A RFID QoS Mechanism for IoT Tracking Applications

Rafael Perazzo Barbosa Mota
Department of Computer Science
University of São Paulo - USP
São Paulo, São Paulo, Brazil
Email: perazzo@ime.usp.br

Daniel M. Batista
Department of Computer Science
University of São Paulo - USP
São Paulo, São Paulo, Brazil
Email: batista@ime.usp.br

***Abstract*—In this paper, we propose a mechanism that reduces useless responses for RFID systems in the Internet of Things (IoT) environment, for tracking applications. The mechanism achieves its objectives by reducing the number of packets exchanged between readers and tags. We analyze the behavior of our proposal by considering the average number of identification rounds. With extensive simulations using an RFID module for the ns-2 simulator, we show the benefit of the proposed mechanism. When compared to the Pure Q Algorithm and Binary Tree Slotted Aloha, our mechanism reduces the number of packets up to 43%, which is a good result in terms of performance of IoT applications and energy consumption of the devices used in the communications.**

I. Introduction

The "Internet of Things" (IoT) consists in a vision where objects become part of the Internet: every object has its unique identification, and is accessible from the network, providing an expanded Future Internet [1]. In this scenario it is expected, for example, that the users use the Internet to check the location of people and their belongings within a pre-defined area. It is needed that readers periodically send requests to store the data of people and objects.

RFID [2] is a key technology of the IoT since small passive RFID tags make it possible to link millions and billions of physical products with the virtual world [3]. When a large number of tags are used, there is a high probability that there will be more than one tag within the reader zone at some time. When the tags transmit their responses simultaneously to the reader, collisions will happen because the communication is done over a shared wireless channel. Therefore, RFID tag anti-collision mechanisms will play an important role in the IoT [3], [4], [5]. Therefore high probability of producing collisions due to the high number of RDID devices available will be an important issue to be solved.

Many efforts have been made in the literature to improve the performance of anti-collision protocols [3], [6], [7], [8], [9], [10], [11], [4], [12]. However, little research has been conducted for IoT scenarios [9]. According to [13] there are several disadvantages of using the Q algorithm, the standard Algorithm for Class 1 Generation 2 RFID systems, because too many packets have to be transmitted, in a single identification process, between the reader and tags. This process adds considerable overhead and increases the power consumption, since the energy consumption is proportional to the number of actions of the readers [14]. In an IoT scenario, where readers regularly consult the tags and make them available on the Internet, the problem is compounded, generating even more overhead.

The aim of this paper is to propose a mechanism to increase the chances to meet QoS requirements for IoT tracking scenarios, whose nodes are RFID tags, reducing the number of delay slots (idle and collision) and consequently the amount of messages exchanged in the network, compared to the Pure Q Algorithm and to the Binary Tree Slotted Aloha - BTSA.

The proposed mechanism had its performance evaluated through simulated experiments in the simulator ns-2 [1], and the results confirm its effectiveness. For instance, in a scenario with 500 tags, and using the proposed mechanism, there was a reduction in the number of delay slots of about 24%–43%.

The contributions of this paper are:

- A mechanism to decrease the delay slots in RFID systems used to deploy IoT applications;
- As a consequence of the first contribution, a decrease of energy consumed by readers;

This paper is different from those found in the literature because it performs experiments simulating real IoT scenarios [15] with an RFID ns-2 module, varying the number of tags, and because the proposed mechanism is compatible with the global standard communication protocol for passive RFID tags. Besides, it considers IoT scenarios, not only generic RFID scenarios without a specific aim.

The rest of this paper is organized as follows: Section II provides the background on anti-collision protocols and their development over the years in the literature. In Section III, we present the proposed mechanism and how our contribution differs from that of prior work. In Section IV we describe the scenarios simulated to evaluate the performance of the proposed mechanism. In Section V we analyze the results of the experiments with the mechanism by comparing it with the Pure Q Algorithm and BTSA. Suggestions of future work are presented in Section VI and we make some concluding remarks in Section VII.

II. Background and Related work

Anti-collision protocols play a critical role for RFID technology to realize multiple-object identification. These pro-

[1] http://www.isi.edu/nsnam/ns/

tocols are classified into two categories: deterministic and probabilistic [16]. Protocols of the first method split colliding tags into two subgroups (trees) until all tags are identified. Protocols of the second method are based on the ALOHA protocol. They are designed to reduce the probability of tag collisions by arranging the tags to respond at different times [16]. As these protocols depend on the generation of random numbers, they are classified as probabilistic. The main goal of current research in anti-collision protocols and/or mechanisms for RFID systems is to study "how to reduce identification wasted slots with a given number of tags in the field of an RFID reader considering an IoT tracking scenario" [16]. Aspects such as simplicity of implementation and similarity with existing standards should be taken into consideration (our mechanism follows the EPCGlobal standard [17]).

