Diseño de un protocolo de identificación por radiofrecuencia (RFID) propietario para una aplicación específica*

Design of a Proprietary RFID Protocol for a Specific Application**

Desenho de um protocolo de identificação por radiofrequência (RFID) proprietário para uma aplicação específica***

*Javier Bateman*****
*Cristian Cortés******
*Pablo Cruz*******
*Hernán Paz-Penagos********

* Fecha de recepción: 29 de marzo de 2009. Fecha de aceptación para publicación: 16 de julio de 2009. Este artículo se deriva del proyecto de investigación denominado *Construcción de un prototipo de un sistema de control de acceso en instalaciones industriales utilizando tecnología RFID*, patrocinado por la Escuela Colombiana de Ingeniería Julio Garavito.

** Submitted on March 29, 2009. Accepted on July 16, 2009. This article results from the research project called *Construction of a Prototype System for Access Control in Industrial Plants with RFID Technology*, supported by the Escuela Colombiana de Ingeniería Julio Garavito.

*** Data de recepção: 29 de março de 2009. Data de aceitação para publicação: 16 de julho de 2009. Este artigo deriva do projeto de pesquisa denominado *Construção de um protótipo de um sistema de controle de acesso em instalações industriais utilizando tecnologia RFID*, patrocinado pela Escola Colombiana de Engenharia Julio Garavito.

**** Ingeniero electrónico, Escuela Colombiana de Ingeniería Julio Garavito, Bogotá, Colombia. Correo electrónico: j-e-b-b@hotmail.com.

***** Ingeniero electrónico, Escuela Colombiana de Ingeniería Julio Garavito, Bogotá, Colombia. Correo electrónico: cristian5cortes@hotmail.com.

****** Ingeniero electrónico, Escuela Colombiana de Ingeniería Julio Garavito, Bogotá, Colombia. Correo electrónico: pcruz4@hotmail.com.

******* Ingeniero electricista, Universidad Nacional de Colombia, Bogotá, Colombia. Magíster en Teleinformática, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia. Profesor de la Escuela Colombiana de Ingeniería Julio Garavito, Bogotá, Colombia. Correo electrónico: hernan.paz@escuelaing.edu.co.

Resumen

Este artículo muestra el desarrollo de un proyecto de investigación acerca del diseño de un protocolo de identificación por radiofrecuencia (RFID) propietario para controlar el acceso de empleados, visitantes y activos a cualquier instalación pública, empresarial, comercial o industrial. La tecnología de RFID, a través de los estándares ISO 15693 (tarjetas vecinas), ISO/IEC 14443 (tarjetas de proximidad), ETSI TS 102.190, ISO/IEC 18092 y ECMA 340-V2, procura garantizar seguridad en el acceso, sin necesidad de utilizar dispositivos sofisticados, ni métodos complejos, y a un costo de implementación relativamente bajo.

Palabras clave

Sistemas de identificación por radiofrecuencia, sistemas de comunicación inalámbrica, identificación (sistemas de control).

Abstract

This article displays the development of a research project on the design of a proprietary RFID protocol for access control of personnel, visitors, and assets for any public, managerial, commercial or industrial installation. The technology RFID across the ISO standards 15693 (smart cards), ISO/IEC 14443 (proximity cards), ETSI TS 102.190, ISO/IEC 18092 and ECMA 340-V2 attempt to guarantee access safety without resorting to sophisticated devices or complex methods and at a relatively low implementation cost.

Key words

Radio frecuency identification systems, wireless communication systems, identification (control systems).

Resumo

Este artigo mostra o desenvolvimento de um projeto de pesquisa sobre o desenho de um protocolo de identificação por radiofrequência (RFID) proprietário para controlar o acesso de empregados, visitantes e ativos a qualquer instalação pública, empresarial, comercial ou industrial. A tecnologia de RFID, através dos padrões ISO 15693 (cartões vizinho), ISO/IEC 14443 (cartões de proximidade), ETSI TS 102.190, ISO/IEC 18092 e ECMA 340-V2, procura garantir segurança no acesso, sem necessidade de utilizar dispositivos sofisticados, nem métodos complexos, e a um custo de implementação relativamente baixo.

