The potential implications of radio frequency identification technology on marine security

Brent WAY
School of Maritime Studies, Fisheries and Marine Institute of Memorial University of Newfoundland, Canada

Abstract

In the past, knowledge of the exact whereabouts of members of a ship's crew was generally beyond the capability of any ship's master. However, RFID (Radio Frequency Identification) tags are an emerging technology that may provide just such information within the proximity of a ship. An RFID tag is similar to a barcode containing a unique identifier for an asset, except that it contains a small integrated circuit chip with limited memory and a small antenna. This allows the RFID tag to be read or programmed at a distance using wireless signals. Driven by retailers such as Wal-Mart, RFID technology has rapidly evolved to allow for the accurate tracking of all types of physical assets through the supply chain. This escalating adoption of RFID technology has driven its cost down to the point where other spin-off applications are becoming feasible. In the post 9/11 marine world of the ISPS code, people are beginning to realize that RFID tags can be used to track mobile human assets, or ships' crews, just like others track physical assets. Apart from the obvious security applications, RFID technology can also alert that an emergency situation has arisen - for instance, if a member of the crew can no longer be located by the RFID system, it may be that he or she has fallen overboard. The challenge for marine industries will be how to best leverage this emerging technology within the world of the ISPS code so that it benefits seafarers without impinging on their rights and freedoms. This article will begin by examining RFID technology to reveal its implementation issues and technological limitations, along with current applications. Then before concluding, the paper will consider potential applications of RFID technology in marine security and safety.

Keywords: RFID, radio frequency identification, ship's personnel, person tracking, maritime security.

1 Introduction

Although described as "the first important technology of the twenty-first century," [1] radio frequency identification (RFID) technology originated during World War II when the British Air Force used it to identify bombers that were returning from night-time raids in Germany. Before RFID came along, there was no easy way to differentiate between British and German, or friend and foe, bombers in the dark, but by fitting each British bomber with a powered RF transmitter, it allowed British ground gunners to recognize them and not shoot them down [2]. Then, in 1948, Harry Stockman realized that the transmitter on the object being identified could be powered from the energy it received from the identifying device [3], and his findings formed the basis of passive RFID, which will be explained in more detail presently. Since that time, the technology has evolved significantly, with many uses of the technology prevalent in society. From mundane applications such as garage door openers to futuristic applications such as chic nightclubs implanting RFID tags under the skin of their VIP patrons, many predict that the application of RFID technology is about to explode as the price of the technology continues to fall.

This paper will begin with a brief introduction to RFID technology, followed by current implementations of the technology and some issues and limitations. Next, the paper will examine potential applications of the technology with respect to maritime security and safety before discussing some of the non-technical issues associated with this technology. A literature review is omitted due to the scant academic literature available on this topic.

2 RFID Technology

Much of the discussion in this section of the paper is based on Chapter 2 of *RFID – Applications, Security, and Privacy* [4]. RFID technology requires three elements – an RFID tag attached to the object being identified, an RFID reader that collects data from the RFID tag using radio waves, and an information processing unit, typically a computer, that can process the information received from the tag via the reader.

The tag itself consists of an antenna and an integrated circuit chip that contains a small amount of memory. Some tags are read-only and some are read-write. The simplest tags store data in the form of a 64- or 96-bit serial number, which is returned to the reader when the reader queries the tag. Some authors have compared RFID tags to barcodes, in that each can store data that can be read by a reader. However, the information storage capacity of a barcode is far less than that of an RFID tag. Also, barcodes must have a close and direct line of sight to a barcode reader, whereas RFID tags can be read at some distance and do not have to be "seen" by an RFID reader to be successfully read.

To contrast the difference, with a barcode each can of Campbell's chicken soup produced will have the same barcode, which identifies two things – the fact that it is made by Campbell's and the fact that it is chicken soup. If RFID tags were

used instead, each can could have a unique serial number that identified not only that it was Campbell's chicken soup, but also when and where it was manufactured and how long it had been sitting on the shelf. That is the level of sophistication that differentiates RFID technology from barcode technology. It is like comparing a computer made in the 1970's, when barcodes became widespread, to a computer made today, when RFID is beginning to spread.

