Journal of Computer Science & Computational Mathematics, Volume 6, Issue 1, March 2016
DOI: 10.20967/jcscm.2016.01.003

A New Mechanism to Tag Collision Avoidance in Radio Frequency Identification (RFID) Systems

Somayeh Aghayi[1*], Ahmad Habibizad Navin[2]

[1]Sama Technical and Vocational Training College, Islamic Azad University, Ardabil Branch, Ardabil, Iran
[2]Department of Computer Engineering, East Azarbaijan Science and Research Branch, Islamic Azad University, Tabriz, Iran
[*]Corresponding author email: somayeh.aghayi@gmail.com

Abstract: RFID tags are increasingly used for identifying and tracking purposes. In many applications, such as shop gateways, it is possible that more than one tag come within the range of the reader, which may interfere with the detection of tags or the data exchange. This paper presents a method based on the combination of CSMA and query tree to manage multiple accesses and avoid collision. This method is implemented in two stages. First, the tags with the unique short addresses are detected, and then remaining tags are identified in the next stage. The simulation results of the proposed method in MATLAB Software show improved common access parameters and reduced latency compared to the similar methods, which is due to the processing of the shortened address rather than the whole address.

Keywords: RFID tag, collision, CSMA, query tree, multiple access.

1. Introduction

Digital data storage peripherals are progressing rapidly in tandem with other branches of computer science. In the past, data were saved and transported in punch cards, floppy disks and compact discs [1]. The features provided by the network systems such as e-mail, wireless networks such as wireless sensor networks (WSNs), integrated Wireless Networks and mobile phones have fostered a remarkable development in the communications industry [2-6].
RFID system is composed of two hardware parts: 1) the tag that contains the stored data, 2) the reader, which not only establishes a wireless conception with the tag, but also can receive and interpret the data stored in the tag. Obviously, writing data in the tag memory requires a writer device, which is among the peripherals and thus not involved in the detection process [7].
As shown in Figure 1, RFID tag is a small electronic device composed of a microchip and an antenna, which is similar to barcodes and magnetic stripes installed on the credit cards or ATM card. This system provides a unique specification for each object that distinguishes it from others. As information can be read from a barcodes or magnetic stripes, it can be read from RFID tags as well. RFID tags can be read to both receive and even modify information [9]. Tags can withstand temperature from 40 to 200 °C, which makes them resistant to fire [10]. RFID technology has changed the way organizations conduct business by providing a way to track materials and products from the production line to the supply chain. It is used in industry to prevent errors, improve efficiency of the existing controls and reduce inspection and handling costs [11].

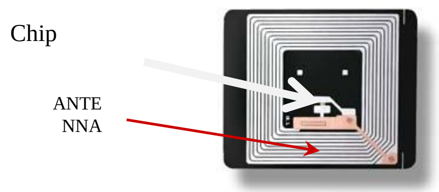

Figure 1. A tag and its components [8]

The technology used, is not limited to tracking products, vehicles, animals and even human. Furthermore, the new tags are washable and highly durable [12]. RFID technology has high potential for the new developments and applications, the success of which depends on the extent the issues such as high costs are addressed properly. Among these problems is the simultaneous transmission of data by multiple tags, which can result in collision and reduced efficiency.
During the detection process, first the transmitter embedded in the reader emits radio waves in the reception range. These waves not only establish connection with the tags, but also provide the power required for the transmission of data. When a tag is within the electromagnetic field of the reader, it is influenced by the signals sent by the tag transmitter. In fact, it activates the chipset in the tag, which emits the information stored in the tag via antenna. Then, the reader receives, decodes and, if necessary, saves the transmitted information. The reader can be attached to computer, and it can send the received information to a database. When recorded in the database, the data are processed and used for a variety of applications in the internal structure of an organization. The radio ranges of the reader, depending on the power of an antenna, can be 100 meters or more [13]. In this system, radio waves are used to exchange data. Unlike mobile waves and microwaves, radio waves are not harmful to human health. As such, the tags can be implanted in humans without any side effects to identify individuals and any time and any place [14].
As noted earlier, it is possible for more than one tag to come into the effective range of the reader, all trying to send their information or identity. In these cases, a collision occurs, which may lead to the failure of data transmission and reduced efficiency of the whole system.
Considering the importance of this issue, this paper seeks to assess the effectiveness of the CSMA method in avoiding collisions by running simulations in the MATLAB software environment. Section II reviews the common methods of shared access to a channel. Section III describes the

proposed method and in Section IV, the efficiency of the proposal is evaluated.

