Container Tracking with RFID and Port Security

UNIVERSITY OF CALIFORNIA, LOS ANGELES
MECHANICAL AND AEROSPACE ENGINEERING DEPARTMENT

MAE 295C: RFID Systems: Analysis, Design, and Applications
Instructor: Professor Rajit Gadh

Louis Tsai
December 7, 2007
Los Angeles, California

TABLE OF CONTENTS

ABSTRACT

RFID technology has numerous applications, one of which includes container tracking in shipping ports. There have been pilot programs completed at various ports around the world. Proven benefits include cut backs on port operation costs, smoother and faster flow of goods, easier access to real-time information, and an overall improvement in security and efficiency. Containers are attached with RFID kits to monitor the goods. RFID kits consisting of RFID tags, sensors, and other hardware are investigated to create a combination of devices that could potentially be implemented. Middleware, specifically WinRFID, is also explored for possible application to data processing and presentation. A rules engine is also developed for a logical means by which data will be processed.

INTRODUCTION

Millions of cargo containers enter the U.S. borders annually. The Port of Long Beach and Port of Los Angeles, located in Southern California, are two major ports in the United States. On a daily average, it is possible for one port to handle up to 30,000 cargo containers. Unfortunately, less than ten percent of cargo containers are ever inspected by U.S. Customs. Ideally, all cargo containers should be opened and inspected. However, if every cargo container were to be inspected, it would lead to massive bottleneck due to the limited amount of resources for that endeavor. This is one of the main reasons only a small percentage of cargo containers are ever inspected.

One idea to ameliorate this issue of security and efficiency has involved the incorporation of RFID technology into shipping ports. There are many applications to shipping ports including attaching RFID tags to port employees. Using RFID, the port can monitor whether an individual has entered a secure portion of the port, or an area where they are not permitted [1]. Another proposal are RFID tags temporarily attached to trucks that enter the ports. For example, Port of Oakland has begun attaching RFID tags to trucks entering its premises. The goal is to automate security, shorten truck waits at the gate and increase the visibility of truck traffic within the port [2].

Container tracking is another option for the use of RFID technology. The focus of this research will center on how RFID tags on containers can improve security and increase efficiency at the Port of Long Beach. RFID has already proven its capability of increasing efficiency within the terminals by speeding the gate check process and provide real-time location of tens of thousands of containers stacked in yards [3]. With the possibility of incorporating sensors to add an extra layer of security, this may greatly improve the overall operation of the port.

PORT OF LONG BEACH SECURITY AND OPERATIONS

CURRENT LOGISTICS

The United States set up the Container Security Initiative (CSI) to address border security at the ports. CSI proposes a security regime to ensure all containers that pose a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels destined for the United States [4]. In addition to government security procedures, Port of Long Beach has other security measures in place. These security measures are to effectively monitor and screen seaport cargo. Beginning at foreign ports, there is a 24-hour rule that requires manifest information on cargo containers to be delivered to U.S. Customs 24 hours before the container is loaded onto a vessel in a foreign port [5]. U.S. Customs then determine which containers are high-risk. Once those containers are inspected, the containers are allowed to be loaded.

Upon arrival at U.S. ports, the cargo containers are unloaded using gantry cranes to the marine terminal. At the terminal, the terminal operator directs the longshore workers to place the cargo containers where they belong on trains, trucks or to terminal property for temporary storage. Some cargo containers are sent immediately to there final destinations. Other containers are sent to intermediate destinations such as railyards, warehouses, distribution centers, or "transload" facilities [6]. The containers are inspected again in varying levels of inspection. Suspect containers that were not scanned at their port of embarkation are scheduled for inspection by one of seven advanced radiation scanners [7], while the rest are scanned once more for radiation before exiting the port. This method of inspection requires a dedicated amount of manpower and time for thorough checks. Adding to the difficulties is figuring which containers to target since so few are ever inspected.

