International Journal of Wireless Networks and Broadband Technologies
Volume 7 • Issue 1 • January-June 2018

An RFID Best Effort Mechanism for in Motion Tracking Applications

Rafael Perazzo Barbosa Mota, University of Sao Paulo, Sao Paulo, Brazil
Daniel Macedo Batista, University of Sao Paulo, Sao Paulo, Brazil

ABSTRACT

In this article, the authors propose an algorithm that reduces useless responses for RFID systems in a motion environment, for tracking applications. The mechanism achieves its goals by reducing the number of packets exchanged between readers and tags. They analyze the behavior of their proposal by considering the average number of identification rounds. With extensive simulations using an RFID module for the ns-2 simulator, the authors show the benefit of the proposed mechanism. When compared to the Pure Q Algorithm and Binary Tree Slotted Aloha, their mechanism reduces the number of packets up to 43%, which is a good result in terms of performance of motion applications and energy consumption of the devices used in the communications.

KEYWORDS

Binary Tree Slotted Aloha, ns-2 Simulator, Pure Q Algorithm, RFID Systems

1. INTRODUCTION

The "Internet of Things" (IoT) consists in a vision where objects become part of the Internet: every physical object has its unique identification, and is accessible from the network, providing an expanded Future Internet (Coetzee & Eksteen, 2011). 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. Thus, it is needed that readers periodically send requests to store the data about people and objects.

RFID (Sheng, Li, & Zeadally, 2008) is a key technology of the IoT, since small passive RFID tags allow to link millions and billions of physical products with the virtual world (Wu, Zeng, Feng, & Gu, 2013). When a large number of tags are used, there is a high probability that there will be more than one tag within a 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 (Wu et al., 2013; Chunli & Donghui, 2012; Jia, Feng, Fan, & Lei, 2012).

Many efforts have been made in the literature to improve the performance of anti-collision protocols (Wu et al., 2013; Leonardo & Victor, 2012; Felemban, 2012; Jia, Feng, & Yu, 2012; Guilan & Guochao, 2010; Zhong, Chen, Wu, & Pan, 2012; Jian Su and Guang-Jun Wen, 2012; Chunli & Donghui, 2012; Han, Park, & Lee, 2012). However, little research has been conducted for IoT scenarios (Guilan & Guochao, 2010). According to (Namboodiri, DeSilva, Deegala, & Ramamoorthy, 2012)

DOI: 10.4018/IJWNBT.2018010104

there are several disadvantages of using the Q algorithm, the standard Algorithm for Class 1 Generation 2 RFID systems, because too many packets need to be transmitted, in a single identification process, between the reader and tags. This process generates considerable overhead and increases the power consumption, since the energy consumption is proportional to the number of actions of the readers (Klair, Chin, & Raad, 2009). 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 re-quirements for IoT tracking scenarios, whose nodes are RFID tags. The mechanism reduces the number of delay slots (idle and collision), and consequently the amount of messages exchanged in the network, when compared to the Pure Q Algorithm and to the Binary Tree Slotted Aloha - BTSA algorithm. The proposed mechanism is based on the principle that the tags do not need to reply to all reader queries if they don't change their locations.

The proposed mechanism had its performance evaluated through simulated experiments in the simulator ns-2, 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% when compared to the classical mechanisms.

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 and an increase to the chances to meet QoS requirements.

Besides the mechanism that reduces the number of delay slots, this paper is different from those found in the literature and advances the state of the art because it performs experiments simulating real IoT scenarios (Welbourne et al., 2009) 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.

The rest of this paper is organized as follows: Section 2 provides the background on anti-collision protocols and their development over the years in the literature. In Section 3, we present the proposed mechanism and how our contribution differs from that of prior work. In Section 4 we describe the scenarios simulated to evaluate the performance of the proposed mechanism. In Section 5 we analyze the results of the experiments with the mechanism by comparing it with the Pure Q Algorithm and BTSA algorithm. Conclusions and suggestions of future work are presented in Section 6.

2. BACKGROUND AND RELATED WORK

(Ming & Yan, 2012) summarized the QoS metrics (Response time, Reliability, Availability) of the IoT which still needed research. They also proposed a dynamic management strategy of QoS for the IoT. They concluded that research is needed to improve the analysis and calculation of IoT QoS in a variety of scenarios. The mechanism proposed by us in this paper can improve the response time and the reliability of the IoT by reducing the overhead during the identification of objects. The availability is also improved since the energy consumption is directly related with the number of collisions and our mechanism reduces this number (Klair et al., 2009).

(Nef, Perlepes, Karagiorgou, Stamoulis, & Kikiras, 2012) has shown that it is necessary to define service models that can categorize IoT applications and determine the Quality of Service (QoS) factors necessary to satisfy the requirements of those models. In (Duan, Chen, & Xing, 2011), QoS is one of the key factors for advancing the state of art of the IoT. They analyzed the QoS requirements (Jin, Gubbi, Luo, & Palaniswami, 2012) in every layer of the IoT and proposed a QoS architecture for the IoT which focuses on a control mechanism for transferring and translation of QoS requirements from top to down. We agree with the importance of advancing studies on QoS in the IoT since our mechanism increases the chances that QoS requirements are met in an IoT environment based on an RFID system.