2. Related Works

Multiplexing is a common method used for shared access on multiple networks to a communication channel, which can be either static or dynamic (respectively in the physical layer and the data link layer) [6]. Frequency division multiplexing, time division multiplexing and wavelength division multiplexing are examples of static methods [6] which would be examined thoroughly. A static method is usually used in telephone networks, fibre-optic and wired communications and they are not recommended for wireless channels like RFID due to the echoes or repetition issues [7].

Dynamic methods are studied in the medium access control (MAC) protocols. A number of algorithms have been proposed for the shared access of multiple networks to one channel including ALOHA, CSMA, Token-passing, Bit-Map, Binary Countdown, MACA and MACAW [6-13].

The basic idea of ALOHA protocol is very simple: the users are allowed to transmit whenever they have any data. If a collision occurs, the data are lost. The collision can be detected using a return channel. That is, when a collision occurs, the transmitter waits for a random period before it transmits again. It can be proved that the efficiency of this method for transmission rate (load) of 0.5 can reach a maximum value of 0.184 [6].

In 1972, a method was proposed that could double the efficiency of ALOHA. In this method, the time was divided into discrete sections that corresponded to the required time for sending a package. To be able to transmit data, each network should wait until the next section. As a result, the vulnerability period was halved, and the efficiency was increased by 0.368% [6].

Before data transmission, CSMA (Carrier Sense Multiple Access) protocols check whether a channel is free, and the transmission process is launched only if the channel is free. Thus, it has better performance than ALOHA method.

CSMA protocols differ in the way they react to a busy channel. They are classified into three major categories: persistent, p-persistent and CSMA with collision detection (CSMA-CD) [6]. In the persistent method, the network senses the transmission medium, i.e. channel, before transmitting any data. If the channel is busy, it waits persistently until it is free. Otherwise, it transmits the data. In p-persistent protocol, where P = [0 1], the probability of transmission by network is equal to P if the channels free, and it is transformed into a persistent protocol in P=1.

As the value of P decreases, the efficiency is improved .In CSMA with collision detection, each network can detect the occurrence of the collision by checking the power consumption or comparing the width of the received signal with the transmitted signal. It can stop the transmission in the event of collision to avoid vain bandwidth consumption [6].

Other protocols are known as non- collision; however, due to the prolonged running time and channel assignment, they are not discussed in this paper.

3. Tag Detection by Combining CSMA and Tree Query

A number of tree-based collision prevention algorithms have been proposed for tag detection. The algorithm based on binary tree studied by Capetanakis [7] and algorithm based on query tree investigated by Zhang [8] have been proposed and discussed to avoid collisions. The algorithm based on binary tree is structurally similar to ALOHA, though the presence of a random number generator, which requires high processing power, has limited its application only to active tags, and it cannot be applied to passive tags [7].

Similar to the network card that has a unique hardware address known as MAC, each tag has a unique identifier too. Tag identifiers comply with EPC standards (Electronic Product Code). The EPC addresses are 96 bits long, and their structure has been shown in Table 1 [1].

Table 1. Best results

Header 8 bits	**General management number 28 bits**	**Object class 24 bits**	**Serial number 36 bits**

The use of 96-bitsEPC unique-address principle, and query tree eliminate the chance of collision in tag detection, however, it is a time consuming process which makes it practically useless. Accordingly, message digest protocols like MD5 shorten standard 96-bit addresses to maximum 22-bit addresses which are used to detect tags [6]. The address shortening, however, generates duplicated addresses. In what follows, we will propose a method to manage the duplicated addresses and to prevent collisions, which use a combination of the query tree algorithm and CSMA protocol.

Query-tree based algorithm consists of the request and response stages. In each round, the reader sends a request with the prefix p (which is very short at the beginning). Only tags whose identifier prefix is matched with the reader's request are able to reply to the request of the reader. If the reply is sent only by one tag, it is detected immediately, and therefore prevents the collision. Otherwise, the reader repeats its request again by prolonging the prefix string.

This process continues until the prefix length is equal to the length of the identifier. In this case, if there are still two or more tags with the same identifier, the algorithms fails and collision is reported. In a study by Binett et al. [1], a method based on query tree and ALOHA called Hybrid Query Tree (HQT) has been discussed, which is 100% efficient, but has long delay [1].

