Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

PC y TI

IDÓNEA COMUNICACIÓN DE RESULTADOS

Detección de objetos perdidos en sistemas RFID

Autor:
Oscar Ledesma Avilés

Investigación presentada para obtener el grado de
Maestro en ciencias y tecnologías de la información

Asesor:
Dr. Víctor Manuel Ramos Ramos
Co-asesor:
M. en C. Leonardo Daniel Sánchez Martínez

Posgrado en Ciencias y Tecnologías de la Información

Defendida públicamente en la UAM-Iztapalapa el 25 de agosto de 2014 a las 10:00 h frente al jurado integrado por :

Presidente: Dr. Enrique Stevens Navarro, UASLP
Secretario: Dr. Víctor Manuel Ramos Ramos, UAM-I
Vocal: Dr. Miguel López Guerrero , UAM-I

Resumen

En los últimos años, la IDentificación por Radio Frecuencia (Radio Frequency IDentification o RFID) se ha convertido en una tecnología emergente de rápido crecimiento y probada utilidad en la industria. Su principal ventaja estriba en la capacidad de identificar objetos de forma inalámbrica, sin necesidad de establecer contacto o mantener una línea de vista entre los dispositivos involucrados, dicha característica hace de esta tecnología una herramienta atractiva para aplicaciones industriales como seguimiento de activos, manejo automatizado de inventarios, tareas de conteo, control de acceso y producción, cobro instantáneo, transporte público y monitorización. Algunos retos asociados con esta tecnología han sido profundamente estudiados, tal es el caso de la resolución de colisiones, la ampliación de la cobertura espacial de los sistemas, la reducción de su consumo energético, entre otros; sin embargo, algunos otros retos, como la detección de objetos perdidos y la implementación de arquitecturas distribuidas de comunicación, continúan ofreciendo oportunidades de mejora. En este trabajo, analizamos los protocolos de detección de objetos perdidos en sistemas RFID propuestos con anterioridad en la literatura, proponemos cuatro mecanismos que permiten reducir el tiempo que le toma a un protocolo de esta índole el detectar a las etiquetas RFID de un conjunto como presentes o perdidas, presentamos un protocolo que los incorpora y analizamos las condiciones bajo las cuales este nuevo protocolo podría implementarse dentro de una arquitectura distribuida. Los resultados muestran una notable mejoría en el desempeño del nuevo protocolo cuando se le compara con aquellos en el estado del arte, mientras que el análisis de su implementación en una arquitectura distribuida describe dificultades que aún deben ser resueltas para que sus ventajas superen a aquellas que ofrece la arquitectura centralizada.

Abstract

Radio Frequency IDentification systems (RFID) have become an emerging technology in the last years, growing quickly and getting more and more useful in industrial applications. Its main feature relies on its ability to identify objects wirelessly without putting objects in contact or maintaining a line of sight among them. This feature represents a powerful tool for the industry when enabling applications like asset tracking, inventory automation, counting tasks, production and access control, instant payment, public transportation, object monitoring, among many others. Some of the challenges motivated by this technology have been deeply studied in the past, such as collision resolution, coverage extension and energy consumption reduction; but some others, like missing RFID tag detection and distributed communication architectures, continue to offer improvement opportunities. In this work, we focus on the analysis of missing RFID tag detection protocols, we propose four mechanisms which allow to reduce the time a protocol takes to detect every single RFID tag from a set as present or missing, we describe a protocol that includes these mechanisms, and we analyze the conditions under which this new protocol would perform better when using a distributed architecture. The results show a considerable improvement on the new protocol's performance when compared with the state of the art. The analysis of its implementation in a distributed architecture identifies some difficulties still to be addressed before it shows advantages over the centralized architecture.

Agradecimientos

Agradezco principalmente a mi asesor Dr. Víctor Manuel Ramos Ramos por haberme brindado la confianza requerida para establecer una relación académica fructífera, por transmitir su conocimiento y experiencia profesional y personal, por generar un equipo de trabajo que propiciara un clima laboral inigualable, y por guiar esta investigación hacia la consecución de sus objetivos.

Al M. en C. Leonardo Daniel Sánchez Martínez por haber co-asesorado mi trabajo, haber aportado tanto de su valioso y escaso tiempo a encauzar mi trabajo e ideas, pero sobre todo, por haber formado parte del grupo de investigación dentro del que me desempeñé, y del cual surgieron importantes productos de investigación y entrañables amistades.

A cada uno de los miembros del autodenominado equipo WiNetSys, que bajo la tutela del Dr. Víctor Manuel Ramos Ramos formaron un espacio de trabajo de condiciones prolíferas en el plano académico y social.

A los profesores que contribuyeron a mi formación durante la estancia en este posgrado, y que se mostraron siempre disponibles e interesados en despejar mis dudas.

A mis compañeros, que fueron parte inexcluíble de la experiencia de la que juntos formamos parte, y en especial a algunos de ellos que se convirtieron en grandes amistades.

A la Universidad Autónoma Metropolina y a la Unidad Iztapalapa, por haberme dado la oportunidad y las condiciones para superar mis expectativas académicas, y al CONACyT por aportar los recursos económicos que hicieron posible llegar hasta aquí.

Por último, pero resaltando la mayor importancia, a mi familia, cuyas aportaciones a la formación de la persona que soy el día de hoy, rebasan mi capacidad de agradecimiento.

Contenido

Lista de figuras

Lista de tablas

Acrónimos

RFID	**R**adio **F**recuency **ID**entification
EPC	**E**lectronic **P**roduct **C**ode
ID	**ID**entifier
ISO	**I**nternational **O**rganization for **S**tandarization
SDMA	**S**pace **D**ivision **M**ultiple **A**ccess
FDMA	**F**requency **D**ivision **M**ultiple **A**ccess
TDMA	**T**ime **D**ivision **M**ultiple **A**ccess
CDMA	**C**ode **D**ivision **M**ultiple **A**ccess
CSMA	**C**arrier **S**ense **M**ultiple **A**ccess
RTF	**R**eader **T**alk **F**irst
TTF	**T**ag **T**alk **F**irst
DARPA	**D**efense **A**dvanced **R**esearch **P**rojects **A**gency
SA	**S**lotted **A**LOHA
FSA	**F**ramed **S**lotted **A**LOHA
BFSA	**B**asic **F**ramed **S**lotted **A**LOHA
DFSA	**D**ynamic **F**ramed **S**lotted **A**LOHA
EDFSA	**E**nhanced **D**ynamic **F**ramed **S**lotted **A**LOHA
BTS	**B**asic **T**ree **S**plitting
ABTS	**A**daptative **B**asic **T**ree **S**plitting
PSC	**P**rogressed **S**lot **C**ounter
ASC	**A**llocated **S**lot **C**ounter
QT	**Q**uery **T**ree
BSA	**B**inary **S**earch **A**lgorithm
EBSA	**E**nhanced **B**inary **S**earch **A**lgorithm
DBSA	**D**ynamic **B**inary **S**earch **A**lgorithm

PDC	**P**ower-based **D**istance **C**lustering
TRP	**T**rusted **R**eader **P**rotocol
IIP	**I**terative **I**D-free **P**rotocol
NS	**N**etwork **S**imulator

Capítulo 1

Introducción

RFID es un término acuñado para referirse a cierta clase de tecnología basada en ondas de radio de corto alcance utilizada principalmente para comunicar información entre un sitio estacionario y un objeto móvil, o bien, entre objetos móviles [1]. La tecnología RFID tiene como principal característica, la capacidad de identificar objetos de forma inalámbrica, sin necesidad de poner en contacto los elementos participantes del sistema o mantener una línea de vista entre ellos [2].

Las características anteriormente descritas han propiciado el gran auge de la tecnología RFID en la última década. In-Stat [3] reportó en 2006 que durante 2005 se produjeron más de 1.3 billones de etiquetas RFID. Más adelante, en 2011, la Allied Business Intelligence [4] afirmó que la aplicación tecnológica de mayor crecimiento entre 2010 y 2016 sería el rastreo de artículos en la administración de las cadenas de suministro, superando una tasa de crecimiento del 37 %. Lo anterior debido principalmente al etiquetado de prendas de vestir, productos farmacéuticos, vinos, tabaco, cosméticos y productos electrónicos, entre muchos otros.

De acuerdo al reporte de investigación de VCD Research Group, en 2011 se vendieron más de dos billones de etiquetas RFID y la proyección para el 2015 es que este número se multiplique por 20, es decir, sobrepase los 40 billones. Otro dato, que proviene de estudios realizados sobre los beneficios logrados por Wal-Mart, nos indica que se pueden lograr reducciones de costos de inventario y logística de entre 5 y 8 %, que representan ahorros de más de ocho billones de dólares anuales [5].

Gracias al impulso de grandes jugadores globales como Wal-Mart en Estados Unidos, Metro en Europa, Procter & Gamble, Johnson & Johnson y Hewlett-Packard, entre otros, hoy no cabe duda de que RFID no es más una tendencia, sino una realidad, no sólo en los países altamente desarrollados, sino también en América Latina. Las empresas ya no se encuentran cuestionando la viabilidad o no del uso de la tecnología RFID, ni el retorno de la inversión asociado a su implementación (como sucedía años atrás), sino que están en el proceso de masificar su aplicación a nivel organizacional para obtener mayores beneficios.

En consecuencia, los sistemas de Identificación por Radio Frecuencia (RFID por sus siglas en inglés) se han convertido en parte de nuestra vida cotidiana, y han probado ser herramientas con la capacidad de incrementar la productividad y la comodidad de las personas. La tecnología RFID ha sido y continuará siendo utilizada en cientos, o tal vez miles de aplicaciones, entre las cuales se encuentran: tarjetas de proximidad, etiquetas contra robo, pequeños dispositivos para el pago automático de peaje y artículos, seguimiento de activos, manejo automatizado de inventarios, tareas de conteo, control de acceso y producción, transporte público, monitorización e incluso control de ganado [6].

Existiendo un rango tan amplio de posibilidades, resulta lógico entender las razones por las cuales muchas tecnologías tradicionales están tendiendo a ser reemplazadas por sistemas RFID. Un claro ejemplo del advenimiento de esta tendencia de reemplazo es el código de barras [7].

El código de barras óptico sufre de múltiples inconvenientes, requiere de la intervención de seres humanos para ser leído, y este proceso puede verse fácilmente afectado por la suciedad, la humedad, la abrasión, etc. Además, la información que un código de barras puede almacenar es muy limitada, y pueden ser fácilmente falsificados, todo ello puede evitarse utilizando etiquetas RFID.

El notable crecimiento de la gama de aplicaciones para los sistemas RFID ha generado una gran actividad de investigación científica en torno a la resolución de los problemas asociados con su implementación, y a la mejora en la eficiencia de los sistemas actualmente implementados.

1.1. Fundamentos

La tecnología RFID implica un sistema de almacenamiento y recuperación de datos remoto. Para tal efecto, los sistemas RFID se componen de tres elementos principales: una o más etiquetas, uno o más lectores y una aplicación de procesamiento.

Etiquetas RFID: También conocidas como *transponders* (término compuesto de las palabras en inglés para "transmisor" y "respondedor"), se adhieren a los objetos que se pretende identificar. Las etiquetas RFID suelen diseñarse con el propósito específico de adherirse a casi cualquier clase objetos, por lo tanto, los almacenes de todo tipo son probablemente el escenario de mayor aplicación para los sistemas RFID.

Una etiqueta consiste de un microchip y una antena (helicoidal o dipolo), cuyo propósito es almacenar y transmitir poca información. La Figura 1.1 muestra una etiqueta RFID pasiva, compuesta por un circuito integrado y una antena. Existen etiquetas RFID que no incorporan un microchip, a ese tipo de etiquetas se les llama *chipless tags*, y actualmente prometen ahorros significativos dado que pueden ser impresas directamente en los productos que las requieren [8].

Las etiquetas RFID activas son aquellas que se energizan total o parcialmente mediante baterías o una fuente de alimentación eléctrica constante. Por esta razón, las etiquetas RFID activas tienen la capacidad de comunicarse entre ellas, monitorizar el medio de comunicación, detectar colisiones e iniciar un diálogo con el lector. Cuando únicamente algunas de las funciones de la etiqueta, por ejemplo cierto sector de su circuitería, se energiza mediante una fuente externa, se les llama etiquetas semiactivas o semipasivas.

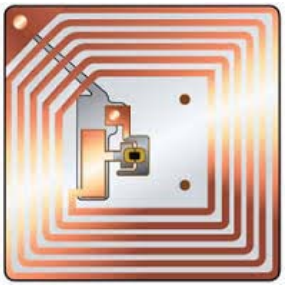

FIGURA 1.1: Etiqueta RFID pasiva

Por otro lado, las etiquetas pasivas no requieren una fuente de energía local, sino que son energizadas por las emisiones electromagnéticas del lector. La recepción de la consulta representa una fuente de energía que se utiliza en parte para energizar su circuitería, y en parte para ser modulada y retrodispersada en forma de respuesta. Esta característica limita sus capacidades de procesamiento y comunicación, las vuelve incapaces de monitorizar el medio y detectar colisiones. Esta última clase de etiquetas ha atraído mayor atención en los últimos años debido a su bajo costo [9]; por lo tanto, la mayor parte de la investigación actual gira en torno a su uso.

Lectores RFID: Lectores o *transceivers* (término compuesto de las palabras en inglés para "transmisor" y "receptor") son dispositivos construidos mediante un módulo RF y una unidad de control. Este elemento es típicamente un dispositivo con suficiente capacidad de procesamiento, memoria y recursos computacionales. Está comunmente comunicado con una base de datos u otro tipo de aplicación que procesa los datos recabados. Sus funciones principales son energizar o activar a las etiquetas, controlar la secuencia de comunicación con ellas, y transferir la información entre la aplicación y las etiquetas. Un ejemplo gráfico de un lector se puede apreciar en la Figura 1.2.

Figura 1.2: Lector RFID

Subsistema de aplicación: Es un subsistema de procesamiento de datos, una base de datos o alguna aplicación de software, que inicia las actividades de los lectores y por lo tanto de las etiquetas. También controla, procesa y utiliza la información de la red RFID.

El criterio más comúnmente utilizado para diferenciar o clasificar a los sistemas RFID es la frecuencia de operación de los lectores, la cual varía en un rango amplio que pasa por los 135 kHz, 13.6 MHz, 433 MHz, $860 - 960$ MHz, 2.45 GHz, y hasta los 5.8 GHz [10].

Este parámetro tiene un impacto directo sobre la amplitud del área de cobertura del sistema, que va desde algunos milímetros hasta varios metros. Cuando un sistema RFID se diseña para cubrir un área milimétrica se le llama *sistema de acoplamiento cercano* y sus aplicaciones suelen relacionarse con medidas estrictas de seguridad o comunicaciones que no requieren mayor distancia, como cerraduras electrónicas y tarjetas inteligentes. Cuando los sistemas se diseñan para operar a distancias mayores se les llama *sistemas de acoplamiento remoto*. Se cree que al menos el 90 % de los sistemas RFID que operan en la actualidad pertenecen a este último grupo [11] y por ello existen un sinnúmero de aplicaciones que surgen de ellos.

El contexto de este trabajo de investigación contempla el uso de etiquetas pasivas para la banda UHF ($860 - 960MHz$) bajo las normas planteadas en el estándar EPC Gen2 (versión corta del nombre original del estándar: EPCglobal UHF Class 1 Generation 2). Existen otros conjuntos de normas referentes a los sistemas RFID, como aquellas agrupadas bajo la denominación ISO/IEC 18000, que establecen los parámetros de aplicación y funcionamiento de las tecnologías RFID para la administración de objetos, rastreo de ganado, sistemas de pago, tarjetas inteligentes y de proximidad, etc. Sin embargo, el estándar de EPCglobal ha desarrollado normas enfocadas en las necesidades específicas de la industria, especialmente las de manejo de la cadena de suministros, la identificación y monitorización de activos, etc., logrando aceptación internacional.

1.2. Identificación de la problemática

Uno de los usos más frecuentes de los sistemas RFID es la identificación de los objetos a los cuales se adhirieron las etiquetas, esta tarea permite mantener un control inventarial útil para múltiples aplicaciones industriales. El proceso de identificación se considera precursor del de monitorización y del de detección de objetos perdidos, dado que es evidente que se requiere conocer con anterioridad los objetos que se desea monitorizar para poder aseverar que, en cada instante posterior, la totalidad de ellos se encuentra en la zona esperada. La identificación de etiquetas RFID y los problemas asociados a la misma han sido ampliamente estudiados con anterioridad, y han generado la necesidad de encontrar mecanismos que permitan agilizar la monitorización de los objetos identificados.