The mode of operation for RFID technology is a call and response system whereby the reader sends out frequent queries, basically polling all tags within its radio range and asking "are you there?" to which any tag that receives the signal will respond with the data contained in its memory. If a tag does not respond, then it is not within the zone that is defined by the range of the reader in question. Of course, just because the tag receives a query from a reader, it does not mean that the reader will receive a response. In order for that to occur, each tag would have to possess the same transmitting power of the reader, making the tags bulky and impractical.

The range that a tag can transmit its data back to the reader depends on a number of factors, including the frequency in use and the size of the antenna. However, the most relevant factor is whether the RFID tag contains its own power source that it can use to transmit. There are two main types of RFID tags in use today – passive and active. Passive tags contain no internal power source and must use the energy received in the query signal from the reader in order to generate a response signal, thus limiting their useful range. Active tags, on the other hand, contain a battery that powers the transmitter in the RFID tag, which allows for a much longer transmission range – meaning they can be read from a much longer distance than passive tags. Crawford and Goldman [5] state that the maximum range of passive tags ranges from a few inches up to 20 feet, and the maximum range for active tags ranges from 25 to 100 feet.

Passive tags are much smaller and cheaper than active tags, and they have become the tag of choice for most RFID applications in use today. To give the reader an idea of how small passive RFID tags have become, there are tags so thin that they can be inserted into a piece of paper and used to track documents; in the United States, the FDA has approved an RFID tag the size of a grain of rice that can be implanted subcutaneously in a human. On the other hand, active tags can be large compared to passive tags, mainly because active tags contain more powerful transmitters that require the active tags to carry a power source. An active tag is typically the length and width of a standard sized credit card, but roughly five times as thick [6].

Of course, once a tag is queried and responds with its data, which is nothing more than a binary number, then the data processing component of the system must take that data and use it to find further information on the object being identified. Using the Campbell's soup example given earlier, a reader might query a can on a grocery store shelf. The can would return its serial number, which would then be passed on to the store's stocking computer to determine when the can had entered the store. If the product was out of date, an alert could then be raised to remove the can from the shelf.

2.1 Issues with RFID implementation

Problems associated with RFID technology in its current state fall into two broad categories – technical and ethical. On the technical side, each manufacturer of RFID equipment is using proprietary standards, meaning that equipment and tags made by one company are not compatible with those of other companies. Until industry standards are developed and adopted, each RFID system purchased will be proprietary in nature, which could have costly implications for a purchaser if the manufacturer went out of business or if the product purchased was incompatible with an existing system. Also, while the adoption of RFID technology has been increasing, economies of scale are eventually expected to lower the prices of tags and equipment much further [7]. Furthermore, the resolution of the technology, or how precise the system can be in determining the exact location of an object, is currently limited. Basically, systems use geographic zones with one RFID reader per zone; the system can only tell the user in which zone, if any, an object is currently located. With technological advances, it may be possible to be much more precise in tracking assets [8].
On the ethical side of the equation, opponents of RFID technology cite privacy issues as one of their main concerns. In particular, they do not like the possibility that the products and clothes they buy may contain RFID tags that allow them to be tracked and identified without their knowledge [9]. In their current stage of development, RFID tags cannot be turned off, or 'killed' in RFID-speak, meaning that when Mr. Jones buys a pair of shoes containing an RFID tag, anyone with the appropriate reader can know when he walks into their store, and perhaps store it in a database. How this data is collected and used is another point of contention; will employers, for example, be able to subpoena information contained in such databases and use it to prove Mr. Smith was out shopping when he called in sick? In the extreme, privacy advocates argue that RFID is a technology that can lead to a 'Big Brother' type of society, where everyone can be monitored constantly. Finally, if/when RFID transaction devices, such as the Exxon Speedpass, are compromised, users of the technology could be vulnerable to significant financial losses.

3 Current applications of RFID technology

As mentioned above, one application for RFID technology is the Speedpass that is being used by Exxon gas stations. With his or her Speedpass in hand, an Exxon customer simply pulls up to a gas pump, waves the Speedpass in front of an RFID reader located in the gas pump, and then proceeds to fuel the car, take the printed receipt, and then drive away – it is the ultimate in gas station convenience. The RFID reader recognizes the serial number of the user's pass, and the transaction information is then fed to a database that contains the patron's credit card number, which is automatically charged the purchase price of the gasoline. While a novel application, opponents of RFID will point out that the system could be compromised, potentially leading to fraudulent purchases. This, in fact, is not an unlikely scenario given that several students at John

Hopkins University did crack the Speedpass and were successfully able to steal customers' Speedpass information without the customers' knowledge, and then purchase goods that were charged to the unsuspecting customers' accounts [10]. However, proponents of RFID technology might point out that RFID has been used in remote control garage door openers for many years, and that any vulnerability would long since have been exposed by enterprising thieves.

