ENHANCING CARGO CONTAINER SECURITY DURING TRANSPORTATION: A MESH NETWORKING BASED APPROACH

Su Jin Kim, Guofeng Deng, Sandeep K.S. Gupta, Mary Murphy-Hoye

Arizona State University, IMPACT Lab
http://impact.asu.edu/

1. Introduction

Motivation:

- **Reduce vulnerability to terrorism and theft**: Today, ~ 5 percent of the 10 million cargo containers entering the U.S. each year can be inspected.
- **Create commercial benefits**: Identify opportunities to transform the required security investments into new commercial value across the chain of custody.

Goals:

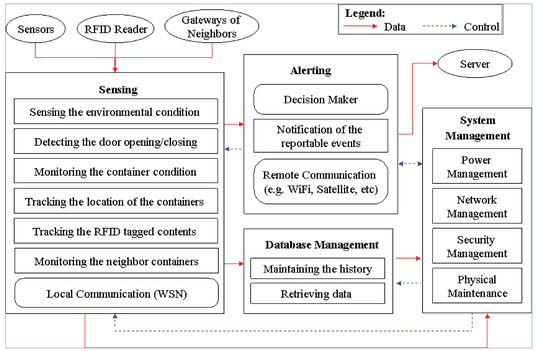
- To support the security requirements of key DHS programs: Advanced Container Security Devices and Marine Asset Tag Tracking
- To enhance the security and operational performance of the global supply chain and improve chain of custody interaction.
- To demonstrate the capabilities and constraints of emerging RF and wireless sensor network technologies for container security.
- **To shift the approach in cargo container security:**
  - ***From* securing each single container**
  - ***To* using a continuously refreshed "mesh network" of containers to enhance individual container security**.

5. Functional Architecture: Integrating RFID

Design Goal:

To support security requirements beyond sensing and communication for ACSD and MATTs, a small form factor RFID Reader capability was Integrated with wireless sensor network components.

This enabled event-triggered functionality for containers to manage the bi-directional movement of cargo.



Sensing: gather data from physical devices within a container and between gateways of neighboring containers

Alerting: make a decision on alerting and generate notification

Database Management: manage all relevant data and events

System Management: control all module operations

2. Mesh Networked Containers

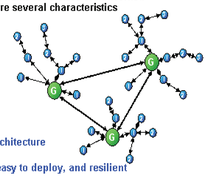
In the global supply chain, cargo containers move together in a ship, truck, or train and are stored in various configurations in a warehouse or container yard. This constant reconfiguration impacts the ability to secure an individual container throughout its lifetime.

What is a Mesh Network?**

A mesh network is a generic name for a class of networked embedded systems that share several characteristics including:

- Multi-Hop
- Self-Configuring
- Self-Healing
- Dynamic Routing
- Distributed Application Architecture
- Low power – Long-lived, easy to deploy, and resilient

With mesh networking, the vision of pervasive and fine-grained sensing becomes reality.



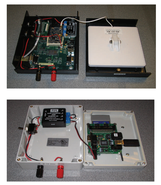
** Crossbow MicaWeb User's Manual, Rev A, Mar 08

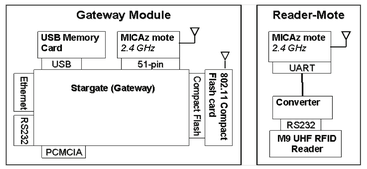
Shifting focus from securing the individual container, use the characteristics of wireless sensor networks to create a ***dynamic mesh network*** changing with each physical realignment of the containers.

Small-scale sensing and radio-enabled devices ("motes") attached in various container-based configurations autonomously interact to create a mesh.

Security of containers is enhanced through continuous interaction between neighboring "networked" containers.

6. Prototype Implementation





Reader-Mote module

- **SkyeTek M9 UHF (915MHz) RFID Reader**: small form factor, cost-efficient, energy-efficient and high performance reader
- **Crossbow MICAz mote**: supports 2.4GHz communication and local processing (command translation, duplicate reading check, etc.)
- **Converter**: supports two-way communication and voltage conversion between a 3V MicaZ mote and 5V M9 RFID reader

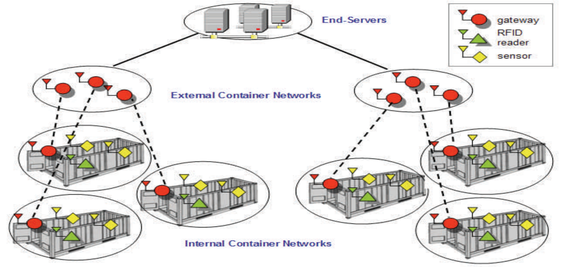
Gateway module

- **Crossbow Stargate**: single-board embedded Linux computing designed for sensor networking applications; a low-power device with various interfaces for storage and communication

Door-opening detector

- **MICAz mote with MTS300/310 sensor board**: detects door-opening/closing actions using light sensors and triggers RFID readings.

