Research Trends To Avoid Collision in RFID Technology: A Review

Umesh Tilake[1], Miss. Priyanka Jaiswal[2], Dr. Manish Jain[3]
[1, 2, 3] Dept of Electronics and Telecommunication Engineering,
[1, 2, 3] R. K. D. F. Institute of Technology, Bhopal (MP), India

Abstract- *Acceptance speed of Radio Frequency Identification (RFID) tools is rising in mass-market implementation will not be achieved until an only some major challenges are addressed. These challenges are privacy, security, efficiency and costs from the end-user's view point and limited power supply to the tag from the engineering perspective. We talk about the follow a line of investigation efforts aimed at addressing these challenges. We focus our attention on research in: RFID collision avoidance schemes for electronics-based RFID devices, power management circuits and techniques, and efficient RF spectrum utilization. We conclude by drawing attention to three additional areas such as privacy and security, antennas that we believe are in need of more research. In this paper we look at on-going research activities in the RFID field as a whole and begin by discussing the major challenges that RFID technology is facing today and next we discuss the research efforts that are underway to try and address these challenges. We also draw attention to main area that we believe need more research in order for the goal of wide high speed and efficient adoption of this technology to be achieved. In this work we aim to illustrate the anti-collision-algorithms investigation used in this technology.*

Motivation for this paper:

Given the support of the fields put in to RFID technology and the fast altering character of the tools it is difficult for students and others who desire to start on research in this area to find a complete survey of the entire landscape. As summarize in the next part some good survey papers on several particular aspects of the technology do exist, but no cause exists where a new researcher can get an overview of the main follow a line of investigation efforts taking place in the field as a total in order to help conclude where one might want to focus one's research.

I. INTRODUCTION

Radio Frequency Identification (RFID) is one of automatic identification methods such as a barcode, a magnetic sensor, and IC card and the like; and means a technology used for wirelessly identifying data stored in a tag's microchip by using RF waves. Ubiquitous tagging is a paradigm where everything related has a unique tag associated with it. Picture the scenario that every object in the world can be uniquely identifiable with some form of electronic tags. This would have tremendous benefits in terms of tracking and identifying an object, making ubiquitous identification possible. As ubiquitous identification systems have become commonplace in access control and security applications areas, RFID systems are increasingly being used a s the automated identification system for these applications. Object identification problem requires the identification of multiple objects at the same time reliably and minimal user intervention. Conventional techniques like bar codes are not so efficient at solving this problem. Optical barcodes suffer from several drawbacks, but RFID can overcome the drawbacks of the barcode.

RFID is regarded as a substitute technology for the barcode which is currently used in distribution and circulation fields and financial services. However, RFID has troubles among the reliability of the recognized data and the interruption of the technology consistency; researches on anti-collision protocols have been required to improve the characteristics of a read rate and an identification speed. Meanwhile there are commonly two types of collisions: reader collisions and tag collisions. The reader collision specifies that a plurality of reader's necessities inquiries to one tag concurrently, so it is puzzling for the tag to identify the inquiries. On the contrary, the tag collisions indicate that a plurality of the tags responds to one reader's inquiry simultaneously and therefore the reader cannot recognize any tag. Especially, in case of the tag collisions for passive RFID systems, the tags which are currently used or which will be used in the large scale distribution and circulation fields are low-cost passive tags, resulting in some restrictions such as complexity of calculating, and cost increase by the memory size and the battery installation when applying usable anti-collision protocols

RFID tag anti-collision procedure designed to solve main collision issue of tags these techniques are grouped into deterministic technique and probabilistic technique. The deterministic technique which are on the based on tree dependent protocols identify tags by creating binary trees

through the use of binary bits of tag IDs and then by forwarding the nodes of the trees. Such deterministic methods can be classified into a memory based algorithm and a memory less based algorithm. In contrast, the probabilistic methods are based on slotted aloha based protocols. They can be classified into an ID-slot algorithm and a bi-slot algorithm. According to the suggestion of EPC global, each of them is adopted in Class 0, Class 1, and Class 1 Generation 2 proposed to ISO/IEC 18000-6C of the International Standard Organization. The remain paper is planned as follows; in Section 2 we review related work and discuss our contributions in selected field in Section 3 we outline the primary challenges for RFID technology today, and then in Section 4 we discuss the main research efforts related to RFID. We conclude with a few remarks in Section 5.

