인증 기능을 갖는 방향 결정 자율이동 RFID 시스템

박철민* · 조형국* · 이훈재*

A Direction-Decision RFID System with a Authentication

Chul-Min Park* · Heung-Kuk Jo* · Hoon-Jae Lee*

본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의
연구결과(IITA-2008-C1090-0801-0026)와 지역혁신 인력양성사업의 연구결과로 수행되었음

요 약

RFID은 다양한 응용이 가능하며, RFID 시스템의 기본적인 목적은 대상물의 인증이다. RFID 시스템은 태그의 인증 후에 시스템이 원하는 프로세스를 수행한다. 태그가 움직이는 대로 뒤따르는 RFID 전동 시스템은 응용 범위가 넓다. 예로서 쇼핑 몰에서 카트가 자율적으로 인증된 고객의 뒤를 따르는 것이다. 고객이 직접 카트를 끌지 않고, 고객의 진행하는 방향을 인지하여 자율적으로 뒤를 따른다면 매우 편리할 것이다. 본 논문에서는 RFID를 이용하여 태그를 소지하고 있는 물체를 자율적으로 뒤따르는 방향결정 자율이동 RFID 시스템에 대해 연구하였다. 제안된 RFID 시스템은 태그, 리더 그리고 호스트 컴퓨터로 구성되며, 시스템을 구현하여 실험 및 분석하였다.

ABSTRACT

RFID is applied in various industry area. The purpose of RFID system is authentication of objects. After Tag's certification, RFID system start to process to be wanted. A RFID electric motor recognizes Tag's action and tails. The application of this system is very wide. For example, a cart in shopping Mall follows customer with a proper Tag. Customer may be very convenient if the cart follows customer autonomously as recognizing the direction of Tag. In this paper, we studied about RFID system that follow objects with a Tag. Finally, we experimented and analysed the proposed system, with Tag, Reader, host computer and electric motion motors.

키워드

Keywords: RFID, security, encryption, cipher, agent, TCP/IP

Ⅰ. 서론

RFID시스템은 다양한 응용이 가능하다. RFID 시스템의 기본적인 사용 목적은 인증이다.

RFID 시스템은 태그(Tag)의 인증 후에 응용 시스템이 원하는 프로세스를 수행한다. RFID 시스템에서 태그가 움직이는 대로 자율적으로 뒤따르는 RFID 전동 시스템은 한 응용 예이다. 그 응용의 예는 쇼핑 몰에서 카트가 자율적으로 인증된 고객의 뒤를 따르는 것이다. 고객이 직접 카트를 끌지 않고 고객의 진행하는 방향을 인지하

* 동서대학교 컴퓨터정보공학부

접수일자 2008. 03. 21

여 자율적으로 뒤를 따른다면 매우 편리할 것이다. 시스템의 구성은 다음과 같다. RFID를 구성하고 있는 안테나와 발진부를 2개(RFID Reader front)로 하고, 이것을 제어하는 호스트 컴퓨터 부분을 하나로 하는 시스템으로 구성하였다. 이 시스템은 태그에서 전달 되어온 전파를 2개의 리더 전단부(reader front)에 있는 안테나로부터 수신한다. 수신된 전파의 세기는 송신 위치에 따라 다르다. 이 두 안테나의 수신 전파의 세기의 차이를 이용하여 마이크로 프로세스는 태그의 위치를 인지할 수 있다. 태그의 위치를 인지한 마이크로 프로세스는 모터 드라이브를 통하여 운반체를 움직일 수가 있다.