Palavras chave

Sistemas de identificação por radiofrequência, sistemas de comunicação sem-fio, identificação (sistemas de controle).

Introducción

La Smart Card Alliance, una asociación multisectorial de industrias sin ánimo de lucro, afirma que la adopción de la tecnología de identificación por radiofrecuencia (RFID, por su sigla en inglés) es clave para lograr disponibilidad, autenticidad, integridad y privacidad de la información en sistemas de control de acceso (RFID Magazine, 2008); sin embargo, se pueden presentar errores, cuando se transmiten simultáneamente los códigos desde varias etiquetas RFID hacia un solo lector; en este caso, la función del protocolo es evitar dichas interferencias mediante técnicas de anticolisión.

1. Marco teórico

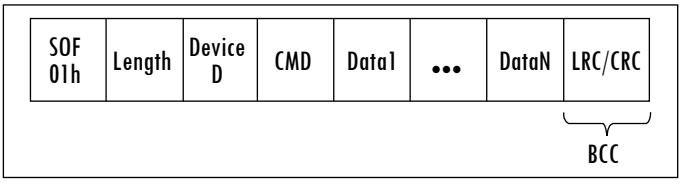
La transmisión de información en cualquier sistema de comunicaciones alámbrico o inalámbrico, de campo cercano o lejano, debe cumplir con unos parámetros básicos para garantizar la realización de la comunicación, la seguridad y la calidad de servicio en los usuarios; uno de ellos es el protocolo que define las reglas, los convenios y las funciones que gobiernan dicha comunicación.

Para que la comunicación entre dos entidades situadas en puntos diferentes del sistema sea establecida se necesita definir e implementar un protocolo, y los elementos que lo conforman son: (1) la sintaxis, que define el formato de los datos y los niveles de señal; (2) la semántica, que incluye información de control para la coordinación y manejo de errores, y (3) la temporización, que incluye la sincronización de velocidades y la secuenciación. Todas estas tareas se subdividen en subtareas y a todo se le da el nombre de arquitectura del protocolo (Paz, 2009).

2. Características del protocolo en RFID

En general, se nombrarán algunas características mínimas que debe cumplir todo protocolo RFID para garantizar una comunicación segura y confiable en una aplicación particular (RFID Journal, 2004). Como lo ilustra la Figura 1, la trama está conformada por ocho campos, así:

Figura 1. Organización de campos para protocolos de comunicación



Fuente: RFID Journal, 2004.

- *SOF* (*start of frame*): indica el inicio de la trama (1 *byte*).
- *Lenght* (longitud de la trama): puede o no incluir la trama de SOF (1 *byte*).
- *Device ID*: es el número de identificación del módulo/tarjeta (1 *byte*).
- *CMD* (*command*): es el código del comando que indica la operación que se va a realizar (1 *byte*).
- *Data*: en estos campos va la información deseada para la aplicación (desde 1 hasta 1.000 *bytes*).
- *LRC/CRC*: técnicas aplicadas para el control de errores (1 *byte*).

Aparte de estos campos, se pueden utilizar otros, que sirven para respaldar la transferencia de datos, por ejemplo:

- *Preámbulo*: consiste en una cadena de 20 ceros consecutivos para lograr la sincronización; en la trama se ubica antes del campo SOF.
- *EOF* (*end of frame*): para finalizar la trama.

Para reforzar la detección y el control de errores se pueden agregar bits de *paridad de byte* y *paridad de paridades*, adicional a los campos (LRC/CRC) (Albright, 2004).

3. Algunos comandos que se utilizan en la comunicación RFID

Para comprender la comunicación RFID entre los módulos *tag* y *reader* es indispensable identificar y conocer las funciones de los siguientes comandos:

- Leer múltiples *tags*: es un código único, no modificable y creado por la empresa, leído cuando la tarjeta está en modo de lectura. Todas las tarjetas poseen una *unique identification* (UID), que puede usarse para construir bases de datos de suministros y otros.
- Silenciar y/o hablar: activa o desactiva el funcionamiento de las tarjetas para que sean leídas o no por el módulo.

