IJCSN - International Journal of Computer Science and Network, Volume 8, Issue 2, April 2019
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Reader Collision and Tag Payoff Matrix Resulting in a Wal-Mart RFID

[1] Apoorva Arora; [2] Sonali Gupta; [3] Umesh Sehgal

[1, 2, 3] Chandigarh Engineering College, Landran

Abstract - Radio-frequency identification (RFID) tags and tag readers make use of proximity and have automated ad hoc setup for transferring small amounts of information. The key features of the RFID tag are a fixed unique identifier and necessary proximity of tags to a tag reader. However, some kinds of RFID tags exist that cycle through a predefined list of identifiers. Also some manufacturers have developed RFID tags that are compatible with WiFi networks to extend location tracking to a whole WiFi network, avoiding the need for an extra tracking network. The cheapest variety of RFID tags are called passive, although 'reactive' would be a better term, because they draw their power to transmit from the radio signal of the tag reader. They are commonly used for tracking the movement of objects, typically at distances of up to a few metres, but potentially up to 200 metres with 'active' or 'semi-active' tags i.e. with their own power source. RFID tags are also widely used to control and monitor access through door and gate entry systems and to 'tag' animals and occasionally people. They are increasingly being used in asset tracking and security applications. The ability to add a unique identifier to objects that can be tracked is very useful and should lead to further innovations, especially in combination with other technologies.

Keywords - *RFID*

1. Introduction

RFID stands for Radio-Frequency Identification. The acronym refers to small electronic devices that consist of a small chip and an antenna. The chip typically is capable of carrying 2,000 bytes of data or less. The RFID device serves the same purpose as a bar code or a magnetic strip on the back of a credit card or ATM card; it provides a unique identifier for that object. And, just as a bar code or magnetic strip must be scanned to get the information, the RFID device must be scanned to retrieve the identifying information.

2. RFID Works Better Than Barcodes

A significant advantage of RFID devices over the others mentioned above is that the RFID device does not need to be positioned precisely relative to the scanner. We're all familiar with the difficulty that store checkout clerks sometimes have in making sure that a barcode can be read. And obviously, credit cards and ATM cards must be swiped through a special reader.

In contrast, RFID devices will work within a few feet (up to 20 feet for high-frequency devices) of the scanner. For example, you could just put all of your groceries or purchases in a bag, and set the bag on the scanner. It would be able to query all of the RFID devices and total your purchase immediately

RFID technology has been available for more than fifty years. It has only been recently that the ability to manufacture the RFID devices has fallen to the point where they can be used as a "throwaway" inventory or control device. Alien Technologies recently sold 500 million RFID tags to Gillette at a cost of about ten cents per tag.

One reason that it has taken so long for RFID to come into common use is the lack of standards in the industry. Most companies invested in RFID technology only use the tags to track items within their control; many of the benefits of RFID come when items are tracked from company to company or from country to country.

3. Common Problems with RFID

Some common problems with RFID are reader collision and tag collision. Reader collision occurs when the signals from two or more readers overlap. The tag is unable to respond to simultaneous queries. Systems must be carefully set up to avoid this problem. Tag collision occurs when many tags are present in a small area; but since the read time is very fast, it is easier for vendors to develop systems that ensure that tags respond one at a time.

Reader collision occurs in RFID systems when the coverage area of one reader overlaps with that of another reader. This causes two different problems:

Signal Interference
The RF fields of two or more readers may overlap and interfere. This can be solved by having the readers programmed to read at fractionally different times. This technique (called time division multiple access - TDMA) can still result in the same tag being read twice.

- **Multiple reads of the same tag**
The problem here is that the same tag is read one time by each of the overlapping readers. The only solution is to program the RFID system to make sure that a given tag (with its unique ID number) is read only once in a session.

Tag collision in RFID systems happens when multiple tags are energized by the RFID tag reader simultaneously, and reflect their respective signals back to the reader at the same time. This problem is often seen whenever a large volume of tags must be read together in the same RF field. The reader is unable to differentiate these signals; tag collision confuses the reader.