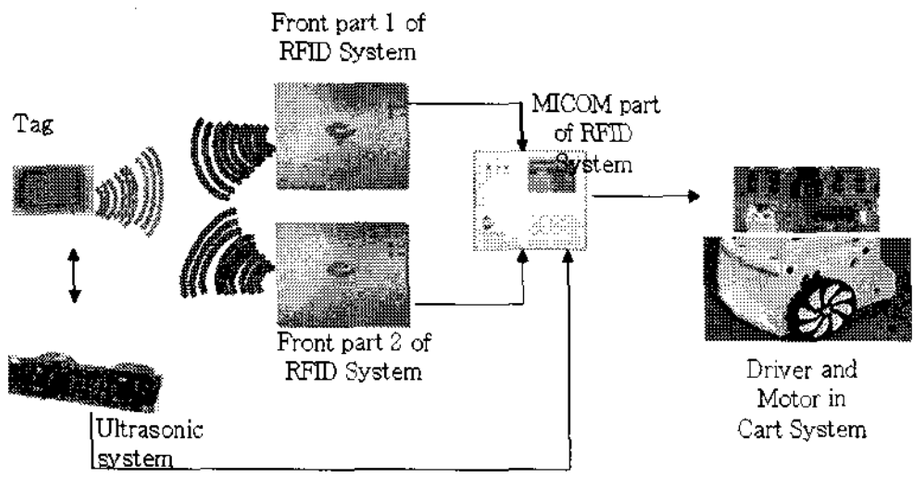


그림 1. 방향 결정 자율이동 보안 RFID 시스템
Fig. 1 Autonomously movable, secure RFID system

대부분의 RFID 시스템은 물체 인식을 위하여 사용된다. RFID 시스템에서 리더기는 안테나부, 송수신부, 동작 주파수 발진부 그리고 마이컴 부분이 있다. 태그 위치 추적 시스템을 만들기 위해서는 다음과 같이 RFID 시스템을 부분별로 나누었다. 우선 RFID 시스템에서 마이컴 부분을 제외한 부분을 RFID 전단부 (RFID front)라고 한다. 이 전단부는 본 시스템에서 2개가 필요하다. 왜냐하면 능동 태그(active Tag)의 위치에 따라 들어오는 신호의 차이를 알기 위함이다. 이 두 전단부는 마이크로 콘트롤러에서 폴링(polling) 방식으로 교번적으로 동작한다. 또한 태그와 운반체의 거리를 일정하게 유지하기 위해서 초음파 센서를 부가한다. 이 센서 또한 마이크로 콘트롤러와 연결되어 있다. 그림 1은 구현하고자 하는 시스템의 개략도를 보인다.

