A New Implementation Methodology for a Secure Distance Bounding Protocol

Hasan Unlu[1], Berna Ors[1] and Gokay Saldamli[2]

[1]Istanbul Technical University, Turkey
hasan.unlu@itu.edu.tr, siddika.ors@itu.edu.tr
[2]Boğaziçi University, Turkey
gokay.saldamli@boun.edu.tr

Abstract

In this paper, the RFID distance bounding protocol proposed by Hancke and Kuhn has been implemented on an FPGA. In this protocol, round/trip delay of the electromagnetic wave is calculated by the reader in order to determine the distance between the tag and the reader. The reader authenticates the tag that is located not more than a specified distance from it.

The protocol has been implemented on a Digilent Spartan 3E FPGA kit. Verilog HDL is used to describe the protocol.

1. Introduction

RFID (Radio Frequency Identification) technology is commonly used in manufacturing, supply chain management, inventory control, etc [1]. Because of its low production costs and small size, RFID replaces traditional identification methods such as barcode. The advantages of RFID technology is the ability of authentication from a distance. Authentication from distance leads to new security problems that have to be solved. These essential problems are confidentiality of the data, observation of the channel by unwanted people, impersonation the tag or reader. Because of these problems the authentication methods used in RFID technology should be implemented securely.

Distance bounding protocols are used to not only authenticate the ID of the tag but also measure the distance between tag and reader [2]. These protocols are used to authenticate the tag and to check that it is located not more than a specified distance from the reader. In this paper, the RFID distance bounding protocol which was proposed by Hancke and Kuhn [3] has been implemented on a Field Programmable Gate Array (FPGA) [4].

2. RFID System Elements

2.1. Tag

The tag includes a microprocessor, memory to store data and an antenna for sending data to the reader via radio frequency. Tags are separated into three group according the power usage as passive, semi-active and active [1].

Passive tags do not contain a power supply. It uses power generated by electromagnetic waves sent from the reader. Electromagnetic wave is also used to respond to the reader. Because of limited power, passive tags have limited data transfers and range. Active tags contain a power supply. In this way, they can communicate without external stimulus and operate on data. They can even work with weak signal sent by the reader. There are a microprocessor, read/write memory and an embedded operating system on them. Semi-active tags contain a power supply as active tags. However, this power supply is an integrated circuit. The tag uses power generated by electromagnetic waves while communicating with the reader as passive tags. They work as passive tags, communication range is also limited. Due to the power supply, ability of data manipulation is more than passive tags.

2.2. Reader

The reader stimulus tag and transfers content of the tag to the database [11]. Depending on the application the reader may be portable or stationary. The reader is the administrator during teh communication.

3. Distance Bounding Protocol

In this section, Hancke and Kuhn's distance bounding protocol is explained. The protocol is used to provide authentication and measurement of the tag's distance from the reader. Round/trip delay of a bit between the tag and the reader, t_m, is calculated by Eq. 1 [3].

$$t_m = 2t_p + t_d \tag{1}$$

t_d is defined as the circuit delay as the sum of the logic gates, demodulation and modulation delays. t_p is the propagation delay of the electromagnetic wave. The velocity of the electromagnetic wave is closed to the velocity of the light in the air. Hence, t_p is proportional to the distance between the reader and the tag. Relationship between the distance d and the delays can be found by Eq. 2. "c" is the velocity of the light [3].

$$d = \frac{c(t_m - t_d)}{2} \tag{2}$$

The distance bounding protocol which is implemented in this work is shown in Fig. 1. In the first step of the protocol "Reader V" sends nonce N_V bit sequence to the "Tag P". This operation is shown Eq. 3 [3]

$$V \rightarrow P : N_V \tag{3}$$

The reader and the tag concatenate the key K and the nonce N_V and calculate the hash of concatenation. The tag splits the result into two bit sequences as R^0 and R^1. The bit length of R^0 and R^1 is n. Equation 4 shows this operation. ":=" denotes assignment operation [3].

$$R_1^0 R_2^0 R_3^0 \dots R_n^0 || R_1^1 R_2^1 R_3^1 \dots R_n^1 := h(K, N_V) \tag{4}$$

