Secure Wireless Mesh Networking for Nuclear Sensing

Advanced Sensors and Instrumentation (ASI) Annual Program Webinar

November 4, 2024

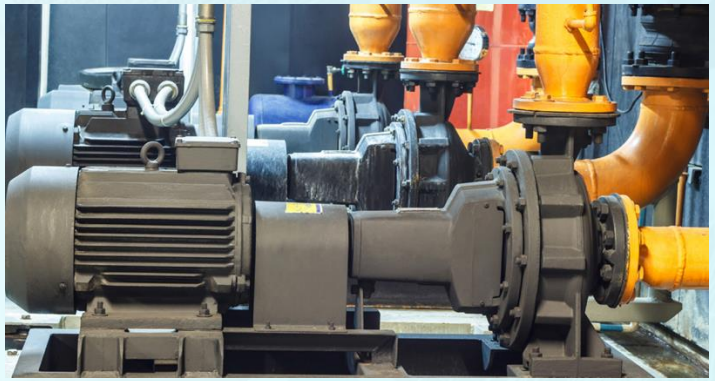
PI / CTO: Randall King

Roger Jungerman

Operant Networks Incorporated

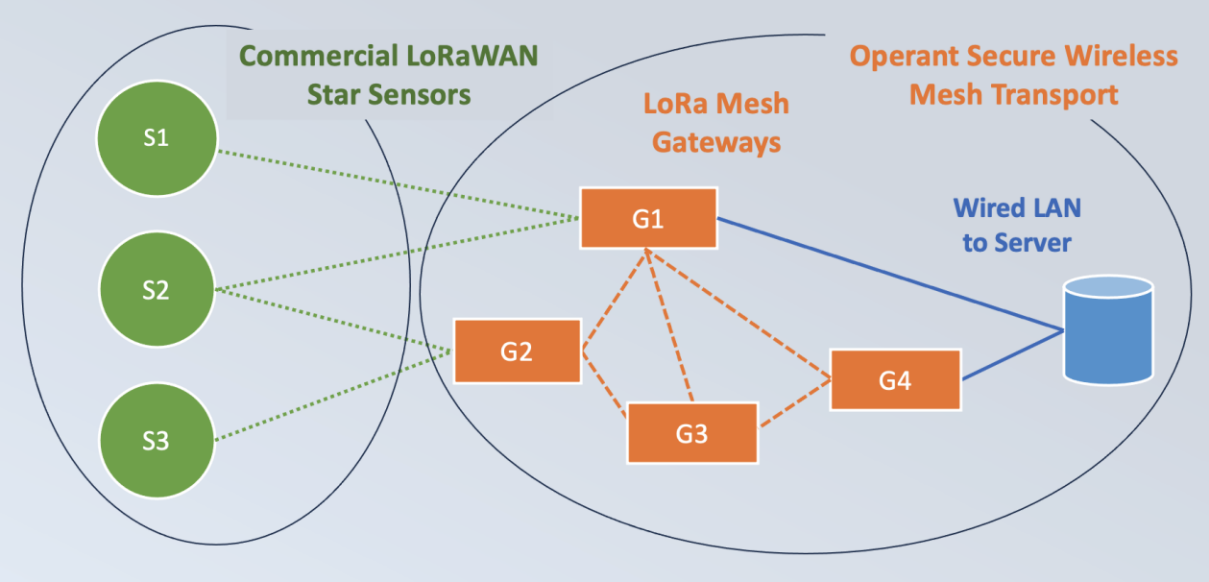
Project Overview / Motivation: Nuclear Wireless Sensors

- **Background:** Operant's Named Data Networking is currently deployed for the secure transport marketing telemetry data from Constellation existing nuclear plants to the control center.
  → This project expands this transport to wireless nuclear sensors.
- **Problem:** Monitoring and predictive maintenance sensors are needed to extend nuclear plant lifetime but retrofit wiring costs are extremely high. Wireless sensors show promise.
  - Vibration, pressure, temperature, and wireless gauge reader sensors.
  - Plant shielding attenuation and interference make reliable wireless NPP connections difficult.
- **Benefits:** Reduced personnel expenses for routine monitoring and predictive maintenance for increased up-time and fewer repairs.