- Leer uno o múltiples bloques: esta función permite que se pueda hacer una lectura a la tarjeta electrónica para obtener la información de uno o varios bloques.
- Escribir un bloque: escribe la información requerida sobre algún bloque específico, para ser usado según la aplicación.
- Bloquear/desbloquear un bloque: permite o restringe la escritura o lectura de algún bloque en específico de las tarjetas, por seguridad.
- *KILL*: destruye y desactiva el funcionamiento total de la tarjeta; utilizable sólo en casos en que la tarjeta es desechable.

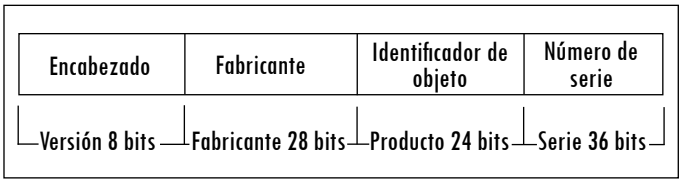
Algunos de estos comandos y sus funciones se encuentran disponibles en ciertos módulos según la aplicación. Por ejemplo, el comando KILL está disponible en microtarjetas y es utilizado en almacenes de cadena, cuyos productos pasan a ser propiedad de los consumidores; por consiguiente, el *tag* debe ser dado de baja. Todas estas características nombradas están relacionadas con la capacidad de la memoria interna con la que cuenta cada tarjeta (EEPROM, EPROM, FLASH).

4. Protocolos actuales basados en la tecnología RFID: RFID-EPC

Definición: el RFID-EPC es un código de producto electrónico que utiliza una cadena de números para identificar al fabricante, el producto y un número de serie exclusivo para cada unidad de artículo (RFID Journal, 2005). Esta serie de números se graba en el chip de la etiqueta RFID (Figura 2).

Función del RFID-EPC: permite hacer un seguimiento preciso del producto recolectando información de su trayecto, desde que se empaca hasta cuando es vendido al consumidor. Su finalidad es favorecer la logística del inventario, a fin de reducir tiempos de almacenaje y costos y de proporcionar un mejor servicio al cliente y al proveedor.

Figura 2. Campos del protocolo EPC



Fuente: EPC Global, 2008.

Por medio de esta estructura, implementada en las tarjetas o microchips, es posible tener toda la información concerniente al producto, por lo cual facilita su seguimiento y organización. EPC Global (2008), como ente de estandarización de la tecnología RFID en el uso de la EPC, ha clasificado las etiquetas en seis clases:

- Clase 0: lectura solamente (la EPC se codifica en el proceso de fabricación).
- Clase 1: lecturas indefinidas y escritura una sola vez (la EPC se le incorpora a la etiqueta después del proceso de fabricación).
- Clase 2: lectura y escritura.
- Clase 3: escritura y lectura, más fuente de alimentación que provee una mayor área de cobertura y funciones avanzadas.
- Clase 4: posee las mismas características de la clase 3, más comunicación activa con etiquetas activas.
- Clase 5: posee las mismas características de la clase 4, más comunicación con etiquetas pasivas.

5. Comunicación de campo cercano

Las comunicaciones de campo cercano (NFC) son las encargadas de dar soporte a la tecnología RFID y describen la interfaz aérea, el inicio, la anulación de colisión, el formato de trama y un bloque orientado al protocolo de intercambio de datos con manejo de error. Están previstas para permitir la interacción de etiquetas y dispositivos electrónicos a distancias menores a 10 cm. La limitada cobertura de esta tecnología es una gran ventaja por dos motivos: (1) resulta idóneo para atender servicios que impliquen una necesaria privacidad y (2) al estar tan cerca ambos dispositivos, se evitan los errores en la comunicación y se asegura una mayor eficacia en la transmisión de datos.

La NFC no se usa para acceder a todo tipo de redes o la transmisión de grandes cantidades de datos, pero sí da soporte a un intercambio de información en tasas de datos moderados, como teléfonos móviles, asistentes digitales personales (PDA), computadores o lectores de etiquetas. Así, la interfaz de NFC y el Protocolo-2 (*Near Field Communication Interface and Protocol* [NFCIP-2]) especifican el mecanismo de selección de modo de comunicación (ECMA 352). Este protocolo distribuye la ubicación de todos los dispositivos NFCIP-1, ISO 14443 e ISO 15693 que operen a 13,56 MHz, pero con diferentes protocolos. Está especificado en NFCIP-2 que los dispositivos puedan entrar en uno de los tres modos de comunicación y son diseñados para no perturbar otros campos de RF a 13,56 MHz (Savi.com, 2001).