Existen múltiples escenarios en los que se requiere saber si los elementos que se han identificado previamente se encuentran aún en el área de identificación. Por ejemplo, es posible monitorizar los artículos que se almacenan en una bodega o los productos con los que cuenta el inventario de una tienda departamental utilizando etiquetas RFID, y dado que se han identificado previamente, una nueva sesión de lectura es capaz de comparar la cantidad de elementos identificados contra la cantidad de elementos registrados en el inventario [9]. Este procedimiento permitirá detectar amenazas como robos, movimientos indeseables, o pérdidas accidentales de artículos. Los comerciantes minoristas pierden cerca de treinta billones de dólares al año, de los cuales el 70 % se debe a errores de administración, fraudes y robos de los propios empleados [12]. Si los objetos referenciados por una identificación previa no son encontrados en una actual, es posible que no estén presentes en el área. Para maximizar la certeza de que se han detectado todos los objetos en el área, se requiere alcanzar un nivel aceptable de incertidumbre al respecto.

Por otro lado, la tendencia actual en la investigación sobre sistemas RFID se ha dirigido a la búsqueda de nuevos paradigmas de comunicación. Uno de los ejemplos más representativos es la inclusión de arquitecturas distribuidas que permitan eficientar la comunicación entre los elementos del sistema. Estas arquitecturas permitirán comunicar mensajes de forma simultánea en zonas espacialmente apartadas, reduciendo el tiempo que toma la comunicación, extender el área de cobertura del sistema y minimizar los costos asociados al uso de múltiples lectores, entre otras ventajas que aún se encuentran bajo análisis científico.

La investigación actual en torno a los sistemas RFID ha explorado de forma vasta procedimientos de evasión y eliminación de interferencia asociada con la comunicación entre los elementos participantes en los procesos de identificación. Sin embargo, existen dos áreas de oportunidad cuyo potencial parece haber sido subestimado durante los últimos años: 1) la detección de etiquetas, y por lo tanto, objetos perdidos, y 2) la implementación de arquitecturas distribuidas que permitan agilizar los procesos de identificación mediante lecturas simultáneas. De aquí que este trabajo de investigación busca explotar ambas oportunidades, proponiendo alternativas para la detección de objetos perdidos y estudiando su aplicabilidad sobre una arquitectura distribuida.

1.3. Objetivos

1.3.1. Objetivo general

Diseñar un protocolo de detección de objetos perdidos para sistemas RFID pasivos, analizando las ventajas y desventajas de su implementación dentro de una arquitectura de red distribuida.

1.3.2. Objetivos específicos

- Realizar un estudio del estado del arte de los protocolos de detección de objetos perdidos en sistemas RFID.
- Realizar un estudio del estado del arte del paradigma distribuido en redes RFID.
- Diseñar un protocolo de detección de objetos perdidos para sistemas RFID pasivos.
- Implementar un escenario de simulación para evaluar el desempeño de la propuesta.
- Analizar la adaptación del protocolo diseñado a un enfoque distribuido y analizar su desempeño.

1.4. Metodología

La metodología utilizada, para lograr la consecución de los objetivos anteriormente planteados, comprendió las etapas que se listan a continuación:

a) Estudiar ampliamente las generalidades de la tecnología RFID.

b) Estudiar los protocolos propuestos en la literatura en torno a la detección de objetos perdidos en redes RFID.

c) Estudiar las propuestas actuales sobre esquemas distribuidos para sistemas RFID.

d) Estudiar las plataformas de simulación para sistemas RFID disponibles.

e) Diseñar un protocolo de detección de objetos perdidos para sistemas RFID pasivos.

f) Evaluar el desempeño de la propuesta, mediante su implementación y la del protocolo existente con mejor desempeño, en un simulador.

g) Adaptar la propuesta a una arquitectura distribuida.

h) Analizar las ventajas y desventajas que proporciona la versión distribuida, así como la conveniencia de su evaluación en el simulador.

1.5. Estructura y contribución

El resto de este documento está organizado de la siguiente forma:
El Capítulo 2 presenta una breve descripción de aquellos trabajos que anteceden a esta investigación y que representan el estado del arte en términos de los procesos de comunicación RFID y la detección de objetos perdidos en estos sistemas. El Capítulo 3 describe con detalle la operación del protocolo diseñado y de cada uno de los mecanismos que lo componen. En el Capítulo 4 se establecen los escenarios de evaluación para la propuesta, se analizan y comparan resultados; además se realiza un análisis de las condiciones bajo las cuales resultaría ventajoso implementar la propuesta en una arquitectura de red distribuida. Finalmente, en el Capítulo 5 se generan conclusiones y perspectivas de trabajo futuro.

A lo largo de este trabajo, se construye un nuevo protocolo para la detección de objetos perdidos en sistemas RFID pasivos, mediante la reducción de la cantidad de mensajes difundidos a través de la red. Además, se analizan las condiciones bajo las cuales resulta conveniente implementar el protocolo generado en arquitecturas de red distribuidas.

Capítulo 2

Estado del arte

2.1. Proceso de comunicación

Dentro de un sistema RFID que utiliza etiquetas pasivas en la banda UHF, sin importar la aplicación o arquitectura utilizada, el proceso de comunicación inicia cuando uno o más lectores difunden una consulta, la cual especifica, mediante un comando, el proceso o la aplicación que se está ejecutando. Las etiquetas RFID son energizadas o activadas gracias a la energía electromagnética que colectan de la transmisión del lector, una parte de esa energía se utiliza para activar la circuitería de la etiqueta y habilitar el procesamiento de la información que recibe la misma, mientras que la energía restante es modulada y retrodispersada en forma de respuesta hacia el lector.

2.1.1. Paradigma centralizado

En un proceso típico de identificación, el lector solicita a las etiquetas el envío de su ID mediante la difusión de una consulta. Posteriormente, las etiquetas responden con la información solicitada, y ésta es integrada a una base de datos o procesada por una aplicación. Nótese que éste, al igual que cualquier otro proceso de comunicación RFID, involucra un lector y una o más etiquetas, a este esquema se le llama *paradigma de comunicación centralizado*. Actualmente, existe mucho trabajo de investigación e implementación relacionado con sistemas basados en el paradigma centralizado, especialmente sobre resolución de colisiones generadas entre etiquetas [7, 8, 13–15].

La mayoría de las aplicaciones para los sistemas RFID cuenta con un conjunto numeroso de etiquetas, las cuales se pretende identificar de forma casi simultánea (en función de la rapidez con la que el proceso pueda llevarse a cabo), y por lo tanto existe la posibilidad de que las respuestas de las etiquetas se interfieran mutuamente. Para contextualizar el problema de las colisiones, pensemos en aquel escenario en el cual las etiquetas han recibido una consulta desde un lector, por un lado, si solamente una etiqueta responde, el lector recibe un sólo mensaje que puede decodificar correctamente. Por el contrario, si dos o más etiquetas responden de forma simultánea, sus mensajes colisionan generando interferencia y no pueden ser recibidos correctamente en el lector. Entre las consecuencias de este efecto se encuentra, el desperdicio de energía y ancho de banda, así como el incremento del retardo de identificación. Este problema se conoce como "colisiones entre etiquetas", y se ha desarrollado una vasta cantidad de procedimientos para minimizar o eliminar su efecto negativo.

Una de las primeras soluciones que pretendieron resolver el problema de la utilización de los recursos de un medio compartido, y controlar cuál de los participantes en una red podía transmitir y en qué momento, fue desarrollada en 1970 en la Universidad de Hawaii, financiada con fondos de la *Defense Advanced Research Projects Agency* (DARPA), y tomó el nombre de **ALOHA**. El protocolo ALOHA funciona bajo la premisa básica de que cualquier participante en un sistema inalámbrico debe transmitir su mensaje en el instante que lo requiera, sin hacer ninguna consideración extra. Una versión más eficiente se denomina ALOHA ranurado (SA) y define secciones temporales, o momentos específicos en los que cualquier participante puede transmitir su mensaje, pero nadie puede hacerlo fuera de esos instantes predeterminados. A continuación se presenta una breve descripción de algunas de las variantes de este protocolo que se han aplicado a los sistemas RFID [7, 8, 16].

ALOHA Ranurado por Tramas (*Framed Slotted ALOHA* o FSA): Este protocolo está basado en ALOHA ranurado, y permite que cada etiqueta responda únicamente una vez por trama. La trama consta de cierto número predeterminado de ranuras. La forma básica de FSA se conoce como *Basic Framed Slotted ALOHA* o BFSA, y se le llama "básica" porque el tamaño de la trama permanece constante durante todo el proceso de identificación. A partir de BFSA, han surgido

variantes que implementan técnicas como el silenciamiento y la terminación adelantada. El silenciamiento implica solicitar a ciertas etiquetas que no participen en rondas subsecuentes, mientras que la terminación adelantada consiste en detener la comunicación cuando se sabe por adelantado que no se obtendrá información extra.

ALOHA Ranurado por Tramas Dinámicas (*Dinamic Frame Slotted ALOHA* o DFSA): El proceso de comunicación se lleva a cabo a lo largo de una serie de ranuras temporales que en su conjunto forman una trama. Al finalizar el periodo de dicha trama se dice que ha concluido un ronda o ciclo del proceso. En BFSA, el tamaño de la trama permanece constante en cada ronda durante todo el proceso de identificación. La diferencia clave en DFSA, radica en ajustar el tamaño de la trama en cada ronda. En un proceso de identificación, la cardinalidad del conjunto es desconocida, y por tanto, se utiliza una función de estimación para determinar la cantidad de etiquetas que restan por identificar. Numerosos trabajos han propuesto funciones para estimar el tamaño óptimo de trama [8]. En general, se utilizan dos metodologías para estimar el número de etiquetas restantes por identificar. Una de ellas se basa en el uso de un multiplicador fijo y, por lo tanto, es llamada estimación estática. Las funciones Cha-I (DFSAC-I), Zhen (DFSAZ) y Vogt-I (DFSAV-I) pertenecen a esta metodología. Por otro lado, las funciones que utilizan métodos probabilísticos o estadísticos son llamadas estimación dinámica. Algunos ejemplos de esta metodología son Cha-II (DFSAC-II) y Vogt-II (DFSAV-II). Las funciones de estimación dinámica proveen de estimaciones más precisas conforme el número de etiquetas en participación aumenta [8]. En un proceso de detección de etiquetas perdidas, la cardinalidad del conjunto en cada instante es conocida, por lo cual no se requiere del proceso de estimación.

ALOHA Ranurado por Tramas Dinámicas Mejorado (*Enhanced Dynamic Framed Slotted ALOHA* o EDFSA): DFSA y sus variantes están restringidos a un tamaño máximo de trama de 256 o 512. Teóricamente el tamaño ideal de la trama corresponde al número de etiquetas presentes en el proceso de identificación. Por lo tanto si el número de etiquetas por identificar supera el tamaño máximo de la trama, se espera que existan colisiones persistentes que causen problemas en la identificación. Con esto en mente, se ha propuesto una versión mejorada de DFSA en la cual las etiquetas son divididas en grupos cuando el total de ellas excede al

tamaño máximo de trama disponible. Esta división sucede una sola vez, a diferencia de lo que sucede en los métodos de separación. Una vez dividido en grupos, el lector procede a leer cada grupo a la vez. De forma similar a BFSA y DFSA, se han generado variantes de EDFSA mediante la inclusión de los conceptos de silenciamiento y terminación adelantada.

Otra clase de protocolos que permiten confrontar los problemas de colisiones entre etiquetas son llamados métodos de separación o de división. En general, para esta clase de algoritmos las colisiones son resueltas mediante la división del conjunto de etiquetas en subconjuntos tantas veces como sea necesario. Las etiquetas pertenecientes al primer subconjunto transmiten durante la primera ranura de tiempo. Las etiquetas que pertenecen a otros subconjuntos permanecen inactivas durante el periodo necesario para que las colisiones en el primer subconjunto sean resueltas, y por lo tanto, todas sus etiquetas se comuniquen de forma efectiva. Si el primer subconjunto genera otra colisión (esta vez de forma interna), este subconjunto vuelve a dividirse en subconjuntos más pequeños. Este proceso sucede de forma recursiva hasta que logren resolverse todas las colisiones dentro de un subconjunto. Una vez resueltas las colisiones en un subconjunto, el mismo procedimiento toma lugar en el resto de ellos de forma secuencial.

La gama más amplia de protocolos anticolisión que utilizan métodos de división son los algoritmos basados en árboles [7, 8]. Estos protocolos son capaces de garantizar la comunicación del total de las etiquetas de un conjunto en tiempo finito, y requieren que éstas implementen silenciamiento tras su identificación exitosa. Por su parte, el lector retroalimenta a las etiquetas con la información acerca de las identificaciones logradas en cada ranura de tiempo, de forma que cada etiqueta conozca su posición en el árbol, el subconjunto al que pertenece, y por lo tanto, el momento en que se le permite transmitir. Las etiquetas utilizan esta información en forma de un contador que se incrementa al suceder una colisión y se decrementa al suceder una identificación exitosa. Las etiquetas sólo tienen permitido transmitir cuando sus contadores se encuentran en cero.

En este trabajo, omitimos la descripción detallada de cada una de las variantes de los protocolos basados en árboles, debido a que los protocolos de detección de objetos perdidos se han visto mayormente beneficiados por el uso de variantes de ALOHA. Sin embargo, no descartamos la posibilidad de que surjan nuevas propuestas basadas en esta segunda clase de protocolos.

2.1.2. Estandarización actual

Como ya se mencionó con anterioridad, el estándar EPCglobal UHF Class 1 Generation 2 (EPC Gen2) agrupa las normas referentes a los sistemas RFID para etiquetas pasivas en la banda UHF. Este estándar implementa DFSA con un mecanismo de adaptación de trama conocido como Algoritmo Q, que está definido específicamente para normalizar el proceso de identificación [2]. Sin embargo, los trabajos actuales sobre detección de objetos perdidos suelen apegarse al estándar en la generalidad de los parámetros que establece. EPC Gen2 está diseñado para operar en una arquitectura centralizada, aunque puede extenderse a una arquitectura distribuida en varios lectores, utilizando mecanismos de multicanalización como los descritos en la sección siguiente. A pesar de ello, no contempla la distribución del proceso mediante la introducción de dispositivos extra a los ya descritos.

2.1.3. Paradigma distribuido

Durante la última década, se han explorado escenarios de identificación alternativos al centralizado. Las propuestas incluyen arquitecturas que implementan varios lectores (multilector) o que introducen dispositivos adicionales al proceso de identificación. Sin embargo, el primer acercamiento a la distribución del proceso de identificación utiliza una arquitectura física centralizada y distribuye la comunicación durante el propio proceso. A continuación, se describen las propuestas recientes en torno a este paradigma.

Distribución por potencia de lectura: Ali y Hassanein son autores de tres de las propuestas recientes que abordan el análisis de arquitecturas distribuidas para los sistemas RFID. En [16], se presenta un primer mecanismo anticolisión entre etiquetas que utiliza un solo lector, pero varias zonas de identificación. Este esquema resulta un primer abordaje del paradigma distribuido para esta clase de sistemas. El **Agrupamiento por Distancia Basado en Potencia** (*Power-based Distance Clustering* o PDC) descrito en [16], agrupa las etiquetas conforme a su distancia del lector. Para lograrlo, la potencia en la antena del lector varía formando subconjuntos de etiquetas, más pequeños que el original, sobre los cuales se aplica algún protocolo de identificación convencional como aquellos basados en ALOHA o en árboles. Al término del proceso de comunicación dentro de una subzona, todas

las etiquetas recién detectadas quedan en silencio durante el resto del proceso. La idea principal yace en el hecho de que la reducción de etiquetas participantes en cada proceso de comunicación, reduce también las colisiones, el tiempo requerido por el proceso e incrementa la eficiencia general de la identificación. El proceso general implica que las etiquetas más cercanas al lector son identificadas al inicio del proceso, y las que se encuentran espacialmente más distantes del lector son identificadas tras un lapso dependiente de dicha distancia.

