Electronic Toll Collection using Active RFID System

[1] A.Ashok, [2] V.Thangavelu, [3]N.Harikrishnan
BIT campus, Anna University-Trichy
Email: [1] ashokannadurai@gmail.com, [2]thangavelc@gmail.com, [3]hariever4it@gmail.com

Abstract

The Radio Frequency Identification system uses two main components namely the RFID card and the RFID reader. The RFID card is similar to magnetic cards except the communication protocol used and the medium of transmission. Here in RFID, the medium for communication wireless whereas in magnetic card it is different. Wireless supports fast and distant accessing instead of coping the card to the reader as if in magnetic cards. The communication protocol used by the RFID card and the reader is weigand. Implement the program in microcontroller to read the data from the reader using the weigand protocol. After comparing the ID data using the microcontroller we can establish the access control for the user. Here the card will be given to each vehicle on the payment of deposit. Thereafter the card acts as the pass for that vehicle. The vehicle information and the owners information will be stored in the system EEPROM memory.

1. Introduction

There are four important issues in developing the active RFID system: 1) the compatibility with heterogeneous systems. For the active RFID system operating in 433MHz, ISO/IEC 18000 part 7 defines the air interface.[2] The compatibility issue can be overcome using the standard air interface. 2) the lifetime of active RFID tags. Because an active RFID tag is powered by the internal energy, the lifetime of the tag is mainly dependent on the lifetime of the battery. For power saving mechanism, one should design the mechanism that the processor can completely turn off the radio or simply put it in sleep mode. 3) the ability to identify multiple tags. This issue is important in the item management environment. To get higher identification rate of multiple objects, proper collision arbitration and error check mechanism should be used. 4)the security mechanism to prevent accessing by malicious users. In this paper, I present the design and implementation of an active RFID system platform which complies with the ISO/IEC 18000-7 standard. Our system platform is composed of tags and a reader which GUI host interface. The hardware design of the tags and the reader is minimal and flexible using commercial off-the-shelf components. The software part of the system is composed of the protocol handler to comply with the standard air interface and host interface to communicate the legacy system. The organization of the paper is as following. We present international standards and related works in the next section. Then I describe the thread to privacy and security issues in section3. Then I describe lightweight mutual authentication protocol in section4. Then, I describe the development of our active RFID system operating in 433MHz in section 5, and explain software developed on the active RFID system in section6. Before concluding this paper, I describe the performance evaluation of the system in section 7.

2. Related work

Standards for RFID systems are defined by ISO/IEC. 15961[4] addresses the tag commands, 15962[5] depicts the data syntax, and 19799 demonstrates about API. In addition, 18000 is intended to address air interface. 18000 consists of the following parts: Part 1, for reference architecture and definition of parameters to be standardized, part 2, for below 135kHz, part 3, for 13.56MHz, part 4,

for 2.45GHz, part 6, for 860~960MHz and part 7, for 433MHz. As aforementioned, part 7 of ISO/IEC 18000 defines the air interface for RFID operating as an active RFID system in the 433 MHz band. The characteristics of the RF communication link between a reader and tags are as following. The carrier frequency is 433.92MHz, and the accuracy is ±20ppm. The modulation type is FSK, and the frequency deviation is ±50kHz. The modulation rate is 27.7kHz. The wake up signal is transmitted by a reader for a minimum of 2.5seconds to wake up all tags within communication range. The wake up signal is a 30kHz sub-carrier tone for 2.5 to 2.7seconds. Upon dection of the wake up signal all tags will enter into a ready state awaiting commands from the reader. In the data link layer, a packet is comprised of a preamble, data bytes and a final logic low period. The preamble is comprised of twenty pulses of 60us period, 30us low, followed by a final sync pulse which identifies the communication direction: 42us high 54us low means communication from tag to reader; 54us high 54us low indicates communication from reader to tag. Data bytes are in Manchester code format, comprised of 8 data bits and 1 stop bit. A falling edge in the center of the bit-time indicates a 0 bit, a rising edge indicates a 1 bit. The stop bit is coded as a zero bit. The CRC is appended to the data as two bytes. Then, a final period of 36us of continuous logic low is transmitted for each packet after the CRC bytes.