Project Overview / Motivation: Nuclear Wireless Sensors

- **Technology:** Operant's networking software uniquely enables extreme range wireless technology (LoRa) in an end-to-end cybersecure **mesh** topology that promises a resilient sensor network.
  - Low-cost commercial LoRaWAN sensors are used.



- **Results:** It worked!

LoRa Mesh Hardware

LoRaWAN Wireless Gauge Reader

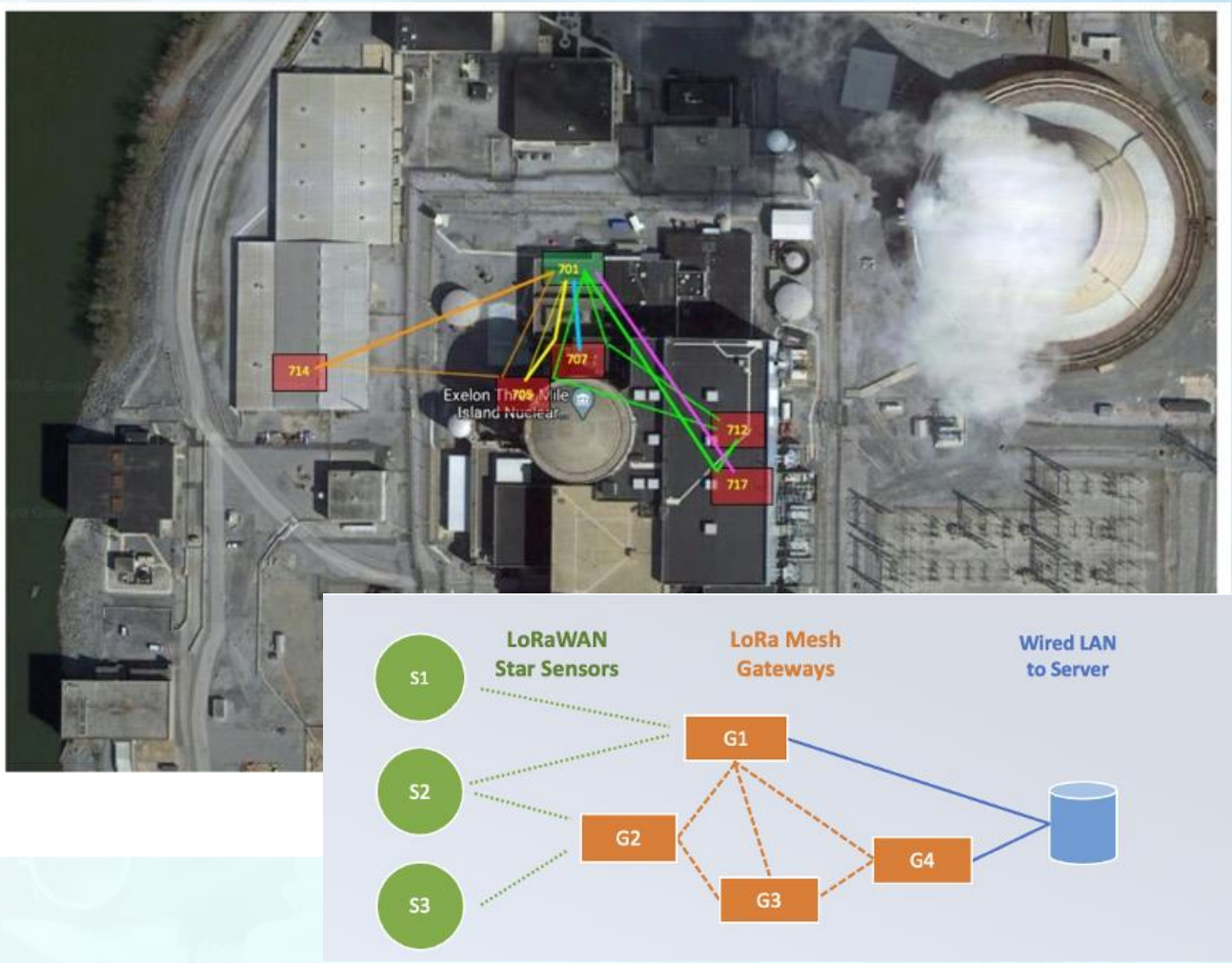
LoRa Mesh Radio Card

Ruggedized Gateway

Phase I Results – Testing in Constellation TMI Nuclear Power Plant

- LoRa successfully penetrates thick plant walls in decommissioned plant.
- Battery-powered LoRaWAN sensors could retrofit existing analog gauges, but range is limited.
- Few wired broadband backhaul locations → LoRa Mesh can likely extend range to entire plant.
- **Resilient Mesh networking needed.**

Constellation announced plans to restart the TMI Unit 1 in 2028 in conjunction with Microsoft for data center applications.