Fig. 3 shows an example of how a query-tree based algorithm works on the condition when there are three tags with 3-bit shortened identifiers that are competing for detection. Suppose there are three tags with short addresses001, 011 and 011 waiting for detection. Since address 011is unique, it can only be detected by the query - tree algorithm, which is shown in green. The other two tags, however, can only be detected by CSMA, which are shown in red due to the occurrence of collision. Query node has been created to detect the tag with address 010, which is shown in blue, but there is no such a tag in reality. This approach to query-tree leads to wasting of time. To avoid collision in this case, we can use CSMA protocol. In the next section of the paper, the efficiency of CSMA protocol in resolving collision problem in cases similar to Fig. 3 will be assessed by simulation.

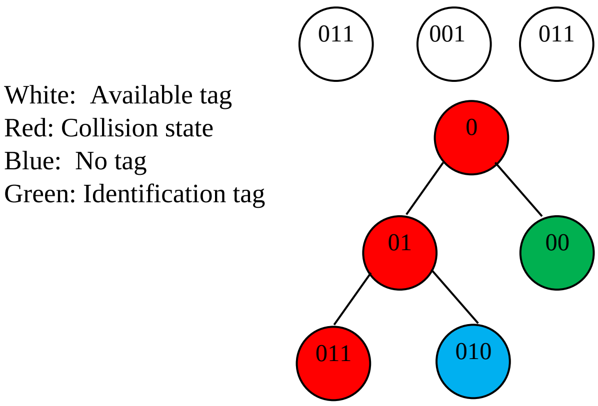

Figure 2. An example of a query tree

4. Evaluating the Efficiency of the Proposed Method

Assuming that there are *n* tags at a time in the range of the reader, and MD5 shortening algorithm transforms EPC address into a bit string with the length, in which m<96, then according to Eq. 1, α is the probability of a tag with duplicate address. It is because in this case only 2^m addresses can be generated.

$$s2^{m}=\alpha \tag{1}$$

According to the same analysis, the probability of two tags with unequal shortened address will be 1-α, which is represented by β. In this case, if *k* is the number of tags, which because of their equal shortened address cannot be detected just by using enquiry tree, then the efficiency of this method (σ) can be calculated from Eq. 2 [1].

$$=1-\sum_{k=2}^{n}\left(1-\frac{nID}{N}\right)\binom{n}{k}\beta^{n-k}a^{k} \tag{2}$$

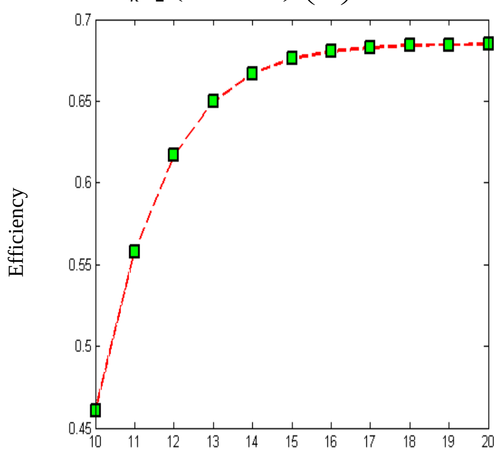

Figure 3. The efficiency of query tree during the short address (m)

Now, if the identification of tags cannot be completed in the first round by using query tree, the identification process with CSMA begins. In this case, if tags find a free channel, they communicate with the reader and attempt to transmit data.

Obviously, all networks can find free channels after a while, which can improve the overall efficiency. The main challenge, however, is time. What matters most is the time required to detect all tags, and the shorter the time, the higher will be the optimality. Figure 5 shows the time required to detect1000 tags in the proposed method in terms of length of microseconds for shortened addresses 14 to22 -bit long. In this diagram, the time delay under similar condition for HQT [1] for N = 2 and N = 4 has been shown for the sake of comparison. N is the length of the frame in ALOHA [1]. Figure 5 shows the reduced average delay in the proposed method compared to previous ones. Thus, this method accelerates the identification of tags. However, if 17-bit shortened address is selected, HQT method with frame length 2 will have shorter delay, though the average delay is always less than HQT.

