The Use of Advanced RFID Tracking Methods for Insuring the Security and Integrity of Container Shipped Cargo

Michael J. Williams and Cheryl Cunningham
Embry-Riddle Aeronautical University, USA

Abstract: The cargo container has made the commercial world smaller through the efficient shipping of goods across oceans and continents. Along with this efficiency have come unprecedented increases in container traffic with the expected concerns over security and safety, given today's political climate. This paper presents the initial research of a continuing project designed to study the issue of container safety and security using the information systems technology: Radio Frequency Identification (RFID). The scope and depth of the container security issue and the applications of relevant technology will be discussed with emphasis on the latest tracking techniques and processes. Computerized tracking using RFID is a promising technology that is being used with mixed success by various organizations and is the primary focus of this paper.

Keywords: Shipping container security, Information systems, RFID, Transportation security

1 Introduction

The numbers are staggering. Thousands of ocean going ships docking every day, tens of thousands of shipping containers in transit at any given moment, and millions of containers processed at various ports each year heading for their destinations behind highway tractors or on mile-long trains. Transporting commercial goods by standardized shipping containers has become the most widely used method of moving products to market. Potential complications from very high traffic levels include terminal congestion, lost or misplaced containers, and even potential hiding places for human or destructive cargo (Levinson, 2006). The research cited in this paper will investigate the problem of container tracking and security and offer potential technological solutions following a review of the latest literature and a discussion of current best practices.

2 Tracking and Security Issues

2.1 Container Volume and Traffic Growth Estimates

The maritime transportation system is at the core of the global supply chain, accounting for more than 90 percent of international trade (Kelly, 2007). The maritime shipping industry, specifically container ships, is considered by the Department of Homeland Security to be one of the key elements of this country's critical infrastructure because of its role in both domestic and global economies. Annual port calls into the United States are estimated at 22,000 dockings and are predominantly containerships. Every day 50,000 containers (imports and exports) are processed at U.S. ports. The World Shipping Council estimates that liner shipping accounts for more than one million jobs and $38 million in annual wages; overall, the maritime shipping industry contributes over $100 billion to the U.S. gross domestic product (World Shipping Council, 2007).

The supply chain distribution network, using the standard 8,000 TEU steel containers, continues to grow. The ease and efficiency of loading and unloading cargo housed in these standardized containers from liner vessels has contributed to its commercial success. The recent growth in containerized shipment is a result of more general cargo tonnage being containerized rather than shipped in bulk. By 2010 containerized cargo can be expected to account for 83% of the general cargo -- an increase of 12% since 2004 (World Shipping Council, 2005).

International container shipments from the major Asia—U.S. trade lanes are expected to expand at a rate of 10% to 12% per year. A more modest growth rate of 1.5% to 3% is projected between major Northern European ports and U.S. harbours. As for the overall global tonnage, approximately 100 million TEUs were processed in 2004 and that total is predicted to reach 150 million TEUs by 2010. In order to manage this increased shipping capacity, an additional 150 container ships in the 8,000 to 9,200 ton class size will be added to the major East-West trade routes by 2008 (World Shipping Council, 2005).

As international global commerce continues to grow so have the challenges of managing port congestion and the associated inter-modal connections (road, air, train, etc.). Many U.S. roadways and rails are feeling the strains of growth even as U. S. ports have been expanding to meet future cargo volume needs, and several of the busiest U.S. ports have recently added dockage or are continuing to expand capacity. In addition to expanding capacity, port facility productivity throughput must improve. A recent study comparing U.S. ports to Asian ports found Asian ports to be 44% more productive than U.S. ports (World Shipping Council, 2005).

2.2 Contraband: Harmful Cargo, Counterfeit Products, Illegal Human Cargo, etc.

Since September 11th, U.S. and other international ports have shifted their emphasis from the detection of economic contraband to the detection, interception, and mitigation of "weapons of mass effect" (nuclear, chemical, biological, radiological and explosive). Noteworthy, for both the government and the commercial sector, are some statistics describing theft, illegal imports, and counterfeiting. Annual cargo theft estimates are said to cost businesses between $10 and $20 billion domestically. Counterfeit products account for nearly $200 billion worldwide. Tobacco products smuggled into both U.S. and international markets account for $16 billion in lost tax revenue. (Ledoux, 2006) Better tracking through RFID tags would allow businesses and insurance companies to better determine the true financial impact of cargo theft and they could reduce the number of lost and misdirected containers.