Distribución basada en múltiples lectores: La forma de distribución más simple, y por lo tanto la única utilizada hasta la fecha en implementaciones reales, es aquella que implica más de un lector. A pesar de que este esquema es simplemenmte una extrapolación del esquema centralizado, al estudiarlo aparece un nuevo problema al cual se denomina "problema de colisión entre lectores", esta clase de interferencia se presenta, comúnmente, cuando la señal transmitida por un lector es lo suficientemente fuerte como para interferir la comunicación entre las etiquetas y un segundo lector, con el cual comparte una zona de traslape para brindar cobertura espacial completa. De forma similar a la colisión entre etiquetas, se han propuesto una serie de protocolos que eliminan esta forma de interferencia. Ahora, se describen brevemente algunos de ellos conforme a lo presentado en [17].

Los **algoritmos basados en cobertura** intentan minimizar el traslape de las regiones de interferencia mediante el ajuste dinámico de los rangos de comunicación de los lectores participantes. Usualmente, requieren un nodo central que realiza el procesamiento necesario para instruir al resto sobre los ajustes de potencia que deben llevar a cabo. Ejemplos de este tipo de algoritmos son: *Low-energy Localized Clustering for RFID Networks*, *Weighted Low-energy Localized Clustering for RFID Networks* y *Distributed Adaptive Power Control*.

Los **algoritmos basados en calendarización** se basan en la incorporación de una agenda o calendario, la cual permite reservar los recursos de transmisión (ranuras de tiempo y frecuencias) para cada uno de los lectores participantes. Algunos ejemplos de esta gama son: *Colorwave*, *Efficient Heterogeneous Reader Anticollision*, *Hierarchical Q-Learning* y *Simulated Annealing*.

Por último, los **algoritmos basados en mecanismos de control** mitigan el problema de las colisiones entre lectores mediante la transmisión de paquetes de control desde un lector que se encuentra transmitiendo hacia los demás lectores.

Los lectores que reciben paquetes de control, esperan en silencio hasta la siguiente ronda, y entonces transmiten. Entre los algoritmos de este tipo se encuentran: *Pulse*, *Distributed Tag Access with Collision-Avoidance* y *Enhanced Distributed Tag Access with Collision-Avoidance*.

Existen propuestas en la literatura que han adaptado protocolos de detección de objetos perdidos a arquitecturas de este tipo con el propósito de cubrir las necesidades de sistemas RFID de gran escala, un ejemplo de ello es [18].

Distribución basada en *fielders* o *cluster-heads*: La distribución del proceso de comunicación puede lograrse sin la implementación de varios lectores. El esquema propuesto en [19] por los autores de PDC, implica la dispersión de las funciones convencionales de los lectores en entidades espacialmente distribuidas dentro de la zona de interrogación. La arquitectura propuesta permite crear microzonas, como se muestra en la Figura 2.1, e implementar una nueva clase de algoritmos anticolisión, como el de **Identificación Paralela** [20], el cual está basado en teoría de árboles binarios de búsqueda y permite generar identificaciones paralelas al seccionar la zona de identificación en varias "microzonas". Se mantiene una instancia independiente del árbol por cada microzona, y es posible identificar una etiqueta a la vez por cada microzona. Por lo tanto, es posible identificar de forma simultánea tantas etiquetas como microzonas se generen. La arquitectura resulta novedosa en el sentido de que el esquema centralizado o tradicional emplea un enlace de comunicación lector-etiquetas (enlace de subida) y otro en sentido inverso (enlace de bajada), mientras que la propuesta distribuida permite establecer múltiples enlaces paralelos para cada efecto.

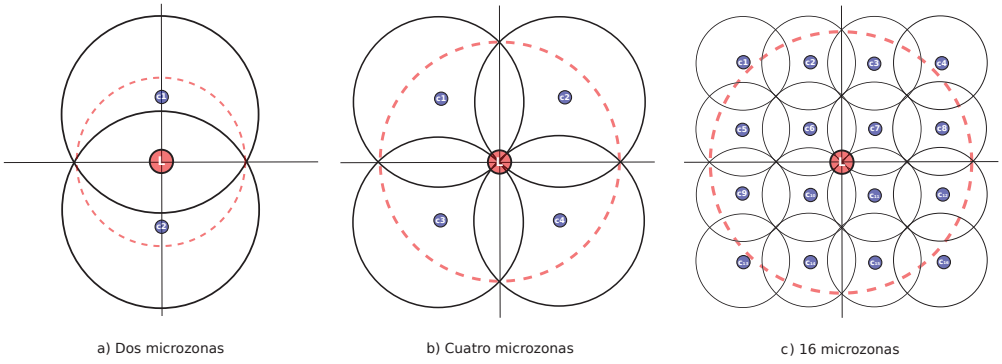

FIGURA 2.1: Seccionamiento en microzonas del área de interrogación.

Básicamente, la arquitectura propuesta descentraliza las funciones del lector y delega algunas a un nuevo elemento del sistema RFID, llamado *fielder*. El término *fielder* es utilizado de forma intercambiable con el término *cluster-head*. La tarea principal de los *fielders* es la recolección y procesamiento de la información generada por las etiquetas en una microzona, para su posterior entrega a los lectores correspondientes. Los diversos *fielders* que encabezan la comunicación en las microzonas, comunican la información recibida y procesada a los lectores y a otros *fielders* suscritos a ellos, vía *multicast*, creando una comunicación multipunto-multipunto.

Los lectores difunden consultas hacia las etiquetas en un canal y reciben información de los *fielders* en otro, como se observa en la Figura 2.2. El segundo canal se diseña como un canal de comunicación de baja potencia mediante el uso de protocolos como ZigBee. Las colisiones entre los *fielders* se resuelven al igual que se hace con las colisiones entre lectores, dado que son dispositivos con capacidades de energía y procesamiento suficientes, para implementar mecanismos de monitorización de canal. Las etiquetas propuestas para funcionar en esta arquitectura son capaces de modificar su coeficiente de reflexión utilizando la información recibida en una consulta, de forma que la señal reflejada por cada etiqueta no abandone la microzona generada por el *fielder*, y no interfiera con otras fuera de su microzona.

Es importante mencionar que, con base en nuestro conocimiento, no existe trabajo alguno en donde se haya propuesto la adaptación de un protocolo de detección de objetos perdidos a esta arquitectura distribuida.

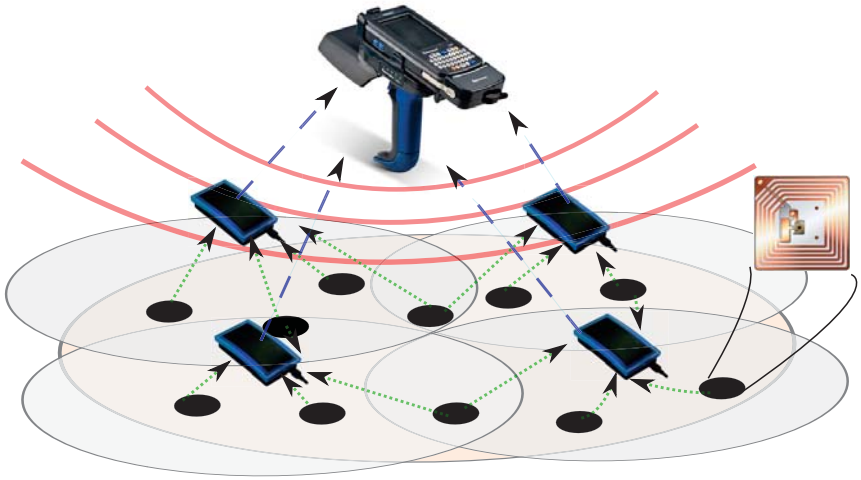

FIGURA 2.2: Esquema de comunicación de la arquitectura basada en *fielders*.

Distribución basada en *listeners*: La propuesta más reciente que respalda la adopción de una arquitectura distribuida para sistemas RFID aparece en [21]. Se mantiene la idea de la delegación de las funciones de los lectores hacia otros dispositivos. Sin embargo, dicha separación de funciones se realiza mediante el desacoplamiento físico de la transmisión y la recepción en el lector. Se introduce la figura de un "RFID *listener*", que realiza las funciones de recepción, mientras que el lector conserva las de transmisión. Es importante hacer notar que el *listener* es capaz de escuchar las transmisiones de las etiquetas, pero también las de los lectores, lo cual es necesario para decodificar los mensajes de las etiquetas. El problema asociado con las colisiones entre lectores desaparece bajo esta arquitectura debido a que existe un solo lector capaz de transmitir dentro del área de identificación.

La introducción de la figura del *listener* permite utilizar un lector con potencia suficiente para interrogar un área sin preocuparse por la capacidad de las etiquetas para retrodispersar la energía almacenada de la solicitud. Lo anterior es posible debido a que los *listeners* se encuentran mucho más cerca de las etiquetas que el lector y son capaces de recibir la respuesta. En este escenario es posible implementar mecanismos de *escucha cooperativa*, la cual permite usar la información que los *listeners* obtienen de las colisiones para mezclarla e implementar técnicas, tales como la combinación suave y la cancelación de interferencia, que permitan recuperar la información aparentemente perdida cuando una colisión hubiere sido causada por sólo un par de dispositivos. Estas técnicas se conocen como Detección Multiusuario y pueden ser implementadas únicamente en escenarios distribuidos [21].

La propuesta requiere que todos los nodos involucrados, lectores y listeners, tengan acceso a un canal de control, ya sea cableado o inalámbrico, de forma que se posibilite la comunicación entre ellos y por lo tanto su cooperación. Se espera que el costo de infraestructura sea más bajo que el de implementar un escenario con múltiples lectores. La propuesta analiza los pros y contras del escenario distribuido respecto al centralizado y viceversa, sin la intención de afirmar que un esquema implique superioridad de desempeño. Ésta es una propuesta novedosa y aún no se han generado trabajos que evalúen su aplicabilidad en términos de costo-beneficio, o su viabilidad bajo la lupa de otras medidas de desempeño. Tampoco se han realizado esfuerzos por adaptar protocolos de detección de objetos perdidos a este esquema.

2.2. Detección de objetos perdidos

Sea cual sea el protocolo anticolisión implementado, se define una sesión de lectura como la unidad de ejecución del protocolo que se requiere para recolectar los ID de todas las etiquetas en el rango del lector. Partimos del hecho de que se cuenta con una base de datos o inventario que contiene todos esos ID y posibilita monitorizar los artículos que se almacenan en algún sitio de interés. En este contexto, existen algunos mecanismos que permiten identificar la ausencia de uno o varios elementos del conjunto de interés. Ejemplos de ellos son los que se describen a continuación.

Estimación de la cardinalidad: En torno al problema de detección de etiquetas perdidas, la primera intuición dicta resolverlo llevando a cabo un conteo o estimación de la cardinalidad del conjunto actual de etiquetas, para después comparar el número obtenido con la cantidad almacenada en una base de datos o en un inventario. Aunque la idea podría funcionar, no sería posible identificar con exactitud cuáles son las etiquetas que hacen falta en el conjunto, y existe cierta probabilidad de cometer errores si se utiliza un método estadístico o probabilístico para estimar la cardinalidad del conjunto actual.

Algunas aportaciones actuales en esta línea de investigación incluyen métodos estadísticos como los de [22], donde se presenta una aproximación llamada multi-captura-recaptura (*multi–capture–recapture*), procedimiento que logra una alta confiabilidad mediante el uso de varias sesiones de lectura. En general, los métodos de captura-recaptura son métodos estadísticos utilizados para estimar el tamaño de una población. El estimador más simple se llama *Lincoln-Petersen*, el cual utiliza dos sesiones de detección o visitas al conjunto de objetos que se desea monitorizar y del cual se desconoce la cardinalidad. En la primera de ellas, identifica a cierto número n_1 de individuos de una población y los marca antes de dovolverlos. En la segunda visita, identifica otro número n_2 de individuos además de que se observa que un cierto número m de individuos había sido previamente marcado. Entonces, se estima el tamaño de la población mediante la expresión $\frac{n_1 n_2}{m}$. Este método se generaliza en [22] para el caso en el que se generan más de dos sesiones o visitas. También, se evalúan otros estimadores como el de Schnabel y el estimador multipaso, obteniendo resultados positivos. En términos de tecnología RFID, los errores en el medio de comunicaciones y las colisiones representan factores que impiden

realizar un conteo simple de los integrantes de un conjunto de etiquetas, de ahí que esta clase de métodos permitan inferir la cardinalidad de un conjunto de etiquetas RFID.

Resulta evidente que en caso de que se estime con muy alta probabilidad que se han identificado exitosamente la totalidad de objetos presentes en el área (x), y además al comparar x con el número y de objetos identificados en procesos previos, entonces es posible afirmar que x - y artículos no están presentes en el espacio en que deberían, pero no sería posible conocer específicamente cuáles son las etiquetas faltantes.

El principio fundamental de la propuesta [22] se basa en dos sesiones de lectura independientes por parte de dos lectores diferentes, los cuales son capaces de actuar de forma cooperativa e intercambiar la información de sus lecturas. Dicho proceso arroja tres resultados: 1) el número de etiquetas identificadas por ambos lectores (k_1), 2) el número de etiquetas identificadas únicamente por el primer lector (k_{2a}) y 3) el número de etiquetas identificadas únicamente por el segundo lector (k_{2b}). La idea principal es que a partir de los valores conocidos k_1, k_{2a} y k_{2b} es posible estimar el número de etiquetas presentes pero no identificadas por ninguno de los lectores, la cardinalidad del conjunto de etiquetas y la probabilidad de que una etiqueta presente en el conjunto, no logre ser leída durante ninguna de las sesiones de lectura. Esta probabilidad disminuirá si se llevan a cabo más sesiones de lectura y de esta forma es posible garantizar que se mantenga en un nivel tolerable. De forma similar, es posible estimar el número de sesiones de lectura requeridas para obtener cierta probabilidad de detección errónea. La propuesta se extiende a la estimación de estos parámetros cuando se utilizan más de dos lectores, y cuando las lecturas actuales no son independientes de las previas.

Omisión de identificadores: En [12], se presenta el trabajo pionero sobre detección de marcas perdidas que ha servido como base de la investigación actual en dicho contexto. Los autores proponen un procedimiento de monitorización de etiquetas RFID que no requiere que las etiquetas transmitan la totalidad de su ID, minimizando así el tiempo de lectura y obteniendo una estimación confiable de la cantidad de etiquetas presentes en el área de lectura. Una vez conocido el número de etiquetas presentes, es posible establecer un umbral fuera del cual, la falta de etiquetas representa un problema.

Se propone el Protocolo de Lector Confiable (*Trusted Reader Protocol* o TRP). TRP basa su funcionamiento en el protocolo anticolisión SA, siendo la principal diferencia que las etiquetas no transmiten la totalidad de su ID en la ranura de tiempo seleccionada, sino que responden con una pequeña cadena de bits aleatorios, alertando al lector de que han elegido esa ranura de tiempo. La selección de la ranura corresponde a una función hash que involucra al ID de cada etiqueta, el tamaño de trama f y un número aleatorio r anunciado por el lector en su consulta inicial. De esta forma, es posible determinar cuántas etiquetas, cuyos ID se conocen previamente en la base de datos de un servidor, han elegido cierta ranura para transmitir. Una vez concluida una trama, el servidor recibe una cadena de bits correspondiente a las ranuras de tiempo en las cuales hubo respuestas (1) y aquellas en las cuales no hubo respuestas (0), lo cual le permite determinar si dicha cadena corresponde a un conjunto de etiquetas completo o incompleto, con cierta certeza. La propuesta incluye el análisis que permite seleccionar el tamaño de trama f dado cierto umbral de tolerancia m, que determina que un conjunto está intacto si se detectan a lo más m etiquetas perdidas, e incompleto cuando se detecta que faltan por lo menos $m+1$ etiquetas, y confiabilidad α, que es la probabilidad de detectar adecuadamente que un conjunto de etiquetas está incompleto.

Detección específica: La propuesta planteada en [12] no permite conocer cuáles son las etiquetas específicas que abandonaron el área de interrogación. A partir de estas consideraciones, en [9] se describe un conjunto de técnicas que permiten mejorar el desempeño del proceso de detección de etiquetas perdidas, con el objetivo de brindar certeza al mecanismo de comparación y permitir la detección exacta de las etiquetas faltantes, si las hubiere.