La evolución de las NFC se basa en el enlace de datos de radiofrecuencia y el estándar MAC ISO/IEC 18092 (idéntico a ECMA 340-v2). Algunas especificaciones de este estándar se pueden examinar en la Tabla 1.

Tabla 1. Parámetros característicos del estándar ISO/IEC 18092 para campo cercano

	Activo		Pasivo	
	Emisor	Receptor	Emisor	Receptor
Tasa de datos baja: 106 kilobits por segundo	Modulación: 100% ASK	Modulación: 100% ASK	Modulación: 100% ASK	Subportadora: 847,5 KHz
	Codificación de Miller modificado; primer *bit* menos significativo	Codificación de Miller modificado; primer *bit* menos significativo	Codificación de Miller modificado; primer *bit* menos significativo	Codificación de Manchester; primer *bit* menos significativo
	Trama de N *bytes*; 1 *bit/byte* de paridad; CRC en algunos comandos	Trama de N bytes; 1 *bit/byte* de paridad; CRC en algunos comandos	Trama de N *bytes*; 1 *bit/byte* de paridad; CRC en algunos comandos	Trama de N *bytes*; 1 *bit/byte* de paridad; CRC en algunos comandos
	1 de 4 ranuras de tiempo igual como LBT	1 de 4 ranuras de tiempo igual como LBT	Árbol de búsqueda	…
	…	…	Igual a su predecesor ISO/IEC 14443-A:1999	Igual a su predecesor ISO/IEC 14443-A:1999
Tasa de datos alta: 212 kilobits por segundo, 424 kilobits por segundo	Modulación: 8-30% ASK	Modulación: 8-30% ASK	Modulación: 8-30% ASK	Modulación: 8-30% ASK Manchester
	Primer *bit* más significativo	Primer *bit* más significativo	Primer *bit* más significativo	Primer *bit* más significativo
	Preámbulo; 2-255 *bytes*; sincrónico; CRC-16	Preámbulo; 2-255 *bytes*; sincrónico; CRC-16	Preámbulo; 2-255 *bytes*; sincrónico; CRC-16	Preámbulo; 2-255 *bytes*; sincrónico; CRC-16
	1 de 4 ranuras de tiempo igual como LBT	1 de 4 ranuras de tiempo igual como LBT	1 de 16 ranuras de tiempo	…

Fuente: ECMA Internacional, 2004.

Algunos de los estándares seguidos en comunicaciones RFID son: ETSI TS 102.190, ECMA 340-V2, NFCIP-1 e ISO/IEC 18092:

- *ECMA 340-V2*: este estándar define los modos de comunicación activo (ambos dispositivos usan sus propios campos de RF) y pasivo para la interfaz entre dispositivos periféricos que tienen acople inductivo y que operan con frecuencia central de 13,56 MHz (ECMA Internacional, 2004).
- *NFCIP-1 (Near Field Communication Interface and Protocol)*: es un protocolo de interfaz inalámbrica; la comunicación se realiza entre dos entidades (punto a punto): aplicaciones de red y dispositivos electrónicos. Opera en la banda de los 13,56 MHz y tiene un alcance de funcionamiento de 20 cm. En este protocolo siempre hay uno que inicia la conversación, y este es el que la vigilará. Este rol es intercambiable entre las dos partes implicadas.

6. Tipos de tarjetas

6.1 Tarjetas de proximidad (ISO 14443)

Esta norma específica dos estándares tipo A y B para el protocolo de transmisión (inicialización, técnica de anticolisión e interfaz aérea) en la capa enlace. Este tipo de tarjetas de identificación electrónica se utiliza para cualquier sistema de comunicación con estándar internacional ISO 14443, en el cual: (1) se establece la comunicación estándar y los protocolos de transmisión entre la tarjeta y el lector; (2) opera a una frecuencia de portadora de 13,56 MHz; (3) trabaja a un rango de hasta 10 cm entre el *reader* y el *tag* para la lectura y escritura de la tarjeta; (4) especifica una velocidad predeterminada de 106 kilobits por segundo, suficiente para evitar colisiones, y (5) establece protocolos de seguridad, los cuales disponen de mecanismos de autentificación y cuentan con un microprocesador en las tarjetas que les proporciona confiabilidad; también tiene "mensajería segura" y "*tokens* criptográficos", como se describe en la ISO 7816, serie estándar (*ISO, 2006*).

