Journal of
Sensor and Actuator Networks

MDPI

Article

FTSMAC: A Multi-Channel Hybrid Reader Collision Avoidance Protocol for RFID Network

Rachid Mafamane [1], Asmae Ait Mansour [2], Mourad Ouadou [1,*] and Khalid Minaoui [1]

[1] LRIT Laboratory, Faculty of Science, Mohammed V University in Rabat, Rabat 10000, Morocco; rachidmafamane@gmail.com (R.M.); khalid.minaoui@fsr.um5.ac.ma (K.M.)
[2] Communication Systems Department, National Institute of Posts and Telecommunications (INPT), Rabat 10000, Morocco; asmae.ait@gmail.com
* Correspondence: mr.ouadou@um5r.ac.ma

Abstract: Due to the emergence of the Internet of Things, the need for effective identification and traceability has increased. Radio-frequency identification (RFID), a simple and cheap approach for gathering information, has therefore drawn the attention of research communities. However, this system suffers from problems caused by high density, such as collisions and duplication. Thus, the deployment of RFID is more effective in a dense environment where it may improve overage and delays. A wide range of solutions have been proposed; however, the majority of these are based on the application context. In this paper, we propose a general MAC layer protocol FTSMAC (Frequency Time Scheme MAC) in which the spectrum frequency is efficiently used by dividing the signal into different time slots via a messaging mechanism used by RFID readers. This limits the collisions in high-density RFID deployment that affect the performance of the system. Thus, our solution allows the communication system to converge to a stable state within a convenient time.

Keywords: RFID system; reader collision problem; reader-to-reader interference; reader-to-tag interference; distributed systems; MAC layer; resource allocation

check for updates

Citation: Mafamane, R.; Ait Mansour, A.; Ouadou, M.; Minaoui, K. FTSMAC: A Multi-Channel Hybrid Reader Collision Avoidance Protocol for RFID Network. *J. Sens. Actuator Netw.* **2021**, *10*, 46. https://doi.org/10.3390/jsan10030046

Academic Editors: Da-Zhi Sun, Yangguang Tian and Yanrong Lu

Received: 19 May 2021
Accepted: 29 June 2021
Published: 9 July 2021

1. Introduction

Radio-frequency identification (RFID) is a technology that automatically identifies objects, and is based on the principle of tagging objects, humans, or animals to facilitate their integration in computing or data systems [1]. The main components of this technology are tags and readers, and, due to its simplicity, the future of RFID is promising. Furthermore, many applications have adopted RFID technology as a base for identification and tracking [2]. RFID technology has been applied in a number of fields, including smart warehouses [3], healthcare [4], indoor localization [5], supply chain management [6], brain-research experiments [7], and modern agriculture [8].

Supply chain management is one of the main application fields for RFID technology. RFID has been used to improve the efficiency of the supply chain by allowing supervisors to control and track product information. However, despite the growing demand, the performance of RFID technology can be reduced by numerous factors, and particularly due to collisions between nodes [9–13].

Tags [14] are small components that consist of integrated circuits connected to an antenna and a small amount of memory to store data. In practice, problems of collisions and interference are mainly related to the deployment of the tags and readers [15].

Therefore, readers must have suitable resources to manage the communication process efficiently, by controlling access to the shared channel. They must also be strategically deployed to provide coverage of a large space to read the maximum number of tags. As shown in Figure 1, the reader uses radio waves to feed the tags. When activated, tags answer to the reader.

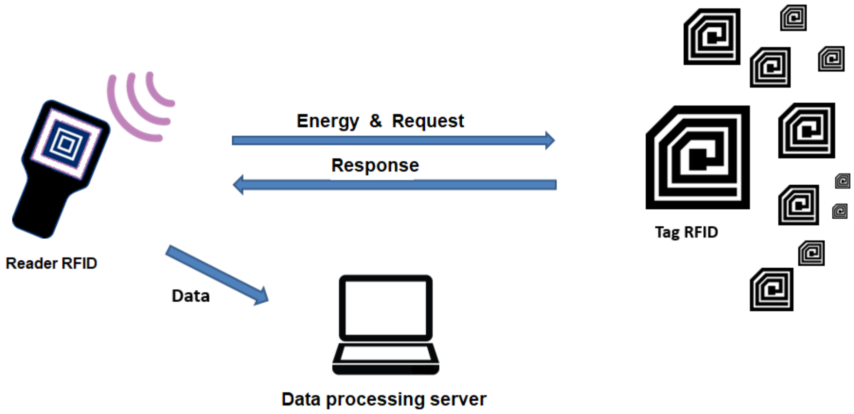

Figure 1. The basic concept of the interaction of an RFID system.

One of the major challenges in RFID networks is improving the throughput [16]. In an RFID network, a high density of readers [17] can have repercussions on the performance of the system due to a large number of collisions. As a result, the system may suffer from degradation of data collection efficiency, increased communication time, and high energy consumption. Thus, collisions represent a critical problem that considerably reduce the performance in RFID systems.

The RFID network considered in this paper is used as a wireless sensor network, on which readers and tags are randomly distributed, readers are fixed, and tags can move. Wireless sensor networks can use RFID systems to create a high-performance rechargeable platform. Several articles [18–23] define architectures for this sort of combination of RFID sensor networks.

Collisions are related to the Medium Access Control layer, which is responsible for access to the shared channel [24–27]. To solve this problem, several anti-collision protocols have been recently proposed [28–37]. These algorithms are based on medium access control techniques that allow the transmission of a large quantity of traffic on single or multiple channels. Among the methods used in RFID systems, TDMA uses a time division of the bandwidth, the principle of which is to distribute the available time between the different nodes. Alternatively, FDMA uses frequency banding to dynamically allocate part of the spectrum to each node. Finally, CSMA is used to detect or avoid message collisions in transmissions.

The algorithm presented in this paper is a hybrid solution combining the different FDMA, TDMA, and CSMA methods.

The remainder of this paper is organized as follows: Section 2 presents the RFID collision problem and related work. Section 3 describes our proposed FTSMAC algorithm, and Section 4 presents and describes the results of our simulation. Finally, Section 5 concludes the paper and gives perspectives.

2. Background and Related Work

2.1. Background

In this paper, we take into consideration two types of collisions [38]; Reader–Reader Interference (RRI) and Reader–Tag Interference (RTI). Figure 2 represents these types of interference by illustrating readers (R1 and R2) and tags (T, T1 and T2), with the reading range (rr1 and rr2) and the interference range (cr1 and cr2) of two readers, successively. dR1R2 represents the distance between these readers.

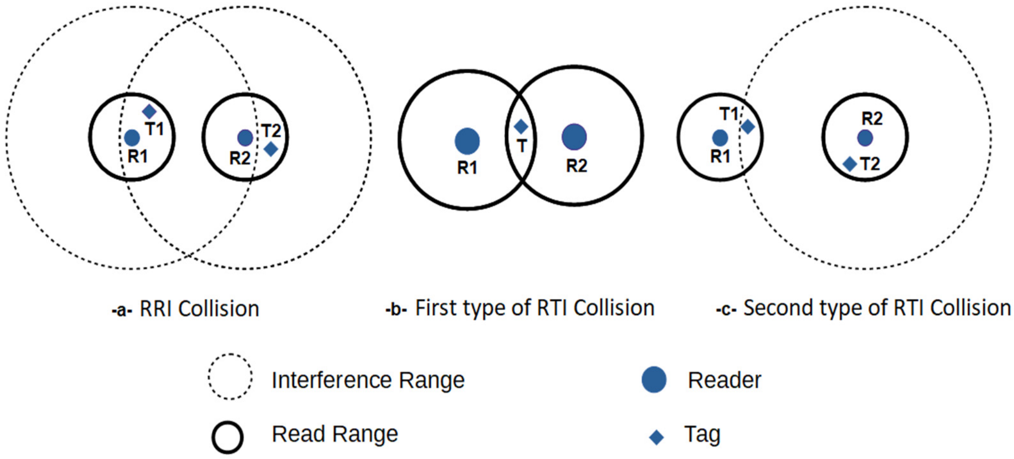

Figure 2. RFID collisions. (**a**) Reader-to-Reader Interference, (**b**) Reader-to-Tag Interference (1st type), (**c**) Reader-to-Tag Interference (2nd type).

2.1.1. RRI—Reader-to-Reader Interference

The RRI shown in Figure 2a occurs when several readers within an interference range (Equation (1)) are communicating simultaneously with the same frequency.

$$rr1 + rr2 < d_{R1R2} < max_{(cr1;cr2)} \quad (1)$$

2.1.2. RTI—Reader-to-Tag Interference

Two types of RTI interference can be distinguished. The first occurs when two or more readers attempt to interrogate the same tag simultaneously in their common reading range (see Equation (2)), independently of the working frequency. A representation of this interference is shown in Figure 2b.

$$d_{R1R2} < rr1 + rr2 \quad (2)$$

The second occurs when a tag is located in the interference range of a reader and in the reading range of another reader (see Equation (3)) that operates on the same frequency. This interference is shown in Figure 2c.

$$max_{(cr1;cr2)} < d_{R1R2} < max_{(cr1+rr2;cr2+rr1)} \quad (3)$$

In the remainder of this work, we discuss our anti-collision protocol for "Reader–Reader" and "Reader–Tag" Interference.

2.2. Related Work

Recently, many anti-collision algorithms have been proposed to reduce RFID-reader collisions and minimize interference. Existing protocols in RFID systems may be classified into two foremost groups, centralized and distributed protocols. An example of these protocols is cited in a previous review [39].

First, Pulse [40] is a distributed protocol based on CSMA that uses a control channel to exchange notifications between the readers and uses a data channel for tag interrogation. To avoid simultaneous reading, the reader in the interrogation range of tags broadcasts a beacon periodically through the control channel. Therefore, the remainder of the readers who listen to the control channel are free. However, in a dense RFID network, readers turn off a large number of their neighbors, which reduces the performance of the system.

Secondly, Coverage Oriented Reader Anti-Collision (CORA) [41] is a distributed mono-channel TDMA-based solution for RFID networks with mobile and time-critical deployment. The reader performs local learning of its neighbors. For this purpose, each reader starts by selecting a time slot, then, informs their neighbors in the collision domain. The collection of this information collected by the readers allows each one to calculate the number of readers in collision (same time slot) and non-collision (different time slot) according to their time slot used. The reader can activate and read the tags if the number of neighboring non-colliding readers is greater than the number of colliding readers.

