A lower bound on the average identification time in a passive RFID system

Nikita Stepanov[1][0000−0001−5524−1168], Nikolay Matveev[1][0000−0002−9746−4746], Olga Galinina[2][0000−0002−5386−1061], and Andrey Turlikov[1][0000−0001−7132−094X]

[1] State University of Aerospace Instrumentation, Saint-Petersburg, Russia,
{nstepanov, n.matveev, turlikov}@vu.spb.ru
[2] Tampere University of Technology, Tampere, Finland
olga.galinina@tut.fi

Abstract. One of the most well-known standards for radio frequency identification (RFID), the standard ISO 18000-6C, collects the requirements for RFID readers and tags and regulates respective communication protocols. In particular, the standard introduces the so-called Q-algorithm resolving conflicts in the channel (which occur when several RFID tags respond simultaneously). As of today, a vast amount of existing literature addresses various modifications of the Q-algorithm; however, none of them is known to significantly reduce the average identification time (i.e., the time to identify all proximate tags). In this work, we derive a lower bound for the average identification time in an RFID system. Furthermore, we demonstrate that in case of an error-free channel, the performance of the legacy Q-algorithm is reasonably close to the proposed lower bound; however, for the error-prone environment, this gap may substantially increase, thereby indicating the need for new identification algorithms.

1 Introduction

One of the most well-known standards for radio frequency identification (RFID), known as EPCglobal Class 1 Generation 2 (ISO 18000-6C) [2, 4], consolidates the requirements for RFID readers and tags as well as regulates respective communication protocols, operating at distances of $0.5 - 10$ meters and frequencies 860-960 MHz.

Inter alia, the standard ISO 18000-6C introduces a specific algorithm that allows an RF reader to poll and identify an unknown number of tags in its coverage area [6, 7]. This algorithm is often referred to as the Q-algorithm, owing to its core parameter typically denoted as Q.

As of today, a vast amount of existing literature addresses various modifications of the Q-algorithm; however, none of them is known to significantly reduce the time required to identify all proximate tags (typically called the identification time). Most of the research attempts in this direction focus on defining parameters of the Q-algorithm, which would minimize the average identification

time, and offer multiple heuristic methods as, e.g., proposed in [9, 1, 8]; however, the algorithm remains unchanged.

Viewed from another angle, the mentioned multiple available variations of the Q-algorithm could already be lying relatively close to a certain bound, thus, limiting the chances for further improvement. In the light of the above, we target our work towards developing a *hypothetical optimal algorithm* that ensures the minimum average time for identifying proximate tags by the reader. Having designed the hypothetical identification algorithm, we derive a recurrent expression for calculating its average identification time, which, in turn, represents *a lower bound* for the identification time within the class of similar algorithms, which also includes the standardized Q-algorithm. To illustrate the behavior of identification algorithms in an imperfect channel, we also extend our calculations by including the *probability of a channel error*.

This paper is organized as follows. In Section II, we introduce the key assumptions of our system model, which is based on the standard ISO 18000-6C, and summarize the collision resolution algorithm (Q-algorithm). Further, in Section III, we introduce a hypothetical algorithm and provide the derivation of our proposed lower bound for the average identification time. Section IV illustrates the behavior of the obtained lower bound in comparison to the performance of the Q-algorithm (separately for the case of error-free and error-prone wireless channels) and demonstrates a substantial gap between the standard solution and our theoretical lower bound in case of channel errors.

2 System model

We focus on a typical passive RFID scenario and study a wireless system that includes a *reader* and a set of RFID *tags* located in its coverage area, which communicate according to ISO/IEC 18000-6C RFID protocol. An example of the corresponding time diagram is illustrated in Fig. 1. Importantly, in our (passive RFID) scenario, the tags do not have an inbuilt source of power, but instead are able to harvest and use the energy received from the reader [3].

Below we introduce the key system assumptions, which on the one hand preserve the core features of algorithms advised by the standard ISO/IEC 18000-6C and, on the other hand, make the model analytically tractable for further evaluation.

2.1 Main system assumptions

The system time is divided into *frames* so that each frame contains a variable number of intervals (termed *slots*), during which the reader may receive and decode the information from one transmitting tag. The number of slots within one frame is determined according to a specified rule and reliably broadcasted at the beginning of each frame by the reader.

After receiving a message from the reader, a tag may respond in one of the available slots of the subsequent frame; the slot is selected randomly according

to the uniform distribution. As more than one device may independently decide to transmit during the same slot, we observe one out of the three following outcomes: no transmission, a conflict (collision) of two or more tags, and the successful transmission. We assume that the reader identifies the channel outcome instantaneously and correctly. Below we provide our assumptions on the above-listed three outcomes.

