Survey of Standardized ISO 18000-6 RFID Anti-Collision Protocols

Marcelo C. de Azambuja, César A. M. Marcon, Fabiano P. Hessel
PPGCC / FACIN / PUCRS
Av. Ipiranga, 6681 - Porto Alegre, Brazil
[marcelo.azambuja, cesar.marcon, fabiano.hessel]@pucrs.br

Abstract

The Radio Frequency Identification (RFID) technology has evolved rapidly in the past few years, due to great industry and scientific community investments. This paper has as its main objectives the complete descriptions and the performance comparison of the anti-collision algorithms of signals coming from the tags of the ISO 18000-6 and EPCglobal Gen2 standards. In our knowledge none of previous work in the literature emphasizes this point that is very important and has great impact to the industry, new researches and new developments. For each type of the standard ISO 18000-6 (A, B and C) a new anti-collision algorithm is specified. Through the algorithm study it was concluded that under certain circumstances the detection (reading) of all tags present in the same place is not guaranteed.

1. Introduction

RFID tags are a powerful enabling technology with ever widening application. This technology is expected to improve automation, inventory control, pallet tracking and checkout operations in stores, factories, etc. However, the detection and reading of many RFID tags that send and receive signals in the same shared frequency constitutes a big deal that demands communication channel sharing techniques. Such techniques are implemented by "anti-collision protocols". The current protocols standardized by ISO and EPCglobal[1] are based mainly on two generic strategies: (i) channel sharing by time (ALOHA algorithms) and (ii) tags identification by reader-machine questioning, generically called "tree-based protocols".

Anti-collision protocol is a fundamental part to the well functioning of RFID systems because it allows the reader (or interrogator) identify and communicate with all tags presents in an environment. The identification of all tags is an important challenge, meanly when we have supply chain application. Each ISO standard is related to an application domain. In this paper we focus in the supply chain and consumer goods (pallet tracking) domains, which is specified by ISO 18000-6 and EPCGlobal Gen 2 standards.

This paper presents a survey of the current ISO standardized anti-collision protocols and a critical analysis for UHF 18000-6 tags (A, B and C types) and EPCglobal Gen2: ALOHA (LST – Long Slot Mode and FST – Fast Slot Mode), Btree (Binary Tree) and Random Slotted (Q algorithm). By analyzing these protocols it is possible to conclude that they are not to be fully trusted, since they can not guarantee the detection of all tags present in an environment. The lowest possibility of this happening will disable the use of this technology in large scale applications, like supply chain and products identification.

The remaining of this work is organized as following: in Section 1.1 the RFID standards organizations are presented and also RFID overview. The anti-collision protocols currently standardized by ISO are presented in Section 2, and a comparative summary of the anti-collision protocols performances is presented also in Section 2. Conclusions are presented in Section 3.

1.1. RFID standard organization

RFID is a wireless tracking technology that allows a reader to activate a transponder on a radio frequency tag attached to, or embedded in, an item, allowing the reader to remotely read and/or write data to the RFID tag [1]. A RFID tags can be classified according to the way they are power supplied. Passive tags draw power from the reader and are cheaper and smaller than active tags, which have a battery used to broadcast the signal to the reader [2]. Due to combination of tag size, read range ability to control the read zone through directional antennas on the reader, potential to drive down tag costs, and the beneficial read rate, most of the efforts to promote RFID at the supply chain and consumer goods currently are directed at the passive 915Mhz tags (ISO 18000-6) [1, 2, 3, 4, 5]. As a consequence, this paper

[1]EPC (Electronic Product Code). http://www.epcglobalinc.org

978-0-7695-3330-8/08 $25.00 © 2008 IEEE
DOI 10.1109/SENSORCOMM.2008.124

concentrates in the anti-collision algorithms used by these tags.