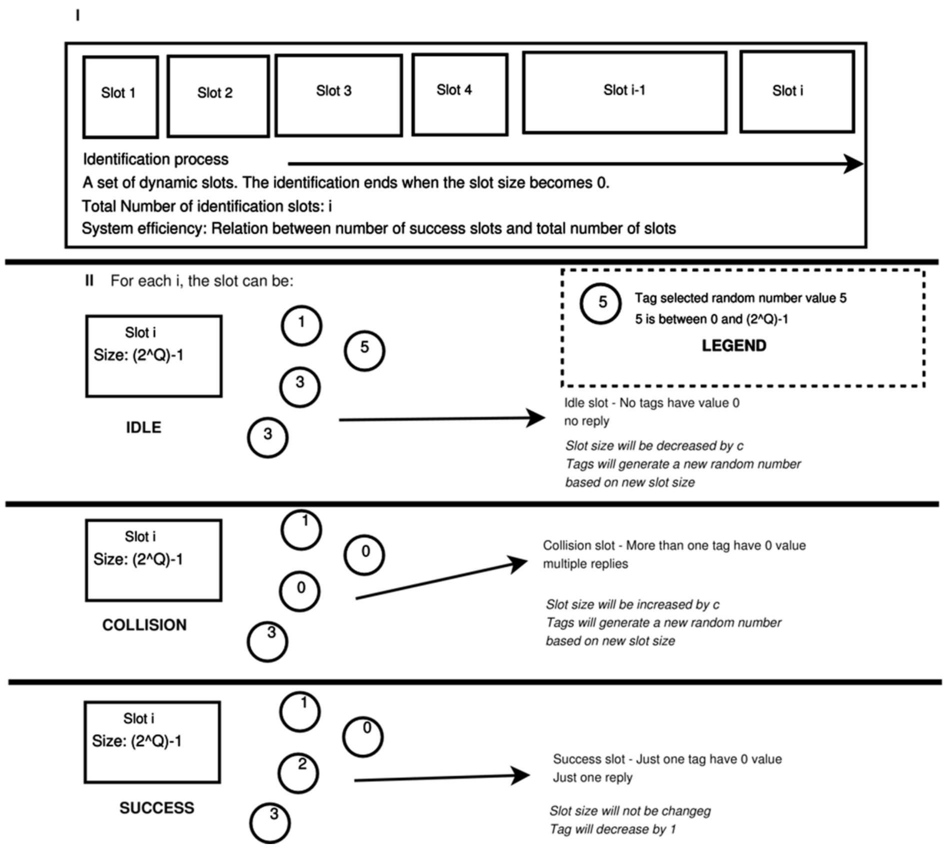
Anti-collision protocols play a critical role for RFID technology to realize multiple-object identification. These protocols are classified into two categories: deterministic and probabilistic (Choi, Lee, Jeon, Cha, & Lee, 2007). Protocols of the first category split colliding tags into two subgroups (trees) until all tags are identified (usually, the names of these protocols have the terms “Binary Tree”). If a collision occurs in a timeslot, the colliding tags are randomly separated into two subgroups by independently selecting 0 or 1, until all tags are identified. The tags that select 0 send their IDs to a reader right away. If a new collision occurs, the collided tags are split again by selecting 0 or 1. The tags that select 1 wait until all the tags that selected 0 are successfully identified by the reader. Otherwise if all the tags that selected 0 are identified, the tags that selected 1 send their IDs to the reader. This procedure is repeated until there are no more collisions. Protocols of the second category 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 (Choi et al., 2007). As these protocols depend on the generation of random numbers, they are classified as probabilistic. The most used Aloha-based protocols in RFID systems have the terms “Dynamic Framed Slotted Aloha” - DFSA in their names. The method employed in these protocols starts by requesting the tags to select a random number between 0 and the initial frame size (timeslot). Then the reader calls each timeslot, one by one. If any collision occurs, the reader calculates a new frame size and the procedure is repeated until no collision occurs in a frame. The DFSA algorithms are different in the way they calculate the next frame size.

A main goal of 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” (Choi et al., 2007). Aspects such as compatibility of implementation and similarity with existing standards should be taken into consideration (our mechanism follows the EPCGlobal standard (EPCglobal, 2008).

The EPCGlobal standard (EPCglobal, 2008) defines tag inventory as a process of tag identification consisting of a number of inventory rounds (total number of slots) (Wang, Daneshmand, Sohraby, & Li, 2009) as illustrated in Figure 1. To perform this task, the Q algorithm was pro-posed (In the rest of this paper, the terms “Q algorithm”, “Pure Q algorithm” and “C1G2” will be used interchangeably). The main idea of the Q algorithm is to assign a random number dynamically by exchanging Q values between the reader and the tags, according to Figure 2. As illustrate in Figure 1 and Figure 2, tags that participate in the identification process select a random value between 0 and $2^Q - 1$, store this value in the slot counter memory, and reply if the slot value is equal to zero. In case of colliding replies (more than one reply will be called a collision slot), the value of Q_{fp} is incremented by a constant C. If no tag replies (idle slot) then Q_{fp} is decremented by the same value of C (Namboodiri et al., 2012). In both cases the reader broadcasts a QueryAdjust command with the new Q value ($Q = ROUND(Q_{fp})$) to the tags, which re-select another random number based on the new Q value. Therefore, if only one reply (successful slot) from tags is received, the reader issues a QueryRep command to the tag, and all other tags update their slots by decreasing one unit. After a tag is identified in a particular inventory round, it will stop to respond to query commands in the same session. The process continues while $Q \geq 0$. The advantage of the Q algorithm is that the frame will converge to a reasonable size without using any estimation technique (Wu et al., 2013). Consequently, the distance value between the frame length and the number of tags in the Q algorithm is more than that in protocols with estimation. The proposed mechanism does not increase or decrease this distance. It only defines whether a tag needs to reply to a reader query. By doing that the system can get fewer replies, which is important in IoT scenarios with millions of devices.