By comparison, MCMAC [42] is a distributed multi-channel MAC protocol for RFID networks that uses several data channels to interrogate tags and a control channel for reader–reader communication. In this solution, each reader calculates its backoff randomly and turns off. When receiving a control message, the reader selects a free frequency and announces new busy channels. If there is no free frequency, it must wait for the next cycle. This protocol suffers from RTI because the simultaneous reading of the same tag by two readers causes collisions even if they use different frequencies, since only the control channel can solve RRI.

Similarly, Distributed Multi-Channel Collision Avoidance (DiMAC) [38] is a distributed multi-channel protocol based on CSMA that can resolve both RRI and RTI. It uses two control channels to exchange notifications between readers, and serves to signal the use of resources. The first channel is used to communicate the busy frequency to the readers in the interference field, and the second channel to inform the readers in the reading field of channel occupancy. Each reader generates “Start” and “End” packets to declare the occupation of the data channel or the freedom. Due to numerous messages exchanged, an overload is generated and affects the delay.

Distance Based RFID Reader Collision Avoidance (DRCA) [43], is a centralized TDMA distance-based protocol that listens to the channel and uses different time slots to avoid collisions. It improves the GDRA [44] protocol by allowing higher throughput using the Sift function to randomly choose time slots. The reader that chooses the previous time slot listens to the channel. If the channel is free, readers interrogate tags. Otherwise, they increase the number of time slots if the distance is long enough. If this does not occur, a reader-to-tag collision may happen.

The Beacon Analysis-Based RFID Reader Anti-Collision Protocol (BACP) [45] is a centralized protocol combining the TDMA and FDMA channel access control methods to reduce RFID reader collisions. These readers must listen to the channel to make their decision after receiving a priority code via the beacon. Similar to DRCA and GDRA techniques, the server signals the start of the round and, unlike NFRA, readers are not required to send the message continuously to their neighbors.

RFID Reader Anti-Collision Protocol with Adaptive Interrogation Capacity (NFRA-AIC) [46], is a centralized protocol based on the anti-collision method used by NFRA [47]. The RFID reader calculates the number of tags in its reading field to determine the time required for the interrogation of the tags.

The Reader-Coverage Collision Avoidance Arrangement (RCCAA) problem has been addressed to study how to enable readers and adjust their reading fields to query more tags without collision. The maximum-weight-independent-set-based [48] algorithm (MWISBA) is a protocol that addresses this problem by using multiple reading fields and proposes a heuristic-based method for the maximum-weight independent set to define the range of reading range from redundant readers. MWISBA, therefore, allows the reader-to-tag interference to be resolved by adjusting the reading field; however, the reader-to-reader interference is not taken into account.

MWISBAII [49] was proposed to improve and overcome the RRI problem of MWISBA by allowing to solve the different types of collision. This protocol converts the Reader Coverage Collision Avoidance (RCCA) problem into the MWIS problem. Then it uses graph theory to address MWIS. Finally, the MWIS solution can be translated back into a solution for the RCCA problem. This proposition is centralized, and the graphical transformation of the MWIS problem may require onerous central server computation.

In contrast to MWISBA and MWISBAII, which are centralized protocols, the goal of the new Distributed-MWISBAII [50] protocol, which represents the distributed version of

MWISBAII, is to assign to each reader the process of calculation and decision making, and to communicate this information to their neighboring readers.

As previously mentioned, the protocols are classified according to their deployment, i.e., centralized or distributed. Table 1 shows other attributes to clearly differentiate the protocols. These attributes are the ability to resolve RRI and RTI, the number of data channels used for tag interrogation, and finally, the channel access method used.

Table 1. Comparison of anti-collision protocols.

Attributes	PULSE	CORA	MCMAC	DIMAC	NFRA-AIC	BACP	DRCA	MWISBA	MWISBAII	Distributed-MWISBAII	FTSMAC (Proposed)
RRI	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓
RTI	✓	✓	-	-	✓	✓	✓	✓	✓	✓	✓
Distributed	✓	✓	✓	✓	-	-	-	-	-	✓	✓
Centralized	-	-	-	-	✓	✓	✓	✓	✓	-	-
Multi data channel	-	✓	✓	✓	-	-	✓	-	-	-	✓
CSMA	✓	-	✓	✓	✓	-	✓	-	-	-	✓
FDMA	-	-	✓	✓	-	✓	-	-	-	-	✓
TDMA	-	✓	✓	✓	✓	✓	✓	-	-	-	✓

Based on different criteria that characterize each protocol, the proposed solution described in the next section is suitable for stable distributed networks. In addition, our algorithm allows management of several data channels to involve more readers in the interrogation of tags and, therefore, increase the number of successful communications. This algorithm represents a hybrid solution using the FDMA, TDMA, and CSMA channel access control methods. To distribute frequency and time slot resources, we use a control channel only in the initialization phase for all readers to avoid notification overloading. Based on these elements, our proposal allows more successful communication and improved performance.

3. Proposed Algorithm

In this section, we describe our proposed FTSMAC protocol based on the CSMA, TDMA, and FDMA channel access control methods.

To avoid collisions between readers, the protocol strategy uses a notification system that allows readers, according to some defined criteria, to select neighbors. The idea is based on the reuse of the same frequency by neighbors at different time slots. This strategy provides readers with an effective reuse and management strategy for frequency resources.

3.1. Basic Principle

To understand the environment of our RFID networks in Figure 3, we denote Rx as the black reader. We assume that all readers are uniform and use multiple data channels to query tags, and a single control channel is used for communication with each other.

Colliding readers Ri (in red color) are competitors in the channel access of Rx because they are located within its interference range, where Ri is a reader among the set of neighbors and cr is the length of the interference range of the data channel.

Readers located in this area must operate on different frequencies and in different time slots to avoid both RRI and RTI collisions. We consider that the neighboring readers Rj (in blue color) reuse the frequency of Rx without problem, and we use crr as the control channel reading range. In view of this context, dxj represents the distance between Rx and its neighbor.

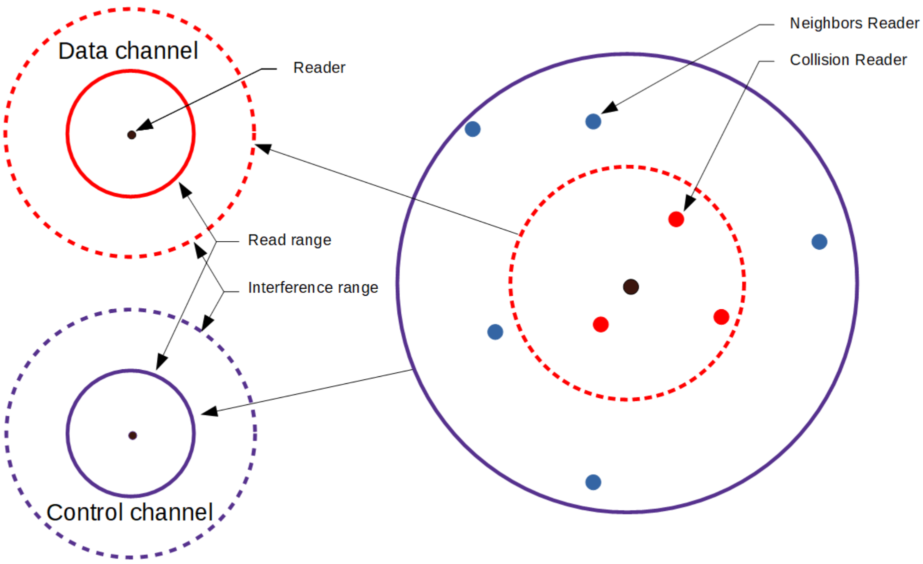

Figure 3. Basic architecture proposed for the RFID reader.

Using the control channel, the goal of Rx is to select one reader among neighbors Rj with the capability to reuse its frequency. We call the set of readers using the same frequency and time slot resource, "FTDMA_Scheme".

Each reader has a "Control table" in its memory (Table 1) that includes four fields:

- USED_PROTOCOL: The channel access methods used, FTDMA or CSMA.
- READER_IN_CHAIN: The readers constitute the FTDMA_Scheme to which this reader belongs.
- AFFECT_FREQ: The frequency to reuse.
- AFFECT_TS: The time slot to reuse.

As illustrated in (Table 2), the control message is constituted of six fields:

- TYPE: The type of message (REQUEST1, REQUEST2, RESPONSE, ADD_TO_CHAIN or NEW_CHAIN) according to the use case.
- READER_SENDER: The reader source identification.
- READER_RECEIVER: The reader destination identification.
- READER_IN_CHAIN: The set of readers' IDs using the same frequency.
- AFFECT_FREQ: The frequency to reuse by the destination reader.
- AFFECT_TS: The time slot to reuse by the destination reader.

Table 2. Proposed control message structure.

Message Type	READER_SENDER	READER_RECEIVER	READER_IN_CHAIN	AFFECT_FREQ	AFFECT_TS
REQUEST1	✓	-	✓	-	-
REQUEST2	✓	-	-	-	-
RESPONSE	✓	✓	-	-	-
ADD_TO_CHAIN	-	✓	-	✓	✓
NEW_CHAIN	-	✓	-	✓	✓

Upon receipt of an assignment request from a reader in the Rx coalition group, the reader compares the information in its control memory (Table 3) with the one in the request received in the control channel, to decide whether it will accept or deny deploying the FTDMA_Scheme and join the Rx set.

Table 3. Structure of the control memory table used.

USED_PROTOCOLUSED_PROTOCOL	READER_IN_CHAIN	AFFECT_FREQ	AFFECT_TS

3.2. The Description of the Proposed Algorithm FTSMAC

Before starting tag interrogation, all readers must know their suitable frequency resources to avoid RRI, and the time slot to avoid RTI. We allocate resources according to certain defined criteria. As illustrated in Figure 4, the reader waits for a backoff random time in the range with a step CW (Contention Window) [51] equal to the convergence time necessary for the readers to create the FTDMA_Scheme. We can therefore ensure that no other reader tries to send a request during the creation phase of the FTDMA_Scheme.