RFID systems are composed of three main components as shown in Figure 1:

- One or more RFID tags, also known as transponders (transmitter/responder), are attached to the objects to count or identify. Tags could be either active or passive. Active tags are those that are partly or fully battery powered, have the capability to communicate with other tags, and can initiate a dialogue of their own with the tag reader. Passive tags, on the other hand, do not need any internal power source but are powered up by the tag reader. Tags consist mainly of a microchip and coiled antenna, with the main purpose of storing data.
- A reader or transceiver (transmitter/receiver) made up of an RFI module and control unit. Its main functions are to activate the tags, structure the communication sequence with the tag, and transfer data between the application software and a tag.
- A Data Processing Subsystem, which can be an application or database, depending on the application.

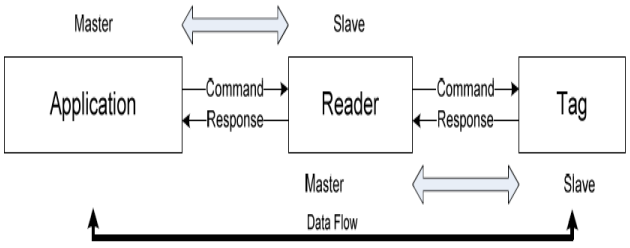

Figure 1: Communication in RFID Systems and application.

The application software initiates all readers and tags activities. RFID provides a quick, flexible, and reliable way to electronically detect, track and control a variety of items. RFID systems use radio transmissions to send energy to a RFID tag while the tag emits a unique identification code back to a data collection reader linked to an information management system. The data collected from the tag can then be sent either directly to a host computer, or stored in a portable reader and up-loaded later to a computer.

1) **Tree based Tag Anti-Collision Protocols**

a) Binary tree working algorithm:

A reader chooses '0' or '1' for the initiative. If the reader makes a choice, the identification Process should keep the way of choice order when the tree splits at a node. Then the binary Tree working algorithm (BTWA) is operated as follows:

Step 1: The reader transmits k-length prefix.

Step 2: Tags send $(K+1)^{th}$ bit if the first k bits of tag ids are the same as the prefix.

Step 3: If the received bits collide, the extended prefix attached '0' or '1' to the prefix is Retransmitted by the reader. If they do not collide, the received bit is attached to the Prefix for the next prefix. If there is no response, the branch is ignored. Also, a Collision occurs at the last bit of the tag ids, the reader assumes there are two tags Because of the uniqueness of the tag ids.

Step 4: The reader repeats the procedure until all branches are searched.

b) query tree algorithm:

The query tree algorithm (QTA) is based on BTWA. The difference between QTA and BTWA Is as follows:

Step 1: Tags send from $(K+1)^{th}$ bit to the end bit of tag ids if the first k bits of tag ids are the same as the prefix.

Step 2: If there is a collision, the extended prefix attached '0' or '1' to the prefix is Retransmitted. Furthermore, if there is no collision, the reader identifies a tag corresponding to the detected id, which is the connection of the prefix and the Response.

c) collision tracking tree algorithm:

The collision tracking tree algorithm (CTTA) is based on QTA except that this scheme uses Collision tracking. The difference between CTTA and QTA is as follows:

Step 2: tags send their IDs from $(K+1)^{th}$ bit to the end bit if the prefix is the same as the first k bits of tag ids. However, the tags stop sending their ids when an ACK signal is received. The reader checks whether a collision occurs or not in each bit on the Received sequences, and transmits an ACK

signal to stop being sent the tag ids by tags if there is a collision.

Step 3: If there is a collision at nth bit in the received sequences, the two new Prefixes, 'the former prefix k bits + the received n-1 bits + 0 or 1', are retransmitted sequentially to the tags in the field of the reader. Furthermore, if there is no collision, the reader identifies a tag corresponding to the detected id, which is the connection of the prefix and the response.