3. Threat to Privacy and Security Issues In a RFID Network

Tags themselves have no access control function, thus, any reader can freely obtain information from them. As a result, an authentication (as well as authorization) scheme must be established between the reader and the tag so as to achieve the privacy issue of a RFID system. Another tag security issue related to the scenario such that since the communication between a tag and a reader is by radio, anyone can access the tag and obtain its output, i.e. attackers can eavesdrop on the communication channel between tags and readers, which is a cause of consumers' apprehension. So the authentication scheme employed in RFID must be able to protect the data passing between the tag and the reader, i.e. the scheme itself should have some kind of encryption capability. RFID Readers may only read tags from within the short (e.g. 75meters) tag operating range, the reader-to-tag, or *forward* channel is assumed to be broadcast with a signal strong enough to monitor from long-range, perhaps 100 meters. The tag-to-reader, or *backward* channel is relatively much weaker, and may only be monitored by eavesdroppers within the tag's shorter operating range. Generally, it will be assumed that eavesdroppers may only monitor the forward channel without detection. This relationship is illustrated in Figure 1:

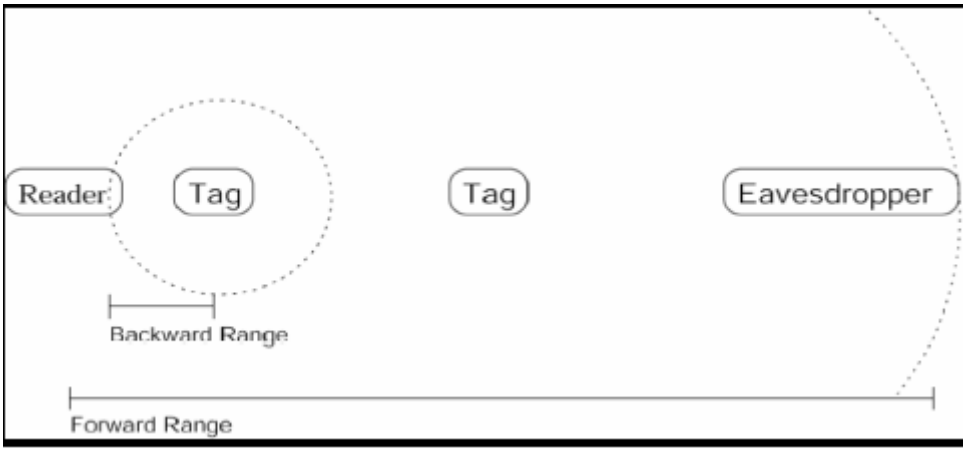


Figure 1. Forward versus

Backward Channel: The reader will detect the nearby tag, but cannot detect the shaded tag. A distant eavesdropper may monitor the forward channel, but not the tag responses. Finally, the reader security issue related to the case such that unauthorized person could set up hidden readers to get access to the information being transmitted from the tag. They can even compromise the authorized

readers so that the information collected by the readers may be incorrect. Therefore, a RFID security framework for authenticating the readers should be setup in order to tackle this issue.

4. Lightweight Mutual Authentication Protocol

Accepting the resource limitations of low-cost passive tags, we offer a simple security scheme based on hash function.The proposed RFID authentication is based on the RFID scheme design suggested by Ohkubo[1] with an additional challenge-response protocol. Ohkubo[1]'s scheme makes use of the hash chain technique to produce the tag output to the reader given initial secret tag information.

