Identifying multiple RFID tags in high interference environments

Jonnatan Avilés-González jonnatan.aviles@gmail.com
Tecnológico de Monterrey

Neale R. Smith nsmith@itesm.mx
Tecnológico de Monterrey

César Vargas cvargas@itesm.mx
Tecnológico de Monterrey

Abstract
Radio Frequency Identification (RFID) plays an important role in Warehouse Management, especially during the automatic identification of items. Unfortunately, a warehouse environment has electromagnetic interferences causing read failures in the RFID system. We propose a method for the identification of multiple RFID tags based on accumulated Hamming distances.

Keywords: RFID, Hamming distances, interference.

Introduction

Radio Frequency Identification (RFID) is a relatively new technology in industry and academia. This technology has many applications, including warehouse management, supply chain management, electronic payments, production control, among others (Zhang et al. 2012). An RFID system is typically composed of: a reader, a set of tags, antennas, and an application host environment.

With RFID, automatic identification takes a very specific form: the object, location, or individual is marked with a unique identifier code contained within an RFID tag, which is in some way attached to or embedded in the target. In turn, a computing device that needs to identify the target employs an RFID reader to search for tags. When it receives a signal that a tag is present in its surrounding area, it instructs the reader to request the code. The retrieved data are then recorded or otherwise processed in any manner that is suitable for the particular application (Roussos 2008). The size of the code on a tag may vary according the application; the most common size is 36 bits.

RFID tags are of three general varieties: passive, active, or semi-active (also known as battery-assisted). Passive tags require no internal power source (they are only active when a reader is nearby to power them), whereas semi-passive and active tags require a power source, usually a small battery. The tag is mounted on an item, for example a pallet of goods in a warehouse, and a device called a reader communicates with the tag via radio waves. Depending on the type of tag that is used, the reader can receive detailed information or it can receive data as simple as an identification number.

The information on each tag is encoded as a binary number and it is transmitted via electromagnetic waves that might suffer alterations in their code due to electromagnetic interferences in the work environment (Dobkin 2008). Furthermore, the readers programmed with the necessary protocols can introduce errors at the moment of receiving or sending the information to a central computer. Any of these events may cause the information transmitted to be wrong, and the reliability of the rate to decrease.

Problem Description.

RFID systems receive and send information; therefore, the reliability of the information received is the key to maintaining accurate records. Our study considers a space with n items (each item with an RFID tag) a subgroup of which will be attempted to be identified.

The main problem is that RFID communication is vulnerable to interference and data corruption that could lead to unreliable object identification. In the actual process of identification of the RFID tags, a reader attempts to read the binary codes of the tags as many times as the configuration of the RFID system requires. The current protocol uses a checksum function using a mathematical technique for verifying the integrity of a data file to make sure that no data has been lost or corrupted. This method is known as the cyclic redundancy check (CRC). When the CRC detects an error the reading is discarded and further attempts are realized until a reading with no error is achieved.

Many authors have worked on error identification methods and on how to improve the reliability of read rates during the transmission process. They have proposed: improved hardware designs for readers, antennas, and tags; different methods for reader and tags location, looking for optimal distances, among which we can mention:

Young Yun Jo proposes an error correction method for a single bit error and an advanced multi-bit error based on the CRC, in which the method corrects the error detected by the CRC before the tag is read again (Young Yun et al 2007).

In contrast Vidyasagar Potdar et al. mention that some lost readings could be detected using a method of comparison with another variable like the brute weight of the items (Potdar 2007). Something similar is proposed by Takeaki Toma; who describes a method in which weight is used like a control variable and compared with the results obtained (Takeaki Toma 2010).

Sakil Ibne Sayeed propose an improvement to the reader method; based on the interference and the “nulls” caused by it. They propose to use more readers in environments with high electromagnetic interference (Ibne et al. 2011).

In contrast, A. Bletsas explain how to develop and evaluate single-antenna detection schemes for collided radio frequency identification (RFID) signals. The proposed detection algorithms take into account the FM0 encoding characteristics, including its inherent memory (Bletsas et al. 2012). This work could augment the detection software of existing commercial RFID readers, including single-antenna portable versions.