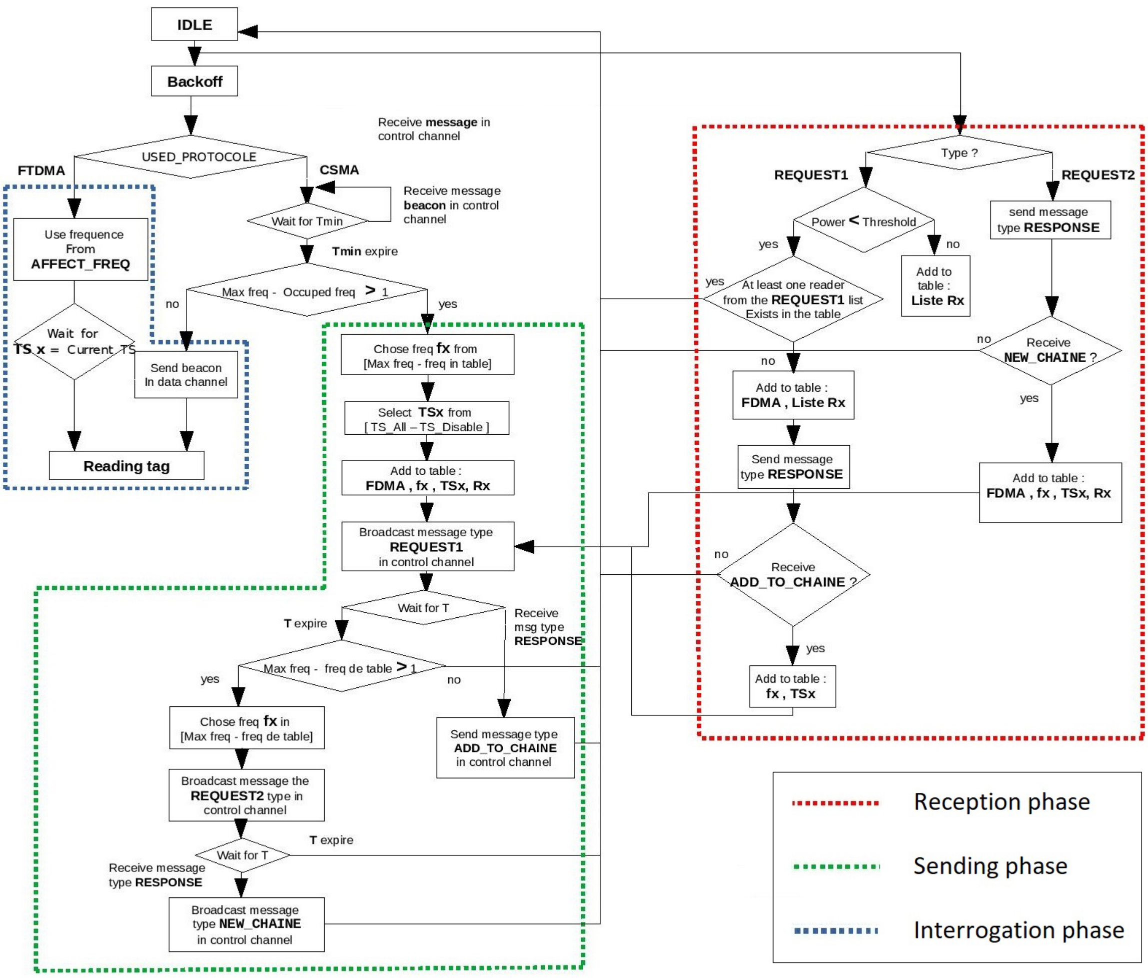

Figure 4. Proposed algorithm structure.

3.2.1. Interrogation Phase

After the Rx reader awakens, it starts by checking its memory table (Table 3). If the USED_PROTOCOL field contains FDMA, then it will execute the blue part of the algorithm; therefore it can use the frequency in the AFFECT_FREQ and time slot in the AFFECT_TS field to start tag interrogation.

Otherwise, the USED_PROTOCOL field has the value CSMA. In this case, the reader listens to the data channel for a Tmin time [52]. If Tmin expires without receiving a beacon, the reader starts using the free frequency.

3.2.2. Sending Phase

According to the previous phase, if there is only one frequency available for use, the reader Rx uses the CSMA protocol. However, if there are more frequencies, the reader performs the processing of the green part (Figure 4). Thus, the reader selects and adds a free frequency and time slot to its table using tag interrogation. It then replaces CSMA by FTDMA and finally registers its ID. This information represents the starting point of the first FTDMA_Scheme. The reader then searches (REQUEST1) and registers a new Neighbor-Reader Rj (Figure 3) in its FTDMA_Scheme using ADD_TO_CHAIN message.

If time expires without receiving any response, the reader broadcasts a REQUEST2 (to both neighbors' readers Rj and collision readers Ri) to search a reader that will initialize a new FTDMA_Scheme.

3.2.3. Reception Phase

If the reader receives a message (REQUEST1 or REQUEST2) during the backoff, it executes the red part of the algorithm (Figure 4). In the case of a REQUEST1 message, the reader compares the received signal power Pr with the threshold power (Threshold = Pr | di = cc), where Pr is the received signal power, di the distance between the two readers, and cc the radius of the data channel collision range. If Pr > Threshold, these readers are classified as collision readers Ri. Then the collision readers Ri registers the READER_IN_CHAIN message. Otherwise, the neighbor reader Rj checks if there is interference with the readers constituting the FTDMA_Scheme in progress.

However, the reader Rj performs the following actions: replace CSMA by FTDMA, update READER_IN_CHAIN field, and wait for resource allocation at the reception in an ADD_TO_CHAIN message.

In the second case, after receiving a REQUEST2 message, the reader sends a RESPONSE message to the sender Rx and leaves the IDLE state regardless of receiving anything. Otherwise, it receives a NEW_CHAIN message, replaces CSMA with FTDMA, and adds the new resources in its table to start creating the new FTDMA_Scheme.

3.3. *Illustrative Example*

To understand the operation of the FTSMAC algorithm, below we discuss a case of study of a random RFID network (Figure 5) and an illustration of the communication process between readers that constitute this network (Figure 6).

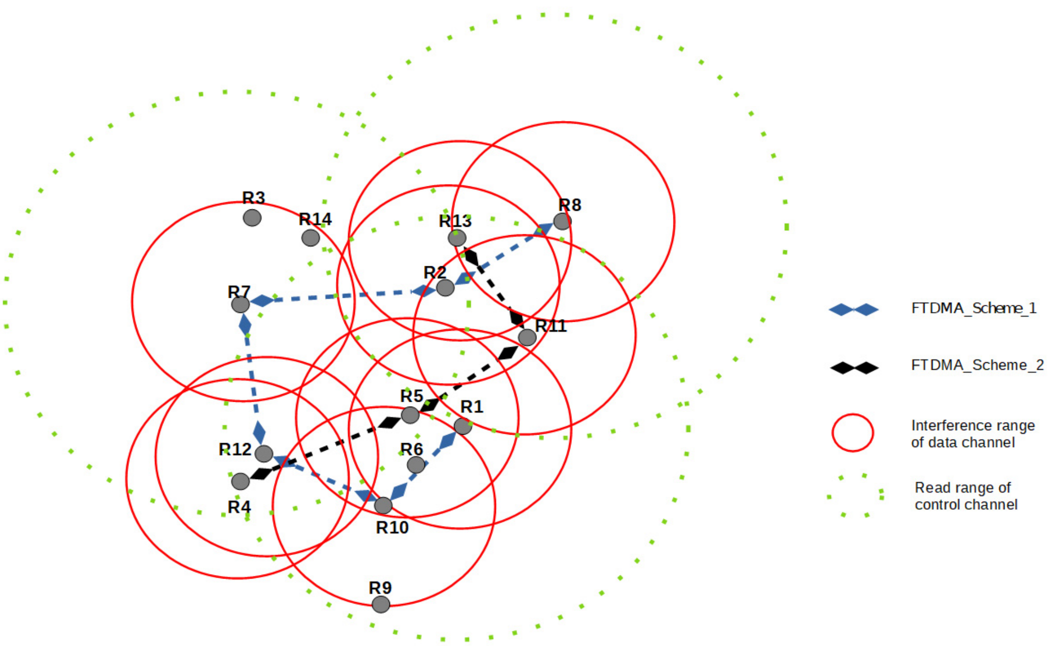

Figure 5. Application of the algorithm on an RFID network.

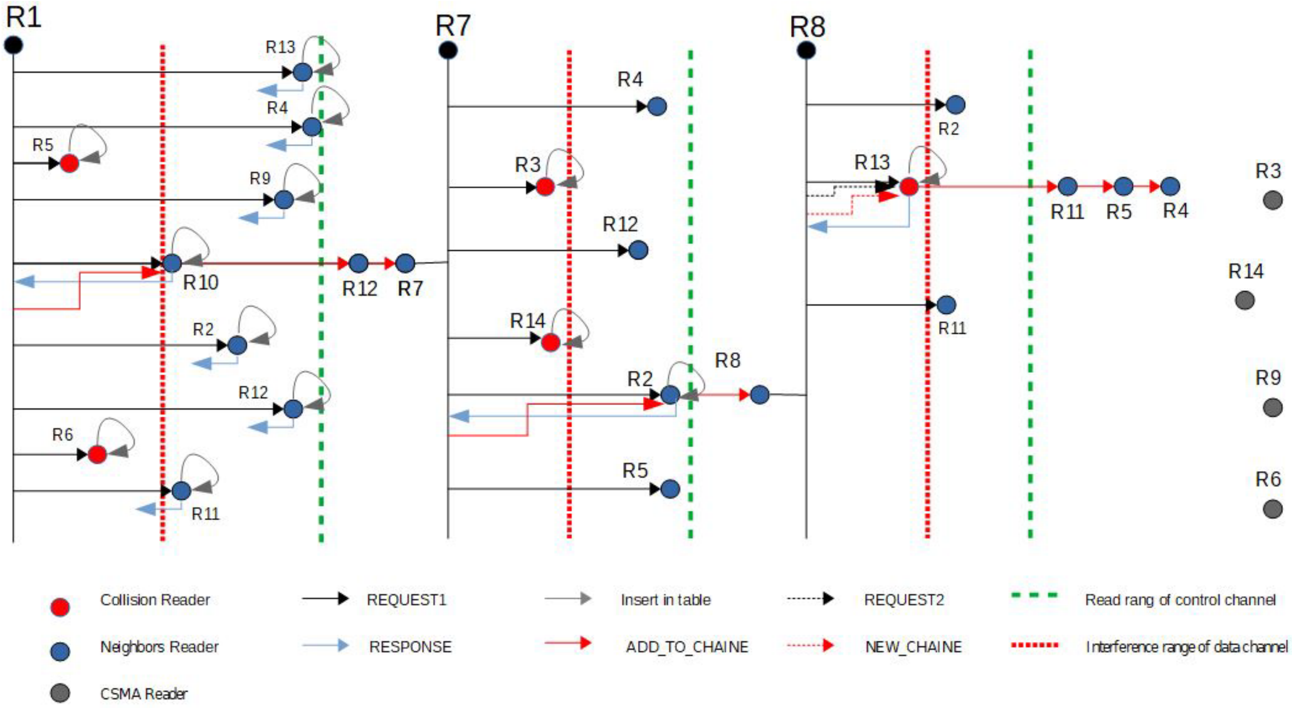

Figure 6. The process of creating FTDMA schemes.