Although human stowaways in cargo containers attempting illegal immigration into the United States accounts for only a very small number of illegal entries, it illustrates the vulnerabilities in post-9/11 maritime security. Three notable incidents were discovered between January 15, 2005, and April 5, 2006, involving a total of 85 Chinese nationals. In each incident the smuggled passengers were not discovered until either arriving on U.S. soil or off shore prior to the cargo's being released by the commercial shipper. Discrepancies in all three manifests were discovered and in each incident the cargo was held for further examination, leading to the smuggling discovery; if there hadn't been a manifest discrepancy, there would not have been an apprehension of the smugglers and the illegals (DHS, 2007).

2.3 Scanning Shipping Containers

As part of the "implementing of 9/11 Commission Recommendations Act" signed into law in August 2007, a provision requires that by 2012 all containers (100%) imported into the United States will be scanned prior to being loaded aboard vessels destined for U.S. territories. The provision requires all containers to be scanned using radiation detection equipment and non-intrusive imaging equipment. Christopher Koch, President and CEO of the World Shipping Council speaking before the House Homeland Security Committee Subcommittee on Border, Maritime and Counterterrorism on October 30, 2007, made a couple of observations about the current provision that could adversely affect international trade. Since containers bound for the United States must be scanned on foreign soil, this would require the cooperation of many foreign governments. The only alternative left to the U.S. would be to forego some international trading partners if those foreign governments refused to oblige. In addition, there are currently no plans for the U.S. to reciprocate and there are no plans to scan U.S. exports before delivery to foreign nations. It is likely that foreign nations will establish "mirror image" requirement on U.S. cargo and this could have a detrimental impact on international trade (World Shipping Council, 2007).

Many experts are concerned that current scanning and imaging technologies are inadequate to support 100% inspections. Current scanning technologies average 150 false positives per day. Opening and searching each suspect container would be very expensive, time consuming, and could create processing logjams.

But from a port security perspective, it is estimated that if a catastrophic event were to close a major U.S. port, the economic impact could reach $1 billion per day (Ledoux, 2006).

2.4 Scanning for "Weapons of Mass Effect" Difficult

Meanwhile, the Department of Homeland Security continues its efforts to develop better methods of detecting nuclear materials and other potential weapons entering U.S. ports. A former chief scientist at the U.S. Arms Control and Disarmament Agency, Peter Zimmerman, recently suggested that it was more likely that a weapon would be assembled within U.S. borders than imported intact through current U.S. security. Although a crude nuclear device could be constructed within the U.S., a terrorist group would most likely have to first smuggle in uranium 235. According to Zimmerman, highly enriched uranium is one of the most difficult radioactive materials to detect and can be shielded by just a few thicknesses of aluminium foil. Because of its size, a dangerous quantity of uranium could be easily missed by inspectors and "wouldn't even upset the balance of the cargo container" (Magnuson, 2007).

3 Radio Frequency Identification Technologies

3.1 Overview of RFID

Modern container facilities contain a variety of equipment designed to unload, identify, sort, track and load shipping containers. Insuring that a container is efficiently routed to its destination can be a monumental task given the variety of originations, destinations and technologies involved. At a modern container facility, computers contain data that includes the container's shipper, contents, destination and even current location. As previously mentioned, locating a container often becomes a challenge, especially on a ship or in a storage area that contains thousands of other containers. Historically, container identification was facilitated through the use of visual scanning of bar codes affixed to a specific location on the container. Visual scanning requires line-of-site visualization of the bar code, making the logistics of identifying a particular container somewhat difficult. One promising technology for tracking containers is a relatively new technology known as Radio Frequency Identification or RFID. Considered an emerging technology and used for tracking physical assets such as an organization's inventory, RFID is being adopted by a number of large organizations, including the U.S. military, mega-retailer Wal-Mart, as well as the pharmaceutical industry (Glover and Bhatt, 2006). While potential uses of RFID are continuing to be identified, many organizations use a "tag and ship" application that involves tracking items within the originating facility to the point of its leaving the premises on an outbound shipment. That "ending point" could really be the beginning for object tracking and could have significant implications for information gathering as well as personal privacy concerns (Glover and Bhatt, 2006 and Heinrich, 2005).