Our research is based principally on the work titled *“Methods of selection and identification of RFID tags”* where Hamming distances are used to identify a tag in an environment with high electromagnetic interference (Hervert et al. 2011). We propose a method that can be applied in high interference environments without additional data or other control variables. The information obtained in each reading is used to identify the tags more effectively.

Proposed Method.

A typical RFID system comprises:

- A RFID tag with a length of 36 bits (binary code); each tag represents an item that has to be identified.
- A RFID reader, which has an antenna (transmitter / receptor with a decoder).
- A database with all the information concerning the items.

When the RFID reader captures the tag signal, it extracts the information and transmits the data to the subsystem receptor. This subsystem includes computer equipment and a communication network system to store and process information from the RFID tag. A database containing the information to identify the objects resides in this subsystem.

The objective of our proposed method is to identify the codes contained in a group of tags. The approximate position of the tags is known (e.g. on a certain shelf) but not the code they contain.

The Hamming distance is commonly used in telecommunications to count the number of flipped bits in a fixed-length binary code as an estimation of error. The Hamming distance between two binary strings of equal length is the number of positions at which the corresponding symbols are different, and it is given by:

$$d_H(t_i, t_j) = \left\{ \sum_{b=1}^{B} \left| z_{t_i}(b) - z_{t_j}(b) \right| \ \ \forall\, z_{t_i} \in \{0,1\} \right\} \qquad (1)$$

Where *ti* and *tj* represent two binary codes of equal length *B* and *Zti(b)* represents the element *b* that takes values of 0 or 1. The subscripts *i* and *j* represent the tags to which the binary codes correspond (Tanenbaum 2003).

First we consider:
p= Number of readings.
k= Element of the set ORIGIN.
j = Element of the set DATA
m = Size of the set DATA

ORIGIN = Set of all tags in a system; represents the database.
DIST_ACUM =Set where all the results of p readings will be accumulated for each member or ORIGIN.
DATA = Set that will store the group of each reading with m size.
MIN DIS = Set that will store the minimum accumulated hamming distances of each group tag after each reading.

The next equation represents how the distances Hamming will be accumulated, for each group reading.

$$d_K = \sum_{p=1}^{P} \sum_{j\,\in J\,(p)} \sum_{b=1}^{B} \left| Z_{t_j}(b) - Z_{t_k}(b) \right| \ \ \forall\, K \in ORIGIN \qquad (2)$$

Where:
b Element b of the code
B The length of the code
$Z_{t_j}\ (b)$ Element b of the tag j that only will have values 1 or 0
$Z_{t_k}\ (b)$ Element b of the tag k that only will have values 1 or 0

Procedure for identification of multiple RFID tags in high interference environments:

1. Read the set DATA using the reader, the set DATA will change with each reading; this set DATA might or might not have errors in some of their elements (bits). We know the number of tags (Netq) that will be read in the set DATA.
2. Hamming distances are accumulated according to the following procedure (the procedure performs the operations represented by Equation 2):
   2.1. Calculating the Hamming distance between j and k, this will be accumulated in the element k of the set DIST_ACUM.
   2.2. Each k element of set ORIGIN will be compared with each element j of set DATA
3. Repeat step number 1 p times (p is predefined). The number of readings is determined with previous experimentation.
4. Selected tags corresponding to the Netq least elements of the set DIST_ACUM.

Computational Testing.

Our method was simulated using C++ programs. We simulated three different methods:

1. Our method proposed "Multiple Identification RFID Tags Method, based on Hamming Distances and applicable in High Electromagnetic Interferences Environments "
2. A method defined as "100% Readings", this method can identify errors with complete reliability. As is the case with the CRC, any readings with errors are discarded and additional readings are performed until readings with no errors are obtained.
3. Using the CRC method (cyclic redundancy control) based on the checksum calculation and the residual value of the code generated and transmitted. Any readings with errors are discarded and additional readings are performed until readings with no errors are obtained.