Se proponen cuatro protocolos. Cada uno de ellos suma una nueva técnica, teniendo todas en común la transmisión de un solo bit por parte de las etiquetas al responder, de forma que adviertan al lector su presencia, sin la necesidad de enviar todo su ID. El protocolo que muestra el mejor desempeño se denomina **Protocolo Iterativo Sin-ID** (*Iterative ID-free Protocol* o IIP), e inicia cuando el lector envía la solicitud que contiene a f y r, además de contener un vector pretrama que consiste de f bits y contiene el estado esperado de cada ranura, 0 si no se esperan respuestas o se espera una sola respuesta, o 1 si se espera una colisión. Cada etiqueta elige una ranura para transmitir un bit de su identificador usando una función hash, si alguna

etiqueta nota que se ha mapeado en una ranura colisionante, decidirá mediante otra función de hash si transmitirá o no. El lector es capaz de saber qué etiquetas no participarán, qué ranuras recibirán una sola respuesta y cuáles colisionarán. El lector sabe que una etiqueta no está presente en el área de detección si ésta no responde cuando se esperaba que lo hiciera. Evidentemente, al suceder una colisión, no es posible saber cuantas etiquetas estuvieron involucradas en ella, dado que alguna de las que seleccionaron dicha ranura puede estar perdida. Si ninguna etiqueta responde durante una trama, el lector la repite utilizando un vector pretrama de ceros, el cual le solicitará a las etiquetas restantes que pudieran existir, que transmitan. Si aún así ninguna etiqueta responde, el protocolo termina. Tras la respuesta de las etiquetas en una trama, el lector verifica el estado de las ranuras y construye un vector postrama de f bits, cada uno de los cuales indica el estado actual de cada ranura (0 para vacío o colisión y 1 para una sola respuesta), es aquí en donde el lector detecta la presencia o ausencia de las etiquetas que seleccionaron una ranura de forma única. La presencia de las etiquetas en las ranuras de una sola respuesta se verifica y el lector las silencia. El lector transmite el vector postrama. Si una etiqueta nota que ha sido mapeada a una ranura con una sola respuesta, no participará de ese momento en adelante. El lector inicia una nueva trama con un tamaño menor, y el proceso continúa.

En [23], se presenta una propuesta para solventar la necesidad de minimizar el tiempo de detección de etiquetas perdidas en sistemas RFID. Se propone un método estadístico dirigido a un ambiente de etiquetas activas que permita, además de minimizar el tiempo de detección, prolongar la vida útil de las etiquetas mediante un manejo energéticamente eficiente de las mismas. La idea principal de esta propuesta proviene de las consideraciones hechas en [12] para el protocolo TRP. La primera diferencia yace en la adopción del principio probabilístico ejemplificado por la "paradoja del cumpleaños". El principio establece que dentro de un conjunto de n personas elegidas al azar, la probabilidad de que un par de ellas comparta el mismo día de cumpleaños alcanza el 100 % cuando $n = 367$. Sin embargo dicha probabilidad alcanza el 99 % con sólo 57 personas y el 50 % con 23 personas. De forma similar, dos conjuntos de etiquetas RFID podrían tener una probabilidad alta de compartir un miembro (etiqueta). Tomando en cuenta que uno de esos dos conjuntos es aquel formado por las etiquetas perdidas y el otro es aquel formado

por k etiquetas tomadas de n existentes en el conjunto original, entonces el lector puede llevar a cabo un proceso de verificación de la presencia de las k etiquetas tomadas del conjunto original. Si el lector no recibe respuesta de alguna de las k etiquetas consultadas, reporta la detección de un evento de pérdida. La idea reside en que para un conjunto suficientemente grande de k etiquetas, dicho conjunto y aquel formado por las etiquetas perdidas, tienen una alta probabilidad de compartir una etiqueta en común. De forma breve, si el lector no es capaz de confirmar la presencia de al menos una etiqueta de k consultadas, asumirá que un evento de pérdida se ha presentado. La propuesta planteada inicialmente es considerada por los autores como un protocolo intermedio.

El protocolo principal es nombrado **Protocolo Eficiente para la Detección de Etiquetas Perdidas** (*Efficient Missing-Tag Detection Protocol* o EMD). EMD inicia con el lector difundiendo una consulta que contiene el tamaño de la trama f, un número aleatorio r y un entero x. Tras la recepción de la consulta, cada etiqueta implementa una función hash que utiliza su propio ID y el número r como parámetros. Si el resultado de la función es menor que el valor x, la etiqueta participará en la monitorización consecuente. De cualquier otra forma, ésta permanecerá en silencio hasta la siguiente ronda. Si la etiqueta decide participar en la monitorización, implementa una segunda función hash (distinta a la primera) con los mismos parámetros, para determinar la ranura de tiempo en la que transmitirá. La base de datos, cuenta con la información necesaria para determinar cuáles de las etiquetas debieron haber participado en la monitorización, y de haberlo hecho, cuáles debieron responder en cada ranura de tiempo. De la misma forma, se sabe cuáles ranuras se encontrarán vacías y cuales ocupadas, ya sea por una sola respuesta o por una colisión. Al término de la trama, si el lector encuentra vacía una ranura de tiempo que debiera estar ocupada, determina que la etiqueta correspondiente se encuentra perdida. Los resultados son comparados con aquellos obtenidos en [12], pero no se toma en cuenta el caso más complejo, en el cual únicamente una etiqueta se pierde.

La propuesta más actual en torno a la detección de etiquetas perdidas en sistemas RFID aparece en [18]. Contiene tres protocolos para la rápida detección de etiquetas perdidas en sistemas RFID de gran escala, sin necesidad de recabar explícitamente todos los ID en cada ocasión. A diferencia de propuestas similares [9, 12], en [18] se utiliza un

esquema multilector que reduce las colisiones entre etiquetas seccionando el conjunto en L zonas de detección, cada una cubierta por uno de los L lectores. Las zonas de detección tienen regiones de traslape de forma que la cobertura abarque la totalidad del espacio disponible. Se asume que las transmisiones de los lectores adyacentes no causan interferencia entre ellas, dado que el servidor instruye a los lectores a transmitir de forma síncrona, esto es, en instantes de tiempo durante los cuales los lectores adyacentes permanecen en silencio. Sin embargo, los lectores que se encuentran físicamente distantes pueden transmitir de forma simultánea. Por lo tanto, también se asume que cada lector es capaz de comunicarse con la base de datos mediante un enlace de alta velocidad.

Los protocolos propuestos basan su funcionamiento en el protocolo anticolisión FSA. Consisten de múltiples rondas o ciclos. En cada ronda, el servidor instruye a los lectores para que realicen un barrido sincronizado para después procesar la información que le sea devuelta. Cada ronda de lectura se lleva a cabo en un esquema intrazona, de modo similar a las implementaciones anteriormente estudiadas. Tras la conclusión de una ronda en todas las zonas, el servidor es capaz de determinar que una etiqueta ha abandonado la zona de detección si no es posible encontrarla en ninguna de las secciones analizadas.

Al protocolo de mejor desempeño en esta propuesta lo llamamos, para fines de referencia en este trabajo, **Protocolo Base**, también implementa múltiples rondas en un proceso iterativo. Inicia cuando el lector implementa algunas actividades previas a la comunicación con las etiquetas, la primera de ellas es determinar el tamaño de la trama requerida por el protocolo FSA. En términos del estándar EPC Gen2, el tamaño de trama se advierte a las etiquetas desde el lector mediante la transmisión de un mensaje $QueryPB$ que contiene el parámetro Q, el cual es simplemente un número de cuatro bits mediante el cual se codifica el tamaño real de la trama. Cuando las etiquetas reciben el valor de Q, ejecutan la función $f = (2^Q) - 1$ y determinan que el tamaño real de la trama consta de 2^Q ranuras temporales en el intervalo $[0, f]$. En este sentido, se requiere determinar un número Q adecuado para cierta cardinalidad del conjunto de etiquetas. La Figura 2.3 muestra la representación gráfica de una trama de FSA.

Una vez que el lector determina el parámetro Q, genera un número aleatorio r de 64 bits. Recordemos que el lector tiene acceso a una base de datos que contiene los ID de todas las etiquetas participantes, de forma que es capaz de generar un *vector preconsulta*, el cual corresponde a una secuencia de pares de números, en donde cada par representa el

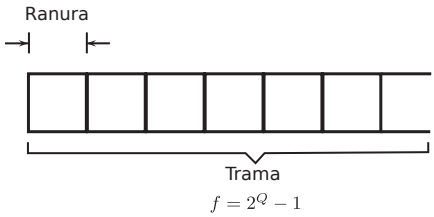

FIGURA 2.3: Representación gráfica de una trama del protocolo FSA.

suceso esperado en cada ranura de tiempo. Para llenar el vector, el lector ejecuta una función hash que involucra al número aleatorio, el ID de cada etiqueta y el tamaño de la trama, y determina la ranura que elegirá cada etiqueta para transmitir cuando realicen exactamente la misma operación. Si ninguna de las etiquetas elige cierta ranura, el lector escribe 00 en el vector, si únicamente una etiqueta elige cierta ranura, el lector escribe 01 en la posición correspondiente a dicha ranura sobre el vector, y si más de una etiqueta elige alguna ranura, se escribe 11 sobre el vector. La Figura 2.4 corresponde a un ejemplo de un vector preconsulta.

En este punto, el lector se encuentra en condiciones de iniciar la comunicación con las etiquetas. El lector difunde una consulta que contiene a los parámetros Q y r. Las etiquetas reciben la consulta, determinan el parámetro f e implementan la misma función hash que el lector, eligiendo así la ranura que el lector ha predicho. Las etiquetas cargan un contador con el número seleccionado, si alguna hubiere elegido el número cero, transmite inmediatamente una respuesta que contiene diez bits de su identificador. El lector continúa transmitiendo tantas consultas *QueryRep* como ranuras existan en la trama, y cada etiqueta decrementa su contador al recibir una consulta de este tipo hasta que su contador se encuentre en cero y pueda transmitir. Cuando el lector, al revisar su vector de preconsulta, espera la respuesta de una sola etiqueta y no la recibe, notifica un evento de pérdida. Sin embargo, si se espera una ranura vacía o una colisión, no es posible extraer información válida sobre la presencia o ausencia de alguna etiqueta, ya que una colisión se interpreta como tal sin importar el número de etiquetas involucradas en la misma.

00	01	11	00	11	01	

FIGURA 2.4: Ejemplo de un vector preconsulta.

Al terminar una trama, el lector envía un *vector de silenciamiento* mediante el cual solicita a las etiquetas que ya fueron detectadas, que no participen en rondas siguientes. A continuación, el lector genera un nuevo número r e inicia una nueva trama que involucra el mismo número de ranuras pero una menor cantidad de etiquetas, esperando que esta vez elijan ranuras distintas y se pueda detectar presentes o perdidas a más de ellas. El protocolo concluye cuando todas las etiquetas han sido detectadas presentes o perdidas, y el lector difunde un comando de reinicio para permitir que las etiquetas participen en futuros procesos de comunicación.

Capítulo 3

Propuesta

3.1. Consideraciones sobre el Protocolo Base

Existen estudios, como aquel plasmado en [24], que aportan un análisis profundo sobre la elección de un valor óptimo para Q dada cierta cardinalidad conocida del conjunto de etiquetas. De esta referencia obtenemos la Tabla 3.1, la cual reporta los resultados experimentales obtenidos al aplicar todos los valores del parámetro Q a conjuntos de etiquetas con cardinalidades en el rango $[1, 32767]$ y determinar cuál de esos valores produce un tamaño de trama más cercano al ideal, recordando que el tamaño de trama ideal se considera igual a la cardinalidad del conjunto de etiquetas.

Para obtener una evaluación justa y confiable, utilizamos el mencionado mecanismo de selección del tamaño de trama para todos los protocolos (Base y propuestas) por considerarlo el más adecuado tomando en cuenta las condiciones de nuestro problema de investigación, y a pesar de que esto significa no poder utilizar directamente los resultados publicados originalmente por los autores del Protocolo Base.

Otra consideración de nuestra implementación del Protocolo Base se refiere a la cantidad de lectores y zonas de detección. El estudio realizado en [18] se extiende a L lectores y zonas, mientras que este trabajo considera únicamente un lector y una zona, lo cual corresponde simplemente al caso en que $L = 1$.

Q óptima	Cantidad de ranuras	Cantidad de etiquetas
1	2	$N < 2$
2	4	$2 \leq N < 4$
3	8	$4 \leq N < 9$
4	16	$9 \leq N < 20$
5	32	$20 \leq N < 42$
6	64	$42 \leq N < 87$
7	128	$87 \leq N < 179$
8	256	$179 \leq N < 364$
9	512	$364 \leq N < 710$
10	1024	$710 \leq N < 1430$
11	2048	$1430 \leq N < 2920$
12	4096	$2920 \leq N < 5531$
13	8192	$5531 \leq N < 11527$
14	16384	$11527 \leq N < 23962$
15	32768	$N \geq 23962$

TABLA 3.1: Q óptima dada la cardinalidad del conjunto de etiquetas.

3.2. Protocolo DOP

Una vez analizada la idea subyacente en los protocolos de detección de objetos perdidos publicados en los últimos años, proponemos tres mecanismos que permiten reducir el tiempo que toman las comunicaciones requeridas por un sistema RFID para detectar la presencia o ausencia de cada una de las etiquetas que componen un conjunto. Los tres mecanismos propuestos se incorporan en lo que denominamos *Protocolo de Detección de Objetos Perdidos (DOP)*, cuyo funcionamiento se detalla a continuación.

3.2.1. Mecanismo 1: Elección persistente del tamaño óptimo de trama

El *Protocolo DOP* inicia cuando el lector realiza algunas actividades previas al inicio de la comunicación, determina el tamaño de trama f óptimo para la detección de un conjunto de etiquetas, dada su cardinalidad, mediante la exploración de la Tabla 3.1. La integración de los resultados presentados en esta tabla y su uso periódico al inicio de cada ciclo de lectura, forman el primer mecanismo para la reducción de la duración del mismo.

Es importante destacar la diferencia que surge de este mecanismo en referencia al Protocolo Base, en el cual se elige un tamaño de trama al inicio y se mantiene constante

durante la ejecución del protocolo, propiciando tamaños de trama que se alejan del óptimo requerido por los protocolos basados en ALOHA en cada ciclo, mientras disminuye la cantidad de etiquetas por detectar. La Figura 3.1 compara las representaciones gráficas de las tramas correspondientes al Protocolo Base y al Mecanismo 1.

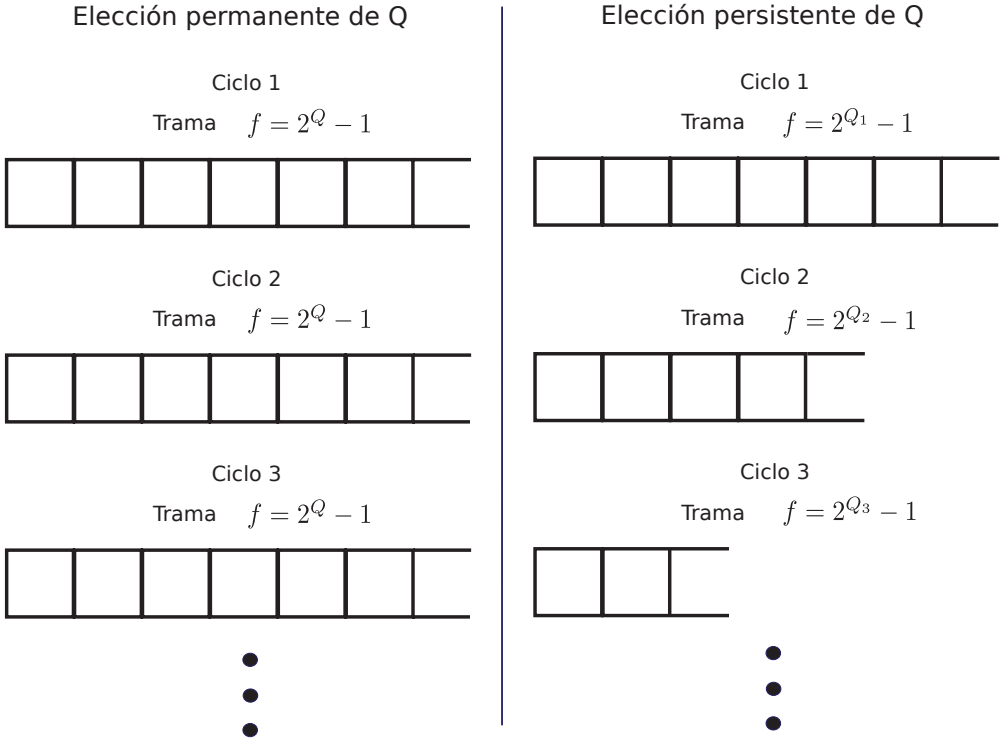

FIGURA 3.1: Tamaño de trama para el Protocolo Base y el Mecanismo 1.

