A Simulation Study Comparing the Performance of Two RFID Protocols

Mamatha Nanjundaiah and Vipin Chaudhary

Institute for Scientific Computing
Wayne State University,
Detroit, MI 48202
mamatha@wayne.edu,
vipin@wayne.edu

Abstract. This paper presents a comparison of version 1.0 Protocol Specification for 900MHz Class 0 RFID Tag with that of Class-1 Generation 2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz for large number of tags. Although the Generation 2 protocol has been released for Class 1, it is intended to be used by all classes of RFID tags. Using detailed simulation we compare their performance and security features. If security is a lower priority over speed in cases where one can be sure that the risk of presence of an eavesdropper is low, Class 0 draft protocol should be used as it provides a definite advantage over Generation 2 protocol. In application areas where the risk of consumer identity/privacy theft is high (consumer goods area), Generation 2 provides the security that eliminates the vulnerability of the RFID EPC structure.

1 Introduction

Radio Frequency Identification or RFID is the latest technology that has taken the supply chain industry by storm in the past few years. Although profitable and effective RFID systems have been in operation since decades, they were generally restricted to less complex – closed loop environments. The hype these days surrounds high-resolution supply chain applications of the future.

While the major concerns related to hardware costs and investment in a yet-to-be proven technology (on the scale it has been hyped to perform), are subsiding to a great extent with successful pilot projects along the length and breadth of the technology-hungry supply chain industry, the software components have only just begun to hold some solid ground.

Several protocols to singulate RFID tags, which are generally presumed to be used in significant numbers, have been put forth. We intend to analyze one such protocol that has been published by the EPCglobal Inc., the organization leading the development of industry – driven standards for the Electronic Product Code (EPC). EPCglobal had previously published a draft of standards for the RFID industry. Recently they have released the Generation 2 protocol specifications that have been intended to be more compatible with the prevailing industry standards.

J. Ma et al. (Eds.): UIC 2006, LNCS 4159, pp. 679 – 687, 2006.

The rest of the paper is organized as follows. Section 2 of this paper describes related work. Section 3 describes the anti-collision protocol as given in the Generation 2 specifications [2]. Section 4 explains the simulation of the Generation 2 protocol. Section 5 gives a comparison between the Generation 2 Protocol and the Draft Protocol and Section 6 discusses the result. We conclude the paper in section 7.

2 Related Work

Several anti-collision algorithms for RFID tags have been proposed in the research literature [4-9]. Hernandez *et. al.* [4] discuss a technique where each tag sends out its ID data continuously with a pause between two consecutive transmissions, where the pause is independent for each tag. Here the probability of all tags being read increases with reading time.

Herald Vogt [5] formulated the reader to broadcast a request, where the message contains an address range, which determines what data the tags should return, and a random number to be used as a seed by the tags in choosing a time slot. After the broadcast, N slots are provided for the tags to answer in. Here, an optimum N is determined so as to maximize the throughput.

Jacomet *et. al.* [6] proposed a technique similar to the binary protocol of [3], but here the tags respond with their next bit in the 1^{st} or 2^{nd} slot following the reader's command, depending on whether the bit's value is '0' or '1'. Hence there will never be a clash in response from tags.

Law *et. al.* [7] describe a query tree protocol that consists of rounds of queries and responses. In each round, if there is more than one tag that has the same prefix requested by the reader, then the reader appends a 0 and 1 to the same prefix and continues the queries. When a tag's ID matches the prefix uniquely, it is identified.

Zhou *et. al.* [8] compare the protocols given in [3] and [7] and provide an improvement to the algorithm in [7] by way of shortcutting the responses of tags that clash.

3 Description of the Generation 2 Protocol

Figure 2 gives the flow of the protocol in the singulation of tags.

The Generation 2 protocol provides three basic operations on how the reader manages tag populations:

- Select: Provides the operation of choosing a tag population for inventory and access
- Inventory: The operation of identifying tags
- Access: The operation of communicating with (reading from and/or writing to) a tag.

When a tag powers up in a reader's field and is not killed it enters the *Ready State*. It remains in this state until it receives a QUERY command whose parameters match its current flag settings. Tags that get selected load their slot counter with a Q-bit random number and transition to the *Arbitrate State* if that number is nonzero or

Reply State if the number is zero. If the tag loses power and is not killed it returns to the *Ready State.* The period of time between two QUERY commands is called an Inventory Round.

