



Performance Evaluation of Slotted Aloha Anti-Collision Protocol for Mobile RFID Tags Identification using NHPP

Dr. Shachi Sharma¹, Abdul Shakoor²

¹Department of Computer Science, South Asian University, New Delhi, India, shachi@sau.int

²Department of Computer Science, South Asian University, New Delhi, India,abdulshakoor.malang@gmail.com

ABSTRACT

Radio Frequency Identification (RFID) plays an important role in identifying objects in evolving field of the internet of things (IoT). One important issue relates to the identification of RFIDs. Despite wide research on this topic, not much work is performed in case when objects with RFID tags are mobile. The paper presents a simulation-based study, employing non-homogeneous Poisson process to model variable number of tags in an interrogation area, to analyze the performance of the slotted aloha anti-collision protocol in the mobile RFID tags identification. It is observed that the maximum throughput of the protocol reduces as the number of tags increases, however, the throughput usually remains higher than that of aloha protocol in static environment. These results will help in developing better probabilistic anti-collision protocols for dynamic environment in future.

Key words : Anti-collision protocol, IoT, mobile RFID, non-homogeneous Poisson process, slotted aloha.

1. INTRODUCTION

Recent years have witnessed tremendous growth in the number of connected devices leading to the realization and expansion of IoT which is a networking technology through which anything (or object or device) can be identified and connected to internet [1] [2]. One of the main enabling technologies for IoT is RFID tags that can be attached to any object thus facilitating it to be identified uniquely [3] [4]. IoT uses RFID as one of the most important technology for tracking, monitoring, and locating things. With IoT expansion, mobile RFID systems have become significantly important. For example, in product registry systems where tags continuously enter and leave the interrogation region. The very idea of auto-identification is not new and it refers to autonomous identification of objects through technology. Object is a generic term used to refer to people, good, or item. With the movement of objects across the countries around the world and many application's requirements to track them, the need for auto-identification is increasing. Various technologies have been developed to identify the objects such as barcodes, smart cards and RFID. Out of these, RFID has gained popularity and has become most widely adopted auto-identification technology [5].

There are three components of an RFID system – tag, reader, and host domain [6]. The RFID tag contains a unique identifier. When attached to an object, this identifier identifies the object. The tag communicates with the reader over a wireless channel and passes the information such as identifier to the reader. The RFID reader is an intermediary between tags and the host domain. It queries the tags continuously and tags respond by sending their identifier. To communicate with the tags, the reader uses radio waves as the transmission medium. Thus, the reader has an antenna. All RFID readers are connected to their respective host domains over networks. The host domain has a server and a database that keeps all the data about the tags. Usually, the manufacturer of the tags creates and maintains the host domain [6]. The reader can retrieve the details about the object by contacting the host domain. This is how the objects are tracked using an RFID system seamlessly [3]. Since the mapping between a tag and the object is stored in the database at the host domain, the tag can be reused by updating the host domain.

There are two types of RFID tags viz. active and passive. Active RFID tags have a battery and thus can be updated. Passive RFID tags take power from the reader and do not have any battery attached to them [6]. The reader can recognize the tags in an area ranging from a few meters to several meters. The communication between the reader and the tags is affected by many factors such as distance, interference due to buildings, trees, etc. [4] [6]. Hence, there are several problems associated with RFID systems. One such problem relates to collision [3]. RFID system suffers from two types of collisions - reader collision and tag collision. The reader collision happens when the coverage area of one reader overlaps with another reader. This leads to two problems viz. signal interference and multiple recognition of the same tag [7]. The problem of signal inference can be solved by using TDMA (Time Division Multiple Access) [8]. Tag collision occurs in an RFID system when more than one tag reply to the reader's query at the same time and the reader does not able to distinguish the messages resulting in a collision. Hence, there is a requirement of anti-collision protocol for RFID tags identification. Broadly, the two categories of anti-collision protocols have been proposed in the literature- probabilistic such as aloha and deterministic such as query tree, the detailed overview of the same is provided in section 2.