3.2.2. Mecanismo 2: Recorte de trama

El siguiente paso, requiere que el lector genere un vector de observación esperada mediante la ejecución de una función hash $h(\mathrm{ID}\,\%r)\,\%f$ por cada identificador en la base de datos. En propuestas anteriores, como aquella de la que surge el Protocolo Base, no se especifica la función utilizada. Elegimos la función módulo dado que muestra un buen desempeño al dispersar la elección de las etiquetas a lo largo de la trama de forma equitativa, siempre y cuando la distribución de los ID tenga una distribución uniforme también, consideración que asumimos para abarcar un caso general, y por no tener evidencia de que se requiere asumir una distribución de los ID diferente.

El resultado de la función hash le permite al lector conocer la ranura temporal que elegirá cada etiqueta para transmitir su respuesta. El lector escribe 0 en cada ranura del vector que no fue seleccionada por ninguna de las etiquetas (ranura vacía) y 1 en aquellas ranuras seleccionadas por una o más etiquetas (ranura con una respuesta y ranura con colisión, respectivamente). El *Protocolo DOP*, a diferencia del Protocolo Base, no requiere que la capa física distinga cuando una ranura recibe una única señal de respuesta o varias (colisión) debido a que el lector cuenta con la información suficiente (base de datos y función hash) para deducir cuándo se espera una o más respuestas. Un ejemplo de un vector de preconsulta con estas características se muestra en la Figura 3.2.

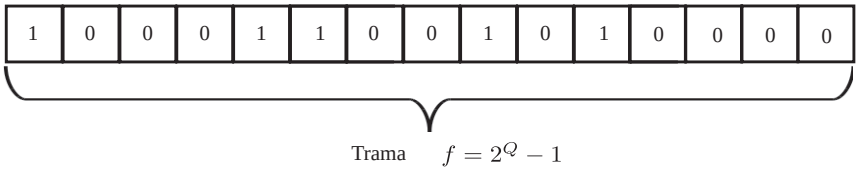

FIGURA 3.2: Ejemplo de vector preconsulta para el protocolo DOP.

Múltiples publicaciones actuales refieren que se requiere de la transmisión de al menos 10 bits de cada identificador para que el lector sea capaz de distinguir una colisión de una respuesta única, y un sólo bit para advertir su presencia [9, 18, 25]. Sin embargo, con el objetivo de llevar a cabo una comparación equitativa con el Protocolo Base, se considera que las etiquetas responden también con 10 bits de su identificador.

Posteriormente, el lector aplica el mecanismo denominado **Recorte de trama**, el cual consiste en identificar la última ranura que será elegida por alguna de las etiquetas y establecer en dicho punto el fin de la trama. Así, el fin de la trama se ubica en el último instante en el cual se espera tener comunicación con alguna etiqueta dado que las consultas posteriores no propiciarían ningún flujo de información desde las etiquetas hacia el lector, pero si requerirían tiempo de transmisión desde el lector y hacia las etiquetas, como sucede en el Protocolo Base. Como resultado de la aplicación de este mecanismo, el lector enviará consultas hasta terminar la búsqueda en una trama de tamaño $f' = f$ - X, en donde X corresponde al número de ranuras recortadas. La operación de este mecanismo se muestra gráficamente en la Figura 3.3.

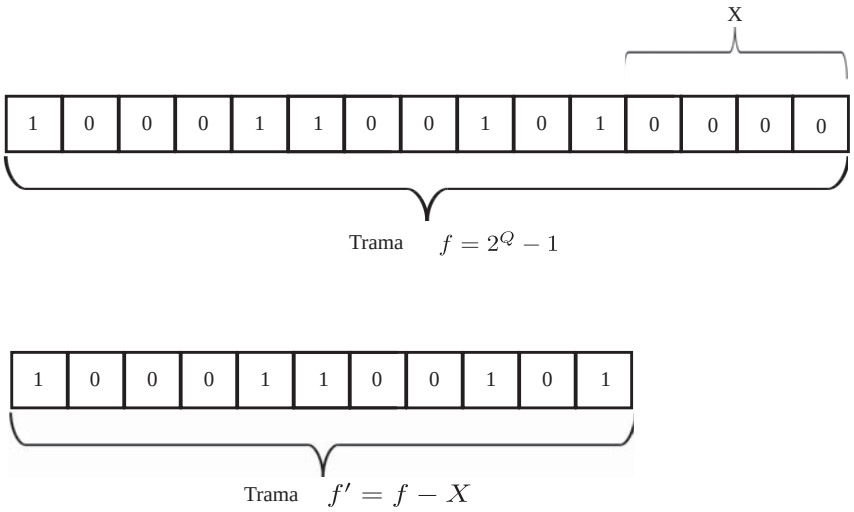

FIGURA 3.3: Representación gráfica de la operación del Mecanismo 2.

3.2.3. Mecanismo 3: Supresión de ranuras vacías y colisionantes

Una vez recortada la trama, el lector inicia el proceso de comunicación enviando una consulta $QueryDOP$ que contiene 22 bits correspondientes al tamaño de una consulta en el estándar EPC Gen2, más 64 bits del parámetro r y 15 bits del parámetro s. La inclusión del parámetro s corresponde a la implementación del tercer mecanismo reductor al que denominamos **Supresión de ranuras vacías y colisionantes**. Como su nombre lo indica, la función de este tercer mecanismo consiste en informar a las etiquetas la cantidad de ranuras vacías y colisionantes que se generaron entre ranuras que sí contienen información, decrementando así la cantidad total de consultas C que el lector difunde en el sistema, la cual resulta de restar la sumatoria de la totalidad de números que tome el parámetro s al tamaño de la trama recortada f'. Entonces, la Figura 3.4 muestra aquellas ranuras suprimidas y aquellas que sí requerirán del envío de transmisiones; nótese que en este ejemplo se suprimen algunas ranuras vacías (ceros) pero también una ranura colisionante (uno). La diferencia entre las ranuras con una respuesta y las colisionantes se distingue gracias a la inspección de la base de datos.

Tras la recepción de la primera consulta o $QueryDOP$, las etiquetas seleccionan una ranura para responder en el intervalo $[0, f']$, ejecutando la misma función hash utilizada por el lector, y copian el resultado en un contador individual que será decrementado en s unidades al recibir cada consulta $QueryRepDOP$, misma que también aumenta su tamaño desde los 4 bits, originalmente planteados en el estándar y el Protocolo Base,

hasta 19 bits, para incorporar en cada mensaje al parámetro s. Las etiquetas que hayan seleccionado la ranura cero para transmitir su respuesta, lo harán inmediatamente, mientras que el resto decrementará su contador en s unidades. El lector continuará el proceso difundiendo C consultas. Tras la aplicación del tercer mecanismo, todas las consultas generadas por el lector obtendrán una respuesta de una sola etiqueta. Aquellas ranuras en las que resultarían colisiones o ausencias de respuesta se ignoran para no perder energía y tiempo de transmisión en ellas. Al término de C consultas y sus respectivas respuestas, el ciclo de detección termina y el lector envía un vector de silenciamiento para solicitarle a todas aquellas etiquetas detectadas como presentes en la zona de detección, que no participen en ciclos posteriores. En ciclos posteriores, el lector iniciará la comunicación tras elegir nuevos parámetros Q, r y s. En cada consulta, se considera que una etiqueta está perdida si no responde en la ranura en la que se espera que lo haga. El protocolo termina cuando la totalidad del conjunto de etiquetas ha sido detectada, ya sea como presente o como ausente. Una vez finalizado el proceso de identificación, el lector transmite un comando de reinicio que le informa a todas las etiquetas que podrán participar en procesos posteriores.

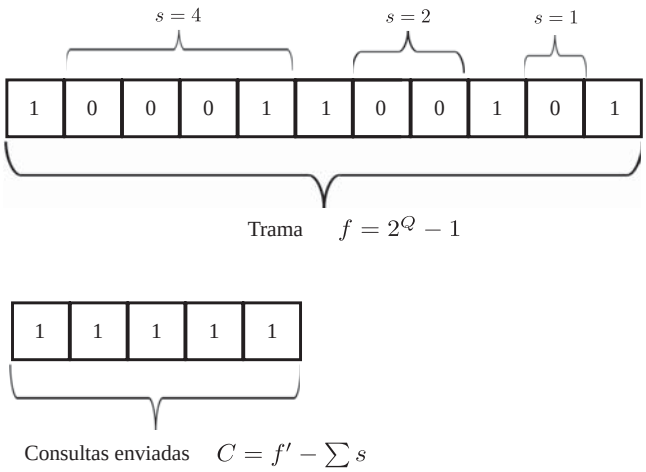

FIGURA 3.4: Representación gráfica de la operación del Mecanismo 3.

3.2.4. Operación detallada

Los Algoritmos 1 (`AR`) y 2 (`AT`) describen las actividades que llevan a cabo el lector y las etiquetas dentro del protocolo DOP, respectivamente. El protocolo DOP inicia realizando algunas tareas de autogestión, antes de iniciar la comunicación con las etiquetas (líneas

1-15 (AR)). El lector inspecciona la Tabla 3.1 para determinar el valor de Q óptimo, y por ende, el tamaño de trama f, con base en la cardinalidad del conjunto de etiquetas, reportado por la aplicación (líneas 6-7 (AR)). A continuación, el lector construye un vector previo o prevector compuesto por f ranuras virtuales, genera un número aleatorio de 64 bits y ejecuta la función hash $h(ID, r)\,\%f$ por cada etiqueta en la base de datos. El lector llena el prevector escribiendo 0 en cada ranura vacía y 1 en cada ranura con una sola respuesta o con colisión (línea 9 (AR)). Una vez que el prevector está lleno, el lector busca la última ranura elegida por una sola etiqueta y recorta o poda el resto de las ranuras sobrantes (líneas 10-14 (AR)). En este punto, el lector inicia la comunicación con las etiquetas mediante la difusión de un mensaje QueryDOP (línea 16 (AR)), el cual está compuesto por 22 bits del mensaje Query establecido por el estándar EPC Gen2 y 64 bits del número aleatorio r. Cuando las etiquetas reciben el mensaje, calculan $f = 2^Q - 1$ y ejecutan la función hash mencionada, de forma que seleccionan la ranura de tiempo que predijo el lector, y cargan el resultado en un contador k (líneas 4-7 (AT)). Si $k == 0$ para alguna etiqueta, ésta transmite de inmediato una respuesta que se construye con los primeros diez bits de su identificador (líneas 16-18 (AT)). El lector recibe las respuestas correspondientes, si existen, y verifica la presencia o ausencia de alguna etiqueta si le es posible (líneas 18-24 (AR)). Entonces, el lector inspecciona el prevector e incrementa el parámetro s tantas veces como ranuras vacías o con colisión encuentre entre ranuras con una sola respuesta (línea 26 (AR)). Ahora, el lector difunde un mensaje QueryRepDOP, el cual contiene cuatro bits del mensaje QueryRep descrito en el estándar EPC Gen2 y quince bits del parámetro s (líneas 27-28 (AR)). Cuando las etiquetas reciben este mensaje, decrementan su contador k en s unidades (líneas 8-9 (AT)), y aquella etiqueta cuyo contador $k == 0$ responde si está presente en la zona de detección, pero si no lo hace, la aplicación reporta un evento de pérdida (líneas 30-36 (AR)). Tras la difusión de C consultas y de sus respectivas respuestas o reportes de pérdida, el primer ciclo de detección termina y el lector difunde un vector de silenciamiento de f bits (línea 38 (AR)), instruyendo a las etiquetas recién detectadas para que permanezcan en silencio durante ciclos posteriores (líneas 11-14 (AT)). Para los siguientes ciclos de detección, el lector inicia la comunicación con las etiquetas difundiendo un mensaje QueryDOP que contiene nuevos parámetros Q y r. Cada vez que una etiqueta no responde en el instante en el que se espera que lo haga, se considera un evento de pérdida. El protocolo termina cuando todas las etiquetas de la base de datos han sido detectadas como presentes o

como perdidas y el lector difunde un comando `Reset` que le permite a las etiquetas previamente silenciadas, participar en futuros procesos de comunicación (línea 41 `(AR)`).

Algoritmo 1: AR Pseudocódigo del protocolo DOP para el lector

```
 1: N = GetTagsID();                                  # ID's
 2: n = #N;                                           # Cardinalidad del conjunto
 3: StateTag(N) = "None";                             # Inicializa el estado de cada etiqueta
 4: TotalTags = n;
 5: while ∃w ∈ N|StateTag(w) == "None" do
 6:     Q = FindFrame(TotalTags);                     # Selecciona el valor de Q en base a la Tabla 3.1
 7:     f = 2^Q − 1;
 8:     r = rng();                                    # Genera un número aleatorio
 9:     PreVectorFill(prevector, N, r);               # Llena el prevector con los resultados del hash
10:     for i = (f − 1) : 0 do                        # Busca la última ranura utilizada
11:         if prevector(i) == 1 then
12:             f' = i;                               # Nuevo término de trama
13:         end if
14:     end for
15:     DetectedTags = 0;
16:     Send(QuqeryFPSD);
17:     ans = ReceiveAnswers;
18:     if prevector(i) == ans and ans == 1 then
19:         StateTag(N(i)) = "Present";               # Recive una respuesta única
20:         SilenceVector(i) = "TRUE";                # La etiqueta N(i) está presente
21:         DetectedTags + +;
22:     else
23:         StateTag(N(i)) = "Absent";                # La etiqueta N(i) está ausente
24:     end if
25:     for i = 2 to f do
26:         s = RdrSlotCount();                       # Número de ranuras sin información
27:         i = i + s;                                # Ignora ranuras sin información
28:         Send(QuqeryRepFPSD);
29:         ans = ReceiveAnswers;
30:         if prevector(i) == ans and ans == 1 then
31:             StateTag(N(i)) = "Present";
32:             SilenceVector(i) = "TRUE";
33:             DetectedTags + +;
34:         else
35:             StateTag(N(i)) = "Absent";
36:         end if
37:     end for
38:     Send(SilenceVector);
39:     TotalTags = TotalTags − DetectedTags;
40: end while
41: Send(Reset);
```

Algoritmo 2: AT Pseudocódigo del protocolo DOP para la etiqueta

```
 1: Detected=false;
 2: Receive(Message);
 3: while not Detected do
 4:     if Message == QueryFPSD then
 5:         f = 2^Q − 1;
 6:         k = h(ID, f);
 7:         t = k;
 8:     else if Message == QueryRepFPSD then
 9:         k = k − s;
10:     else if Message = SilenceVector then
11:         if SilenceVector(t) == 1 then
12:             Detected = True;
13:             Break;
14:         end if
15:     end if
16:     if k == 0 then
17:         Send(P − ID);
18:     end if
19: end while
```

3.3. Protocolo DDOP

En los últimos años, se ha observado una tendencia en la investigación por dar un giro al paradigma de comunicación en los sistemas RFID. Se ha explorado el reemplazo de las arquitecturas tradicionales de comunicación, que exponen un modelo centralizado, por arquitecturas distribuidas que permitan eficientar los procesos inherentes a esta tecnología. Especialmente, se ha estudiado el comportamiento del proceso de identificación de etiquetas RFID, las ventajas y desventajas que experimenta al desarrollarse sobre arquitecturas centralizadas o distribuidas, y la adaptación de protocolos inicialmente diseñados para desempeñarse dentro del esquema tradicional de comunicación a los nuevos esquemas.

La tarea de adaptar un protocolo para la detección de objetos perdidos a una arquitectura RFID distribuida no es simple, es más bien compleja debido a la naturaleza de la propuesta medular de esta clase de algoritmos. Recordemos que la detección de objetos perdidos se basa en la premisa de que el lector conoce o tiene acceso a la información de la base de datos, y por lo tanto, es capaz de utilizarla para detectar a cada una de las etiquetas como presente o como perdida. Ahora bien, si se plantea la incorporación de dispositivos de bajo costo para descentralizar funciones del lector, estas nuevas entidades no serán capaces de acceder a la base de datos, dado que se pretende que tengan capacidades de memoria y procesamiento limitadas. Entonces, se requiere, abordar otros métodos mediante los cuales se pueda sacar provecho de estas arquitecturas en el proceso de detección.