(Choi et al., 2007) 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-

Figure 1. Explanation of the Q Algorithm

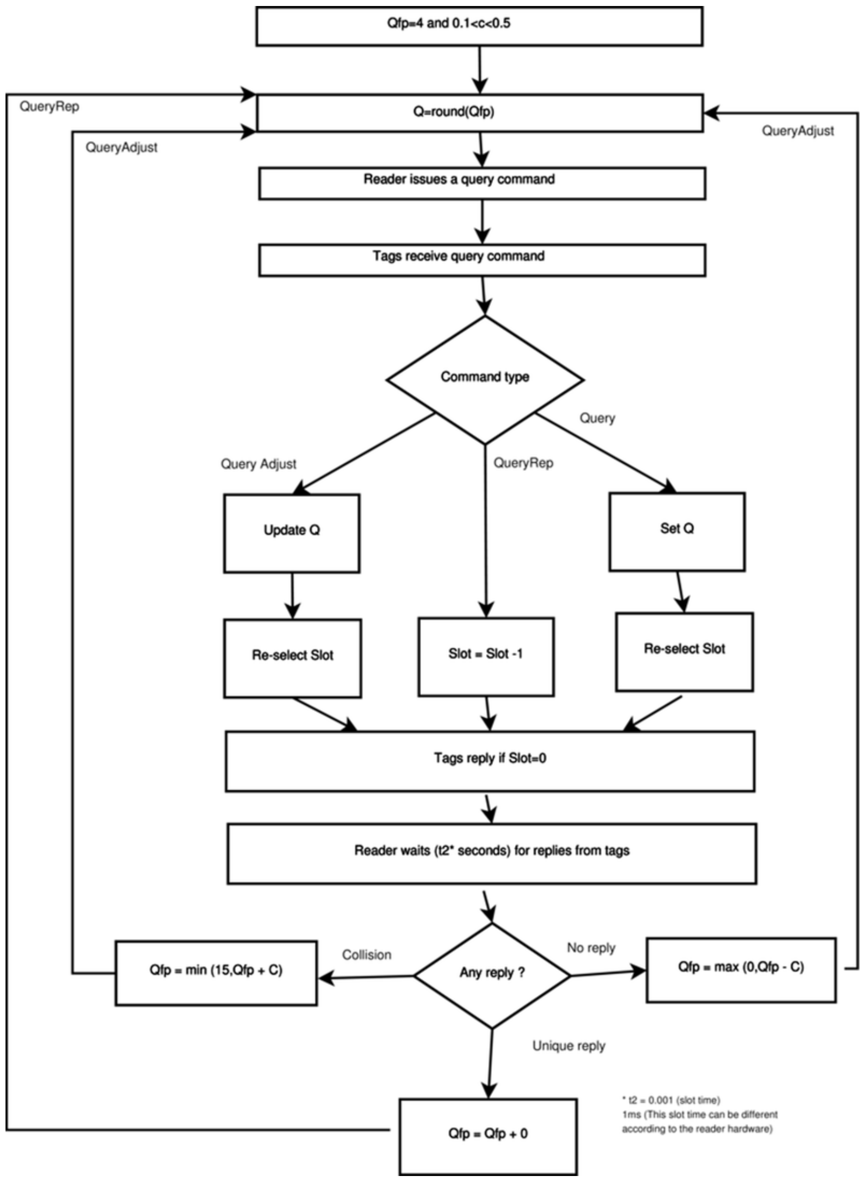


slotted tree-based RFID tag anti-collision protocols require less time for tag identification than the existing tag anti-collision protocols. (Zhong et al., 2012) proved that adopting DFSA algorithms, and adjusting the length of the frame and the number of groupings, improves system performance over traditional Aloha. (Jian Su and Guang-Jun Wen, 2012) 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.

(Wu et al., 2013) has designed the most recent Aloha-based 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 high identification speed; however, it is not optimized for practical settings, will not be as simple to implement as Frame Slotted Aloha - FSA or C1G2 with no known experimental prototype (Namboodiri et al., 2012) and it does not consider the mobility aspect and periodic queries, characteristics 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 with any existing anti-collision protocols, since it does not change the way the reader identifies each tag.

Figure 2. Q Algorithm flowchart - Reader operation



3. 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 if they don't change their locations. It can be used with any anti-collision algorithm summarized in Section 2. If an identified tagged object has not left the current reader range, it does not need to send a reply, since in this case the application middleware has already stored the object location. 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 themselves mute because the middleware already knows their locations.

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 (EPCglobal, 2008).