Along the lines of using RFID to activate a garage door for entry into a home, many offices and buildings are secured with electronic key access systems. Many of these systems use RFID technology to identify an electronic key holder and provide him or her access to only designated areas. These systems have been in use for many years and essentially use technology to replace a mechanical lock and key system. More recent applications, however, are harnessing the power of RFID to track and locate objects such as library books and luggage [11, 12]. A library book that has been placed on the wrong shelf could take a long time to locate using traditional means. The use of an RFID system to tag books would make locating a missing book much easier. Likewise, at some airports, luggage is now being tagged with RFID tags to aid in processing and tracking baggage.

3.1 RFID used to track people

A more controversial use of RFID technology is tracking people and their whereabouts. There are varying levels of tracking employed in different systems. For example, at one end of the spectrum, inmates in many prisons have now been fitted with non-removable bracelets that contain RFID tags [13]. This makes it possible to track the whereabouts of each inmate in the prison, and, more importantly, to ensure that no prisoners have left the premises prematurely.

Another example of RFID used to track people is being employed in the nursery wards of hospitals. The 'Hugs' infant protection system sees every newborn fitted with an RFID bracelet to prevent infant abductions and parent-child mismatches. In fact, in July 2005, the system proved its worth by thwarting an abduction attempt at the Presbyterian Hospital in Charlotte, North Carolina [14].

In a different attempt at using RFID to monitor children's whereabouts, however, parents objected. A trial project saw a school in California issue mandatory ID badges to students that, unbeknown to students and parents, contained RFID tags. Tag readers were installed in each classroom to help teachers with attendance, but parents were not impressed when they learned that scanners had been placed in some washrooms as well. Due to protests, the project was cancelled [15].

4 Maritime security and safety

Given the current political state of affairs in the world, maritime security has never been more important. The regulatory environment of marine industries is likely to become more restrictive as governments look for new and better

measures to counter terrorism; the implementation of the ISPS code is one step in that direction. What role RFID can and should play is an interesting question. Very little work has been done in this area, meaning this section will deal mostly with what could be done, rather than what is being done today because there is very little RFID technology in use for the purposes of maritime security. With the current level of RFID technology, it would be possible to outfit every member of a ship's crew with an RFID tag that could be used to track his or her location on the ship. Given the limited range of passive tags, active tags would have to be utilized for the system to have any practical value. The current size and cost of active tags might make deploying such a system impractical at this time; however, that is likely to change over time. While this author does not necessarily advocate implementing such a system, even if it was practical today, some potential applications for security and safety at sea are apparent. From a safety perspective, if a crew member falls overboard, the RFID system would know instantly and sound an alert. Also, crew could be tracked to ensure that they are not entering areas for which they do not have security clearance, or an incapacitated crew member could be located during an emergency. Also, when it comes to getting ship's personnel on shore, passports containing RFID tags can help expedite the process. Such a system is currently being implemented by the United States [16].

4.1 Ethical issues with RFID technology

Tagging prisoners, infants, and children for the purpose of tracking them is one thing, but tagging free adults is a different matter. Whereas the former group has limited rights and privileges, the latter have come to expect a certain level of privacy and freedom. However, it is generally accepted that adults must forfeit some of that when they go to their place of work. For a person working on land, one might argue that the employer would have the right to monitor the movement of an employee while he or she is being paid to be at work, but that right would expire at the end of the work day when the employee goes home. In fact a company in the United States has developed a system that tracks restaurant employees to ensure that they wash their hands after visiting the washroom [17]. While the employee may not appreciate being monitored at work, is it unreasonable to expect employees to endure such monitoring on company time? This is one issue that must be resolved as RFID technologies become more widespread.