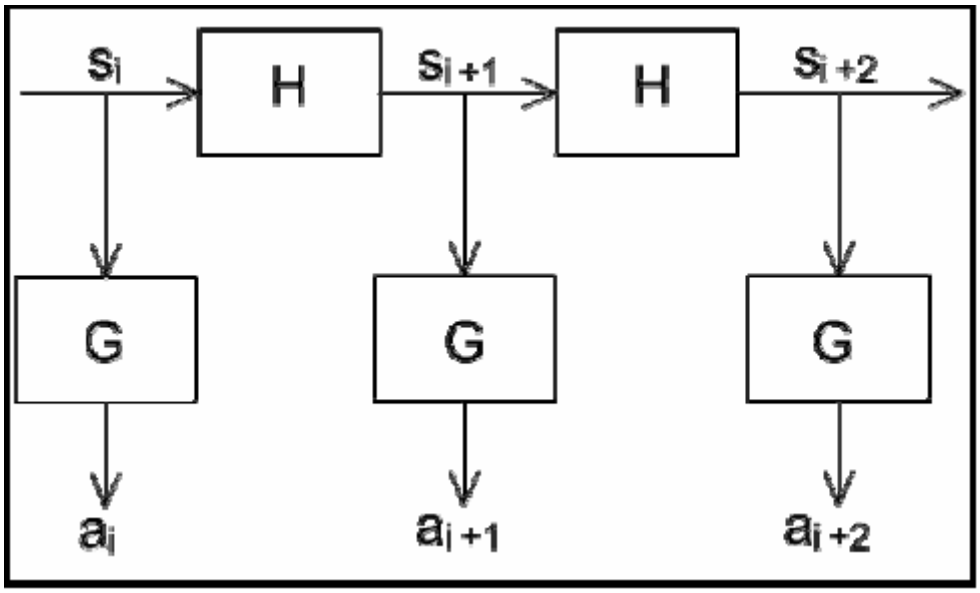


Figure 2. Ohkubo[1]'s hash chain technique

From Ohkubo[1]'s hash chain scheme, si is the secret information being used at ith transaction (read/write query) and ai is then tag output for that transaction. The proposed security protocol employs the same use of hash chain for updating the tag's secret information so as to achieve the forward security requirement. H and G are the hash functions. However, the tag output of the scheme does not solely depend on ai but along with some other 'random' parameters in order to make itself much more indistinguishable. In addition to the non-constant tag output, a security framework is also constructed for the whole RFID network that includes a backend system and RFID reader with tag. The backend system is mainly for verifying and processing the data transferred from/to the tag on behalf of the reader so as to achieve a RFID security infrastructure. As a result, it is recommended to set up a public-key algorithm like RSA between the reader and the backend so as to ensure only the authorized reader is permitted connecting to the backend system. It is easy to observe that the reader basically does nothing other than just passing the indistinguishable information between the backend system and the tag. The basic framework is shown in the following diagram:

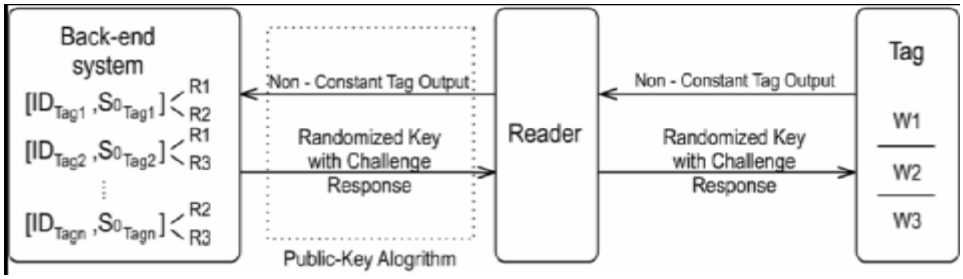
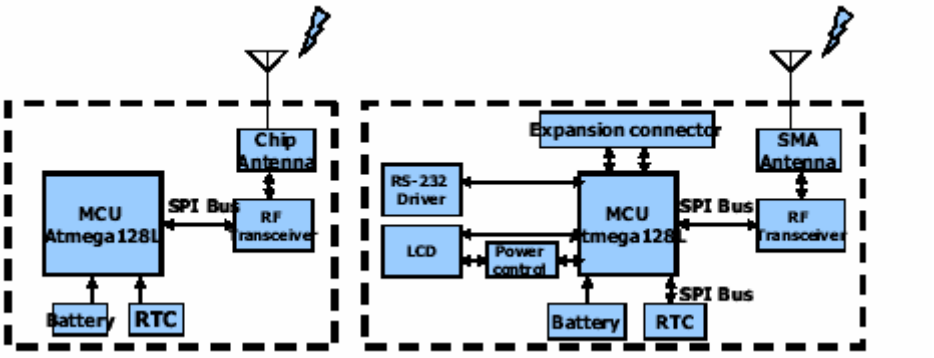