We considered the following characteristics for these simulations:

1. Random numbers were generated in order to simulate the databases ORIGIN and DATA.
2. The interference in the environment was simulated using random values that follow a uniform distribution between 0 and 1; such interference values were compared with predefined values to define whether the interference makes the change bit in the binary code by a Bernoulli trial. The default values (interference) used were 0.1, 0.05, 0.2, 0.3 and 0.4, which represents the probability of any bit being in error.
3. We simulated with size databases 100, 500, 1000, 2000, 2500, all 36-bit codes.

Simulation procedure:

a) First, we simulated our proposed method in order to identify how many readings are needed to identify all codes correctly for each interference level.

b) Once the results of the different levels of interference are found, we simulated the other two methods, "100%" and CRC, using identical test instances. The 100% and CRC methods were allowed the same numbers of group readings as used by the proposed method.

The results obtained were as shown in table 1:

In table 1:
Group: Refers to the database that contains the information of items with tags.
Nro. Tags to Read: Shows the number of tags to be analyzed in each instance.
Error: Refers to the percentage of interference simulated in each instance.
The values in the table 1, refers to the percentage of error in code identification.

Table 1- Percentages of error during code identification

			PROPOSED METHOD								
Groups	**Tags to read**	**Error**	**NUMBER OF GROUP READINGS**								
			1 (%)	**2 (%)**	**3 (%)**	**4 (%)**	**5 (%)**	**6 (%)**	**7 (%)**	**8 (%)**	**9 (%)**
100	30	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	30	0.05	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	30	0.2	16.66	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	30	0.3	56.66	26.67	13.33	6.67	3.33	0.00	0.00	0.00	0.00
	30	0.4	90.00	73.33	73.33	70.00	60.0	43.3	40.0	30.0	25.0
500	150	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	150	0.05	0.67	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	150	0.2	27.33	6.00	1.33	0.00	0.00	0.00	0.00	0.00	0.00
	150	0.3	75.33	42.00	21.33	14.00	7.33	3.33	2.00	2.00	0.00
	150	0.4	94.00	91.33	86.00	78.00	70.7	59.3	59.3	55.3	45.3
1000	300	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	300	0.05	0.33	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	300	0.2	34.67	5.67	0.33	0.00	0.00	0.00	0.00	0.00	0.00
	300	0.3	83.33	60.67	37.00	17.67	8.33	4.33	0.67	0.33	0.33
	300	0.4	98.67	93.00	90.66	81.00	76.3	67.3	62.0	51.0	47.3
2000	600	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	600	0.05	0.33	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	600	0.2	39.17	6.67	1.16	0.00	0.00	0.00	0.00	0.00	0.00
	600	0.3	82.67	52.33	32.00	18.00	6.83	2.83	1.17	0.50	0.50
	600	0.4	97.83	94.67	91.33	83.83	81.3	71.3	68.0	58.2	54.7
2500	750	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	750	0.05	1.20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	750	0.2	50.40	13.73	2.67	0.00	0.00	0.00	0.00	0.00	0.00

	750	0.3	88.00	66.53	41.47	23.07	11.2	7.87	3.45	2.00	0.53
	750	0.4	99.20	97.33	94.67	90.53	84.5	80.0	74.9	68.8	63.2

Analyzing table 1, notice that with a few number of group readings we were able to reduce the percentage of error during the identification of tags in the hostile work environment.

In fact the error is very small: with one or two group readings the error is reduced to 0%.

Table 2 represents the results of the several simulatios for the three methods.
The values on table 2 represent the percentage of error of each method (with a limited number of readings used to compare each method)