2) slotted aloha based tag anti-collision Protocols

a) I-code

I-code is similar to the frame slotted aloha (FS-ALOHA). In FS-ALOHA, a reader gives the Information, which includes read range, clock, and frame size, to tags. Then the tags choose a slot with random back off time in a frame to send their IDs. If a tag is identified by the Reader, the tag changes its state as `inactivated'. Do this procedure during the number of Cycles determined by target accuracy in markov process. How to choose a frame size with the unknown number of tags can be a good research subject.

b) STAC

STAC is based on FS-ALOHA. The only difference is that STAC reduces the waste of time Caused by empty slots in a frame. In the FS_ALOHA algorithm, there is no consideration for Empty slots which makes the algorithm inefficient. In the STAC algorithm, a reader sends the 'close slot sequence' to tags when an empty slot occurs. Thus, the empty slot interval is reduced.

c) Bit-Slot

The bit-slot algorithm is a kind of reservation based algorithm, which assigns the order of Transmitting tag ids by using the reservation sequences. With the reservation sequences, the Overhead for assigning slots to transmit the tag ids is reduced. In the bit-slot algorithm, tags Send reservation sequences randomly generated by only one `1' and several `0's, and a Reader checks the reservation sequences whether the positions of `1' in the sequences are Collided or not. Then, the reader stores the record of the matching reservation sequences to call each tag, and communicates with each tag sequentially.

d) PS-ALOHA in EPC class 1 gen.2 protocol

The performance of aloha based systems is usually measured by the throughput indicating the efficiency of a system, which can be expressed as the number of success slots over the Total number of attempt slots. Typical aloha systems with a fixed frame size show good Throughput only for the specific number of tags in the field of a reader, but the throughput Decreases dramatically as the number of tags increases. To solve this problem, a dynamic Frame slotted DFS-ALOHA algorithm is devised to maintain the good throughput for any Number of tags, where its frame size is flexibly changed according to the number of tags. EPC class 1 gen.2 protocol adopts the probabilistic slotted PS-ALOHA algorithm as its Anti-collision scheme. Most parts of the ps-aloha in EPC class 1 gen.2 protocol are like to the usual DFS-ALOHA, but the algorithm has its own uniqueness as Follows:

I. Slots controlled by readers: each slot is controlled not by the Synchronized clock but by the commands of a reader. Thus, the reader makes a slot finish its duration when the slot is empty, and makes the next slot start for reducing The waste of time caused by the empty slot occurring in the middle of a frame.
II. Temporary ids: instead of the tag ids with dozens or hundreds of bits in a slot, The temporary ids, which consist of 16-bit random numbers (rn16s), are used for the Collision detection in a slot, and also used when the reader queries identified tags. The temporary ids reduce the duration of the slots, and enhance the security of Reader-tag communications because the randomly generated temporary id is used as the key of taking the tag id.
III. States of tags: the identified tags change their states from 'arbitrary' to 'acknowledged ', and do not participate in the next inventory rounds (frames). Thus, the Number of tags, which attends the next inventory rounds, decreases.

Figure 6 briefly indicates the EPC class 1 gen.2 protocol. At first, a reader broadcasts the Frame size and notifies the beginning of a frame to all tags with a query command. After the Frame is started, each tag generates a 16-bit random number (M16) as a temporary id, and Selects a slot in the frame. Next, the reader proceeds to transmit a QueryRep command to The tags for being counted the slot index by the tags. The tags count the slot indexes, and Backscatter their rn16s in their own slot time. If a collision occurs, the reader queries the Next slot by sending another QueryRep command. If only one tag responds to the slot, the Reader transmits an ACK command with the received rn16. Then, the tag replies its tag id With 16-bit CRC redundancy bits to detect errors. After receiving the tag id, finally, the reader Checks errors, and transmits the QueryRep command if the tag id is valid. Otherwise, the Reader transmits a NAC command.

