Resilient Data Collection of Wireless Sensor Networks in Oil and Gas Refineries

Tianyuan Liu, Klara Nahrstedt
University of Illinois at Urbana-Champaign

Nov 3, 2017

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security | cred-c.org

Motivation – Wireless Sensors

- Wireless sensing improves refinery operations
  - Emerson process management suggests a saving of $12.3M/year for a typical 250-Mbpd refinery by deploying wireless sensing technology.

TABLE 1. Savings, implementation costs and ROI for a 250-Mbpd refinery

Application	Monitoring and analytics	Savings, $MM	Implementation cost, $MM	ROI, months
Heat exchanger monitoring	Fouling rate and limits	$2.7–$3.6	$0.62	3 months
Cooling tower monitoring	Efficiency and health	$0.3–$0.5	$0.16	4 months
Steam trap monitoring	Failure	$2.5–$3.3	$1.48	5 months
Relief valve monitoring	Releases and leaks	$2.4–$3.2	$1.59	6 months
Pump monitoring	Cavitation, pump health	$0.5–$0.6	$0.55	11 months
Air-cooled heat exchanger monitoring	Fan health and fouling	$0.9–$1.1	$1.20	13 months
Mobile workforce	Turnaround diagnostics	$1.6–$2.1	$0.40	3 months
Safety shower and eye wash monitoring	Trigger indication	Per incident	$0.39	Safety
TOTAL		**$10.9–$14.4**	**$6.40**	**5 months**

Motivation – Refinery Resiliency

- The sensors are deployed in open areas
  - Subject to cyber-attacks and hazardous environment

- Hurricane Harvey destroyed the nation’s largest refinery in August 2017.

- Motivates
  - Fast failure detection
  - Large-scale failure tolerance
  - Efficient failure recovery
  - Minimizing risks for cyber-attacks

CREDC

Motivation – Defining Resiliency

- The resiliency from networking aspect:
  Ability of the sensor network to maintain connectivity to the data center under large scale failures.

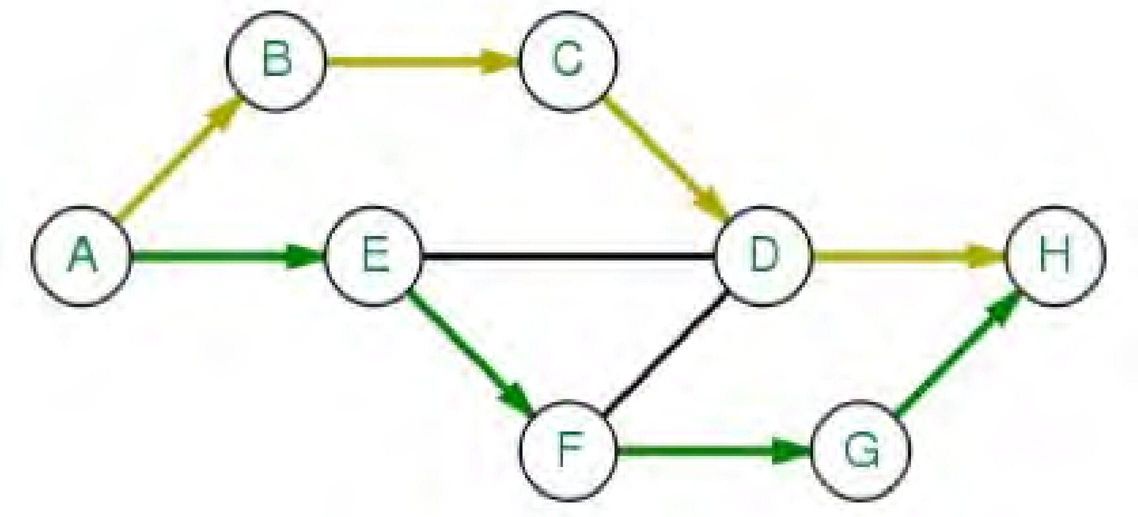
Related Technology – WirelessHART

- WirelessHART
  - A wireless mesh network communication protocol for process automation applications.
  - Based on the Highway Addressable Remote Transducer Protocol (HART).

Related Technology – WirelessHART

- WirelessHART
  - A wireless mesh network communication protocol for process automation applications.
  - Based on the Highway Addressable Remote Transducer Protocol (HART).