Phase II - Mesh Technology / Advanced Multi-Party Communications

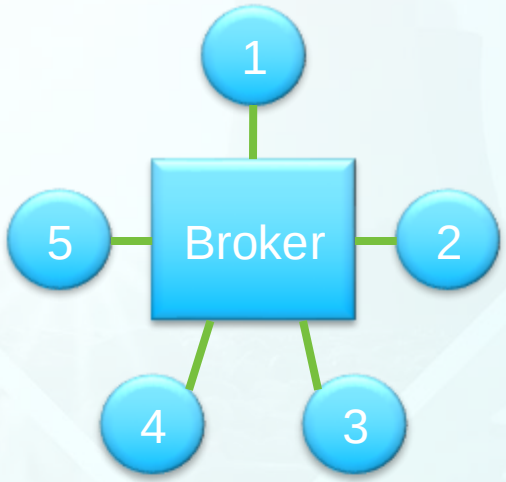
Wireless mesh provides end-to-end cybersecurity and native communications support for advanced multi-party communication patterns such as Publish/Subscribe

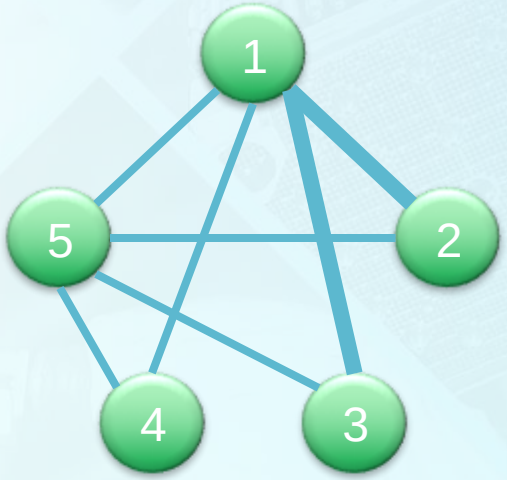
Publishers of messages, do not specify specific recipients by their identity but instead define a topic name which allow subscribers to register their interests ahead of time

TCP/IP-based Pub/Sub must send all messages to a central Broker so that each message is a simple ‘A-to-B’.

TLS security.

The Broker is a single point of failure for security and delivery.