6.2 Tarjetas vecinas (ISO 15693)

El estándar describe el protocolo de transmisión, la técnica de anticolisión y la interfaz aérea en la capa de enlace. A diferencia de las tarjetas de proximidad, estas se rigen por el estándar internacional ISO 15693, el cual: (1) establece las características físicas del *tag* y sus protocolos de transmisión; (2) opera a una frecuencia de modulación de 13,56 MHz; (3) trabaja a un rango mayor a un metro entre el *reader* y el *tag* para la lectura y escritura de la tarjeta; (4) especifica

una velocidad predeterminada de 26 kilobits por segundo, suficiente para evitar colisiones, y (5) incorpora normalmente máquinas de estado (condiciones económicas) en lugar de microprocesadores. Estas tarjetas pueden usarse para identificación y control de acceso (*ISO, 2006*).

7. Elementos de direccionamiento en RFID

La norma ISO 18000 define la interfaz aérea, los mecanismos de detección de colisión y el protocolo de comunicación para una etiqueta en diferentes bandas de frecuencia. La norma se divide en seis partes: la primera parte describe la arquitectura, mientras de la segunda hasta la sexta se especifican las características de radiocomunicaciones para las diferentes bandas de frecuencias, así:

- Parte 2, etiquetas que operan en bajas frecuencias (F<135 KHz).
- Parte 3.1, etiquetas que operan en altas frecuencias (F=13,56 MHz).
- Parte 3.2, sistemas RFID que operan en altas frecuencias (F=13,56 MHz), con anchos de banda superiores a 848 kilobit.
- Parte 4, sistemas RFID que operan a ultraaltas frecuencias (F=2,45 GHz); esta parte se divide en dos modos: modo 1: sistema *back-scattering* pasivo, y modo 2: sistema de alta tasa de datos, mayor alcance y con etiquetas activas.
- Parte 5, sistemas RFID que operan a extremadamente altas frecuencias (F=5,8 GHz); en la actualidad, esta parte está en investigación.
- Parte 6, define un sistema de *back-scattering* pasivo alrededor de 900 MHz (la banda sólo es parcialmente disponible en Europa).
- Parte 7, especifica un sistema RFID con *tags* activos en la banda de 433 MHz.

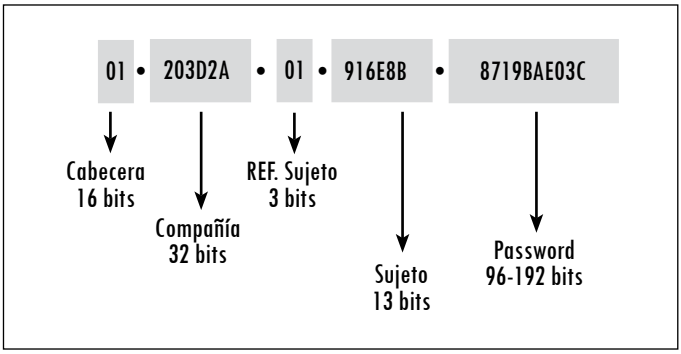
8. Diseño e implementación del prototipo para control de acceso

A través del sistema de control de acceso se les hizo seguimiento a las entradas y salidas de los empleados, visitantes y activos de una empresa. El prototipo contó con un protocolo que regula las comunicaciones y un sistema de información que registra la identidad de quien ingresa o sale, la hora de ingreso o de salida y la dependencia a la cual ingresa o de la cual sale el empleado, el visitante o el activo. En el protocolo de comunicaciones se utilizaron los siguientes campos de información (Figura 3):

- *Header*: tiene una longitud de 16 bits. Es la cabecera de la información que puede ser utilizada por otros tipos de protocolos en el futuro.
- *Compañía*: este espacio identifica la empresa que solicitó el servicio; el código es único e intransferible (32 bits).