[16] proposes bi-slotted tree based tag anti-collision protocols, a bi-slotted query tree algorithm (BSQTA), and a bi-slotted collision tracking tree algorithm (BSCTTA), which reduce both prefix overhead and iteration overhead. After simulation results, they concluded that the bi-slotted tree based RFID tag anti-collision protocols require less time for tag identification than the existing tag anti-collision protocols. [10] proved that adopting the Dynamic Frame Slotted ALOHA (DFSA) algorithm, and adjusting the length of the frame and the number of groupings, improves system performance over traditional ALOHA. [11] proposes a novel anti-collision algorithm to increase the throughput of RFID systems, which considers the capture effect in the context of the framed ALOHA protocol; their results show that the proposed algorithm significantly outperforms other existing schemes. [3] has designed the most recent anti-collision algorithm, to the best of our knowledge, called Binary Tree Slotted ALOHA (BTSA), which mixes the Binary Tree and Aloha techniques. It has a better identification speed, however it is not optimized for practical settings, will not be as simple to implement as Frame Slloted Aloha - FSA or C1G2 with no known experimental prototype [13] and it does not consider the mobility aspect and periodic queries, such as are present in an IoT scenario. Although the mechanisms explained above have better performance than the standard algorithm Q, none of them was thought of in the context of Internet of Things scenarios, i.e., when applied in IoT environments, they carry unnecessary readings, increasing system overhead.

It is important to observe that our proposed mechanism can be applied by any of existing anti-collision protocols [16], [10], [11], since it does not change the way the reader identifies each tag.

III. The proposed mechanism: Mute Q Algorithm for the Internet of Things

The proposed mechanism is based on the principle that the tags do not need to reply to all reader queries. It can be used with any anti-collision algorithm proposed in Section II. If an identified tagged object has not left the current reader range, it does not need to send a reply. In this case the application middleware has already stored the object location. Hence the correct location is available to system users. Imagining an IoT scenario for tracking/localization, we can formulate this idea: not all objects leave the reader range space at the same time. As in this scenario readers send periodic queries, we can make the hypothesis that the packet traffic exchanged between readers and tags will be decreased because only necessary replies will be transmitted. Algorithm 1 shows the proposed Mute Q Algorithm for the Internet of Things (MQAIT). The mechanism needs only to be implemented on tags. The readers keep their normal operations. In summary, the tags should reply when they get requests from different readers (they must check their memory), otherwise they keep mute because the middleware knows their locations.

Algorithm 1: MQAIT: tag operation

```
   Data: Query Command - Assuming the tag has 0 as
         slot number
   Result: tag ID, or ∅
1  Receive Reader's Query
2  if (First request) then
3  |   Go to REPLY state;
4  |   Send ID;
5  |   if (tag has received an ACK command from reader)
   |   then
6  |   |   Store the reader ID on memory
   |   |   (tagMemory←readerID);
7  |   |   Go to ACKNOWLEDGE state;
8  |   end
9  else
10 |   if (tagMemory=readerID) then
11 |   |   Stays on ARBITRATE state;
12 |   else
13 |   |   Go to REPLY state;
14 |   |   Send ID;
15 |   |   if (tag has received an ACK command from
   |   |   reader) then
16 |   |   |   Store the reader ID on memory
   |   |   |   (tagMemory←readerID);
17 |   |   |   Go to ACKNOWLEDGE state;
18 |   |   end
19 |   end
20 end
```

The tags have to store the reader identification (lines 5–7 and 15–17) at the moment of ACK reception (lines 5–6). They will send a reply only if the reader identification is different from the identification stored in their memory (lines 10–14) or if they are receiving the first request for some reader (line 2). The readers' operation follows the same algorithm standard defined in [17].

The efficiency of the MQAIT algorithm will be compared to the efficiency of the traditional Q algorithm and BTSA in Section V.