En esta sección, analizamos algunas modificaciones necesarias para que el protocolo DOP pueda desempeñar sus funciones en la nueva arquitectura basada en *fielders* [19]. A la nueva propuesta le llamamos *Detección Distribuida de Objetos Perdidos (**DDOP**)*. En principio, la mayor ventaja de DOP sobre los protocolos propuestos en la literatura yace en la capacidad de eliminar la transmisión de las ranuras que experimentarán colisiones o que quedarán vacías. Para DDOP, el envío de las consultas correspondientes a las ranuras colisionantes es necesario. Asumamos que se cuenta con una función hash capaz de provocar que tantas etiquetas como microzonas haya disponibles en el sistema elijan la misma ranura temporal para transmitir su respuesta. A esta selección le llamamos *colisión hash*. Para lograr detecciones simultáneas, se requiere que exista

una colisión hash y que las etiquetas involucradas en la misma se encuentren espacialmente situadas en microzonas diferentes, además de estar fuera de cualquier zona de traslape, de forma que sus respuestas no causen una colisión electromagnética en el *fielder*. Esta situación permitiría detectar la presencia o ausencia de todas las etiquetas involucradas en la ranura temporal actual. El protocolo inicia con la realización de las mismas actividades previas que DOP, se envía una consulta $QueryDOP$ y las etiquetas eligen una ranura para transmitir su respuesta, utilizando la función hash que se mencionó previamente. Las etiquetas responden a sus *fielders* correspondientes, mismos que retransmiten las respuestas vía ZigBee hacia el lector, uno a la vez, siempre y cuando no hayan experimentado una colisión física en su propia microzona. Esta última actividad detiene el proceso paralelo y lo vuelve secuencial. Si no se experimentaran colisiones en los *fielders*, el tiempo de ejecución del protocolo se vería dramáticamente reducido, sin embargo, resulta evidente la dificultad que representa el contar con una función hash de las características requeridas y encontrarse en la realidad con un caso en el que justo las etiquetas requeridas para elegir cierta ranura se encuentren también distribuidas de forma adecuada.

Capítulo 4

Evaluación

4.1. Herramientas de simulación

La simulación de redes es una técnica en la cual un programa computacional modela el comportamiento de una red, ya sea calculando la interacción entre los diferentes entes en la red, usando fórmulas matemáticas o capturando y reproduciendo observaciones de una red en producción. El comportamiento de la red, así como de las aplicaciones y servicios que soporta, pueden ser observados en un ambiente de laboratorio cuyos atributos pueden ser controlados y modificados para establecer distintas condiciones de funcionamiento. Un simulador predice el comportamiento de una red sin la necesidad de construirla físicamente. Usualmente, dicha red es modelada mediante las entidades individuales que la componen (dispositivos, flujos de información, etc.) con el objetivo de variar las características de esos elementos y analizar los resultados correspondientes.

De esta manera, es posible generar una amplia gama de escenarios diferentes a un costo muy bajo (comparado con una implementación real). De cualquier forma, los simuladores no son capaces de modelar con exactitud todos los detalles de una red, pero pueden acercarse a la realidad lo suficiente como para aportar datos cruciales sobre la influencia de cada uno de los atributos de la red en la operación de la misma.

En la actualidad, existen varias alternativas para la simulación de eventos discretos [1, 26]. La simulación de eventos discretos es capaz de generar una lista de eventos pendientes o calendarizados que se suscitan al transcurrir el tiempo de simulación. Se pueden contabilizar más de 10 herramientas disponibles para la simulación de redes [27].

Ejemplos de ellos son: *Network Simulator* (**NS**), **TOSSIM**, **OMNeT++**, **OPNET** (*Optimized Network Engineering Tools*), **J-sim** y *Global Mobile Information System Simulator* (**GloMoSim**). Sin embargo, ninguno de ellos proporciona herramientas para simular escenarios RFID. A pesar de que NS, en sus versiones 2 y 3, permite crear módulos propios y adherirlos al núcleo del simulador para generar escenarios específicos, el contexto de la detección de objetos perdidos en sistemas RFID continúa a la espera de una aportación en este sentido.

Como alternativa a la simulación de eventos discretos, la simulación numérica proporciona las herramientas suficientes para analizar el comportamiento de sistemas de bajo dinamismo como aquellos centrados en la detección de objetos perdidos en sistemas RFID. Así, algunas herramientas de cálculo nos permiten evaluar el comportamiento temporal de los protocolos estudiados. Dadas las condiciones mencionadas, los resultados presentados en este trabajo corresponden a simulaciones numéricas implementadas en MATLAB y sus representaciones gráficas generadas con la misma herramienta. MATLAB está disponible en plataformas Windows y Unix, y cuenta con una interfaz de usuario simple acompañada de un lenguaje de alto nivel que permite agilizar el desarrollo de las simulaciones, además de incorporar generadores de gráficos de gran versatilidad.

4.2. Protocolos centralizados

4.2.1. Escenarios de evaluación

La mayor parte de las aplicaciones de la detección de objetos perdidos en sistemas RFID requieren de protocolos de corta duración temporal, de forma que puedan tomarse acciones oportunas en caso de presentarse un evento de pérdida, por ejemplo, detectar la pérdida de un objeto antes de que un ladrón se aleje de una tienda, y poder detenerlo. Por ello, la medida de desempeño es el tiempo que toma al protocolo transmitir los mensajes necesarios para detectar la presencia o ausencia de la totalidad de las etiquetas de un conjunto.

Se desarrolló una plataforma de simulación en MATLAB sobre la cual se implementaron los protocolos y mecanismos descritos con anterioridad, en igualdad de condiciones. En todos los casos, se considera que el tiempo requerido para la transmisión y recepción

de mensajes toma en cuenta la estructura descrita en el estándar EPCglobal Class-1 Gen-2 (preámbulos, tramas de sincronización, tiempos de guarda, etc.) [13, 24, 28], conforme a lo referido en la Tabla 4.1. En todos los casos, se simula que una sola etiqueta está perdida, lo cual representa el peor o más complicado de los casos, dado que el resto de las etiquetas responderán generando un mayor número de colisiones, lo cual significa un aumento en la cantidad de transmisiones, y por lo tanto, incremento del tiempo de ejecución. Cada punto en las gráficas representa el promedio de $50,000$ simulaciones utilizando la misma base de datos. Dicha cantidad de simulaciones, garantiza la obtención de resultados dentro de un intervalo de confianza del $95\,\%$ con un error menor a 0.001.

El escenario de simulación comprende a un conjunto de etiquetas, cuyos ID se generan de forma aleatoria con distribución uniforme, cuya cardinalidad varía desde 50 hasta $2,000$ con aumentos de 50 unidades. En consideración a la equidad de la comparación, ambos protocolos utilizan el mismo mecanismo de cálculo de Q, la misma función hash y el mismo conjunto de etiquetas. Si se considera el intervalo de confianza mencionado, es necesario generar aproximadamente $2,500$ simulaciones, por lo tanto se determinó exceder este número.

Parámetro	**Símbolo**	**Valor**
Código Electrónico del Producto	EPC (ID)	96 bits
Tiempo de referencia para "data-0" en la señalización Lector-Etiqueta	TARI	12.5μs
Duración de "data-0" en la señalización Lector-Etiqueta	DATA0	1.0 TARI
Duración de "data-1" en la señalización Lector-Etiqueta	DATA1	1.5 TARI
Símbolo de calibración Etiqueta-Lector	TRcal	64μs
Símbolo de calibración Lector-Etiqueta	RTcal	31.25μs
Factor de División	DR	8
Frecuencia de Retrodispersión	LF	DR/TRcal
Número de ciclos de subportadora por símbolo en dirección Etiqueta-Lector	M	1,2,4,8
Tasa Lector-Etiqueta	Rtrate	64 kb/s
Tasa Etiqueta-Lector	Trrate	LF/M
Intervalo de Repetición del Pulso en el Enlace	T_{pri}	$1/LF$
Preámbulo Etiqueta-Lector	TRP	$6T_{pri}$
Fin de la Señalización Etiqueta-Lector	T-R EoS	$2T_{pri}$
Delimitador	Del	12.5μs
Preámbulo Lector-Etiqueta	RTP	Del+DATA0+TRcal+RTcal
Trama de Sincronización Lector-Etiqueta	RTF	RTP-RTcal
Tiempo entre la transmisión del lector y al respuesta de la etiqueta	T_1	Max(RTcal,$10T_{pri}$)
Tiempo entre la respuesta de la etiqueta y la transmisión del lector	T_2	$5T_{pri}$
Tiempo que el lector espera, después de T_1 antes de enviar otro comando	T3	$5T_{pri}$
Tiempo mínimo entre comandos del lector	T_4	2RTcal
Paquete "Query"	Query	22 bits
Paquete "QueryRep"	QuerRep	4 bits
Paquete "QueryPB"	QueryPB	$22 + 64$ bits
Paquete "QueryDOP'	QueryDOP	$22 + 64 + 15$ bits
Paquete "QueryRepDOP"	QuerRepDOP	$4 + 15$ bits
Tamaño de respuesta	TagReply	10 bits

Tabla 4.1: Parámetros de simulación.

Extrapolando el esquema de comunicación planteado en el estándar para un proceso de identificación al terreno del proceso de detección de objetos perdidos podemos calcular el tiempo que le toma a un lector enviar un mensaje a las etiquetas y esperar hasta recibir una respuesta usando la siguiente expresión:

$$T_{\text{msj}} = \text{Preambulo} + \frac{\text{Mensaje(bits)}}{\text{RTrate}} + T_1 + TRP + \frac{\text{TagRep}}{\text{TRrate}} + T_2 \tag{4.1}$$

Todos los datos necesarios para realizar este cálculo pueden extraerse de la Tabla 4.1, por ejemplo, la duración del preámbulo depende del tipo de consulta, para una consulta *Query* el preámbulo corresponde al valor del símbolo RTP y el tamaño del mensaje es 22, y para una consulta *QueryRep*, el preámbulo corresponde al valor del símbolo RTF y el tamaño del mensaje es 4.

4.2.2. Resultados

La Figura 4.1 muestra el desempeño del **Protocolo Base**, en términos del tiempo que requiere para detectar a todas las etiquetas del conjunto como presentes o como perdidas. Se observa una elevación abrupta del tiempo de ejecución al aumentar el tamaño del conjunto por encima de cada límite en el que el parámetro Q cambia de valor. Lo anterior se debe a que el tamaño de la trama aumenta al doble, y por lo tanto, para cierta cardinalidad del conjunto de etiquetas, el tamaño elegido para la trama resulta inadecuado, en otras palabras, se usa demasiado tiempo extra respecto al realmente requerido. Además, al terminar cada trama o ciclo de detección, la cantidad de etiquetas por detectar se ve disminuída, pero la trama conserva su tamaño, el cual se aleja cada vez más del tamaño ideal.

De acuerdo con los datos recabados del estándar EPC Gen2, transmitir una consulta *QueryPB* y recibir una respuesta toma: 304.25μs. Esta transmisión se lleva a cabo una sola vez por ciclo al inicio del mismo. El resto de las transmisiones corresponden a consultas del tipo *QueryRep*. La transmisión de un *QueryRep* del que no se recibe respuesta toma: 176.25μs y la de aquel del cual se recibe respuesta (o colisión) toma: 204.025μs. El tiempo de ejecución del Protocolo Base puede expresarse en términos de la cantidad de ranuras utilizadas en total y el tiempo que se requiere para transmitir los mensajes y respuestas correspondientes. La cantidad total de ranuras utilizadas se

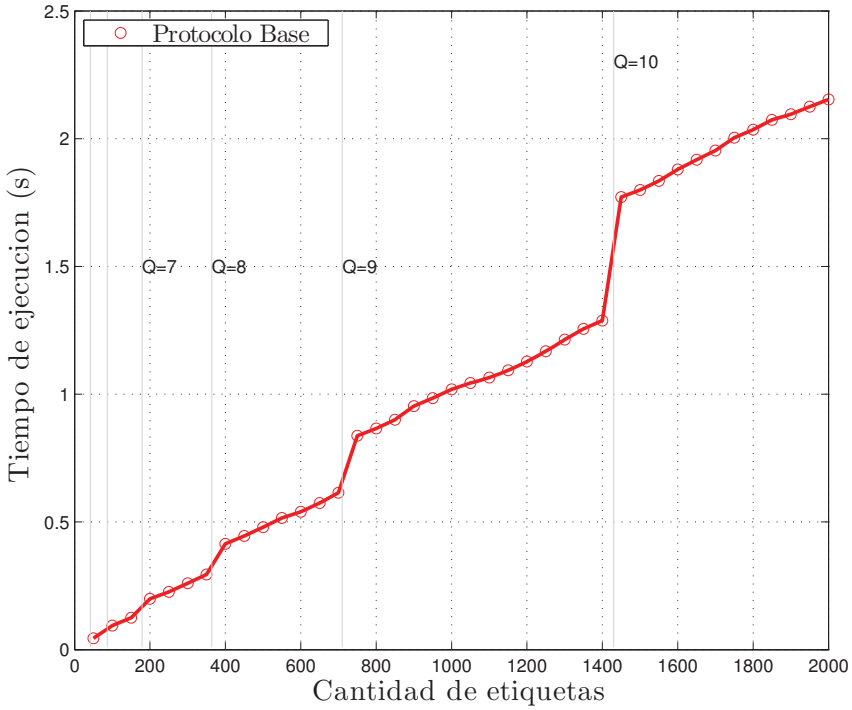

FIGURA 4.1: Tiempo de ejecución del Protocolo Base para conjuntos de diferentes tamaños.

encuentra sumando el número de ranuras en las que se transmite un $QueryRep$ sin recibir respuesta (k_V) más aquellas en las que se recibe respuesta o colisión (k_{SC}) y restando al resultado la cantidad de ranuras que requieren la transmisión de un $QueryPB$, número que corresponde a la cantidad de ciclos C utilizados. Posteriormente, debe considerarse la duración de los C mensajes $QueryPB$ previamente descartados, además del tiempo que toma la transmisión del vector de silenciamiento al finalizar cada ciclo, cuya longitud depende del tamaño de la trama que se utilice (C_{silencio}). Finalmente se transmite un comando de reinicio (C_{reinicio}) de sólo cuatro bits durante 176.25μs. La Expresión 4.2 es el resultado de considerar todos estos tiempos.

$$T_{\text{PB}} = 176.25(k_V + 1) + 204.025(k_{SC} - C) + C(304.25 + C_{\text{silencio}}) \tag{4.2}$$

Los valores obtenidos mediante la expresión anterior son muy cercanos a aquellos obtenidos de la simulación, a partir de la cual se obtienen valores con un margen de error del orden de 2.1 milisegundos.

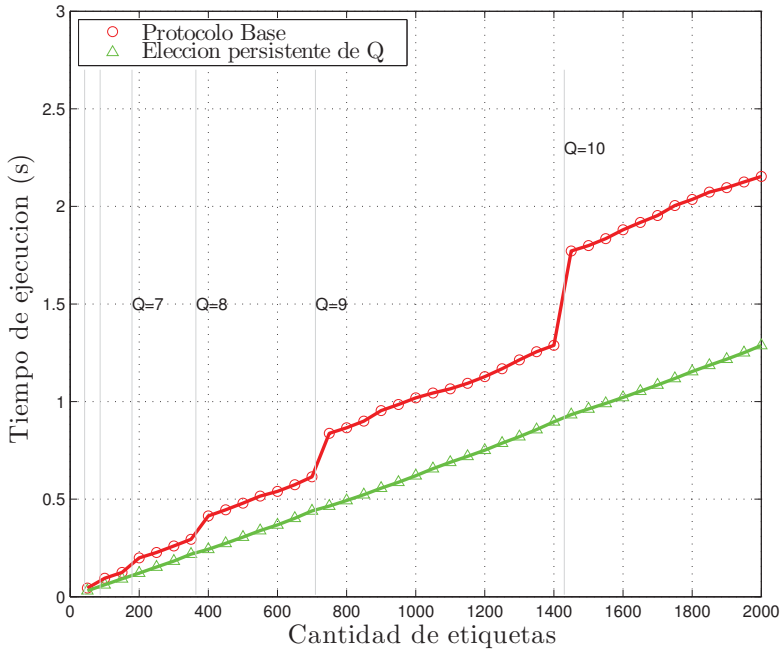

FIGURA 4.2: Tiempo de ejecución del Protocolo Base y Mecanismo 1.