After this operation, random bit sequence $C = (c_1, c_2, \cdots, c_n)$ is generated by the reader. The reader sends all c_i subsequently to the tag. When c_i is received by the tag, then the tag sends $R_i^{c_i}$ to the reader. Equation 5 and 6 show bit transfers of the reader to the tag and the tag to the reader, respectively [3].

$$V \rightarrow P: \; c_i \in \{0,1\} \quad \forall i \quad 1 \leq i \leq n \tag{5}$$

$$P \rightarrow V: \; R_i^{c_i} \in \{0,1\} \quad \forall i \quad 1 \leq i \leq n \tag{6}$$

After all the responses of the tag are taken before, t_m, the tag is not further than a specified distance d. In the last step, the reader compares the calculated bit sequence with the received bit sequence. If they are the same the tag is authenticated.

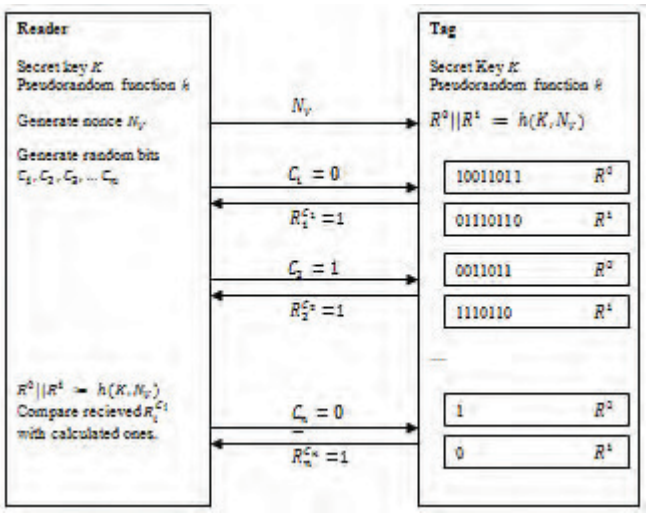

Fig. 1. Summary of the protocol [3]

4. Implementation of the Protocol

4.1. Circuit Design

The Hancke and Kuhn distance bounding protocol has been implemented on a Digilent Spartan 3E Development Board [5]. There is a XC3S500E FPGA produced by Xilinx on this board. The board has 8 LEDs, 4 switches, 4 buttons, VGA port, PS/2 port, serial communication interface, digital analog converter, analog digital converter and RAMs, 50 MHz oscillator [5].

Verilog Hardware Description Language (HDL) is used to describe the designed circuit [6]. In this work Xilinx ISE Design Suite 12.2 [9] synthesis tool, Verilog HDL and ISIM simulator [10] are used.

In the implementation step, tag and reader should satisfy some conditions. The most important condition that the tag should satisfy is that tag should respond to the reader as soon as it gets a message from the reader without waiting for any signal. Hence, it should be designed asynchronously [3]. If it is a synchronous circuit, the tag always waits for a rising or a falling edge of a clock signal. As the result of synchronous operation with a clock signal, the distance can be perceived further than the actual location.

Hancke and Kuhn protocol offers two channels. If two channels are used, asynchronous circuit can never recognize subsequent 00…0 or 11…1 bit sequence. In order to resolve this problem, number of channels must be increased. Figure 2 shows the first proposed system that uses four channels.

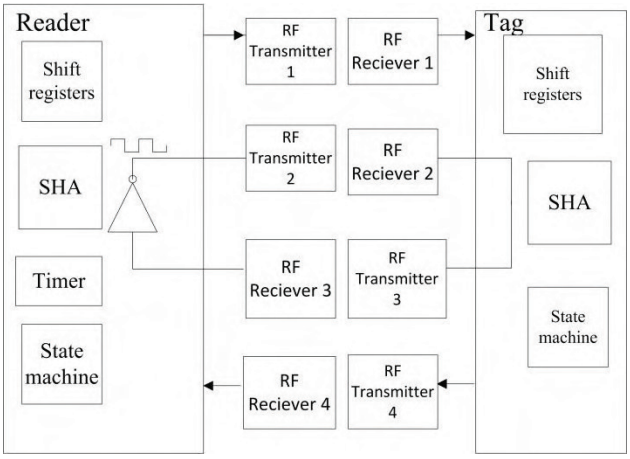

Fig. 2. The First Proposed System

In Fig. 2, ring oscillator [12] whose frequency varies with the distance is established between channel 2 and channel 3. A simple ring oscillator structure is shown in Fig. 3.