RFID was first effectively used during World War II as a way of distinguishing friendly aircraft from unfriendly. This Identification Friend or Foe (IFF) technology used a radio transmitter on board an aircraft to send a coded radio transmission that revealed its identity to allied forces and therefore became the first use of a system that has evolved and is still widely used today. RFID technology includes four basic components: a tag, an antenna, a reader, and a computer system (Garfinkel and Rosenberg, 2006). RFID is used in a variety of industries for tracking inventory or individuals and includes such benefits as the ability to quickly scan and track many items simultaneously and the elimination of line-of-sight monitoring. Commercial RFID systems can efficiently package the tag, antenna, reader, and associated computer system (Glover & Bhatt, 2006). The next section will discuss these components as well as relevant technologies.

3.2 RFID: Active and Passive Tags

Tags used in RFID systems are actually complete radio systems and may be as large as a loaf of bread or small as a grain of rice. A typical RFID tag consists of two basic components: an integrated circuit (IC) and an antenna. The IC provides the instructions that allow interrogation by a reader and it also contains identifying information such as a serial number or other unique identifier. The Electronic Product Code (EPC) is a possible successor to the printed barcode found on millions of products and is often the identifier contained within an RFID tag. The antenna allows for activation of the tag and permits the transmission of data. There are two basic types of RFID tags: passive and active. Passive tags are the lesser expensive and the more common tag type. Passive tags usually do not contain a power source. Instead, they use radio frequency (RF) radio to activate the circuit and facilitate a transmission. They typically provide only identifying information and are activated when the object, with a tag attached, is moved into the electromagnetic field of a reader's antenna. Passive tags are often relatively inexpensive printed labels that can be easily activated and attached. Active RFID tags are used when greater distances are involved or more information about the object is needed. They usually contain their own power source such as batteries or solar cells and may have an additional feature such as a GPS receiver for determining location, environmental or tamper detection sensors; and circuit logic and memory that contain much more information than a passive tag (Glover & Bhatt, 2006).

3.3 Standard RFID Frequency Ranges

The next RFID system component is the reader, which transmits a radio signal through an antenna that activates a tag and then listens for a response. In addition to "listening" for information from various tags, readers may also add or change information on a tag. For example, as an object with a tag attached is scanned by a reader at a particular station, additional information such as a specific time and a particular station operator may be added onto the tag so a more complete record of the production process is obtained. In an operational environment, readers are constantly transmitting and waiting for responses from tags. In order to communicate with the tags, a reader uses radio components connected to an antenna for signal transmission and reception. A component integrated into most modern readers is a controller, which allows communication between the reader and tags. Using current technologies, RFID transmissions may be broadcast and read over distances ranging from 3 meters to more than 100 meters using low frequencies (LF - 125-134 KHz), high frequencies (HF – 13.56 MHz), ultra-high frequencies (UHF – 300MHz to 1 GHz), and microwave (frequencies over 1 GHz). A relatively new RFID technology known as Ultra-Wideband (UWB) uses a band of frequencies in the 3.1GHz-10.6 GHz range to send very short pulses (Collins, 2004 and Gambon, 2007). UWB will be discussed in further detail later in this discussion.

3.4 RFID Communication Systems

The final major RFID component is the computer network (hardware and software) that provides connectivity and interaction with other parts of the system. In addition to facilitating the interface that integrates the tags, readers, and antennae, the network also provides the middleware as well as the enterprise connections that allow communications with a company's business information system to include supply-chain management, product security, and inventory management functions (Lahiri, 2006).

4 Emerging Technologies as Solutions to Container Shipping Problems

4.1 RFID Impact on Security

Two of the most promising emerging technologies to be discussed are smart container technology and ultra-wideband RFID; they address both security and economic issues within the global supply chain. Several smart containers are being tested at sea or nearing deployment by a number of companies such as Schenker, iControl, Inc., Savi, GE-NYK, and IBM - just to name a few. Researchers are developing stronger RFID security standards which may require revisions to the SAFE Port Act of 2006. Additionally, RFID systems are being included in cellular telephone technology and how it will be integrated into the cellular supply chain as a tracking tool is speculative.