Arbitrate State holds tags that are participating in the current inventory round with non-zero values in their slot counters. This counter value is decreased for every QUERYREP command. When the value reaches zero, tags transition to the *Reply State*.

When tags enter the *Reply State,* they backscatter a 16-bit random number. If the tag receives a valid acknowledgement from the reader, it transits to the *Acknowledged State* and backscatters the PC (Protocol Control), EPC and the CRC-16 bits.

Tags in the *Acknowledged State* whose access password is nonzero shall transition to the *Open State* upon receiving a REQ_RN command and backscatter a new 16-bit random number. The reader uses this number along with subsequent commands to the tag.

Tags in the *Acknowledged State* whose access password is zero shall transition to the *Secured State* upon receiving a REQ_RN command and backscatter a new 16-bit random number. The reader uses this number along with subsequent commands to the tag. Tags in the *Open State* will transition to the *Secured State* upon receiving a valid ACCESS command maintaining the same handle that was exchanged with the reader while transitioning from the *Acknowledged State* to the *Open State.*

Tags can be permanently disabled with the KILL command, which transitions them to the *Killed State* when received with a valid nonzero kill password and a valid handle.

4 Simulation

For simulation purposes, the complexity of the above protocol has been reduced by the following assumptions:

- No miscommunications between readers and tags have been allowed. Therefore there will be no variations between transitions from one state to another apart from the path taken for the simulation as shown in the Figure 1.
- The simulation ends when all tags have been identified. There are no 'ACCESS' commands simulated here.
- The Electronic Product Code has been assumed to be 32 bits long and has been generated using CSIM inbuilt uniform, beta and geometric random number generators.

The exact algorithm followed for the purpose of simulation can be explained with the help of Figure 2.

The simulation has been designed to run 16 inventory rounds. Each QUERY command uses one of the 16 combinations of the first 4 bits of the tag IDs (0000, 0001, 0010 …). This way, all the tags are divided into 16 groups, irrespective of the distribution of the tag IDs.

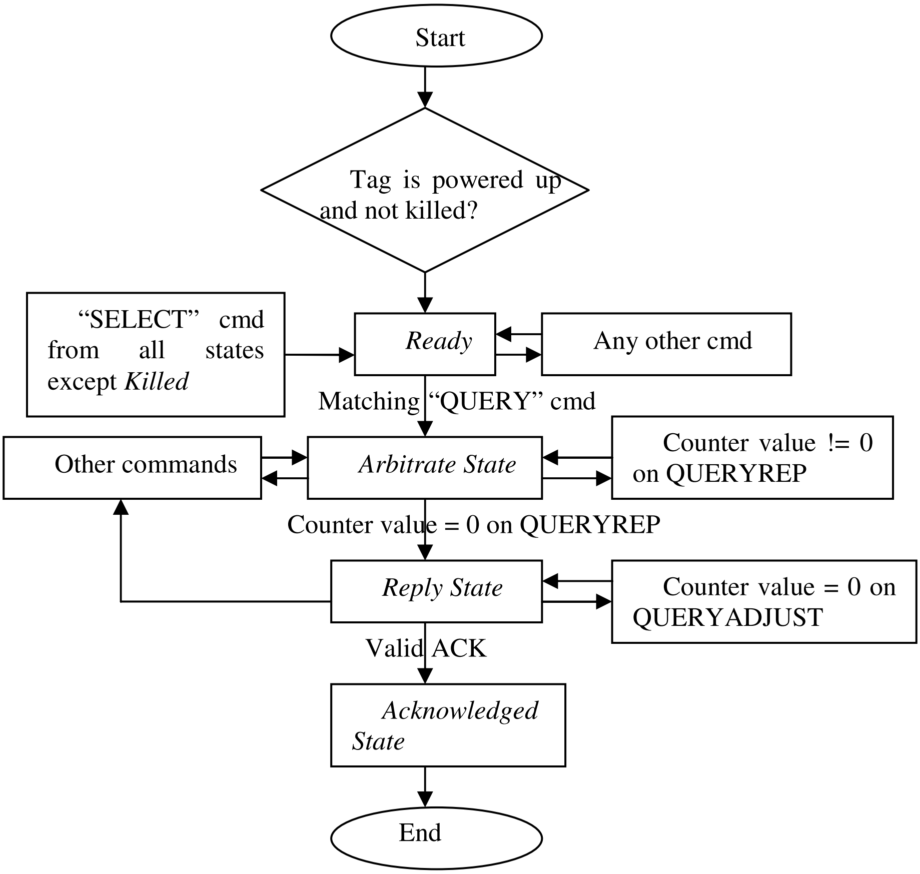
Start
Tag is powered up and not killed?
"SELECT" cmd from all states except *Killed*
Ready
Any other cmd
Matching "QUERY" cmd
Other commands
Arbitrate State
Counter value != 0 on QUERYREP
Counter value = 0 on QUERYREP
Reply State
Counter value = 0 on QUERYADJUST
Valid ACK
Acknowledged State
End