The ISO and the EPCglobal are the main standardize organizations to the RFID area. The EPCglobal is responsible for create and control the unique identification number (UID) for each RFID tags around the world, which is called Electronic Product Code (EPC). This code, as a bar-code, provides support to identify the manufacturer, the kind of product, serial number and other information to track tagged objects along the productive chain [6]. Besides, the EPC standards supply the wireless communication technologies and the data base with information about the electronic tags. The ISO, in turn, operate in the development of RFID technical standards, such as frequency operations, codification and anti-collision protocols. These standards comprehend the current frequencies used to RFID around the world [7, 8]. Frequency operation standards and protocols of ISO and EPC were unconformable. Nevertheless, in January 2005 the EPC submitted its UHF class 1 Generation 2 standard to a possible inclusion as an ISO standard, and in June 2006 the ISO added this standard in the UHF class of ISO 18000 [6]. The standard called EPCglobal Gen2 is now equivalent to the ISO/IEC 18000-6 type C standard or, simply, ISO 18000-6C.

The EPCglobal Class Structure is composed by 7 levels: class 0 to 5 and class 1 Gen 2. The difference among these classes is the implemented functionalities. For example, Class 0 and Class 1 tags represent basic capability like read/write data. Class 2 has the same functionalities of classes 0 and 1, and describes the memory data encryption functionality to passive tags. The batteries utilization in tags is specified in Class 3. Active tags are described in Class 4 standard. Class 5 describes the readers (interrogators) architecture.

The ISO 18000-6 is divided into three types: ISO 18000-6A, ISO 18000-6B and the ISO 18000-6C, which, this last, is related to EPCglobal Class 1 Gen2.

2. Tag identification and message collision

A serious problem faced in the RFID transmissions is the collisions caused by the communication channel sharing. This problem is called “tag collision”. It might be considered one of the great challenges in the RFID systems development because the signals collision coming from tags is a factor which currently limits these systems performance [9, 10, 11].

In this Section we will discuss the concepts behind this problem and the types of collision controls used in the ISO 18000-6 standards. The collision control may be compared with the services offered by the data link layer in multi-layer networks such as ISO/OSI [7].

2.1. Signals collision from tags

The incidence of multiple responses from multiple tags reaching simultaneously to the interrogator prevents it of identifying each response individually, unless some strategy can make the responses come in isolated time or anyhow controlled by the interrogator.

The RFID signal collision delays the tag recognition and possibly loses information. For example, a supermarket cart full of products could have only a part of the products identified by the interrogator and the lowest possibility of this happening would invalidate the use of this technology by the companies. Protocols able to detect all tags presented in the reading area, although the collision occurrence (that are inevitable [12]), are subject of great interest and researched by the scientific community. These protocols need to make a fast and correct identification of all tags present in a certain environment, just because they might get out of the reading area before being completely identified.

2.2. ISO 18000-6A standard: ALOHA LST / FST anti-collision protocol

The first version of the ISO 18000-6A anti-collision protocol was based on ALOHA protocol [8]. In the review process of the first version by ISO, the protocol received the Fast Slot Mode (FST) operation mode [7]. The basic operation mode of the protocol consists in places the tag transmissions in rounds and slots. A round is composed by a number of slots. Each slot has sufficient time duration for the interrogator to receive the answer from a tag. The Figure 1 shows the state diagram of ALOHA protocol.

The reading process starts with the reception by tags of an energy field generated by the interrogator. Before the energy reception, the tag is in *RF field off* state. After that, the tag changes the internal state to *Ready*. In this state, the interrogator starts the identification or the collision arbitration process sending an Init_round command. When the tags receive this command they randomly select a slot in which they will answer (they do not transmit immediately, they wait for a random moment to initiate the transmission). The number of slots in a round, called round size, is determined by the interrogator and informed to the tags in the Init_round command. The first round size is determined by the user, and can be adapted by the interrogator in the next rounds. The adaptation process occurs when the interrogator detects an excess or lack of slots to the amount of tags present in the environment (e.g.

collisions will make the round size to be increased by the interrogator).