The SAFE Port Act of 2006, which was signed into law by President Bush, defines three provisional applications: 1) international supply chains, 2) radiation detection equipment and 3) container security devices. Smart containers using RFID and sensor technologies are key solutions to the Safe Port Act. The Act requires: "a device or systems, designed, at a minimum, to identify positively a container, to detect and record the unauthorized intrusion of a container, and to secure a container against tampering throughout the supply chain. Such a device, or system, shall have a low false alarm rate as determined by the Secretary" (Giermanski & Lodge, 2007).

4.2 Smart Containers

James Giermanski, Professor and Director of the Centre for Global Commerce at Belmont Abbey College and Chairman of the Board of Powers International, suggests that following guidelines of the SAFE Port Act is at the forefront of articulating a strict definition of a smart container in a post 9/11 environment. Smarts do more than use GPS with RFID technology or GPS alone. He insists that a true smart container that supports both security and corporate interests must comply with the following criterion to fulfill the economic and security needs of the intermodal supply chain. Smart containers:

- need to be part of a systems approach coordinating all facets of the supply chain process ensuring both visibility and security from the cargo's origin to its destination. At the both the origin and destination, the container can be monitored during the loading, securing and unloading of the smart container. It should be able to identify the authorized personnel loading and unloading the container contents.
- must electronically capture key trade data with the possibility of linking to other types of documentation.
- must detect and report a security breach in real time or nearly real time with date, time and geographic location of the violation for **all** possible entry points into the body of the shipping container. Breach detection monitoring must not be limited to the main cargo door.
- can give its geographic location throughout the supply chain when queried, and will automatically report deviations from the designated route.
- should be able to have adaptable sensors for detecting and reporting deviations in such areas as temperature, humidity, radiation, movement and entry (Giermanski, 2007).

4.3 Ultra-Wideband RFID

The 433 MHz frequency was approved by the Federal Communications Commission (FCC) as the optimal radio frequency for active RFID systems for shipping containers. It is considered to be the best possible frequency in an environment with many international standards where multiple tags are in use. The range reaches a 100 meters and the wavelength is approximately 1 meter enabling the signal to diffract around the large objects found in ports.

Ultra-wideband (UWB) RFID has proven to be effective in tracking objects or people within an area defined by reader placement. Where conventional RFID requires a tag to pass near a reader, UWB allows a reader to locate specific tagged items. An example of this involves tracking hospital equipment, patients and employees within specific departments or floors. Determining the location of expensive hospital equipment has significantly reduced both access time and reduced costs simply because fewer items are needed (Collins, 2004). Another application of UWB permits tracking of nuclear power plant workers and includes both a location tag and a wireless radiation monitoring device that monitors employee location and exposure. UWB RFID and relay techniques may also be used for communication between another container buried within a stack on a ocean-going ship. A signal from a RFID tag attached to a container on a ship in the middle of an ocean may communicate its location to distant land stations by a relay from container-to-container and then to a satellite-capable radio transmitter (Lahiri 2006 and Glover & Bhatt 2006). One particular example of this is the Maritime Asset Tag Tracking System (MATTS) commissioned by the U.S.

Department of Homeland Security. The intent of MATTS is to provide container movement history and access. Once the tag is in range of an Internet-equipped device, it will report information about its journey and any anomalies will cause the container to be flagged for a detailed inspection. The MATTS tag contains a sensor, a data storage device, an RF transceiver, and a GPS tracking system about the size of a small calculator. A test consisting of approximately 100 containers with MATTS that tags were shipped from Japan to the U.S. has recently been conducted and included sea, rail and highway modes of transportation. (Anonymous, 2007). Results of this experiment are not yet available.

4.4 The Impact of RFID on the Business Model

Although security concerns and regulations mandates are heightening interests in smart containers, it is the economic gains that will motivate adoption. In a survey conducted by A.T. Kearney, concern for container security was considered a top priority of major importers and exporters. However, several economic concerns followed with an expressed desire to reduce inventory holdings, inventory lead time variance, and inventory stock outs. Preventing lost containers was also an industry expectation (Kearney, 2005).