Fig. 1. Algorithm followed in the simulation of the protocol

Tag IDs are generated randomly using "Uniform Distribution", "Beta Distribution" and "Geometric Distribution", over the entire range of 0 to (2^32-1).

All tags power up in the *Ready State.* Tags selected by a matching QUERY command, generate random numbers for their slot counters, based on the value of Q and transition to the *Arbitrate State*. Tags reduce their counter value at every QUERYREP command. At zero counter value, the tags transition to the *Reply State*, backscattering a 16-bit random number. If the reader at this state detects a single tag, the reader acknowledges the tag with the same 16-bit random number.

When the tag receives a positive acknowledgement from the reader, it transitions to the *Acknowledged State* backscattering its PC, EPC and CRC-16 bits. If a QUERY, QUERYREP or SELECT command follows this transmission, it means that the reader has identified the tag. The simulation ends when all tags reach the *Acknowledged State.*

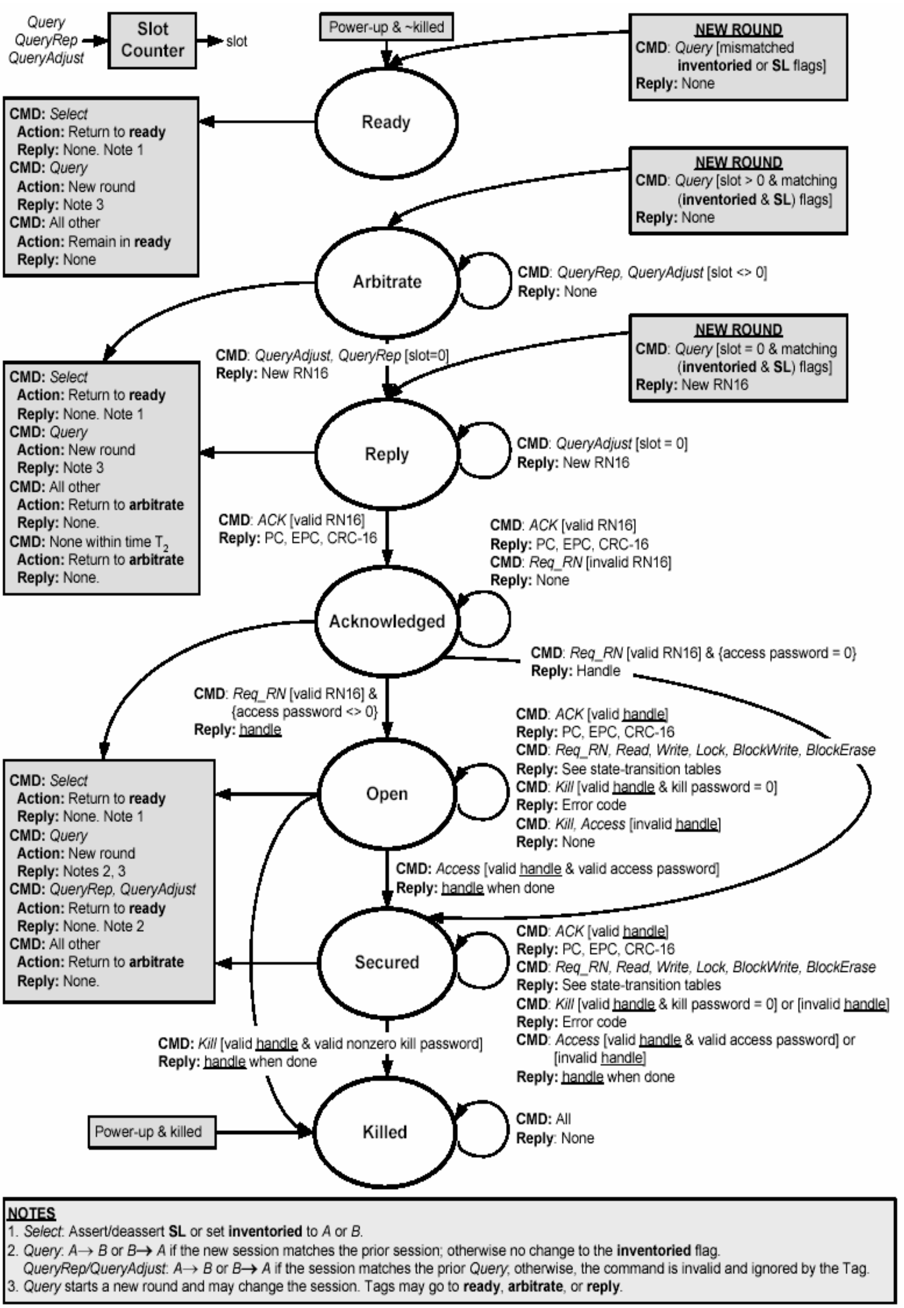
Query
QueryRep
QueryAdjust
Slot Counter
slot
Power-up & ~killed
NEW ROUND
CMD: Query [mismatched inventoried or SL flags]
Reply: None
Ready
CMD: Select
Action: Return to ready
Reply: None. Note 1
CMD: Query
Action: New round
Reply: Note 3
CMD: All other
Action: Remain in ready
Reply: None
NEW ROUND
CMD: Query [slot > 0 & matching (inventoried & SL) flags]
Reply: None
Arbitrate
CMD: QueryRep, QueryAdjust [slot <> 0]
Reply: None
NEW ROUND
CMD: Query [slot = 0 & matching (inventoried & SL) flags]
Reply: New RN16
CMD: QueryAdjust, QueryRep [slot=0]
Reply: New RN16
CMD: Select
Action: Return to ready
Reply: None. Note 1
CMD: Query
Action: New round
Reply: Note 3
CMD: All other
Action: Return to arbitrate
Reply: None.