Figure 3. The basic framework of the proposed lightweight security protocol

5. Hardware development of an active RFID system

The RFID equipment is composed of two principal components: a tag, referred to as a transponder, and a reader, referred to as an interrogator. These two components are powered by 3V AA batteries attached to the bottom of the board. PIC 16F73 was chosen as the processing unit of our platform. It is able to operate at a maximum frequency of 8MHz, providing reasonable processing power to explore a wide variety of applications. The PIC 16F77A(reader) provides sufficient memory resources for a wide range of experiments.

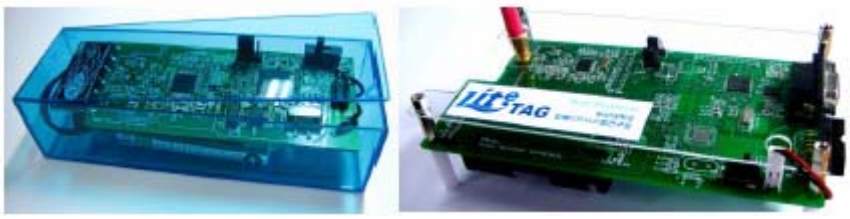


(a)Tag system (b) Reader system

Figure 4. Block diagram of our active RFID

The communication subsystem of our active RFID system is based on the XEMICS's XE1203F radio[7], which is connected to the processor through an SPI interface. The XE1203F is 433, 868, and 915MHz compliant single-chip RF transceiver, which is designed to provide a fully functional multi-channel FSK communication. It has an effective data rate of 153.2kbps, making it ideally suited for applications where high data rates are required. The processor can completely turn off the radio or simply put it in sleep mode through the SPI interface, while the XE1203F can wake up the processor when an RF message has been successfully received. In addition, the radio chip provides a variety of 4 different output power levels that can be used for transmission. The power consumption of the radio during transmission heavily depends on the output power level used. Furthermore, chip antenna is used for miniaturization in the tag system.

Figure 4 shows the block diagram of (a) the tag and (b) the reader. The tag consists of a processor, an RF transceiver, and an RTC(real time clock)[8]. The processor can completely control the radio through the SPI interface, and transmit/receive data using the processor's port D. To make it easy to change the operating mode, we control a RF switch[9] through port B. In addition, to visualize the RF communication between the reader and the tag, three LEDs are added. The reader basically contains a radio frequency module (transceiver), a microcontroller unit, an antenna and the interface (RS-232[10]) to the host system. To supply higher voltage to the LCD module, LT1302[11], that converts 3V to 5V DC supply, is used. In addition, an expansion connector is added for interfacing with sensors.



(a) Tag (b) Reader

Figure 5. Hardware components

Figure 5 shows the hardware components of the tag and the reader and module names, respectively. The hardware components are commercial off-the-shelf products. In addition, the reader can add an extra processor for improving the computing power.

6. Software development of an active RFID System

Software for the active RFID system is separated into three types: a host program, a reader program, and a tag program. The host system controls the data flow between the reader and tags. It can be as simple as a personal computer connected to the reader by an RS- 232 serial cable. More complex systems are possible where there are many readers in different locations and data is transferred to host servers through LANs or even over the Internet.I will deal with this problem in the near future. The host receives information from user, analyzes the command, generates packets, and then sends them to the reader system. The communication between the reader and the tag is of master-slave type, where the reader always initiates communication and listens for response from a tag. Figure6 shows the operation of the reader. Upon receiving data from the host program, the reader classifies data into commands and data, and then generates a new packet. Subsequently, CRCCCITT[12] 2 bytes are appended to verify the data in tags. The complete packet is sent through radio frequency after wake-up signal is sent. As the RF subsystem transmits data by FSK modulating, I encode each bit with the Manchester code. The UART has to be initialized before any communication can take place. The initialization process normally consists of setting the baud rate, setting frame format and enabling the Tx or Rx depending on the usage. Although baud rate is possible up to 250kbps using double speed operation, we just use 9.6kbps baud rate. Then the reader waits for a response message from the tags. The received message will be transmitted to the host.