FUTURE LOGISTICS

Incorporating RFID technology has the potential to help the ports operate more efficiently and securely. Beginning at foreign ports, containers leaving foreign ports will have RFID tags and sensors attached to the containers doors. Written on the RFID tags

will be manifest information as well as any other form of identification, such as an ID number for each container. In addition, sensors can be connected to the RFID tag to monitor the contents within the cargo containers. When the cargo ships arrive at the port, gantry cranes equipped with RFID readers will unload and read the RFID tags simultaneously. Information gathered will be sent to a central database. A middleware will process tag information and automatically determine where the containers will be routed. The port will be roughly divided into two sections. One is for containers that do not need to be inspected, allowing the containers to be delivered immediately. The second is for containers that have been flagged as high-risk. These containers will be inspected before they are exit the port. Most of these steps will be automated so that port security can focus on inspecting. Prior to exiting the port, the RFID kits are removed form the containers to be reused.

RFID HARDWARE

The necessary hardware for the design and application of this RFID kit include RFID tags, sensors, and readers. RFID tags will be attached to the door and sensors will be placed inside the containers. Choice of sensors and other items used in correspondence with the tag are at the discretion of the user depending on need. Equipping one container can cost a few hundred to thousands of dollars. Although cost may be of concern, a new generation of active tags has brought the cost down considerably, making it more feasible to tag the tens of thousands of containers in use [8]. Also, as the RIFD technology matures, cost will also likely come down. The following are some basic hardware chosen to meet the basic needs.

RFID TAG

Tag selection was of major concern because the tag is required to meet specific needs. Active tags were chosen because they are able to achieve longer range, more complex protocols for better security and communication, and larger data writing and storage. Savi Technology, which has performed a number of tests with its product, is a prominent manufacturer of RFID technology. Currently, one RFID tag that is being utilized is the

Savi SensorTag ST-676. The ST-676 is an active tag based on the ISO 18000-7 standards. This standard allows for usage worldwide. One benefit of the ST-676 is the inclusion of a light sensor and door sensor. Unauthorized breaches can then be detected and recorded in a log in the tag memory, so that this information can be later viewed. The ST-676 can also detect environmental changes such as temperature, humidity, and shock. Another benefit of this tag is the sensor expansion port. With the ability to support more sensors, this will expand the security possibilities for the containers.

There are also specifications leading to the decision to use the ST-676. It operates at ultra-high frequency (UHF) of 433.92 MHz, ideal for long-range communication. The range is 300 feet for fixed readers and 200 feet for mobile readers, which is great for usage at large ports such as the Port of Long Beach. This RFID tag also has a read/write option allowing it to write data onto its onboard 128 kbytes user memory or 32 kbytes sensor memory. As for its battery life, it uses a 3.6V primary lithium battery that can last for up to 4 years.

RADIATION SENSOR

One major concern of national security is the illegal transportion of radioactive material into the country. Today's approaches to nuclear detection rely primarily on fixed inspection portals at national borders and sea-ports through which shipping containers or vehicles pass, fixed radiation detectors positioned at traffic chokepoints within the national interior, or handheld detectors used by government agents or nuclear emergency search teams (NEST) when specific intelligence is available [9]. By attaching a radiation sensor, it will allow for continuous detection of radiation inside the cargo containers. The RFTrax RAD-CZT was found to be one sensor used in cargo containers. Due to its compact size, it is an ideal addition to the RFID kit. It is able to detect trace amounts of radiation and the user determines the threshold at which the radiation level will be considered dangerous. The range of sensitivity is from 0.1 milliREM/hour to 1.0 REM/hour. The RAD-CZT also has an on-board memory of 512 Kbytes so that data and events logs can be written onto it for later access. As for battery life, it draws less than 600μA at 3.6V allowing it run for 2-3 years in reduced power mode.

GAS AND CHEMICAL SENSOR

There is also an option for using gas and chemical sensor to detect varying types of chemicals. The gas and chemical sensor will work in the same manner as the radiation sensor. However, it will instead detect gases expelled by dangerous chemicals. After looking at multiple manufacturers, it was determined not feasible to include this type of sensor due to one limiting factor, battery life. The previous two devices can be used for at least one year at normal usage, but the gas and chemical sensors can only last up to a few hours.