IV. Scenarios and experiments

We consider a generic RFID tracking/localization system, as illustrated in Fig 1. In this scenario, fixed RFID readers (READER 1, READER 2, and READER 3) query the moving tags periodically (every minute, for example). The tags move with random speeds and cross the readers' identification ranges. Each identified *EPC code* is sent to a database connected to the Internet, where online users can track the location of the desired *thing*. The available location is based on the reader range. For instance: Room 1, Room 2, Exit, Emergency Exit, etc. A real generic example can be described as follows: Objects from Room 1 will be identified as long as they remain in this compartment. This scenario is based on experiments reported in [15]. A new identification will be made if they move to another compartment. The speed of moving objects does not affect the operation of the algorithm. This type of application is already used in several current situations as school uniforms, inventory control, scientific conferences and others [5]. It is important to observe that the increase in the number of readers do not modify the operation of the algorithm, since the readers are positioned in different compartments.

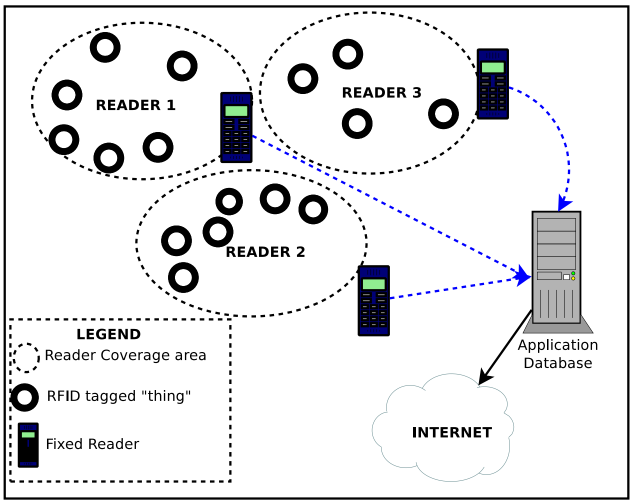

Fig. 1. Simulated tracking/localization scenario

Table I describes the parameters of the experiments.

TABLE I. PARAMETERS OF THE EXPERIMENTS

Simulated time	1800 seconds
Number of tags	100 to 900
Number of readers	3
Steps	200
Initial positions	Random (0–30 meters x 0–15 meters)
Movements	Random (0–30 meters x 0–15 meters)
Meaning	3 compartments with a reader covering only one location
Readers queries	Each reader issues a query command every minute
Topology	30x15 (meters)
Nodes speed	0–1.5 (meters/second)

The scenario was simulated for different numbers of tags and it was repeated ten (10) times. The total delay slots for each simulation was calculated as the arithmetic mean representing the sum of all collisions and idle slots from all readers during the entire simulation. The simulations were performed on a server equipped with an Intel Core i7-2700K 3.5GHz, 16GB of RAM and 1TB of disk space running the Debian GNU/Linux version 6.0 operating system.

The experiments were realized using the ns-2 simulator because it is widely used by the communication networks research community [18]. Besides this fact, the ns-2 was chosen because we can use several features such as mobility. We have extended ns-2 version 2.35 in order to add support to the RFID system and the IoT, including passive tags, readers, and the EPCGlobal [17] protocol. We developed a module to extend ns-2 with these new features[2].

V. SIMULATION RESULTS AND PERFORMANCE EVALUATION

We present in this section the results we obtained with the simulations. The benefits of our mechanism in IoT tracking scenarios compared to the global standard of RFID passive tags [17] are explained. We consider the number of identification delay slots as a performance metric [6][3] for evaluating our proposal. By this way we measure the average number of collision and idle slots needed to identify the whole set of RFID tags in the reader's coverage range during the total time of the simulation. Thus, we express the identification slots in absolute numbers because the energy consumption is directed related to the delay slots existing among the reader and the tags communication[14] and we are interested in evaluating the possible gain in terms of energy consumption when our mechanism is employed.

Fig. 2 shows the number of delay slots in tracking scenarios, based on [15], when the number of tags varies from 100 to 900 and Fig. 3 shows the difference in percentage between the MQAIT protocol and the C1G2 protocol. The improvement in the number of delay slots is due to the fact that we are avoiding unnecessary replies from already identified tags. The graph in Fig. 2 clearly reveals the slot waste of the C1G2 protocol when applied to an IoT tracking scenario. For example, when there are 500 tags, we got a reduction from 3800 to 2500 in the average number of delay slots. Considering the confidence interval, the decrease is 24%–43%, according to Fig. 3. Even if the MQAIT protocol is outperformed with a few number of tags, for instance 100, its overall performance is clearly higher (12%–38%) as we can also see in Fig. 3.