When the command Init_round is received, the tags select the slot number which they will use to answer. This selection is preformed through a pseudo-random number generator.

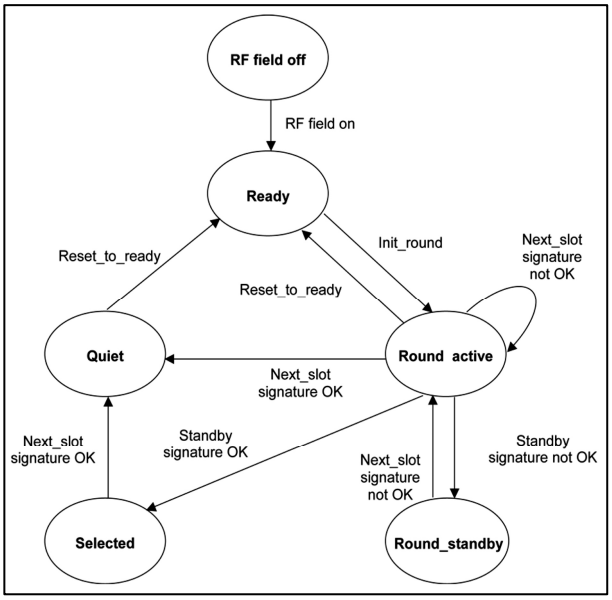

Figure 1: State diagram of ALOHA protocol [7, 8]

After the Init_round command transmission, the interrogator waits for the answer of the first tag that is the one that randomly selected slot 1. If there is no answer from the tags, the interrogator sends the Close_slot command. This command makes all tags, which are in *Round_active*, increase their slot counter in 1 (e.g. one which received value 2 in the number generation will be able to answer). The command Close_slot is also used by the interrogator when it detects a collision in the current slot (which means that more than one tag has random selected the same value to the slot number and are colliding their answers).

Finally, when the interrogator receives a tag answer with no error, it sends the Next_slot command and the tag signature along so that this tag that has just answered may confirm the correct reception of its data. When that happens, the tag may move to *Quiet* state which makes it remains silent from now on. The Next_slot command also makes the other round tags increase their slot counter in 1.

If the slot counter reaches the same value of the round size (indicating that the current round has ended), none identified tags random select a new value to their slot and start a new round.

2.2.1. ALOHA ISO 18000-6A performance analysis

In [13, 14, 15], the Slotted-ALOHA algorithm and a performance analysis about its performance are described. The authors concluded the performance presented for this algorithm is a 36.8% maximum throughput (average of successfully packets transmitted by timeslot), in which can be concluded that, in the best case, there will be, in a little more than a third of all slots generated by the reader, a transmission of a tag's ID without collision.

2.2.2. FST – ALOHA improvement

The second version of ISO 18000-6 standard [7] specifies a complement to the functioning of an anti-collision algorithm that must be used in type A RFID devices. This complement refers to the FST mode, which is optional, being on the criterion of the manufacturer to configure its tags to start the identification process, which began to be identified in the ISO standard as LST (Long Slot Mode). Basically, the new mode intends to make the algorithm faster, reducing stages.

When the tag is configured to start in FST mode, it directly passes to *Round_Standby* state (Figure 1), and it stays in this state until receiving an "advance" command from the interrogator: Next_slot, Close_slot, New_round or Init_Fast_Slot.

Each slot has at least the duration of the tag preamble size. This preamble is the initial sequence of bits that notifies the beginning of a communication between the tag and the interrogator. When a tag is selected to answer, the duration of the slot is increased until reaching the necessary size for the transmission of all data that the tag needs to send. There is a reduction in the waiting time between one slot and another one in case no tag is communicating in one determined slot - an interesting modification between the FST and the LST. In order to prevent other tags to initiate the communication at the same time another one is communicating, the interrogator sends a command to silence the others (Mute command), leaving them in the *Round_standby* mode (as the time of each slot is changeable, the Mute is essential in this new algorithm).