RFID READER

To access the information stored in the RFID tags, the reader used will be from the same manufacturer as the RFID tag. Savi's fixed reader, the SR-650, is one reader that is compatible with the ST-676. Since the ports occupy a fairly large area, the RFID reader must be able to read RFID tags from a long distance, not just a few feet. Fortunately, the SR-650 has a range of approximately 100 meters and also operates at the same frequency as the ST-676 of 433.92 MHz. The SR-650 is capable of reading data at a rate of 27.8 Kbps and can store the data in its 512 Kbytes memory for temporary storage. For designing a port using RFID, the SR-650 will be attached to each gantry crane so that as the containers are being unloaded, the SR-650 can access the information in the RFID tag and transfer the data to a central database where it can accessed by port security personnel. As mentioned previously, the SR-650 can also be positioned throughout the port to monitor cargo containers at all times.

MIDDLEWARE

MIDDLEWARE BACKGROUND

Information received by the RFID reader from the RFID tag must be processed and presented in a manner that would help improve and provide efficiency and security. The key is likely to be found not in the RFID readers or in the enterprise systems, but in the middle—more precisely, in the middleware [10]. One recommended middleware to use is

the WinRFID currently being used and researched by researchers in Professor Gadh's WINMEC laboratory at UCLA. Middleware, in general, refers to the software layer which resides between the physical layer components (hardware), firmware or operating systems and the upper layer standalone or even distributed enterprise applications generally interacting via the network [11]. The main goal of this middleware is to process data from tags collected by the readers deployed in the RFID infrastructure, or to write ID numbers and/or business process data to the tags and it may also deal with a number of important issues related with avoidance of data duplication, mitigating errors and proper presentation of data [11]. WinRFID from UCLA's WINMEC laboratory is one middleware that is being researched to handle these issues.

WinRFID ARCHITECTURE

WinRFID has five main layers. The first layer is the RFID hardware. The three main parts of the RFID hardware are the tags, readers, and other sensors. WinRFID's abstraction of these parts allows for new RFID technology to be compatible with the middleware.

The second layer is the protocol layer. This layer is to ensure that multiple tag protocols are compatible and new tag protocols can also be added. WinRFID are able to handle a number of different ISO and EPC protocols. For this research, it must support the ISO 18000-7 standard of the ST-676. An alternative to WinRFID is the Savi's SmartChain® Transportation Security Application (TSA) in the event WinRFID is not used. It performs tasks similar to WinRFID such as data processing, optimizing movement of goods, and alert system. There will no compatibility issue because the application and RFID tag are from the same manufacturer.

The third layer is the data processing layer. In this layer, issues are addressed by having processing rules which will weed out duplicate reads, verify the tag reads, and when advanced records are available such as advanced shipping notices, this layer reconciles the records with the tag reads. Any discrepancy is processed as exceptions and a variety of alerting systems are available for resolution – emails, messages, or user defined

triggers [11]. WinRFID will need to process thousands of tag information on a daily basis. The possibility for errors in readings and the myriads of options of what to do with the tag information may lead to a complex system.

The fourth layer is the XML framework. Basically, in this layer, the information gathered from the tag is formatted to a high-level XML based representation. Authorized people such as vendors, suppliers, shippers, and port workers can then have access to tag information according to their own needs.

The fifth layer deals with data presentation. This is the application layer and it gets the data for visualization and decision making from the XML framework.

RULES ENGINE

A rules engine will be required to handle tag information received by the readers. The port is the final decision maker as to how they want tag information to be processed. A possible simple rules engine is as follows.

The first step is to verify the RFID tag itself. Every RFID tag will have its own identification number. Once the reader obtains the identification number, the rules engine poses several questions. Is the RFID tag identification number valid, as in does it exist? If it matches the information already stored in the central database, then proceed to the next step. If it does not, then the reader is instructed to read the tag identification again or else it will be recorded on a list of containers with the same problem so it can be checked later. Next, is the identification number a duplicate? If so, reread the tag to verify and correct any misreads. If it is still a duplicate after several checks, it will also go on the list of containers with problems. This list can then be provided to port security to look through.