Existing literature on anti-collision protocols for RFID tags identification is mostly focused on the case when the number of tags in an area is fixed. However, with growing IoT applications, the objects and thus the tags can be mobile or the number of tags in the neighborhood of an RFID reader are not static. One example is garbage selection in a smart garbage collection system in a smart city. In such a system, the moving RFID reader scans the reusable garbage with tags attached. Then, the number of tags in the vicinity of the reader always varies with time. Such an environment is dynamic. In spite of wide literature available on RFID tags identification, there is very limited work present on the anti-collision protocol for mobile RFID tags identification. One notable work is by Jia *et al.* [9] who proposed a dynamic anti-collision protocol, called Dynamic Collision Tree (DCT) for identifying tags in mobile RFID identification systems where tags move into and leave the reading area. Another more general framework, called PrIME (Priority based tag Identification in Mobile Environments), is developed in [10]. The main drawback of PrIME is its two-step procedure resulting in delays and complexity. On the other hand, aloha-based protocols are simple to implement. Hence, it is pertinent that their suitability and performance for mobile RFID identification system is evaluated first. The paper contributes towards this direction. The dynamic environment of the mobile tags is modeled by the Non-Homogeneous Poisson Process (NHPP) and a simulation-based performance evaluation of slotted aloha anti-collision protocol is carried out. The paper is organized into five sections. An overview of popular anti-collision protocols for RFID tags identification is provided in section 2. The model of the slotted aloha protocol for mobile RFID system is proposed in section 3. The details of NHPP are also discussed in the same section. The simulation procedure and the results are presented in section 4. The last section concludes the paper.

2. REVIEW OF ANTI-COLLISION PROTOCOLS

One of the main issues in an RFID environment relates to tag collision as it reduces the system efficiency and results in longer delay in identifying tags. Two approaches viz. probabilistic and deterministic are discussed in this section.

2.1 Probabilistic Protocols

Probabilistic protocols use a random-access strategy and allow tags to transmit their data in randomly selected time slots. This strategy reduces the possibility of a tag collision because a tag is only allowed to send its data in a randomly selected slot. Probabilistic protocols do not guarantee that all the tags will be identified successfully in the reading process. Aloha based protocols belong to the probabilistic protocol's category. Aloha-based protocols can be divided into four classes [9].

Pure Aloha (PA)

In early 1970, Norman Abramson and his associates proposed

pure aloha protocol at the University of Hawaii to address the problem of the traffic congestion in the network [11]. PA considers time as continuous. The tags can transmit their data whenever they have the data to send. If multiple tags transmit data together, then a collision occurs. The solution for collided tags is to retransmit their data after a random amount of time. PA is the simplest anti-collision algorithm and easy to implement. By choosing time randomly, tags reduce the probability of collision. In PA, tags send their data without checking whether the channel is free or not. In case, two or more tags simultaneously transmit, the reader identifies that there are multiple tags that are trying to send their data, so they become unidentified and complete collision occur. The maximum efficiency of the pure aloha protocol is 18.4% [11].

Slotted Aloha (SA)

In this protocol, the time is divided into discrete time interval slots. Each tag has the chance to randomly choose one of the slots and transmits data within a single slot. Tags are only allowed to send their data at the beginning of a slot, otherwise, they must wait until the beginning of the next slot. With this procedure in the slotted aloha protocol, either the tags collide completely or do not collide at all. The collided tags wait for the random number of time slots and then retransmit. The maximum throughput of the SA is 36.8% [11].

Framed Slotted Aloha (FSA)

The slotted aloha cannot perform better where there are large number of tags in the RFID system. Frame slotted aloha protocol overcomes this drawback of slotted aloha. The FSA divides the time into different number of frames, and each frame contains the same number of time slots. A tag is allowed to transfer its data only once in each frame. By using this method FSA reduces the collisions significantly compared to slotted aloha. In case if the frame is large and there are small number of tags then FSA wastes a large number of time slots [12]

Dynamic Framed Slotted Aloha (DFSA)

DFSA is an extension of FSA. In the first step, DFSA estimates the number of tags. In the second step, it accordingly fixes the frame length and proceeds like FSA. The main disadvantage of DFSA is the first step that degrades its efficiency significantly [13]. Also, approximating number of tags accurately in dynamic environment is a difficult task.