The efficiency of the MQAIT will be compared to the efficiency of the traditional Q algorithm, Pure Aloha and BTSA in Section 5.

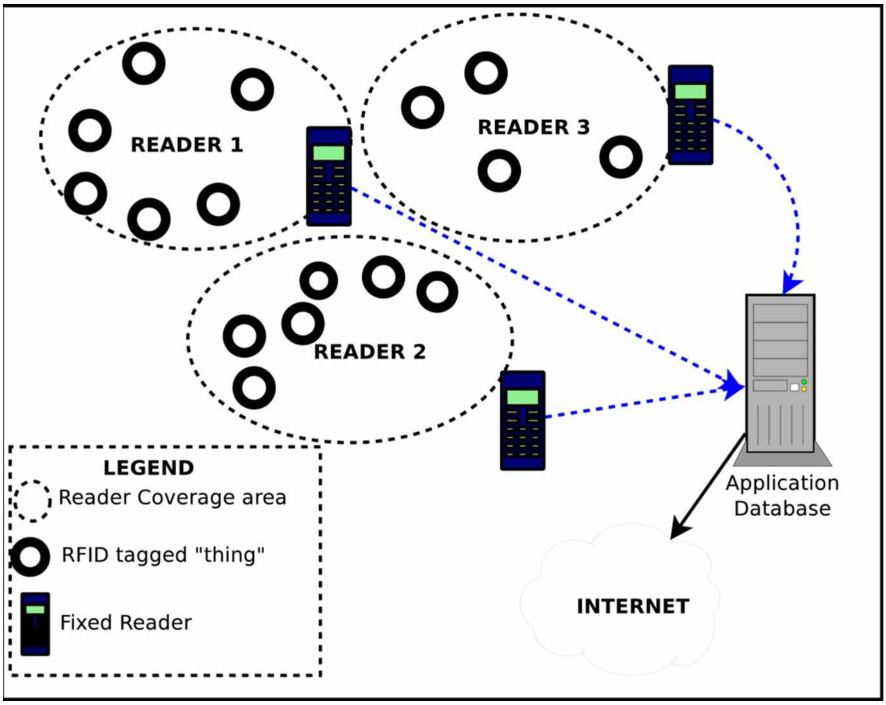
4. SCENARIOS AND EXPERIMENTS

As the first scenario, we consider a generic RFID tracking/localization system, as illustrated in Figure 3. 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. This scenario is based on experiments reported in (Welbourne et al., 2009) and models several current situations as identification of school uniforms, inventory control, tracking of attendees in scientific conferences,