- Failure Tolerating Approach
  - Disjoint multi-path structure
  - Tolerates single point of failure
    - does not tolerate large scale failures



Related Technology – WirelessHART

- WirelessHART
  - A wireless mesh network communication protocol for process automation applications.
  - Based on the Highway Addressable Remote Transducer Protocol (HART).

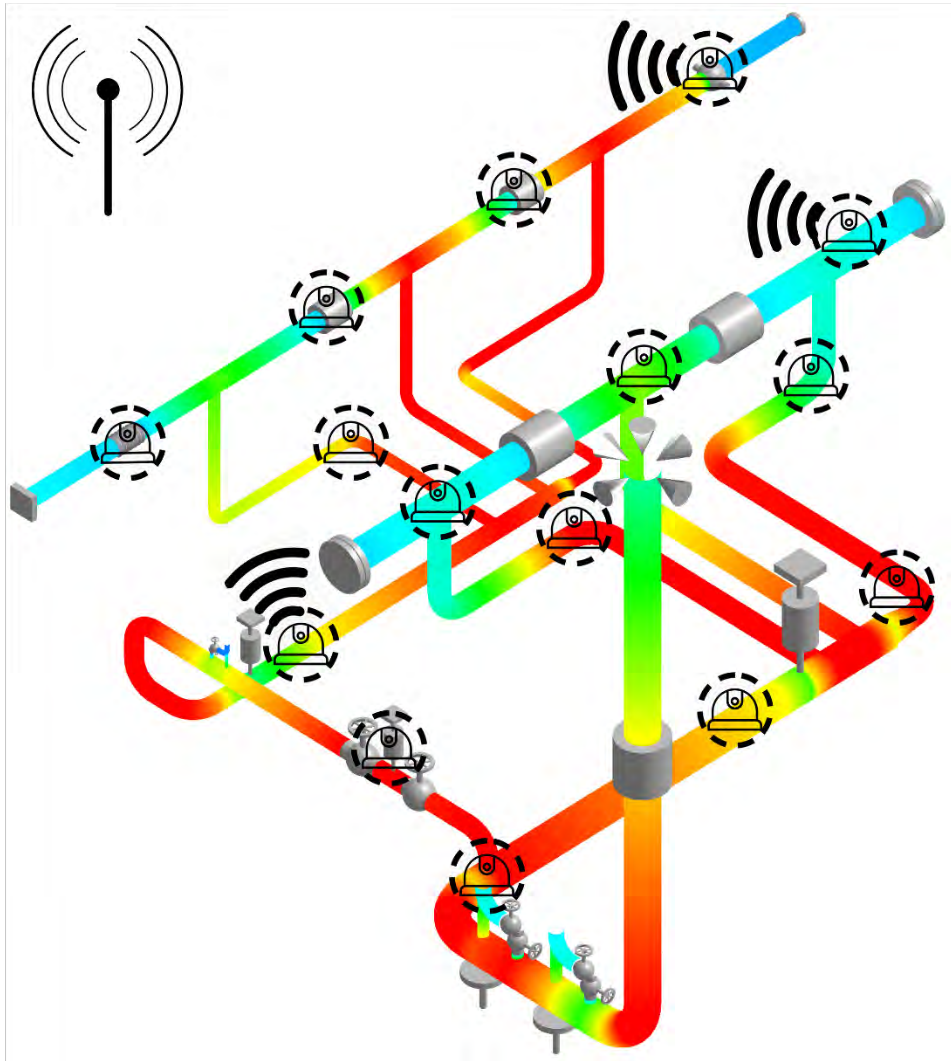
- Security design
  - Defense for jamming, eavesdropping, replay attacks, man-in-the-middle attacks, and Sybil attacks
  - Devices use a shared join key to authenticate themselves to the Gateway - an attacker may have access to the key by compromising a device

Our Approach

- Embedding resiliency into data collection framework
  - Wireless mesh network
  - Multi-tree structure
  - Tolerate large scale failures by a distributed self-healing protocol
  - Reduce the risk of leaking shared join key

