MATHEMATICAL MODEL FOR A MULTIREAD ANTICOLLISION PROTOCOL

P. Hernández, J.D. Sandoval, F. Puente, F. Pérez

Departamento de Ingeniería Telemática
Universidad de Las Palmas de Gran Canaria
Campus Universitario de Tafira, Las Palmas de Gran Canaria, 35017, Spain
e-mail: {pablo, sandoval, fpuente, fperez}@cma.ulpgc.es

Abstract

As any multiaccess communication system, the radio frequency identification is not free from interferences when more than one transmission using the same frequency are sent out simultaneously on the common channel. Based on an anticollision protocol, this paper introduces a mathematical model for calculating analytically some parameters which let us configure the protocol for our application and get the results expected.

1 INTRODUCTION

RFID (Radio Frequency Identification) systems [1][2] allow contactless identification of objects using radio frequency. In recent years industries have incorporated several identification systems (barcodes, smart cards) to its production processes, distribution, etc., which allow collecting automatically information about goods, people and animals.

RFID system has only two devices: the transmitter or transponder and the receiver or reader. An inductive coupling element and a chip with memory that stores the object identification normally makes up the transmitter. The coupling element is used to transfer power from the receiver to the transmitter. The power wakes the transmitter up which then sends the data stored. The power transferred by inductive coupling is very low and depends upon the distance between transmitter and receiver, so the receiver will only receive the data from the transmitters located within the interrogation zone of the receiver (area around the receiver where the transmitter receives the power required for sending data).

When there is more than one transmitter within the interrogation zone of a receiver, all the transmitters send data simultaneously. If transmitters work with the same operating frequency the transmissions will lead to mutual interference, and therefore to data loss. This event is known as *collision.*

The protocol described in this paper implements neither detection nor recovery mechanism. Each transmitter sends data continuously with a pause between two consecutive transmissions. The period of time between two consecutive transmissions is known as *thinking time*. The success of the anticollision procedure depends on the relation between the thinking time, the data transmission length and the number of transmitters in the interrogation zone.

The advantage of this protocol over other protocols [3][4] is its lower cost. Transmitters and receivers only have transmission and receiver hardware respectively. In addition the protocol is so basic that the implementation in a chip is simpler, which means less chip area and therefore lower cost of the protocol control logic.

The protocol is intended for those applications where we need to detect the objects located within a specific zone, during a given interval of time. For this purpose, every object is equipped with a transmitter. Consecutive collisions of the same transmitter during the time interval will not allow detecting that object. Some applications where the protocol can be used are:

- Identification of suitcases passing by a conveyor belt. When the suitcase transmitter is within the reader's interrogation zone, it sends the suitcase identification.
- A person with a reader can monitor a group of children (each one with a transmitter) by defining the boundaries from which kids should not go beyond. The boundary will be the limit from where transmitter doesn't receive power. When a child crosses that border, the transmitter doesn't send frames and the receiver will activate an acoustic alarm for indicating the event.

Although transmitters are not sure that the data sent has been received correctly, however it is possible to calculate the collision probability and, the most important for practical systems, the probability of not receiving a correct frame from a particular transmitter during a given period of time (*reading time*). This value depends on some parameters of the protocol and system, and user can configure them to achieve a given collision probability in a specific application.

The purpose of this paper is to develop an expression to calculate the optimal time required to identify the RFID tags within the interrogation zone for a given application.

2 TRANSMISSION PROTOCOL

A transmitter sends a frame, waits a period of time called thinking time and transmits again. This loop is executed continually.

0-7803-7080-5/01/$10.00 ©2001 IEEE

2.1 Collisions

Due to the common channel (all transmitters use the same frequency) and the lack of a multiaccess control (no MAC-medium access control layer) there are collisions. A collision occurs when two or more transmitters transmit at the same time. The frames that collide are not received.

Many consecutive collisions of a same frame during a set period of time (reading time) can make the receiver think the transmitter is not in the interrogation zone when the transmitter is near enough. This event is called *False Rejection* (FR) and it is shown in figure 1.

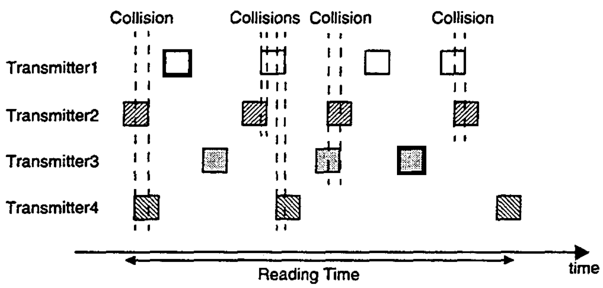


Figure 1. False Rejection for transmitter2

The protocol may generate a FR when the transmitter is near enough but collisions and transmission errors prevent a frame from being received from a given transmitter during a reading time period.

In order to know whether the protocol is operative, the problem of channel saturation is reformulated as *what is the probability of False Rejection?*

2.2 Protocol behavior

The protocol will be analysed under a temporal point of view [5][6], where we assume that all transmitters are at the same distance from the receiver (the maximum allowed), so the collision probability will be greater than the real one. The reduced size of the interrogation zone of the receiver makes the error introduced by the above assumption small.