- *Referencia sujeto*: este campo de 3 bits clasifica el tipo de persona o activo que se le asigna a cada *tag*, por ejemplo: empleado, visitante (visitante ocasional o cliente) y activo.
- *Sujeto*: es el código que identifica al sujeto que posee la tarjeta; este tiene un código único de 13 bits que es personal e intransferible.
- *Password*: es el número de encriptación del *tag* que garantiza la no lectura de la tarjeta por alguna persona que no sea autorizada; su longitud va de 96 a 192 bits.

Figura 3. Organización de campos en el protocolo del modelo propuesto



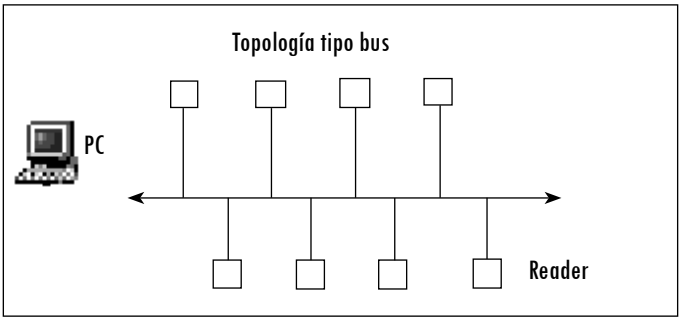
Fuente: presentación propia de los autores.

9. Interfaz RS485

Se optó por esta interfaz de comunicación entre lectores, porque ofrecía control de error y manejo de colisiones; además, se podía transmitir a 9.600, 19.200, 38.400 y 76.800 bits por segundo; esta última tasa de bit facilita el manejo de hasta 8 módulos a 9.600 bits por segundo cada uno. Adicionalmente, cada chip de esta interfaz era capaz de manejar hasta 32 estaciones a distancias de hasta 1.200 metros, lo cual hizo dicha interfaz adecuada para el desarrollo del proyecto.

Se implementó una conexión tipo bus (Figura 4) en configuración maestro-esclavo utilizando una estructura *full* dúplex para realizar la comunicación entre el computador y los lectores, lo que convirtió el protocolo RS232, que suministra el computador (maestro) y el *reader* (esclavo), a RS485, que se necesitaba en la red de lectores RFID.

Figura 4. Topología maestro-esclavo



Fuente: presentación propia de los autores.

Para el diseño e implementación del prototipo utilizamos un kit de desarrollo de RFID que tiene las siguientes especificaciones:

- Fabricante: PLINTEC.
- Banda de frecuencia: 13,56 MHz.
- Protocolo de comunicación: ISO 15693.
- Distancia máxima de operación: 30 cm.
- Tipo de tarjetas: *tag* pasivo.
- Voltaje de alimentación: 5 Vdc.

10. Organización de los datos

Los lectores que se interconectaron en la red de transmisión de datos se comunicaron mediante el estándar ISO 15693. Para integrar este protocolo con el protocolo propietario de red se utilizó el campo *datos* del estándar ISO 15693 para agregar los campos del protocolo propietario. La organización de los datos en los campos tuvo las especificaciones que muestra la Tabla 2.

El campo BlkData de esta tabla, que tiene una longitud de 32 *bytes*, se utilizó para identificar al SUJETO. Este se dividió en 4 *bytes* por bloque, para un total de 8 bloques; en dichos bloques se introdujeron los datos de identificación de empleados, visitantes y activos del protocolo propietario.

11. Resultados

El control de acceso (o cualquier otra aplicación en la cual haya trazabilidad) mediante la tecnología RFID es buena opción, porque garantiza agilidad, seguridad y múltiples usuarios que se comunican desde varios dispositivos conectados a la red y operan simultáneamente (Lindsay y Reade, 2003); sin embargo, la

interfaz de radio puede presentar algunos problemas en la comunicación (CWTI, 2005), como: interferencia mutua, interferencia y soluciones técnicas.