Using our algorithm, we manage three frequencies and time slots. As a result, we can define FTDMA_Scheme_1 as the set of readers R1, R10, R12, R7, R2, and R8 using the first pair resource (freq1 and TS1). In addition, FTDMA_Scheme_2 is composed of R13, R11, R5, and R4, which use the second pair resource (freq2 and TS2). The readers that do not join the latter FTDMA_Scheme_2 must use the last frequency using CSMA.

Figure 6 describes the communication process used by the protocol in this example. We present the process of the algorithm for different situations of readers (R1, R2, R3, R8, R10, R13) in Appendix A.

First, all readers are in the backoff state. In this case, R1 (Rx) is the reader with the minimal backoff, and is therefore the first one to wake and start the FTDMA_Scheme creation process. Then, it broadcasts REQUEST1 on the control channel to announce its presence and ask neighbor readers (Rj blue readers) to reuse its resource (frequency and time slot). The readers receive requests and update their tables. The collision readers R5 and R6 (Ri red readers (Figure 3)) receive low threshold power. Therefore, they do not answer the request. Among the neighbor readers, R10 (Rj blue readers (Figure 3)) responds first to the R1 request. Therefore, it will be selected as a new neighbor, and confirms by sending an ADD_TO_CHAIN message. Then, R10 (new Rx) continues the process of creating the FTDMA_Scheme by adding R12 and R7.

According to the REQUEST1 of reader R7, R2 will be the new member of the current FTDMA_Scheme. The R3 and R14 readers do not respond to the REQUEST1 message because they are already in the interference range of R7. The reader R12 does not answer the request because it is a member of the current FTDMA_Scheme (AFFECT_FREQ = f1 and AFFECT_TS = TS1). The readers R4 and R5 do not respond to the request because they are colliding with the other readers of the current FTDMA_Scheme. Therefore, R7 accepts the request of R2.

Then, the reader R2 selects its neighbor R8 (Figure 6). R8 attempts to locate a neighbor but, in this case, cannot receive an answer after sending a REQUEST1 message because the reader's neighbors R2 and R11 determine that the field READER_IN_CHAIN of the received message contains reader IDs that already exist in their tables. Then, R8 sends a new REQUEST2 message to select the reader initiator for the new FTDMA_Scheme.

Because the R3 reader is closest, it answers first. Then R8 sends a NEW_CHAIN message to transfer the new resources to reader R13, which will start the next FTDMA_Scheme that will contain R11, R5, and R4.

Finally, only one frequency remains, which will be reserved for the readers R3, R6, R9, and R14 outside the collision domain. Following the suspension of their attempt to create the FTDMA_Scheme, these readers will switch to CSMA, based on the Listen Before Talking (LSB) principle.

4. Simulations and Results

In this section, we present the performance and results obtained by simulating the RFID network using our FTSMAC algorithm. In this simulation, we used the distributed-based anti-collision protocol PULSE, MCMAC, and CORA defined in Section 3 to compare our technique with existing approaches.

For this purpose, we used the MATLAB platform to simulate a wireless network using RFID communication technology, including RRI and RTI collision problems. Then, we simulated our algorithm and the protocols from the literature. Using MATLAB, we also developed the RFID reader and tag models. To communicate between the two entities, we simulated reader-to-reader and reader-to-tag communication.

The simulation parameters are presented in Table 4. The deployment of the readers was randomized in a space of 300 m × 300 m. All readers were uniform and used three data channels with a reading field of 3.5 m and an interference field of 8 m, and a control channel with a reading field of 16 m and an interference field of 30 m.

Table 4. Simulation parameters.

Parameter	Value
Simulation range	300 × 300 m
Number of readers (case 1)	10, 20, 30, 40, 50
Number of readers (case 2)	50
Simulation time (case 1)	300
Simulation time (case 2)	0, 50, 100, 150, 200, 250, 300
Number of tags (case 2)	20, 40, 60, 80, 100
Reader and Tag position	Random
Type of antenna	Omni-directional
Read range of data channel (rr)	3.5 m
Collision range of data channel (cr)	8 m
Read range of control channel (crr)	2 × cr
Collision range of control channel (crc)	30 m
Number of Data Channel (case 1)	3
Number of Data Channel (case 2)	1, 2, 3, 4, 5
Number of Time Slot (case 1)	3
Number of Time Slot (case 2)	1, 2, 3, 4, 5
Number of control channel	1
Number of samples for evaluation	10
protocols compared	PULSE, MCMAC
Backoff	(ReaderID-1) × CW
CW	Convergence time of all readers
Tmin	5 ms (Standard EPC)
T	Neighboring readers response time

In this study, four scenarios were defined. In the first scenario, the simulation was applied according to the number of readers (10, 20, 30, 40, 50), whereas the second was applied depending on the simulation duration (50, 100, 150, 200, 250, 300). The third scenario was applied depending on the number of tags (20, 40, 60, 80, 100). The final scenario was applied depending on the number of frequencies and TS (1, 2, 3, 4, 5). In these scenarios, we measured system performance and the number of active readers.

An anti-collision protocol should ensure a high number of successful readings in a collision environment, which is an important criterion for measuring protocol performance. We consider a successful interrogation if the reader receives the response from the query by the tags in the reading range.

We define the System Performance (Average Success Reading) as follows:

$$SystemPerformance(\%) = \frac{Total_{success} \times 100}{Total_{interrogation}} \quad (4)$$

where *Total_success* represents the number of successful reader-tag interrogations and *Total_interrogation* represents the total number of reader-tag interrogations.

Based on Figure 7, we note that the number of interrogation successes in our algorithm is higher. It exceeds 80% in the case of 50 readers because it allows a maximum number of readers to exploit the available frequency resources. MCMAC has a poorer performance because it manages individual resources, which makes it difficult to use the frequencies. Pulse protocol is the weakest among the remainder. We note the same result is achieved with CORA because it can manage only one data channel.

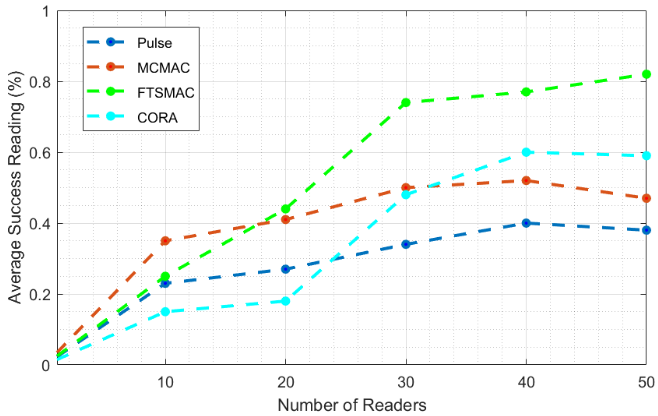

Figure 7. System performance vs. number of readers.

Figure 8 illustrates the average successful interrogation according to the variation of simulation time. Our protocol is faster because it does not use additional time to achieve a better result, and stabilizes at 82% of the reading efficiency of simulation times greater than 150, whereas MCMAC reaches 66%. Results for CORA and MAC are similar, but these approaches stabilize at 70%. Pulse requires more time to interrogate tags because only one data channel is shared by all readers in a collision domain.

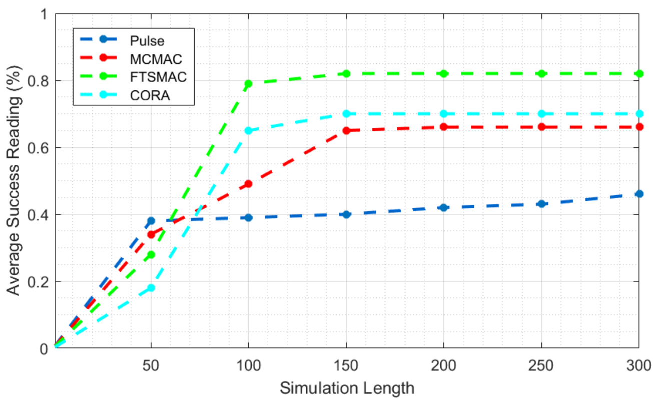

Figure 8. System performance vs. simulation length.

The parameter for active readers represents the number readers that achieve a successful tag interrogation. This is an important factor for the evaluation of the system performance.

To obtain the number of active readers in each simulation, we calculate the number of readers that can interrogate the tags without interfering with neighboring readers. In Figure 9, the evolution of the Pulse protocol does not exceed 10 active readers, whereas the other algorithms increase the number of active readers. In a network of more than 40 readers, MCMAC and CORA stop their evolution. In contrast, our proposal continues the evolution of the number of active readers and achieves better results because it allows the maximum number of readers in the network to obtain a frequency and avoid collisions by intelligently reusing the frequency schemes.

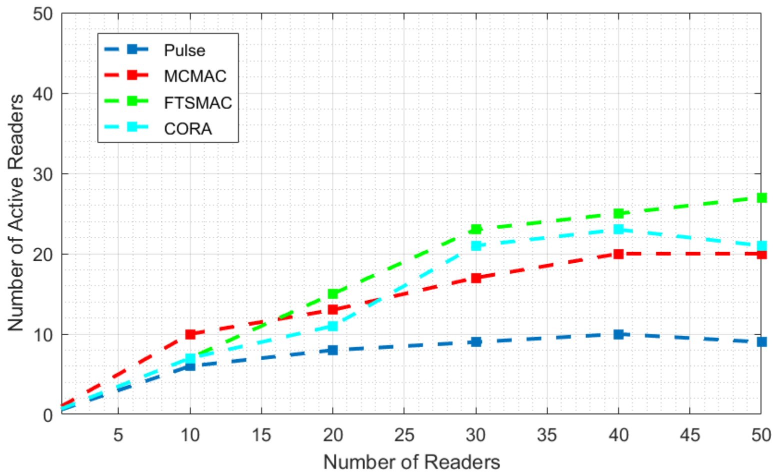

Figure 9. Number of active readers vs. number of readers.

