Intelligent Networked Containers for Enhancing Global Supply Chain Security and Enabling New Commercial Value[†]

Su Jin Kim, Guofeng Deng, Sandeep K.S. Gupta
School of Computing and Informatics
Arizona State University
Tempe, Arizona 85281, USA
Email: {su.kim,guofeng.deng,sandeep.gupta}@asu.edu

Mary Murphy-Hoye
Intel Corp.
Chandler, AZ 85226, USA
Email: mary.c.murphy-hoye@intel.com

***Abstract*—Due to the global nature of today's economy, cargo containers are the most commonly used form of transportation for the world's trade. Many government initiatives, regulations and mandates have introduced new requirements for cargo security since the events of 9/11. These necessary security investments for containers can produce new advantages in the global supply chain and the participating industry partners. However, the existing systems which have been developed for ecosystem players are not yet sufficient to address all identified security issues. In this paper we explore a new set of business models, architectures, and emerging technologies that together we believe create a new level of security. First, we propose a system architecture using emerging technologies such as RFID and Wireless Sensor Networks to enhance the security of each container via the creation of ad-hoc dynamic container networks. Second, we describe our prototype implementation to demonstrate the technology capability and constraints. We also discuss lessons learned from the real-life tests. From our experiments, we believe that our approach can achieve the security goals driven by the government as well as create new business value for global supply chain participants.**

I. Introduction

Today, there are more than 20 million cargo containers moving around the world each day [1]. Cargo containers transport 90% of the world's trade and more than 10 million cargo containers enter U.S. ports each year. However, some reports have stated that only 5 percent can be inspected with today's capability [2]. Since the events of 9/11, numerous government regulations, initiatives, and mandates have emerged for container cargo, including: Automated Targeting System (ATS) [3], Customs Trade Partnership Against Terrorism (C-TPAT) [4], Container Security Initiative (CSI) [5], and Smart & Secure Trade lanes (SST) [6]. For example, one program initiated by the Department of Homeland Security (DHS) in 2004 is the Advanced Container Security Device (ACSD), focusing on the detection and reporting of container wall breaches to enhance the security in U.S. ports [7]. Another program defined by DHS in 2004 is the Marine Asset Tag Tracking System (MATTS), which is aimed at universal tracking of cargo in the marine environment [8]. Today, most container security devices focus on detecting container intrusion and tracking of each cargo container or package. In order to address these security issues and respond to the government regulations, we propose to take advantage of the fact that containers are in close physical proximity while in transit or stacked in container yards or in the port. Figure 1 shows containers stacked in a port awaiting ship loading. *Instead of focusing on the security of each individual container in isolation, we suggest creating a dynamic network among these containers changing with each physical realignment.* In addition, container network communication to ocean- or land-based infrastructure can also be provided in a reliable and efficient way. The belief is that the security of containers will be enhanced by this interaction between neighboring networked containers.

Fig. 1. Stacked Containers

While the security requirements of DHS are a primary motivation, there must be additional commercial benefits to enable the business investments required for scale to occur. In the global supply chain, lost packages and damage to goods in transit can result in heavy loss and delay. These networked intelligent containers can provide *end-to-end visibility* from a supplier to end customers via the networked tracking and sensing capabilities. This end-to-end visibility can enhance the operational performance and efficiency as well as the security of the global supply chain.

In addition, the transportation ecosystem is a disparate and loosely coupled collection of players, with distinct roles and

[†] This research is supported in part by Intel Corp.

responsibilities. Currently, there is no comprehensive method for understanding and managing the history of the conveyance from origin to destination available to the Chain of Custody (CoC). However, using intelligent containers, this data could be recorded and maintained. Because of these reasons, we believe that intelligent containers could bring collateral benefits to the supply chain and the CoC.

To support the security requirements of Homeland Security and enhance the commercial benefits in business, we propose to use Wireless Sensor Networks (WSN) and Radio-Frequency Identification (RFID). RFID technology supports the ability for automatic and unique identification. Multi-level tracking (of products, packages, pallets, containers, etc) can be accomplished through RFID tagging by rethinking the size, placement, and use of the RFID infrastructure. WSN provides the sensing capabilities to monitor container's conditions and the communication capabilities to transmit information across the container network and beyond to existing traditional infrastructure. Therefore, these technologies may provide the sensing and tracking required for intelligent containers.

To explore these possibilities, this paper first examines a new set of business models as well as assesses the intersection of the requirements for DHS programs such as MATTS, CSD, and ACSD. Second is assessment of the viability of a system architecture using WSN and RFID to support key DHS security requirements and enhance the supply chain. Third, to demonstrate and understand the technological capabilities and constraints in greater depth, we have implemented a prototype system using currently available technology. Fourth, since successful live tests in real environments (in container yards and on-board ship) have provided additional insight, we have suggestions and ideas based on these experiences and lessons learned that we believe will be valuable for future work.