Assumption 1. If none of the tags responds, then no signal is detected by the reader (in our model, this outcome is further termed 'Empty'). The duration of an 'Empty' slot equals T_e time units.

Assumption 2. If two or more tags are transmitting simultaneously, the reader cannot identify any of them, and therefore, the corresponding slot is recognized by the reader as 'Conflict' and lasts for T_c time units.

Assumption 3. Finally, if exactly one tag transmits during the considered slot, then this tag is successfully identified with the probability $1-p$, and its duration occupies precisely T_s time units (this outcome is termed 'Success'). With the complementary probability p (that is, the *probability of a channel error*), the tag will not be identified, and the slot length changes to T_c (equivalent to 'Conflict').

We assume that the probability p of the channel error is the same for any tag in our system, e.g., due to the fact that all tags are located at equal distances from the reader and in similar electromagnetic conditions.

If the tag is successfully identified at the end of its transmission (i.e., we observe 'Success'), the reader sends a corresponding command, which automatically excludes the successful tag from the further polling procedure. Otherwise, if the signal has been distorted and the transmission attempt fails, the tag continues contending for the channel in the next frame.

We refer to a sequence of frames, during which all proximate tags could be successfully identified, as the *identification time*. Below we aim at constructing an algorithm that defines a *dynamic sequence* of frame lengths and by that minimizes the average identification time.

2.2 Collision resolution algorithm (Q-algorithm)

In this subsection, we extend our assumptions introduced above and further elaborate on the random multiple access algorithm specified by the standard ISO 18000-6C (the Q-algorithm), which drew on a random selection of the frame length.

Typically, the length of the frame is represented by the number 2^Q, where Q is a variable parameter, which is initialized by default as $Q = 4$ and may vary from 0 to 15. We remind that the value of Q is broadcasted by the reader (as the Query command) at the beginning of each frame. All tags that have received the value of Q (that is, according to our assumptions, all proximate tags) generate a random slot number within the interval $[0, 2^Q - 1]$ and save it as a slot counter.

The tags, whose slot counters equal to 0, respond immediately (enter the 'Reply' stage) by sending a unique random sequence of 16 bits (called *RN16*), identifying an RFID tag.

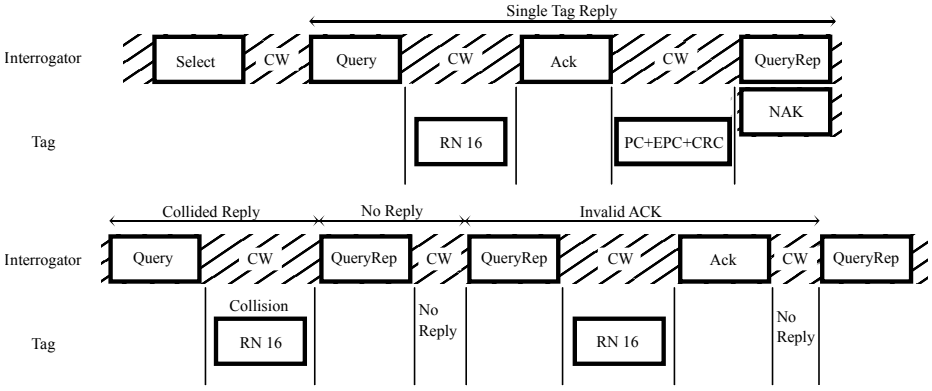

Fig. 1. Illustration of the RF identification process in the standard EPCglobal Class 1 Generation 2 [2]. The error in an RN16 sequence (uniquely identifying the tag) transmission results in the same processing time as the processing time in case of a collision. Contention window is denoted as CW.

Further, if exactly one tag replies, the value of the parameter Q for the next frame remains the same, and the reader transmits the QueryRep command, instructing the tags to decrement their slot counters by 1. When the tag counter reaches 0, it immediately starts transmitting its RN16 sequence to the reader. A block-scheme of the Q-algorithm is illustrated in Fig. 2.

If the tag is successfully identified after transmission of RN16, then the reader confirms by sending the ACK command to the tag and excludes the tag from further identification process. After the last tag is successfully identified, the reader stops the identification procedure.

If no tags or more than two tags access the channel, the reader sends the QueryAdjust command, which may increase/decrease the value of the parameter Q by the step C, where C is implementation-dependent and belongs to the interval $[0.1, 0.5]$. Usually, readers employ lower values of C, when Q is relatively large, and vice versa.

