UNIVERSIDAD AUTÓNOMA METROPOLITANA
UNIDAD IZTAPALAPA División de Ciencias Básicas e Ingeniería.

Estimación de marcas en redes RFID

Tesis que presenta:

Leonardo Daniel Sánchez Martínez

Para obtener el grado de:

Maestro en Ciencias en Tecnologías de la Información

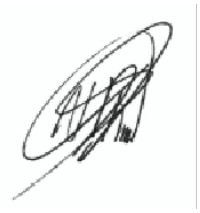
En el área : Redes y Telecomunicaciones
del Departamento de Ingeniería Eléctrica

Asesor:

Dr. Víctor Manuel Ramos Ramos.

Defendida públicamente en la UAM-Iztapalapa el 2 de agosto de 2011 a las 09:00 hrs
frente al jurado integrado por :

Presidente :	Dr. Ricardo Marcelín Jiménez UAM-I, Redes y Telecomunicaciones
Secretario :	Dr. Víctor Manuel Ramos Ramos UAM-I, Redes y Telecomunicaciones
Vocal :	Dr. Marcelo Carlos Mejía Olvera ITAM, Depto. Acad. de Computación



RESUMEN

Actualmente RFID es una tecnología utilizada dentro de diversas áreas. El gran atractivo de RFID es la capacidad de identificar objetos de manera inalámbrica sin necesidad de contacto o línea de visión entre los dispositivos participantes. Debido al gran impacto de la tecnología RFID, es necesario que ésta cuente con mecanismos que mejoren su funcionamiento y optimicen su rendimiento.

La tecnología RFID afronta grandes retos, tales como la resolución de colisiones, el ahorro de energía, la seguridad, etc. Una mejora dentro de cualquiera de estos campos implica invariablemente una mejora en el desempeño y funcionamiento de esta tecnología, que a su vez se puede traducir en la apertura de nuevas aplicaciones que utilicen tecnología RFID.

En esta tesis de maestría nos enfocamos a resolver uno de los problemas principales que atañen a las redes RFID: las **colisiones entre marcas**. Este problema es uno de los más importantes que se presentan dentro de las redes RFID, ya que no solamente se pierde la información transmitida por las marcas, sino que además se desperdicia el ancho de banda, la energía, y se incrementa el retardo de identificación, siendo este último una de las medidas de desempeño más significativas en este tipo de redes.

A lo largo de este documento presentamos una breve descripción de los fundamentos de las redes RFID, componentes principales, descripción de los dispositivos participantes, etc., detallamos el problema de colisiones entre marcas, así como el contexto bajo el cual se presenta. De igual forma, presentamos una revisión de los protocolos anticolisión más representativos presentados hasta el momento para redes RFID, y discutimos las ventajas y desventajas que ofrecen.

En base al estudio realizado, en este trabajo proponemos un protocolo anticolisión basado en CSMA p-persistente, el cual muestra mejores resultados con respecto a los estándares utilizados dentro de los entornos RFID activos, y algunas propuestas presentadas previamente en la literatura. Evaluamos nuestra propuesta en base al retardo de identificación, buscando obtener resultados confiables y válidos.

Finalmente, concluimos discutiendo los resultados obtenidos, las implicaciones de estos y el trabajo a futuro que realizaremos en diferentes extensiones de este trabajo.

ABSTRACT

Nowadays, RFID is a technology widely used in several areas. The attractiveness of RFID is the ability to identify objects without contact or a direct sight line between the devices involved. Due to its large impact, it is necessary that the RFID technology accounts with mechanisms that improve its functionality while at the same time, optimizing its performance.

The RFID technology has great challenges, such as collision resolution, energy saving, security, etc. An improvement in any of these fields invariably involves an improvement in performance and operation of this technology, which in turn can translate into the opening of new applications using technology RFID.

In this master's thesis we focus on solving one of the main problems concerning RFID networks: **tags collisions**. This problem is one of the most important in RFID networks, since besides the loss of information sent by the tags, there is also a waste of bandwidth and energy, which causes an increase of identification delay, being the latter one of the most important performance metrics in such networks.

Throughout this master's thesis, we present an overview of the fundamentals of RFID networks, their principal components, a description of the participating devices, etc. We then detail the problem of tag collisions and the context in which they occur. Similarly, we present a review of several anticollision protocols that have been proposed so far in the literature for RFID networks, and finally we discuss the advantages and disadvantages they offer.

Based on our study, we propose an anticollision protocol based on p-persistent CSMA, which overperforms the existing standards for RFID used and a couple of recent proposals in the literature. We evaluate our proposal based on identification delay obtaining reliable and valid results.

We conclude our work by discussing the results, and describing our future work on RFID systems.

AGRADECIMIENTOS

Antes que nada, dar gracias a Dios por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a las personas correctas durante todo el periodo de estudio.

Agradecer hoy y siempre a mi familia, ya que ellos son el mayor soporte en mi vida. A mis padres, Leonardo y Ma. Dolores, que siempre han estado a mi lado y me han apoyado, aún cuando mi estado de ánimo no fue el mejor. A mi hermana Nayeli, quien me ha dado grandes lecciones de vida. A mi esposa Jessica por su gran apoyo, paciencia, tolerancia, comprensión, sabiduría, conocimientos y ánimo. Es pieza fundamental en mi vida, y le estoy sumamente agradecido por estar a mi lado.

Al Dr. Víctor Manuel Ramos Ramos, por sus sabios consejos y palabras, los cuales no solamente me ayudaron a llevar a cabo este proyecto, sino que me ayudan a llevar mi vida día a día. De igual forma, le agradezco por haberme aceptado como su alumno de proyecto, debido a que es un honor trabajar a su lado. Extiendo mi agradecimiento a todos lo profesores del PCyTI, quienes con sus enseñanzas me ayudaron a la realización de este proyecto. Extiendo mi gratitud a mis compañeros y amigos del PCyTI, por su apoyo, ánimos, conocimientos e ideas que surgieron en cada etapa que se pasa durante este largo recorrido.

En general, quiero agradecer a todas y cada una de las personas que han vivido conmigo la realización de este trabajo con sus altos y bajos, y que no necesito nombrar, porque tanto ellas como yo sabemos que desde lo más profundo de mi corazón les agradezco el apoyo, colaboración, y ánimo brindado, y sobre todo su cariño y su amistad.

A la Universidad Autónoma Metropolitana por darme la oportunidad de desarrollarme académica y personalmente. Al Consejo Nacional de Ciencia y Tecnología, por el apoyo económico que me otorgó para la realización de esta maestría, sin el cuál habría sido muy difícil llegar a buen término.

Agradezco igualmente, al Dr. Ricardo Marcelín Jiménez y al Dr. Marcelo Carlos Mejía Olvera por hacerme el honor de formar parte del jurado revisor y calificador para la defensa pública de este trabajo.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

ACRÓNIMOS

RFID: Identificación por radio frecuencia (*Radio Frequency IDentification*).

MAC: Control de Acceso al Medio.

SDMA: Acceso Múltiple por División de Espacio (*Space Division Multiple Access*).

FDMA: Acceso Múltiple por División de Frecuencia (*Frequency Division Multiple Access*).

CDMA: Acceso Múltiple por División de Código (*Code Division Multiple Access*).

TDMA: Acceso Múltiple por División de Tiempo (*Time Division Multiple Access*).

CSMA: Acceso Múltiple por Detección de Portadora (*Carrier Sense Multiple Access*).

PA: ALOHA Puro.

SA: ALOHA Ranurado (*Slotted ALOHA*)

FSA ALOHA Ranurado en Tramas (*Framed Slotted ALOHA*)

BFSA ALOHA Ranurado en Tramas Básico (*Basic Framed Slotted ALOHA*)

DFSA ALOHA Ranurado en Tramas Dinámico (*Dynamic Framed Slotted ALOHA*)

TS: División de Árbol (*Tree Splitting*).

BTS: División Básica de Árbol (*Basic Tree Splitting*).

ABTS: División Adaptativa de Árbol Binario (ABTS) (*Adaptive Binary Tree Splitting*).

QT: Árbol de Consulta (*Query Tree*).

ACK: Acuse de recibo (*ACKNOWLEDGEMENT*).

CI: Ciclo de Identificación (*Identification Cycle*).

ID: Identificador único.

BD: Base de Datos

CAPÍTULO 1

INTRODUCCIÓN

Hoy día, la Identificación por Radio Frecuencia (*Radio Frequency IDentification* o RFID) es una de las tecnologías más incidentes dentro de diversas áreas de la industria. Esto se debe, a que la tecnología RFID tiene la capacidad de identificar objetos de manera inalámbrica, sin necesidad de contacto o línea de visión entre los dispositivos participantes, a diferencia del código de barras.

Según [1], para el año 2005 se habían producido 1.3 billones de marcas RFID, y se estima que para el año 2010 la cantidad de marcas producidas aumentó aproximadamente, a unos 33 billones de marcas RFID.

Algunas de las ventajas que ofrece RFID frente al código de barras son:

- Lectura/Escritura de datos.
- Identificación simultánea de objetos.
- Eliminación de la limitación impuesta por la línea de visión.
- Seguridad con respecto a la unicidad del identificador asociado, debido al modo en que son manufacturados.

A continuación presentamos los fundamentos relacionados con un sistema RFID, tales como los dispositivos participantes y sus funciones principales.

1.1. Fundamentos

Un sistema RFID se constituye de tres componentes: marcas RFID, uno o más lectores RFID, y un sistema terminal o *software* de procesamiento (comúnmente llamado *middleware*), el cual es el encargado de enlazar los lectores RFID a una base de datos (BD) centralizada, en

la que se almacena la información relacionada a los objetos a los que se encuentran adjuntas las marcas RFID.

Una red RFID forma parte de una sistema RFID, y no son lo mismo. Las redes RFID están conformadas por 2 diferentes tipos de dispositivos, los cuales se comunican de forma inalámbrica y conforman una red [17]:

- **Lectores:** Son dispositivos de lectura, típicamente potentes que cuentan con una considerable capacidad de almacenamiento y poder de procesamiento. Cada lector tiene un área de cobertura o zona de interrogación, que depende de las características físicas de este tipo de dispositivos. Su función principal es identificar todas las marcas que se encuentran dentro de su área de cobertura, por lo que en una red RFID puede haber más de un lector [1]. Existen lectores para redes con marcas pasivas y para redes con marcas activas.

- **Marcas:** Las marcas son la base sobre las que se construyen las redes RFID. Son "pequeños" dispositivos con un identificador único (ID), que se encuentran adjuntos a los activos u objetos que se desean identificar u opcionalmente almacenar información detallada de ellos. Las marcas contienen información del activo u objeto y además pueden incorporar sensores [17]. Existen diferentes tipos de marcas, con características diferentes y, por ende, con aplicaciones diferentes. Hay muchos criterios para clasificar las marcas (e.g. tamaño, frecuencia de operación), sin embargo, comúnmente se clasifican por su fuente de energía [12, 3]:

  - ***Activas***. Conforman el segundo grupo más grande de marcas RFID. Tienen capacidades considerables de almacenamiento y procesamiento, detectar el canal y detectar colisiones, además de contar con una fuente de poder o energía para la transmisión de datos. Debido a las múltiples características de las marcas activas, su rango de alcance es mayor, su costo es elevado y su complejidad de diseño/fabricación es alta.
  - ***Pasivas***. Conforman el grupo más grande de marcas RFID. Cuentan con capacidades limitadas de almacenamiento, procesamiento, y transmisión de datos. A diferencia de las marcas activas, las marcas pasivas no son capaces de detectar el canal, detectar colisiones, ni de comunicarse entre ellas. De igual forma, no tienen fuente de poder; en vez de esto, obtienen energía inducida mediante las ondas electromagnéticas emitidas por el lector. Debido a las características que poseen este tipo de marcas, su costo y su complejidad de diseño/fabricación son bajos.
  - ***Semipasivas***. Tienen capacidades similares a las de las marcas pasivas, a diferencia de que las marcas semipasivas tienen fuente de poder para el controlador o microchip y que pueden tener dispositivos adicionales (e.g. sensores).
  - ***Semiactivas***. Cuentan con capacidades similares a las de las marcas activas, a diferencia de que las marcas semiactivas no cuentan energía activa para percibir la información transmitida por el lector o por otras marcas.

En la Tabla 1.1 se presentan algunas características adicionales de las marcas pasivas y activas[17].

Tipo de marca RFID	Frecuencia de comunicación	Rango de alcance	Tamaño del ID
Pasiva	860-960 MHz	hasta una decena de metros	64/96 bits
Activa	433 MHz	hasta un par de cientos de metros	32 bits

Tabla 1.1: Detalles extras de las marcas activas y las marcas pasivas.

Dependiendo de las características requeridas en un sistema RFID, el uso de marcas pasivas, activas, semipasivas o semiactivas es mas adecuado. Debido a su bajo costo y baja complejidad, las marcas pasivas son las más utilizadas dentro de diversos sectores de la industria.

En base al tipo de marcas que se utilizan dentro de una red, las redes RFID conforman diferentes ambientes o entornos, que se pueden clasificar como: pasivos, activos, semipasivos o semiactivos.

1.2. Contexto e identificación de la problemática

1.2.1. Contexto

Debido a que RFID es una tecnología muy prometedora y debido a que las redes RFID son utilizadas dentro de diversos ámbitos, en los que se tienen diferentes requerimientos (tales como confiabilidad, seguridad, rapidez) es necesario que éstas cuenten con mecanismos que mejoren su funcionamiento y optimicen su rendimiento. Una mejora en cualquiera de los campos antes mencionados, podría significar la apertura para crear nuevas aplicaciones que utilicen redes RFID.

Actualmente, las redes RFID se utilizan para llevar a cabo diferentes actividades dentro de distintas áreas, algunas de las cuales son [6]:

- Transporte público.
- Control de acceso.
- Control de producción.
- Seguimiento de activos.
- Identificación de objetos.
- Tareas de conteo.

Tipos de Colisiones	Involucrados
Marca-Marca	2 o más Marcas
Lector-Marca	1 Marca y 1 Lector
Lector-Lector	2 o más Lectores

Tabla 1.2: Tipos de colisiones dentro del ámbito RFID.

- Manejo de inventarios automatizados.

En una red RFID se debe realizar una identificación fiable, rápida y "simultánea" de varios objetos, para lo cual uno o más lectores deben realizar un proceso de identificación.

En un proceso típico de identificación, el lector difunde un mensaje hacia las marcas en el que les solicita su ID o información almacenada. Tras recibir este mensaje, todas o algunas marcas envían su respuesta hacia el lector. Por un lado, si solamente una marca responde, el lector recibe solamente un mensaje que puede decodificar correctamente. Por el contrario, si dos o más marcas responden de manera simultánea, sus mensajes colisionarán sobre el canal de radio frecuencia (*Radio Frequency* o RF) y no serán recibidos correctamente en el lector. Este problema se conoce como **"colisiones entre marcas"** o **"colisiones marca-marca"**, y actualmente es uno de los principales problemas de investigación en este tipo de redes, ya que no solamente se pierde la información transmitida por las marcas, sino que se desperdicia energía por parte de los dispositivos involucrados en la colisión, se desperdicia el ancho de banda, y se incrementa el retardo de identificación [1], siendo este último una de las medidas de desempeño más importantes en este tipo de redes.

Si bien, el problema de colisiones entre marcas es el más común y el principal reto en este tipo de redes, es importante mencionar que existen otros tipos colisiones. En la Tabla 1.2 se presentan los diferentes tipos de colisiones que existen, junto con los dispositivos involucrados en la colisión [9].

Las colisiones **"lector-lector"** ocurren cuando las señales de dos o más lectores interfieren entre ellas, es decir, están configurados para operar en el mismo canal. Las colisiones **"lector-marca"** ocurren cuando dos o más lectores intentan comunicarse de manera simultánea con la misma marca [15].

1.2.2. Problema

Ya que las colisiones entre marcas son uno de los problemas más comunes y uno de los más estudiados dentro del ámbito de las redes RFID, enfocamos nuestro trabajo a resolver el problema de colisiones entre marcas bajo el esquema de un lector y varias marcas, asumiendo que el número exacto de marcas es desconocido, con el fin de realizar una identificación fiable, rápida y simultánea de varios objetos.