In addition, supply chain visibility under the SAFE Port Act is seen by many companies as a way to increase savings since smart container shipments will receive expedited customs border protection treatment. Savings will also be realized through an electronic document management system. In case of a security failure or terrorist threats at any U.S. or international port, many businesses seek to be in the desirable position of being able to move their cargo through customs as quickly as possible (Tier 3 green lane benefits). A smart container equipped with radiation sensors and other specialized sensors will increase the likelihood of its goods being routed through ports of entry more quickly. Also, companies with strong brand value wish to protect their public image and want to avoid the chance of a security breach. Taking an offensive stance and going above and beyond the mandated minimums, places a company in better standing if such a breach would occur (Kearney, 2005). Finally, container security is now a necessary component of many companies' business models and it's also a necessity if goods are to move expeditiously through the supply chain. Transparency in the supply chain can facilitate rerouting goods in transit. Although the later is monetarily difficult to measure, protecting a company's reputation is important in our media drenched society.

5 Conclusion and Future Research

Tracking objects in the supply chain has proven to be a substantial challenge over the years and recent world events such as 9/11 have only further complicated the problem. As the world economy continues to rely on the exchange of commercial goods across international borders, tracking and maintaining reliable security will be major areas of concern. Government agencies, manufacturers and shipping companies are all taking measures to both insure the integrity of container shipments and implement security methods that will hopefully prevent disaster while permitting the timely routing of goods to their intended destinations. The focus of our current research is to study the applications of Radio Frequency Identification (RFID). Current effort are primarily aimed at reducing the time spent locating a specific item, knowing its current status, and perhaps even recording specific operational parameters such as temperature and security breaches. Future research efforts will focus on specific transportation areas that include container tracking, airline passenger baggage routing and location, aircraft ground support equipment locating and usage, and component tracking in maintenance shops and repair facilities.

References

Anonymous (2007). 'Tracking the elusive shipping container', *Industrial Engineer* (Institute of Industrial Engineers, November 2007), Vol. 39, No. 11, p 14.

Collins, J. (2004). 'Hospital Gets Ultra-Wideband RFID', *RFID Journal*: August 19, 2004. Available at: http://www.rfidjournal.com/article/articleprint/1088/-1/1.

Department of Homeland Security (DHS), Office of the Inspector General. (May 2007). 'A Review of CBP and ICE Responses to Recent Incidents of Chinese Human Smuggling in Maritime Cargo Containers', OIG, Vol. 07, No. 04.

Gambon, J. (2007). 'Ultra-Wideband RFID Tracks Nuclear Power Plant Workers', *RFID Journal*., March 8, 2007. Availabel at: http://www.rfidjournal.com/article/articleprint/3126/-1/1.

Garfinkel, S. & Rosenberg, B. (Eds.), (2006). *RFID – Applications, Security and Privacy,* Addison-Wesley, Inc.

Giermanski, J. & Lodge, P. (2007). 'The Problem of Errors, DHS, and the 'False Positive' Standard', *HIS Journal of Homeland Security,* Available at: http://www.homelandsecurity.org/newjournal/Articles/displayArticle2.asp?article=166.

Glover, B. & Bhatt H. (2006). 'RFID Essentials', O'Reilly Media, Inc.

Heinrich, C. (2005). 'RFID and Beyond, Growing Your Business Through Real World Awareness', Wiley Publishing, Inc.

Kearney, A.T. (2005). 'Smart Boxes – RFID Can Improve Efficiency, Visibility and Security in the Global Supply Chain, International Cargo Security Council', Available at: http://www.atkearney.com/shared_res/pdf/Smart_Boxes_S.pdf.

Kelly, R. (2007). 'Containing the Threat: Protecting the Global Supply Chain Through Enhanced Cargo Container Security', *The Reform Institute*. Available at: http://www.reforminstitute.org/uploads/publications/Container_Security_Final_10-02-07_(in_template).pdf.

Lahiri, S. (2006). 'RFID Sourcebook', Pearson Education, Inc.

Ledoux, R. (2006). 'The Value of Threat Reduction', *Journal of Commerce,* New York: April 2006.

Levinson, M. (2006). 'The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger', Princeton University Press.

Magnuson, S. (2007). 'Experts Throw Double on Container Screening Plans,' *National Defense,* Vol. 91, No. 639, p. 13.

World Shipping Council (2005). 'Remarks of Christopher Koch before the American *Association of Port Authorities' Annual Spring Co*nference, Washington D.C'. Available at: http://www.worldshipping.org/aapa_speech.pdf.

World Shipping Council (2007). 'Testimony of Christopher Koch before the House Homeland Security Committee Subcommittee on Border, Maritime and Global Counterterrorism'. Available at: http://www.worldshipping.org/hhsc_testimony103007.pdf.