In case of a collision that is when more than two tags reply simultaneously, the reader cannot identify any of them; in this case, the tag counter values of all collided tags increase sharply (in particular, change to 32767, 2^{15}-1, or 7FFFh) to prevent the tags from transmitting in the current frame.

3 Derivation of the lower bound of the average identification time

In this section, we introduce a class of RFID algorithms, which includes, among others, the Q-algorithm discussed above. Within the defined class of algorithms, we consider an optimal scheme, which provably delivers the least values of the average identification time and therefore, provides the lower bound for the entire class and, in particular, for the Q-algorithm.

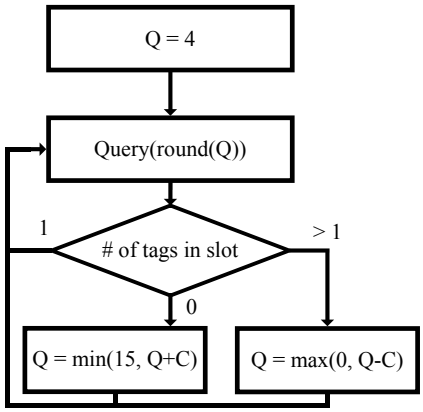

Fig. 2. A block-scheme for the Q-algorithm.

We recall that for any identification procedure, the current frame length is broadcasted by the reader at the beginning of each frame so that every tag immediately selects a slot for the subsequent transmission of its RN16 sequence. Moreover, after any of the slots, the reader may interject the operation, that is, broadcast a new value of the frame length and restart activity of its tags. We further refer to this decision of the reader to change the operation to as an *interrupt*.

Here, we define *an RFID algorithm* as a set of two rules: (i) according to the first one, the reader selects the frame length, and (ii) the second rule drives decisions to interrupt. We further study a class of such algorithms, i.e., including all possible identification schemes that meet these two requirements. We also assume that the number of slots in the frame may be represented by an integer number from 1 to ∞ (it is unconstrained and not necessarily the power of 2 in contrast to the Q-algorithm).

Importantly, the standard Q-algorithm belongs to the defined class of RFID algorithms, and therefore, an algorithm that is optimal within this class will deliver equal or better performance in terms of the average identification time than any variation of the Q-algorithm.

Let us further assume that at any moment of time the exact number of tags is known (which is not possible in practice for the scenario in question) and consider a hypothetical algorithm that makes his decisions based on this knowledge. As any RFID algorithm targets selecting the frame length and making a decision on interruption optimally, we may formulate the following proposition.

Proposition 1. *The average identification time of the hypothetical RFID algorithm, aware of the exact current number of tags, is minimal within the considered class.*

Proof. The proof is trivial and left out of the scope of this paper.

Proposition 2. *If the exact current number of tags is known, an RFID algorithm that creates interruptions after the first slot delivers the average identi-*

fication time not greater than that of an algorithm with any other interruption rule.

Proof. The proof is left out of the scope of this paper.

We consider a particular state of the system with n unidentified tags. Let V_n represent *the optimal frame length* in case of n tags. In general, we may also interpret V_n as a rule, according to which the reader decides on the frame length to broadcast. Knowing this rule, we may calculate the average identification time for our optimal scheme, that as well constitutes *the lower bound* on for the Q-algorithm.

Theorem 1 *Given n currently unidentified tags and the corresponding optimal frame length V_n, the average identification time for the optimal algorithm may be obtained according to the following recurrent expression:*

$$l_n(V_n) = \frac{T_c P_c(V_n, n) + T_e P_e(V_n, n) + ((1-p)\,(l_{n-1}(V_{n-1}) + T_s) + pT_c)\,P_s(V_n, n)}{1 - P_c(V_n, n) - P_e(V_n, n) - pP_s(V_n, n)}, \tag{1}$$

where T_e, T_c, and T_s is the duration of the empty, conflict, and successful slots, correspondingly, while p is the probability of a channel error during the RN16 transmission, and $P_s(V_n, n)$, $P_c(V_n, n)$, $P_e(V_n, n)$ are the probabilities of the outcomes 'Success', 'Conflict', 'Empty' during the first slot of the current frame.

Proof. We consider our system in a state where $n > 0$ tags are to be identified and the optimal frame length is given by V_n. Naturally, we assume that $V_0 = 0$, thus, the average identification time is zero, $l_0(V_0) = 0$.