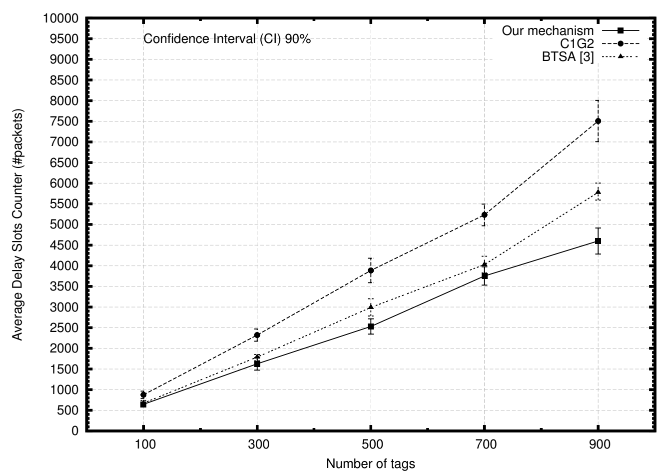

Fig. 2. Total delay comparison (MQAIT, C1G2 and BTSA)

The approaches described in [19], [20] and [21] also improves Q Algorithm. When these algorithms are applied to the previous illustrated IoT scenario the maximum average gain over Q Algorithm is around 6%, 21% and 9% respectively. The reason previous approaches do not offer significant gains compared to the MQAIT algorithm is due to they were designed to operate in simple RFID systems, where there aren't

[2]It is publicly available at http://www.ime.usp.br/~perazzo/rfid_module.php

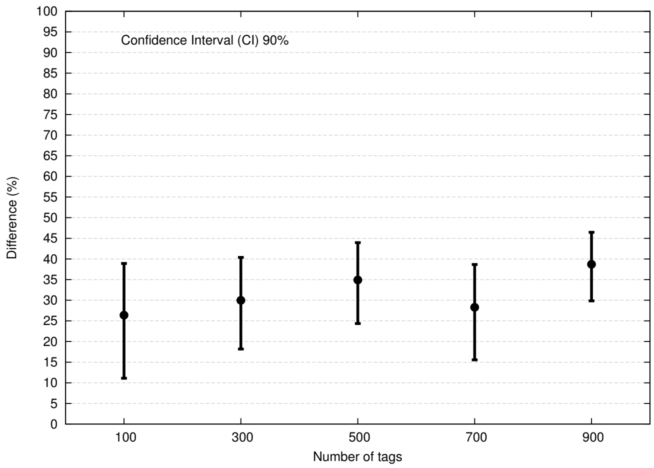

Fig. 3. Total number of packets reduction in percentage (MQAIT vs C1G2)

continuous readings of tags, without the possibility of mobility or IoT scenarios.

We also compared the MQAIT with one of the more efficient anti-collision protocols in the literature, to the best of our knowledge, the BTSA, proposed by [3]. Fig. 2 shows that the gain was up to 17% (for 900 tags) when comparing MQAIT to BTSA. Table II summarizes the difference between the curves of MQAIT and BTSA in Fig. 2. It shows the maximum possible percentage reductions considering the confidence interval. Table II confirms the benefits of MQAIT even in relation to BTSA. Besides, while BTSA requires many changes to the standard protocol, the MQAIT can be implemented with only minor changes to the operation of tags because it maintains full compatibility with the operation of the reader.

TABLE II. TOTAL PERCENTAGE NUMBER OF PACKETS REDUCTION IN PERCENTAGE (MQAIT VS BTSA) WHEN COMPARED TO C1G2 - CONFIDENCE INTERVAL: 90%

Number of tags	Max Average Gain (BTSA)	Max Average Gain (MQAIT)	Difference
100	$\cong 37\%$	$\cong 39\%$	$\cong 2\%$
300	$\cong 31\%$	$\cong 41\%$	$\cong 10\%$
500	$\cong 33\%$	$\cong 44\%$	$\cong 11\%$
700	$\cong 30\%$	$\cong 39\%$	$\cong 9\%$
900	$\cong 30\%$	$\cong 47\%$	$\cong 17\%$

VI. FUTURE WORK

Our future work will analyze the energy consumption reduction and security/privacy concerns from our QoS mechanism. We notice that reducing the number of delay slots has implications for the energy consumed by the reader, and we intend to show this by means of an analytical study.

VII. CONCLUSION

We have proposed a novel RFID mechanism to improve the compliance with QoS requirements of an RFID system for IoT tracking scenarios. The proposed mechanism reduces the number of exchanged messages of an RFID system by using the characteristics of any anti-collision protocol. We have provided a delay analysis of the proposed algorithm by comparing it with the original Q algorithm and with BTSA. The performance analysis and simulation results using an ns-2 RFID module show that the proposed anti-collision algorithm can decrease the total delay slots when compared with the BTSA. Thus, the reliability of an IoT scenario using RFID technology system is improved.