Mathematical Model of Slotted Aloha Anti-Collision Protocol

All probabilistic anti-collision protocols work on slotted time slots. The performance of SA has been analyzed by developing a mathematical model [14]. Let G be the attempt rate i.e. the expected number of packets transmitted in a time slot, n be the number of backlogged tags, λ is the arrival rate,

q_r is the probability that a backlogged packet is retransmitted in a time slot. The number of packets per slot is approximated by a Poisson random variable with mean [14]

$$G = \lambda + nq_r \quad (1)$$

The probability of m attempts then becomes

$$P(m) = G^m \cdot e^{-G} / m! \quad (2)$$

If there are no attempts in a time slot i.e. idle slot, its probability is

$$P(0) = e^{-G} \quad (3)$$

The probability of successful transmission equals to the probability of only one attempt in a slot i.e.

$$P(1) = Ge^{-G} \quad (4)$$

and the probability of collision becomes

$$P(\text{Collision}) = 1 - P(\text{Success}) - P(\text{Idle}) \quad (5)$$

If the attempt rate G is greater than unity, there will be too many idle slots and if G is less than unity then there will be too many collisions. It can be easily noted from (4) that the maximum throughput is obtained when G tends to 1 then the external arrival rate of $1/e \approx 0.36$ packets per slot can be sustained [14]. If backlog increases beyond an unstable point, then it tends to increase without limit and the departure rate drops to zero. The expected change in backlog over a time slot, called drift in state n is given by [14]

$$D(n) = \lambda - P(\text{Success}) = \lambda - G(n)e^{-G(n)} \quad (6)$$

2.2 Deterministic Protocols

Unlike probabilistic protocols, deterministic protocols have enough time to detect the whole set of RFID tags in the reading area and thus results in more accuracy. Binary tree protocol, query tree protocol, collision tree protocol, and dynamic collision tree protocol are the main types of deterministic RFID anti-collision protocols [11].

Binary Tree Protocol (BT)

Binary tree protocol guarantees that the whole set of tags in an area can be identified during each cycle. BT protocol splits the tag's ID into groups using pseudo random number generator until all tags are identified. The tags have a counter associated which is initialized with zero. When the reader sends a query, only the tags with counter zero reply and send their ID. After receiving responses, the reader provides three types of notification - identification, collision, and no answer. In case of collision, all tags with counter zero modify its value by adding random bit 0 or 1. This way, the tags are grouped in two at each step. The process continues till all tags are identified [11].

Query Tree Protocol (QT)

It is a memoryless protocol, in which the reader broadcasts query with a tag prefix (a bit string) into the reading area and the tags whose ID matches with the prefix, can respond to the reader. If one tag responds, then the tag gets identified successfully by the reader. In case of no response is received by the reader, it identifies that there is no tag with the sent

prefix, hence the query is rejected and the slot is known as idle slot. If more than one tag ID matches with the prefix sent by the reader, then the reader generates two new queries by appending the zero (0) and one (1) to the stored prefix. The process repeats continuously until only one tag responds to the reader query [11]. Since the response of the tags depends on the query by the reader only and not on the history of the queries, QT is called memoryless.

Collision Tree Protocol (CT)

Both BT and QT protocols suffer from idle slots problem leading to degradation in their performance. To avoid idle slots, CT protocol [12] has been proposed with efficiency of up to 50%. In CT protocol, prefixes are generated and tags are divided into groups based on the first collided bit. Given a query with m bits $q_1q_2 \dots q_m$ and the reply $r_1r_2 \dots r_{c-1}r_c$ where r_c is the first collided bit, the reader generates $q_1q_2 \dots q_m r_1r_2 \dots r_{c-1}0$ and $q_1q_2 \dots q_m r_1r_2 \dots r_{c-1}1$ as two prefixes dividing the group of tags matching with the query into two [12]. Also, in the CT, the tags respond by transmitting only the unmatched part of the ID i.e. the part of the ID which matches with the prefix is not included in the reply. As compared to BT and QT, CT protocol requires fewer cycles to identify same number of tags in an area [12].