Consider a system with N transmitters and one receiver where the periods of time between two transmissions are independents and defined by an exponential random variable t_i (for transmitter i) whose distribution function is given by

$$F(t_i) = P(t_i \leq x) = 1 - e^{-\lambda x}$$

where $P(t_i \leq x)$ is the probability that t_i takes a value equal or lower than x [7], and λ is the inverse of the mean of the random variable t_i ($\bar{t}_i$).

$$\bar{t}_i = \frac{1}{\lambda_i}$$

Another parameters of the system are:

L_m is the frame length in bits
C is the channel transmission rate in bits per second
$T_o = \frac{L_m}{C}$ is the frame length in seconds

The probability of collision of any transmitter is the probability that another transmitter sends a frame in T_o or the actual transmitter starts a transmission when there was another ongoing transmission. So, for every transmitter, we can define a collision window of size $2T_o$, where the beginning of a transmission of any other transmitter will produce a collision (see figure 2).

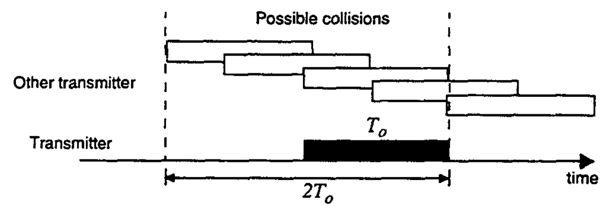


Figure 2. Collision window

The collision probability of the transmission from transmitter i with another transmission, i.e. transmitter j is

$$P_c = P(t_j \leq 2T_o)$$

There are N-1 transmitters whose transmissions may collide with the ongoing transmission so the collision probability of transmitter i is:

$$P_c^i = 1 - P_{nc}^i = 1 - \prod_{\substack{j=1 \\ j \neq i}}^{N} P(t_j > 2T_o)$$

where P_{nc}^i is the probability of no collision of transmitter i, and t_j is the random variable which sets the period of time between two consecutive transmissions of transmitter j.

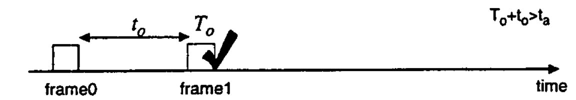
If we consider that the λ-parameter is identical for the random variables of all transmitters (it is so because all transmitters are identical), we obtain the collision probability for the frames of any transmitter:

$$P_c = 1 - [P(t > 2T_o)]^{N-1} = 1 - e^{-2\lambda T_o(N-1)}$$

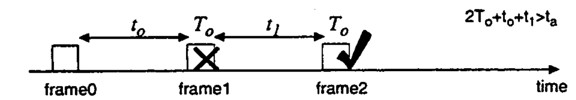
Consider t_a as the value for the reading time, in a way that if the receiver does not receive a correct frame from a transmitter within the period of time t_a it will not be detected (False Rejection). If t_x is the period of time between two correctly received frames from the same transmitter, the probability of above event will be denoted as $P_{fr}=P(t_x>t_a)$.

In order to obtain this probability we have to consider the following cases (from 0 to infinite collisions):

Case 1: No collisions and time between two consecutive frames received from the same transmitter greater than t_a.

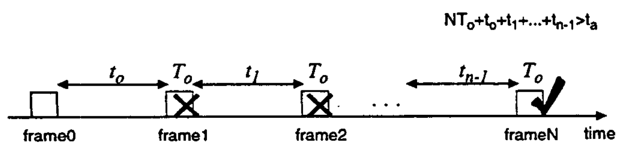


Case 2: One collision and time between consecutive correct frames received from the same transmitter greater than t_a.



.
.
.

Case N: N-1 collisions and time between consecutive correct frames received from the same transmitter greater than t_a.



The probability P_{fr} is equal to the probability of each case weighted by the probability of its occurrence (i incorrect frames followed by a correct one), that is

$$P_{fr} = P(case1) + P(case2) + \ldots + P(caseN) + \ldots =$$
$$(1-P_c)P(T_o+t_o>t_a) + (1-P_c)P_cP(2T_o+t_o+t_1>t_a) + \ldots$$
$$\ldots + (1-P_c)(P_c)^{N-1}P(NT_o+t_o+t_1+\ldots+t_{n-1}>t_a) + \ldots$$

As the random variable of all transmitters are identical, we have $t_o=t_1=\ldots=t_{n-1}=t$, and then

$$P_{fr} = (1-P_c)\sum_{i=1}^{\infty} P(it>t_a-iT_o)(P_c)^{i-1}$$

If we see the frame arrivals to the receiver as a Poisson process, the probability that the frame i is received at a time greater than t_a-iT_o is equal to the probability that the number of frames received in the interval of time $[0, t_a-iT_o]$, $n(t_a-iT_o)$, is equal or lower than i-1. So

$$P_{fr} = (1-P_c)\sum_{i=1}^{\infty} P(n(t_a-iT_o) \le i-1)(P_c)^{i-1} =$$

$$(1-P_c)\sum_{i=1}^{\infty}\left(\sum_{j=0}^{i-1}\frac{e^{-\lambda(t_a-jT_o)}\cdot[\lambda(t_a-jT_o)]^j}{j!}\right)(P_c)^{i-1} \quad (1)$$

Above expression indicates the probability that a sequence of incorrect frames bounded by a correct start frame and another correct one at the end (all of them from the same transmitter), has duration greater than the reading time t_a.