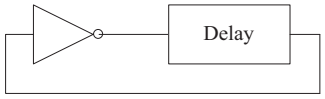

Fig. 3. Ring Oscillator [12].

Frequency of the ring oscillator is inversely proportional to the distance. The frequency f_{osc} is calculated by Eq. 7.

$$f_{osc} = \frac{1}{2(2t_p + t_d + t_{gd})} \tag{7}$$

t_{gd} is a inverter gate delay. The ring oscillator is connected to the shift registers. Thus, bit transfer time is proportional to the distance. In order to determine the distance, the time needed to transfer all the bit sequence is measured, instead of the time needed to transfer just one bit. Because, the time needed to transfer just one bit cannot be measured with enough precision.

The most important problem for the implementation is that the modulation and the demodulation delays of the RF modems are not constant. This problem leads to change the oscillator frequency for each measurement.

Another problem occurs due to the short distance between the tag and the reader. As the result of this problem, the oscillator frequency reaches gigahertz scale. But, the hardware operating frequency should be below gigahertz scale.

Because of these problems, in order to have a model of the actual system, the protocol is implemented on an FPGA and the channels and the RF modems are modeled by using shift registers. In order to change the distance, the number of flip-flops in the shift registers is changed. The alternative system is shown Fig. 4. The flow chart of the reader and the tag are shown Fig. 5 and 6.

All the shift operations are triggered by the distance controlled ring oscillator in the tag and the reader. In Fig. 5, the reader starts the timer before sending the random bits. The timer resolution determines the precision of the distance. Because we

are using the time needed to transfer all the bit sequence, we can use lower frequency for the time in the reader. Hence the resolution can be higher.

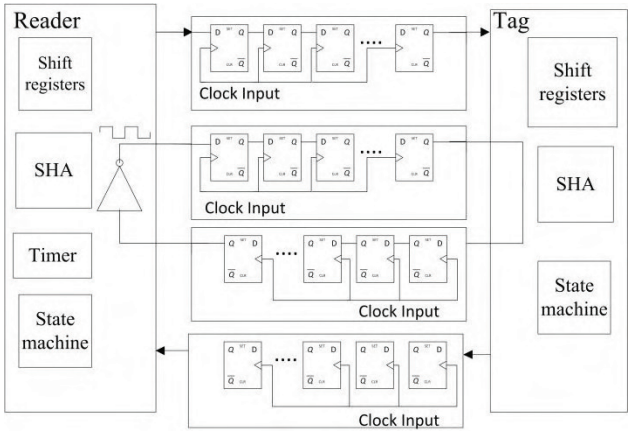

Fig. 4. Implementation without RF Modems

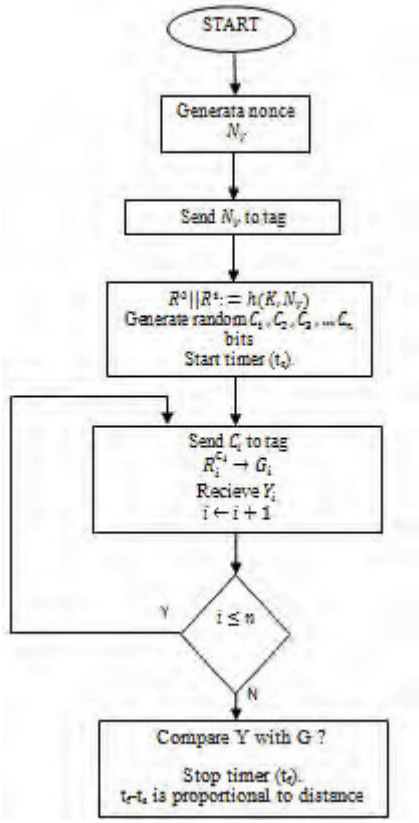

Fig. 5. Reader flow chart

Device utilization summary of the design generated by ISE Design Suite is shown in Fig 7. Maximum operating frequency of the design is 113.7 MHz.