Dynamic Collision Tree Protocol (DCT)

DCT [9] is an extension of CT protocol for the dynamic RFID environment and hence assumes that tags are coming to or leaving from the reader's coverage area during the identification process. DCT uses a stack data structure to store the reader prefixes. If the stack is empty, then the reader pushes an empty prefix string ϵ . The identification process of DCT begins with extracting the query prefix from the stack and sending it in the interrogation zone. Tags match their ID with the prefix and respond to the reader. If the prefix is empty string ϵ , then all unidentified tags reply with their whole ID. Otherwise, the tags send only unmatched part of their IDs to the reader like in CT protocol. In case of collision, the DCT generates the prefix according to the first collided bit as in CT. DCT uses Manchester code for tracking the position of collided bits in the reply [9].

There are two types of nodes in DCT - internal node and leaf node. Collision happens in the internal node so it is also called the collision node and a leaf node is also called tag node. To identify a tag, the reader starts scanning from root to the leaf and from left to right repeatedly. After completing the scan, the tag at the leaf node gets identified and then the tag node and its parent are deleted from the tree. When a new tag enters into the mobile RFID system, the reader creates both leaf and tag nodes in the tree. Hence, in DCT, the tree keeps changing with time as and when tags enter or leave the area.

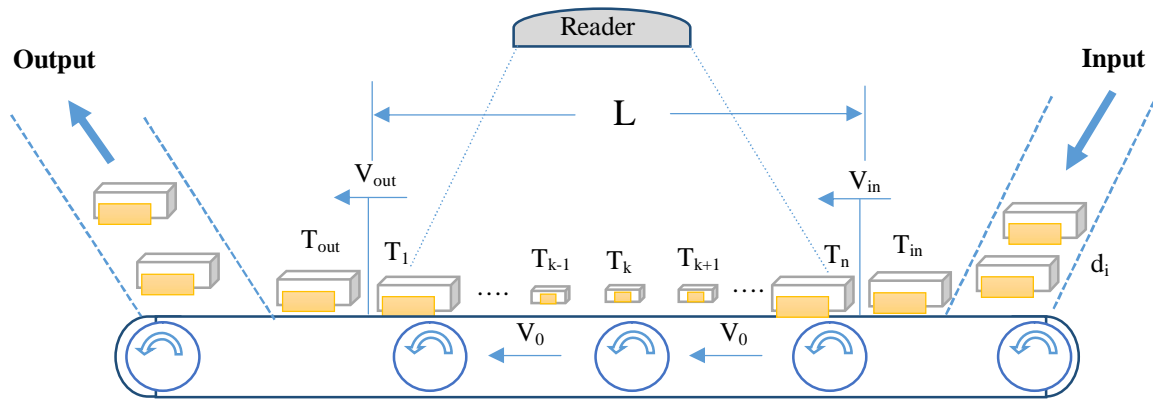


Figure 1: Mobile RFID system as conveyor belt, adapted from [9].

Collision is the critical issue in the RFID systems which leads to the waste of bandwidth and increases latency. To solve this issue, many anti-collision protocols have been proposed in both categories of probabilistic and deterministic protocols. In the case of mobile RFID environment, the performance of DCT has been analyzed in the past, however, there is no study conducted on the probabilistic anti-collision protocol in dynamic environment.

3. MOBILE RFID SYSTEM AND SLOTTED ALOHA ANTI-COLLISION PROTOCOL

There are two types of RFID systems - static and mobile. In static RFID system, the tags stay in the reader's interrogation zone until they are recognized. However, in the mobile RFID system, the tags are coming and leaving the interrogation area with time and thus make the system dynamic. Usually, the mobile RFID system is modeled by drawing an analogy from the conveyor belt as shown in the Figure 1. The conveyor takes items that have RFID tags attached to them. These items come from the input and pass through the reader region and exit from the output. The transporter system installs the reader above the belt and detects the tags that cross the reading area. The length of the transporter belt is $L(m)$. Input system puts the tags on the transporter belt with linear density d_0 (tags/m) that cross the interrogation region with the speed of $V(m/s)$ from right to left. In the Figure 1, T stands for tags, T_{in} and T_{out} are the tags that are coming and leaving and T_k is the tag passing through the reader's reading area [9].