Let the random variable $[L_n|V_n]$ denote one realization of the identification time. For the sake of brevity, $[L_n|V_n]$ is further referred to as L_n. Then, for the system of n tags with frame interruptions, we may write down the following expression:

$$\begin{aligned} L_n = {} & \text{I\{'Success'\}}\ (T_s + L_{n-1}) + \ \text{I\{'Failure'\}}\ (T_c + L_n) + \\ & \text{I\{'Conflict'\}}\ (T_c + L_n) + \ \text{I\{'Empty'\}}\ (T_e + L_n), \end{aligned} \tag{2}$$

where I{'Success'} is an indicator of that exactly one tag transmits and there are no errors during the subsequent transmission of the RN16 sequence, I{'Failure'} indicates that one tag accesses the channel but the transmission of RN16 fails, I{'Conflict'} and I{'Empty'} reflect a conflict and an empty slot, respectively. We remind that T_s, T_c, and T_e denote the duration of empty, conflict, and successful slots, correspondingly.

In order to obtain the average identification time $l_n = E[L_n]$, we find expected values of the left and right sides of the equation (2):

$$\begin{aligned} E[L_n] = {} & E[\ \text{I\{'Success'\}}\ (T_s + L_{n-1})] + E[\ \text{I\{'Failure'\}}\ (T_c + L_n)] + \\ & E[\text{I\{'Conflict'\}}\ (T_c + L_n)] + E[\ \text{I\{'Empty'\}}\ (T_e + L_n)]. \end{aligned} \tag{3}$$

Taking into account the possibility of interruptions after the first slot of the current frame and the fact that:

$$\begin{array}{c} E[\text{ I\{'Success'\} }] = P_s(V_n,n)(1-p), \quad E[\text{ I\{'Failure'\} }] = P_s(V_n,n)p, \\ E[\text{ I\{'Conflict'\} }] = P_c(V_n,n), \quad E[\text{ I\{'Empty'\} }] = P_e(V_n,n), \end{array} \tag{4}$$

we may arrive at the following expression for the average identification time:

$$\begin{array}{c} l_n(V_n) = P_c(V_n,n)\left(l_n(V_n)+T_c\right) + P_e(V_n,n)\left(l_n(V_n)+T_e\right) + \\ P_s(V_n,n)\left[(1-p)\left(l_{n-1}(V_{n-1})+T_s\right) + p\left(l_n(V_n)+T_c\right)\right], \end{array} \tag{5}$$

where p is the probability of error in case of 'Success' (i.e., the reader identifies the outcome as 'Conflict'). The probabilities $P_s(V_n,n)$, $P_e(V_n,n)$, and $P_c(V_n,n)$ of 'Success', 'Empty', and 'Conflict', correspondingly, may be obtained as:

$$P_s(V_n,n) = n\frac{1}{V_n}\left(1-\frac{1}{V_n}\right)^{n-1}, \tag{6}$$

since 'Success' corresponds to the case when one tag transmits in a particular slot with the probability $\frac{1}{V_n}$, and the remaining $n-1$ tags are silent,

$$P_e(V_n,n) = \left(1-\frac{1}{V_n}\right)^{n}, \tag{7}$$

where all n tags are not transmitting, and, finally,

$$P_c(V_n,n) = 1 - P_s(V_n,n) - P_e(V_n,n). \tag{8}$$

Further, we simplify the expression (5), removing the parentheses and relocating the terms corresponding to $l_n(V_n)$ as follows:

$$\begin{array}{c} l_n(V_n) - l_n(V_n)\cdot P_c(V_n,n) - l_n(V_n)\cdot P_e(V_n,n) - \\ pl_n(V_n)\cdot P_s(V_n,n) = T_c\cdot P_c(V_n,n) + T_e\cdot P_e(V_n,n) + \\ \left((1-p)\left(T_s + l_{n-1}(V_{n-1})\right) + pT_c\right)\cdot P_s(V_n,n). \end{array} \tag{9}$$

Here, we may divide both left and right sides of the equation by $(1-P_c(V_n,n)-P_e(V_n,n)-pP_s(V_n,n))$ and, finally, obtain the following:

$$l_n(V_n) = \frac{T_cP_c(V_n,n) + T_eP_e(V_n,n) + \left[(1-p)\left(l_{n-1}(V_{n-1})+T_s\right) + pT_c\right]P_s(V_n,n)}{1-P_c(V_n,n)-P_e(V_n,n)-pP_s(V_n,n)}, \tag{10}$$

which was to be demonstrated.