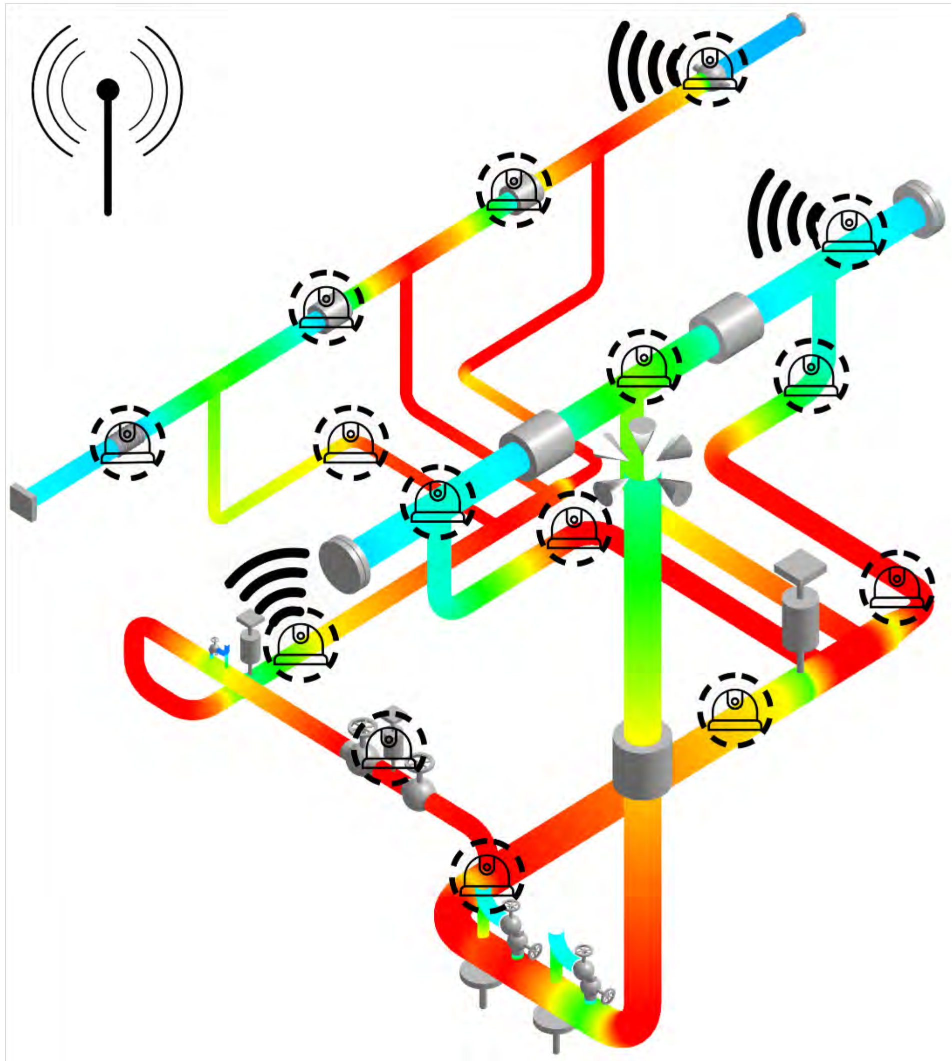
- Construct optimal data collection paths
- Recover connectivity under failures by self-healing