Figure 10 illustrates the average of successful interrogation of the FSDMAC, CORA, MCMAC, and Pulse protocols in terms of the number of tags (20 to 100) read by 30 readers. The performance of Pulse is typically low because a single data channel does not allow successful interrogation. MCMAC and CORA reach around 60% performance, whereas our protocol exceeds 70%. The results illustrate that our protocol can read a higher range of tags. Therefore, in terms of the reading efficiency of tags, FSDMAC is more stable and more efficient compared to other protocols.

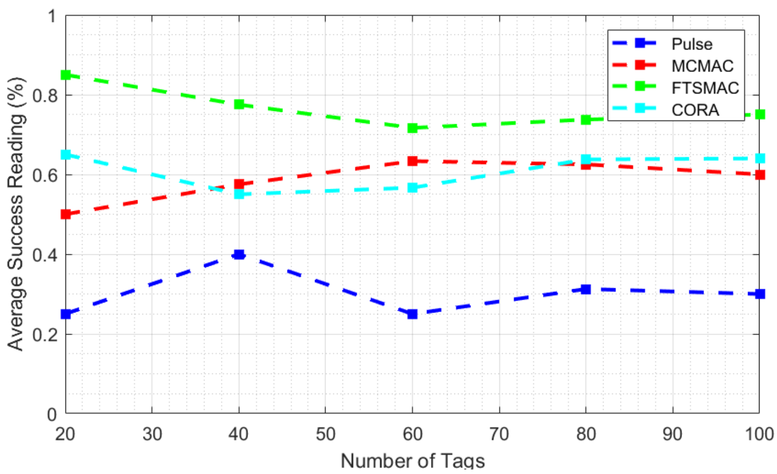

Figure 10. System performance vs. number of tags.

Figure 11 illustrates the evolution of the FSDMAC protocol as a function of the number of frequencies and time slot available for readers from 10 to 50. The principle of our approach is based on the generation of the FTDMA_scheme. The scheme uses the two pairs of frequency and time slot resources. The creation of these schemes allows a large set of readers to integrate into one of the schemes and obtain resources for tag interrogation. As shown in Figure 11, this allows the RFID network to use more resources to create more FTDMA_schemes, and therefore more active readers are able communicate without collision, thereby increasing system performance. Using a single frequency and TS achieved 42% of the system efficiency, whereas the increase in parameters, using five resources, increased the results to 88% of the system efficiency.

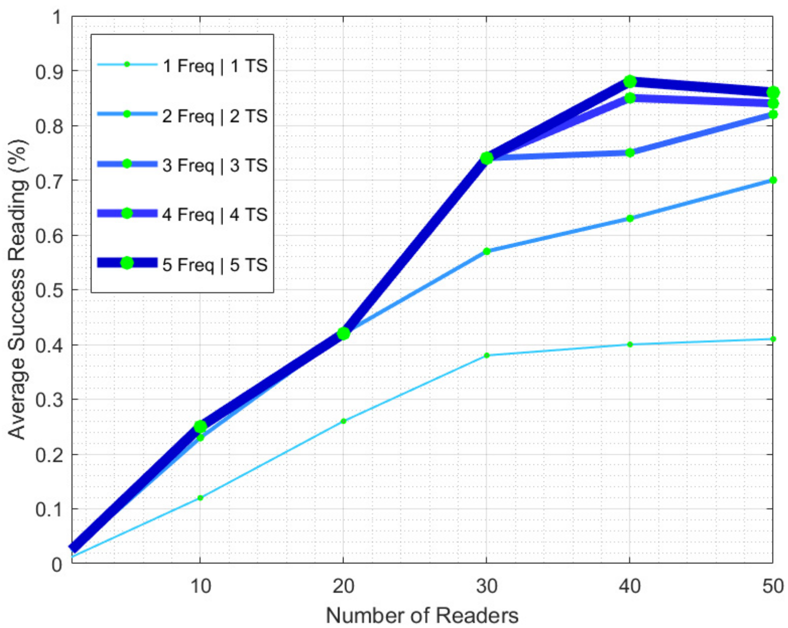

Figure 11. System performance vs. number of readers according to frequency and time slot.

The different technical contributions of this article that distinguish it from other solutions to achieve these results are as follows:

- A notification mechanism is used to exchange the frequency and temporary resource allocation packets through the control channel in a distributed mode by the readers to create the different FTDMA_Schemes.
- FTDMA_Scheme can include and activate a maximum number of readers to obtain available resources and interrogate the tags without collision.
- Use of a hybrid solution based on the MAC layer shared channel access methods: FDMA, TDMA, and CSMA.
- FDMA is used for permanent data channel allocation to readers to solve the RRI collision problem.
- TDMA is used for temporary allocation of the data channels to readers to solve the RRI collision problem. The number of TDMA periods is equal to the number of generated FTDMA_Schemes.
- CSMA is used by readers that do not belong to any FTDMA_Scheme to manage concurrent access to the backup data channel.
- Use of a backoff adapts the time of creation of the FTDMA_Scheme according to the number of readers to avoid control channel access collisions.

5. Conclusions and Future Work

In this paper, we proposed a robust protocol that avoids both RTI and RRI reader collisions in dense multi-channel RFID networks. This protocol is based on a notification system that distributes the resources using a FTDMA_Scheme.

For this purpose, the readers wait for a backoff random time to avoid collisions in the control channel. The reader with the minimum backoff wakes first and starts the FTDMA_Scheme creation process.

In the next step, the readers use the control channel to assign frequencies and time slots to the nearest readers outside the collision domain. Each reader that receives the control package memorizes both resources in its table and later begins the process of creating the FTDMA_Scheme.

The proposed approach involves all readers that receive notification on the control channel to create the FTDMA_Scheme. Therefore, the maximum number of readers can be reached using frequency and time slots as resources for tag interrogation.

To prove the effectiveness of our protocol, we used simulation to illustrate the ability of RFID readers to address reader-to-reader and reader-to-tag interference using this distributed strategy by increasing the reading efficiency and the number of active readers with a minimum of resources.

The advantage of our algorithm compared to other solutions is that it uses a new scheme-based resource distribution technique that allows efficient and faster allocation and management of resources to RFID readers.

The aim of our future work is to ensure the solution is complete and robust. Thus, we will adapt this method based on the frequency and time scheme to improve the performance of the FTDMA_Scheme by using a new algorithm that will improve the efficiency of the distribution of resources.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: R.M., A.A.M.; programming: R.M.; analysis and interpretation of results: R.M., M.O., A.A.M.; draft manuscript preparation: R.M., M.O.; reviewed the results and confirm the final version of the paper: R.M., M.O., A.A.M.; project administration: K.M.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

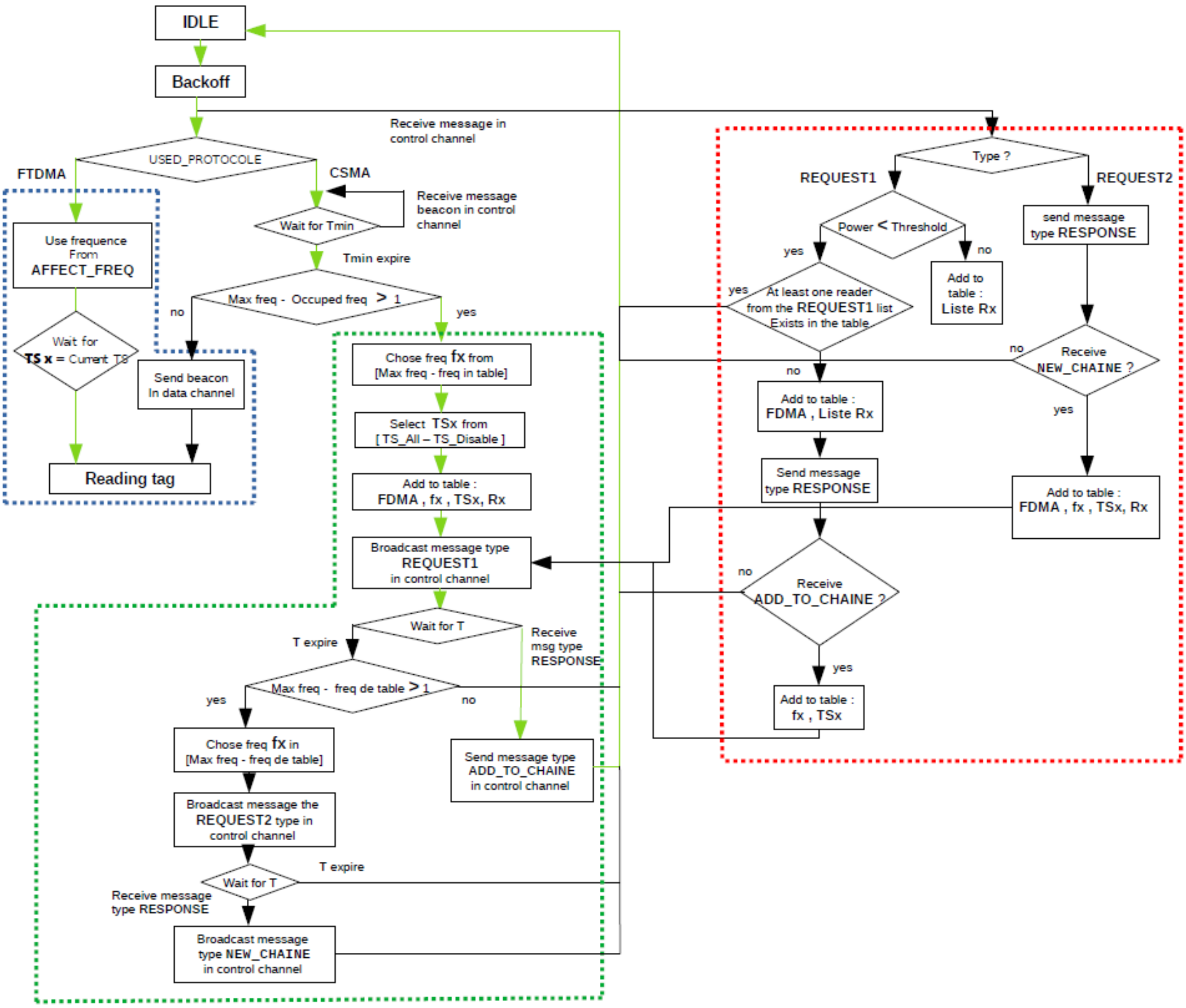

Figure A1. R1 process.