Debido a que existen diferentes entornos (definidos por el tipo de marca RFID utilizada) dentro de la tecnología RFID, es necesario que exista un mecanismo estándar que permita solucionar el problema de colisiones. Actualmente, las redes RFID ya siguen estándares que

permiten resolver el problema de colisiones entre marcas, según el entorno definido por el tipo de marca utilizado: EPC Gen 2 Class 1 [21] para ambientes RFID pasivos e ISO-18000-7 [8] para ambientes RFID activos. En secciones posteriores abordaremos el funcionamiento de estos estándares.

1.3. Motivación

Los estándares resuelven el problema de colisiones entre marcas dentro de sus respectivos entornos, sin embargo, se puede mejorar las técnicas que se utilizan durante el proceso de identificación para optimizar su desempeño. Prueba de ello es que numerosas propuestas se han presentado hasta el momento para tal fin, y actualmente se realiza mucho trabajo de investigación en torno a ésta temática.

La redes RFID han tenido un gran auge en los últimos años debido a las multiples características con las que cuentan. Su uso es inevitable dentro de diversas áreas, ya que permite facilitar tareas y optimizar procesos. Por ende, es sustancial que este tipo de redes cuenten con mecanismos que ayuden a mejorar su funcionamiento. Es un hecho que el problema de colisiones es uno de los problemas más importantes que atañen a las redes RFID, y mejorar las técnicas de resolución de colisiones en redes RFID, ofrece invariablemente una mejora en su desempeño.

1.4. Objetivos

1.4.1. Objetivo General

- ***Proponer y/o mejorar algún protocolo anticolisión en el contexto de redes RFID.***

1.4.2. Objetivos Particulares

- Realizar un profundo estudio y análisis de los protocolos anticolisión para redes RFID.
- Modificar y/o proponer un protocolo anticolisión para redes RFID.
- Evaluar la propuesta realizada mediante simulación.

1.5. Metodología

1. Revisión de la literatura en el tema.
2. Identificación del trabajo realizado en cada uno de los entornos RFID.

3. Identificación de los parámetros de evaluación de desempeño más importantes dentro del contexto de redes RFID.

4. Selección del protocolo anticolisión a proponer.

5. Selección de una herramienta para llevar a cabo la simulación.

6. Implementación del protocolo propuesto, y de los protocolos a comparar.

7. Evaluación de los protocolos implementados.

8. Comunicación de resultados.

Con el fin de cumplir los objetivos plantados y encontrar una nueva solución, en el **Capítulo 2** presentamos los fundamentos de una red RFID, así como el marco teórico y el trabajo realizado en torno al problema de colisiones entre marcas en redes RFID. En el **Capítulo 3** presentamos el trabajo relacionado al problema de colisiones entre marcas activas, junto con la descripción del protocolo CSMA p-persistente propuesto. En el **Capítulo 4** presentamos las métricas y escenarios evaluación, junto con los resultados obtenidos. Finalmente, en el **Capítulo 5** concluimos el documento presentando algunas conclusiones y el trabajo a futuro.

CAPÍTULO 2

MARCO TEÓRICO

En este capítulo presentamos una revisión de los protocolos anticolisión más representativos, que se han propuesto bajo el contexto de RFID hasta el momento.

2.1. Resolución de colisiones en redes RFID

Debido a la naturaleza inalámbrica de las redes RFID, y con el fin de de mitigar el problema de las colisiones, las redes RFID implementan protocolos de lectura o anticolisión para llevar a cabo el proceso de identificación. Estos protocolos anticolisión son los encargados de regular el acceso al medio de transmisión. Actualmente, dentro del ámbito de RFID, existen diversas maneras en la que se puede regular el acceso al medio a nivel de la capa física [3], sin embargo, algunas de ellas requieren que todos los dispositivos cuenten con características especiales:

- **Acceso Múltiple por División de Espacio (*Space Division Multiple Access* o SDMA)**. Consiste en separar el canal en sectores usando antenas unidireccionales o varios lectores para identificar todas las marcas.
- **Acceso Múltiple por División de Frecuencia (*Frequency Division Multiple Access* o FDMA)**. Consiste en dividir el canal en subcanales, que corresponden a distintos rangos de frecuencia, dentro de los cuales las marcas pueden transmitir.
- **Acceso Múltiple por División de Código (*Code Division Multiple Access* o CDMA)**. Consiste en separar las marcas mediante la generación de un código único, y con esto lograr que esta información se difunda por todo el espectro.
- **Acceso Múltiple por División de Tiempo (*Time Division Multiple Access* o TDMA)**. Consiste en dividir el canal en ranuras de tiempo que son asignadas a las

marcas, de tal manera que durante una fracción de tiempo es asignado todo el canal a la transmisión de una marca.

- **Acceso Múltiple por Detección de Portadora (*Carrier Sense Multiple Access* o CSMA)**. En este caso, las marcas censan el canal antes de enviar su información. Si no hay una transmisión en curso, tras censar libre el medio de transmisión, una marca comienza la transmisión de su información. Desafortunadamente, este mecanismo solo se puede usar en entornos RFID activos, ya que la marcas pasivas no son capaces de censar el medio.

Diversos protocolos anticolisión se han propuesto hasta el día de hoy. En la Figura 2.1 se presenta una taxonomía de protocolos anticolisión. El primer nivel de la taxonomía se encuentra clasificado por el manejo a nivel de la capa física, mientras que el siguiente nivel se encuentra clasificado por el manejo a nivel de capa de control de acceso al medio (MAC), debido a que se trabaja con el esquema de un lector y múltiples marcas.

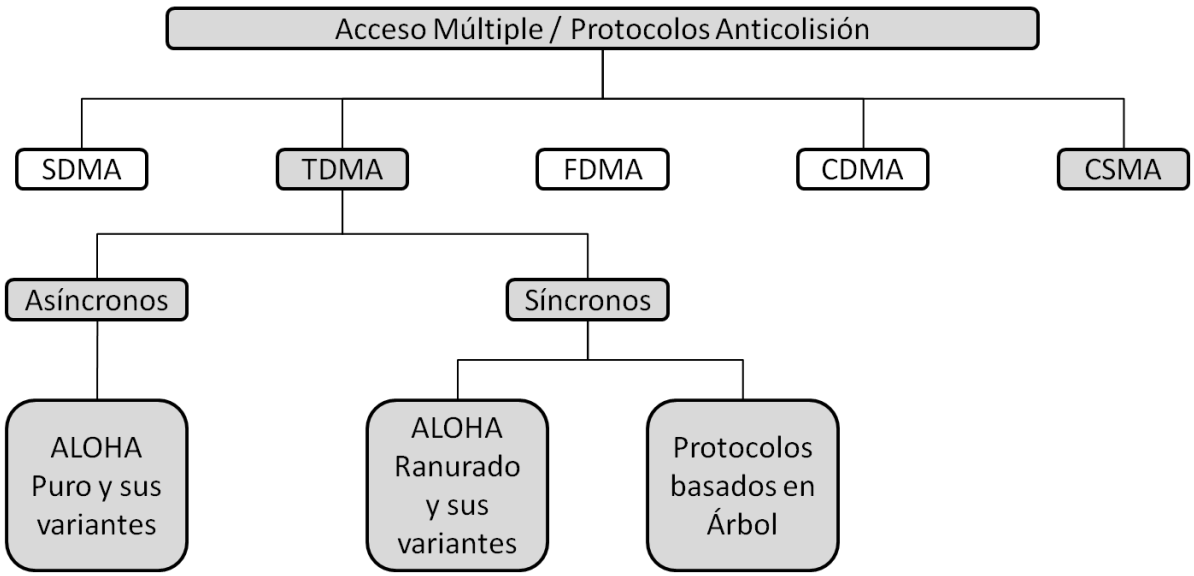


Figura 2.1: Taxonomía de protocolos anticolisión para redes RFID.

Ya que TDMA es el grupo más representativo de protocolos anticolisión para redes RFID, en secciones posteriores presentamos una revisión de los protocolos más representativos que pertenecen a este grupo, explicamos sus ventajas y desventajas, así como su funcionamiento y la importancia que estos tienen dentro de las redes RFID. Por otro lado, ya que los protocols basados CSMA han mostrado tener un buen desempeño dentro de las redes RFID, en secciones posteriores presentamos una revisión de los protocolos más representativos que pertenecen a este grupo, explicamos su funcionamiento, ventajas y desventajas.

Si bien los protocolos que se presentan a continuación ya han sido estudiados en otros contextos (e.g. LAN's que tienen una comunicación dinámica y continua), su funcionamiento

difiere bajo el contexto RFID debido a que la comunicación entre los dispositivos participantes es centralizada y temporal. Como se mencionó en secciones anteriores, el lector es el dispositivo central al cuál las marcas deben transmitir su información, quién tiene que identificar todas las marcas de forma ordenada y lo más rápido posible.

2.2. Protocolos basados en ALOHA

ALOHA es uno de los protocolos precursores dentro del control de acceso al medio, por lo que actualmente existen diversos protocolos para redes RFID basados en ALOHA: Protocolo ALOHA Puro (PA), Protocolo ALOHA Ranurado (SA), y Protocolo ALOHA Ranurado con Tramas(FSA).

Protocolo ALOHA Puro (PA)

En las redes RFID basadas en ALOHA, el proceso de identificación es como se describe a continuación: el lector envía un comando de solicitud de datos o ID's. Tras recibir esta solicitud de información, cada marca responde de forma aleatoria con la información solicitada por el lector, y espera a que el lector le responda con un mensaje ACK indicando que la transmisión fue exitosa o un mensaje NACK indicando que ocurrió una colisión. Para resolver el inconveniente de las colisiones, las marcas esperan un tiempo aleatorio para retransmitir sus datos [5]. Este procedimiento es realizado de manera cíclica, como se muestra en la Figura 2.2.

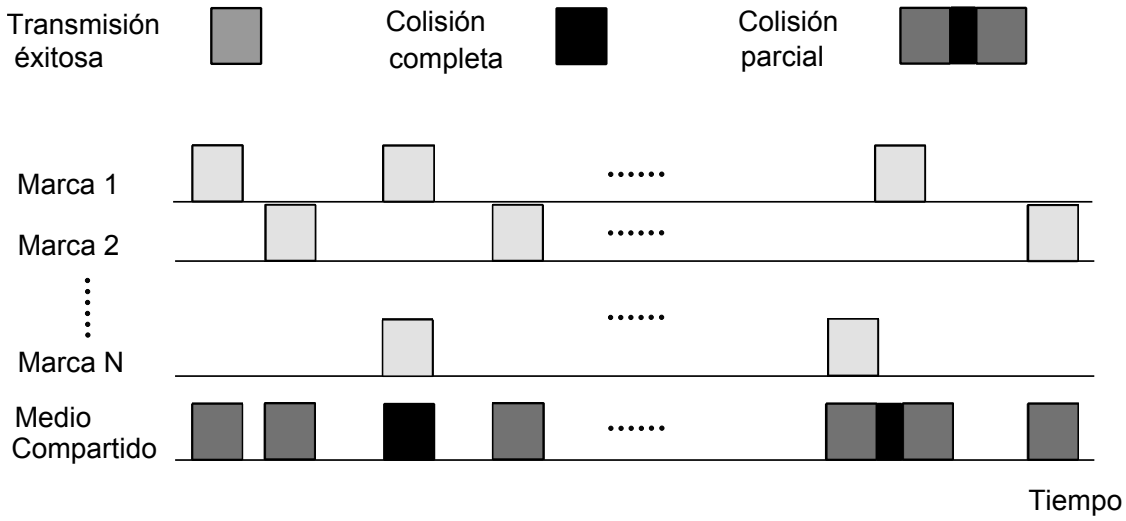


Figura 2.2: Esquema de funcionamiento del protocolo ALOHA Puro.

La eficiencia de este protocolo se ve afectada por las múltiples colisiones que tienen lugar debido a la aleatoriedad introducida, es decir, debido a que la respuesta de las marcas no está organizada en ninguna forma.

Protocolo ALOHA Ranurado (SA)

SA es una variante del protocolo ALOHA en la que se asume el tiempo ranurado. Una ranura o *slot* es un intervalo de tiempo en el que las marcas pueden transmitir su ID [2].

En SA las marcas transmiten su ID en ranuras de tiempo síncronas, lo que quiere decir que cada ranura tiene el mismo tamaño y que dependen del lector para ser accionadas. En este esquema cada marca genera un número aleatorio, el cual corresponde a la cantidad de tiempo (ranuras de tiempo) que tendrá que esperar la marca antes de transmitir su ID. Si ocurre una colisión, cada marca que colisionó retransmite su información después de esperar un cierto número aleatorio de ranuras. Si ocurre un identificación exitosa, el lector envía un mensaje ACK a la marca identificada inmediatamente después de que la marca ha sido identificada [12, 1]. El funcionamiento del protocolo SA se ilustra en la Figura 2.3.

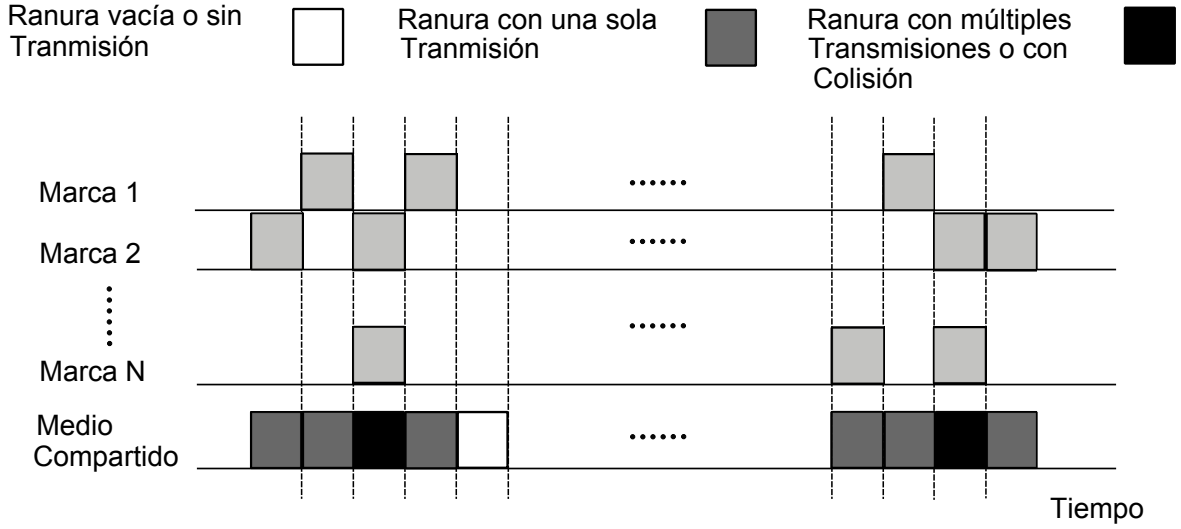


Figura 2.3: Esquema de funcionamiento del protocolo ALOHA Ranurado.

Al asumir el tiempo ranurado, esta variante del protocolo ALOHA reduce la posibilidad de colisiones entre marcas dentro de una ranura, por lo que la eficiencia de la red se ve beneficiada.

Protocolo ALOHA Ranurado con Tramas(FSA)

FSA es una variante del protocolo SA, que asume el tiempo ranurado y agrupado por tramas. Nuevamente, una ranura es un intervalo de tiempo en el que las marcas pueden transmitir su ID [2].