Once the container is properly identified, the next step is to check the information stored in the tag. The foremost question to ask for concerns its security risk. Is the container labeled as high-risk? If yes, then the middleware will immediately command to have the

container sent to the appropriate area of the port where it will be inspected. If not, then proceed to the next question. The next question would be to check the tag information. Does the tag information match the manifest information received by the port separately? If not, then there was possible tampering and this container will also be quarantined so it can be inspected. If it matches, then it can continue to the last step. The last step will inquire about the event log. Does the event log record any tampering or dangerous elements detected? If there are any dangerous elements detected, the container is also flagged and will need to be inspected. If the container passes all of these questions, the container can be moved to the other part of the port to be picked up and sent out of the port.

From this simple rules engine, tag information is verified and processed so that the container can be handled without any human intervention. The port will decide which notifications will be sent by the message system based on the condition of the container, such as has it been tampered with or the containers is considered high-risk. This allows them to focus their attention on containers that come to them instead of guessing which containers to inspect.

CONCLUSION

Large-scale implementation of RFID into ports has not occurred yet. It is still in its early stages. Many trials and tests have been conducted at ports throughout the world. Benefits ranging from lower operating cost to higher efficiency of flow of goods have been experienced. RFID is able to provide reliable information at any time and be able to perform security tasks that would otherwise require many people and much time. An investment in RFID can, thus, serve two purposes: as a business accelerator in terms of supply chain efficiency, and as an enabler for improved security [12].

REFERNCES

[1] **Swedberg, Claire**, "Barbados Uses RFID to Secure Cricket World Cup Final," *RFID Journal*, 28 March, 2007. [Online] URL< http://www.rfidjournal.com/article/articleview/3179/1/1/>

[2] **Swedberg, Claire**, "Port of Oakland Sees Signs of Security in RFID," *RFID Journal*, 15 March, 2007 [Online] < http://www.rfidjournal.com/article/articleview/3148/1/1/>

[3] **Young, Linda**, "RFID and U.S. Ports – Where Does Security Fit into the Equation," [Online] 19 July, 2007. URL <http://www.aimglobal.org/members/news/templates/template.aspx?articlei d=2700&zoneid=26>

[4] **U.S. Customs and Border Protection**, "CSI in Brief," [Online] URL <http://www. cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml>

[5] **The Port of Long Beach**, "Port Security," [Online] URL <http://www.polb.com/about/port_security/default.asp>

[6] **The Port of Long Beach**, "Import Cargo Containers," [Online] URL <http://www.polb.com/civica/filebank/blobdload.asp?BlobID=3513>

[7] (**Fickes, Michael**, "Containing Risk," Government Security, 1 April, 2007. [Online] URL <http://govtsecurity.com/mag/containing_risk/>

[8] **Mullen, Dan**, "The Application of RFID Technology in a Port," *Port Technology International*, pp. 181-182.

[9] **Srikrishna, Devabhaktuni, Chari, A. Narasimha, Tisch, Thomas**, "Nuclear Detection: Fixed detectors, portals, and NEST teams won't work for shielded HEU on a national scale; a distributed network of in-vehicle detectors is also necessary to deter nuclear terrorism," [Online] URL < http://www.devabhaktuni.us/research/disarm.pdf>

[10] **Evans, Nicholas D.**, "Middleware Is the Key to RFID," *RFID Journal*, 5 April 2004. [Online] URL < http://www.rfidjournal.com/article/articleview/858/1/82/>

[11] **B. S. Prabhu, X. Su, H. Ramamurthy, C-C. Chu, R. Gadh**, "WinRFID – A Middleware for the enablement of Radio Frequency Identification (RFID) based Applications," *In Mobile, Wireless and Sensor Networks: Technology, Applications and Future Directions*, Eds. Rajeev Shorey, et al., John Wiley, 2006, 313-338.

[12] **Evans, Nicholas D.**, "RFID's Finest Hour," *RIFD Journal*, 17 April, 2006. [Online] URL < http://www.rfidjournal.com/article/articleview/2214/1/82/>