3. System Architecture: Interconnectivity



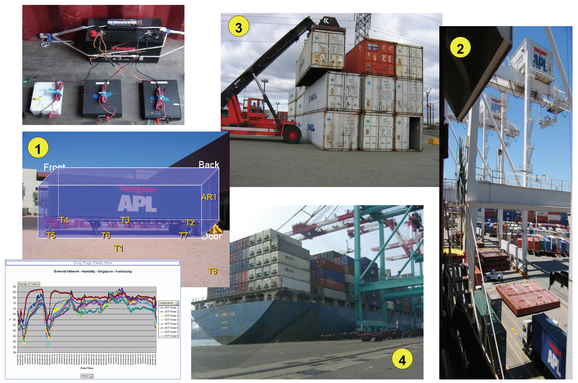
Hierarchical Structure brings *flexibility* and *scalability* to our system.

- **End-sever:** resides at a shipper's control center.
- **External Container Networks:** are formed by neighboring gateways. This network provides interface between end-servers and internal container networks.
- **Internal Container Networks:** supports the communication between devices within a container.

Internal Container Networks are ***isolated*** from External Container Networks. Any changes outside a container do NOT affect Internal Container Networks.

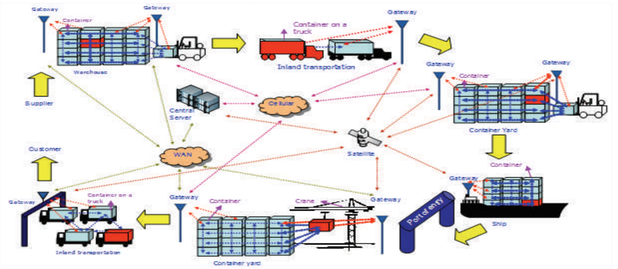
7. Live Testing and Results

1. **Single container** internal and external communication reporting sensor data – *Arizona*
2. **RF characterization** on-board ship – *California*
3. **Container to container** communications: Container Hub – *New Jersey*
4. **Containers on board ship**– *Singapore enroute to Taiwan*

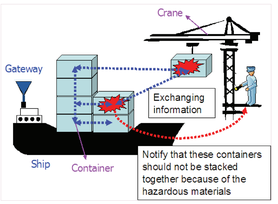


4. Scenarios: Mesh Network Benefits

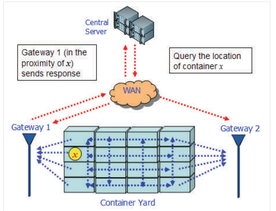
Scenario 1: End-to-end Container Lifecycle



Scenario 2: Hazardous Material Segregation

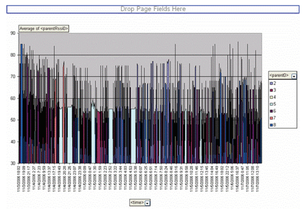


Scenario 3: Container Visibility & Loca-



8. Lessons learned and Conclusion

- Low cost maintenance-free devices with **highly energy-efficient** (parasitic power harvesting) AND **energy-intelligent** (auto-sleep mode, adjustable reading/sensing/broadcasting) capabilities are required for large scale deployment.
- Cost-sensitive **opportunistic communication protocol selection** (802.15.4 mesh, WiFi, cellular, GPRS, satellite, WiMAX) needed for en-route data and alert transmission.
- Situational (standards compliance, regulation, geo, country) **auto-selection of RFID antenna frequency and power** settings needed.
- **Viable and highly resilient mesh networks were sustained** throughout the four container tests, supporting the hypothesis of increased security through networked assets.
  - Additional studies continue across other transportation environments for scale requirement definition and resolution.
  - Information from dynamic container mesh sensor networks will provide new insights into the transportation chain of custody.



ACKNOWLEDGEMENTS: Intel, APL Logistics, MIT, Arch Rock