La Figura 4.2 compara la propuesta del Protocolo Base con la implementación del mecanismo denominado *Elección Persistente de Q*. Al aplicar este primer mecanismo, podemos observar un crecimiento continuo del tiempo de detección mientras se incrementa el número de etiquetas en el conjunto, sin embargo, no se presentan los saltos abruptos ocasionados por la elección permanente de Q implementada en el *Protocolo Base*. Lo anterior sucede gracias al recálculo de Q realizado al inicio de cada ciclo de detección, el cual garantiza el uso de un tamaño de trama útil en referencia al número de etiquetas participantes para cada ciclo. Al implementar este primer mecanismo, el tiempo de ejecución del protocolo se reduce hasta en un 40 % y se eliminan los aumentos abruptos del tiempo de ejecución.

Siendo el tiempo de ejecución el parámetro por reducir, resulta innecesario llevar a cabo transmisiones una vez que el intercambio de mensajes haya concluido. La Figura 4.3 describe el desempeño del sistema al incorporar el mecanismo de *Recorte de Trama* además del mecanismo anterior. En otras palabras, cada mecanismo propuesto se acumula o incorpora a los anteriores. Esta implementación no proporciona una mejora notable en el tiempo de ejecución, dado que en ciertos casos ni siquiera se acciona, por ejemplo cuando alguna etiqueta elige la última ranura disponible de la trama, pero en otras ocasiones

elimina transmisiones innecesarias y reduce el tiempo de ejecución. De cualquier forma, consideramos su implementación como una buena práctica.

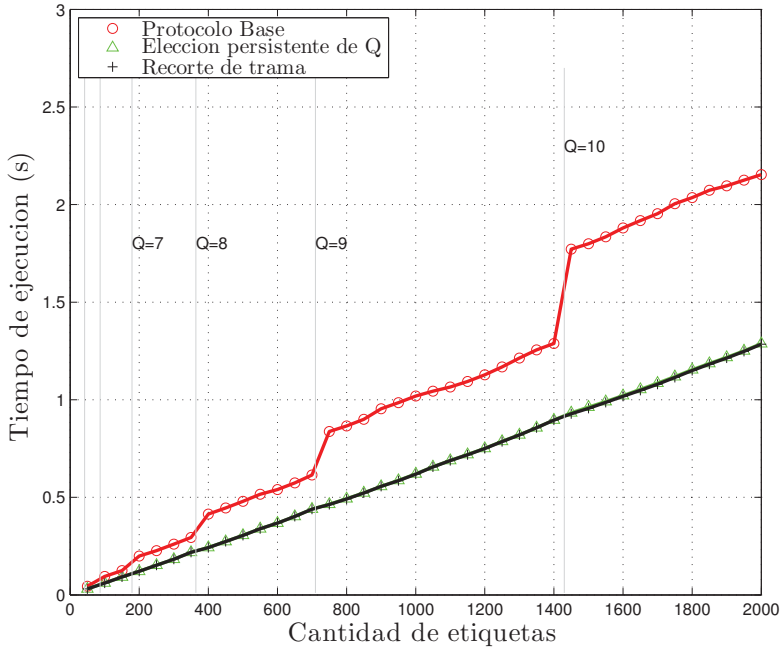

FIGURA 4.3: Tiempo de ejecución del Protocolo Base y dos de los mecanismos propuestos.

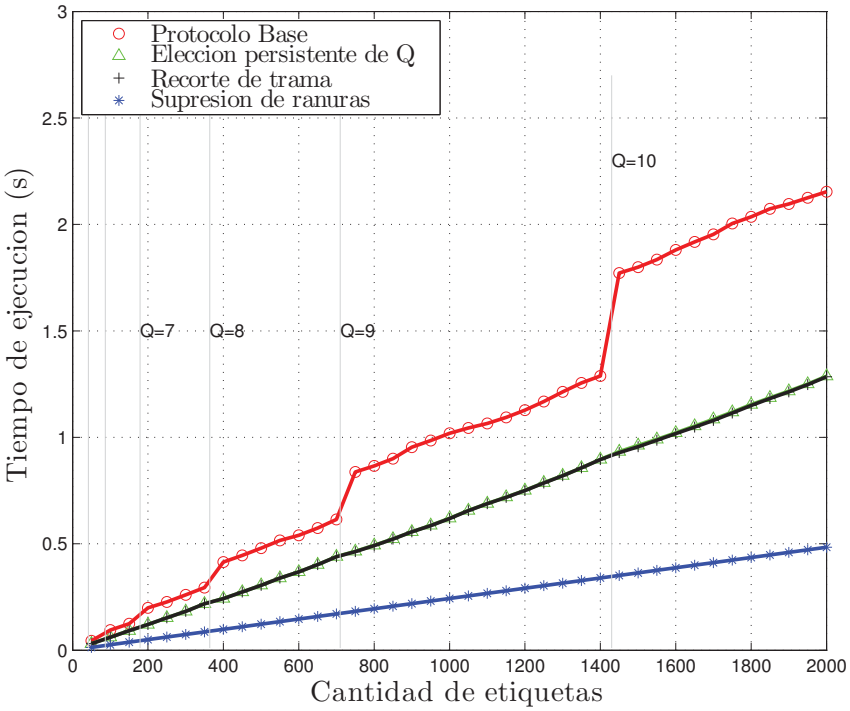

FIGURA 4.4: Tiempo de ejecución del Protocolo Base y los tres mecanismos propuestos.

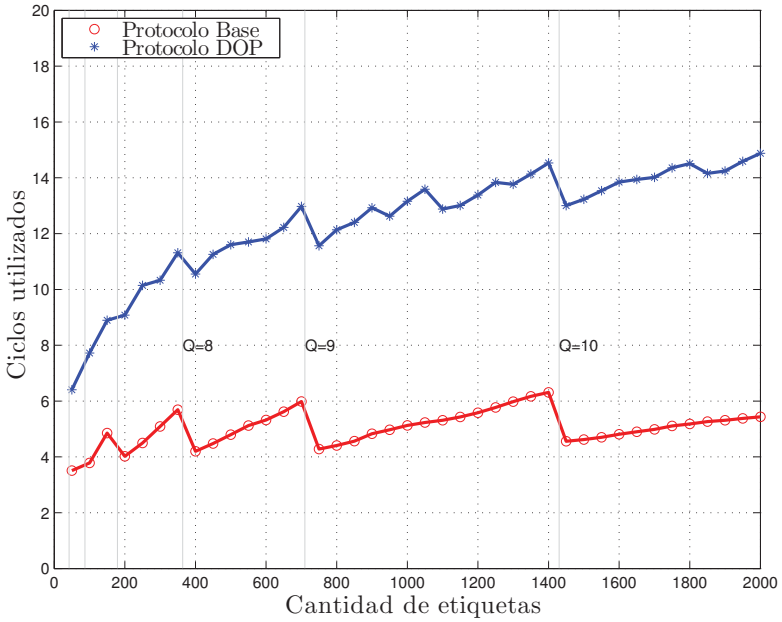

FIGURA 4.5: Cantidad de ciclos requerida por el Protocolo Base y por DOP.

La conjunción de la supresión de ranuras y los dos mecanismos anteriores conforma el protocolo *DOP*. En la Figura 4.4, se observa una drástica mejora en el desempeño del sistema, con reducciones temporales de hasta el 75 % al implementar los tres mecanismos. Además, se evidencia que la diferencia entre los tiempos requeridos por cada protocolo aumenta conforme lo hace la cardinalidad del conjunto utilizado, y por lo tanto, el porcentaje de reducción temporal aumentará conforme el tamaño de dicho conjunto lo haga.

Por otro lado, al analizar la cantidad de ciclos que requieren ambos protocolos, Protocolo Base y DOP, para ejecutarse por completo, notamos que DOP requiere una cantidad mayor y más variable de ciclos que el Protocolo Base, como describe la Figura 4.5.

Este comportamiento se justifica dado el mecanismo de Elección Persistente de Q, el cual ocasiona que las etiquetas tengan un número de ranuras suficiente para poder hacer una elección en cada ciclo, y no permite que se generen tramas muy grandes. Este mecanismo permitió en un inicio reducir el tiempo de ejecución del protocolo DOP, pero aumentó la cantidad de ciclos utilizados respecto al Protocolo Base, ya que este último utiliza tramas demasiado grandes, desperdiciando tiempo, pero usando pocos ciclos para alojar las respuestas de todas las etiquetas.

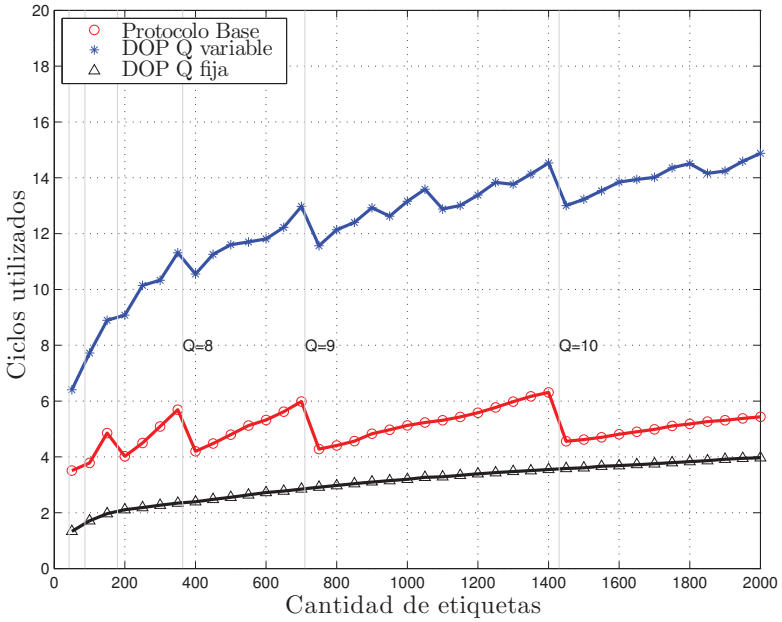

FIGURA 4.6: Cantidad de ciclos requerida por DOP tras su modificación.

Podemos notar que la inclusión del tercer mecanismo, incluye las bondades del primero y el segundo, al implementarlo se anula la importancia de implementar los anteriores, dado que sin importar la cantidad de ranuras de las que dispongan las etiquetas para elegir el momento de su respuesta, el tercer mecanismo eliminará todas aquellas ranuras sobrantes. Bajo esta premisa, podemos proponer una modificación a DOP para reducir la cantidad de ciclos que requiere su ejecución.

Al inicio del protocolo, el parámetro Q se fija en su nivel máximo (quince), de forma que las etiquetas tienen una cantidad máxima de ranuras para elegir, reduciendo la probabilidad de generar colisiones, y por lo tanto, reduciendo la cantidad de ciclos requeridos para ejecutar el protocolo. Este tamaño de trama se usa siempre, independientemente de la cardinalidad del conjunto. La Figura 4.6 muestra la cantidad de ciclos utilizados por el Protocolo Base, por DOP antes del ajuste y por DOP después del ajuste. Aquí, podemos observar también, la reducción de la variabilidad que presenta DOP, dicha reducción obedece a la fijación del espacio de elección que se ofrece a las etiquetas. Este ajuste, por supuesto, implica eliminar la implementación de los primeros dos mecanismos propuestos en este trabajo y conservar el tercero.

La reducción de la cantidad de ciclos que requiere el protocolo DOP reduce también la cantidad de mensajes de tipo $QueryDOP$, y por lo tanto, reduce el tiempo de ejecución

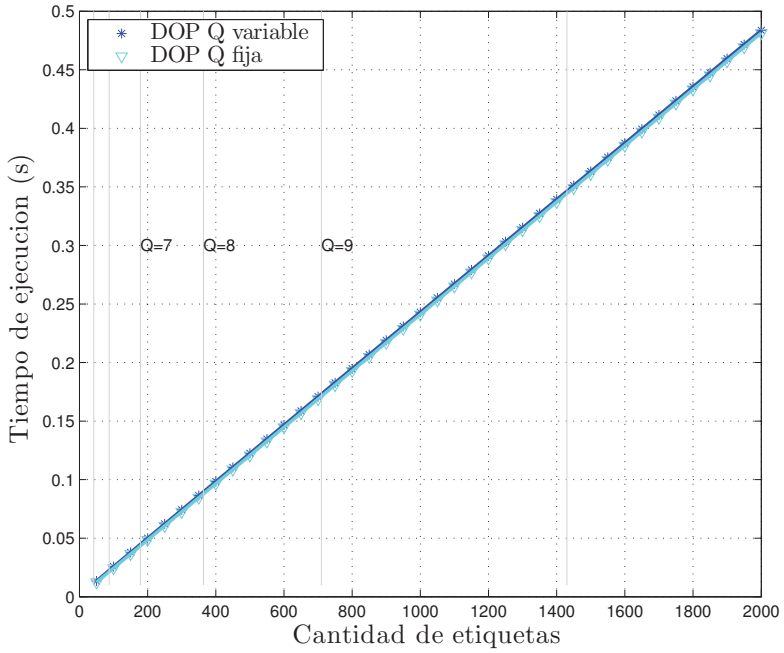

FIGURA 4.7: Porcentaje de reducción temporal generada por la modificación a DOP.

total del protocolo en unos pocos milisegundos. En la Figura 4.7, se puede observar la reducción del tiempo de ejecución producida por la modificación final al protocolo DOP. Los intervalos de confianza generados son demasiado pequeños para mostrarse gráficamente, corresponden a un error menor a 0.001.

Utilizando una dinámica similar a la utilizada para construir la Expresión 4.2, podemos expresar el tiempo de ejecución del protocolo DOP en términos de la cantidad de ranuras con una sola respuesta k_R, que corresponde con la cardinalidad del conjunto de etiquetas, la cantidad de ciclos utilizados, y la duración de la transmisión de un comando $QueryDOP = 304.25\mu$s, $QueryRepDOP = 240.25\mu$, $C_{\text{silencio}} = 176.76\mu$ y $C_{\text{reinicio}} = 176.25\mu$.

$$T_{DOP} = 240.25(K_R - C) + 544.53C + 176.25. \tag{4.3}$$

La Expresión 4.3, permite calcular el tiempo de ejecución del protocolo DOP a partir de la cardinalidad del conjunto de etiquetas y la cantidad de ciclos utilizados. Los valores obtenidos mediante la expresión anterior son muy similares a aquellos obtenidos de la simulación, dentro de un margen de error del orden de 1.3187 microsegundos.

Otras modificaciones menores podrían optimizar el desempeño del protocolo, sin embargo la complejidad del análisis para su correcta implementación rebasa los beneficios que éstas pudieran aportar a la reducción del tiempo de ejecución. Tal es el caso de codificar en pocos bits el parámetro s. Supongamos el uso de una función J que permita representar al parámetro s utilizando únicamente cuatro bits, de forma similar a la codificación que se realiza en el parámetro Q para transmitir el tamaño de trama f. La dificultad para la implementación de esta modificación, radica en la correcta construcción de la función J, ya que utilizar una menor cantidad de bits para representar al parámetro s significa una reducción del tamaño de los mensajes transmitidos por el lector, pero es posible que también aumente la cantidad de mensajes transmitidos, de forma que no resulta evidente si se generarán reducciones o aumentos en el tiempo de ejecución del protocolo.

Por ejemplo, si J se selecciona de forma similar a Q ($s = 2^J - 1$) existen dos casos posibles: 1) El valor calculado de s es menor al valor s realmente requerido, lo cual significa que algunas ranuras vacías se transmitirán a pesar de no culminar en la transmisión de información relevante, y 2) El valor calculado de s es mayor al valor s realmente requerido, lo cual significa que algunas ranuras que proporcionarían información relevante serán suprimidas y las etiquetas que serían detectadas en ese instante deberán participar en rondas posteriores de detección. En ambos casos, se advierte un beneficio a cambio de un perjuicio, una disminución y un aumento temporales.

En este punto, es útil evaluar el caso en el cual el beneficio se maximiza, para verificar si es conveniente implementar la modificación. El caso ideal se presenta cuando el parámetro s se codifica en pocos bits (por ejemplo cuatro) y su cálculo por parte de las etiquetas corresponde siempre al parámetro s original; de esta forma, se suprimen exactamente las ranuras necesarias y se reduce el tamaño de los mensajes. Una simulación simple muestra que la ganancia temporal generada por la reducción del tamaño de los mensajes es muy pequeña, al grado que no se percibe, dada la resolución del simulador. Para un conjunto de 2000 etiquetas, el protocolo requiere 0.4800 segundos con o sin la modificación en el caso ideal. Un caso promedio resulta en beneficios menores que el caso ideal, y por lo tanto desechamos la inclusión de esta última modificación en nuestro protocolo.