An important modification between LST and FST mode is that in FST the tags always start with round size equal to 16, and all tags initiates in the *Round_Standby* state. Moreover, the state where the interrogator sends the Init_round command and the initial size of round is eliminated.

Another important alteration to prompt the tags recognition is that in FST mode the interrogator does not need to send a Next_slot command to each message received. The tags have an internal counter of timeslots. If the interrogator did not place them in the

Round_standby state (with Mute command), the tags themselves will determine the instant to change from the current slot to the next one, which increases the tags counter. If this new value of counter slot is equal to the slot randomized by one of the tags, the communication of this tag will start.

When receiving a valid preamble from a tag, the interrogator sends the Mute command that informs all the tags that have not initiated the transmission yet to stay in the *Round_standby* state.

2.2.3. Performance analysis of the ALOHA-FST ISO 18000-6A protocol

By analyzing the ALOHA-FST algorithm it was concluded that it was developed based on the Dynamic frame length ALOHA algorithm [15]. In this reference a performance analysis is presented: maximum throughput of 42.6% (which is, for the best case, 2.34 slots are necessary to each package to be successfully transmitted).

2.3. ISO 18000-6 B standard: Btree anti-collision protocol

From the four standardized anti-collision protocols by ISO 18000-6 series, Btree is the only one not based in ALOHA algorithms. Despite this fact it has some similarities with these protocols, such as the random selection that must be performed by the tags in order to determine which will be able to transmit in each instant. In addition, as ALOHA algorithms, Btree has the concept of transmission slot.

Btree always has only one transmission slot available for all the tags, the zero slot, and the tags random select values that will make them to come closer or farther from zero value. When a tag reaches zero in their counter slot, it will be able to transmit. The collisions happen when more than one tag reaches the value zero in their slot counter in a same stage of the algorithm execution. Empty slots happen when none of the tags have zero in their counter slot. The amount of readings performed by the interrogator (i.e., the amount of interactions with slot zero) gives the amount of slots used by Btree for the reading of all tags in the environment [4].

As an example, the Figure 2 shows a typical situation of the beginning of the Btree identification process. The Tag column shows the binary identification (ID) of five tags. In the beginning of the process all tags have the value zero in the counter (COUNT column in Figure 2). For this reason, whenever there is more than one tag in the Btree interrogator reading environment, in the first interaction of the algorithm all the tags are going to send their data simultaneously and collide the signals.

Tag (ID)	COUNT	Rand
0101	0	
0011	0	
1111	0	
0001	0	
1000	0	

Figure 2: Start state of Btree algorithm

After a collision, the tags make a random selection using only values zero and 1. The tags which have random selected 1 must increase the counter by 1. Figure 3 gives continuity to the example. The Rand column shows the random values between zero and 1 performed by all tags. Those that have random selected zero have kept the initial value of the counter, and the ones that have random selected 1 increased this counter, as the second gray COUNT column shows.

Tag (ID)	COUNT		Rand
0101	0	0	0
0011	0	0	0
1111	0	0	0
0001	0	1	1
1000	0	1	1

Figure 3: New values of COUNT columns

When the random selection is made, all the tags that continue with zero in its counter transmit their data again. In the example, three tags {0101, 0011 and 1111} have randomly selected zero and did not changed the counter value. These tags will send their data again and their signals will collide. The described process in Figures 2 and 3 is repeated until only one tag has value zero in the counter and can transmit without collisions. To each collision and new random selection, the counter value is increased by 1 in those tags with value different from zero, and these tags become more and more distant from the moment that they will transmit.

Finally, when a single tag transmits and its data can be read by the interrogator, all the other tags can decrease the counter, and the one that reaches zero at this moment will be able to transmit.

