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

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

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.
- Create shared value: Enhance the security and operational performance of the global supply chain.
- Shifting focus from securing the container to enhancing the security and operational performance of the global supply chain.

Goals:
- To support the security requirements of key DHS programs: Advanced Cargo Security System (ACSS) and Maritime Advanced Technologies and Tactics (MATTs).
- 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: To using a continuously refreshed “mesh network” of containers to enhance individual container security.
- To support security requirements beyond sensing and communication for container security.

Design Goal:
- To shift the approach in cargo container security: To using a continuously refreshed “mesh network” of containers to enhance individual container security.

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 term for a class of underground communication approaches that share non-radiative media, including:
  - Low-power (802.15.4 mesh)
  - Low-power, long-haul, optical or wireless

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.

Strengthening focus from securing the container to enhancing the security and operational performance of the global supply chain.

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.

3. System Architecture: Interconnectivity

Hierarchical Structure brings flexibility and scalability to our system.

End-server: resides at a shipper’s control center.

External Container Networks: are formed by neighboring gateways. This external 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.

4. Scenarios: Mesh Network Benefits

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 ACSS and MATTs, a small form factor RFID Reader capability was required security investments into new commercial value across the chain of custody.

Goals:
- To support the security requirements of key DHS programs: Advanced Cargo Security System (ACSS) and Maritime Advanced Technologies and Tactics (MATTs).
- 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: To using a continuously refreshed “mesh network” of containers to enhance individual container security.
- To support security requirements beyond sensing and communication for container security.

6. Prototype Implementation

Reader-Mote module:
- SkyTag M2 UHF (815MHz) RFID Reader: small form factor, cost-efficient, energy-efficient and high performance reader
- Crossbow Mica2 mote supports 2.4GHz communication and local processing (command translation, duplicate reading check, etc.)
- Converter: supports two-way communication and voltage conversion between a UHF Mica2 mote and 9V 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:
- MICA mote with MTS30/310 sensor board: detects door-opening/closing actions using light sensors and triggers RFID readings.

Acknowledgements: Intel, APL Logistics, MIT, Arch Rock