II. Functional Requirements for Intelligent Containers

First of all, intelligent containers should be able to support security requirements driven by government regulation. In this section, we explore the intersection of the requirements of related DHS programs used to inform our system design.

ACSD and MATTS, two major programs initiated by DHS Homeland Security Advanced Research Projects Agency (HSARPA), have different objectives and requirements with some key overlaps and synergies.

The objective of the ACSD program is to provide the next generation of maritime shipping container security devices with multiple sensing modalities, smart condition monitoring, automated alerting, and advanced communications [7]. The proposed devices must provide a quantum increase in the level of protection and assurance. Primary emphasis is on assuring the physical security of the container including container breach and status of any seals or locks. Secondary emphasis is on detection of certain prohibited cargoes, internal ambient conditions, manipulation or change of state of the contents, and recording container interaction history. The Container Security Device request (CSD) is for the identification of currently available inter-modal shipping container devices [9]. CSD has very similar goals with ACSD program, but requires less functionality.

MATTS focuses on developing and prototyping Tag System using RF (Radio frequency), IR (Infrared) or other modality for shipping containers in the marine environment in order to facilitate universal tracking. The MATTS is a multi-modal communication gateway for ACSD to provide global remote communications and tracking information for a container. A recently published RFI (Request for Information), *Single Pricing Structure for Global Connectivity to Cellular Data Services To Support Marine Asset Tag Tracking System (MATTS) Communication*, is intended to address the communication requirements of these devices [10]. In order to send alarm and status information, HSARPA proposed to use the existing cellular data services with highly reliable global connectivity for the MATTS devices.

Table I summarizes the functional requirements of CSD, ACSD and MATTS devices. We applied the superset of these functional requirements of CSD, ACSD, and MATTS for our system design.

III. System Design

A. System Architecture

In order to meet requirements of CSD, ACSD, and MATTS devices, we propose a hierarchical architecture for intelligent containers. In order to facilitate container-to-container interaction and container communication to cross-enterprise infrastructure, we also need to address the physical constraints on the system (i.e. due to high interference from metal and dense materials in and around the containers).

Using RF technologies that do not require line of sight and using the physical environment constraints (such as metal) as a mechanism to enhance the *performance* of the dynamic networks also provide a new approach to this proposed system architecture.

In order to describe the detailed architecture, a few key definitions are required. A **mote** is a tiny wireless computing platform with a CPU, memory, storage, I/O, and radio components, optimized for long life on low power - often battery operated [11]. It enables distributed sensing of the physical world and communicates through its self configuring 802.15.4 *mesh* network technology. 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, and low power (long-lived, easy to deploy, and resilient). With mesh networking, the vision of pervasive and fine-grained sensing becomes reality [11].

A mesh network delivers the network *scalability* into our hierarchical architecture because it can be easily expanded as needed. In addition, a hierarchical architecture is suitable for *flexibility* and *scalability*. Containers are moved together in a ship, and then into ports, container yards trucks, or onto another ship. Therefore, containers need to form and participate in networks with their new neighbors *dynamically*.

TABLE I
THE FUNCTIONAL REQUIREMENTS OF CSD, ACSD, AND MATTS [7] [8] [9]

Function		CSD	ACSD	MATTS
Sensing	Detection of door opening/closing/removal	Yes	Yes	Yes
	Detection of breaching of the container walls, floor, or ceiling (6 side)	No	Yes	No
	Monitoring container seal or lock status	Optional	Yes	Yes
	Sensing loading/unloading of RFID tags	No	Yes	No
	Sensing environmental conditions (temperature, humidity, shock, etc)	Yes	Yes	Yes
	Detection of a person or animal	No	Yes	No
	Tracking and monitoring the location of the container	Optional	No	Yes
Alerting	Monitoring the sensors for reportable events	Yes	Yes	Yes
	Notification	Yes	Yes	Yes
Data	Recording and maintaining alert events	Yes	Yes	Yes
	Input and retrieval of data	Optional	No	Yes
Communication	Local and remote communications	Yes	Yes	Yes
Life-time	4.5 trips per year (21 days duration & 7 days loading/unloading)	No	30,000 hours	1 year
Cost	per transit	$50.00		

The network inside a container is designed to remain isolated from the dynamic networks outside a container. Any changes inside a container should not affect other networks in our hierarchical architecture as well.

In mesh networking, multiple nodes are interconnected through the network. Because this creates redundant network paths, the mesh network enhances the network *reliability*. Besides, the distributed database system in our hierarchical architecture improves the overall reliability of the system.

To support *better connectivity*, the hierarchy includes a gateway supporting multiple network protocols (e.g. 802.15.4, 802.11, 802.16, satellite, cellular, etc) for transmission of the mesh networks' information. These protocols can be dynamically selected based on current transmission requirements (e.g. alerts, data push, instructions, etc), and the current availability or efficiency of communication.

