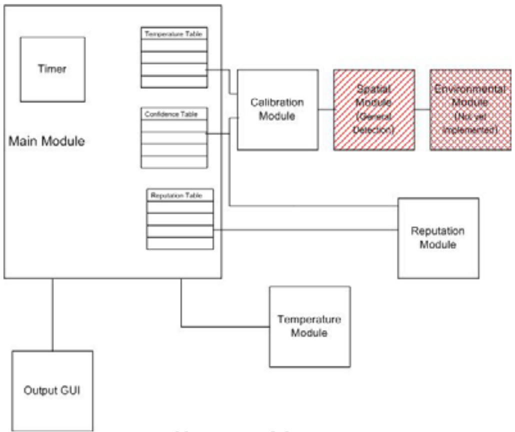
- **Sensor networks already follow a community model**
  - Collaborative information gathering, data processing and relaying.
- **Missing element is trust…..**
  - Nodes are simple and collaborate with everybody.
- **RFSN incorporates intelligence into nodes**
  - Cooperate with only those that are trustworthy.

Node level skeleton structure of RFSN



Watchdog mechanism
Reputation
Trust
Behavior
Second hand information
Protocol Development
Monitoring, Data Analysis, Statistics….
Cryptography
Decision theory

RFSN: Middleware Service



- **Calibration Module**
  - Analysis and modeling of calibration error on MTS300 sensor boards.
- **Outlier Detection**
  - Have implemented both distance and density-based outlier detection.

- **RFSN is available as a middleware service on Mica2 motes.**
- **Case-study on a lab-scale temperature monitoring system.**
- **Emulated faulty nodes by bringing a heat-source close to them.**
- **System successfully removes a minority of faults.**
- **An in-depth empirical study is in progress!**

Sensor Network Fault Emulator

- **We have developed an emulator that allows inserting fault models and imposing a topology on a sensor network remotely.**
- **Implemented on the top of SOS.**
  - **Allows for run-time reconfiguration and customization.**
- **Provides a test-bed for gauging the resiliency of sensor networking protocols against faults.**

UCLA – UCR – Caltech – USC – CSU – JPL – UC Merced