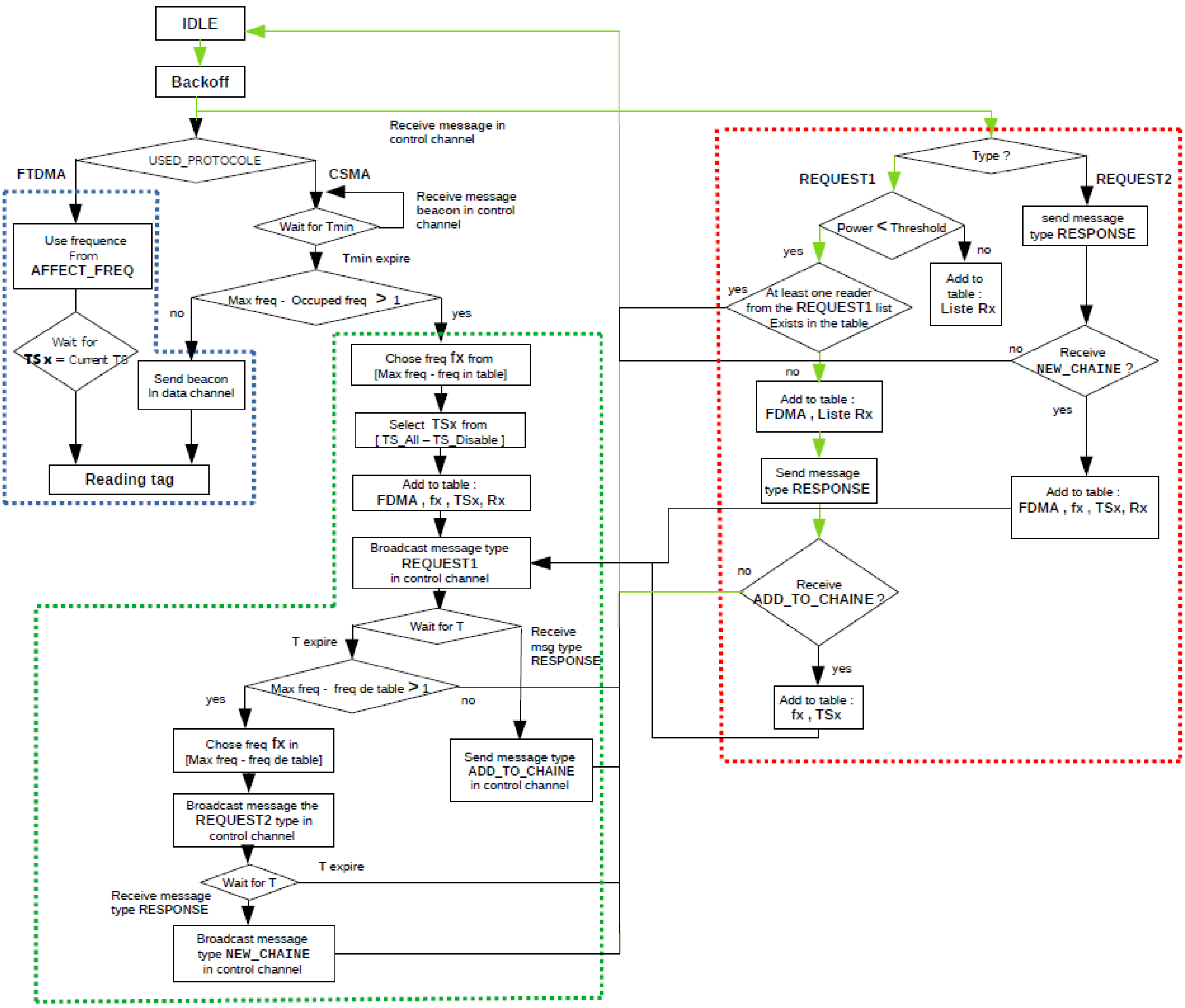

Figure A2. R2 process.

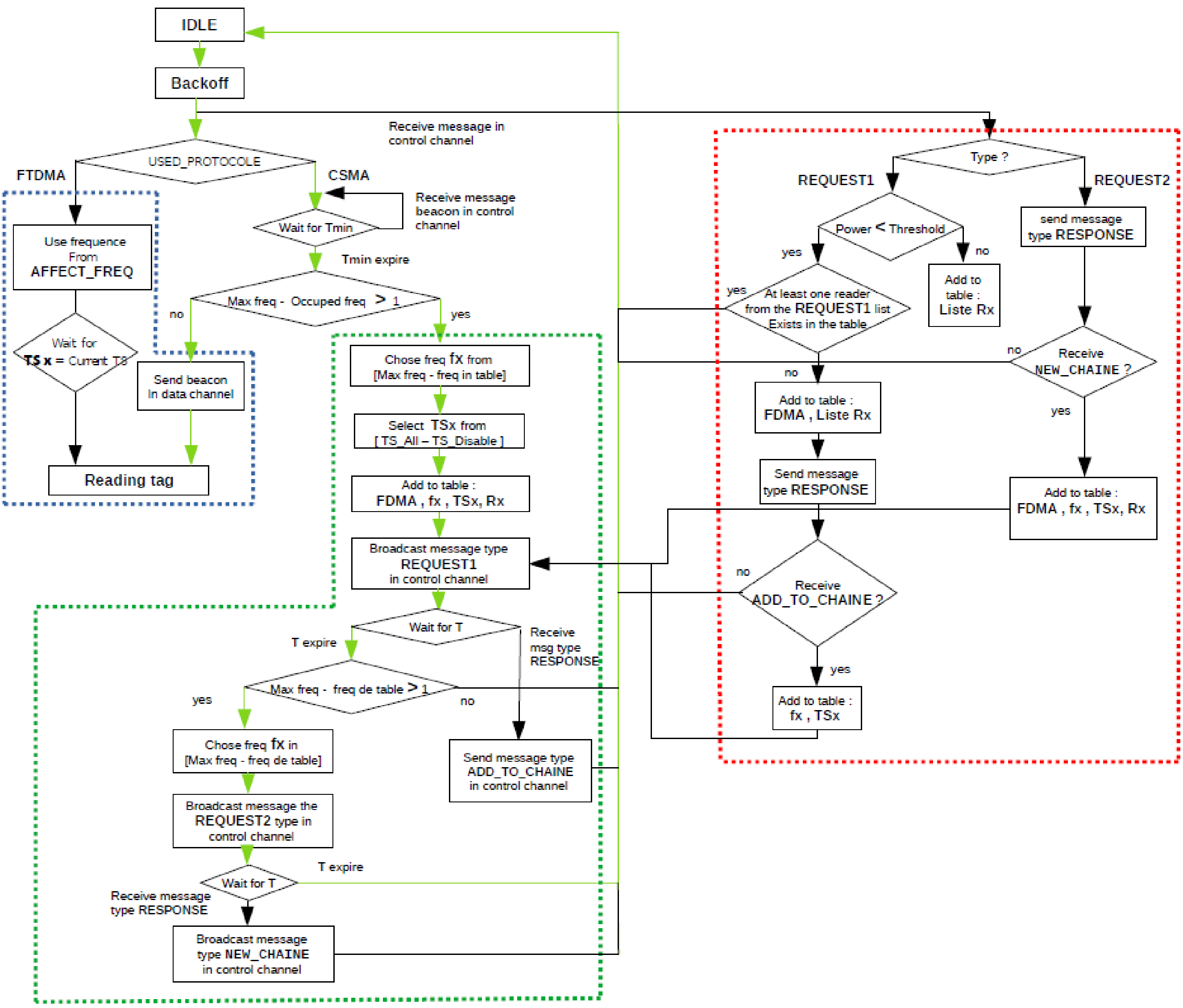

Figure A3. R3 process.

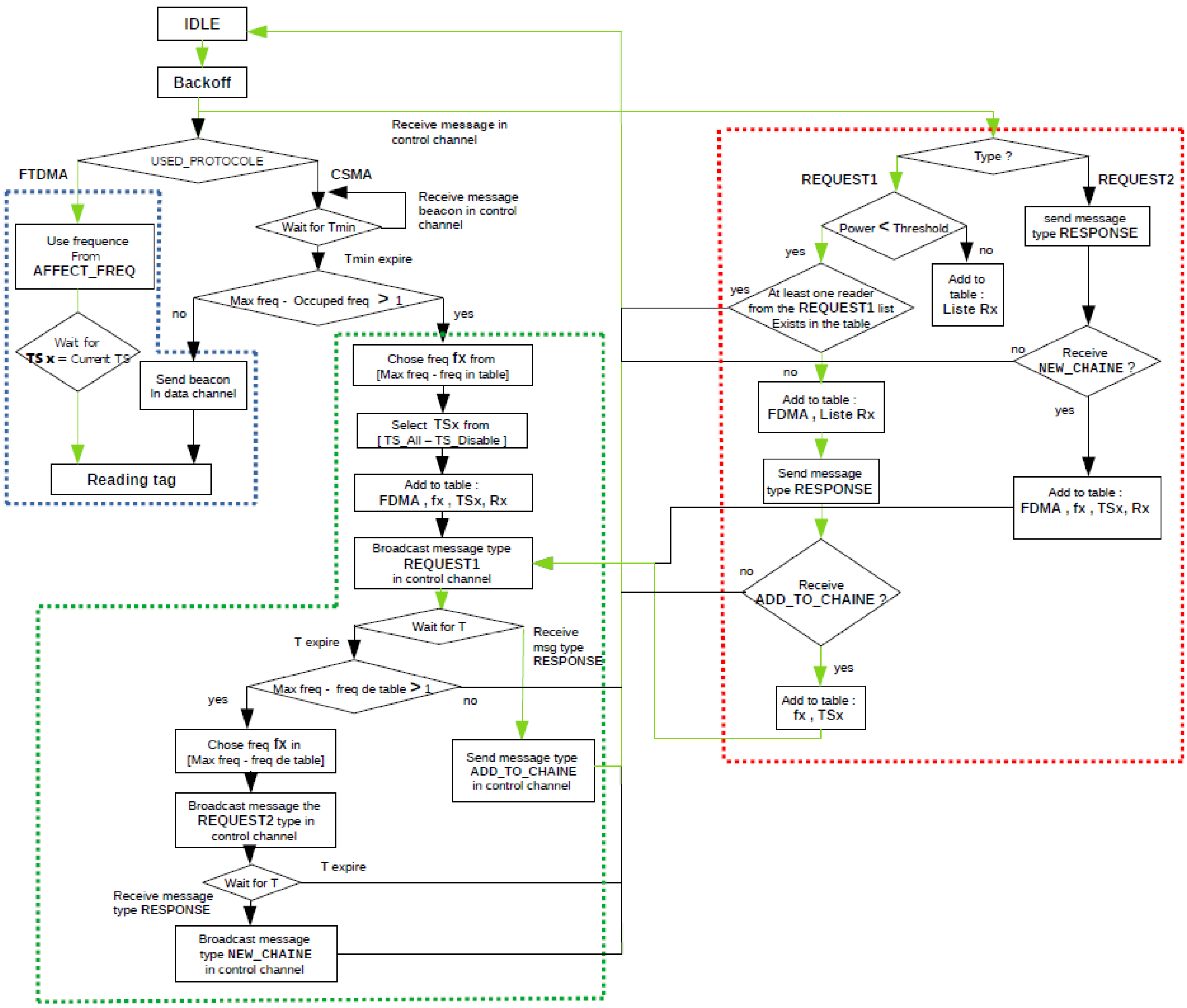

Figure A4. R10 process.