Figure 2 shows the proposed hierarchical structure which consists of the *Server/Data Center*, *External Container Network*, and *Internal Container Network* and Figure 3 shows *External Container Network* and *Internal Container Network* in detail.

- *Server/Data Center*: resides at a shipper's control center or a DHS facility. It receives information (e.g. the environmental condition, containers' status, alert, etc) from gateways via the External Container Network.
- *External Container Network*: provides communication between gateways in a ship/truck/trail. The External Container Network also supports the communication interface between the Server/Data Center and Internal Container Network.
- *Internal Container Network*: supports the communication between devices within a container.

B. Internal Container Networks

There are two types of internal sensing and communication networks. The first provides an unique identifier capability through the use of a small form factor RFID reader connected to a WSN sensor device. The second network provides a wide variety of sensing capabilities participating in their own mesh network inside the container.

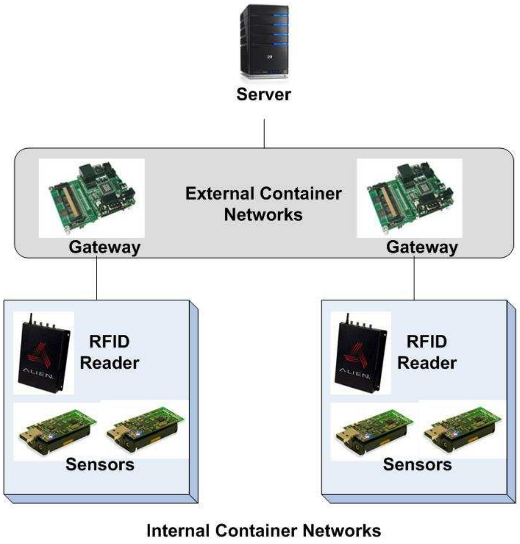


Fig. 2. Hierarchical Network Structure for Intelligent Containers

The *Identifier Internal Container Network* contains an RFID reader and motes placed within a container. Each container also has a low-power mobile gateway, (in this case a CrossBow StarGate device [12]) which provides the external communication interface between the internal network and the external infrastructure. A gateway is located on a container door and wirelessly communicates with motes and the RFID reader. The gateway can send commands to those devices participating in this container's identifier internal mesh network and gather information from them. To ensure a more reliable and efficient architecture, all sensor network data collected by the gateway can also be saved into its local database and then sent to the remote Server/Data Center periodically or upon request.

In summary, an RFID reader placed inside a container door provides visibility into the physical cargo IDs moving

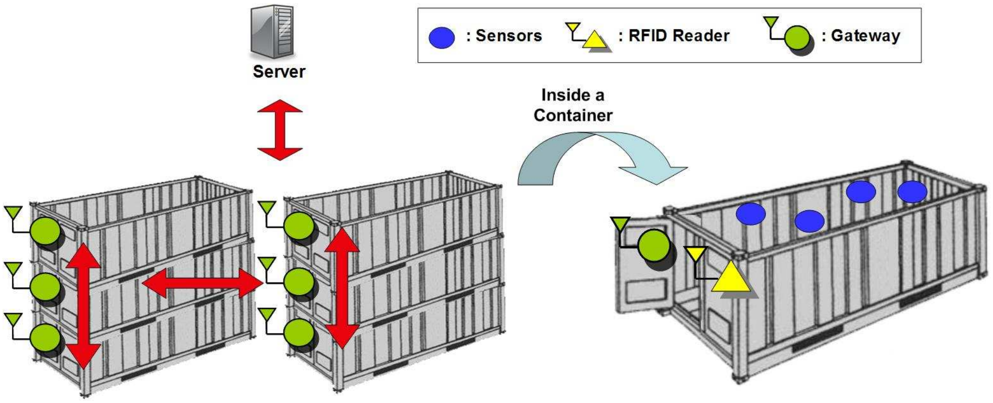


Fig. 3. Internal and External Container Networks

in and out of the container. RFID tagging on a container's doors enables location tracking of that particular container. Therefore, RFID technology applied in different manners can support tracking contents through the hierarchy of cases, boxes, containers, ships, etc.

The *Sensing Internal Container Network* can contain a wide variety of motes providing continuous or event-triggered condition monitoring capabilities in the container. This mesh network also requires access to external communication infrastructure via a multi-protocol gateway device.

C. External Container Networks

External Container Networks are created via the dynamic interaction of externally mounted gateways. These networks form and change due to proximity as well as to the current physical environment conditions. The ability to interact and create networks among containers leads to enhanced security. In addition, by using the container stacks to communicate up and out of the ship via the mesh network, a container can compensate for a lack of clear line of sight for GPS sensing. The ad-hoc external mesh networks between containers provide an efficient mechanism for sharing information from outside and moving information through the mesh up and out of the ship.