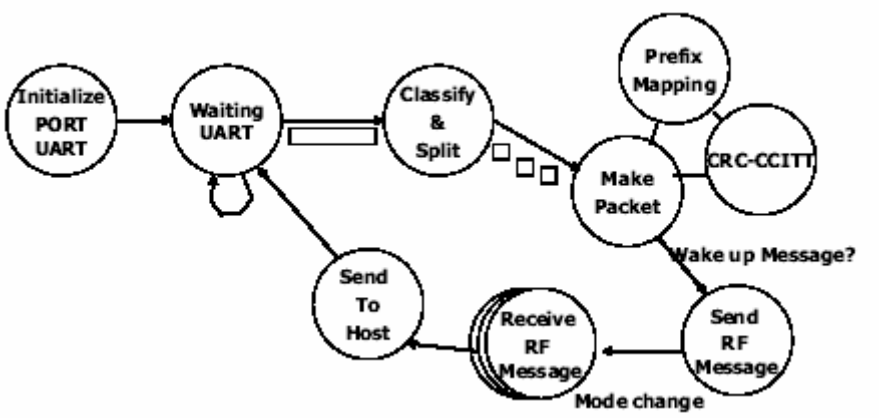


Figure 6. State diagram for the reader system

Figure 7 depicts the operation of the tag. When the tags placed within the reader RF communication range receive a wake-up signal that is broadcast by the reader, they will move into the active state. The selection is determined by a random number generator. On receiving a collection command, tags will detect by checking invalid CRC. If a tag received with valid CRC, the tag will select their slot and respond with messages to reader. In addition, in order to store a tag's unique ID, we use 4K bytes of data EEPROM memory. We also add a simple security mechanism to prevent accessing by malicious users Basically, the message type between the reader and the tag has two different formats: broadcast message and point-to-point message. P2P message format, which includes all commands except collection commands, requires a tag ID in order to access a particular tag. P2P message is one of sleep, status, user ID length, user ID, owner ID, firmware revision, model number, read/write memory, set password, password protect, and unlock commands. The broadcast commands are used to collect tag IDs, user IDs or short blocks of data

from the selected group of tags using a batch collection algorithm. Broadcast commands are used for tag ID collection within reader RF communication range.

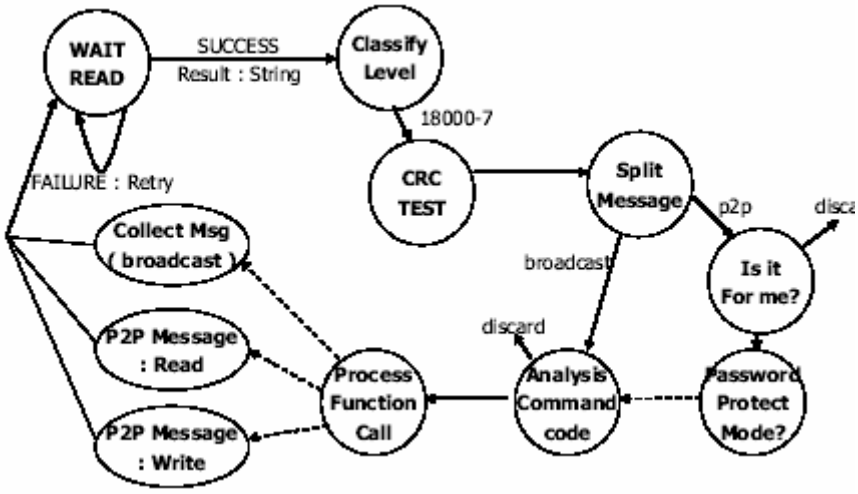


Figure 7. State diagram for the tag system

To perform an efficient and orderly collection of the tags placed within the reader communication range and to receive information on the tag capabilities and data contents in a single sequence, collision arbitration mechanism is used as slotted ALOHA[1,2]. The information that the tag returns is specified by flags set in the command of the reader.