Como se puede apreciar en la Figura 2.4, en FSA se realizan varios ciclos de lectura o ciclos de identificación (CI) para identificar todas las marcas que se encuentran dentro del rango de cobertura de un lector, en el que cada ciclo de lectura consiste de una trama. Una trama es el intervalo de tiempo entre solicitudes de un lector, que está conformado por un cierto número de ranuras [2]. A diferencia de PA y SA, en FSA las marcas están limitadas a

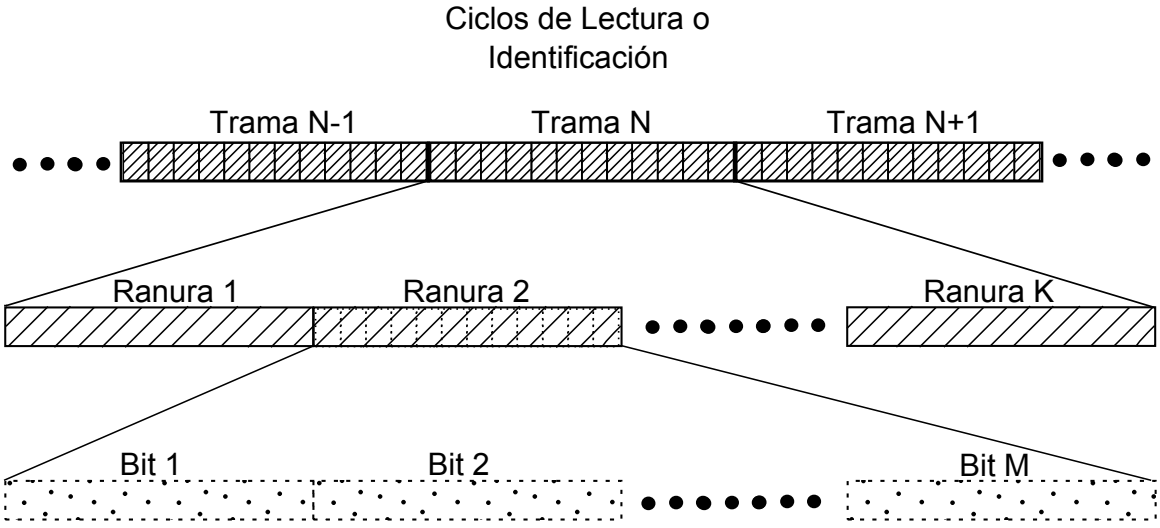


Figura 2.4: Esquema de funcionamiento del protocolo FSA.

transmitir una vez por trama, ya que de lo contrario ocurren colisiones frecuentes entre las mismas marcas.

El funcionamiento de este protocolo se describe a continuación: el protocolo inicia con un mensaje de solicitud de información, en el cual se indica el tamaño de la trama, a saber "N", desde el lector hacia las marcas. Una vez que las marcas conocen el tamaño de la trama, cada una de ellas genera un número aleatorio con una distribución uniforme entre 0 y "$N-1$". El número generado corresponde a la ranura de tiempo en la que transmitirán su ID. Cuando dos o más marcas transmiten en la misma ranura, ocurre una colisión, generando de esta manera un nuevo ciclo de identificación en el que participarán solamente las marcas que colisionaron en la trama actual. Por otro lado, si en una ranura solamente ocurrió una transmisión, la marca correspondiente se identifica exitosamente y se notifica con un mensaje ACK, evitando de esta manera que participe en el siguiente ciclo de identificación.

Existen 2 diferentes tipos de FSA:

- **FSA Básico (BFSA):** El tamaño de la trama es fijo y no cambia durante el proceso de identificación [19]. La consecuencia de mantener fijo el tamaño de la trama, es que éste procedimiento tiende a no ser escalable, ya que conforme aumenta la cantidad de marcas a identificar, también lo debería hacer el tamaño de la trama.

- **FSA Dinámico (DFSA):** El tamaño de la trama (k) es variable y se ajusta conforme el proceso de identificación avanza [23]. Utiliza una función de estimación al final de cada ciclo de lectura para ajustar el tamaño de las tramas subsecuentes. De esta manera, se estima el número de marcas sin identificar con la retroalimentación de la lectura de la trama actual. Generalmente, una función de estimación involucra el número de ranuras vacías o sin respuesta (c_0), el número de ranuras con solamente una transmisión o respuesta (c_1), y el número de ranuras con múltiples transmisiones o ranuras con

colisión (c_k). Algunas de las funciones más representativas de este tipo de protocolos se presentan en la Tabla 2.1.

Propuesta	Función	Descripción
Vgot en [23].	$\epsilon_{vd}(N, c_0, c_1, c_k) = min_t \left\| \begin{pmatrix} a_0^{N,t} \\ a_1^{N,t} \\ a_k^{N,t} \end{pmatrix} - \begin{pmatrix} c_0 \\ c_1 \\ c_k \end{pmatrix} \right|$ $a_0^{N,t} \rightarrow$ Número esperado de ranuras sin transmisión. $a_1^{N,t} \rightarrow$ Número esperado de ranuras con una sola transmisión. $a_k^{N,t} \rightarrow$ Número esperado de ranuras múltiples transmisiones.	Se basa en el principio de máxima verosimilitud, para lo cual utiliza la desigualdad de Chebyshev para minimizar la diferencia entre los valores esperados de c_0, c_1 y c_k, y los valores obtenidos en la trama actual.
Zhen en [26].	$c_1 + 2{,}39 * c_k$	Se basa en la idea de que en una colisión al menos 2 marcas están involucradas.
Schoute et. al. en [19].	$\widehat{n} = c_k * 2{,}3992$ $k_{i+1} = round(\widehat{n} - c_1)$	Se basa en el número esperado de ranuras con colisión.

Tabla 2.1: Funciones de ajuste de trama para FSA.

Al considerar el tiempo ranurado, agrupado por tramas y limitar la respuesta de las marcas a una sola dentro de una trama, FSA evita colisiones frecuentes, identifica múltiples marcas dentro de una trama, y aumenta la eficiencia de la red.

Como se mencionó anteriormente, el uso del protocolo ALOHA en redes RFID tiene un gran impacto, ya que los estándares utilizados dentro de las redes RFID están basados sobre una versión modificada de FSA.

2.3. Protocolos basados en árbol

Los protocolos basados en árbol son capaces de detectar y leer todas las marcas presentes en la zona de interrogación de un lector. Este tipo de protocolos requieren que las marcas implementen la característica "silencio", que se refiere a que estas son "silenciadas" después de que han sido identificadas [12].

En general, los protocolos basados en árbol exhiben un retardo de identificación superior a los protocolos basados en ALOHA; sin embargo, los protocolos basados en árbol son capaces de evitar el problema de la "marca hambrienta o colisionante" [2], que consiste en que una marca puede pasar un largo tiempo sin ser identificada, debido a la aleatoriedad introducida por los protocolos basados en ALOHA.

En la Figura 2.5 se presenta la estructura común que siguen los protocolos basados en árbol. Dependiendo del protocolo de árbol que se implementa como protocolo anticolisión, el tamaño y recorrido del mismo varia, y en base a éste se pueden tener tres diferentes tipos de nodos dentro del árbol: vacíos, con una sola transmisión o con colisión.

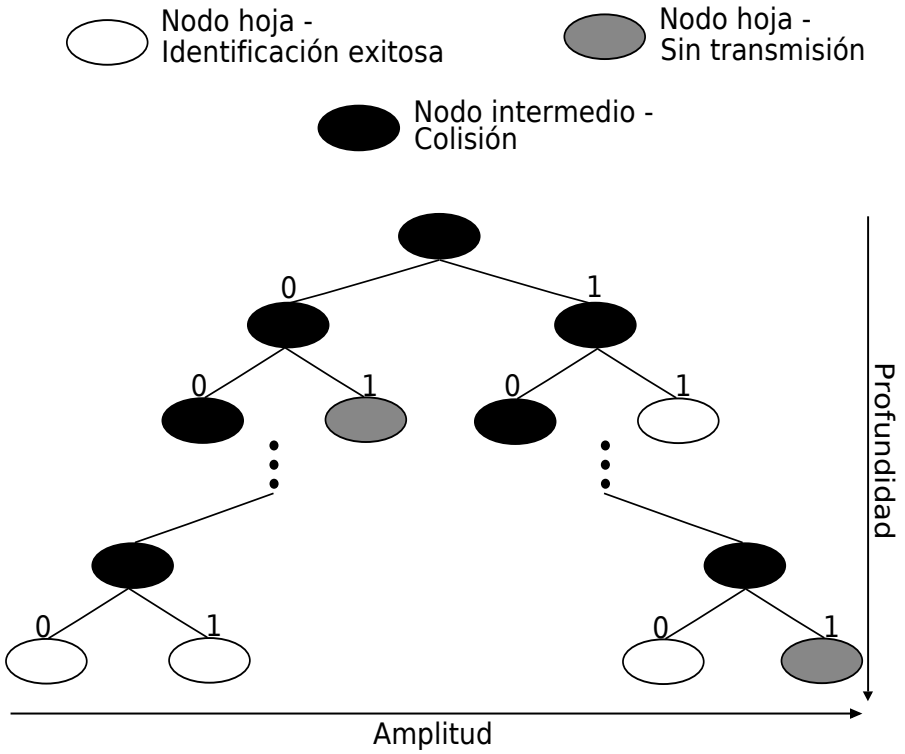


Figura 2.5: Estructura general de un protocolo basado en árbol.

Este tipo de protocolos utilizan los bits asociados al ID de las marcas, para llevar a cabo el proceso de identificación, y siguen una estructura de árbol (generalmente la de un árbol binario). En este esquema, cada nodo en el árbol representa una ranura de lectura. Los nodos padres corresponden a colisiones, mientras que los nodos hoja corresponden a una identificación exitosa. Algunos de los protocolos basados en árbol más representativos son: División de árbol (TS), División Básica de árbol (BTS), División Adaptativa de árbol Binario (ABTS), y árbol de Consulta (QT)[2].

División de árbol (TS)

La idea básica de los protocolos TS consiste en dividir las respuestas de las marcas en varios subconjuntos, para lo cual las marcas utilizan un generador de números aleatorios. BTS (*Basic Tree Splitting*) es un algoritmo que resuelve el problema de colisiones dividendo el número de marcas que colisionaron dentro de "*b*" subconjuntos disjuntos. Conforme la ocurrencia de colisiones sucede de manera progresiva, estos subconjuntos se van haciendo más pequeños hasta contener una sola marca [7].

En BTS, los nodos hoja del árbol corresponden a una identificación exitosa, mientras que los nodos intermedios corresponden colisiones entre marcas.

División adaptativa de árbol binario (ABTS)

ABTS es una variante de BTS que reduce las colisiones y elimina las ranuras vacías innecesarias, mediante el manejo de 2 contadores por parte de las marcas: *Progressed Slot Counter* (PSC) y *Allocated Slot Counter* (ASC). Cada marca puede transmitir solo cuando sus contadores son iguales. El PCS de cada marca es alterado cuando el lector identifica una marca, mientras que el ACS de cada marca es modificado por el resultado de una colisión o de una ranura vacía [16].

Por su parte, el lector incluye el contador *terminating slot counter* (TSC) que le permite terminar el proceso de identificación una vez que todas las marcas han sido identificadas.

Árbol de consulta (QT)

La idea básica en el protocolo Query Tree (QT), consiste en que el lector envía un prefijo de consulta "q" a todas las marcas, y solamente aquellas cuyo ID coincida con el valor difundido por el lector, responderán a la consulta. Si este proceso lleva a una colisión, el lector agrega un "0" a la cadena de consulta, y mete en la pila la cadena de consulta aumentada con "1" para posteriormente difundirla. Este proceso se repite hasta que se realiza una transmisión exitosa, en cuyo caso el lector comienza una nueva ronda con otro prefijo de consulta [14].

En los protocolos QT se requiere que el lector almacene el árbol construido durante el proceso de identificación, y que las marcas incluyan un circuito de acoplamiento de prefijo [27].

Existen diversas variantes de este protocolo:

- ***Shortcutting.*** Reduce el retardo de identificación de QT mediante la eliminación de consultas redundantes [14].
- ***Aggressive Enhancement.*** Cuando ocurre una colisión, se agregan varios bits a la consulta en lugar de agregar un solo bit [14].
- ***Enhanced Query Tree Protocol.*** Utiliza la información obtenida a partir de una identificación exitosa para CI's posteriores [24].

Sidewalk

Este protocolo basado en árbol aprovecha la estructura secuencial del ID de las marcas, con el fin de alcanzar una eficiencia máxima. Hace una búsqueda primero en profundidad hasta identificar exitosamente una marca, para posteriormente recorrer de manera horizontal los nodos que se encuentran al mismo nivel [13].

2.4. Protocolos híbridos

Los protocolos híbridos son una nueva rama de los protocolos anticolisión, que combinan las ventajas de los protocolos basados en árbol y de los protocolos basados en ALOHA. En la Tabla 2.2 se presentan algunos de los protocolos híbridos más representativos propuestos hasta el momento.

Propuesta	Nombre	Descripción
M. A. Bonuccelli, F. Lonetti, y F. Martelli [2].	Tree Slotted ALOHA (TSA).	Incorpora las ventajas del protocolo FSA con una estructura de árbol para el proceso de identificación. En este esquema, el nodo raíz del árbol corresponde a la trama a ser transmitida en el primer ciclo de lectura.
G. Miselli, C. Petrioli, y C. Vicari [15].	Dynamic Tree Slotted ALOHA (DTSA).	En esta variante, los autores proponen aprovechar el conocimiento adquirido en los resultados de las primeras tramas para redimensionar el tamaño de las siguientes tramas hermanas, es decir, en base a las tramas que se encuentran al mismo nivel. De esta manera se refina la estimación de marcas, logrando una mayor exactitud.
J. Ryu, H. Lee, Y. Seok, T. Kwon, y Y. Choi [25].	Hybrid Query Tree (HQT).	Combina el protocolo QT con un mecanismo de back-off aleatorio ranurado, lo que quiere decir que las marcas consideran ranuras de tiempo para la retransmisión después de un número aleatorio de ranuras, en vez de esperar a ser identificadas. El proceso de identificación es similar al del protocolo QT.
J.-D. Shin, S.-S. Yeo, T.-H. Kim, y S. K. Kim [20].	Combinan las características de QT y FSA.	Utiliza FSA para que las marcas seleccionen una ranura para trasmitir su ID, y dentro de cada ranura se utiliza QT para identificar las marcas que hayan seleccionado esa ranura.
		Utiliza FSA para difundir el tamaño de la trama junto con un prefijo, y solamente aquellas marcas cuyo prefijo coincida con el prefijo difundido podrán participar en el ciclo de lectura que comienza.

Tabla 2.2: Protocolos híbridos.

2.5. Protocolos basados en CSMA

Los protocolos basados en CSMA, son protocolos anticolisión que manejan eficientemente el control de acceso al medio en las redes RFID. Sin embargo, este tipo de protocolos requieren todo el potencial ofrecido por las marcas activas para el proceso de identificación, lo que representa una desventaja frente a otro tipo de protocolos como FSA. Por otro lado, algunas de las propuestas de CSMA se enfocan en otro de los principales problemas de las redes RFID activas; el ahorro de energía. En este sentido, si bien es cierto que el disminuir las colisiones disminuye el consumo de energía, también lo es que un modelo anticolisión no es un modelo de ahorro de energía, ni es la única manera en la que se puede ahorrar energía.

CSMA/CA con RTS/CTS

En [11], los autores presentan un protocolo anticolisión derivado de CSMA/CA, CSMA con RTS/CTS (*Request To Send/Clear To Send*). Los autores trasladan el funcionamiento de CSMA dentro de RFID a que cada marca transmita su información en base a si detectan el medio libre u ocupado. La idea principal de este protocolo consiste en evitar las posibles colisiones generadas por el fenómeno de la terminal oculta. En este trabajo, los autores muestran que el uso de RTS/CTS es la solución a este problema, y que el caudal de datos (*throughput*) se incrementa con ello.

CSMA no-Persistente

En [22], los autores presentan un trabajo en el que evalúan el funcionamiento del protocolo CSMA no-persistente en el ámbito de las redes RFID. El protocolo CSMA no-persistente presentado en este trabajo, utiliza la función de distribución presentada en [10] para que cada marca seleccione de manera aleatoria una micro-ranura dentro de una ventana de contienda, para posteriormente transmitir su ID o información específica.

La distribución *Sift* (2.1), asocia a la micro-ranura "r" la probabilidad "p_r" en base a su posición dentro de la ventana de contienda, y al máximo número de contendientes o marcas, generando que la probabilidad de selección para las primeras micro-ranuras sea baja, y alta para las últimas micro-ranuras.

$$p_r = \frac{\alpha^{-r}(1-\alpha)\alpha^k}{1-\alpha^k} \tag{2.1}$$

con:

- $r = 1 \ldots K$
- $\alpha = M^{\frac{-1}{K-1}}$.
- K el tamaño de la ventana de contienda
- M un parámetro pre-configurado por el usuario, el cual representa el número máximo de contendientes.