CMD: None within time T2
Action: Return to arbitrate
Reply: None.
Reply
CMD: QueryAdjust [slot = 0]
Reply: New RN16
CMD: ACK [valid RN16]
Reply: PC, EPC, CRC-16
CMD: ACK [valid RN16]
Reply: PC, EPC, CRC-16
CMD: Req_RN [invalid RN16]
Reply: None
Acknowledged
CMD: Req_RN [valid RN16] & {access password = 0}
Reply: Handle
CMD: Req_RN [valid RN16] & {access password <> 0}
Reply: handle
CMD: ACK [valid handle]
Reply: PC, EPC, CRC-16
CMD: Req_RN, Read, Write, Lock, BlockWrite, BlockErase
Reply: See state-transition tables
CMD: Kill [valid handle & kill password = 0]
Reply: Error code
CMD: Kill, Access [invalid handle]
Reply: None
Open
CMD: Select
Action: Return to ready
Reply: None. Note 1
CMD: Query
Action: New round
Reply: Notes 2, 3
CMD: QueryRep, QueryAdjust
Action: Return to ready
Reply: None. Note 2
CMD: All other
Action: Return to arbitrate
Reply: None.
CMD: Access [valid handle & valid access password]
Reply: handle when done
Secured
CMD: ACK [valid handle]
Reply: PC, EPC, CRC-16
CMD: Req_RN, Read, Write, Lock, BlockWrite, BlockErase
Reply: See state-transition tables
CMD: Kill [valid handle & kill password = 0] or [invalid handle]
Reply: Error code
CMD: Access [valid handle & valid access password] or [invalid handle]
Reply: handle when done
CMD: Kill [valid handle & valid nonzero kill password]
Reply: handle when done
Power-up & killed
Killed
CMD: All
Reply: None
NOTES
1. Select: Assert/deassert SL or set inventoried to A or B.
2. Query: A→ B or B→ A if the new session matches the prior session; otherwise no change to the inventoried flag.
QueryRep/QueryAdjust: A→ B or B→ A if the session matches the prior Query; otherwise, the command is invalid and ignored by the Tag.
3. Query starts a new round and may change the session. Tags may go to ready, arbitrate, or reply.