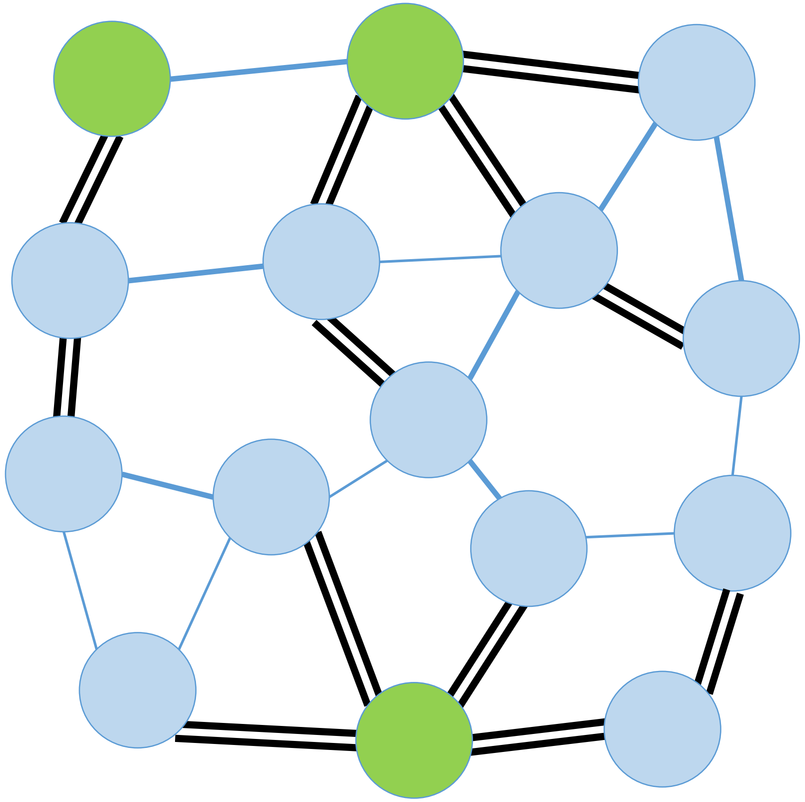
Model



- Model:
  - Sensors send data to master via SCADA-like protocol
  - Short-range v.s. long-range communication capabilities
  - Hop-by-hop communication
  - Fail-stop model