II. CONCLUSION

RFID is a technology with the potential to improve the way we live our lives and the way we conduct business. However, for this potential to be realized the challenges listed above, particularly those relating to security and privacy, will have to be thoroughly addressed. It is our hope that this paper has highlighted the technology's potentials, the on-going research to address the challenges, and the areas in need of more attention in terms of research.

REFERENCES

[1] R. Weinstein, "RFID: A Technical Overview and Its Application to The Enterprise," *IEEE IT Professional*, Vol. 7, Iss. 3, pp. 27-33, May-Jun. 2005.

[2] Y. Xiao, X. Shen, B. Sun, and L. Cai, "Security and Privacy in RFID and Applications in Telemedicine," *IEEE Communications Magazine*, Vol. 44, Iss. 4, pp. 64-72, Apr. 2006.

[3] J. Landt, "The History of RFID," *IEEE Potentials*, Vol. 24, Iss. 4, pp. 8-11, Oct.-Nov. 2005.

[4] D.-H. Shih, P.-L. Sun, D. C. Yen, and S.-M. Huang, "Short Survey: Taxonomy and Survey of RFID Anti-collision Protocols," *Computer Communications*, Vol. 29, Iss. 11, pp. 2150-2166, Jul. 2006.

[5] J. Myung, W. Lee, and J. Srivastava, "Adaptive Binary Splitting for Efficient RFID Tag Anticollision," *IEEE Communications Letters*, Vol. 10, No. 3, pp. 144-146, Mar. 2006.

[6] B. Johansson, "An Introduction to RFID – Information Security and Privacy Concerns," TDDC'03 Projects, Spring, 2004.

[7] S. A. Weis, S. Sarma, E. R. L. Riovest, and D. W. Engels, "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems," *Lecture Notes in Computer Science (LNCS)*, Vol. 2802, pp. 201-212, 2004.

[8] A. Juels and R. Pappu, "Squealing Euros: Privacy Protection in RFID Enabled Banknotes," *LNCS*, Vol. 2742, pp. 103-121, 2003.

[9] S. E. Sarma, S. A. Weis, and D. W. Engels, "RFID Systems and Security and Privacy Implications," *LNCS*, Vol. 2523, pp.454- 469, 2003.

[10] S. H. Weigart, "Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses," *LNCS*, Vol. 1965, pp.302-317, 2000.

[11] R. Anderson, and M. Kuhn, "Low Cost Attacks on Tamper Resistant Devices," *LNCS*, Vol. 1361, pp.123-136, 1997

[12] A. Juels, "Minimalist Cryptography for Low-cost RFID Tags," *LNCS*, Vol. 3352, pp. 149-164, 2004.

[13] A. Juels, R. L. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," *ACM Conference on Computer and Communications Security*, pp. 103–111, Oct. 2003.

[14] A. R. Koelle, S. W. Depp, J. A. Landt, and R. E. Bobbett, "Shortrange Passive Telemetry by Modulated Backscatter of Incident CW RF Carrier Beams," *Biotelemetry*, Vol. 3, pp. 337-340, 1976.

[15] D. Krebs and M. J. Liard, "White Paper: Global Markets and Applications for Radio Frequency Identification," *Venture Development Corporation*, 2001.

[16] T. S. Flor, W. Niess, and G. Vogler, "RFID: The Integration of Contact-less Identification Technology and Mobile Computing," *The 7th Inter. Conf. on Telecommunications*, Vol. 2, pp. 619-623, Jun. 2003.

[17] S. M. Birari and S. Iyer, "Mitigating The Reader Collision Problem in RFID Networks with Mobile Readers," *Jointly held with the 2005 IEEE 7th Malaysia Inter. Conf. on Communication Networks and 2005 13th IEEE Inter. Conf. on Networks*, Vol. 1, pp. 463-468, Nov. 2005.

[18] D. W. Engels and S. E. Sarma, "The Reader Collision Problem," Proc. IEEE Inter. Conf. on Systems, Man and Cybermetics, Vol. 3, Oct. 2002.