Fig. 2. Tag State Diagram. Source - "EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz", EPCglobal Inc., [2].

5 Comparison with Draft Protocol

The pros and cons of the Generation 2 Algorithm as compared to the Draft protocol can be categorized as follows:

Simplicity:

- Draft Protocol - Simple binary tree approach. Tags go through minimal number of "States" in order to be recognized. The acknowledgment from the reader is a single bit.
- Gen 2 - The number of states the tags need to go through is higher. Reader's acknowledgment consists of 16 bits.

Speed:

- Draft Protocol - Due to reduced number of tag "States", and single-bit acknowledgments, this protocol is more speed-efficient. There is no exchange of handles between the tags and reader.
- Gen 2 - The larger number of states the tags need to go through, coupled with the 16-bit handles and acknowledgments slows down the protocol

Security:

- Draft Protocol - Since the reader acknowledges every bit the tag sends out, an eavesdropper could easily know the IDs of all the tags recognized from listening to the reader, though it cannot listen to the tags directly.
- Gen 2 - Here, the reader never repeats the ID of the tag. The only thing an eavesdropper reader can hear is the 16-bit acknowledgement from the reader. When information is sent to the tag from the reader, it is cover-coded with the handle. (EXORed with 16-bit random number generated by the tag)

Compatibility:

- Draft Protocol - The tag structure is not compatible with the current ISO standards followed by the industry.
- Gen 2 - Tag structure is such that existing ISO standards can also use the protocol easily.

Tag Structure:

- Draft Protocol - Simple 64/96/256 – bit continuous memory with header, first bits, domain manager, object class and serial number
- Gen 2 - Tag memory is larger and complicated being divided into 4 banks each with different subdivisions

Time:

- Draft Protocol - Minimum, optimal time is utilized in the recognition of tags.
- Gen 2 - Significantly greater time is consumed to incorporate the greater security measures.

6 Results

In order to compare the performance of the Generation 2 protocol with the Draft Class 0 Protocol analyzed in our previous paper [1], we have simulated both the protocols for the maximum case of 19 tags. The results of the simulation are shown in Figures 3-5.

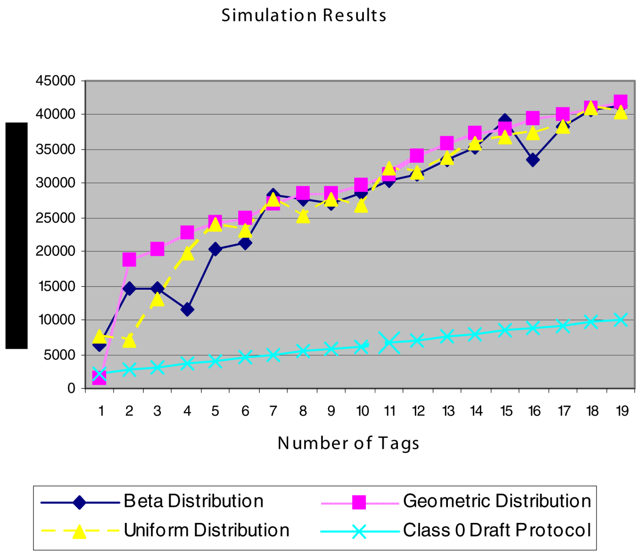

Fig. 3. Comparison of Class 0 Draft Protocol and Generation 2 protocol (for Beta, Geometric and Uniform distribution cases of generation of tag IDs)