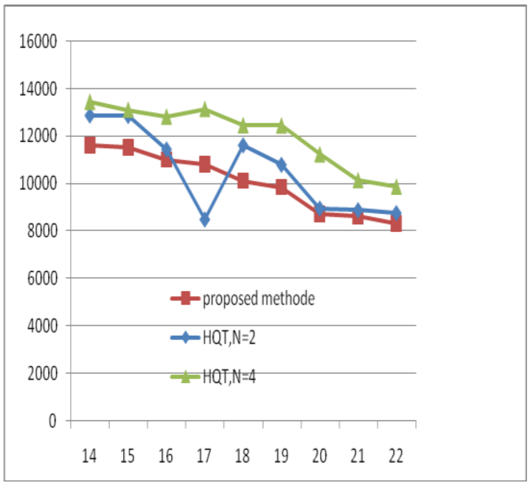

Figure 4. Comparison of the delay in the proposed method and HQT

5. Conclusion

Given the importance of shared access to the channel, this paper presents a method that combined query tree algorithm and CSMA protocol to detect addresses of RFID tags. The simulation results of the proposed method showed that the use of CSMA as the supplement to enquiry tree improved the efficiency and reduced the latency. Moreover, since most processing was on the side of reader, the processing overhead of the tag was very low, which allowed applying the proposed method to passive tag with low power. Despite the high scalability of the proposed method, its main disadvantage was the increased overhead resulted from mode storage in fitting with the increased number of tags. The study and improvement of the algorithms to access the content of tag memory would be the next research project undertaken by the author.

References

[1] G. Binetti, G. Boggia, P. Camarda, L. A. Grieco, "A Hashing-based Anti-Collision Algorithm for RFID Tag Identification," in: *4th International Symposium on Wireless Communication Systems*, ISWCS 2007.

[2] M. Golsorkhtabaramiri, M. Hosseinzadeh, A. Golsorkhtabaramiri, S. R. Heikalabad, "HCABS: The hierarchical clustering algorithm based on soft threshold and cluster member bounds for wireless sensor networks," in: *IEICE Electron. Express*, vol. 9, no. 7, pp. 685-690, 2012.

[3] M. Golsorkhtabar, M. Hosinzadeh, M. Heydari, S. Rasouli, "New Power Aware Energy Adaptive protocol with Hierarchical Clustering for WSN," *(IJCNS) International Journal of Computer and Network Security*, vol. 2, no. 4, April 2010.

[4] M. Golsorkhtabar, F. Kaviani nia, M. Hosseinzadeh, Y. Vejdanparast, "The Novel Energy Adaptive protocol for Heterogeneous Wireless Sensor Networks," in *Proc. of IEEE ICCSIT 2010*, Chengdu, China, vol. 2, pp. 178-182, July 9-11, 2010.

[5] M. Golsorkhtabaramiri, M. Hosseinzadeh, "A novel stable cluster-based protocol for heterogeneous RFID enhanced wireless sensor networks," *QScience Connect*, 2013.

[6] A. Tanenbaum, D. Wetherall, Computer Networks (5th Edition), October 7, 2010 | ISBN-10:132126958.

[7] J. I. Capetanakis, "Tree algorithms for packet broadcast channel: Protocol and capacity considerations," Ph.D. dissertation, MIT, Dept. of Electrical Engineering and Computer Science, 1977.

[8] A. Chenrui Zhang, T. Xianwei Li, "SAW-RFID enabled temperature Sensors and Actuators," A: Physical, vol. 20, pp. 105-113, 2013.

[9] EPC Generation 1 Tag Data Standards v. 1.1 rev. 1.27, EPC, May 2005.

[10] R. Rivest, The MD5 Message-Digest Algorithm, IETF RFC 1321, 1992.

[11] W. Stallings, Cryptography and Network Security, 4th ed. Prentice Hall, 2006.

[12] C. Metzger, F.Thiesse, St. Gershwin, E. Fleisch, "The impact of false-negative reads on the performance of RFID-based shelf inventory control policiesComputers & Operations Research," vol. 40, no. 7, pp. 1864-1873, 2013.

[13] J-L. Chen, M-C. Chen, C-W. Chen, Y-C. Chang, "Architecture design and performance evaluation of RFID object tracking systems", *Computer Communications*, vol. 30, no. 9, pp. 2070-2086, 2007.

[14] M. K. Lim, W. Bahr, S. C. H. Leung, "RFID in the warehouse: A literature analysis (1995–2010) of its applications, benefits, challenges and future trends", *International Journal of Production Economics*, vol. 145, no. 1, pp. 409-430, 2013.