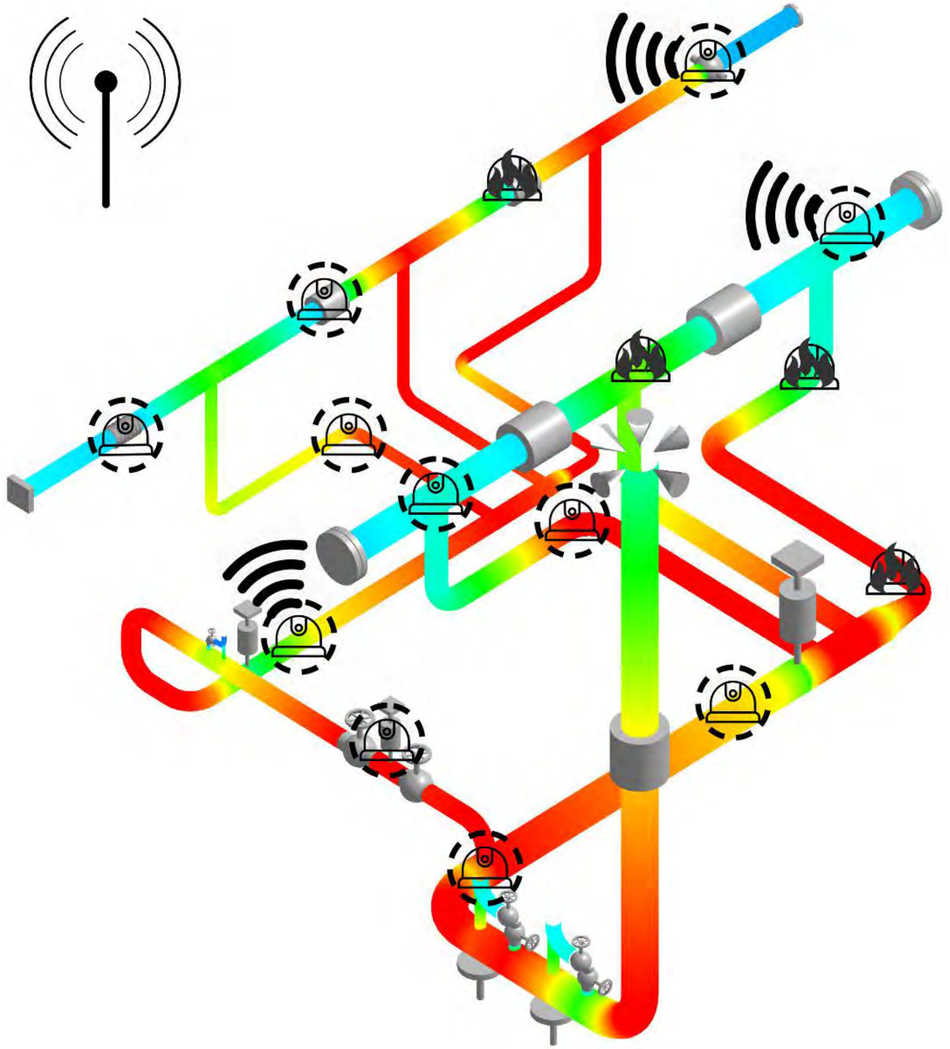
Construct Data Collection Path

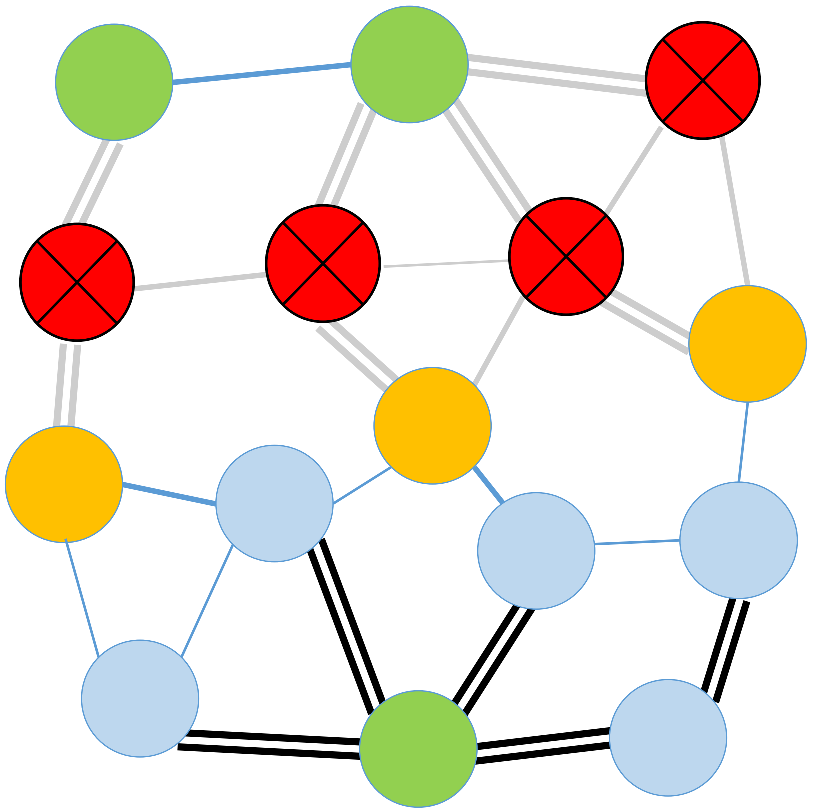




- Optimization goals:
  - Minimize data collection time (tree height)
  - Bound key leakage probability (tree size)