El funcionamiento de este protocolo se describe a continuación: el lector difunde una solicitud de ID's, en la que indica el tamaño de la ventana de contienda actual y el máximo numero de participantes (ya que no es conocido a priori el número de marcas presentes en la zona de interrogación). Tras recibir este mensaje, las marcas seleccionan una micro-ranura dentro de la ventana de contienda siguiendo la distribución *Sift*, con el fin de transmitir su información dentro de la micro-ranura seleccionada. Posteriormente, cada marca sensa el medio hasta el número de micro-ranura seleccionada, y transmite si y sólo si el medio permaneció libre hasta entonces. De lo contrario, se retira hasta la próxima orden emitida por el lector. Si no hay colisión, el lector envía una orden ACK-Collection, que indica la marca ya ha sido identificada y solicita más ID's. Las marcas aún sin identificar participan nuevamente en el proceso. En la Figura 2.6 se ilustra el funcionamiento del protocolo CSMA no-persistente con distribución *Sift*.

Bajo este esquema una ventana de contienda es el equivalente a una trama en FSA, y a diferencia de FSA, el tamaño de la ventana de contienda es constante. Cabe mencionar que bajo este esquema se identifica una marca por CI.

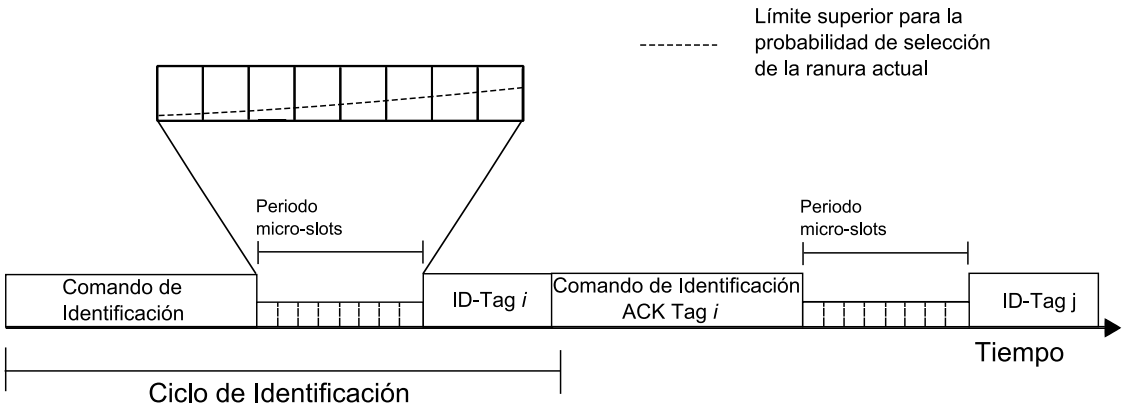


Figura 2.6: Esquema de funcionamiento del protocolo CSMA no persistente con distribución *Sift*.

En general, los resultados presentados en [22], muestran que CSMA no-persistente con distribución *Sift* es superior al estándar utilizado en entornos RFID activos [8].

CSMA no-Persistente con multi-fases

En [18], se presenta un trabajo reciente en el que los autores presentan una mejora sobre la propuesta presentada en [22], llamada CSMA/MS. La idea principal de este esquema consiste en dividir el proceso de identificación en G etapas con el fin de maximizar la probabilidad de éxito al transmitir. Cada etapa cuenta con K_i micro-ranuras de contienda, las cuales son

seleccionadas por las marcas tras seguir la distribución *Sift*. En cada una de las etapas el conjunto de marcas participantes va decreciendo, debido a que solo unas cuantas seleccionan los primeros *slots* y el resto detecta el medio ocupado. Los resultados presentados en esta propuesta, muestran que su protocolo es superior a los presentados en [22] y [8].

2.6. Conclusión preliminar

Existen diversos protocolos anticolisión que permiten resolver eficientemente el problema de colisiones dentro de los diferentes entornos RFID. Si bien existen varias propuestas de protocolos anticolisión que permiten evitar y resolver este problema, los más notorios son las variantes del protocolo FSA debido a la rapidez que ofrecen, la capacidad de variar la carga del sistema, la exactitud ofrecida en la estimación de marcas para una población grande, y en general a la alta eficiencia ofrecida.

Existen diversas propuestas basadas en árboles que permiten solucionar el problema de colisiones. Dentro de los protocolos más simples y prometedores son aquellos que están basados en QT. Si bien, los protocolos basados en árboles no son tan rápidos como los protocolos basados en ALOHA, son muy efectivos y confiables.

La combinación de las características de los protocolos de árbol y ALOHA, resultan en una poderosa técnica que permite resolver más rápidamente el problema de las colisiones. El detalle fino de este enfoque, recae en encontrar la combinación exacta que permita realizar una identificación más rápida y fiable.

Con respecto a los protocolos basados en CSMA, existen diversos trabajos enfocados en el ahorro de energía, que es otro de los principales problemas dentro de los entornos RFID activos. Al disminuir el consumo de energía se mitiga de manera indirecta el problema de colisiones entre marcas, sin embargo, al ser un modelo de energía y no un modelo de resolución de colisiones, los resultados no son comparables con los de un modelo de resolución de colisiones. Por otro lado, existen propuestas basadas en CSMA que fueron adaptadas para trabajar en redes RFID, que demuestran tener un buen desempeño.

CAPÍTULO 3

CSMA *P*-PERSISTENTE: UN PROTOCOLO ANTICOLISIÓN PARA ENTORNOS RFID ACTIVOS

Como ya se mencionó, existen diversas formas para llevar a cabo la resolución de colisiones entre marcas en redes RFID. Ya que nuestra propuesta se basa en ambientes RFID activos, y con el fin de introducir los detalles de este tipo de entornos, en este capítulo describimos el funcionamiento del estándar ISO-18000-7 para entornos RFID activos, y profundizamos en el funcionamiento del protocolo CSMA no-persistente propuesto en [22].

3.1. Trabajo relacionado

3.1.1. Estándar ISO-18000-7 para entornos RFID activos

El estándar ISO-18000-7, es el estándar propuesto para resolver colisiones entre marcas activas. Propone utilizar *FSA* como protocolo anticolisión, sugiriendo el uso de un mecanismo de adaptación de trama, pero sin especificar uno en particular.

El funcionamiento del estándar ISO-18000-7 se ilustra en la Figura3.1 y se describe a continuación: se tiene un lector y una población de "N" marcas que se desean identificar. El proceso de identificación comienza tras recibir una orden de inicio de identificación, en el que de indica el tamaño de la trama, por parte del lector. A partir de este punto, las marcas eligen de forma aleatoria siguiendo una distribución uniforme, una ranura de tiempo de entre "K" ranuras posibles para transmitir su ID. Por un lado, si dos o más marcas seleccionan la misma ranura de tiempo, se produce una colisión. Por otro lado, si en una ranura se presenta solamente una respuesta, se tendrá una identificación exitosa. Al final de cada ciclo de identificación, el lector envía un paquete ACK a cada una de las marcas identificadas exitosamente dentro de la trama actual, evitando de esta forma que intervengan en futuras tramas. Si se implementa un mecanismo de adaptación de trama, se ajusta el tamaño de la trama en base a los resultados obtenidos en las ranuras de la trama actual.

Como se puede observar, un ciclo de identificación en este esquema abarca los comandos de orden de identificación enviados por el lector y las "K" ranuras de tiempo que conforman la trama.

En el estándar ISO-18000-7, aún cuando las marcas se pueden comunicar entre ellas (debido a las capacidades con las que cuentan), solamente existe la comunicación de marcas al lector y del lector a las marcas.

Debido a que el estándar ISO-18000-7 deja abierto el uso de un mecanismo de redimensionamiento de trama, generalmente no se utiliza ninguno de ellos, lo que genera que no sea escalable con respecto al número de marcas a identificar, ya que al mantener fijo el tamaño de la trama se tendrán [22]:

- Bastantes ranuras vacías. Esto puede suceder al principio o al final del proceso de identificación. El primer caso ocurre debido a que el tamaño de la trama es más grande que el número de marcas a identificar. El segundo caso ocurre debido a que el número de marcas a identificar disminuye conforme avanza el proceso de identificación .
- Bastantes ranuras con colisión. Esto ocurre debido a que el tamaño de la trama es mucho más pequeño que el número de marcas a identificar.

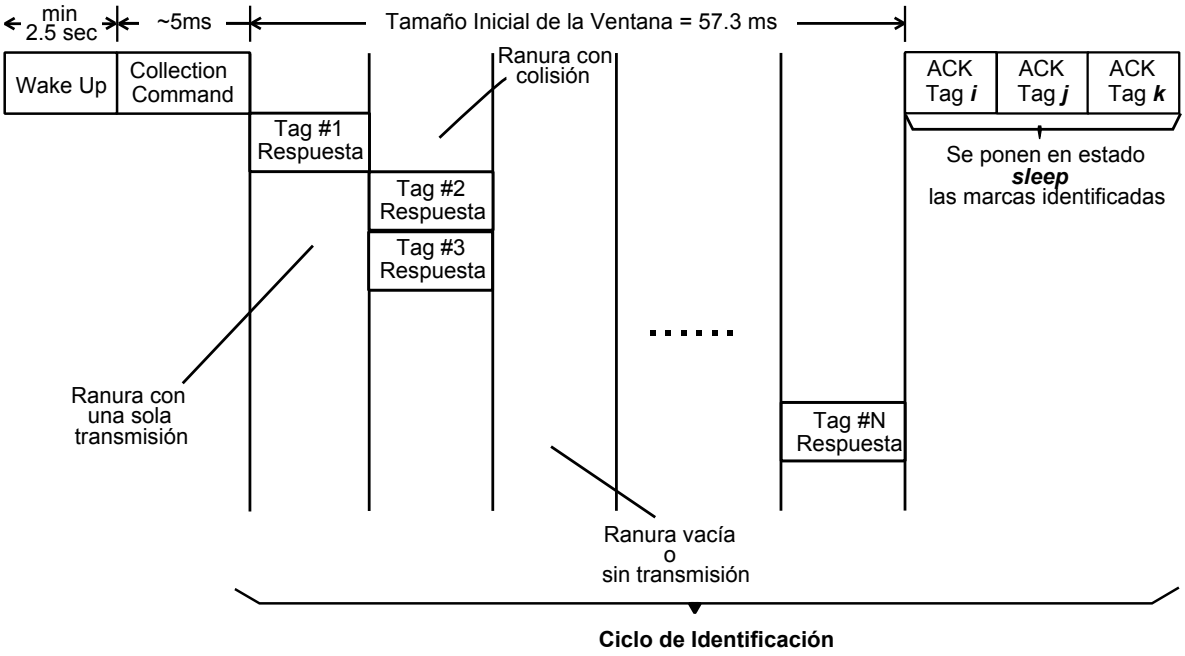


Figura 3.1: Esquema de funcionamiento del estándar ISO-18000-7.

3.1.2. Estándar EPC "Gen 2"

La organización EPCglobal, líder industrial en el desarrollo del estándar en este campo, ha fijado el estándar EPC "Gen 2" como referencia [21]. Según [21], el procedimiento anticolisión

de "Gen 2" es independiente del tipo de dispositivo en el que esté implementado, es decir, pasivo o activo. Al igual que el ISO-18000-7, el EPC "Gen 2" propone utilizar *FSA* como protocolo anticolisión, sin embargo, a diferencia del ISO-18000-7, el EPC "Gen 2" sugiere un algoritmo específico para el mecanismo de adaptación de longitud de trama.

El estándar trabaja bajo el esquema de un lector y una población de "N" marcas que se desean identificar. El proceso de identificación comienza tras recibir una orden de inicio de identificación por parte del lector, a la cual todas las marcas responden generando una colisión. Cuando el lector detecta la colisión inicia un nuevo ciclo de identificación. Un ciclo de identificación comienza la difusión de un paquete *Query* por parte del lector, en el cual se incluye el valor de "Q", con $Q\epsilon[0,\ldots,15]$, para indicar que el tamaño de la trama actual es de 2^Q ranuras. A partir de este punto, las marcas escogen de forma aleatoria siguiendo una distribución uniforme, una ranura de tiempo "r" dentro del intervalo $[0, 2^Q - 1]$. El valor de "r" representa la ranura dentro de la trama en la cual cada marca transmitirá su ID. En la trama, el comienzo de cada ranura es controlado por el lector a través del envío de un paquete *QueryRep*, a excepción de la primer ranura que inicia después del comando *Query*. Por su lado, las marcas utilizan el valor de "r" como un contador, el cual es decrementado por cada paquete *QueryRep* recibido. Cuando el valor de "r" en una marca se vuelve 0, la marca transmite su ID generando tres posibles casos:

- Si dos o más marcas seleccionan la misma ranura de tiempo, se produce una colisión. Por un lado, el lector detecta la colisión y envía un paquete *QueryRep*. Por otro lado, las marcas involucradas actualizan el valor de su variable "$r = 2^Q - 1$".

- Si en una ranura se presenta solamente una respuesta, se tendrá una identificación exitosa. El lector responde con un paquete *ACK*, y aunque todas las marcas reciben el paquete, solamente la marca que logró transmitir en la ranura responderá con un paquete *Data*. Posteriormente, una vez que el lector recibe el paquete *Data* responde con un paquete *QueryRep*.

- Si el lector no recibe respuesta antes de que termine la ranura, el lector asume que la ranura fue vacía y comienza una nueva tras enviar un comando *QueryRep*.

Este procedimiento continúa ranura por ranura hasta que el ciclo termina, es decir, hasta el fin de la trama. Al final de cada trama, el lector ajusta el valor de "Q" en base al número de ranuras vacías, con una sola respuesta y con múltiples respuestas, y por ende el tamaño de la trama subsecuente. El proceso de identificación termina cuando se han identificado todas la marcas, lo que genera que todas las ranuras de la trama sean vacías.

El mecanismo de adaptación de trama que sigue el EPC "Gen 2" se describe en la Figura 3.2. Como se puede observar, este mecanismo incrementa el valor de "Q" por cada ranura con colisión, y lo decrementa por cada ranura vacía en la trama actual. El estándar propone usar la variable $C\ \epsilon(0.1,\ldots,0.5)$ para controlar el mecanismo de adaptación de trama ranura por ranura, sin embargo, no especifica cómo seleccionar el valor de "C", solamente recomienda usar valores altos de "C" para valores bajos de la "Q" actual y viceversa.

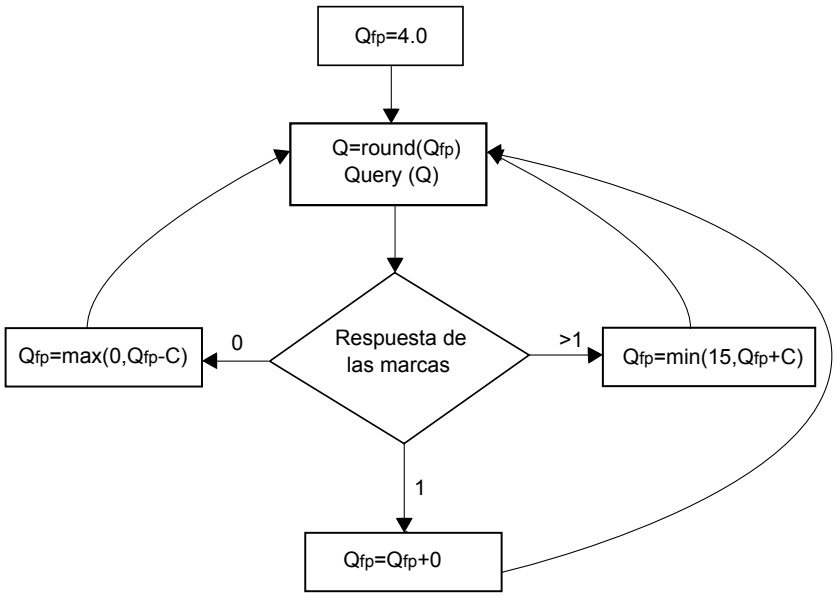


Figura 3.2: Diagrama de funcionamiento del Algoritmo Q.