IV. Functional Architecture

In this section, we describe the functional architecture for intelligent containers. Figure 4 illustrates the functional architecture which consists of four modules: sensing, alerting, database management and system management.

A. Sensing

The sensing module gathers the data from the motes, RFID reader and others devices within a container and provides the following functions:

- *Sensing the environmental condition*, such as temperature, fire, shock, humidity and light.
- *Detecting the door opening and closing*. The devices require the detection of door opening/closing actions.
- *Monitoring the container condition*, such as container integrity or damage.
- *Tracking the location of the containers*, including the period which the container is stacked on a ship, train, or truck.
- *Tracking the RFID tagged cargo contents* during loading/unloading.
- *Monitoring the neighboring containers*. The information from neighbors can be used to improve the alerting.

The sensing module uses the *local communication* such as WSN between devices in a container in order to exchange data.

B. Alerting

Based on the data from the sensing module, the alerting module makes a decision on alerting. One of the simple solutions is to alert when the sensing data is under or over a certain threshold. The alerting module requires the *notification* function, which reports the extreme conditions or important events to the Server/Data Center through the *remote communication* (WiFi, Satellite, etc). The alerting module also provides the signal processing to increase probability of detection and reduce the false alarm rate. For more accurate and intelligent decision, it could access the history of the relevant data in the database management module. The detection can be improved by collecting and analyzing data from neighbors via the dynamic external container networks. Increasing the probability of detection while reducing the false alarm rate is a challenging issue. This module could also interact with the sensing module to change sensing rates or trigger a special sensor.

C. Database Management

The database management module has two functions:

- *Maintaining the history*, such as the time stamped records of all alert events, sensor readings, log of loading and unloading, and bills of lading.
- *Retrieving data* from database by a request.

To record the history of all data, this database management module will interact with the alerting and sensing module. All time stamped data will be used to track and monitor the current container trip. The recorded data could be accessed by

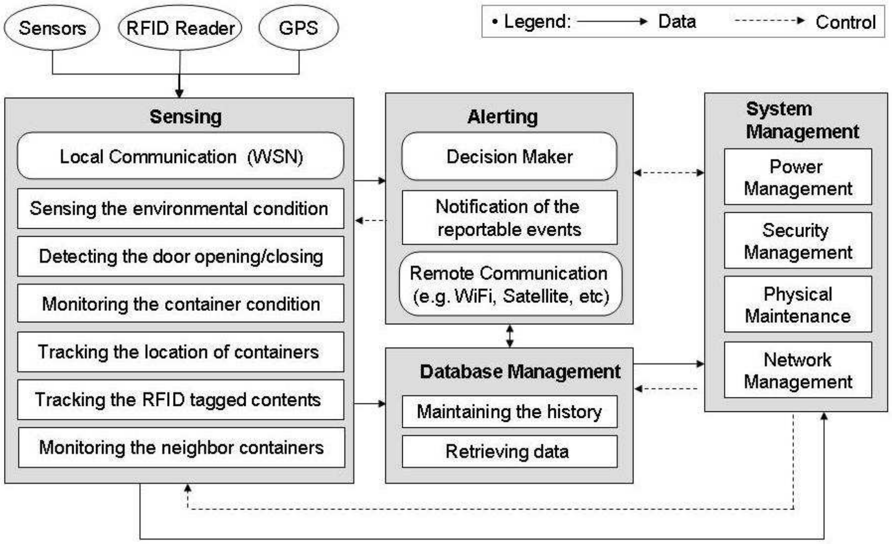

Sensors
RFID Reader
GPS
• Legend: Data Control
Sensing
Local Communication (WSN)
Sensing the environmental condition
Detecting the door opening/closing
Monitoring the container condition
Tracking the location of containers
Tracking the RFID tagged contents
Monitoring the neighbor containers
Alerting
Decision Maker
Notification of the reportable events
Remote Communication (e.g. WiFi, Satellite, etc)
Database Management
Maintaining the history
Retrieving data
System Management
Power Management
Security Management
Physical Maintenance
Network Management

Fig. 4. Functional Architecture

the server or authorized users during a trip and uploaded to the server after a trip.