2.3 A case study

Consider a system of N transmitters where the thinking time is given by an exponential random variable with λ equals to 100 (average time between two transmissions of 0,01 seconds).

Every transmitter sends continually a frame with a length of 50 bits. If we assume that the channel transmission rate is 250.000 bits per second, the transmission time for a frame will be 0,0002 seconds.

Figure 3 shows the P_{fr} given by expression (1) for different reading time values (from 0,02 to 1 second by steps of 0,02) and different number of transmitters (from N=10 to N=90). As we could expect, the P_{fr} decreases as the reading time value gets longer. Also, given a reading time value, the P_{fr} decreases when the number of transmitters decreases, because the traffic on the channel is lower.

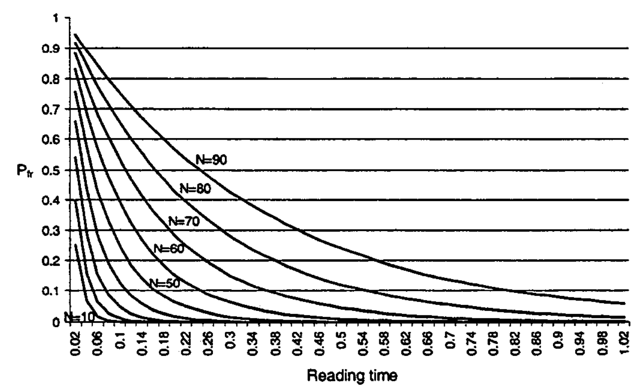


Figure 3. P_{fr} versus reading time for a different number of transmitters

In the other hand, the described system was simulated in a computer. Figure 4 shows the differences between the P_{fr} calculated by expression (1) and the P_{fr} measured in the simulation for a different number of transmitters. The differences for low values of reading time are due mainly to the low precision in the simulation results.

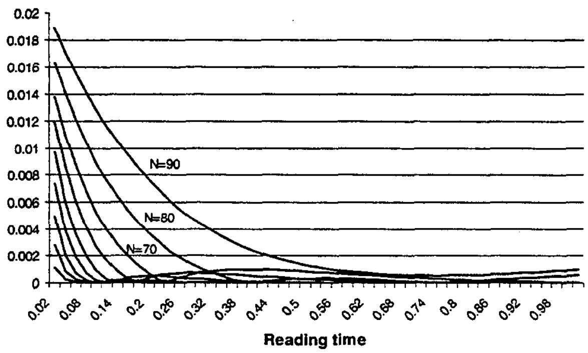


Figure 4. Differences between P_{fr} measured and calculated

In order to know if the values of P_{fr} measured in our simulation can be approximated by expression (1), we computed the Kolmogorov-Smirnov test [8] which shows that expression (1) is a good approximation for the simulation results (with a confidence interval greater than 95%) in the range from 0,02 to 1 second for the reading time value.

3 CONCLUSION

We have introduced an anticollision protocol that can be used for several applications: monitoring a group of persons, goods detection, etc. The protocol doesn't implement either detection or recovery mechanism, and the interframe duration of any transmitter is given by an exponential random variable. The protocol is so simple that the implementation can be very cheap.

When the RFID transmitter of an object is within the reader's interrogation zone, it sends its own identification number. The problem arises when we have to set the reading time interval, as low values will increase the false rejection probability, and high values will result in a poor performance system, keeping in mind that our main goal is to identify or to count the exact number of objects. Once we have determined the false rejection probability, from figure 3 we can obtain the optimal reading time for a given number of transmitters.

The mathematical model introduced let us calculate analytically the optimal reading time value for our application without the need of a computer simulation, which is time consuming.

REFERENCES

[1] K. Finkenzeller, "RFID Handbook", John Wiley & Sons. 1999.

[2] M. di Paolo, W. Furr, N.N. Hearn, K. Kyoo, "RFID: Replacement or Supplement to Bar Codes?". http://198.11.21.25/capstoneTest/Students/Papers/docs/RFID_proceedings37171.

[3] P. Hawkes, "Some of the possible methods of orchestrating the operation of multiple RFID-tags enabling fast, efficient reading without singulation", Amsterdam. 1997.

[4] D.R. Hush, C. Wood, "Analysis of Tree Algorithms for RFID Arbitration", Proc. of International Symposium on Information Theory, pages 107-117, 1998.

[5] W. Stalling, "Data and computer communications", Prentice Hall, 1999.

[6] A. Hoyland, M. Rausand, "System Reliability Theory: models and statistical methods", John Wiley & Sons, 1994.

[7] Narayan C. Giri, "Introduction to probability and statistics. Marcel Dekker", 1993.

[8] George C. Canavos, "Applied Probability and Statistical Methods", Mac Graw-Hill, 1988.