REFERENCES

[1] L. Coetzee and J. Eksteen, "The internet of things - promise for the future? an introduction," in *IST-Africa Conference Proceedings, 2011*, 5 2011, pp. 1 –9.

[2] Q. Sheng, X. Li, and S. Zeadally, "Enabling next-generation rfid applications: Solutions and challenges," *Computer*, vol. 41, no. 9, pp. 21–28, 2008.

[3] H. Wu, Y. Zeng, J. Feng, and Y. Gu, "Binary tree slotted aloha for passive rfid tag anticollision," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 19 –31, 1 2013.

[4] L. Chunli and L. Donghui, "Application and development of rfid technique," in *2nd CECNet*, 4 2012, pp. 900 –903.

[5] X. Jia, Q. Feng, T. Fan, and Q. Lei, "Rfid technology and its applications in internet of things (iot)," in *Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on*, 2012, pp. 1282–1285.

[6] D. Leonardo and M. Victor, "Adding randomness to the epc class1 gen2 standard for rfid networks," in *23rd PIMRC*, 9 2012, pp. 609 –614.

[7] E. Felemban, "A revisit on modeling framed slotted aloha anti-collision protocol for rfid systems," in *RFID-TA*, 11 2012, pp. 315 –318.

[8] X. Jia, Q. Feng, and L. Yu, "Stability analysis of an efficient anti-collision protocol for rfid tag identification," *Communications, IEEE Transactions on*, vol. 60, no. 8, pp. 2285 –2294, 8 2012.

[9] L. Guilan and Z. Guochao, "A improved anti-collision algorithm in rfid system of internet of things," in *ICMT*, 10 2010, pp. 1 –4.

[10] W. Zhong, J. Chen, L. Wu, and M. Pan, "The application of aloha algorithm to anticollision of rfid tags," in *MIC*, vol. 2, 5 2012, pp. 717 –720.

[11] Jian Su and Guang-Jun Wen, "A capture-aware anti-collision algorithm for iso 18000-6c rfid protocol," in *ICWAMTIP*, 12 2012, pp. 291 –294.

[12] H. Han, J. Park, and T.-J. Lee, "Rfid anti-collision protocol for monitoring system of tags in motion," in *4th ICUFN*, 7 2012, pp. 318 –321.

[13] V. Namboodiri, M. DeSilva, K. Deegala, and S. Ramamoorthy, "An extensive study of slotted aloha-based rfid anti-collision protocols," *Computer Communications*, vol. 35, no. 16, pp. 1955 – 1966, 2012.

[14] D. Klair, K.-W. Chin, and R. Raad, "On the energy consumption of pure and slotted aloha based rfid anti-collision protocols," *Computer Communications*, vol. 32, no. 5, pp. 961 – 973, 2009.

[15] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, and G. Borriello, "Building the internet of things using rfid: the rfid ecosystem experience," *IEEE Internet Computing*, vol. 13, no. 3, pp. 48–55, 2009.

[16] J. H. Choi, D. Lee, H. Jeon, J. Cha, and H. Lee, "Enhanced binary search with time-divided responses for efficient rfid tag anti-collision," in *IEEE ICC*, 6 2007, pp. 3853 –3858.

[17] E. IncTM, "Epctm radio-frequency identity protocols class-1 generation-2 uhf rfid protocol for communications at 860mhz-960mhz version 1.2.0," 2008.

[18] C. Petrioli, R. Petroccia, J. Shusta, and L. Freitag, "From underwater simulation to at-sea testing using the ns-2 network simulator," in *IEEE OCEANS*, 6 2011, pp. 1 –9.

[19] F. Schoute, "Dynamic frame length aloha," *Communications, IEEE Transactions on*, vol. 31, no. 4, pp. 565–568, 1983.

[20] Y. Cui and Y. Zhao, "A modified q-parameter anti-collision scheme for rfid systems," in *Ultra Modern Telecommunications Workshops, 2009. ICUMT '09. International Conference on*, 2009, pp. 1–4.

[21] J.-B. Eom and T.-J. Lee, "Accurate tag estimation for dynamic framed-slotted aloha in rfid systems," *Communications Letters, IEEE*, vol. 14, no. 1, pp. 60–62, 2010.