D. System Management

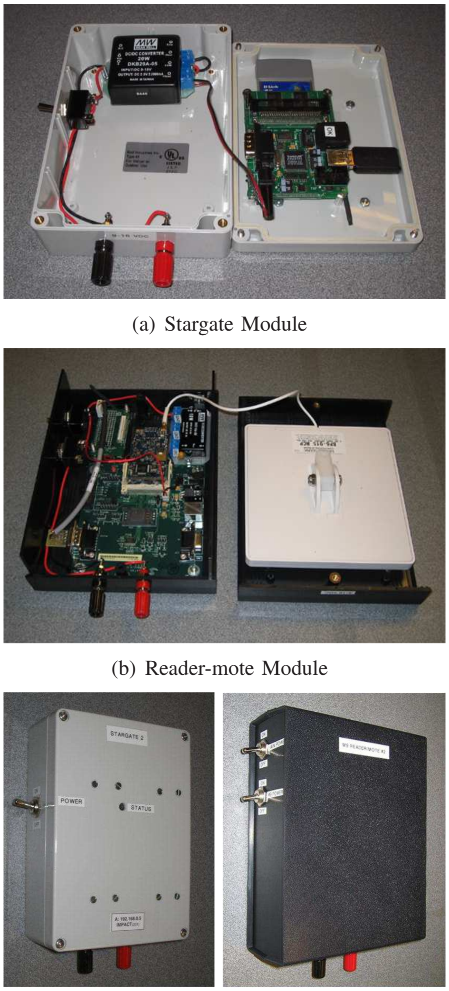
The system management module controls all modules in a system to help their operations.

- *Power Management*. For an energy-efficient system, it could decrease sensing rates or turn off sensors if battery is critically low.
- *Security Management*. All communication in a system should be secured against eavesdropper and unauthorized users.
- *Network Management* supports dynamic and reliable networks. It is incharge of identifying connectivity problems and reporting on network performance.
- *Physical Maintenance* is in charge of ensuring all hardware components are functioning and reporting on expected outages/failures as well as battery replacements.

V. Prototype Implementation

To demonstrate the technological capabilities and constraints of this proposed system architecture, we implemented a prototype using current commercially available technologies. Within a container, there are: a CrossBow Stargate device [12] which acts as the gateway, a Door-Opening CrossBow MicaZ mote [13] which detects door opening/closing actions, a Reader-mote Module which reads RFID tags, and several Arch Rock TelosB motes [14] to monitor the container's condition. A PDA-based application was also implemented to control and monitor the system remotely. To ensure short-term survivability at sea, the devices were packaged with waterproof materials.

Figure 5 shows our prototype implementations for the Stargate Module and Reader-mote Module.


(a) Stargate Module

(b) Reader-mote Module

(c) Waterproof Packages

Fig. 5. Prototype Implementation

A. Gateway Implementation

The CrossBow Stargate gateway is a low-power mobile computing and communication device [12]. It is a powerful single-board embedded Linux computer designed for sensor signal processing, control, and wireless sensor networking applications. The Stargate can provide various communication and processing capabilities through USB, PCMCIA, CF (Compact Flash), and 51-Pin interfaces.

Using the 51-pin Stargate interface connected to Crossbow's MicaZ mote allows 2.4 GHz 802.15.4 communication between the gateway and the mesh networks. The Stargate is also loaded with a Postgres SQL database system and a USB memory card to store sensed data during the on-board ship trial. The wireless 802.11 CF card provides remote WiFi access to the Server/Data Center. A GPRS PCMCIA modem and GPS receiver mounted to a MicaZ mote can also be used to get exact location of the container.

B. Door-Opening Sensors

In this application, an RFID reader only operates during loading/unloading. The wireless sensor network components are designed from hardware, through operating system, and applications to consume minimum power and keep the devices in sleep mode as much as possible. The mobile RFID readers can be triggered to read by an external event (motion or light detection), therefore limiting operation to loading and cargo inspection. Accurately detecting these events will improve energy efficiency as well as operational performance.

To trigger RFID reading, we used a standard MicaZ mote light sensor on a Crossbow MTS300/310 sensor board [15] to create a container door open / close event. The MicaZ mote mounted inside the door senses light in the container when the door is opened and communicates to the Stargate the door opening and closing when the value is over and under the threshold, respectively. (Sensors tuned for the appropriate motion patterns would be used in a final implementation.)

C. Reader-mote Modules

The SkyeTek UHF M9 is a small form factor, cost-efficient, energy-efficient and high-performance RFID reader [16]. We integrated the M9 RFID reader with a MicaZ mote to provide the wireless communication and computation capability. We connected the RS-232 serial port of the M9 RFID reader and the UART of the MicaZ mote using the Superdroid Robots's converter cable [17]. This converter cable provides two way communications and the voltage conversion between the M9 RFID reader (5V) and the MicaZ mote (3V).

The MicaZ mote receives `Start Read` and `Stop Read` commands from the Stargate (based on door open/close events) and forwards these commands to the M9 RFID reader. During reading process, the M9 RFID reader immediately passes RFID Tag information (e.g. IDs) to the MicaZ mote without freshness checking. On the MicaZ mote, the duplicated IDs are eliminated and only fresh readings are sent out to the Stargate.