4 Numerical results

In this section, we compare the performance of our lower bound and the standard Q-algorithm described above. In our illustrative example below, we set realistic

protocol timings borrowed from [5], in particular, we assume that $T_s = 8$ ms, $T_c = 0.9$ ms, $T_e = 0.61$ ms.

We begin with comparing our lower bound and the average identification time delivered by the standard Q-algorithm (for convenience the parameter C is set to 1) depending on the number of tags in the system (see Fig. 1). Here, we let the probability of error in the RN16 transmission be equal 0.5 as suggested in [5] for realistic conditions. In case of an ideal channel (the two lower curves), the average gain remains around 8%. Thus, we may conclude that *any* modification of the Q-algorithm cannot outperform the lower bound and, hence, the respective gain will not exceed this value.

If the RN16 transmission is not protected, that is when a potentially successful slot is treated as a conflict with the probability $p = 0.5$, and the tag remains unidentified (the upper set of curves), the Q-algorithm deviates from the lower by up to 15%. The latter indicates that the performance of the Q-algorithm may be further improved before it reaches its lower limit.

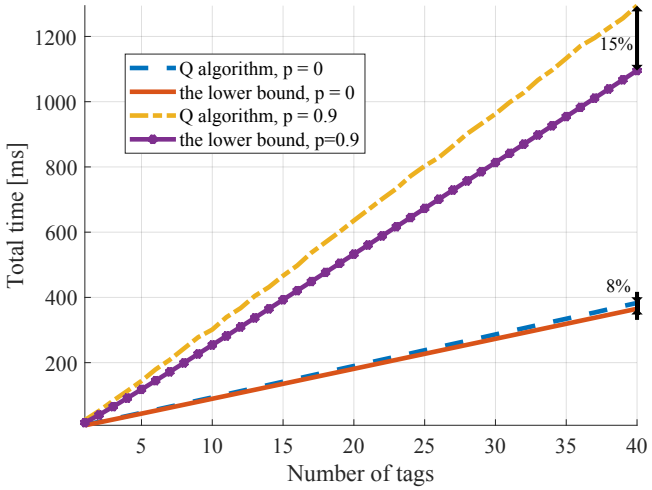

Fig. 3. Comparison of the average identification time of the standard Q-algorithm and the lower bound: (i) for an ideal channel and (ii) in case of RN16 transmission failure (error-prone channel).

Further, Fig. 4 shows the dependence of the average identification time on the value of the parameter $\tilde{V}_n$ if the total number of tags is ten and the probability p is varied. In particular, we assume that $V_i, i = 1, ..., 9$ are known and V_{10} is to be determined based on minimization over potential values of the optimal frame length denoted as $\tilde{V}_{10}$. We intentionally change our parameters to $T_s = 0.5$ ms, $T_c = 0.3$ ms, and $T_e = 1$ ms, as the previous set does not provide results illustrative enough for our purposes. As shown in Fig. 4, with the growth of p, the average identification time increases as more transmission attempts are required for the success. We may also observe a curious effect: all curves reach their minimums at the same value of $\tilde{V}_n$. We note that varying parameters T_s, T_c, T_e

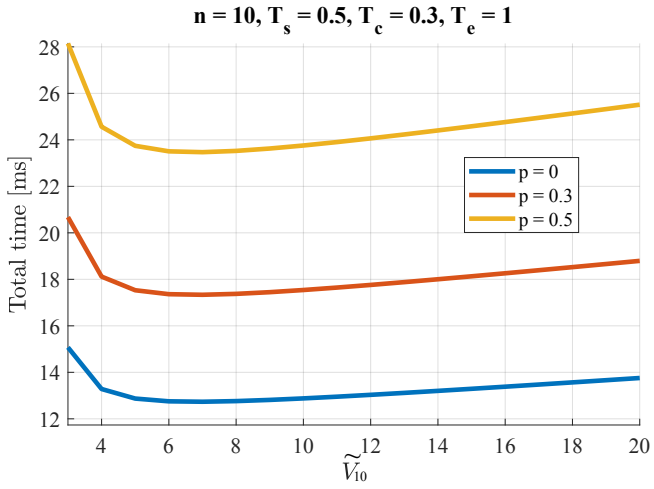

Fig. 4. Average identification time vs. the length of the frame.

displays quite a similar behavior, however, the minimums might become less visible. As such, we conclude that V_n may not depend on p; however, strict proof of this hypothesis is out of the scope of this paper.