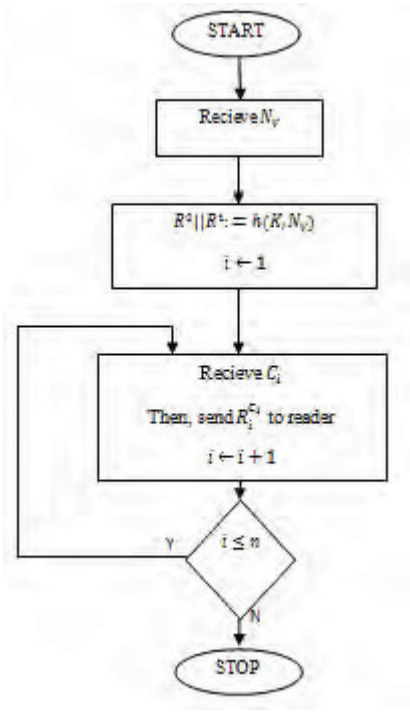

Fig. 6. Tag flow chart

4.2. Test Results of the Design

The simulation results are shown in Figure 8. The tag_signal_in and reader_signal_in pins show oscillation between the tag and the reader. As a first step the reader sends N_V bit sequence. The tag reads data in the falling edge of the tag_signal_in. After N_V is sent, (after 400 ms), the reader starts to send the C random bit sequence. Simultaneously, the timer is started. If C is logic-0 R^0 is selected, else R^1. package_R0 and package_R1 shows R^0 and R^1. If any bit is sent, registers are shifted by 1 bit. The expected_bit_sequence and the reader_received signals are compared with each other. The simulation results show that the received and the expected bit sequence are the same for the last 10 bits. After bit transfer is completed, the timer is stopped. In order to determine the distance, the timer register's most significant six bits can be used. If the resolution is not enough for the distance, the timer frequency or the number of bits can be increased.

Device Utilization Summary				
Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Number of Slice Flip Flops	109	9,312	1%	
Number of 4 input LUTs	339	9,312	3%	
Number of occupied Slices	222	4,656	4%	
Number of Slices containing only related logic	222	222	100%	
Number of Slices containing unrelated logic	0	222	0%	
Total Number of 4 input LUTs	392	9,312	4%	
Number used as logic	81			
Number used as a route-thru	53			
Number used as Shift registers	258			
Number of bonded IOBs	14	232	6%	
Number of BUFGMUXs	4	24	16%	
Average Fanout of Non-Clock Nets	1.81			