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
```

Figure 3. Simulated tracking/localization scenario (First scenario)



etc. (Jia, Feng, Fan, & Lei, 2012). It is important to observe that the increase in the number of readers and the speed of moving objects do not modify the operation of the MQAIT.

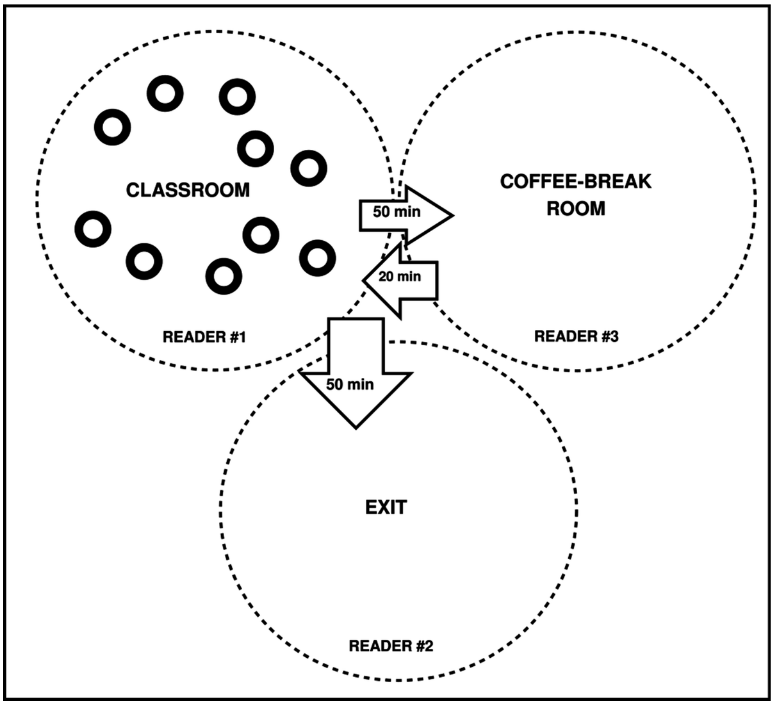
Table 1 lists the parameters of the first scenario of experiments. The scenario was simulated for different numbers of tags and it was repeated ten (10) times. The total delay slots for each simulation was calculated as the sum of all collisions and idle slots from all readers during the entire simulation.

The second scenario is less dynamic than the first one. It models students being monitored by RFID readers in three different locations. Figure 4 illustrates the scenario. The students are monitored by READER #1 in the classroom while they stay there. If any student goes out, the READER #2 or READER #3 get this information. The RFID application middleware computes if each student had

Table 1. Parameters of the first scenario

Simulated time	1800 seconds
Number of tags	100 to 900
Number of readers	3
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)

Figure 4. Simulated classroom scenario (Second scenario)



stayed enough time inside the classroom. The parameters of this second scenario of experiments are shown in Table 2.

Both scenarios were simulated using the ns-2 simulator, because it is widely used and accepted by the communication networks research community (Petrioli, Petroccia, Shusta, & Freitag, 2011). Moreover, the ns-2 was chosen because it is possible to use several features already implemented, such as mobility. To get support to the RFID system and the IoT on ns-2, including passive tags, readers, and the EPCGlobal (EPCglobal, 2008) protocol, the nsRFIDsim (Mota & Batista, 2013a) (Rafael Perazzo Barbosa Mota, 2013) module was used with the ns-2 version 2.35. All 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.

Table 2. Parameters of the second scenario

Simulated time	7200 seconds
Number of tags	50 to 1050
Number of readers	3
Initial positions	Random inside the classroom
Movements	Random inside each location
Readers queries	Each reader issues a query command every minute
Topology	30x15 (meters)
Nodes speed	0–1.5 (meters/second)

5. SIMULATION RESULTS AND PERFORMANCE EVALUATION

We present in this section the results we obtained with the simulations. All the code and data used in the experiments are publicly available at http://www.ime.usp.br/~perazzo/data. Thus, other researchers are able to reproduce the experiments and to use or modify the code in their works.

The benefits of our mechanism in IoT tracking scenarios, when compared to the global standard of RFID passive tags (EPCglobal, 2008), are evaluated. We consider the number of identification delay slots (Leonardo & Victor, 2012; Wu et al., 2013) and the number of lost packets (Mota & Batista, 2013b) as performance metrics 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 each simulation. Also, we evaluate the number of transferred bytes and packets because the energy consumption is directed related to both the delay slots and the number of transferred bytes among the reader and the tags (Klair et al., 2009) and we are interested in evaluating the possible gain in terms of energy consumption when our mechanism is employed.