4.3. Protocolo distribuido

Una vez que se ha estudiado el funcionamiento del protocolo DOP, y conociendo los detalles de estructura de las arquitecturas distribuidas, podemos notar que el uso de DOP directamente sobre la arquitectura basada en *fielders* no proporciona ninguna ventaja temporal. El protocolo DOP, al igual que todos los protocolos de detección de objetos perdidos estudiados, requiere del aislamiento temporal de las respuestas de las etiquetas, impidiendo la detección simultánea de varias de ellas. Si se implementara un escenario de simulación distribuido usando DOP, el tiempo de ejecución simplemente se incrementaría debido a las retransmisiones entre *fielders* y lector. Mediante la expresión 4.4, se calcula la duración de una ranura del protocolo DOP en la arquitectura distribuida. Este tiempo depende de la cantidad de microzonas y, por lo tanto, de la cantidad de etiquetas que responden de forma simultánea, y sus retransmisiones hacia el lector. Por lo tanto, determinamos que no es necesario ni valioso implementar dicho escenario de simulación.

$$T_{msj} = Preambulo + \frac{Mensaje(bits)}{RTrate} + T_1 + TRP + \frac{TagRep}{TRrate} + T_2 + k_{etiquetas}\frac{TagRep}{ZigBeerate} \quad (4.4)$$

Por otro lado, la versión distribuida de DOP, llamada DDOP, se acopla de mejor manera a la arquitectura propuesta. No nos es posible simular el comportamiento de este protocolo, dado que su funcionamiento supone el uso de una función hash de características especiales con la cual no contamos, por ejemplo, requerimos de una función hash que permita a un número específico de etiquetas elegir la misma ranura para transmitir, pero no más de dicho número de etiquetas, para evitar las colisiones en el medio de transmisión, y que al mismo tiempo pueda ser ejecutada por una etiqueta RFID pasiva. Aunado a ello, la función hash deberá funcionar para cualquier conjunto de etiquetas, de forma que no es posible utilizar un conjunto de ID's conocido para construirla. A pesar de carecer de una función con estas características, continuaremos el análisis del desempeño de DDOP asumiendo su uso, para determinar si es viable dirigir la investigación a la localización o construcción de dicha función.

El protocolo logra su máximo desempeño cuando tantas etiquetas, como microzonas contenga la arquitectura, eligen la misma ranura para transmitir su respuesta. Por lo tanto, su tiempo de ejecución debe considerar las ranuras que hemos llamado colisionantes, aquellas que fueron elegidas por más de una etiqueta para transmitir, de forma que sea posible detectar paralelamente a las etiquetas que respondan a *fielders* diferentes. Esta necesidad elimina buena parte del mecanismo que genera la mayor reducción del tiempo requerido por DOP, permitiendo únicamente eliminar las ranuras sin respuesta del total de transmisiones por llevar a cabo. Son las ranuras colisionantes las que nos interesan ahora, debido a que permiten detectar de forma paralela, aunque no simultánea, un número mayor de etiquetas y reducir el tiempo total de ejecución.

En este sentido, el escenario de mejor desempeño involucraría una mayor cantidad de microzonas. Planteemos un escenario distribuido en el cual intervienen N etiquetas distribuidas de forma aleatoria con distribución uniforme en k microzonas. El tiempo que toma la transmisión de una consulta y la recepción de sus respectivas respuestas varía en función del tamaño de k, ya que el lector debe esperar, tras la transmisión de cada consulta, la respuesta de los k *fielders* correspondientes a cada microzona, y determinar si alguna de las k etiquetas mapeadas en la ranura actual no respondió a su *fielder* como se esperaba para poder reportar un evento de pérdida. Queda claro que la duración de una ranura varía conforme varían las condiciones del escenario.

DDOP realiza las mismas actividades previas a la comunicación que su versión centralizada, y requiere del envío de consultas de las mismas características. En el mejor de los casos, k etiquetas son mapeadas a una misma ranura, y están distribuidas en k microzonas diferentes sin localizarse dentro de áreas de traslape, de forma que sus respuestas no colisionen en el medio de comunicación. Este escenario permitiría lograr k detecciones simultáneas en los *fielders* y requeriría un solo ciclo del protocolo para concluir. Sin embargo, este escenario se presenta con una probabilidad muy pequeña como se observa en la Expresión 4.5.

$$P = \frac{1}{k!} \prod_{j=1}^{k} (1 - Pc_j)\,, \tag{4.5}$$

en donde la probabilidad de que cada una de k etiquetas se encuentre situada en una microzona diferente está dada por $1/k!$, mientras que la probabilidad de que cualquier

etiqueta se encuentre en un área de traslape ha sido definida en [28] como:

$$Pc_i = \frac{A_{\text{overlap}}}{Ac_i} \times Vc_i,$$

en donde Ac_i es el área de la microzona i, Vc_i es la cantidad de vecinos de dicha microzona y A_{overlap} es el tamaño de la zona de traslape que incide sobre esa microzona, de acuerdo con la siguiente expresión:

$$A_{\text{overlap}} = 2R_c^2 arcsin\left(\frac{a}{2R_c}\right) - \frac{1}{2}a\sqrt{4\left(R_c^2\right) - \left(a^2\right)}$$

Siendo R_c el radio de la microzona, y a la longitud de la línea descrita entre las intersecciones que forman la zona de traslape. Estos parámetros se describen gráficamente en la Figura 4.8. Por ejemplo, para un radio de comunicación de $R_r = 5$m, el radio de una microzona cuando $K = 2$ es $R_c = \frac{\sqrt{5}}{4}R_r = 5.6$m y $a_{k=2} = 10$m, cuando $K = 4$ es $R_c = \frac{\sqrt{2}}{2}R_r = 3.53$m y $a_{k=4} = 5$m, y cuando $K = 16$ es $R_c = \frac{\sqrt{2}}{4}R_r = 1.76$m y $a_{k=16} = 2.5$m. Con estos datos, es posible calcular la probabilidad de que se presente el mejor caso para cualquiera de estos tres ejemplos comunes. Entonces, cuando $k = 2$, $Pc_i = 0.4466$, cuando $k = 4$, $Pc_i = 0.3654$, y cuando $k = 16$, esta probabilidad depende de la cantidad de vecinos que compartan zonas de traslape con aquella que está siendo estudiada, por ello, existen tres casos: para una microzona con dos vecinos (esquina) $Pc_i = 0.369$, para una microzona con tres vecinos (arista) $Pc_i = 0.5535$ y para una microzona con cuatro vecinos (centro) $Pc_i = 0.7381$.

En general, si suponemos un escenario con k microzonas, observamos que la Expresión 4.5 refiere una probabilidad muy pequeña, ya que la división entre el factorial de k se decrementa dramáticamente cuando k crece, y es después multiplicado por un número inferior a uno, operación que resulta en un número por lo menos otro orden de magnitud menor. En el caso de 16 microzonas, la probabilidad es muy cercana a cero.

De forma que si elevamos el número de microzonas para buscar un mejor desempeño de DDOP sobre DOP, reducimos la probabilidad de que un escenario prolífico se presente, y todo ello asumiendo que la función hash adecuada esté a nuestro alcance.

Por otro lado, al considerar el mejor de los casos, queda claro que existe la posibilidad de encontrarse también con el peor de los casos, en el cual las N etiquetas se encuentran en

una misma zona de traslape, y la naturaleza de la función hash utilizada no le permitiría al protocolo concluir nunca, dadas las colisiones persistentes en el medio. La probabilidad de ocurrencia de este escenario puede calcularse usando la expresión 4.6.

$$P_{(N,1)} = \left(\frac{1}{k^n}\right) * (Pc_k)^n \tag{4.6}$$

Dadas las posibilidades planteadas y sabiendo que la adopción de un paradigma distribuido significa una inversión económica importante para los administradores de sistemas RFID, resulta arriesgado sumarse al cambio de paradigma a partir de una promesa vaga de mejora.

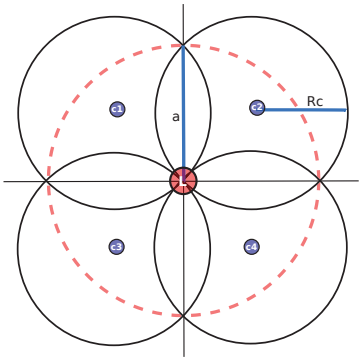

FIGURA 4.8: Radio e intersección entre microzonas.

Capítulo 5

Conclusiones y trabajo futuro

Después de realizar un significativo estudio de la tecnología RFID, así como de los protocolos de detección de objetos perdidos y las arquitecturas novedosas sobre las cuales pueden funcionar estos sistemas, se propuso una serie de mecanismos que desembocaron en el nacimiento de un protocolo de detección de objetos perdidos cuyo desempeño rebasa el de los protocolos planteados en la literatura hasta la fecha de esta escritura, por lo menos cuando la medida de desempeño es el tiempo que le toma al protocolo transmitir los mensajes necesarios para detectar a todas las etiquetas de un conjunto como presentes o como perdidas.

Posteriormente, se adaptó el protocolo a una arquitectura distribuida y se analizaron las condiciones bajo las cuales podría ser ventajoso implementar esta alternativa. Los requerimientos de la versión distribuida del protocolo son tales, que resulta prácticamente imposible, hasta este momento y con las herramientas disponibles, generar los escenarios en los que el tiempo de ejecución del mismo se vea beneficiado por este enfoque.

Al asumir un caso general en donde la distribución de los ID y de las etiquetas en el espacio es uniforme, las probabilidades de que se presenten escenarios ventajosos alcanzaron límites inferiores que se interpretan como imposibles en la práctica.

En general, el paradigma centralizado continúa ofreciendo múltiples ventajas sobre el distribuido cuando se evalúa la eficiencia temporal de los protocolos de detección de objetos perdidos. A pesar de ello, existen otras medidas de desempeño en las cuales es probable hallar ventajas para las arquitecturas distribuidas, como la ampliación del rango de comunicación sin la necesidad de invertir en un sistema de múltiples lectores.

Este trabajo sirve como base para algunas investigaciones posteriores que permitan mejorar el desempeño del protocolo DOP, por ejemplo minimizando al máximo la cantidad de información transmitida en cada consulta del lector y en cada respuesta de las etiquetas, utilizando diversos protocolos anticolisión híbridos, o implementando los protocolos existentes sobre otras arquitecturas distribuidas como aquella basada en *listeners*. LOs resultados obtenidos hasta el momento, así como la naturaleza del protocolo diseñado, sugieren ventajas extensas si se le evalúa desde la perspectiva de la eficiencia energética y se le compara con los protocolos que conforman el estado del arte. Otras vertientes de estudio, para dar continuidad a este trabajo, pueden incluir la evaluación del protocolo DOP en escenarios diferentes a los ya planteados, por ejemplo, aquellos en los cuales se introducen etiquetas ajenas al conjunto original, en el área de detección. Diversos aspectos, como la seguridad e integridad de la información transmitida dentro de este tipo de redes y generada por la interacción de sus componentes, continúan exponiendo nichos de oportunidad para los investigadores.

Referencias

[1] J. Landt, "The history of RFID," *IEEE Potentials*, pp. 274–279, diciembre 2005.

[2] L. D. Sánchez, "Estimación de marcas en redes RFID." M.S. thesis, Universidad Autónoma Metropolitana, Unidad Iztapalapa, 2011.

[3] In-Stat, "Explosive growth projected in next five years for RFID tags, http://www.instat.com," 2005.

[4] A. B. Intelligence, "RFID Growth Potential Remains Strong Despite Current Apparel Rollout Slowdown," 2011. `http://www.abiresearch.com/press/rfid-growth-potential-remains-strong-despite-curre`.

[5] M. Wong, "La evolución del RFID, desde sus orígenes hasta nuestros días," 2013. `http://innovasupplychain.pe/articulos/4668-la-evolucion-del-rfid-desde-sus-origenes-hasta-nuestros-dias`.

[6] R. Journal, "ABI: RFID Market Poised for Growth," 2003. `http://www.rfidjournal.com/articles/view?506`.

[7] D.-H. Shihand, P.-L. Sun, D. C. Yen, and S.-M. Huang, "Taxonomy and survey of RFID anti-collision protocols: Short survey," *Computer Communications, ACM*, pp. 2150–2166, julio 2006.

[8] D. K. Klair, K.-W. Chin, and R. Raad, "A Survey and Tutorial of RFID Anti-Collision Protocols," *IEEE Communications Surveys & Tutorials*, pp. 200–421, abril 2010.

[9] T. Li, S. Chen, and Y. Ling, "Identifying the Missing Tags in a Large RFID System," in *The Eleventh ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 1–10, septiembre 2010.

[10] B. Violino, "A Summary of RFID Standards," 2005. `http://www.rfidjournal.com/articles/view?1335`.

[11] K. Finkenzeller, *RFID Handbook*. John Wiley and Sons, second ed., 2003.

[12] C. C. Tan, B. Sheng, and Q. Li, "How to Monitor for Missing RFID Tags," in *The 28th IEEE International Conference on Distributed Computing Systems*, pp. 295–302, junio 2008.

[13] A. Technology, "EPCglobal Class 1 Gen 2 RFID specifications," 2005. `http://www.alientechnology`.

[14] C. Ying and Z. Fu-hong, "Study on Anti-collision Q Algorithm for UHF RFID," *Communications and Mobile Computing (CMC), IEEE*, pp. 168–170, abril 2010.

[15] N. Nasri, A. Kachouri, M. Samet, and L. Andrieux, "CSMA-based MAC protocol for collision avoidance in a dense RFID network," in *The 7th International Conference on Informatics and Systems (INFOS)*, pp. 1–5, marzo 2010.

[16] W. Alsalih, K. Ali, and H. Hassanein, "Optimal distance-based clustering for tag anti-collision in RFID systems," in *Proceedings of the 33rd IEEE Conference on Local Computer Networks (LCN '08)*, pp. 266–273, octubre 2008.

[17] Z. Li, C. He, and H.-Z. Tan, "Survey of the advances in reader anti-collision algorithms for RFID systems," in *2011 Chinese Control and Decision Conference (CCDC)*, pp. 3771–3776, mayo 2011.

[18] R. Zhang, Y. Liu, Y. Zhang, and J. Sun, "Fast Identification of the Missing Tags in a Large RFID System," in *8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, pp. 278–286, junio 2011.

[19] K. Ali and H. Hassanein, "Distributed Receiving in RFID Systems," in *IEEE Conference on Local Computer Networks (LCN)*, pp. 69–76, octubre 2009.

[20] K. Ali and H. Hassanein, "Parallel Singulation in RFID Systems," in *IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1–6, diciembre 2009.

[21] D. D. Donno, F. Ricciato, L. Catarinucci, A. Coluccia, and L. Tarricone, "Challenge: Towards Distributed RFID Sensing with Software-Defined Radio," in *ACM MobiCom*, septiembre 2010.

[22] P. Popovskiand, K. Fyhn, R. M. Jacobsen, and T. Larsen, "Robust statistical methods for detection of missing RFID tags," *IEEE Wireless Communications*, pp. 74–80, agosto 2011.

[23] W. Luoy, S. C. T. Liy, and S. Chenz, "Efficient Missing Tag Detection in RFID Systems," in *IEEE INFOCOM*, pp. 356–360, abril 2011.

[24] M. V. Bueno-Delgado, J. Vales-Alonso, E. Egea-López, and J. García-Haro, "Optimum Frame-length configuration in passive RFID systems installations," *Proceedings of International Workshop on RFID Technology, Concepts, Applications and Challenges (IWRT'09)*, pp. 69–78, 2009.

[25] P. Semiconductors, "I-CODE Smart Label RFID Tags," 2004. http://www.nxp.com/acrobat download/other/identification/SL092030.pdf .

[26] M. Korkalainen, M. Sallinen, N. Kärkkäinen, and P. Tukeva, "Survey of Wireless Sensor Networks Simulation Tools for Demanding Applications," in *Fifth International Conference on Networking and Services (ICNS '09)*, pp. 102–106, abril 2009.

[27] H. Sundani, H. Li, V. Devabhaktuni, M. Alam, and P. Bhattacharya, "Wireless Sensor Network Simulators, A Survey and Comparisons," *International Journal Of Computer Networks (IJCN)*, pp. 249–265.

[28] L. Sánchez and V. Ramos, "Adding randomness to the EPC Class1 Gen2 standard for RFID networks," in *IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, pp. 609 – 614, septiembre 2012.