2.3.1. Btree ISO 18000-6 B performance analysis

According to [14], the average number of necessary iterations to detect a tag among several tags L depends on the total number of tags in the interrogation environment of the interrogator equipment N, and can be calculated by the formula: $L(N) = ld(N)+1 = (\log(N)/\log(2))+1$. For instance, the average number of

necessary iterations to identify a unique tag in an environment with 32 tags is 6.

2.4. ISO 18000-6 C standard: Random Slotted (or Q algorithm) anti-collision protocol

As well as in both standard 18000-6 ALOHA algorithms, the base of the Random Slotted algorithm (also called Q algorithm) is structuralized in the generation of a random number method for a slot counter to be stored in the tag. In accordance with the interrogator instructions, the value of the counter slot is decreased in the tags, and when this counter riches zero in any tag, this initiates the communication. The Random Slotted algorithm possesses important evolutions when compared to the Btree, as it will be seen in the following sections.

2.4.1. Random Slotted: Sessions

An important modification in the Random Slotted algorithm is the possibility of a tag to work simultaneously with more than one interrogator by the use of sessions. In other anti-collision algorithms, there is the possibility that an interrogator intervenes in the current inventory in progress of another interrogator's. To prevent this problem, the Random Slotted introduced the session identification concept. The interrogator must support and the tags must offer the capacity to keep 4 simultaneous sessions (called S0, S1, S2 and S3). Each ISO 18000-6 C standard tag will be able to operate in some of the 4 different sessions. The system user will be able to configure his interrogators to operate in different sessions. For example, the an fixed-wall interrogator in an environment will be always able to use Session 1, while a mobile interrogator will always operate in Session 2.

2.4.2. Identifying solely tags with the Random Slotted protocol

An interrogator manages a set of tags to be identified through three basic operations that can be related with the data link layer in a multilayer model network, as the ISO/OSI [7]:

- **Select**: operation to select a set of tags for inventory and access, in order to select them in accordance with the user specifications.
- **Inventory**: process of tag identification. An interrogator initiates this process sending a Query command identifying one of the four sessions to be initiated with values between S0 and S3.
- **Access**: communication operation with a unique tag (written or reading).

The Random Slotted tag identification commands are: Query, QueryAdjust, QueryRep, ACK and NAK.

Query initiates an identification process and decides which tags will have to participate of the process. It possesses a parameter for the slot counter, called Q parameter. The tags that participate of the identification process and receive the Query command, randomize a value between zero and 2^Q-1 and store it in the slot counter. Tags that have random selected the value zero move to the *Reply* state and answer immediately. The remaining tags move to the *Arbitrate* state and wait for the commands QueryAdjust or QueryRep. Assuming that only one tag has answered, the identification algorithm follows the next steps:

1. The tag answers RN16 (random value of 16 bits), a new randomized value, that serves as the only identification for the tag to the next communications with the interrogator;
2. The interrogator confirms the reply reception with an ACK command containing the same RN16 value;
3. The confirmed tags in step 2 move to *Acknowledged* state, replying their data;
4. The interrogator sends the QueryAdjust or QueryRep command, making the tag that has just communicated to move to the *Ready* state again, as well as indicating that the other tags of the current identification process must decrease their counter slot. The next tag that reaches value zero in their counter initiates step 1 of this sequence.

The interrogator QueryAdjust command possesses the functionality to adjust the value of Q parameter. When the tags receive a QueryAdjust command, they randomly select again the value to the slot counter (between zero and 2^Q-1), based now in the new value of Q.

The QueryRep command is the one which controls all the tags to decrease their slot counters. The tag that reaches zero starts the communication process.

2.4.3. Random Slotted ISO 18000-6 C performance analysis

By analyzing the Random Slotted algorithm it is concluded that, except for the additional implementations of control, such as session and inventory, the algorithm functioning is based on the Slotted-ALOHA, and according to what has already been cited in Section 2.4.1, it possesses 36.8% of maximum throughput.