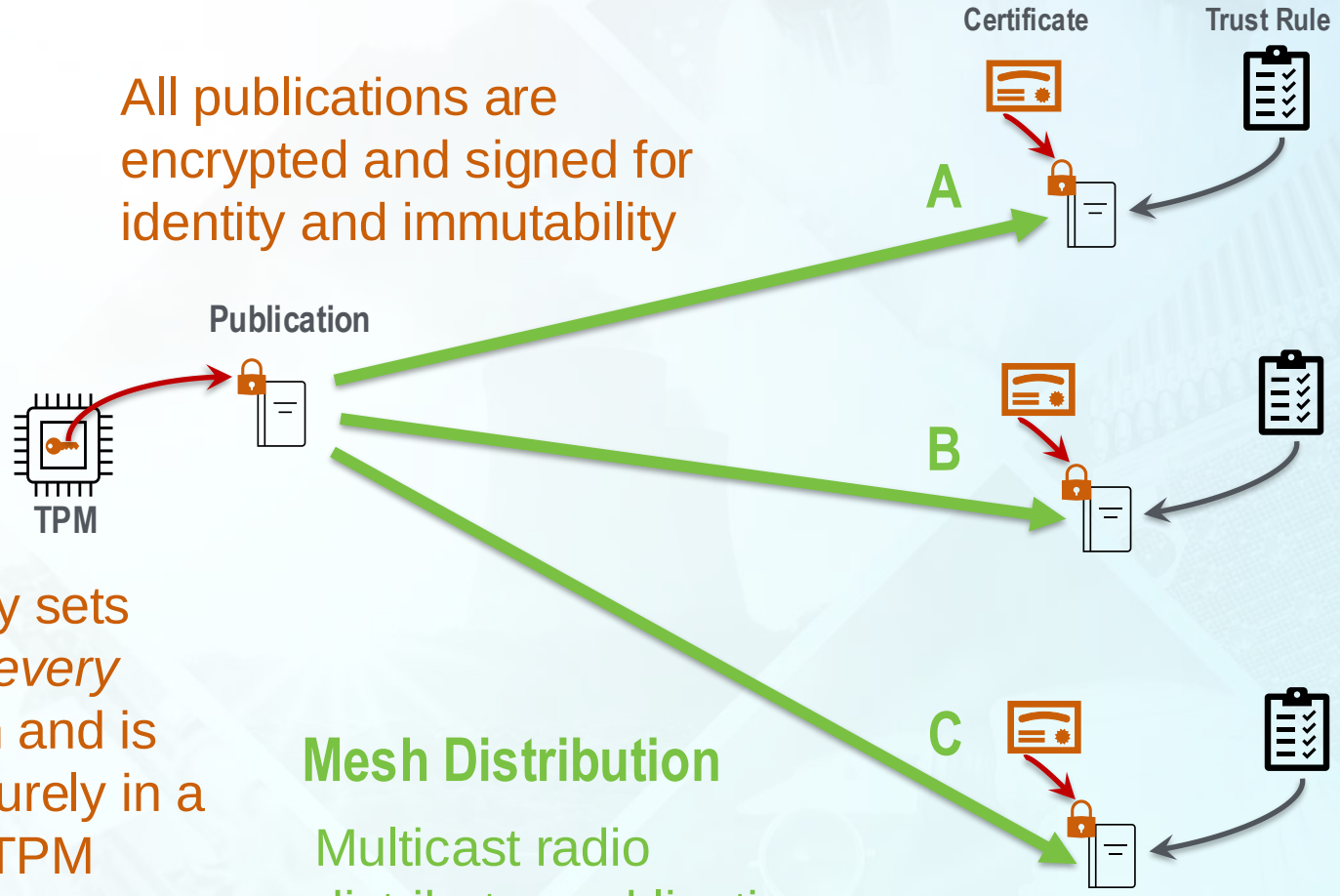




Operant Named Data Networking (NDN) Pub/Sub is fully distributed and efficiently delivers messages over any available link with forwarding, caching and end-to-end cybersecurity assured by design.

Security and Resiliency: Trust-based Pub / Sub

All publications are encrypted and signed for identity and immutability



Private Key sets identity of *every* publication and is stored securely in a hardware TPM