En [4] los autores presentan un análisis sobre el mecanismo de adaptación de trama utilizada por el estándar EPC "Gen 2" indicando que al elegir la "Q" óptima se acelera el proceso de identificación y se incrementa el caudal de datos. Los autores proporcionan una tabla (ver Tabla 3.1) en la que se especifica el valor de la "Q" óptima en base al número estimado de marcas sin identificar.

Q óptima	Rango de marcas	Q óptima	Rango de marcas
0	n=1	8	117<n≤355
1	1<n≤3	9	355<n≤710
2	3<n≤6	10	710<n≤1420
3	6<n≤11	11	1420<n≤2839
4	11<n≤22	12	2839<n≤5678
5	22<n≤44	13	5678<n≤11357
6	44<n≤89	14	11357<n≤22713
7	89<n≤117	15	n>22713

Tabla 3.1: Valor óptimo Q.

3.1.3. CSMA no-persistente

Como se mencionó, este protocolo implementa la distribución *Sift* [10] para que cada marca seleccione una micro-ranura dentro de la ventana de contienda, permitiendo asignar diferentes probabilidades de selección a las micro-ranuras en base a su posición dentro de

la ventana de contienda, y al máximo número de contendientes o marcas, logrando de esta forma que la probabilidad de selección para las primeras micro-ranuras sea baja y alta para las últimas micro-ranuras. De esta forma, el protocolo CSMA no-persistente con distribución *Sift*, aumenta la probabilidad de éxito al inicio de la ventana de contienda para acelerar el proceso de identificación, por lo que se utilizan menos micro-ranuras, y por ende menos tiempo.

Las ventajas que ofrece la distribución *Sift* son muy grandes cuando el número de marcas tiende a ser bajo; sin embargo, cuando el número de marcas tiende a ser mayor, el beneficio ofrecido por la distribución *Sift* comienza a deteriorarse. En base a los resultados mostrados en [22], observamos que el deterioro se debe a que conforme aumenta el número de marcas a identificar, también lo hacen las colisiones, aún cuando la probabilidad de selección de las primeras micro-ranuras es baja. Por otro lado, la desventaja con la que se cuenta en este esquema, es que se depende de un sólo parámetro configurable por el usuario para garantizar el éxito al inicio de la venta de contienda, lo cual repercute en el tiempo necesario para realizar la identificación de un conjunto de marcas, es decir, en el retardo de identificación.

3.2. Protocolo CSMA *p*-persistente para redes RFID

3.2.1. Motivación

Debido al poco trabajo existente sobre CSMA, en torno al problema de colisiones en redes RFID, e inspirados en el trabajo presentado en [22], se propone el uso de CSMA p-persistente con distribución *Sift* como protocolo anticolisión para redes RFID.

3.2.2. Diseño

El CSMA p-persistente original trabaja bajo un esquema ranurado y funciona como describimos a continuación: una estación que está lista para transmitir detecta o barre el canal. Si el canal se encuentra libre, la estación transmite con una probabilidad "p" y retrasa su transmisión hasta la siguiente ranura con probabilidad "$q = 1 - p$". Si la siguiente ranura está desocupada, la estación transmite o retrasa de nuevo su transmisión con una probabilidad "p" y "q" respectivamente. Este proceso se repite hasta que la ventana de contienda se termine, o bien, que otra estación haya comenzado a transmitir. En el último caso, la estación que intenta transmitir su información, actúa como si hubiera existido una colisión. Si la estación en un inicio detecta el canal ocupado, espera hasta que llegue la siguiente ranura y, entonces, aplica el algoritmo antes mencionado.

Extendiendo el funcionamiento de CSMA p-persistente a RFID, tenemos que CSMA p-persistente funciona de la siguiente forma: existen "N" marcas dentro del área de cobertura de un lector, las cuales se desean identificar de manera ordenada usando una ventana de contienda de tamaño fijo. Por su parte, el lector difunde un comando de recolección de datos junto con el tamaño de la ventana de contienda y la probabilidad de transmisión. Tras recibir el comando de recolección de datos, cada marca selecciona una micro-ranura dentro de

la ventana de contienda de siguiendo la distribución *Sift*. Posteriormente, cada marca verifica el valor de la probabilidad de transmisión indicada por el lector. Por un lado, si "$p = 1$", las marcas transmiten dentro de la ranura seleccionada. En caso contrario, cada marca calcula la probabilidad de transmisión asociada a la micro-ranura seleccionada; si una marca decide transmitir, detecta o barre el medio hasta el número de micro-ranura seleccionada y transmite si y solo si el canal permaneció libre. En caso contrario se abstiene hasta recibir el siguiente comando de recolección de datos, es decir, hasta el siguiente ciclo de identificación.

La diferencia esencial entre el funcionamiento del protocolo CSMA no-persistente y CSMA *p*-persistente consiste en la probabilidad de transmisión que calcula cada una de las marcas, ya que en base a ésta decide si transmite en la micro-ranura seleccionada o no. Esta probabilidad no solo permite reducir el número de participantes dentro de una micro-ranura de contienda, sino que además permite a las marcas ahorrar energía.

En base a los resultados presentados en [22], observamos que un aumento en el número de marcas a identificar es directamente proporcional al número de colisiones, aún cuando la probabilidad de selección de las primeras micro-ranuras es muy baja. En este sentido, se ha observado que se requiere que la probabilidad de transmisión de cada marca esté en función de la micro-ranura seleccionada, y que gracias a la distribución *Sift*, una vez que una marca ha escogido una de las primeras micro-ranuras para transmitir, la probabilidad de que cambie de decisión sea casi nula.

Probabilidad de transmisión basada en la micro-ranura seleccionada

Con el fin de asignar diferentes probabilidades de transmisión a las diferentes micro-ranuras dentro de la ventana de contienda, en esta propuesta utilizamos (3.1) para que cada marca calcule la probabilidad de transmisión "p_t" en base a: tamaño de la ventana de contienda, y la micro-ranura seleccionada dentro de la ventana de contienda. Una vez que se ha calculado la probabilidad de transmisión, cada marca decide si transmite o no en base a esta probabilidad y a un número aleatorio.

$$p_t = \frac{K - r}{K} \tag{3.1}$$

- K: el número total de micro-ranuras en la ventana de contienda.
- r:$1 \ldots K$. La micro-ranura seleccionada para la transmisión.

En nuestra propuesta utilizamos la ventaja de la distribución *Sift*, ya que cuando una marca ha seleccionado una de las primeras micro-ranuras, la probabilidad de que cambie de decisión de transmisión es casi nula. Esto se debe a que la probabilidad de selección de una de las primeras micro-ranuras es muy baja.

Debido a la aleatoriedad introducida en nuestra propuesta, resulta complicado determinar la identificación del total de las marcas presentes, es decir, determinar cuando ya no hay marcas por identificar, ya que el uso de la probabilidad de transmisión no permite asegurar este hecho. Para resolver este problema, la probabilidad de transmisión se torna "$p_t = 1$"

cuando se tiene el primer ciclo de identificación vacío. De esta manera, aseguramos identificar todas las marcas presentes en el área de cobertura de un lector.

En la Figura 3.3 se presenta el esquema del funcionamiento del protocolo CSMA *p*-persistente propuesto. Como se puede observar, la probabilidad de selección de un *slot* tiende a ser mayor hacia los últimos *slots* de la ventana de contienda (debido a la distribución Sift), mientras que la probabilidad de transmisión tiende a ser mayor hacia los primeros *slots*.

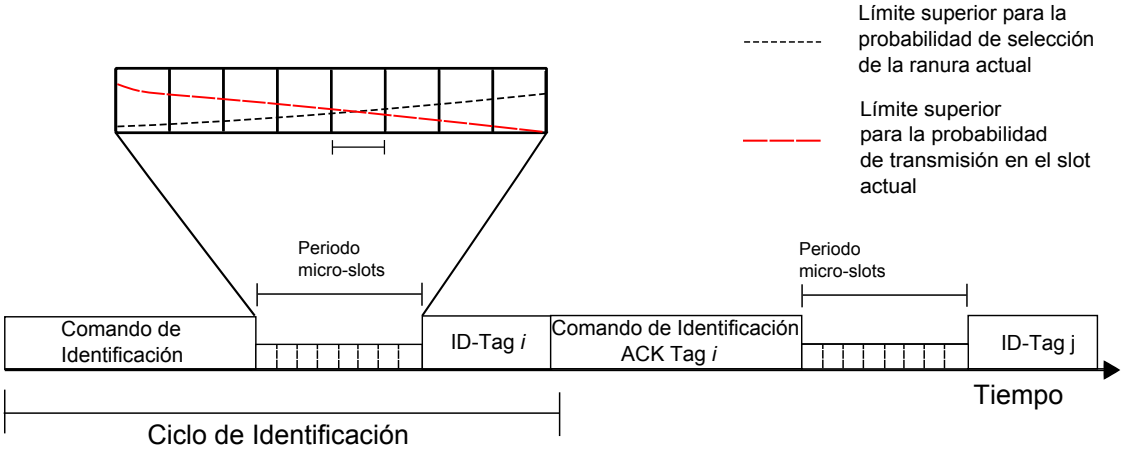


Figura 3.3: Funcionamiento del protocolo CSMA *p*-persistente con distribución *Sift*.

A continuación presentamos el algoritmo que conforma el protocolo propuesto CSMA *p*-persistente. A su vez, el algoritmo está conformado por los algoritmos que deben implementar el "Lector" y las "Marcas" bajo nuestra propuesta:

Algoritmo 1 Pseudocódigo para el protocolo CSMA p-persistente para RFID.

```
Reader procedure:
prob=0; //transmission probability
wS=8; //window size
M=64; //maximum number of participants
Response=1;
EmptyCI=0; //number of identification cycles empty
CommandCollection(wS, M, prob);
while EmptyCI < 2 or Response == 1 do
    tagCollision=0, tagIdentification=0, Response=0;
    for s = 1; s ≤ WindowSize; s++ do
        ReadSlot[s];
        if channelStatus[s]==1 then
            tagIdentification=1;
            tagCollision=0;
            Response=1;
            break;
        end if
        if channelStatus[s]==2 then
            tagIdentification=0;
            tagCollision=1;
            Response=1;
            break;
        end if
    end for
    if tagIdentification == 1 and tagCollision == 0 then
        commandCollection(wS, M, prob, ACK_ID);
    end if
    if tagCollision == 1 and tagIdentification == 0 then
        commandCollection(wS, M, prob);
    end if
    if Response == 0 and (tagIdentification == tagCollision ) then
        EmptyCI++;
        prob=1;
        commandCollection(wS,M,prob);
    end if
end while

Tag procedure:
identified=false;
receive(commandCollection(wS, M, prob));
while not identified do
    s=selectSlotSift(wS, M);
    if prob≠1 then
        p=randomNumber mod 1;
        prob_t = (wS−s)/wS
        if p > prob_t then
            break;
        else
            sendAnswer in Slot s;
        end if
    else
        sendAnswer in Slot s;
    end if
    recive Msg;
    if Msg == ACK_ID then
        identified=true;
    else
        recive(commandCollection(wS, M, prob));
    end if
end while
```

CAPÍTULO 4

EVALUACIÓN DE DESEMPEÑO

4.1. Parámetros

Debido a que en las redes RFID, una de las principales medidas de desempeño es el retardo de identificación, tomamos como medida de comparación el tiempo promedio para llevar a cabo la identificación del número total de marcas presentes en la zona de interrogación. De esta forma, en nuestra evaluación de desempeño, los ciclos de identificación se traducen a tiempo absoluto, ya que la duración de un ciclo de identificación depende directamente del número de ranuras utilizadas, de los mensajes intercambiados entre el lector y las marcas, y de la duración de los mismos.

Aunque la propuesta presentada en [22] y nuestra propuesta operan de forma diferente a los estándares utilizados dentro de entornos RFID activos, buscamos comparar estos protocolos de forma equitativa bajo los parámetros que se mencionan a continuación.

Comparamos nuestra propuesta contra los dos estándares utilizados dentro de los entornos RFID activos, así como con la propuesta presentada en [22]. Para todos los casos, los parámetros para la evaluación se toman de [22].

4.1.1. Parámetros de comparación ISO-18000-7

Para ISO-18000-7, tomando en cuenta que la velocidad de transmisión es de 27kbps, un ciclo de identificación dura un comando de recolección de datos (5ms), más el tiempo que dura cada ranura (8ms), y un paquete ACK por cada marca identificada (mensaje del lector a la i-ésima marca con el que se le indica que ya ha sido identificada, el cual dura 5ms).

Para CSMA no-persistente y CSMA p-persistente consideramos que un ciclo de identificación dura un comando de recolección de datos (5ms), más lo que dura un paquete ID (respuesta de una o varías marcas al lector, lo cual dura 8ms), más lo que dura cada micro-ranura en la ventana de contienda (1ms), y lo que dura un paquete ACK (en caso de

haber realizado una identificación exitosa, que dura 8ms).

4.1.2. Parámetros de comparación EPC Gen2

Para el caso del EPC "Gen 2" las ranuras vacías y con colisión son más cortas que las ranuras con un ID correcto. Si la capacidad del canal es de 40kbps, una ranura con un ID correcto dura 2.505ms, mientras que las ranuras vacías y con colisión duran 0.575ms.

Para CSMA no-persistente y CSMA p-persistente consideramos que un ciclo de identificación dura un comando de recolección de datos (0.55ms), más lo que dura un paquete ID (respuesta de una marca al lector, lo cual dura 1.4ms), más la duración de cada micro-ranura en la ventana de contienda (0.1ms), y lo que dura un paquete ACK (en caso de haber realizado una identificación exitosa, que dura 1.4ms).

4.2. Implementación

Ya que simulamos un proceso de identificación, la duración de una simulación con respecto las otras varía debido a que cada una de ellas finaliza cuando se han identificado todas las marcas, lo que se debe a la aleatoriedad introducida por los protocolos simulados y a que las simulaciones son procesos aleatorios independientes.

Implementamos los protocolos ISO-18000-7, EPC "Gen2" con y sin selección de Q óptima, CSMA no-persistente y CSMA p-persistente en la herramienta MATLAB, con los siguientes valores:

- ISO-18000-7. Se considera que el tamaño de la trama es fijo e igual a $k = 64$ ranuras, lo que implica que no cambia durante el proceso de identificación. Se toma $k = 64$ ranuras debido a que en [22] realizaron pruebas para diferentes valores de k, y éste mostró tener mejores resultados bajo el rango de marcas a evaluar.

- EPC Gen2. Bajo este esquema se utiliza el mecanismo de adaptación de trama indicado en [21] para redimensionar el tamaño de la trama al final de cada CI.

- EPC Gen2 con selección de Q óptima. Para redimensionar el tamaño de la trama al final de cada CI se utiliza el mecanismo de adaptación de trama indicado en [21], mientras que para seleccionar el valor óptimo de Q se utiliza el estimador presentado en [19].

- CSMA no-persistente. Se considera que el tamaño de la ventana de contienda es fijo e igual a $k = 8$ micro-ranuras, y que el valor del parámetro M requerido por la distribución *Sift* es igual a 64. Al igual que para el caso del ISO-18000-7, se toma $k = 8$,micro-ranuras debido a que en [22] realizaron pruebas para diferentes valores de k, y éste mostró tener mejores resultados bajo el rango de marcas a evaluar.

- CSMA p-persistente. Se considera que el tamaño de la ventana de contienda es fijo e igual a $k = 8$ micro-ranuras, y que el valor del parámetro M es igual a 64. Estos valores se toman de ésta forma debido a que buscamos una comparación equitativa.

Bajo las siguientes consideraciones:

- Suponemos que los dispositivos participantes implementan un CCA (*Clear Channel Assessment*) coherente, es decir, que el canal se considera ocupado cuando el preámbulo del paquete se detecta.
- Se considera que la red se encuentra libre del efecto de captura[1].
- El número de marcas a identificar varía de 10 a 100 en intervalos de 10 marcas.
- Con el fin de obtener resultados confiables, se ejecutaron 300,000 simulaciones de cada protocolo para obtener intervalos de confianza del 95 % con precisión menor a 1 segundo.