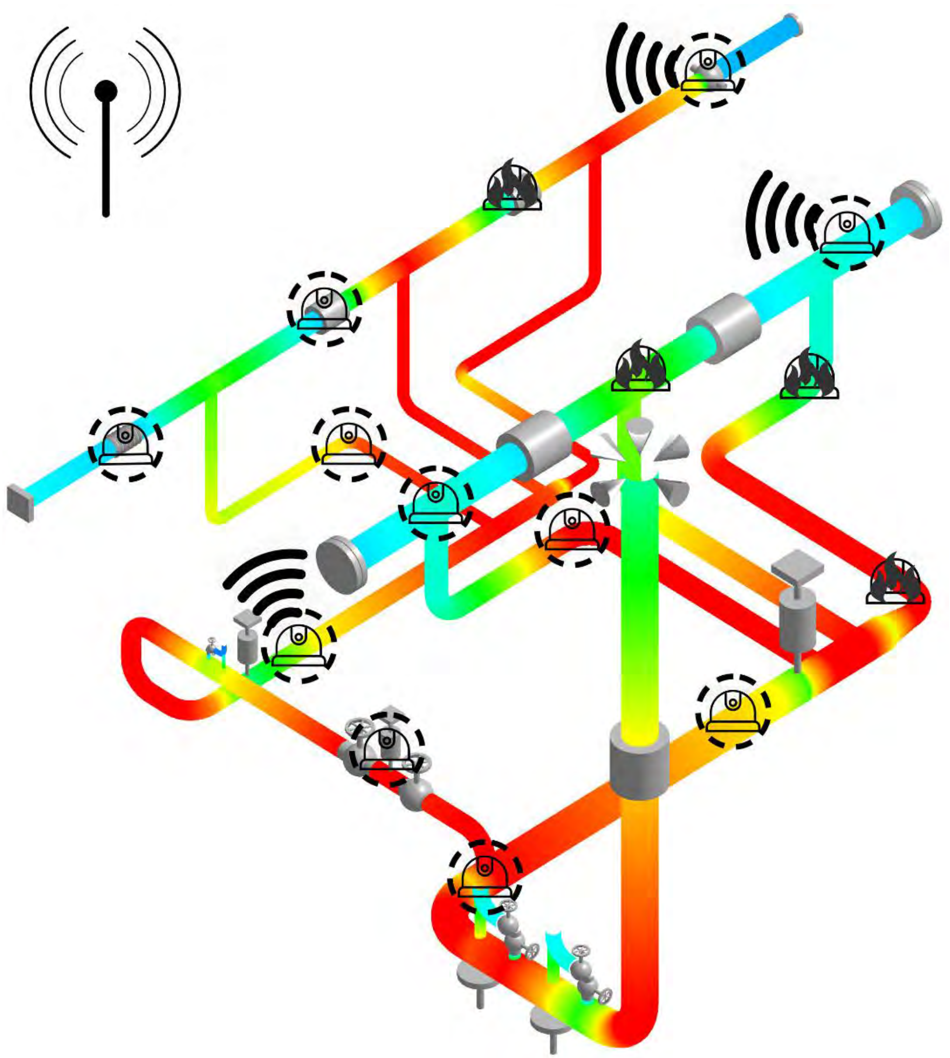
Failure Detection

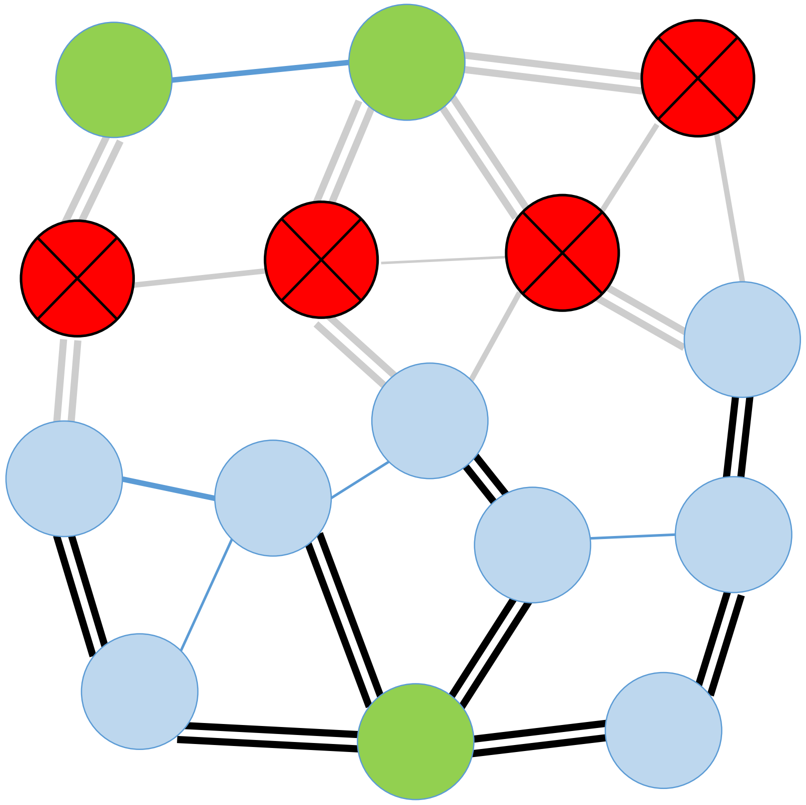




- Every sensor runs failure detection for its parent
- Upon parent failure detected, trigger self-healing

Recover Connectivity





Solution Highlights

- Construct data collection trees
  - Centralized planning
  - Data collection time optimization by Mixed-Integer Linear Programming (MILP)
  - Shared key leakage probability is bounded

$$P_{\text{leak}}(\mathcal{T}) = 1 - \prod_{i \in \mathcal{T}} (1 - p_i) \leq P_{\text{th}}.$$