Mesh Distribution

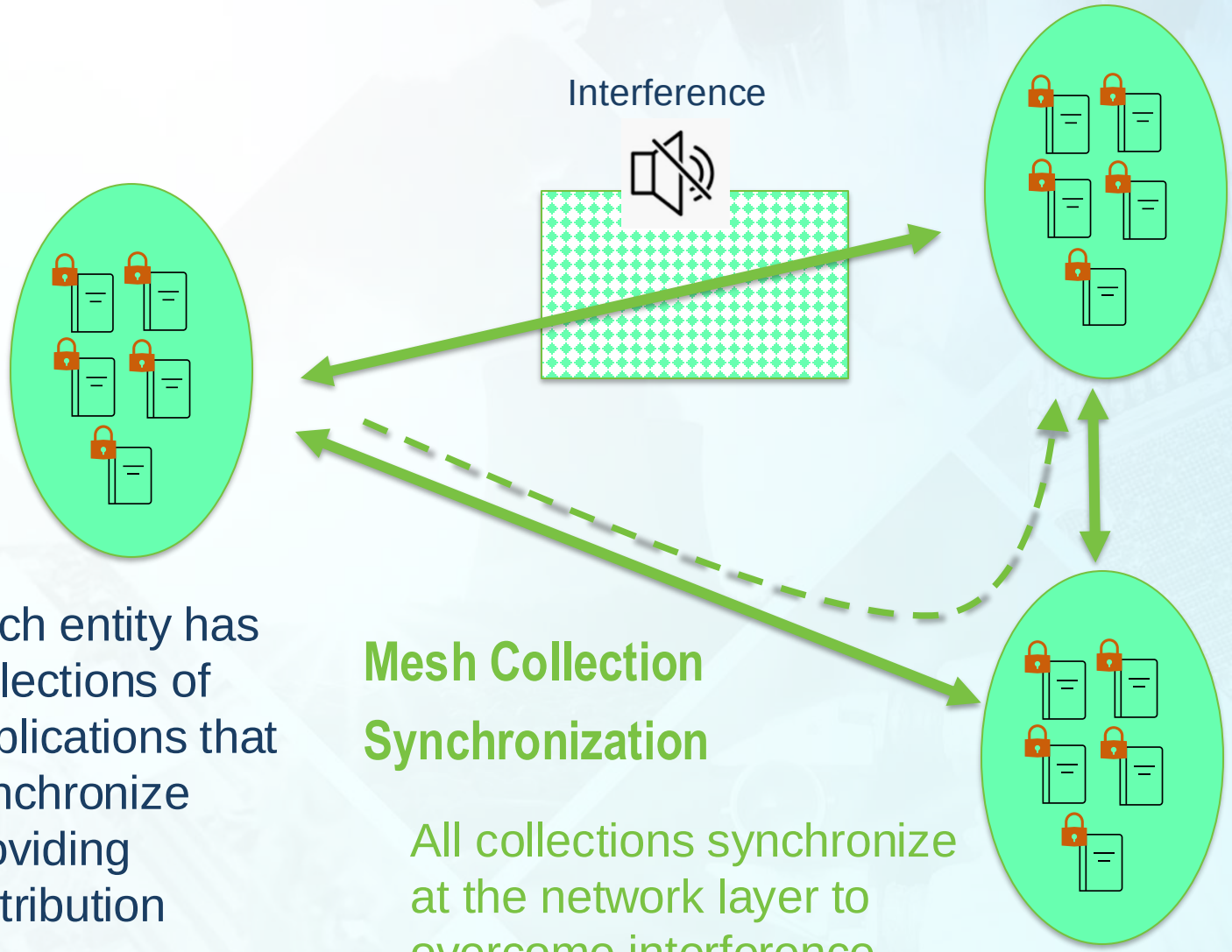
Multicast radio distributes publications to all nodes in range

Distributed Enforcement

Fully distributed enforcement validates:

- Publication ”Lock” with distributed certificates
- Distributed Trust Rule specifies *who* is authorized to subscribe to *each* publication and is enforced throughout the network

Mesh Resiliency - Synchronization and Caching



Each entity has collections of publications that synchronize providing distribution

Mesh Collection Synchronization

All collections synchronize at the network layer to overcome interference

Collections act as a “cache” if needed so that they eventually synchronize to overcome intermittent connections

System Testing at INL – Resiliency and Latency

1. ***Current Best-Practice for sensor readings in a legacy NPP is manual with a clipboard.***

2. ***DAS enables broadband radio in the plant for LoRaWAN sensors but requires high (~$2000 / ft) wired retrofit cost***

3. ***LoRa Mesh is much lower-cost***

INL Testing:

Compare the performance of the new LoRa Mesh with alternative Distributed Antenna Systems (DAS).

- Look at range and resiliency with interference and intermittent connectivity

INL Testing – Mesh vs. DAS

Gateway Name	Source WGR	Reading (Temperature °F)	No. of Packet	Time Difference (sec)
DAS+Multi-tech	WGR-5C	73.49	27	1.26
Operant	WGR-5C	73.49	27	
DAS+Multi-tech	WGR-AD	81.95	28	8.49
Operant	WGR-AD	81.95	28	
DAS+Multi-tech	WGR-5C	73.58	32	1.27
Operant	WGR-5C	73.58	32	
DAS+Multi-tech	WGR-AD	81.86	35	1.23
Operant	WGR-AD	81.86	35	

Acceptable added mesh latency:

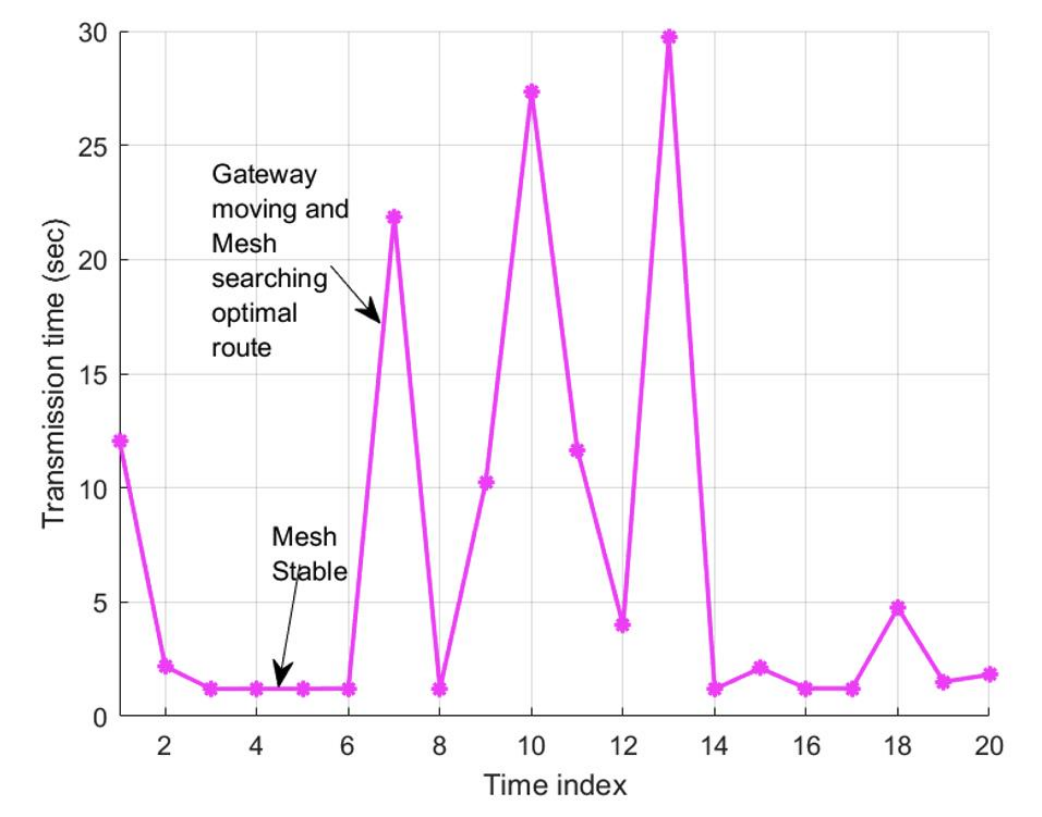
- ~ 1.25 seconds added latency
- ~ 15-minute battery-powered sensor update period

Trade-off:

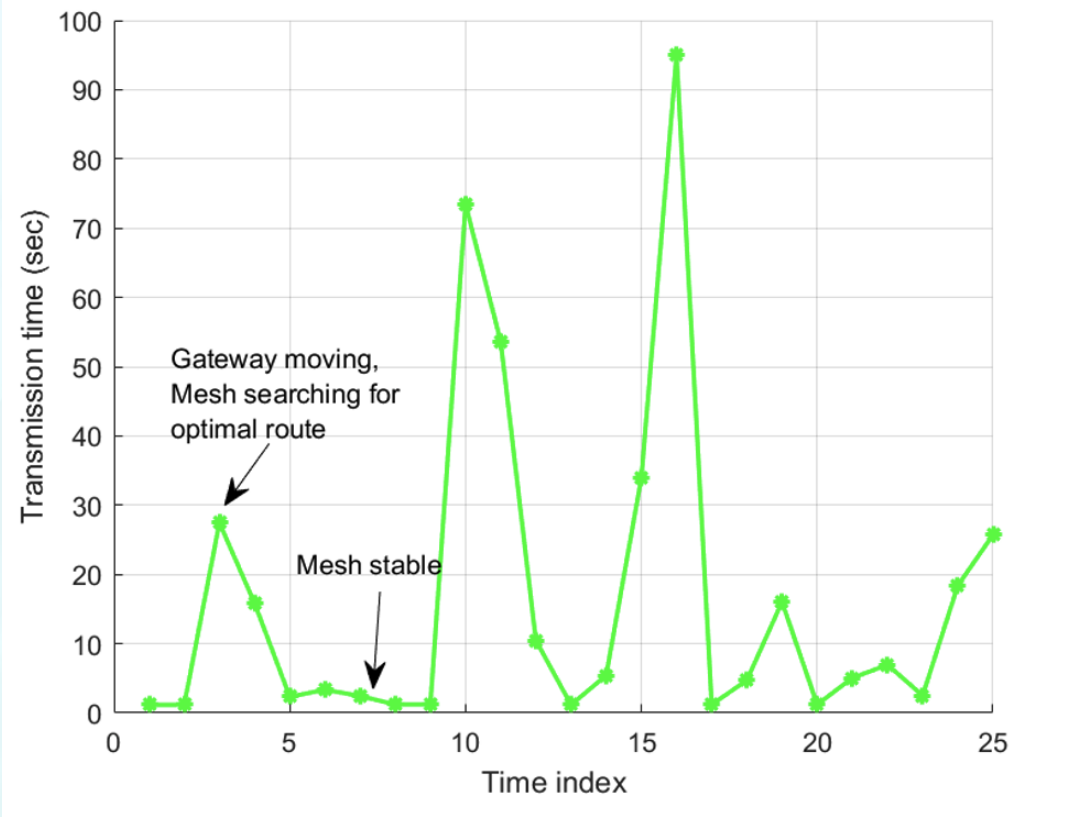
Mesh has much lower cost and installation time.

INL Testing – Resilient Reconfiguration

Robust mesh reconfiguration after network topology disruption. *No data dropped.*