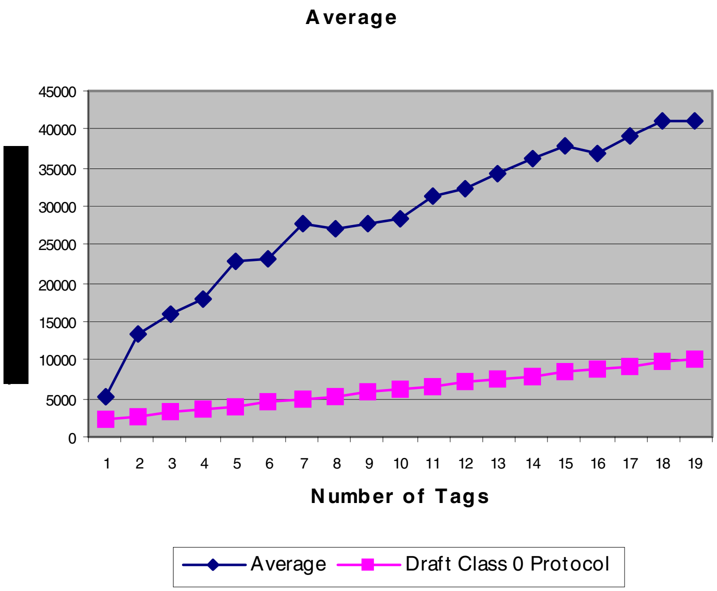

Fig. 4. Illustration of comparison with average values

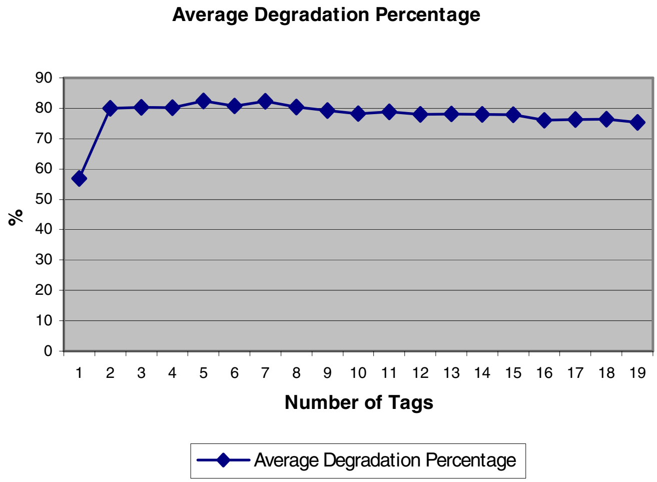

Fig. 5. Degradation of Gen 2 protocol over the Draft protocol

The degradation in performance over the Draft Class 0 protocol is apparent. For the case of 19 tags simulated here, an average degradation of 77.6% was observed.

7 Conclusion

The Generation 2 protocol has a very high standard of security. This comes with a heavy trade off against the rate of recognition of tags. At the same time RFID application in consumer goods area may not have much of a choice in considering an alternative anti-collision protocol as the risk of consumer identity/privacy theft is high and Generation 2 protocol provides the security that eliminates the vulnerability of the RFID EPC structure. From the point of view of a less rigorous application of the RFID system, where risk of presence of an eavesdropper is low, Class 0 draft protocol should be used as it provides a definite advantage over Gen 2.

References

1. Nanjundaiah, M., Chaudhary, V.: Improvement to the anticollision protocol specification for 900 MHz Class 0 Radio Frequency Identification Tag, IEEE Computer Society Press, proceedings the First International Workshop on Ubiquitous Smart Worlds (2005) 616-620
2. EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz, EPCglobal Inc., 31st January (2005), www.epcglobalinc.org
3. Draft Protocol Specification for a 900MHz Class 0 Radio Frequency Identification Tag, MIT Auto-ID Center, 23rd Feb (2003), www.epcglobalinc.org
4. Hernandez, P., J.D. Sandoval, J.D., Puente, F., Perez, F.: Mathematical Model for a Multiread Anticollision Protocol, IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, (2001) 647-650

5. Vogt, H.: Multiple Object Identification with Passive RFID Tags, IEEE International Conference on Systems, Man and Cybernetics, (2002) 6-9
6. Jacomet, M., Ehrsam, A., Gehrig, U.: Contactless Identification Device with Anticollision Algorithm, IEEE Conference on Circuits, Systems, Computers and Communications (1999) 269-273
7. Law, C., Lee, K., Siu, K.Y.: Efficient Memoryless Protocol for Tag Identification, Proceedings of the 4th ACM International workshop on Discrete algorithm s and methods for mobile computing and communications, (2000) 75-84
8. Zhou, F., Jin, D., Huang, C., Hao, M.: Optimize the Power Consumption of Passive Electronic Tags for Anti-collision Schemes, ASIC Proceedings of 5th International Conference, (2003) 1213-1217
9. R. Hush, D.R., Wood, C.: Analysis of Tree Algorithms for RFID Arbitration, Proceedings of International Symposium on Information Theory, (1998) 107