Figure 5 shows a graph plotting the average delay slots in the first scenario, when the number of tags varies from 100 to 900 and Figure 6 shows a graph plotting the difference range 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 Figure 5 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 around 24%–43%, according to Figure 6. 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 Figure 6.

Figure 7 illustrates the gains when MQAIT is applied in the classroom scenario (Second scenario). In this specific case we have used the Pure Aloha method and the MQAIT applied to Pure Aloha,

Figure 5. Comparison of total number of delay slots (MQAIT vs C1G2) – First scenario

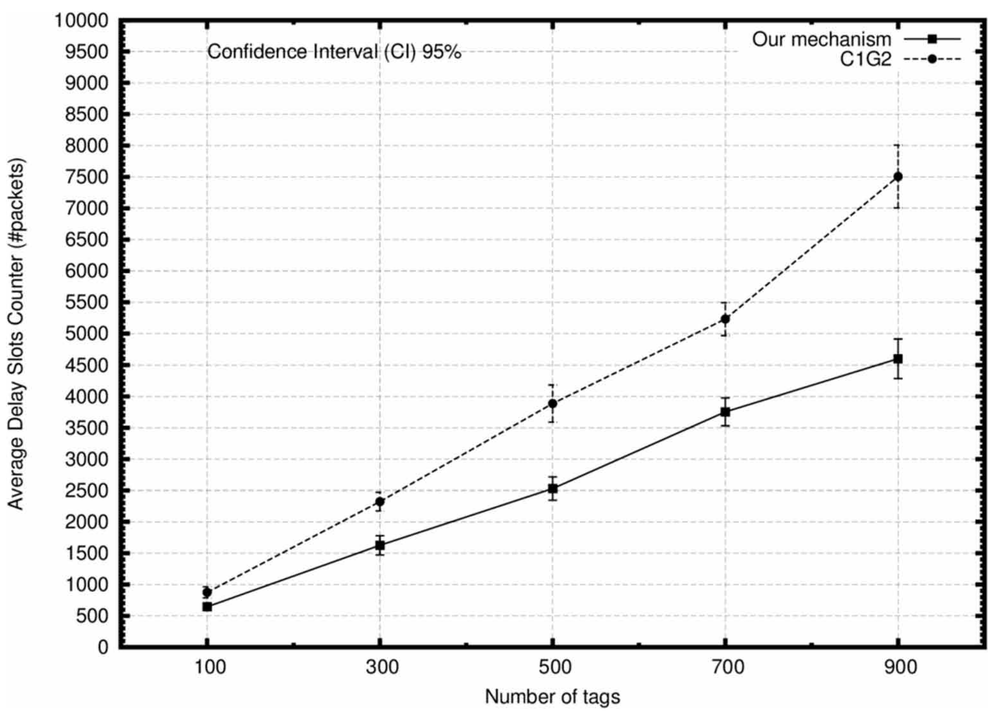


Figure 6. Reduction in percentage of total number of delay slots (MQAIT vs C1G2) – First scenario

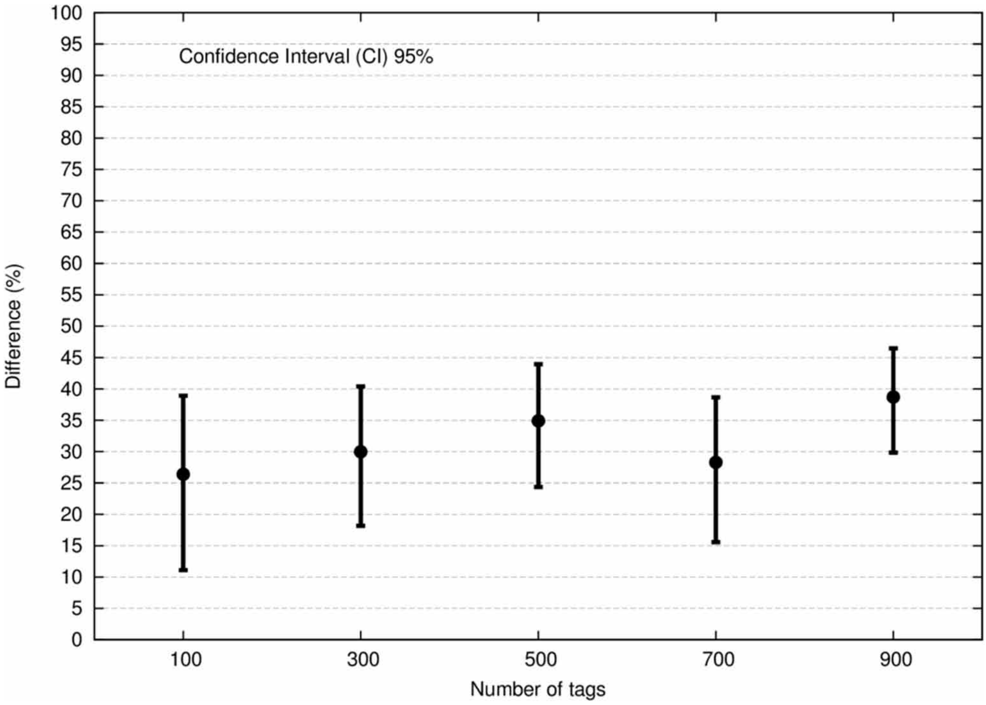
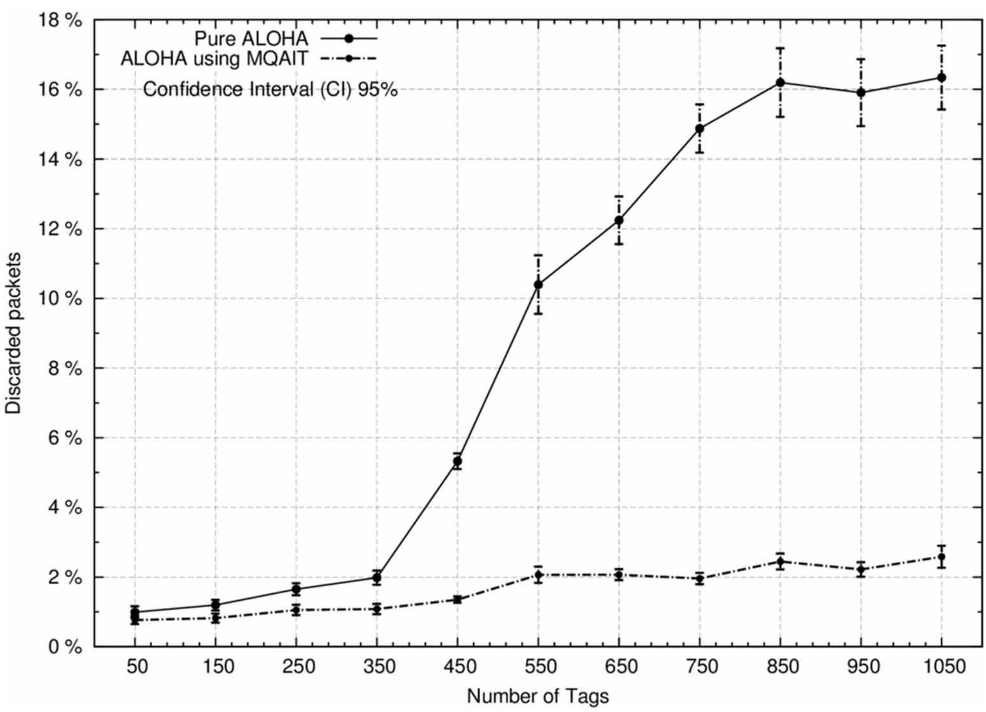


Figure 7. Percentage of discarded packets (Pure Aloha Vs Aloha with MQAIT) – Second scenario



so we have the concept of discarded packet. The percentage of discarded packets was defined as the relation between the number of discarded packets and the total number of transmitted packets. We made the average of this metric and plotted in the graph. As the scenario is not very dynamic, the percentage of delay slots can be reduced from 18 to approximately 2%, when the number of tags is 1050. Besides, the percentage when the MQAIT is applied, tends to remain constant, regardless of the number of tags, which also represents a gain in overall performance.

To measure the gains in the number of bytes that are exchanged in the communication, Figure 8 shows the number of bytes transferred during the communication process. The performance gains can reach approximately 38% when the number of tags is higher than 350. Besides, the use of MQAIT mechanism also makes traffic curve almost linear, which also helps to reduce energy consumption by readers, when compared to Pure Aloha.

We also compared the MQAIT with one of the more efficient Aloha-based anti-collision protocols in the literature, to the best of our knowledge, the BTSA, proposed by (Wu et al., 2013). Table 3 compares MQAIT and BTSA in terms of reduction of number of packets in relation to the C1G2 mechanism in the first scenario. It shows the maximum possible percentage reductions considering the confidence interval. The table confirms the benefits of MQAIT even in relation to BTSA. For example, with 900 tags the gain of MQAIT in relation to BTSA was up to 17%. 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.

6. CONCLUSION AND FUTURE WORK

In this paper 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

Figure 8. Kbytes transferred (Pure Aloha Vs Aloha with MQAIT) – Second scenario

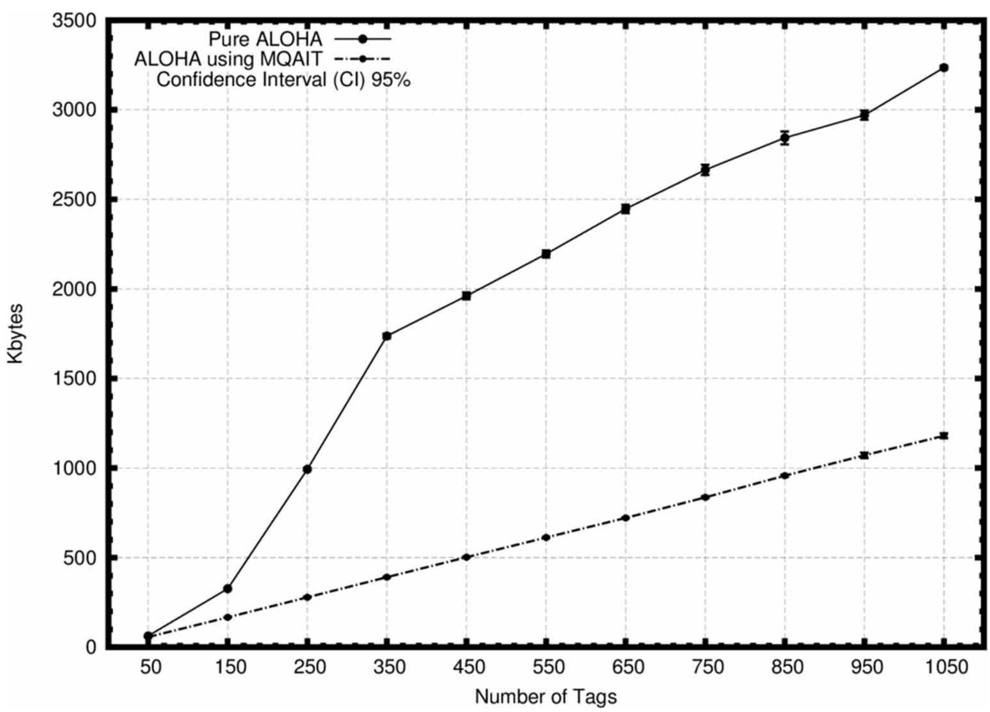


Table 3. Reduction of number of packets in percentage (MQAIT vs BTSA) when compared to C1G2 – First scenario – Confidence Interval: 90%

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