Table 2 - Comparisons of percentages among methods

				PROPOSED METHOD	**100%**	**CRC**
GROUP	**Nro TAGS TO READ**	**ERROR**	**No. Readings**	**ERROR**	**ERROR**	**ERROR**
100	30	0.01	30	0.00%	40.00%	46.67%
	30	0.05	30	0.00%	83.33%	86.67%
	30	0.2	60	0.00%	100.00%	100.00%
	30	0.3	180	0.00%	100.00%	100.00%
	30	0.4	390	0.00%	100.00%	100.00%
500	150	0.01	150	0.00%	31.33%	34.00%
	150	0.05	300	0.00%	76.00%	88.00%
	150	0.2	600	0.00%	100.00%	100.00%
	150	0.3	1350	0.00%	100.00%	100.00%
	150	0.4	3750	1.33%	100.00%	100.00%
1000	300	0.01	300	0.00%	30.33%	32.67%
	300	0.05	600	0.00%	68.33%	84.00%
	300	0.2	1200	0.00%	100.00%	100.00%
	300	0.3	3000	0.00%	100.00%	100.00%
	300	0.4	7500	2.33%	100.00%	100.00%
2000	600	0.01	600	0.00%	25.83%	28.17%
	600	0.05	1200	0.00%	69.00%	82.33%
	600	0.2	2400	0.00%	100.00%	100.00%
	600	0.3	6600	0.00%	100.00%	100.00%
	600	0.4	15000	4.83%	100.00%	100.00%
2500	750	0.01	750	0.00%	28.80%	31.20%
	750	0.05	1500	0.00%	70.80%	84.53%
	750	0.2	3000	0.00%	100.00%	100.00%
	750	0.3	12750	0.00%	100.00%	100.00%
	750	0.4	18750	5.20%	100.00%	100.00%

In Table 2, notice that in a same group of tags with a limited number of group readings our proposed method has less error during the identification than the method

"100% Readings" and CRC. It also shows that the method of identifying multiple RFID tags based on Hamming Distances is applicable in high-interference environments, reducing error to 0% faster than the two other tested methods.

Conclusions and Further Research

RFID automatic identification systems can be used in different situations. Unfortunately electromagnetic interference in the environment can cause errors in tag readings (in the binary code).

This situation has been solved using security protocols and error correction protocols. Related papers can be found in the literature, most of them focusing on improvements in the hardware, with some addressing in the software and middleware.

The proposed method can be implemented as software. This method is better identifying errors and is useful in environments where electromagnetic interference is high.

Current protocols operate efficiently and effectively in environments where electromagnetic interference is low. However, environments where the interference is more hostile the current protocols are not very reliable. On the other hand, improving accurate identification using our proposed method affected the computational effort.

We conclude that in environments where the electromagnetic interference is low, current protocols work with a high level of reliability, but in hostile environments with high interference, the proposed method could improve read reliability.

For future research, we propose studying how to combine the proposed method with existing protocols. Such a hybrid method could increase the effectiveness and efficiency of readings in high interference environments, and may work in environments where the number of tags in the group to be read is unknown.

References

Bletsas, A., J. Kimionis, A. Dimitriou, G. Karystinos. 2012. Single-Antenna Coherent Detection of Collided FM0 RFID Signals. *IEEE Transactions on Communications.* 60(3) 756-766.

Dobkin, D. 2008. *The RF in RFID.* Newnes, London.

Hervert, L., N. Smith, J. Rodriguez. 2011 Methods of selection and identification of RFID tags. *Work in Process.*

Ibne, S., K. Young Soo, H. Yang, J. Yook. 2011. A Solution to the RFID Reader Interference Problem using Adaptive Beam-forming Approach. *IETE Technical Review* 28(1):17-28.

Potdar, V. 2007. Improving RFID Read Rate Reliability by a Systematic Error Detection Approach. *1st RFID Annual Conference Euroasia 2007. Istambul* 1: 1-6.

Roussos, G. 2008. *Networked RFID. Systems Software and Services*. Springer, London.

Takeaki Toma, D. 2010. Improving the readability of RFID system with database information and optimization techniques. *Proceedings of the 2010 Industrial Engineering Research* 1: 1-6.

Tanenbaum. A. 2003. Computer Networks. Prentice Hall, Amsterdam.

Young Yun, J., Sung Ho, C., Ki Young, J. 2007. An error correction method to improve the tag identification. *1st RFID Annual Conference Euroasia 2007. Istambul* 1: 1-6.

Zhang, Y., Y. Laurence, C. Jiming. 2012. *RFID and Sensor Networks: Architectures, Protocols, Security, and Integrations Wireless Networks and Mobile Communications.* CRC, Boca Raton.