- Recover connectivity under failures
  - Distributed self-healing protocol
  - Heuristic approach to re-construct backup data collection paths

Experiments

- Simulation
  - Generate topologies with up to 500+ sensors
  - Inject large scale failures with 2% of nodes
  - Evaluate success rate for recovery (reliability) and data collection time (efficiency)

- Testbed of Prototype on Raspberry Pi 3
  - CPU utilization (< 2%)
  - End-to-end delay for self-healing protocol (< 5s)

Experiments

- Simulation results

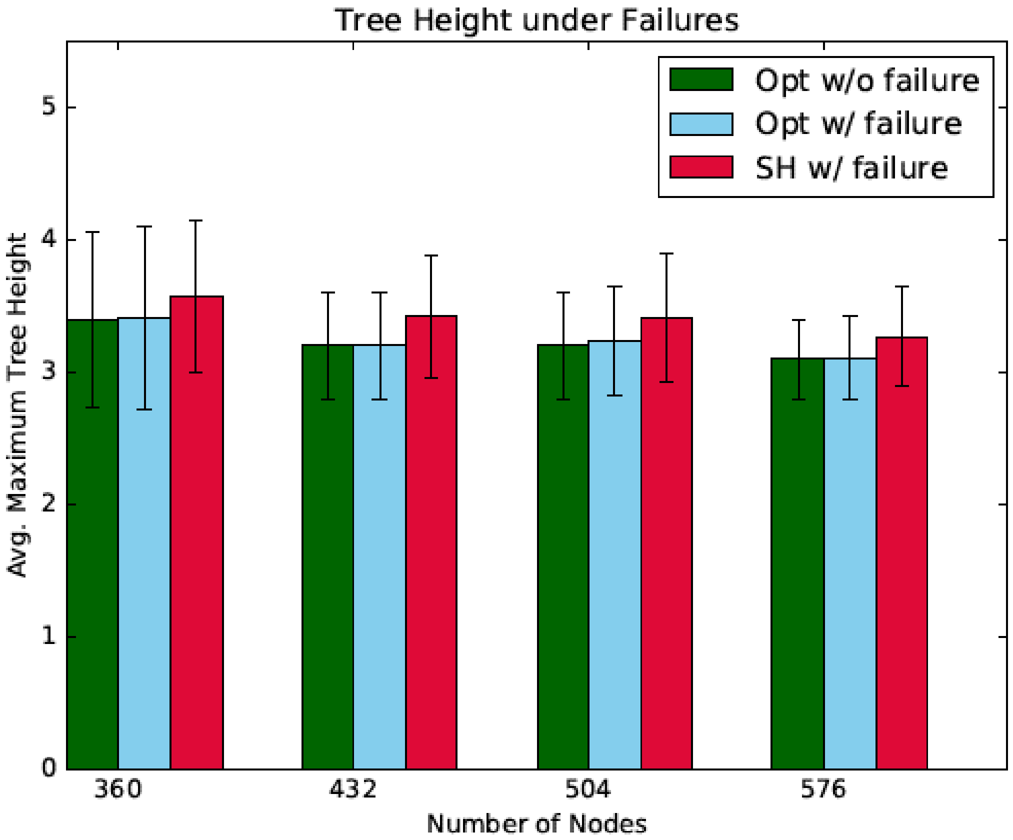
RSR OF SELF-HEALING V.S. RELIABLE GRAPH ROUTING

N_{node}	Self-healing	Reliable Graph Routing
360	91.1%	33.8%
432	92.3%	34.3%
504	92.4%	36.2%
576	93.0%	36.9%

- Compare the recovery success rate between our self-healing and WirelessHART (2-disjoint multi-path).

Experiments

- Simulation results



- The data collection time increases by <7% after recovery.

Publication and Software

- A paper at CNC workshop 2018, and a technical report.
- A planning software which computes the optimal data collection paths.
- An extendable testbed for self-healing protocols.

Future Direction

- Our research scope is designing resilient protocols for O&G infrastructures
- In 2018, we will focus on more general monitoring technologies with an emphasis on location-based services, e.g. in drone monitoring systems.

Questions?

Tianyuan Liu and Klara Nahrstedt
{tliu60, klara}@illinois.edu