To extend the discussion to what occurs on a ship is more complicated, considering ships' crews do not leave to go home at the end of the work day. Members of a crew generally spend extended periods of time on the ship, which is split between being on or off duty. So, some would question whether the captain has the right to monitor crew members when they are off duty, or at all for that matter. As well, while a prisoner can be forced to wear a non-removable RFID bracelet, it is questionable whether members of a ships crew would willingly wear a tracking device at all times. If they were forced to do so, they might resent being treated in the same manner as common criminals, but if crew

members have the option to not wear the RFID tag, it could defeat the whole purpose for which the system was implemented.

5 Conclusions

RFID has the potential to become a very powerful and pervasive technology. While some technological challenges persist, it is the non-technical issues that likely pose the biggest problems for RFID systems. A question that has been asked before about technological innovations is this: just because it can be done, does that mean that it should be done? This question is a valid one in this case because the technology is approaching the point where things that people never considered possible will soon become a reality.

On the technical side, standardization of the technology is a significant issue. Other than that, the true technical challenges will be to increase the range of passive tags while keeping their size small, or decreasing the size of the active tags while maintaining their long range capabilities. As well, developing systems that are more affordable and that can track people and things with greater resolution will be some of the technical challenges that the RFID industry will face.

With respect to the shipboard environment in particular, attenuation of the signal through, and reflection of the signal off metal walls on steel ships might also be an area worthy of further technical research. As the state of RFID technology stands right now, person tracking on board of a ship might not be practical given the size of active tags and the question of whether members of a ship's crew would voluntarily wear them or legally be forced to do so.

On the ethical side, societies and lawmakers must decide the amount of privacy to which employees, both on land and at sea, should be entitled. This is not an easy question at the best of times, but it becomes even more difficult to answer in a political climate that stresses increased maritime security measures. The challenge with RFID technology, as has been the case with all new technologies, will be to best reap its benefits while avoiding the pitfalls.

References

[1] Ashton, K. in Garfinkel, S. and Rosenberg. B., eds., *RFID – Applications, security, and privacy*, Addison-Wesley: Upper Saddle River, New Jersey, p. xxi, 2006.

[2] Garfinkel, S. and Rosenberg. B., eds., *RFID – Applications, security, and privacy*, Addison-Wesley: Upper Saddle River, New Jersey, p. 5, 2006.

[3] Stockman, H., Communication by means of reflected power. *Proceedings of the IRE*, pp.1196-1204, October 1948.

[4] Garfinkel, S. and Holtzman, H.. in Garfinkel, S. and Rosenberg. B., eds., *RFID – Applications, security, and privacy*, Addison-Wesley: Upper Saddle River, New Jersey, pp. 15-36, 2006.

[5] Crawford, K. and Goldman, A., RFID Primer: Where the WLAN hits the RFID fan, December 23, 2003, www.isp-planet.com/fixed_wireless/technology/2003/rfid_primer.html.
[6] Taylor, S. Personal communication, 15 July 2005, President, Cathexis Innovations, St. John's, Canada.
[7] Kopakchick, J. III and Monk, C., RFID risk management. *Internal Auditor*, **62(2),** pp. 66-72, April 2005.
[8] Taylor, S. Personal communication, 15 July 2005, President, Cathexis Innovations, St. John's, Canada.
[9] Archer, Q. and Salazar, G., RFID: a threat to privacy? *Computer Weekly*, p. B, 5 April 2005.
[10] Bono, S. et al, Security analysis of a cryptographically-enabled RFID device, 28 January 2005, http://rfid-analysis.org/DSTbreak.pdf.
[11] library books
[12] Security friend and foe, *Industrial Engineer*, **35(11),** pp. 39-40, November 2003.
[13] Financing for RFID prison systems, *RFID Journal*, 31 December 2002, www.rfidjournal.com/article/articleprint/241/-1/1.
[14] RFID prevents infant abduction at North Carolina hospital, *Wireless IQ*, 19 July 2005. www.wirelessiq.info/content/topstories/745.html.
[15] Smith, L., RFID report, *The Humanist*, **65(3)**. pp.37-38,46, May/June 2005.
[16] Smith, L., RFID report, *The Humanist*, **65(3)**. pp.37-38,46, May/June 2005.
[17] Tagging toothpaste and toddlers, *Information Management Journal*, **38 (5),** p. 22, September/October 2004.