Wireless Gauge Reader: WGR-AD



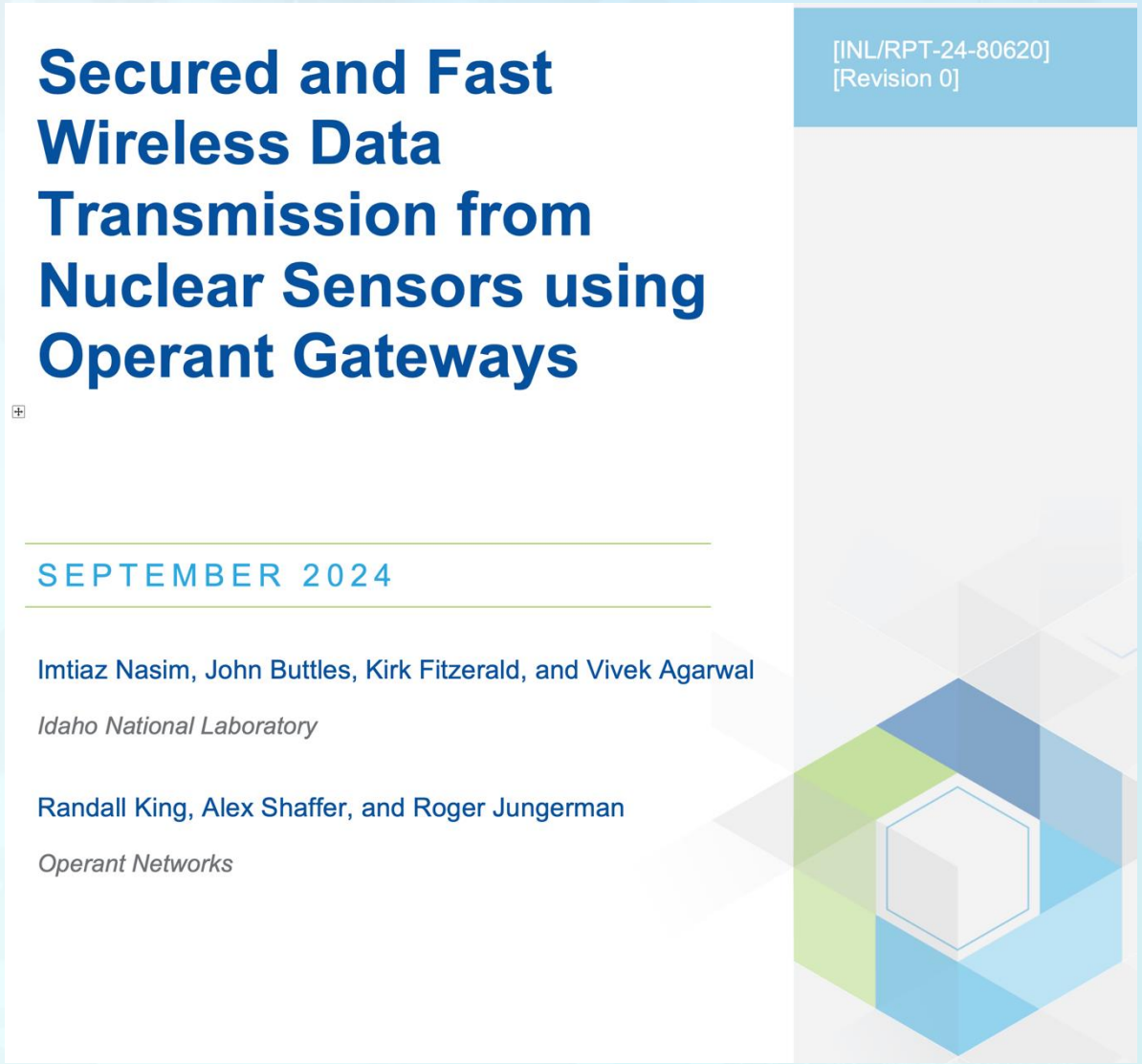
Wireless Gauge Reader: WGR-5C

INL Testing – Report: Results

- Minimal added latency compared to DAS.
- Efficiently addresses wireless connectivity
- Stable connections re-established even with gateways are moved or separated by large distances
- No data lost during reconfiguration

This current was work was focused on connectivity and resiliency, not security….

→ See comments on the next slide.



[INL/RPT-24-80620]
[Revision 0]

Secured and Fast Wireless Data Transmission from Nuclear Sensors using Operant Gateways

SEPTEMBER 2024

Imtiaz Nasim, John Buttles, Kirk Fitzerald, and Vivek Agarwal

Idaho National Laboratory

Randall King, Alex Shaffer, and Roger Jungerman

Operant Networks

National Renewable Energy Lab (NREL) Cybersecurity Testing

Test	Parameter Tested	Result
Key Strength	Cryptography	☑
Man in the Middle	Authentication	-- ← Requires re-testing
Fraudulent Publication	Authentication	☑
Publication Flooding	Transport	☑
Black Hole	**Resiliency**	-- ← Requires re-testing
Cache Attack	Authentication	☑
Cache Privacy	Encryption	☑
Traffic Throughput	Transport	☑
Transport Privacy	Encryption	☑
Publication Privacy	Encryption	☑

	INL	NREL	Combined
Resiliency	☑	?	☑
Cybersecurity	?	☑	☑

Future Work -

Recent News:

Operant awarded $5M (3-year) DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER) grant:

Improve and validate transport cybersecurity for DER Renewables, including adding post-quantum cryptography, completing the NREL cyber testing, and evaluating scaling.

Future Nuclear Opportunities:

- Develop ways to visualize and specify Trust Domains with a GUI:
  - *"Who can Access What from Whom".*
- Further development and in-plant testing of this wireless mesh for Legacy Nuclear Retrofit.
- Explore other high bandwidth radio protocols for new Advanced Reactor applications of the sensor mesh:
  - LoRa: Typically, < 50 kb/s but very long range
  - WiFi 6: Up to 10 Gb/s with moderate range

Concluding Remarks

- Demonstrated a new LoRa mesh with range and resiliency adequate for Nuclear Power Plant retrofit.
- The protocol improves resiliency and adds caching for high reliability in INL tests.
- INL testing helped refine the Operant system for mesh radio transport.
- Cybersecurity performance continues to be validated at NREL on an ongoing basis.
- Wireless mesh connectivity provides a secure, cost-effective, and resilient method of interfacing to nuclear sensors.
- Develop and test the transport for future NPP applications, including Advanced Reactors and securing AI communications.

Randy King
CTO Operant Networks
randy.king@operantnetworks.com
Cellular: (707) 326-6084
https://operantnetworks.com/about/

Thank You