Tabla 2. Estructura de campos unificados del estándar ISO 15693 y el protocolo propietario

Campo	Contenido	Descripción
SOF	01	Inicio de la trama
PacketLen	15 00	Longitud de paquete de 16 *bytes*
DeviceID	03	Identificación del dispositivo
C md1	04	Entidad ID ISO 15693
C md2	69	Escribir múltiples bloques
IsSelectMsg	00	Ningún mensaje seleccionado
RespType	01	Preguntar por una respuesta
StartBlk	02	Comenzar escribiendo en el bloque 2
NumBlks	01	Escribir también en el siguiente bloque
BlkBytes	04	4 *bytes* por bloque
BlkData	12 35 36 38 21 53 63 83	Datos para escribir en el bloque 2 Datos para escribir en el bloque 3
BCC	C7 38	LRC y ~LRC

Fuente: presentación propia de los autores.

11.1 Interferencia mutua

La interferencia mutua se presenta cuando dos o más *readers* se traslapan e interfieren al comunicarse con los *tags*; esto hace que los lectores reporten la presencia de una tarjeta a la vez, y en tal caso no se sabría cómo manejar la información proveniente de los *readers*. Suele ser causado por exceso de potencia por parte de los *readers* o cuando las zonas de lectura se traslapan entre sí.

Usualmente, este problema se puede solucionar de dos formas: (1) los módulos pueden controlar la potencia de radiación, de tal manera que la zona de lectura quede limitada dentro de la zona que realmente se desea censar, a fin de evitar el traslape con otros *readers*. (2) Ubicar una pantalla conductora o malla de blindaje en los límites de cobertura, de tal manera que limite la zona de lectura (Collins, 2005).

11.2 Interferencia

La interferencia se presenta cuando dos o más tarjetas están simultáneamente dentro del campo de lectura de un *reader* y hacen solicitud al mismo tiempo. Esto causa colisión e inconvenientes en el procesamiento de los datos por parte del *reader*. Los nuevos circuitos integrados de Atmel utilizan un algoritmo determinístico de anticolisión, para evitar este tipo de interferencias.

Una solución que se propone es dotar tanto al *reader* como a la tarjeta con la opción de trabajar en múltiples frecuencias, de tal manera que seudoaleatoriamente se transmite en cualquier subportadora de *n* disponibles —según la FCC, con 50 frecuencias distintas es suficiente— (ES310 Introduction to Naval Weapons Engineering, 2005). De acuerdo con las probabilidades, hay una posibilidad del 0,04% que dos tarjetas transmitan al tiempo y su información interfiera. Sin embargo, esta solución es costosa y compleja, ya que se requieren módulos capaces de trabajar en varias bandas de frecuencias.

Otra solución es la propuesta europea, que consiste en activar los módulos de lectura durante un tiempo corto, pero suficiente para realizar la lectura de las tarjetas (Mobile Operators Association, 2005); sin embargo, el problema radica en la pérdida de la información cuando se desactiva el módulo que estaba leyendo, porque el tiempo asignado termina.

También es recomendable estudiar el entorno de la aplicación, ya que las comunicaciones RFID en ciertas frecuencias o en ambientes rodeados de materiales conductores que son obstáculos en la propagación de las señales, como el agua, los metales y otros varios, desvanecen la comunicación (Universidad EPN, 2008).

11.3 Soluciones técnicas

En la aplicación, fue necesario utilizar una comunicación *full* dúplex con dos pares balanceados de transmisión y recepción para evitar problemas de colisión entre lectores de la red. Si la recepción se encontraba separada de la transmisión, no se presentaba ningún problema de acceso múltiple y simultáneo.

Otra razón por la cual se utilizaron dos hilos para recepción y dos hilos para transmisión fue por principio de operación del protocolo RS485, el cual garantiza la transmisión de información sin pérdidas de potencia a distancias aceptables (RS-486/RS-422 Transceivers, 2003).

Un inconveniente de la aplicación fue el problema de acoplamiento. Este se presentó cuando los módulos estaban en modo de transmisión, con baja impe-

dancia a la salida, de manera que el flujo de datos desde un módulo cualquiera encontraba varias terminales con baja impedancia, la señal se dispersaba y el nivel se desvanecía amenazando con no llegar al módulo maestro.