TABLE II
GOVERNMENT REGULATIONS FOR UHF RFID [18]

Region	Power Levels	Frequency Bands
Singapore	0.5 Watts ERP	866-869 MHz
Taiwan	0.5 Watts ERP	922-928 MHz
Philippines	0.5 Watts ERP	918-920 MHz
Europe, South Africa	2 Watts ERP	865.6-867.6 MHz
China	2 Watts ERP	840.5-844.5 MHz
U.S	4 Watts EIRP	902-928 MHz
Australia	4 Watts EIRP	920-926 MHz
New Zealand	4 Watts EIRP	864-868 MHz
Japan	4 Watts EIRP	952-954 MHz
South Korea	4 Watts EIRP	908.5-910 MHz

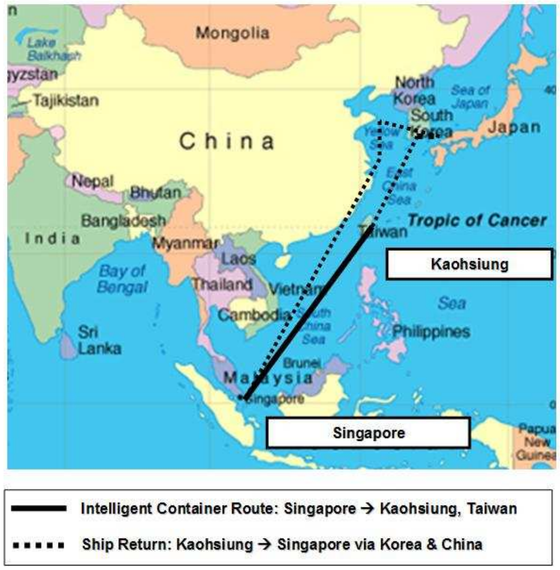


Fig. 6. Route for the test from Singapore to Taiwan

The Stargate can also send commands to change the RF frequency and output power of the reader during the trip based on physical location information. This ensures compliance to regulated reading power levels and frequency bands in different countries. Table II summarizes the regulations of the power level and frequency bands [18]. The power is expressed either as EIRP (Effective Isotropic Radiated Power) or ERP (Effective Radiated Power). Here, the European regulated power level of 2 Watts ERP is equivalent to 3.28 Watts EIRP [19].

VI. Experimental Results

The Reader-mote-Gateway assembly was unit and system tested first in a standalone container over several months, then in a container yard in a 3x3 stacked container configuration to assess inter-network interference and network communication strength, and finally in port before and after a multi-day shipment between Singapore and Taiwan shown in Figure 6.

A. RFID Read Ranges

For our test from Singapore to Kaohsiung, Taiwan, extensive analysis was required to determine the correct combination of RFID reader, antenna and RFID tag to support the read ranges required for container door coverage and compliant with the

TABLE III
RFID READ RANGES

Antennas	UHF RFID Tags		
	EPC Class 1 Gen 2		ISO 180006B
	Alien [20]	Avery [21]	AWiD [22]
Cushcraft S9028PC (8 dBiC) [23]	20 inches	37 inches	70 inches
Symbol Z1747 (6.4 dBdc) [24]	16 inches	37 inches	75 inches
Sensormatic (6.75 dBd) [25]	43 inches	88 inches	86 inches

0.5 Watts ERP requirement. First, we measured the average read ranges of a SkyeTek M9 UHF RFID reader [16] with the maximum output power (27 dBm). According to the datasheet from SkyeTek [16], the M9 reader can reach approximately 3.5m (about 138 inches) with 27 dBm output power and 6 dBi antenna. However, we observed the actual read range from our experiment shown in Table III was much smaller than the values from SkyeTek. We used three different types of UHF RFID tags (Alien EPC Class 1 Gen 2 [20], Avery EPC Class 1 Gen 2 [21], and AWiD ISO 180006B [22]) and three different types of external antennas (Cushcraft S9028PC 8 dBiC [23], Symbol Z1747 6.4 dBdc [24], and Sensormatic 6.75 dBd [25]). Second, we adjusted the output power of these three antennas to 0.5 Watts ERP required for the test from Singapore to Taiwan. Using 0.5 Watts ERP, the average read ranges of all combination of antennas and tags are 10 - 18 inches.

From our experiments, we found that additional investigation and experimentation is required here to ensure the viability of on-board container RFID readers.

B. Energy Consumption

During our test, we confirmed that energy-efficiency will be a key gating factor to scale implementation of these battery-powered devices. Containers make several roundtrips per year, have an extended multi-year lifespan, and do not have an entity with umbrella ownership for maintenance and support. Therefore these solutions must be standalone and relatively maintenance-free, preferably taking advantage of ambient vibration to harvest power.

Since the MATTS requirements recommend at least one year lifetime with 1 year (3,000 hours) operations, and the ACSD requires 30,000 hours of annual operation, the components of a wireless sensor network solution, such as the gateway and motes need to be highly energy efficient. Unlike the gateway and motes, the RFID reader needs to support only the 760 hours needed for loading/unloading operations. As we discussed above, we can reduce energy consumption of the RFID reader using sleep mode.