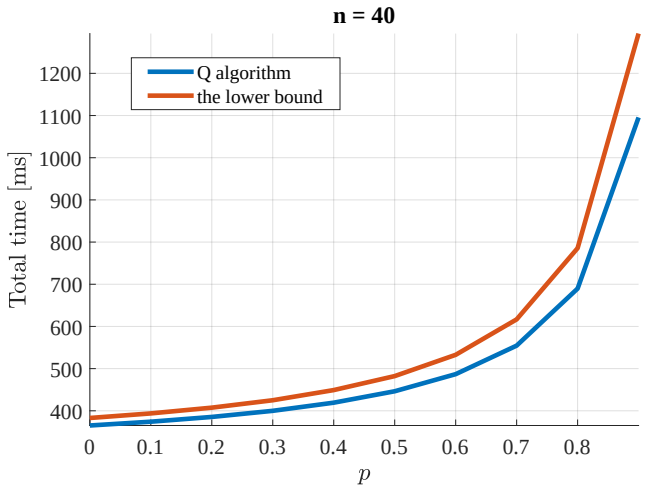

Fig. 5. Dependence of the total identification time on the probability p in case of 40 tags.

Finally, we increase the number of tags in the system up to 40 and vary the probability p (see Fig. 5). As the probability of incorrect decoding of the RN16 sequence increases, the average identification time rises exponentially and naturally tends to infinity with $p \to 1$. We note that the difference between the

lower bound and the standard algorithm will also widen with the growth of p. Hence, we may conclude that the presence of channel errors creates possibilities for improving the performance of the standard algorithm, and its modifications may bring significant benefits for the system in general.

5 Conclusion

In this paper, we study an RFID system operation based on the standard Q-algorithm, for which there exist a variety of modifications that aim at minimizing the average identification time. Here, we derive a lower bound for the average identification time by introducing a hypothetical algorithm, which is aware of the current number of unidentified tags. We as well demonstrate that in case of an error-free channel, the performance of the legacy Q-algorithm is reasonably close to the proposed lower bound and any further modifications will not bring additional benefits. However, for the error-prone environment, where the RN16 sequence may be decoded incorrectly, the gap between the performance of the standard scheme and the lower bound substantially increases, thereby indicating the need for new identification algorithms in this area.

Acknowledgment

The work of N. Stepanov, N. Matveev, and A. Turlikov is supported by scientific project No. 8.8540.2017/8.9 "Development of data transmission algorithms in IoT systems with constraints on the devices complexity".

References

1. Arjona, L., Landaluce, H., Perallos, A., Lopez-Garcia, P., Cmiljanic, N.: Analysis of RFID anti-collision protocols based on the standard EPCglobal Class-1 Generation-2. In: European Wireless 2015; 21th European Wireless Conference; Proceedings of. pp. 1–6. VDE (2015)
2. Global, EPC: EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz–960 MHz. Version **1**(0), 23 (2008)
3. Instruments, Texas: TI UHF Gen2 Protocol Reference Guide
4. Kamrani, A.: Design and Development of a State Transition Tablefor the EPCglobal UHF Class1 Gen2 RFID standard. Ph.D. thesis, University of Pittsburgh (2011)
5. Namboodiri, V., DeSilva, M., Deegala, K., Ramamoorthy, S.: An extensive study of slotted ALOHA-based RFID anti-collision protocols. Computer communications **35**(16), 1955–1966 (2012)
6. Ometov, A., Solomitckii, D., Olsson, T., Bezzateev, S., Shchesniak, A., Andreev, S., Harju, J., Koucheryavy, Y.: Secure and Connected Wearable Intelligence for Content Delivery at a Mass Event: A Case Study. Journal of Sensor and Actuator Networks **6**(2), 5 (2017)
7. Prudanov, A., Tkachev, S., Golos, N., Masek, P., Hosek, J., Fujdiak, R., Zeman, K., Ometov, A., Bezzateev, S., Voloshina, N., et al.: A trial of yoking-proof protocol in RFID-based smart-home environment. In: Proc. of International Conference on Distributed Computer and Communication Networks. pp. 25–34. Springer (2016)

8. Uysal, I., Khanna, N.: Q-frame-collision-counter: A novel and dynamic approach to RFID Gen 2's Q algorithm. In: RFID Technology and Applications (RFID-TA), 2015 IEEE International Conference on. pp. 120–125. IEEE (2015)
9. Zheng, F., Kaiser, T.: Adaptive ALOHA anti-collision algorithms for RFID systems. EURASIP Journal on Embedded Systems **2016**(1), 7 (2016)