number of exchanged messages of an RFID system when the tags don't change their location. Besides, it follows the EPCGlobal standard and can be applied with any existing anti-collision protocols. We have provided a performance evaluation of the proposed algorithm by comparing it with the original Q algorithm, BTSA and Pure Aloha. The simulation results using nsRFIDsim module show that the proposed anti-collision algorithm can decrease the number of delay slots, the number of lost packets and the amount of transferred bytes, when compared with the BTSA and Pure Aloha. Thus, the reliability and the availability of an IoT scenario using RFID tags are improved.

As future work we will analyze the energy consumption reduction in absolute numbers. 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. We also intend to analyze the security and privacy concerns related to our mechanism.

REFERENCES

Choi, J. H., Lee, D., Jeon, H., Cha, J., & Lee, H. (2007). Enhanced Binary Search with Time-Divided Responses for Efficient RFID Tag Anti-Collision. In IEEE International Conference on Communications ICC'07 (pp. 3853-3858). IEEE. doi:10.1109/ICC.2007.635

Chunli, L., & Donghui, L. (2012). Application and development of RFID technique. In *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)* (pp. 900-903). IEEE. doi:10.1109/CECNet.2012.6201574

Coetzee, L., & Eksteen, J. (2011). The Internet of Things - Promise for the Future? An Introduction. In *2011 IST-Africa Conference Proceedings* (pp. 1-9). IEEE.

Duan, R., Chen, X., & Xing, T. (2011). A QoS Architecture for IOT. In *2011 International Conference on Internet of Things (iThings/CPSCom) and 4th International Conference on Cyber, Physical and Social Computing* (pp. 717-720). IEEE. doi:10.1109/iThings/CPSCom.2011.125

EPCglobal. (2008). EPCTM Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz-960MHz Version 1.2.0. EPCGlobal Inc.

Felemban, E. (2012). A Revisit on Modeling Framed Slotted Aloha Anti-Collision Protocol for RFID Systems. In *2012 IEEE International Conference on RFID-Technologies and Applications (RFID-TA)* (p. 315 -318). IEEE. doi:10.1109/RFID-TA.2012.6404537

Guilan, L., & Guochao, Z. (2010). A Improved Anti-Collision Algorithm in RFID System of Internet of Things. In 2010 International Conference on Multimedia Technology (ICMT) (p. 1 -4). IEEE. doi:10.1109/ICMULT.2010.5629628

Han, H., Park, J., & Lee, T.-J. (2012). RFID Anti-Collision Protocol for Monitoring System of Tags in Motion. In *2012 Fourth International Conference on Ubiquitous and Future Networks (ICUFN)* (p. 318 -321). IEEE. doi:10.1109/ICUFN.2012.6261720

Jia, X., Feng, Q., Fan, T., & Lei, Q. (2012). RFID Technology and its Applications in Internet of Things (IoT). In 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet) (p. 1282-1285). IEEE. doi:10.1109/CECNet.2012.6201508

Jia, X., Feng, Q., & Yu, L. (2012). Stability analysis of an efficient anti-collision protocol for RFID tag identification. *IEEE Transactions on Communications*, *60*(8), 2285–2294. doi:10.1109/TCOMM.2012.051512.110448

Jin, J., Gubbi, J., Luo, T., & Palaniswami, M. (2012). Network Architecture and QoS Issues in the Internet of Things for a Smart City. In 2012 International Symposium on Communications and Information Technologies (ISCIT) (p. 956-961). IEEE. doi:10.1109/ISCIT.2012.6381043