Con el fin de establecer una comparativa entre el retardo de identificación (RID) utilizado por cada uno de los protocolos implementados, calculamos la distancia relativa que existe entre nuestra propuesta y los estándares, así como con las propuesta presentada en [22]. Definimos la distancia relativa como:

$$distancia\_relativa = \frac{RID_P - RID_{PP}}{RID_P} * 100 \tag{4.1}$$

con:

- RID_P: retardo de identificación del protocolo con el que se compara el protocolo propuesto.
- RID_{PP}: retardo de identificación del protocolo propuesto CSMA p-persistente.

Para mayor información con respecto a la forma en la que se realizaron las simulaciones, ver el Anexo A.

4.3. Resultados

En esta sección se presentan los resultados obtenidos mediante simulación numérica. Por un lado, en la subsección **Resultados generales** presentamos los resultados obtenidos que no dependen del tiempo, mientras que en la subsección **Resultados particulares** presentamos los resultados obtenidos que dependen directamente del tiempo, es decir, de los parámetros de evaluación establecidos en la sección anterior.

[1]El efecto de captura dentro del ámbito de redes RFID, se refiere al evento que ocurre cuando 2 o más marcas intentan transmitir a un lector de manera simultánea y una de ellas lo logra debido a que se encuentra en mejores condiciones físicas (tales como la potencia de transmisión, cercanía al lector).

4.3.1. Resultados generales

En la Tabla 4.1 se presentan los resultados obtenidos con respecto al número promedio de ranuras utilizadas por cada uno de los protocolos implementados. En la primer columna se tiene el número total de marcas presentes en la zona de interrogación del lector, mientras que los resultados obtenidos con respecto al número promedio de ranuras utilizadas por cada uno de los protocolos implementados, se presentan en las columnas subsecuentes.

No. de marcas	**ISO - 18000-7 (k=64 ranuras)**	**EPC Gen2**	**EPC Gen2 con Q óptima**	**CSMA no-persistente (k=8 micro-ranuras)**	**CSMA p-persistente (k=8 micro-ranuras)**
10	98.778981	27.651267	26.162527	73.894537	79.745753
20	137.865335	63.869613	52.018180	122.144417	128.402363
30	167.088911	159.027860	83.634147	163.359070	170.772787
40	196.087752	354.658400	114.183060	200.460227	209.305600
50	221.626693	642.373613	146.748913	234.998967	244.904960
60	249.677682	882.920107	182.055460	267.865397	278.497127
70	276.498861	1001.482607	213.455640	299.350137	310.531880
80	305.051109	1045.530413	245.496080	329.982777	341.501523
90	334.759321	1061.165560	277.713247	360.101160	371.586790
100	366.153207	1067.905947	312.185740	389.753003	400.855177

Tabla 4.1: Número promedio de ranuras utilizadas.

Estos resultados muestran, que el estándar EPC "Gen 2" sin selección de Q óptima utiliza mayor cantidad de ranuras que el estándar EPC "Gen 2" con selección de Q óptima y que el ISO-18000-7, mientras que el protocolo CSMA p-persistente utiliza más micro-ranuras que el protocolo CSMA no-persistente.

Si bien, los resultados en esta comparación indican que los protocolos CSMA son peor que los estándares utilizados dentro de los entornos RFID activos, es importante recordar que debido a que los protocolos CSMA y los estándares funcionan de forma diferente, el tiempo que utiliza una ranura bajo estos esquemas es diferente, siendo menor para los protocolos CSMA que para los estándares. Es evidente que la diferencia entre el número de micro-ranuras utilizadas por el protocolo CSMA p-persistente con respecto al protocolo CSMA no-persistente es muy pequeña y casi irrelevante tomando en cuenta el tiempo de duración de cada ranura.

En la Tabla 4.2 se presentan los resultados obtenidos con respecto al número promedio ciclos de identificación utilizados por cada uno de los protocolos implementados. En la primer columna se tiene el número total de marcas presentes en la zona de interrogación del lector, en la segunda, tercer, cuarta, quinta y sexta columna se presentan el número de ciclos de identificación promedio utilizados por el estándar ISO-18000-7, el estándar EPC "Gen 2", el

estándar EPC "Gen 2" con selección de Q óptima, el protocolo CSMA no-persistente con distribución *Sift*, y el protocolo CSMA p-persistente con distribución *Sift*, respectivamente

No. de marcas	ISO-18000-7 (k=64 ranuras)	EPC Gen2	EPC Gen2 con Q óptima	CSMA no-persistente (k=8 micro-ranuras)	CSMA p-persistente (k=8 micro-ranuras)
10	1.543422	4.265330	4.350863	14.228187	14.638630
20	2.154146	4.824527	6.688123	28.094347	27.596613
30	2.610764	4.236790	8.253900	42.379887	40.691697
40	3.063871	3.814837	8.855070	57.082113	54.081633
50	3.462917	3.701630	9.848060	72.227253	67.826613
60	3.901214	3.664493	10.617110	87.873313	82.013213
70	4.320295	3.859927	10.921193	103.965340	96.656640
80	4.766424	4.280947	11.082593	120.582633	111.752980
90	5.230614	4.847853	11.765113	137.751800	127.326633
100	5.721144	5.439763	12.157490	155.493693	143.337283

Tabla 4.2: Número promedio de ciclos de identificación utilizados.

Nuevamente, aunque los resultados con respecto al número de ciclos de identificación promedio indican que los protocolos CSMA son peor que los estándares utilizados dentro de los entornos RFID activos, es importante recordar que debido a que los protocolos CSMA y los estándares funcionan de forma diferente, la duración de los ciclos de identificación es diferente.

Los resultados de simulación muestran que, conforme el conjunto de marcas a identificar es más grande, el protocolo CSMA p-persistente utiliza menos ciclos de identificación que el protocolo CSMA no-persistente, indicando que nuestra propuesta realiza la identificación de las mismas más rápido, utilizando menos ventanas de contienda y logrando un menor retardo de identificación (ver Tabla 4.3 y Tabla 4.6), ya que el tiempo o retardo de identificación es directamente proporcional al número de ciclos de identificación, al número de ranuras y mensajes utilizados para llevar a cabo el proceso de identificación. Por otro lado, el protocolo EPC "Gen 2" con selección de Q óptima utiliza más ciclos de identificación que el protocolo EPC "Gen 2" sin selección de Q óptima y que el ISO-18000-7.

En la Figura 4.1 se presenta una comparación entre los ciclos de identificación utilizados por los protocolos CSMA no persistente y CSMA p-persistente. Al inicio de la gráfica, se pude apreciar que el protocolo CSMA p-persistente utiliza más ciclos de identificación que la propuesta presentada en [22], lo que sucede cuando el número de marcas es muy pequeño, pero conforme el número de marcas aumenta la mejora es evidente.

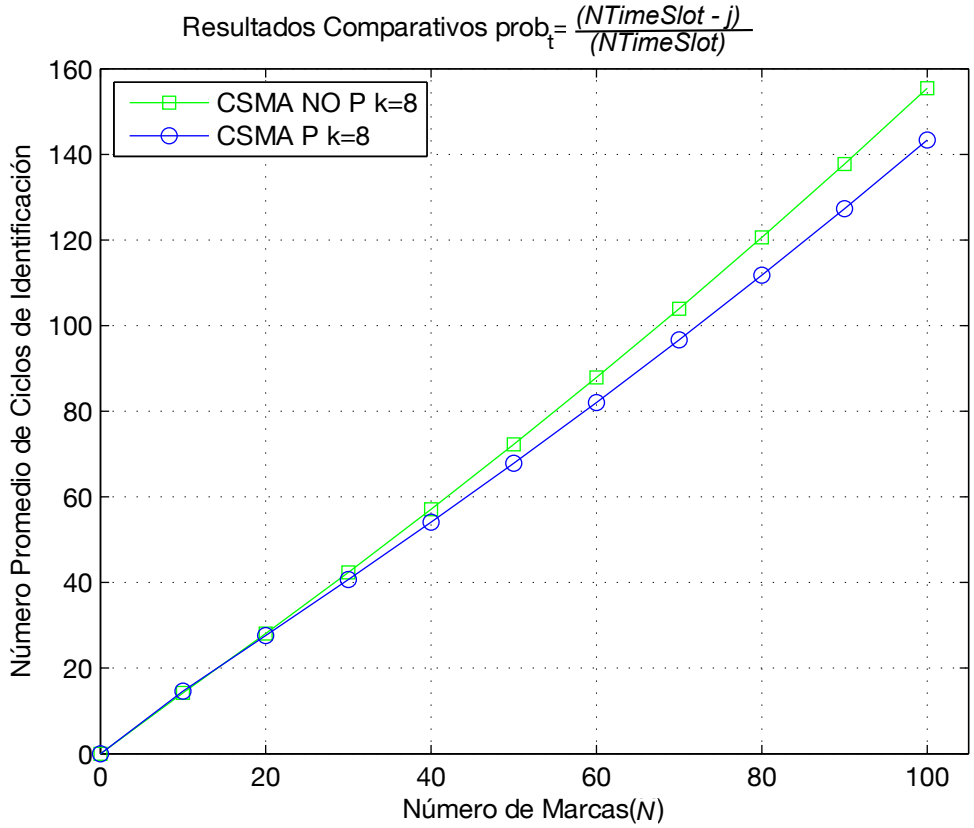


Figura 4.1: Gráfica comparativa entre el protocolo CSMA no-persistente y CSMA *p*-persistente con respecto a los ciclos de identificación utilizados.

En esta gráfica no se incluye el número de ciclos de identificación utilizados por el estándar ISO-18000-7 y el estándar EPC "Gen 2", ya que éstos operan de forma diferente a los protocolos CSMA, sin embargo, en secciones posteriores presentamos una comparación en base al retardo de identificación en la que se reflejan los resultados obtenidos.

4.3.2. Resultados particulares

Resultados con respecto a ISO-18000-7

Los resultados que se muestran en la Tabla 4.3, corresponden al retardo de identificación obtenido por cada uno de los protocolos bajo los parámetros establecidos por el estándar ISO-18000-7. En la primer columna se tiene el número de marcas presentes en la zona de interrogación del lector, en la segunda, tercera y cuarta columna se presenta el tiempo utilizado por el estándar ISO-18000-7, el protocolo CSMA no-persistente con distribución *Sift*, y el protocolo CSMA *p*-persistente con distribución *Sift* para identificar el total de marcas presentes en la zona de interrogación, respectivamente.

Marcas presentes	**ISO-18000-7 (ms)**	**CSMA no-persistente con distribución *Sift* (ms)**	**CSMA *p*-persistente con distribución *Sift* (ms)**
10	847.948956	330.808951	334.014256
20	1213.693407	639.197368	631.323067
30	1499.765110	945.911693	923.893791
40	1784.021374	1254.370465	1216.396249
50	2040.328132	1566.101459	1510.849735
60	2316.927527	1882.241174	1808.886503
70	2583.592363	2202.834885	2111.343442
80	2864.240989	2529.723037	2418.572218
90	3154.227637	2863.129935	2730.347502
100	3457.831374	3202.537273	3048.287542

Tabla 4.3: Retardo de identificación.

En la Figura 4.2 se presentan los resultados de la Tabla 4.3. Al comienzo de la gráfica, el protocolo CSMA *p*-persistente tiene un deterioro en el rendimiento en comparación con la propuesta en [22], lo que sucede cuando el número de marcas es muy pequeño, pero conforme el número de marcas aumenta la mejora es evidente. El deterioro en el rendimiento de nuestra propuesta sucede cuando el conjunto de marcas es de tamaño 10, y la mejora en el rendimiento ocurre a partir del conjunto de marcas de tamaño 20.

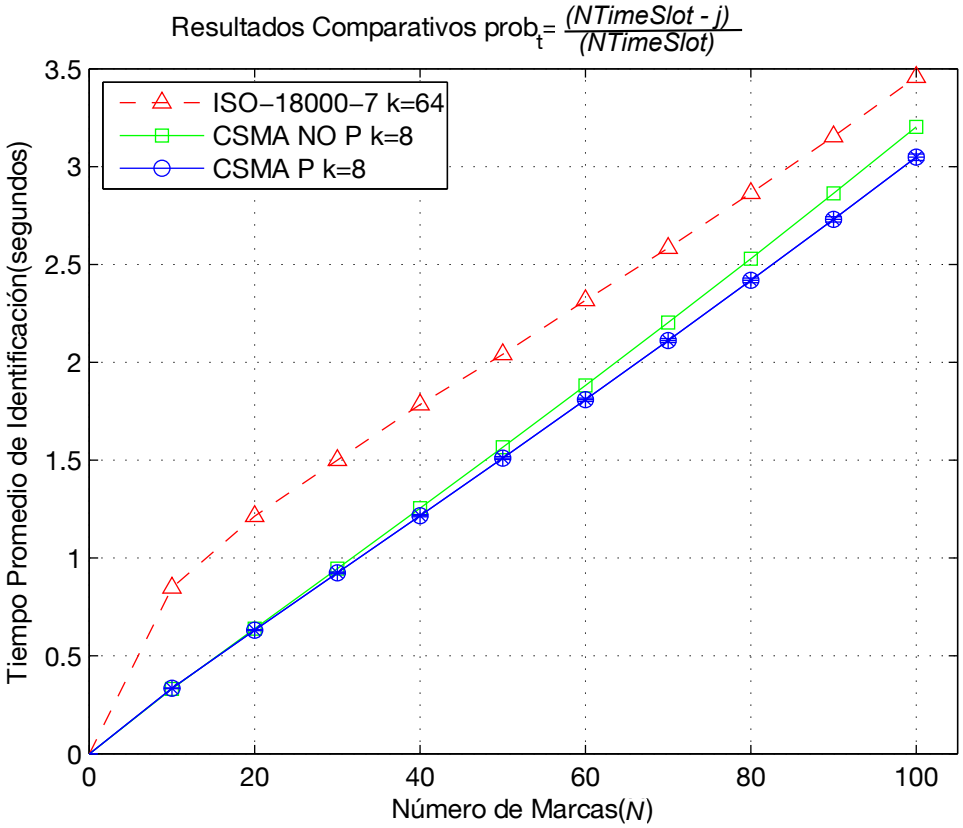


Figura 4.2: Retardo de identificación de los protocolos ISO-18000-7, CSMA no-persistente y CSMA p-persistente.

En la Tabla 4.4 se presentan los resultados comparativos entre los protocolos implementados con respecto al retardo de identificación. En la primer columna se tiene el número de marcas presentes en la zona de interrogación del lector, en la segunda columna se presenta la distancia relativa (porcentaje) entre los resultados obtenidos a partir del estándar ISO-18000-7 y el protocolo CSMA p-persistente, mientras que en la tercer columna se presenta la distancia relativa (porcentaje) entre los resultados obtenidos a partir de la propuesta presentada en [22] y el protocolo CSMA p-persistente.

Marcas presentes	Distancia relativa ISO-18000-7 y CSMA p-persistente (%)	Distancia relativa CSMA no-persistente y CSMA p-persistente (%)
10	60.6092	-0.9689293
20	47.9833	1.231904
30	38.3974	2.327691
40	31.8172	3.027353
50	25.9506	3.527979
60	21.9274	3.897198
70	18.2788	4.153350
80	15.5598	4.393794
90	13.4385	4.637667
100	11.8440	4.816485

Tabla 4.4: Distancia relativa del protocolo CSMA p-persistente con respecto al estándar ISO-18000-7 y CSMA no-persistente.

Finalmente, en la Tabla 4.5 se presentan los resultados obtenidos para el retardo de identificación del protocolo CSMA p-persistente bajo los parámetros del estándar ISO-18000-7, junto con intervalos de confianza del 95 % y una precisión de 1 ms.

Número total de marcas presentes	Retardo de identificación (segundos) con intervalos de confianza de 95 % con precisión del 1 ms	Varianza (segundos)
10	0.334014 ± 0.000167	0.001453
20	0.631323 ± 0.000236	0.002900
30	0.923894 ± 0.000286	0.004270
40	1.216396 ± 0.000328	0.005621
50	1.510850 ± 0.000369	0.007090
60	1.808887 ± 0.000407	0.008645
70	2.111343 ± 0.000444	0.010266
80	2.418572 ± 0.000482	0.012120
90	2.730348 ± 0.000521	0.014172
100	3.048288 ± 0.000561	0.016384

Tabla 4.5: Resultados CSMA p-persistente.