The conveyor belt analogy clearly explains the dynamic aspect of a mobile RFID system. Many tags arrival models have been studied [15] in the past. The most generic is dynamic arrival model where the number of tags in the interrogation area keeps on changing with time. To the best of our knowledge, there is no work exists to analyze the performance of any anti-

collision protocol under dynamic arrival model. The number of tags in an interrogation area in the dynamic arrival model is a counting stochastic process $\{N(t), t > 0\}$. Since slotted aloha is a basic probabilistic anti-collision protocol used widely in RFID tags identification, we study its performance in dynamic environment.

In mobile RFID system, both the new arrival rate of tags and number of backlogged tags become time dependent leading to a time dependent version of (1) as

$$G(t) = \lambda(t) + n(t).q_r \tag{6}$$

With this, the number of tags in an interrogation area of mobile RFID system can no longer be Poisson, rather it can be better modeled by the Non-Homogeneous Poisson Process with its intensity function given by (6).

NHPP

Poisson processes are usually used for predicting events' arrival. The homogeneous Poisson process is a simple representation of an arrival process where the mean arrival rate is constant. In contrast, NHPP is a more complex model in which the arrival rate is not constant and varies with time [16].

A counting process $\{N(t), t > 0\}$ is said to be NHPP with intensity function $G(t)$, if it satisfies following [16]

- $N(0) = 0$, almost surely
- $\{N(t), t > 0\}$ has independent increments
- $P\{N(t + \Delta t) - N(t) \geq 2\} = o(\Delta t)$
- $P\{N(t + \Delta t) - N(t) = 1\} = G(t) \Delta t + o(\Delta t)$

where $\lim_{\Delta t \rightarrow 0} \frac{o(\Delta t)}{\Delta t} \rightarrow 0$, as $\Delta t \rightarrow 0$.

It is difficult to solve the NHPP with intensity function $G(t)$ in (6) analytically, hence we resort to simulate slotted aloha protocol using NHPP to model number of tags.

Algorithm 1: Thinning Algorithm [16]

- Step 1:** $t = 0, I = 0.$
- Step 2:** Generate $U_1 \sim Uniform(0,1).$
- Step 3:** set $t = t - (\ln(U_1))/\bar{\lambda}$
 If $t > T,$ stop;
 else go to step 4.
- Step 4:** Generate $U_2 \sim Uniform(0,1),$ independent of $U_1.$
- Step 5:** If $U_2 \leq \frac{\lambda(t)}{\bar{\lambda}},$ set $I = I + 1, S(I) = t.$
- Step 6:** Go to Step 2.

4. SIMULATION EXPERIMENTS AND RESULTS

With an objective to simulate the dynamic environment of mobile RFID system, we use popular thinning algorithm [16] to generate NHPP events i.e., the number of tags in an area. The thinning algorithm generates events of an NHPP with rate $\lambda(t)$ on the interval $t \in [0, T]$ by selecting $\bar{\lambda}$ such that $\lambda(t) \leq \bar{\lambda}$ for all $t \in [0, T].$ The detailed algorithm is presented in the Algorithm 1.

We simulate the slotted aloha protocol for mobile RFID system in MATLAB. The flow chart of the simulator is shown in the Figure 2. The simulator generates the number of mobile RFID tags using the thinning algorithm. Then for each tag, a timeslot is selected randomly. All the time slots are further checked for a collision. If there is no collision, a tag gets identified successfully. In case of collision, the process is repeated with a new number of tags to emulate the dynamic environment. The simulator also calculates the total identified and unidentified tags. The throughput (the rate at which successful transmissions are processed per time slot) of the protocol is also measured in the simulator.

At the beginning of an experiment, the number of tags is fixed randomly and is an input to the simulator. The simulator runs till the total number of input tags is processed. The variation of number of identified tags versus number of tags for a total of 66856 tags is depicted in the Figure 3. The number of identified and unidentified tags in each experiment are shown in the Table 1. Contradictory to the expectation, the percentage of total number of identified tags does not decrease as the total number of tags are increased. This happens because of the dynamic nature of the mobile RFID system. Some tags may leave the interrogation area after the reader has sent the query. The variation of average and maximum throughput with the number of tags is presented in the Table 2. It can be observed that the average successful transmissions per time slot is 39.09 % and the maximum successful transmissions is 50.0 % for a total 256 tags experiment. It implies that maximum of half of the mobile RFID tags can be identified successfully per time slot. Both the average and maximum throughput reduces as the total number of tags are increased.