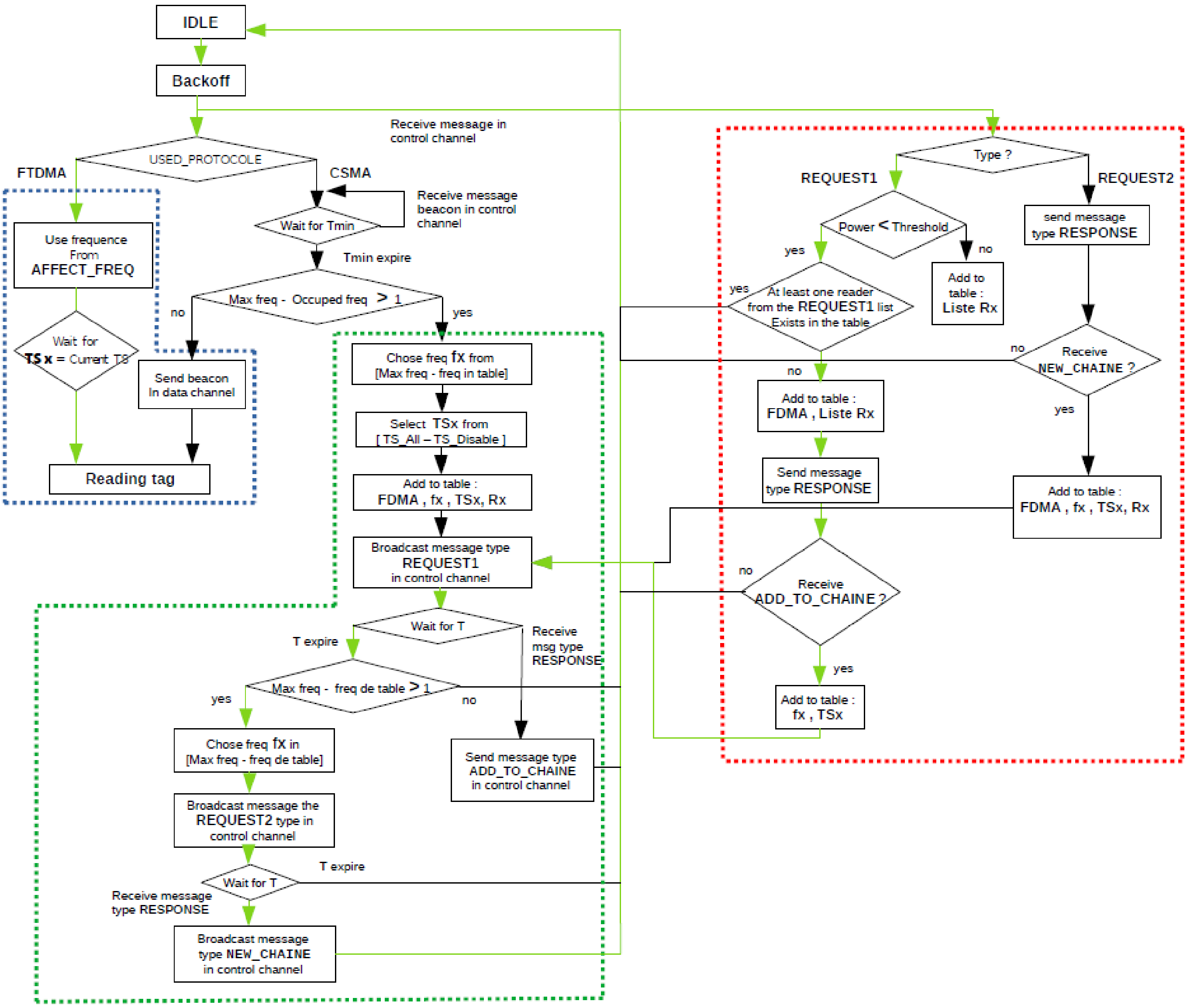

Figure A5. R8 process.

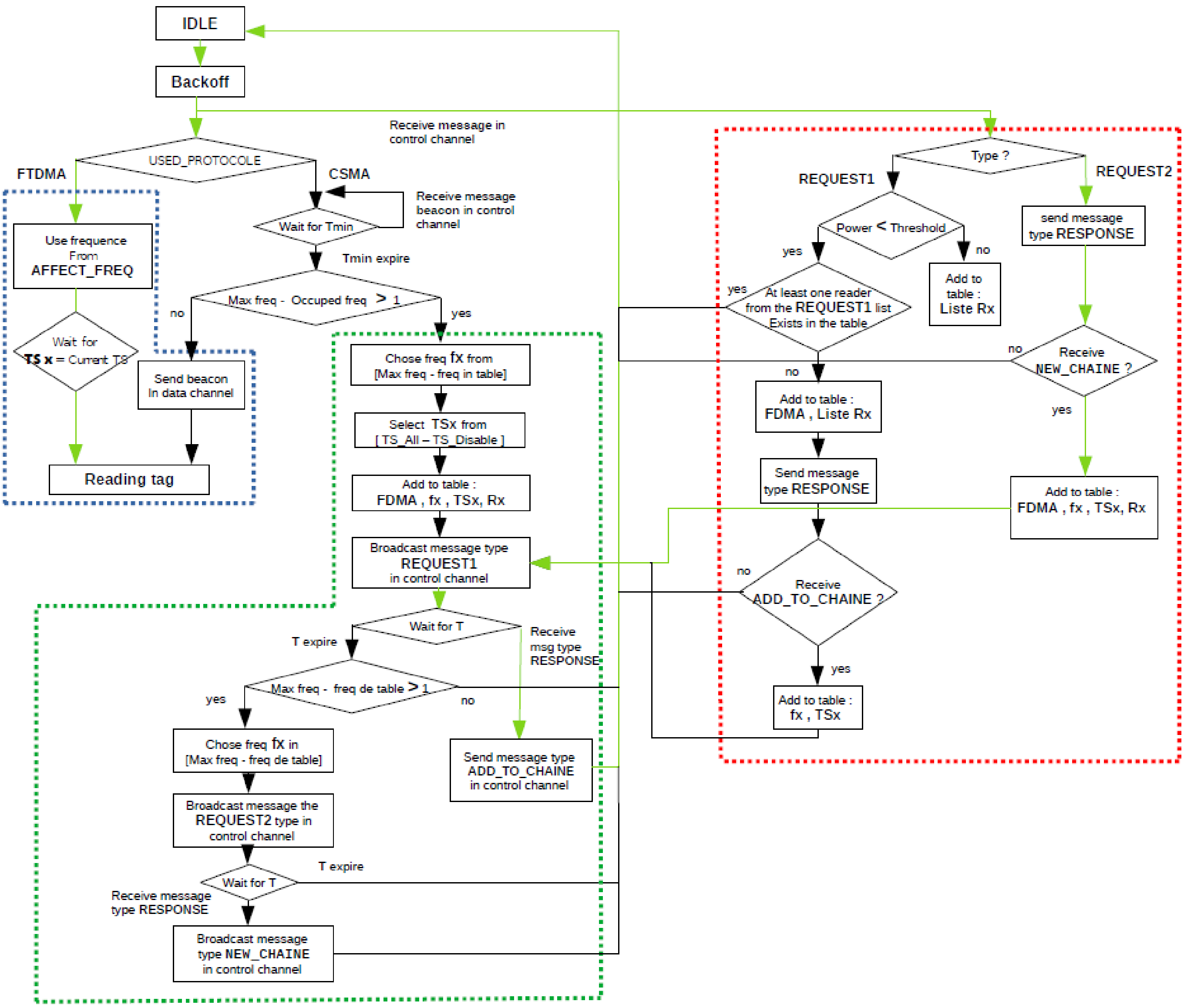

Figure A6. R13 process.

References

1. Juels, A. RFID security and privacy: A research survey. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 381–394. [CrossRef]
2. Ahson, S.A.; Ilyas, M. *RFID Handbook: Applications, Technology, Security, and Privacy*; CRC Press: Boca Raton, FL, USA, 2017.
3. Zhao, K.; Zhu, M.; Xiao, B.; Yang, X.; Gong, C.; Wu, J. Joint RFID and UWB Technologies in Intelligent Warehousing Management System. *IEEE Internet Things J.* **2020**, *72*, 11640–11655. [CrossRef]
4. Abuelkhail, A.; Baroudi, U.; Raad, M.; Sheltami, T. Internet of things for healthcare monitoring applications based on RFID clustering scheme. *Wirel. Netw.* **2021**, *27*, 747–763. [CrossRef]
5. Ma, Y.; Wang, B.; Pei, S.; Zhang, Y.; Zhang, S.; Yu, J. An indoor localization method based on AOA and PDOA using virtual stations in multipath and NLOS environments for passive UHF RFID. *IEEE Access* **2018**, *6*, 31772–31782. [CrossRef]
6. Musa, A.; Dabo, A.A.A. A review of RFID in supply chain management: 2000–2015. *Glob. J. Flex. Syst. Manag.* **2016**, *17*, 189–228. [CrossRef]
7. Al Ajrawi, S.; Bialek, H.; Sarkar, M.; Rao, R.; Ahmed, S.H. Bi-directional channel modeling for implantable UHF–RFID transceivers in brain–computer interface applications. *Future Gener. Comput. Syst.* **2018**, *88*, 683–692. [CrossRef]
8. Jyothi, P.M.S.; Nandan, D. Utilization of the Internet of Things in Agriculture: Possibilities and Challenges. In *Soft Computing: Theories and Applications*; Springer: Singapore, 2020; pp. 837–848.
9. Pal, A.; Kant, K. Internet of perishable logistics: Building smart fresh food supply chain networks. *IEEE Access* **2019**, *7*, 17675–17695. [CrossRef]