To determine the actual lifetime of our system, we first measured the energy consumption of the MicaZ [13] and TelosB [14] motes used in our prototype implementation. The MicaZ mote with a MTS310 sensor board [15] attached drew 11.25 mA of current consuming a power of 33.75 mW, while the TelosB mote just drew 0.09 mA of current consuming 0.42 mW of power. As expected, this clearly shows that MicaZ is the more energy inefficient of the two. We decided to measure the actual lifetime of the MicaZ mote because the MicaZ motes were used for Door-Opening Sensors and Reader-mote modules, and also deployed inside the container. We programmed a MicaZ mote with MTS310 sensor board to broadcast a packet once every 10 seconds with sensor readings. After the readings have been broadcast the mote shifts to power saving mode (switching off radio and the sensor board). Each time the mote broadcasts sensor data (in a packet) it also forwards the current voltage level of the battery. At the start of the experiment the mote had 2 new AA batteries which measured 3.0V. We conducted the experiment till the mote started indicating a low battery around 2.0V mark. Below this mark (2.0V) we were not able to receive the transmitted signals at the distance of 4 meters. We experienced negligible packet loss at the base station which was placed about 4 meters away. Figure 7 presents the variation in the battery voltage with time. Even though the voltage value was being collected once every 10 seconds, we just show two values per day (one taking in the morning and another in the evening) to illustrate the trend. We can see that the mote lasts about 46 days before the battery on the mote has to be replaced. Obviously, reducing frequency of sensing and broadcasting data can increase the lifetime of MicaZ motes.

At the next step of our experiment, we examined the high energy consumption of the Stargate and RFID reader. The Stargate with MicaZ and AmbiCom CF WiFi card attached drew 406 mA of current consuming a power of 1827 mW. The M9 RFID reader on single reading drew 270 mA of current consuming a power of 1215 mW while a continuous reading mode drew 615 mA of current consuming a power of 2767.50 mW. During a multi-day shipment from Singapore to Taiwan, we used a large (car size) battery. However, ACSD restricts the size of a container security device so as to not reduce the volume of a container or impact handling. To meet 1 year operations requirements, the energy efficiency should be improved.

C. Lessons Learned and Future Plans

In order to prove that our approach is workable as well as refine the system architecture and increase our understanding of these technologies and the physical constraints of this demanding environment, we implemented the prototype with currently available technologies and devices. From our experimental results, we have learned many of the technology constraints as well as broader issues that must be resolved in order to support all the DHS container security requirements.

Our early architectural investigations included suitability of current sensor platforms and assessment of the current cost of various component configurations as compared to regulated cost limitations. We found that there is a need for *mobile edge computing devices* (MECD) - an hardware/software platform that helps in bridging the WSNs with backbone network. MECDs would enable cost-effective and low-power imple-

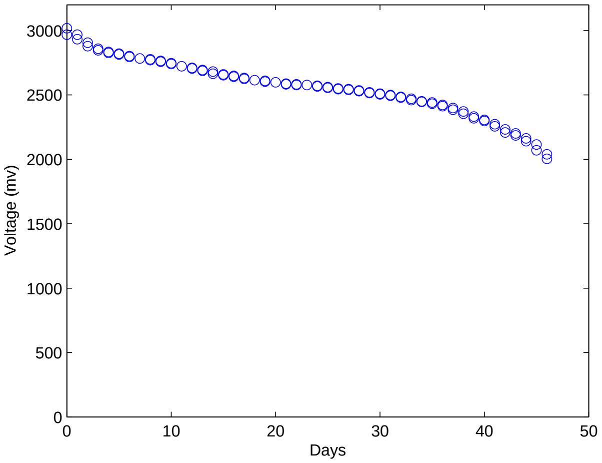


Fig. 7. Battery drain on functioning MicaZ mote over time

mentation of functionalities required by ACSD and MATTS. Current cost requirements of $50.00 US per transit is difficult to achieve with today's technology offerings. However, these RF technologies have been rapidly decreasing in cost while increasing in performance and reliability due to numerous breakthroughs in silicon, component, and solutions design.

From the experimental results, we found the RFID reading ranges were not large enough to cover a container. To address this problem, multiple readers as well as targeted antenna and tag design can be used. In addition, the highly energy efficient devices as well as management (sleep mode, adjusted frequency of reading/sensing/broadcasting) are required.

In this paper we focused mainly on the current implementation of the Identifier Internal Container Network. Extensive work has also been completed on the Sensing Internal Container Network and the External Container Network focused on sensing fusion and network dynamic behaviors. In the future, we will address the creation and maintenance of this system of networks in highly interactive, reliable, and efficient forms.