7. Performance evaluation

In this section, I report on some results from a preliminary performance evaluation of our active RFID system. Our goals in conducting this evaluation study were twofold. First, because active RFID tags can use up their limited supply of energy simply performing computations and transmitting information in a wireless environment, energy conserving forms of communication and computation are essential. The other is multi-tag collection. Collecting multiple collocated tags within communication range is difficult and often unreliable because collisions may be detected

7.1. Energy budget

The sleep mode enables the application to shut down the processor of unused modules, thereby saving power. Table 1 shows the different power consumptions according to the operation mode. In the RF part, possible states are one of transmitter, receiver, or sleep mode. Additionally, an extra state, called standby state, is added for state transitions and the initial state. Power consumptions to each state are shown in table 2.

[Table 1] Power consumption in the MCU

State	Condition	Typ.	Max.	Unit
Active	All		5.5	mA
Sleep	WDT	<15	25	uA

Our system runs on a pair of AA batteries, with a typical capacity of 2.5 ampere hour (Ah). I make a conservative estimate that the batteries will be able to supply 2.5Ah at 3V. Assuming the system will operate uniformly over the deployment period, each tag has 0.303876mA per day available for use. 2AA (2500mAh) battery allows us to use for 1 year.

[Table 2] Power consumption in the RF

State	Condition	Typ.	Max.	Unit
Tx	5dBm	33	40	mA
Rx		14	17	mA
Standby	Osc. on	0.85	1.10	mA
Sleep		0.2	1	uA

7.2. Identifying multiple tags

I assume simple models. First, the time interval is a period between a point of time when the previous message was sent completely and the start time of next message. Second, the length of message is 50bytes except for the preamble message, and the number of messages is limited to be thousand. For this experiment, the time intervals are 51.125usec, 101.125usec, 1msec, 10msec and 30msec. The result of performance evaluation shows great performance, over 99% shown as table 3. Table 3 shows that successful transmission rate is sufficiently high(over 99%) whichever time interval is selected.

[Table 3] Identifying multiple tags

Time interval between messages	# of sent msg.	# of received msg.	miss	Pr. (%)
30.0msec	1000	1000	0	100
10.0msec	1000	1000	0	100
1.0msec	1000	998	2	99.8
101.125usec	1000	994	6	99.4
51.125usec	1000	997	3	99.7

8. Conclusion

In this paper, I presented an active RFID system platform including tags and the reader. We describe the detailed design and implementation of our platform. Our active RFID system has features such as high identification rate of multiple tags, reliable energy budget, and standard compliance with ISO/IEC18000-7. Our tag and the reader are effective for development and evaluation of prototype applications because of the flexibility of the design of both hardware and software. So, our platform will be suitable for versatile item management applications. The future works include as follows: 1) the investigation of cost reduction of the platform, and 2) the sophisticated design of the collision arbitration of the active RFIDs.

9. References

[1] Klaus Finkenzeller, "RFID Handbook: fundamentals and applications in contactless smart cards and identification," Wiley press, 2003.

[2] ISO/IEC 18000-7, "Information technology – radio frequency identification for item management - Part 7: parameters for active air interface communications at 433 MHz," ISO/IEC, 2004.

[3] Michael, K., McCathie, L., "The Pros and Cons of RFID in Supply Chain Management," International Conference on Mobile Business, July 2005.

[4] ISO/IEC 15961, "Information technology – radio frequency identification (RFID) for item management – data protocol: application interface," ISO/IEC, 2004.

[5] ISO/IEC 15962, "Information technology – radio frequency identification (RFID) for item management – data protocol: data encoding rules and logical memory functions,"ISO/IEC, 2004.

[6] Atmel, Atmega128(L) datasheet, http://www.atmel.com, 2005.

[7] XEMICS, XE1203F datasheet, http://www.xemics.com, 2005.

[8] RICOH, RTC Rx5C348A datasheet, http://www.ricoh.com, 2003.

[9] Skyworks, AS214-92 datasheet, http://www.skyworksinc.com, 2004.

[10] Maxim, MAX3221 datasheet, http://www.maxim.com, 2005.

[11] Linear technology, LT1302 datasheet, http://www.linear.com, 2004.

[12] B. Schneier, Applied Cryptography, John Wiley & sons, New York. 1996.

Article received: 2009-01-28