10. Shousong, C.; Xiaoguang, W.; Yuanjun, Z. Revenue model of supply chain by internet of things technology. *IEEE Access* **2018**, *7*, 4091–4100. [CrossRef]
11. Sidorov, M.; Ong, M.T.; Sridharan, R.V.; Nakamura, J.; Ohmura, R.; Khor, J.H. Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains. *IEEE Access* **2019**, *7*, 7273–7285. [CrossRef]
12. Tao, Q.; Gu, C.; Wang, Z.; Rocchio, J.; Hu, W.; Yu, X. Big data driven agricultural products supply chain management: A trustworthy scheduling optimization approach. *IEEE Access* **2018**, *6*, 49990–50002. [CrossRef]
13. Jiang, W. An intelligent supply chain information collaboration model based on Internet of Things and Big Data. *IEEE Access* **2019**, *7*, 58324–58335. [CrossRef]
14. Li, C.; Mo, L.; Zhang, D. Review on UHF RFID Localization methods. *IEEE J. Radio Freq. Identif.* **2019**, *3*, 205–215. [CrossRef]
15. Hamid, S.A.; Ismail, W.; Zulkifli, C.Z.; Abdullah, S. Dual Band RFID-Based Blood Glucose Monitoring System in Wireless Sensor Network Platform. *Wirel. Pers. Commun.* **2018**, *103*, 2229–2244. [CrossRef]
16. Ferrero, R. Evaluation of Throughput of TDMA Anti-Collision Protocols in Static and Mobile RFID Networks. In Proceedings of the 2019 4th International Conference on Smart and Sustainable Technologies, Split, Croatia, 18–21 June 2019; pp. 1–7.
17. Golsorkhtabaramiri, M.; Issazadehkojidi, N.; Pouresfehani, N.; Mohammadialamoti, M.; Hosseinzadehsadati, S.M. Comparison of energy consumption for reader anti-collision protocols in dense RFID networks. *Wirel. Netw.* **2019**, *25*, 2393–2406. [CrossRef]
18. Landaluce, H.; Arjona, L.; Perallos, A.; Falcone, F.; Angulo, I.; Muralter, F. A review of iot sensing applications and challenges using RFID and wireless sensor networks. *Sensors* **2020**, *20*, 2495. [CrossRef]
19. Ji, W.; Li, L.; Zhou, W. Design and implementation of a RFID reader/router in RFID-WSN hybrid system. *Future Internet* **2018**, *10*, 106. [CrossRef]
20. Sobral, J.V.; Rodrigues, J.J.; Rabelo, R.A.; Lima Filho, J.C.; Sousa, N.; Araujo, H.S.; Holanda Filho, R. A framework for enhancing the performance of Internet of Things applications based on RFID and WSNs. *J. Netw. Comput. Appl.* **2018**, *107*, 56–68. [CrossRef]
21. Adame, T.; Bel, A.; Carreras, A.; Melia-Segui, J.; Oliver, M.; Pous, R. CUIDATS: An RFID–WSN hybrid monitoring system for smart health care environments. *Future Gener. Comput. Syst.* **2018**, *78*, 602–615. [CrossRef]
22. Alfian, G.; Rhee, J.; Ahn, H.; Lee, J.; Farooq, U.; Ijaz, M.F.; Syaekhoni, M.A. Integration of RFID, wireless sensor networks, and data mining in an e-pedigree food traceability system. *J. Food Eng.* **2017**, *212*, 65–75. [CrossRef]
23. Deng, R.; He, S.; Cheng, P.; Sun, Y. Towards balanced energy charging and transmission collision in wireless rechargeable sensor networks. *J. Commun. Netw.* **2017**, *19*, 341–350. [CrossRef]
24. Luo, Z.; Jing, C.; Chen, Y.; Xiong, X. A new underdetermined NMF based anti-collision algorithm for RFID systems. *ISA Trans.* **2021**. [CrossRef]
25. Li, Z.; He, G.; Xu, D.; Wang, S. Evaluation of Centralized Reader Anti-Collision Protocols for Mobile RFID System Based on Maximum Independent Set: A Simulation Study. *IEEE Access* **2020**, *8*, 123381–123397. [CrossRef]
26. Xuan, X.; Li, K. Efficient Anti-collision Algorithm for RFID EPC Generation-2 Protocol Based on Continuous Detection. *Int. J. Wirel. Inf. Netw.* **2020**, *27*, 133–143. [CrossRef]
27. Cao, B.; Gu, Y.; Lv, Z.; Yang, S.; Zhao, J.; Li, Y. RFID Reader Anti-Collision Based on Distributed Parallel Particle Swarm Optimization. *IEEE Internet Things J.* **2020**. [CrossRef]
28. Kumar, A.; Aggarwal, A.; Gopal, K. A novel and efficient reader-to-reader and tag-to-tag anti-collision protocol. *IETE J. Res.* **2018**, 1–12. [CrossRef]
29. Deng, W.; Li, Z.; Xia, Y.; Wang, K.; Pei, W. A widely linear MMSE anti-collision method for multi-antenna RFID readers. *IEEE Commun. Lett.* **2019**, *23*, 644–647. [CrossRef]
30. Rezaie, H.; Golsorkhtabaramiri, M. A fair reader collision avoidance protocol for RFID dense reader environments. *Wirel. Netw.* **2018**, *24*, 1953–1964. [CrossRef]
31. Chuang, P.J.; Tsai, W.T. SwitchTable: An efficient anti-collision algorithm for RFID networks. *Iet Commun.* **2017**, *11*, 2221–2227. [CrossRef]
32. Su, J.; Sheng, Z.; Xie, L. A collision-tolerant-based anti-collision algorithm for large scale RFID system. *IEEE Commun. Lett.* **2017**, *21*, 1517–1520. [CrossRef]
33. Wang, X.; Yang, L.T.; Li, H.; Lin, M.; Han, J.; Apduhan, B.O. NQA: A nested anti-collision algorithm for RFID systems. *ACM Trans. Embed. Comput. Syst.* **2019**. [CrossRef]
34. Abbasian, A.; Safkhani, M. CNCAA: A new anti-collision algorithm using both collided and non-collided parts of information. *Comput. Netw.* **2020**, *172*, 107159. [CrossRef]
35. Zhou, W.; Jiang, N. Research on hybrid of ALOHA and multi-fork tree Anti-collision algorithm for RFID. *Procedia Comput. Sci.* **2021**, *183*, 389–394. [CrossRef]
36. Saia, R.; Carta, S.; Recupero, D.R.; Fenu, G. Internet of Entities (IoE): A Blockchain-based Distributed Paradigm for Data Exchange between Wireless-based Devices. In Proceedings of the 8th International Conference on Sensor Networks, Prague, Czech Republic, 26–27 February 2019; pp. 77–84.
37. Liu, B.; Su, X. An anti-collision algorithm for rfid based on an array and encoding scheme. *Information* **2018**, *9*, 63.
38. Safa, H.; El-Hajj, W.; Meguerditchian, C.; Safa, H.; El-Hajj, W.; Meguerditchian, C. A distributed multi-channel reader anti-collision algorithm for RFID environments. *Comput. Commun.* **2015**, *64*, 44–56. [CrossRef]
39. Mbacke, A.A.; Mitton, N.; Rivano, H. A survey of RFID readers anticollision protocols. *IEEE J. Radio Freq. Identif.* **2018**, *2*, 38–48. [CrossRef]

40. Birari, S.M.; Iyer, S. PULSE: A MAC protocol for RFID networks. In Proceedings of the International Conference on Embedded and Ubiquitous Computing; Springer: Berlin/Heidelberg, Germany, 2005; pp. 1036–1046. [CrossRef]
41. Aziz, M.A.; Mitton, N.; Rivano, H. Rfid reader anticollision protocols for dense and mobile deployments. *Electronics* **2016**, *5*, 84.
42. Olaleye, O.G.; Ali, A.; Perkins, D.; Bayoumi, M. Modeling and performance simulation of PULSE and MCMAC protocols in RFID-based IoT network using OMNeT++. In Proceedings of the 2018 IEEE International Conference on RFID, Orlando, FL, USA, 10–12 April 2018; pp. 1–5.
43. Golsorkhtabaramiri, M.; Issazadehkojidi, N. A distance based RFID reader collision avoidance protocol for dense reader environments. *Wirel. Pers. Commun.* **2017**, *95*, 1781–1798. [CrossRef]
44. Bueno-Delgado, M.V.; Ferrero, R.; Gandino, F.; Pavon-Marino, P.; Rebaudengo, M. A geometric distribution reader anti-collision protocol for RFID dense reader environments. *IEEE Trans. Autom. Sci. Eng.* **2012**, *10*, 296–306. [CrossRef]
45. Assarian, A.; Khademzadeh, A.; HosseinZadeh, M.; Setayeshi, S. A beacon analysis-based RFID reader anti-collision protocol for dense reader environments. *Comput. Commun.* **2018**, *128*, 18–34. [CrossRef]
46. Li, Z.; He, G.; Wang, S. NFRA-AIC: A RFID reader anti-collision protocol with adaptive interrogation capacity. *IEEE Access* **2019**, *7*, 86493–86509. [CrossRef]
47. Eom, J.B.; Yim, S.B.; Lee, T.J. An efcient reader anticollision algorithm in dense RFID networks with mobile RFID readers. *IEEE Trans. Ind. Electron.* **2009**, *56*, 23262336.
48. Liu, B.H.; Nguyen, N.T.; Pham, V.T.; Yeh, Y.H. A maximum-weight-independent-set-based algorithm for reader-coverage collision avoidance arrangement in RFID networks. *IEEE Sens. J.* **2015**, *16*, 1342–1350. [CrossRef]
49. Meddeb, A.; Jaballah, A. Algorithm for readers arrangement without collision in RFID networks. In Proceedings of the 2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), Taipei, Taiwan, 18–20 December 2017; pp. 316–321.
50. Yan, P.; Choudhury, S.; Wei, R. A machine learning auxiliary approach for the distributed dense RFID readers arrangement algorithm. *IEEE Access* **2020**, *8*, 42270–42284. [CrossRef]
51. Golsorkhtabaramiri, M.; Hosseinzadeh, M.; Reshadi, M.; Rahmani, A.M. A reader anti-collision protocol for RFID-enhanced wireless sensor networks. *Wirel. Pers. Commun.* **2015**, *81*, 893–905. [CrossRef]
52. Finkenzeller, K. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*; John Wiley & Sons: Hoboken, NJ, USA, 2010.