VII. Conclusions

In this paper, we proposed a system architecture for intelligent containers using a variety of RF technologies (wireless sensor networks and RFID readers). To demonstrate that the proposed system architecture could support the requirements of DHS defined CSD, ACSD and MATTS solutions, we defined a functional architecture. Future solutions potentially based on these system architecture concepts may provide the *end-to-end visibility* needed for the global supply chain and also support inter-container communication for enhanced cargo container security. Therefore, we believe that this approach may provide new value for the security community and the container shipping industry in securing and enabling the global supply chain.

Acknowledgment

We thank Richard Tyo and Scott Thomas from Intel, James Rice and Matt Malinowski from MIT, David Culler and Wei Hong from Arch Rock Corp., George Cavage from APL Logistics, and Krishna-Kumar Venkatasubramanian and Edward Raleigh from IMPACT Lab. at Arizona State University for their valuable inputs.

References

[1] "RFIDNews: Savi's RFID Licensing for Cargo Containers," May 2007. [Online]. Available: http://www.rfidnews.org/weblog/2007/05/10/savis-rfid-licensing-for-cargo-containers/

[2] "Port security: The 5% myth," Mar. 2006. [Online]. Available: http://www.americanchronicle.com/articles/viewArticle.asp?articleID=6780

[3] "Privacy impact assessment for the automated targeting system," Nov. 2006. [Online]. Available: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf

[4] "C-TPAT: Customs-Trade Partnership Against Terrorism." [Online]. Available: http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/

[5] "CSI: Container Security Initiative." [Online]. Available: http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/

[6] "RFID and Homeland Security," Dec. 2003. [Online]. Available: http://www.aimglobal.org/technologies/rfid/resources/articles/dec03/homeland.htm

[7] "HSARPA BAA 04-06 Advanced Container Security Device Program," 2004. [Online]. Available: http://www.hsarpabaa.com/Solicitations/AdvContSecDev_BAA_FINAL_508.pdf

[8] "HSARPA SBIR H-SB04.1-005 Marine Asset Tag Tracking System," 2004. [Online]. Available: http://www.hsarpasbir.com/PastSolicitationDownload.asp#21

[9] "RFI: The Container Security Device," 2005. [Online]. Available: http://www.hsarpabaa.com/Solicitations/CSD-RFI-ver-8.pdf

[10] "RFI: The Single Pricing Structure for Global Connectivity to Cellular Data Services to Support Marine Asset Tag Tracking System (MATTS) Communications," 2006. [Online]. Available: http://www.hsarpabaa.com/main/RFI-GCCDS.htm

[11] "Crossbow moteview user's manual." [Online]. Available: http://www.xbow.com/Support/Support_pdf_files/MoteView_Users_Manual.pdf

[12] "CrossBow SPB400- Stargate Gateway." [Online]. Available: http://www.xbow.com/Products/productdetails.aspx?sid=229

[13] "CrossBow MicaZ 2.4GHz." [Online]. Available: http://www.xbow.com/Products/productdetails.aspx?sid=164

[14] "ArchRock Primer Pack/IP Data Sheet." [Online]. Available: http://www.archrock.com/downloads/datasheet/primerpack-ip_datasheet.pdf

[15] "CrossBow MTS300/310 Sensor Board." [Online]. Available: http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MTS_MDA_Datasheet.pdf

[16] "SkyeModule M9 Developer Kit." [Online]. Available: http://www.skyetek.com/ProductsServices/DeveloperKits/SkyeModuleDKM9/tabid/289/Default.aspx

[17] "RS232-Male 3-5V TTL Type 1 Serial Converter Cable." [Online]. Available: http://www.superdroidrobots.com/shop/item.asp?itemid=696

[18] "Regulatory status for using RFID in the UHF spectrum," Sept. 2007. [Online]. Available: http://www.epcglobalinc.org/tech/freq_reg/RFID_at_UHF_Regulations_20070904.pdf

[19] "UHF Applications." [Online]. Available: http://tii.developerconference.ext.ti.com/post-conf/downloads/rfid-tutorial3.pdf

[20] "Alien EPC Class 1 Gen 2 RFID Tags." [Online]. Available: http://www.barco.cz/data/products/download/ALL-9440Gen2Datasheet.pdf

[21] "Avery EPC Class 1 Gen 2 RFID Tags." [Online]. Available: http://www.rfid.averydennison.com/_media/us/pdf/datasheets/Portfolio.pdf

[22] "AWiD." [Online]. Available: http://www.awid.com/

[23] "Cushcraft S9028PC Circularly Polarized Panel Antenna." [Online]. Available: http://www.cushcraft.com/support/pdf/S9028PC12NF.pdf

[24] "Symbol Fixed RFID Reader Antennas." [Online]. Available: http://www.symbol.com/products/rfid-readers/rfid-antenna5

[25] "Sensormatic Omniwave Antenna (EPC Class 1 Circular)." [Online]. Available: http://www.sensormatic.com/SensormaticGetDoc.aspx?FileID=9519