Los resultados de la Tabla 4.3 y de la Tabla 4.4 muestran que el retardo de identificación del protocolo CSMA p-persistente, en general, es menor con respecto al retardo de identificación del estándar ISO-18000-7, y del protocolo CSMA no-persistente presentado en [22].

Los resultados de la Tabla 4.5, muestran que nuestra propuesta tiene una mejora de hasta un 60 % y en el peor de los casos de hasta un 11 % con respecto al retardo de identificación del estándar ISO-18000-7. Para los resultados presentados en [22], nuestra propuesta tiene una mejora de hasta un 5 %, mientras que en el peor de los casos se tiene una disminución en el desempeño de hasta el 1 %, lo cual ocurre cuando el número de marcas a identificar es pequeño. Ya que un conjunto de 10 marcas no es muy representativo, el deterioro en el rendimiento realmente no es significativo, ya que para 10 marcas el retardo de identificación obtenido por ambos protocolos CSMA es de 0.3 segundos.

Resultados con respecto a EPC "Gen 2"

En la Tabla 4.6 se presentan los resultados obtenidos para el retardo de identificación bajo los parámetros establecidos por el estándar EPC "Gen 2". En la primer columna se tiene el número de marcas presentes en la zona de interrogación del lector, en la segunda columna se presenta el tiempo utilizado por el estándar EPC "Gen 2" en la tercer columna el tiempo utilizado por el estándar EPC "Gen 2" con selección de Q, en la cuarta columna el tiempo utilizado por el protocolo CSMA no-persistente con distribución *Sift*, y en la quinta columna el tiempo utilizado por el protocolo CSMA p-persistente con distribución *Sift* para identificar el total de marcas presentes en la zona de interrogación.

No. de marcas	EPC Gen 2 (ms)	EPC Gen 2 con Q óptima (ms)	CSMA no-persistente (ms)	CSMA p-persistente (ms)
10	35.199478	34.343453	43.214956	44.025822
20	75.325028	68.510454	83.666332	84.018374
30	149.341020	105.989634	123.644845	123.457712
40	281.128580	142.855260	163.441185	162.675458
50	465.864828	180.880625	203.224886	201.795133
60	623.479061	220.481890	243.116862	240.956980
70	710.952499	257.836993	283.115951	280.214340
80	755.579988	295.560246	323.318726	319.614291
90	783.870197	333.385117	363.773606	359.188327
100	807.045919	372.506801	404.496832	398.921024

Tabla 4.6: Retardo de identificación.

En la Figura 4.3 se presentan los resultados de la Tabla 4.6. Como se puede apreciar, para el caso de los protocolos CSMA, los resultados presentados en la Figura 4.3 son similares a los presentados en la Figura 4.2 con diferente escala de tiempo.

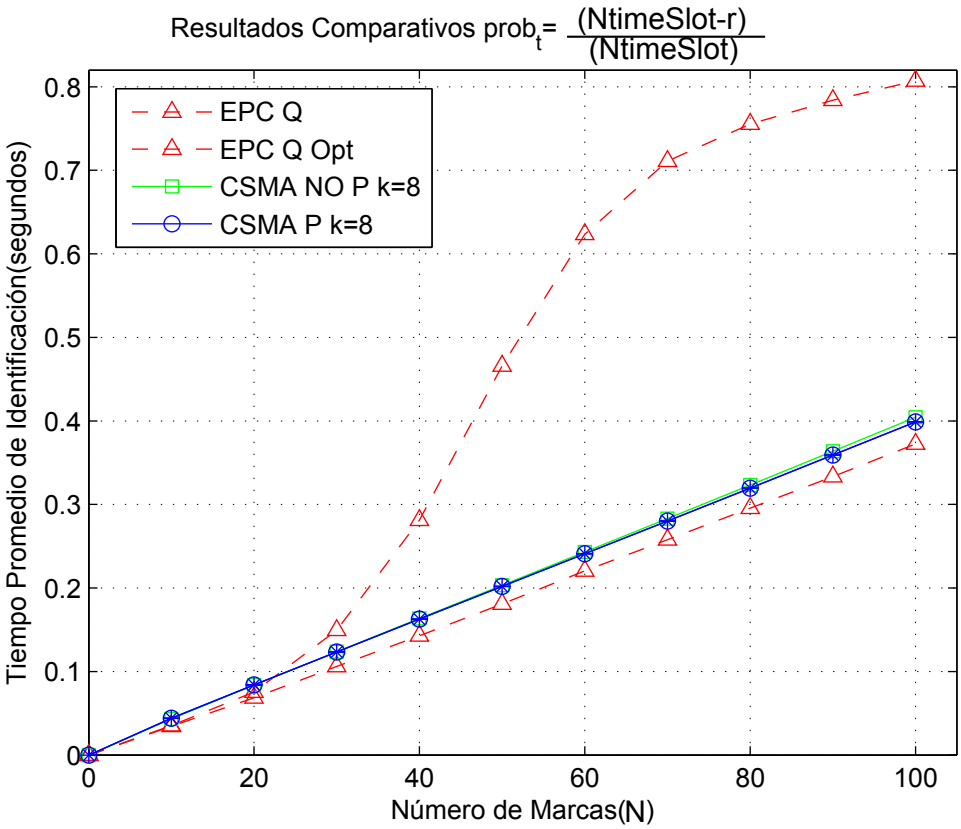


Figura 4.3: Retardo de identificación de los protocolos EPC Gen 2, EPC Gen 2 con Q óptima, CSMA no-persistente y CSMA p-persistente.

En la Tabla 4.7 se presentan los resultados comparativos entre los protocolos implementados. En la primer columna se tiene el número de marcas presentes en la zona de interrogación del lector, en la segunda columna se presenta la distancia relativa (porcentaje) entre los resultados obtenidos a partir del estándar EPC "Gen 2" y el protocolo CSMA p-persistente, en la tercer columna se presenta la distancia relativa (porcentaje) entre los resultados obtenidos a partir del estándar EPC "Gen 2" con selección de Q óptima y el protocolo CSMA p-persistente, mientras que en la cuarta columna se presenta la distancia relativa (porcentaje) entre los resultados obtenidos a partir de la propuesta presentada en [22] y el protocolo CSMA p-persistente.

No. de marcas	Distancia relativa EPC Gen 2 y CSMA p-persistente (%)	Distancia relativa EPC Gen 2 con Q óptima y CSMA p-persistente (%)	Distancia relativa CSMA no-persistente y CSMA p-persistente (%)
10	-25.07521	-28.19277	-1.876354
20	-11.54111	-22.63585	-0.4207682
30	17.33168	-16.48093	0.1513471
40	42.13527	-13.87432	0.4685029
50	56.68375	-11.56260	0.7035323
60	61.35283	-9.286518	0.8884131
70	60.58606	-8.678874	1.024884
80	57.69947	-8.138458	1.145753
90	54.17757	-7.739761	1.260476
100	50.57021	-7.090937	1.378455

Tabla 4.7: Distancia relativa del protocolo CSMA p-persistente con respecto al estándar EPC Gen 2, EPC Gen 2 con selección de Q óptima y CSMA no-persistente.

Los resultados de la Tabla 4.6 y de la Tabla 4.7, muestran que se tiene una mejora con nuestra propuesta sobre el estándar EPC "Gen 2" y el protocolo CSMA no-persistente, sin embargo, no es así sobre el estándar EPC "Gen 2" con selección de Q óptima.

Finalmente, en la Tabla 4.8 se presentan los resultados obtenidos para el retardo de identificación del protocolo CSMA p-persistente bajo los parámetros del EPC "Gen 2" junto con intervalos de confianza del 95 % y una precisión de 0.1 ms.

Número total de marcas presentes	Retardo de identificación (segundos) con intervalos de confianza de 95 % con precisión del 0.1 ms	Varianza (segundos)
10	0.044026 ± 0.000008	0.000006
20	0.084018 ± 0.000012	0.000010
30	0.123458 ± 0.000014	0.000015
40	0.162675 ± 0.000016	0.000019
50	0.201795 ± 0.000017	0.000023
60	0.240957 ± 0.000019	0.000027
70	0.280214 ± 0.000020	0.000032
80	0.319614 ± 0.000022	0.000037
90	0.359188 ± 0.000023	0.000042
100	0.398921 ± 0.000025	0.000048

Tabla 4.8: Resultados CSMA p-persistente.

Los resultados obtenidos mediante simulación que se presentan en la Tabla 4.7, muestran que se tiene una mejora de hasta un 61 % y una baja en el rendimiento de hasta un 25 % con respecto al retardo de identificación del estándar EPC "Gen 2". Con respecto al retardo de identificación del estándar EPC "Gen 2" con selección de Q óptima, los resultados muestran que no se tiene ninguna mejora. Para los resultados presentados en [22], se tienen una mejora de hasta un 1 %, mientras que en el peor de los casos se tiene una disminución en el desempeño de hasta el 1 %.

La disminución en el desempeño de nuestra propuesta, en el caso del estándar EPC "Gen 2" y del protocolo CSMA no-persistente, ocurre en casos en el que el número de marcas a identificar es pequeño (10-20 marcas), y el tiempo necesario para identificar ese conjunto de marcas no es demasiado, por lo que el rendimiento se ve ligeramente afectado debido a la escala de tiempo manejada, sin embargo, la mejora es evidente conforme el número de marcas a identificar aumenta.

4.4. Conclusiones preliminares

En general, los resultados obtenidos mediante simulación para ambas comparaciones (ISO-18000-7 y EPC "Gen 2"), muestran que nuestra propuesta es superior a la propuesta presentada en [22] y a los estándares utilizados en entornos RFID activos con respecto al retardo de identificación, y no así para la versión mejorada del estándar EPC "Gen 2".

Debido a que para identificar un conjunto de marcas, nuestra propuesta utiliza menos ciclos de identificación que la propuesta presentada en [22], y a que el retardo de identificación es directamente proporcional al número de ciclos de identificación utilizados para ello, se tiene una mejora con respecto a dicha propuesta aún cuando nuestra propuesta utiliza más ranuras

para ello.

La mejora que se obtiene con el protocolo CSMA p-persistente propuesto, se debe a que reduce el número de contendientes dentro de una micro-ranura de contención, los cuales aumentan conforme el número de marcas a identificar aumenta. Si bien es cierto que la distribución *Sift* permite reducir el número de contendientes dentro de una micro-ranura de contienda, también lo es que conforme el número de marcas a identificar aumenta, también lo hace el número de contendientes dentro de una micro-ranura, provocando que sucedan colisiones al principio de la ventana de contienda y no identificaciones exitosas como se espera con el uso de la distribución *Sift*.

Falta por mejorar el funcionamiento de nuestra propuesta con el fin de lograr un menor retardo de identificación aún cuando el conjunto de marcas a identificar es pequeño, ya que cuando esto ocurre se tienen un deterioro en el desempeño de nuestra propuesta con respecto al estándar EPC "Gen 2" y la propuesta presentada en [22].

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES PARA TRABAJO FUTURO

En este trabajo se ha presentado una revisión de los protocolos anticolisión existentes para redes RFID. De igual manera, se presentó el desarrollo de una propuesta basada en el protocolo CSMA p-persistente con distribución *Sift*. En base al modelo de simulación propuesto y a los resultados obtenidos, se observa que se tiene un mejor comportamiento al del protocolo CSMA no-persistente presentado en [22], con una mejora en el desempeño de hasta el 4.8 % para el caso de comparación bajo los parámetros del estándar ISO-18000-7, y del 1.3 % para el caso de comparación bajo los parámetros del EPC "Gen 2". De igual forma, se tiene una mejora de hasta un 11.8 % y 50.57 % para el caso del estándar ISO-18000-7 y EPC Gen2, respectivamente.

Observamos que el tiempo involucrado en un ciclo de identificación afecta directamente el desempeño de cualquier protocolo, ya que se intercambia una mayor cantidad de mensajes entre el lector y las marcas, por lo que al disminuir el número de ciclos de identificación se mejora el desempeño de cualquier protocolo. Por otro lado, se observó que entre mayor sea el tiempo utilizado en un ciclo de identificación (tal como la duración de los mensajes intercambiados entre los dispositivos, duración de las ranuras dentro de la ventana de contienda o trama), la mejora con respecto a otros protocolos es más evidente.

Resta trabajo por hacer, tal como medir la tasa de pérdidas y el caudal de datos de nuestra propuesta.

APÉNDICE A

CÓDIGO CSMA *P*-PERSISTENTE

En el Cuadro A.1 se muestra el código del protocolo CSMA p-persistente para MATLAB. Como se puede observar, el Cuadro A.1 presenta la función CSMAP, la cual recibe como parámetros el número de marcas presentes en la zona de interrogación del lector, y el número de veces que se repetirá el proceso. Esta función utiliza las siguientes funciones para realizar la simulación y calcular el tiempo utilizado en cada simulación:

- RFIDSim. Esta función permite que las marcas seleccionen una ranura dentro de la ventana de contienda, para lo cual utilizan la distribución *Sift*. Como se puede observar, esta función recibe como parámetros el número total de micro-ranuras dentro de la ventana de contienda, el número total de marcas presentes, el parámetro "M" utilizados por la distribución *Sift*, y la probabilidad de transmisión.
- RFIDCalcTime. Esta función calcula el tiempo utilizado por el protocolo CSMA p-persistente durante un CI. Recibe como parámetros el número de micro-ranuras "n" utilizadas hasta una ranura con una identificación exitosa o con colisión, un indicador de identificación exitosa, y un indicador de colisión.
- RFIDCalcData. Esta función calcula la cantidad de bytes transmitidos de las marcas al lector en un CI. Recibe como parámetros el tipo de comando que se está enviando y el número de marcas identificadas.