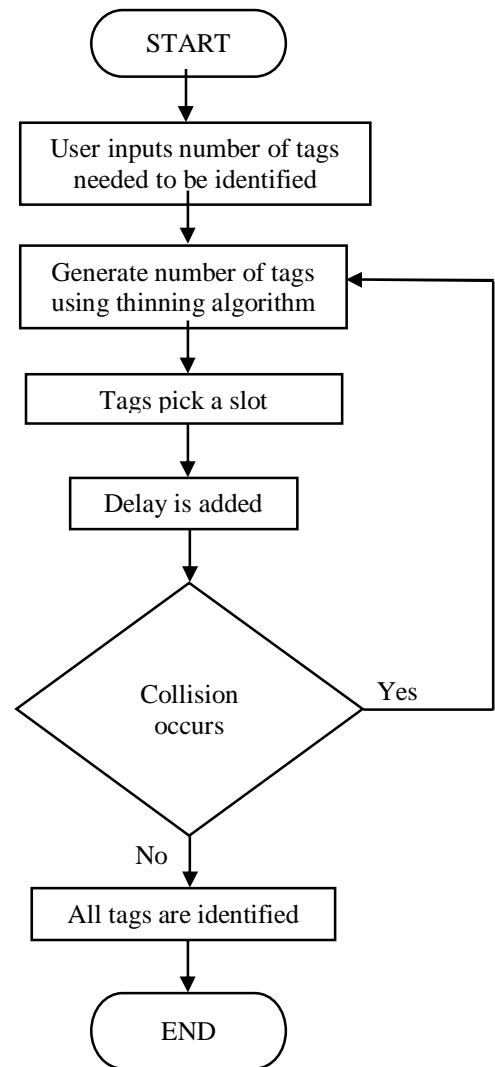


Figure 2: Flow chart of simulator.

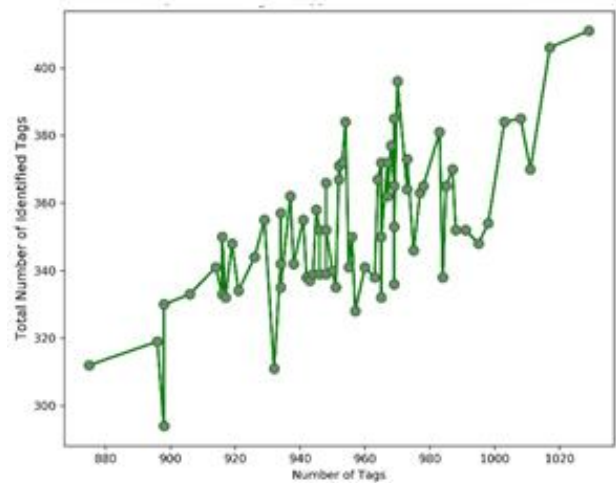


Figure 3: Variation of number of identified tags for total number of 66856 tags.

Table 1: Results on number of identified tags

Number of tags	Number of identified tags	Percentage of identified tags	Number of unidentified tags	Percentage of unidentified tags
20	10	50.0 %	10	50.0 %
30	12	40.0 %	18	60.0 %
55	16	29.09 %	39	70.91 %
66	24	36.36 %	42	63.64 %
85	34	40.0 %	51	60.0 %
256	96	37.5%	160	62.5%
5938	2264	38.12%	3674	61.87%
66856	24710	36.96 %	42146	63.03 %

Table 2: Results on throughput

Number of tags	Average throughput	Maximum throughput
256	39.09 %	50.0 %
5938	36.38 %	41.82 %
66856	34.5 %	36.75 %