3. Conclusion

A system RFID performance (velocity and reliability) is based on, in a last analysis, the anti-collision algorithm quality. This work presented a relation of basic RFID technologies, having as the main objective the understanding of how the anti-collision algorithms of signals coming from the ISO 18000-6 and EPCglobal Gen2 tags function, as well as to analyze and to compare the algorithms performance.

The related basis allow a wide understanding of the algorithms functioning, being possible to observe that the subject is complex and still needs new solutions to make RFID systems faster and safer, so that the RFID equipment do not need the human intervention to guarantee a bigger trustworthiness of the identification systems. This necessity for human intervention to the correct functioning the RFID systems, for example, through manual adjustments in the speed of the tags expositions and session configuration, is always dangerous for large systems.

To make technology evolution possible and emerge new techniques as the new anti-collision algorithms, the deep study of the characteristics of RFID network physical layer (frequencies, types of wave signals modulation and methods of data codification) and the data link layer (current anti-collision algorithms) is fundamental because from these basic technologies in communication new implementations can be proposed in the future.

References

[1] J. Curtin, R. Kauffman, F. Riggins. "Making the MOST out of RFID technology: a research agenda for the study of the adoption, usage and impact of RFID". *Information Technologic Manage*, p. 87-110, vol. 8, 2007.

[2] G. Borrielo. "RFID: tagging the world". *Communications of the ACM* 48(9), p. 34-37, 2005.

[3] R.Weinstein. "RFID: A Technical Overview and Its Application to the Enterprise". *In: IEEE IT Professional*, p.27-33, 2005.

[4] D. Thompson. "RFID technical tutorial". *In: The Journal of Computing Sciences in Colleges*, p. 8-9, Vol. 21, No. 5. Available at <http://www.csce.uark.edu/~drt/publications/rfid-tutorial-ccsc-ms-conf-slides-060328.pdf>.

[5] T.Hassan, S.Chatterjee. "A Taxonomy for RFID". *In: Proceedings of the 39th Hawaii International Conference on System Sciences* – IEEE, p. 1-10, 2006.

[6] RFIDUpdate. "ISO Incorporates Gen2 into RFID Standard" [Online]. Available at <http://www.rfidupdate.com/articles/index.php?id=1156>

[7] ISO/IEC 18000-6. "Information technology – Radio frequency identification for item management – Part 6: Parameters for air interface communications at 860 MHz to 960 Mhz. Amendment 1 (2006-06-15): Extension with Type C and update of Types A and B".

[8] ISO/IEC 18000-6. "Information technology automatic identification and data capture techniques – Radio frequency identification for item management air interface - Part 6: Parameters for air interface communications at 860-960 Mhz".

[9] J. Myung, W. Lee, J. Srivastava. "Adaptative Binary Splitting for Efficient RFID Tag Anti-Collision". *In: IEEE Communications Letters*, p.144-147, Vol.10, No.3, 2006.

[10] J. Myung, W. Lee. "Adaptive Splitting Protocols for RFID Tag Collision Arbitration". *In: MobiHoc'06*, p.202-213. Florence, Italy, 2006.

[11] C.Law, K.Lee, K.Siu. "Efficient Memoryless Protocol for Tag Identification". *In: 4th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications – ACM Mobicom*, p.1-22. Boston, Massachusetts, 2000.

[12] D.Paret. "Technical State of Art of 'Radio Frequency Identification – RFID' and implications regarding standardization, regulations, human exposure, privacy". *In: Joint sOc-EUSAI Conference*, p. 9-11. France, 2005.

[13] L.Biao, H.Ai-qun, Q.Zhong-yuan. "Trends and Brief Comments on Anti-collision Techniques in Radio Frequency Identification System". *In: IEEE 6th International Conference on ITS Telecommunications Proceedings*, p. 241-245, 2006.

[14] K.Finkenzeller. *RFID Handbook*. West Sussex: Wiley & Sons Ltd, 2003.

[15] F.Schoute. "Dynamic Frame Length ALOHA". *IEEE Transactions on Communications*, p. 565-568, Vol.31, No.4, 1983.