Para el caso de las funciones RFIDCalcTime y RFIDCalcData los parámetros se toman según el estándar con el que se desee comparar.

```
%*************************************************************************
%*************************************************************************
%Autor: Leonardo Sánchez
%Fecha: 20101108
%*************************************************************************
%       Este programa permite simular un proceso de identificación
```

```
%       realizado por el protocolo CSMA P Persistente
%*************************************************************************


function [AverageBytesReadertoTag, AverageBytesTagtoReader,
        AverageNumberTag, NTimeranuraTotal, AverageCI, resultTime,
        med, var]=CSMAP(NTag,repeatN)

%Inicialización de variables a utilizar
WindowSize=8;               %Tamaño de la ventana de contienda
M=64;                       %Parámetro requerido por la distribución Sift
                            %que representa el máximo número de participantes
                            %Generalmente dada a priori por el usuario.

time=0;                     %Tiempo utilizado por CI
totalTime=0;                %Tiempo utilizado para llevar a cabo el proceso de
                            %identificación

resultTime=0;
AverageCI=0;
NTimeranuraTotal=0;         %Numero de ranuras totales utilizados durante toda
                            %la simulación
AverageNumberTag=0;         %Numero promedio de marcas identificadas para el
                            %el número total de experimentos


AverageBytesReadertoTag=0;  %Número de bytes promedio transmitidos del
                            %lector a las marcas
AverageBytesTagtoReader=0;  %Número de bytes promedio transmitido de
                            %las marcas al lector

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%Medidas Estadísticas
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
med_ant=0;
med=0;
var=0;

for iteration=1:repeatN
    NTimeranura=WindowSize;     %Tamaño actual de la venática
    NCollision=0;               %Indicador de colisión
    NIdent=0;                   %Indicador de identificación exitosa
    totalTag=NTag;              %Contador de marcas identificadas
    NCI=0;                      %Numero de ciclos de identificación
                                %utilizados
    NTimeranuraTotalCI=0;       %Numero total de ranuras utilizados en un
                                %ciclo de identificación
    numberTags=0;               %Contador de marcas identificadas hasta
                                %el momento
    numberEmpty=ones(1,NTimeranura);
    nEmpty=0;                   %Número de CI vacíos
```

```
prob=0;                         %Probabilidad de transmisión
atime=0;                        %Promedio de tiempo por repetición

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%Posibles comandos utilizados durante el proceso de identificación
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
commandRequest='request';
commandResponse='response';

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%Número de bytes intercambiados entre el lector y las marcas
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
bytesReadertoTag=0;             %Lector a marcas
bytesTagtoReader=0;             %Marcas al lector

bytesReadertoTagCI=0;           %Lector a marcas por CI
bytesTagtoReaderCI=0;           %Marcas al lector por CI


%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%Calculamos el numero de bytes para un comando de recolección de
%datos. En este paso se inicia el proceso de identificación.
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
[bytesReadertoTagCI,bytesTagtoReaderCI]=RFIDcalcData(commandRequest, 0);
bytesReadertoTag=bytesReadertoTag+bytesReadertoTagCI;
bytesTagtoReader=bytesTagtoReader+bytesTagtoReaderCI;


%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%El proceso de identificación termina cuando se tienen 2 CI vacíos
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
while(sum(numberEmpty==zeros(size(numberEmpty)))<NTimeranura || nEmpty<2)
    NCI=NCI+1;

    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    %Simulamos la selección de la ranura en el que va a transmitir cada una
    %de las marcas
    %Se les indica la probabilidad con la que deben transmitir:
    %   -0. Cuando no se ha tenido un CI vacío
    %   -1. A partir de que se ha tenido el primer CI vacío.
    %La idea es que la probabilidad de trasmisión de cada marca sea
    %la correspondiente a la ranura seleccionada, y cambie a partir del
    %primer CI vació.
    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    [ranuraInf]=RFIDsim(NTimeranura,totalTag,M,prob);

    numberEmpty=ranuraInf;
    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    %En esta parte simulamos la respuesta de las marcas.
    %Cada marca sensa el canal hasta el número de ranura seleccionado:
    %   - Transmite si el canal permaneció vació hasta el número de
```

```
%   ranura seleccionado
%   -Se retira del proceso de identificación en otro caso.
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
NIdent=0;
NCollision=0;
for n=1:NTimeranura
    if(ranuraInf(n)>1)
        NIdent=0;
        NCollision=1;
        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        %Calculamos el numero de bytes para un comando de
        %recolección del lector a las marcas debido a una colisión
        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        [bytesReadertoTagCI,bytesTagtoReaderCI] =
                        RFIDcalcData(commandRequest, NIdent);
        bytesReadertoTag=bytesReadertoTag+bytesReadertoTagCI;
        bytesTagtoReader=bytesTagtoReader+bytesTagtoReaderCI;
        break;
    elseif(ranuraInf(n)==1)
        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        %Siempre se identifica una marca a la vez
        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        NIdent=1;
        NCollision=0;
        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        %Calculamos el numero de bytes transmitidos por la respuesta
        %de una de las marcas al lector
        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        [bytesReadertoTagCI,bytesTagtoReaderCI]=
                        RFIDcalcData(commandResponse, NIdent);
        bytesReadertoTag=bytesReadertoTag+bytesReadertoTagCI;
        bytesTagtoReader=bytesTagtoReader+bytesTagtoReaderCI;

        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        %Una vez que una marca ha enviado exitosamente su
        %identificador al lector, calculamos el numero de bytes para
        %un comando de recolección del lector a la marca identificada
        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        [bytesReadertoTagCI,bytesTagtoReaderCI]=
                        RFIDcalcData(commandRequest, NIdent);
        bytesReadertoTag=bytesReadertoTag+bytesReadertoTagCI;
        bytesTagtoReader=bytesTagtoReader+bytesTagtoReaderCI;
        break;
    end;
end;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%Cuando se tienen 2 CI vacíos se  termina el proceso de
%identificación.
%Con el fin de identificar todas las marcas presentes en la zona de
%interrogación de un lector, se transmite con probabilidad p=1 a
```

```
        %partir del primer CI vació. Cuando se tienen 2 CI se termina el
        %proceso de identificación.
        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        if(sum(numberEmpty==zeros(size(numberEmpty)))==NTimeranura)
            nEmpty=nEmpty+1;
            prob=1;
            %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
            %Calculamos el numero de bytes para un comando de
            %recolección del lector a las marcas debido a un ci vació
            %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
            [bytesReadertoTagCI,bytesTagtoReaderCI]=
                            RFIDcalcData(commandRequest, NIdent);
            bytesReadertoTag=bytesReadertoTag+bytesReadertoTagCI;
            bytesTagtoReader=bytesTagtoReader+bytesTagtoReaderCI;
        end;

        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        %Esta parte simula el comando ACK-Collection, en el que se le
        %indica a una marca que ha sido identificada y al mismo tiempo se
        %solicitan más datos
        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        %Si NIdent=0 quiere decir que ocurrió una colisión antes de que
        %una marca enviara su identificador
        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        totalTag=totalTag-NIdent;

        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        %Contamos las marcas identificadas hats el momento
        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        numberTags=numberTags+NIdent;

        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        %El número de ranuras utilizados por el protocolo es el último que se
        %ejecutó, es decir, en el cual o bien se tiene una sola transmisión
        %o bien se tiene una colisión
        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        NTimeranuraTotalCI=NTimeranuraTotalCI+n;

        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        %En esta parte calculamos el tiempo utilizado en el ciclo de
        %identificación actual.
        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        %Hay que recordar que si no se utilizan todos los ranuras, solo hay
        %que contemplar el valor de 'n' como el número de micro ranuras
        %utilizados en el ciclo de identificación actual
        %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        time=RFIDcalcTime(n,NIdent,NCollision);
        totalTime=totalTime+time;
        %Calculamos el tiempo por repetición
        atime=atime+time;
    end;
```

```
    AverageCI=AverageCI+NCI;
    NTimeranuraTotal=NTimeranuraTotal+NTimeranuraTotalCI;
    AverageNumberTag=AverageNumberTag+numberTags;

    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    %Total de bytes transmitidos entre el lector y las marcas
    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    AverageBytesReadertoTag=AverageBytesReadertoTag+bytesReadertoTag;
    AverageBytesTagtoReader=AverageBytesTagtoReader+bytesTagtoReader;

    atime=atime/1000;
    med=med_ant+(atime-med_ant)/iteration;

    if(iteration>1)
        var=((1-(1/(iteration-1)))*var)+(iteration*((med-med_ant)^2));
    else
        var=0;
    end;
    med_ant=med;
end;
```

Cuadro A.1: Función que simula el proceso de identificación seguido por el protocolo CSMA *p*-persistente.

```
%**********************************************************************
%**********************************************************************
%Autor: Leonardo Sánchez
%Fecha: 20101024
%**********************************************************************
%**********************************************************************
%  -Devuelve el una arreglo que indica el número de marcas que
%   seleccionaron un número de ranura determinado (ranuraInf)
%**********************************************************************
function [ranuraInf]=RFIDsim(NTimeranura,NTag,M,p)
    alfa=M^((-1)/(NTimeranura-1));
    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    %Se crea un vector de tamaño NTimeranura lleno de 0's.
    %Es la información correspondiente a los resultados obtenidos en cada
    %ranura
    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    ranuraInf=zeros(1,NTimeranura);
    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    %Genera un arreglo de numeros aleatorios entre 0 y 1 de tamaño NTag con
    %distribución uniforme.
    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    %Calculamos la probabilidad correspondiente a cada ranura en base a la
    %distribución Sift
    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

```
for i=1:NTimeranura
    x(i) = (alfa^(-i))*(1-alfa)*(alfa^NTimeranura)/(1-(alfa^NTimeranura));
end;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%Se definen los intervalos para asignar la ranura que le corresponde a cada
%marca en base al número aleatorio uniformemente distribuido generado
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
sum = 0;
for i = 1:NTimeranura
    sum = sum+x((NTimeranura+1)-i);
    y(i) = sum;
end;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%Al generar un número aleatorio uniformemente distribuido, la
%probabilidad de que esté en el i-esimo ranura es directamente
%proporcional al tamaño del ranura.
%La suma de probabilidades que es asignada a cada ranura es 1
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%Cada marca genera un número aleatorio uniformemente distribuido
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
index=rand(1,NTag);

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%Asignamos el ranura correspondiente  al número aleatorio generado por
%cada marca en base a la distribución sift, es decir, en base a los
%intervalos definidos en y(i).
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%Cada marca selecciona una ranura de tiempo dentro de
%la ventana de contienda.
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
for i=1:NTag
    for j=1:(NTimeranura-1)
        if((0<=index(i)) && (index(i)<=y(1)))
            ranuraInf(NTimeranura)=ranuraInf(NTimeranura)+1;
            break;
        elseif(((y(j)<index(i)) &&(index(i)<=y(j+1))))
            ranuraInf(NTimeranura-j)=ranuraInf(NTimeranura-j)+1;
            break;
        end;
    end;
end;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%Simulación del procedimiento realizado por las marcas.
%Una vez que cada una de las marcas ha seleccionado una ranura, decide
%(en base a la probabilidad indicada en el mensaje de recolección de
```

```
%datos indicada por el lector) si transmite o no.
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%Se recorre las ranuras de la ventana de contienda verificando si
%existen marcas que la seleccionaron. Una vez que se sabe que al menos
%hay una marca que lo seleccionó, se verifica si a probabilidad no es
%uno, para posteriormente determinar la probabilidad con la que
%transmite, en base a la ranura seleccionada.
%El número aleatorio generado determina si se transmite o no., siendo
%p< la probabilidad de transmisión, y p> la probabilidad de
%abstinencia.
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
for j=1:NTimeranura
    if(ranuraInf(j)>0)
        for k=1:ranuraInf(j)
            if(p!=1)
                p=rand;
                prob_j=abs((NTimeranura-j)/(NTimeranura));
                if(p > prob_j)
                    ranuraInf(j) = ranuraInf(j)-1;
                end;
            end;
        end;
    end;
end;
```

Cuadro A.2: Función que simula a selección de una ranura dentro de la ventana de contienda en base ala distribución *Sift*.

REFERENCIAS

[1] S. Ahson and M. Ilias. *RFID Handbook: Applications, Technology, Security, and Privacy*. 2008.

[2] M. A. Bonuccelli, F. Lonetti, and F. Martelli. Instant collision resolution for tag identification in RFID networks. volume 5, pages 1220 – 1232, Amsterdam, The Netherlands, The Netherlands, November 2007. Elsevier Science Publishers B. V.

[3] M. V. Bueno Delgado. *Contribución a los protocolos anticolisióny técnicas de dimensionamiento para sistemas deidentificación por radio frecuencia*. PhD thesis, Universidad Politécnica de Cartagena,Departamento de Tecnologías de la información y lasComunicaciones, 2010.

[4] M. V. Bueno-Delgado, J. Vales-Alonso, and F. González-Castaño. Analysis of dfsa anti-collision protocols in passive RFID enviroments. In *35th International Conference of the IEEE Industrial Electronics Society (IECON 2009)*, Porto (Portugal), Nov. 2009.

[5] L. A. Burdet. RFID multiple access methods. Technical report, Apr. 2008.

[6] L. I. L. M. G. González. *RFID: Oportunidades y Riesgos, su aplicació práctica*. 2008.

[7] D. R. Hush and C. Wood. Analysis of tree algorithms for RFID arbitration. In *The IEEE intl. Symposium on Information theory*, page 107, Aug. 1998.

[8] ISO. *ISO/IEC 18000-7.2004 Information technology Radio frequency identification for item management Part 7. Parameters for active air interface at 433 MHz*, 2004.

[9] S. Jain and S. R. Das. Collision avoidance in a dense RFID network. In *Proceedings of the 1st international workshop on Wireless network testbeds, experimental evaluation & characterization*, WiNTECH '06, pages 49 – 56, New York, NY, USA, 2006. ACM.

[10] K. Jamieson, H. Balakrishnan, and Y. Tay. Sift: a MAC Protocol for Event-Driven Wireless Sensor Networks. In *Third European Workshop on Wireless Sensor Networks (EWSN)*, Feb. 2006.

[11] N. N. Kachouri and A. S. M. Andrieux. CSMA-based MAC protocol for collision avoidance in a dense RFID network. In *Informatics and Systems (INFOS), The 7th International Conference on*, volume 978-1-4244-5828-8, pages 1 – 5, Mar. 2010.

[12] D. Klair, K.-W. Chin, and R. Raad. A survey and tutorial of RFID anti-collision protocols. In *Communications Surveys & Tutorials, IEEE*, volume 12 Issue:3, pages 400 – 421, Apr. 2010.

[13] H. Koh, S. Yun, and H. Kim. Sidewalk: a RFID tag anti-collision algorithm exploiting sequential arrangements of tags. In *Communication.IEEE International Conference on*, pages 2597 – 2601, May 2008.

[14] C. Law, K. Lee, and K.-Y. Siu. Efficient memoryless protocol for tag identification (extended abstract). In *Proceedings of the 4th international workshop on Discrete algorithms and methods for mobile computing and communications*, DIALM '00, pages 75 – 84, New York, NY, USA, 2000. ACM.

[15] G. Maselli, C. Petrioli, and C. Vicari. Dynamic tag estimation for optimizing tree slotted ALOHA in RFID networks. In *Proceedings of the 11th international symposium on Modeling, analysis and simulation of wireless and mobile systems*, MSWiM '08, pages 315 – 322, New York, NY, USA, 2008. ACM.

[16] J. Myung and W. Lee. Adaptive binary splitting: A RFID tag collision arbitration protocol for tag identification. In *Broadband Networks, 2005. BroadNets 2005. 2nd International Conference on*, volume 1, pages 347 – 355, Oct. 2005.

[17] L. T. Y. Olu Yan, Yan Zhang and H. Ning. *RFID: Internet of Things: from RFID to thee next-generation perasive networked systems*. 2008.

[18] A. Palomo-López, M. V. Bueno-Delgado, Esteban Egea-López, J. J. Alcazar-Espín, and J. Vales-Alonso. CSMA multi-stage anti-collision protocol for active RFID. In *4th International Workshop on RFID Technology - Concepts, Applications, Challenges (IWRT 2010)*, Funchai Madeira, Portugal, June 2010.

[19] F. C. Schoute. Dynamic frame length ALOHA. In *IEEE Transactions on Communications*, volume 31 Issue:4, pages 565 – 568, Apr. 1983.

[20] J.-D. Shin, S.-S. Yeo, T.-H. Kim, and S. K. Kim. Hybrid tag anti-collision algorithms in RFID systems. In *Proceedings of the 7th international conference on Computational Science, Part IV: ICCS 2007*, ICCS '07, pages 693 – 700, Berlin, Heidelberg, 2007. Springer-Verlag.

[21] A. Technology. *Class 1 Generation 2 UHF Air Interface Protocol Standard Specifications*, 2004.

[22] J. Vales-Alonso, F. González-Castaño, E. Egea-López, M. V. Bueno-Delgado, A. Martínez-Sala, and J. G. Haro. Evaluación de CSMA no persistente como protocolo anticolisión en sistemas RFID activos. In *Primeras Jornadas Científicas sobre RFID*, pages 313 – 320, Ciudad Real, Nov. 2007.

[23] H. Vogt. Efficient object identification with passive RFID tags. In *Proceedings of the First International Conference on Pervasive Computing*, Pervasive '02, pages 98 – 113, London, UK, 2002. Springer-Verlag.

[24] Xinqing and G. Zhu. An enhanced query tree protocol for RFID tag collision resolution with progressive population estimation. In *Mobile Adhoc and Sensor Systems*, pages 935 – 940, Oct. 2009.

[25] H. Zhang, L. Han, and Y.-L. Li. Design of hash-tree anti-collision algorithm. In *Third International Conference on Natural Computation (ICNC)*, pages 176 – 179, China, 2007.

[26] B. Zhen, M. Kobayashi, and M. Shimizu. Framed ALOHA for multiple RFID objects identification. In *IEICE-Transactions on Communications*, volume E88-B;NO.3, pages 991 – 999, Japan, 2005.

[27] F. Zhou, C. Chen, D. Jin, C. Huang, and H. Min. Evaluating and optimizing power consumption of anti-collision protocols for applications in RFID systems. In *Proceedings of the 2004 international symposium on Low power electronics and design*, ISLPED '04, pages 357 – 362, New York, NY, USA, 2004. ACM.