Klair, D., Chin, K.-W., & Raad, R. (2009). On the Energy Consumption of Pure and Slotted Aloha based RFID Anti-Collision Protocols. *Computer Communications*, *32*(5), 961–973. doi:10.1016/j.comcom.2008.12.019

Leonardo, D., & Victor, M. (2012). Adding Randomness to the EPC Class1 Gen2 Standard for RFID Networks. In *2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)* (p. 609 -614). IEEE. doi:10.1109/PIMRC.2012.6362856

Ming, Z., & Yan, M. (2012). A Modeling and Computational Method for QoS in IoT. In *2012 IEEE 3rd International Conference on Software Engineering and Service Science (ICSESS)* (p. 275-279). IEEE. doi:10.1109/ICSESS.2012.6269459

Mota, R. P. B. (2013). RFID module for ns-2 simulator. *Centro de Competência em Software Livre*. Retrieved from http://ccsl.ime.usp.br/en/rfid-module-ns-2-simulator

Mota, R. P. B., & Batista, D. (2013a). An NS-2 Module for Simulating Passive RFID Systems. In 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC EUC) (pp. 2263-2270). IEEE.

Mota, R. P. B., & Batista, D. (2013b). Um Mecanismo para Garantia de QoS na "Internet das Coisas" com RFID. In *Proceedings of the SBRC 2013 (Brazilian Symposium on Computer Networks and Distributed Systems)* (pp. 297–310).

Namboodiri, V., DeSilva, M., Deegala, K., & Ramamoorthy, S. (2012). An Extensive Study of Slotted Aloha-Based RFID Anti-Collision Protocols. *Computer Communications*, *35*(16), 1955–1966. doi:10.1016/j.comcom.2012.05.015

Nef, M.-A., Perlepes, L., Karagiorgou, S., Stamoulis, G. I., & Kikiras, P. K. (2012). Enabling QoS in the Internet of Things. In Proc. of the 5th Int. Conf. on Commun., Theory, Reliability, and Quality of Service (CTRQ 2012) (pp. 33–38).

Petrioli, C., Petroccia, R., Shusta, J., & Freitag, L. (2011). *From Underwater Simulation to At-Sea Testing Using the ns-2* network simulator. In OCEANS, 2011 IEEE-Spain (pp. 1-9). IEEE. doi:10.1109/Oceans-Spain.2011.6003638

Sheng, Q., Li, X., & Zeadally, S. (2008). Enabling Next-Generation RFID Applications: Solutions and Challenges. *Computer*, *41*(9), 21–28. doi:10.1109/MC.2008.386

Su, J., & Wen, G.-J. (2012). A Capture-Aware Anti-Collision Algorithm for ISO 18000-6C. In 2012 International Conference on Wavelet Active Media Technology and Information Processing (ICWAMTIP) (pp. 291–294). IEEE. doi:10.1109/ICWAMTIP.2012.6413496

Wang, C., Daneshmand, M., Sohraby, K., & Li, B. (2009). 5). Performance analysis of RFID Generation-2 protocol. *IEEE Transactions on Wireless Communications*, *8*(5), 2592–2601. doi:10.1109/TWC.2009.080437

Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., & Borriello, G. et al. (2009). Building the Internet of Things Using RFID: The RFID Ecosystem Experience. *IEEE Internet Computing*, *13*(3), 48–55. doi:10.1109/MIC.2009.52

Wu, H., Zeng, Y., Feng, J., & Gu, Y. (2013). Binary Tree Slotted ALOHA for Passive RFID Tag Anticollision. *IEEE Transactions on Parallel and Distributed Systems*, *24*(1), 19–31. doi:10.1109/TPDS.2012.120

Zhong, W., Chen, J., Wu, L., & Pan, M. (2012). The Application of ALOHA Algorithm to Anticollision of RFID Tags. In 2012 International Conference on Measurement, Information and Control (MIC) (Vol. 2, p. 717 -720). doi:10.1109/MIC.2012.6273392