- **Different systems have been invented to isolate individual tags**; the system used may vary by vendor. For example, when the reader recognizes that tag collision has taken place, it sends a special signal (a "gap pulse"). Upon receiving this signal, each tag consults a random number counter to determine the interval to wait before sending its data. Since each tag gets a unique number interval, the tags send their data at different times.
- **Unfortunately, not very often in the systems** to which consumers are likely to be exposed. Anyone with an appropriately equipped scanner and close access to the RFID device can activate it and read its contents. Obviously, some concerns are greater than others. If someone walks by your bag of books from the bookstore with a 13.56 Mhz "sniffer" with an RF field that will activate the RFID devices in the books you bought, that person can get a complete list of what you just bought. That's certainly an invasion of your privacy, but it could be worse. Another scenario involves a military situation in which the other side scans vehicles going by, looking for tags that are associated with items that only high-ranking officers can have, and targeting accordingly.
- **Companies are more concerned with the increasing use of RFID devices** in company badges. An appropriate RF field will cause the RFID chip in the badge to "spill the beans" to whomever activates it. This information can then be stored and replayed to company scanners, allowing the thief access - and your badge is the one that is "credited" with the access.
- **The smallest tags that will likely be used for consumer** items don't have enough computing power to do data encryption to protect your privacy. The most they can do is PIN-style or password-based protection.

RFID has been implemented in different ways by different manufacturers; global standards are still being worked on. It should be noted that some RFID devices are never meant to leave their network (as in the case of RFID tags used for inventory control within a company). This can cause problems for companies.
Consumers may also have problems with RFID standards. For example, ExxonMobil's SpeedPass system is a proprietary RFID system; if another company wanted to use the convenient SpeedPass (say, at the drive-in window of your favorite fast food restaurant) they would have to pay to access it - an unlikely scenario. On the other hand, if every company had their own "SpeedPass" system, a consumer would need to carry many different devices with them.
Since RFID systems make use of the electromagnetic spectrum (like WiFi networks or cellphones), they are relatively easy to jam using energy at the right frequency. Although this would only be an inconvenience for consumers in stores (longer waits at the checkout), it could be disastrous in other environments where RFID is increasingly used, like hospitals or in the military in the field.
Also, active RFID tags (those that use a battery to increase the range of the system) can be repeatedly interrogated to wear the battery down, disrupting the system.
Reader collision occurs when the signals from two or more readers overlap. The tag is unable to respond to simultaneous queries. Systems must be carefully set up to avoid this problem; many systems use an **anti-collision protocol** (also called a **singulation protocol**. Anti-collision protocols enable the tags to take turns in transmitting to a reader.

4. Conclusion

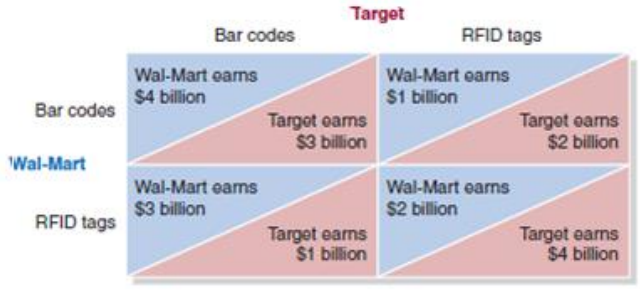

Figure 1

Reference

[1] ieeexplore.ieee.org/document/5998331/ https://www.cse.wustl.edu/~jain/cse574-06/ftp/rfid/index.html

[2] www.chegg.com/.../radio-frequency-identification-rfid-tracking-tags-may-ultima-cha.
searchsecurity.techtarget.com/answer/What-are-the-dangers-of-using-radio-frequency.
[3] https://www.technologyreview.com/s/411444/rfids-security-problem/
www.voyantic.com