Para solucionarlo fue necesario implementar, para cada módulo, un habilitador de transmisión, configurando un temporizador 555, de modo que los módulos presentaran alta impedancia cuando no estaban transmitiendo, y el único que presentaba baja impedancia era el maestro. La señal del monoestable habilitaba la transmisión del conversor TTL/RS485 del módulo que tenía autorización para transmitir y que interconectaba la red de lectores con el módulo maestro (Coughlin y Driscoll, 2000).

12. Conclusiones

- El espacio en memoria que utiliza el protocolo propietario es de 32 *bytes*, distribuidos en 8 bloques. En este se hizo control de acceso a empleados, visitantes y activos; este espacio de memoria lo puede ofrecer suficientemente cualquier *tag* RFID.
- El protocolo propietario se desarrolló para adecuarse a cualquier protocolo dedicado a la identificación por radiofrecuencia, ya que no intervienen otros campos establecidos en los estándares.
- El protocolo propietario cuenta con un nivel de seguridad alto, porque asigna longitudes de palabra para *password* desde 96 a 192 bits, difíciles de quebrantar con limitados recursos informáticos.

Referencias

ALBRIGHT, A. *RFID tag placement* [web en línea]. California: Frontline Solutions, 2004. <http://www.frontlinetoday.com/frontline/article/articleDetail.jsp?id=98552> [Consulta: 09-12-08].

COLLINS, J. HP Expands tagging, plans "noisy lab" [document en línea]. *RFID Journal*, 2005. <http://www.rfidjournal.com/article/articleview/1341/1/1/.> [Consulta: 06-12-08].

COUGHLIN, R. F. y DRISCOLL, F. F. *Operational amplifiers and linear integrated circuits*. New York: Pearson Education, 2000.

COUNCIL ON WIRELESS TECHNOLOGY IMPACTS (CWTI) [web en línea], 2005. <http://www.energyfields.org/.> [Consulta: 03-11-08].

ECMA INTERNATIONAL. *Near Field Communication Interface and Protocol (NFCIP-1)*. Standard ECMA-340. 2ª ed., 2004.

EPC GLOBAL. EPCglobal Tag Data Standard, Versión 1.4, 2008.

ES310, INTRODUCTION TO NAVAL WEAPONS ENGINEERING. *Propagation of waves* [web en línea], 2005. <http://www.fas.org/man/dod-101/navy/docs/es310/propagat/Propagat.htm.> [Consulta: 01-10-08].

INTERNATIONAL STANDARD ORGANIZATION (ISO). *Identification cards-contactless integrated circuit cards-Vicinity cards. ISO/IEC 15693-2.* 2nd ed., 2006.

LINDSAY, J. D. y READE, W. *Cascading RFID tags* [documento en línea], 2003. <http://www.jefflindsay.com/rfid3.shtml.> [Consulta: 15-12-08].

MOBILE OPERATORS ASSOCIATION. *What is a radio wave* [web en línea], 2005. <http://www.mobilemastinfo.com/information/radiowaves_and_health/radiowaves.htm.> [Consulta: 24-09-08].

PAZ, H. *Sistemas de comunicaciones digitales*. Bogotá: Editorial de la Escuela Colombiana de Ingeniería Julio Garavito, 2009.

RFID JOURNAL. *10 questions to ask RFID vendors* [documento en línea], 2005. <http://www.rfidjournal.com/article/articleview/1330/1/129/.> [Consulta: 21-09-08].

—. *FCC certifies ubisense's UWB* [documento en línea], 2004. <http://www.rfidjournal.com/article/articleview/1285/1/1/.> [Consulta: 11-10-08].

RFID MAGAZINE. *Noticias.* [Web en línea], 2008. <http://www.rfidmagazine.com/noticias/detalle.php?id=785> [Consulta: 15-12-2008].

RS-486/RS-422 Transceivers, Maxim Integrated Products, 19-0122; Rev 7, 2003.

SAVI.COM. *Spectrum characteristics for RFID* [web en línea], 2001. <http://members.surfbest.net/eaglesnest/rfidspct.htm> [Consulta: 21-11-08].

UNIVERSIDAD EPN [documento en línea], *2008.* <http://www.Clusterfie.epn.edu.ec/ibernal/html/CURSOS/AbrilAgosto06/Inalambricas/TRABAJOS/T1/Seguridad%20RFID.doc.> [Consulta: 06-12-2008].