5. CONCLUSION

The paper highlights the requirement to analyze the performance of probabilistic aloha based anti-collision protocols for mobile RFID systems. The mathematical model of slotted aloha protocol has been modified to capture the time dependent dynamics of mobile RFID system. Such a model is difficult to solve analytically. Hence, a simulation procedure using NHPP is proposed to study the performance of slotted aloha anti-collision protocol for mobile tags identification. It is observed that the percentage of identified tags is more than 35% in the majority of the experiments. However, in a few cases, the percentage of identified tags is less than 30%. The average throughput is found to decrease as the number of tags increases. It is only when the number of tags is more than 5000 that the average throughput goes down below the static slotted aloha protocol. These results will help in providing future research directions on the development of probabilistic anti-collision protocols for mobile RFID systems which is essential in the domain of IoT.

REFERENCES

1. J. S. Bhanu, JKR Sastry, V. S. Kumar, V. Sai, and K. V. Sowmya, **Enhancing performance of IoT networks through high performance computing**, International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, no. 3, 2019.
2. S. Sharma, **Attribute based discovery architecture for devices in Internet of Things (IoT)**, in *5th Intl. Conf. on Convergence in Technology*, 2019.
3. H. Saadi, Y. Mustapha, and R. Touhami. **Role and application of RFID technology in internet of things: communication, authentication, risk, and security concerns**, The ISC Int. J. of Info. Security, vol. 11, no. 3, pp. 9–17, August 2019.
4. J. Xiaolin, F. Quanyuan, F. Taihua, and L. Quanshui. **RFID technology and its applications in Internet of Things (IoT)**, in *2nd Int. Conf. on Consumer Electronics, Communications and Networks, CECNet*, Yichang, 2012, pp. 1282-1285.
5. Z. Al-Amir, F. A. Al-Saidi, and H. Abdulkadir, **Design and implementation of RFID system**, in *5th Intl. Multi-Conf. on Systems, Signals and Devices*, Amman, 2008, pp. 1-6.
6. M. Bolic, D. Simplot-Ryl, and I. Stojmenovic. **RFID Systems: Research Trends and Challenges**, 1st ed. Wiley, 2010.

7. C.Nikola, L. Hugo, and P. Asier. **A comparison of RFID anti-collision protocols for tag identification**, Appl. Sciences, vol. 8, 2018.
8. W. Yoon, and N. H. Vaidya. **RFID reader collision problem: performance analysis and medium access**, Wireless Communications and Computing, vol. 10, no. 5, pp. 420-430, 2012.
9. X. Jia, M. Bolic, Y. Feng, and Y. Gu. **An efficient dynamic anti-collision protocol for mobile RFID tags identification**, IEEE Commun. Letts., vol. 23, no. 4, pp. 620-623, April 2019.
10. D. Benedetto, G. Maselli, and C. Petrioli. **Fast identification of mobile RFID tags**, in *IEEE 9th Intl. Conf. on Mobile Ad-Hoc and Sensor Systems*, 2012.
11. X. Jia, Q. Feng, T. Fan, and Q. Lei. **Analysis of anti-collision protocols for RFID tag identification**, in *2nd Intl. Conf. on Consumer Electronics, Communications and Networks*, 2012.
12. J. Yu, and L. Chen. **Stability analysis of frame slotted aloha protocol**, in *IEEE 23rd Intl. Symp. on Quality of Service*, 2015.
13. C. T. Nguyen, K. Hayashi, M. Kaneko, P. Popovski, and H. Sakai. **Probabilistic dynamic framed slotted ALOHA for RFID tag identification**, Wireless Pers. Commun., vol. 71, pp. 2947–2963, 2013.
14. D. Bertsekas, and R. G. Gallager. **Data Networks**, 2nd ed. Prentice Hall, 1992.
15. W. Zhu, J. Cao, H. C. B. Chan, X. Liu, and V. Raychoudhury. **Mobile RFID with a high identification rate**, IEEE Trans. on Computers, vol. 63, no. 7, pp. 1778 – 1792, Jul. 2014.
16. P. A. W. Lewis, and G. S. Shedler. **Simulation of nonhomogeneous Poisson Processes by thinning**, Naval Research Logistics Quarterly, vol. 26, no. 3, pp. 403-413, 1979.