Fig. 7. Device Utilization Summary

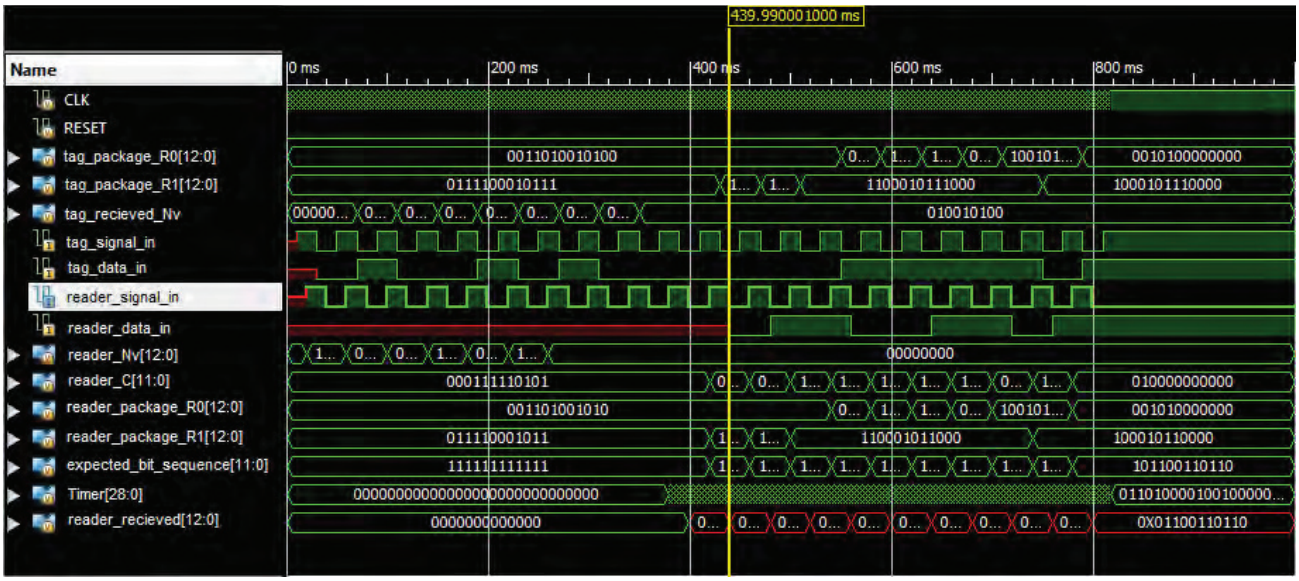

Fig. 8. Simulation Result

The distance is proportional to number of flip-flops in the shift register. Sensitive of measurement is recognizing minimum number of flip-flops. Sensitivity of the implementation is one flip-flop. This ability depends on shift register frequency and timer frequency. If frequency of timer in the reader is higher than frequency of shift register in the channel, sensitivity of measurement is higher. In the implementation shift register frequency is 10 KHz and timer frequency is 50 MHz.

5. The Previous Implementations

Rasmussen and Ćapkun's implementation [13] demonstrated that the protocol can be implemented to match the strict processing this protocol requires. Their protocol measures 1 bit transfer time. This time measurement requires hardware that runs at several gigahertz or more. If they want to more precision measurement, needs better hardware. Our design measures the distance using summation of all propagating delay. Hence, our design does not need high resolution timer and processing unit. This summation decreases error rate. Because, summation of bit sequence transfer time can be measured by lower hardware.

Hancke's design [14] uses sync pulse. This pulse causes sampling error. Therefore, the distance measured with error. Hancke's design also measures 1 bit transfer time. Then, it has same problems as Rasmussen and Ćapkun's implementation. Ring oscillator in our design generates distance dependence sync clock. Only measurement error occurs, due to varying modulation, demodulation time and timer frequency stability. But, disadvantage of our design is that uses more number of channels than other designs.

6. Conclusion

As a result of implementation of the protocol gives idea of how to implement. Most important part of our design is that it can sum all propagation delay of one bit transfer. This means we not need to measure one bit transfers, measure n*(1 bit transfer time). n represents number of bit will be transferred.

The implementation, tag can cheat the reader. If the tag signal out is connected to any variable frequency oscillator, the delay is independent from distance.

The tag configures frequency of oscillator in order to change distance. But, in the authentication step, tag should response correct bit sequence. If the tag estimates these n bits, possibility of authentication is $(1/2)^n$. Bit length can be increased for more security.

7. Acknowledgments

Note that, Gokay Saldamli is partially funded by TUBITAK research project No: 109E180 and Berna Ors is partially funded by TUBITAK research project No: 110E172.

8. References

[1] K. Finkenzeller, "RFID Handbook", Carl Hanser Verlag, Münih, 2003.

[2] S. Brands and D. Chaum, Distance-bounding protocols. Advances in Cryptology EUROCRYPT '93, Springer Verlag, LNCS 765, pp. 344–359.

[3] Hancke G., Knuh M., An RFID Distance Bounding Protocol, Proceeding of SECURE COMM'05, pp. 67-73, IEEE Computer Soceity, 2005.

[4] J. M. Rabaey, Digital Integrated Circuits, 2nd ed., Prentice Hall, 2002.

[5] UG230, 2006, Spartan 3E Starter Kit Board User Guide.

[6] J. Mermet, Fundamentals and Standards in Hardware Description Languages, Springer, 1993.

[7] M. D. Ciletti, Advanced Digital Design with the Verilog HDL, Prentice Hall, 2003.

[8] P. J. Ashenden, The Designer's Guide to VDHL, 2nd ed., Morgan Kaufmann, 2001.

[9] Introduction to Xilinx ISE 8.2i, University of Pennsylvania.

[10] UG660, 2009, Xilinx ISIM User Guide.

[11] D. E. Brown, RFID Implementation, McGraw-Hill, New York, 2007.

[12] T. H. Lee, The Design of CMOS Radio-Frequency Integrated Circuits. Cambridge, U.K.: Cambridge Univ. Press, 1998.

[13] K. B. Rasmussen, S. Capkun, Realization of RF distance bounding protocol, 19th USENIX Security Symposium, 2010

[14] G. Hancke, Design of a Secure Distance Bounding Channel for RFID, 2010