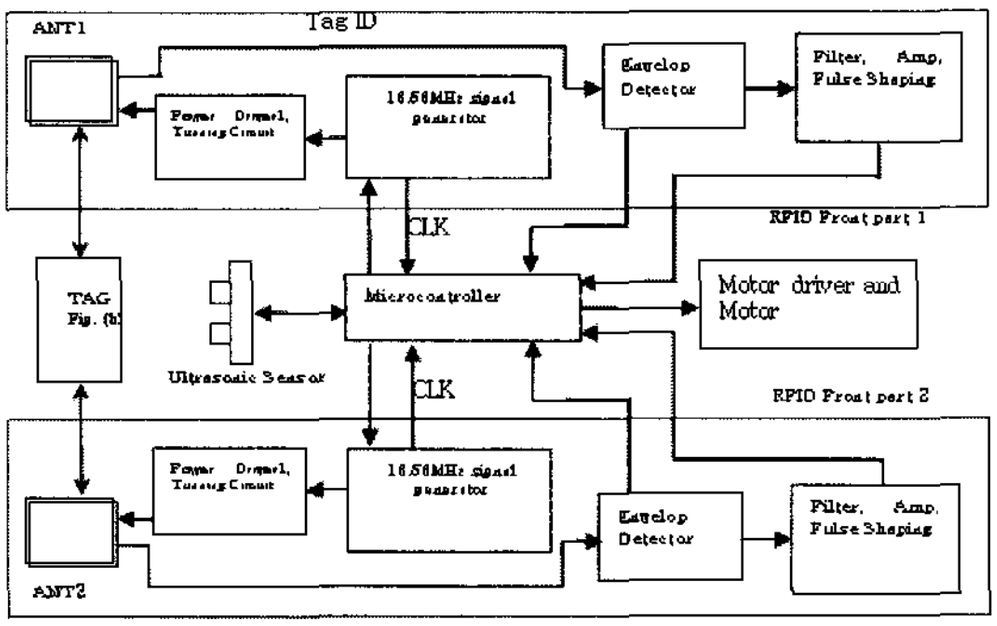
RFID 전단부 2가지 동작을 수행한다. 첫째는 태그의 인증과정이고, 두번째는 태그의 위치를 인지하는 것이다. 우선 인증과정은 다음과 같다. 동작신호의 발생은 13.56MHz 발진기를 이용하고, 태그로 데이터를 보낼 때 필요한 반송파로 이용된다. 이 반송파는 증폭되고, 이 신호는 마이크로 콘트롤러에서 보내온 데이터와 AND 게이트를 통하여 동조회로로 보내진다. 동조회로를 통하여 신호는 안테나를 통하여 능동태그로 보내어 진다. 태그는 수신된 데이터를 포락선 검파를 거쳐 태그 내부의 마이크로 콘트롤러로 입력되며, 인증과정을 거친다. 능동 태그는 응답 신호를 리더기와 같은 방법으로 리더기의 전단부 안테나로 보낸다. 수신된 태그 데이터는 포락선 검파를 수행한다. 검파된 신호파를 필터(filter), 증폭기(amplifier), 그리고 펄스 정형화(pulse shaping)를 거쳐 CPU가 인식할 수 있는 파형으로 정형화된다. RFID 후반부인 컨트롤러는 이 파형을 호스트 컴퓨터와 통신을 하도록 데이터 디코딩을 수행한다. 태그의 위치 인지는 2개의 RFID 전단부의 각 안테나에 들어온 태그의 데이터를 포락선 검파를 수행한 후 A/D 변환기를 통하여 컨트롤러에 입력된다. 컨트롤러에서 두 신호는 비교하여, 두 신호의 차이 값으로 태그의 위치를 알 수 있다.

본 논문에서는, RFID를 이용하여 태그를 소지하고 있는 물체를 자율적으로 뒤따르는 방향 결정 자율이동 RFID 시스템에 대해 연구하고자 한다. 제안된 RFID 시스템은 2개의 RFID 전단부를 하나의 컨트롤러에서 폴링 방식으로 제어를 구현한다. 두 개의 안테나에 수신되는 태그의 데이터는 포락선 검파기에서 수신 전력의 차이를 알 수 있다. 이 신호를 A/D를 이용하여 계수화 한 다음 컨트롤러로 보내어 태그 좌측 또는 우측 안테나에 가까이 있는지를 인지하는 시스템을 구현하고, 실험 및 분석하고자 한다.

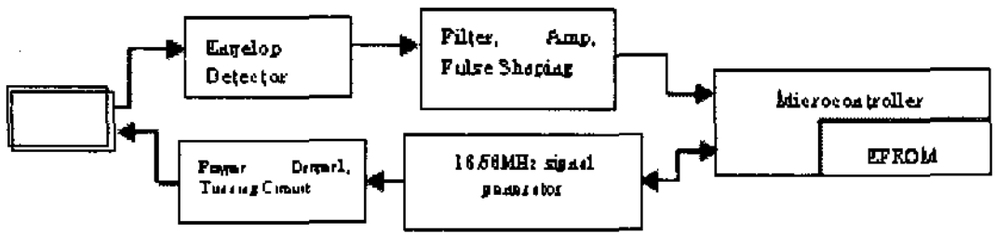
II. 시스템 제안 및 구성

그림 1의 개념도에 대한 세부 블록 다이어그램은 그림 2와 같다.

그림 2의 (a)에서 마이크로 콘트롤러는 13.56MHz 신호 발진기에서 받은 CLK신호로 동작한다. 이 주파수는 반송 주파수로 사용된다. 또한 마이크로 콘트롤러에서 폴링 방법으로 전력 구동부 1 (Power Driver 1) 및 전력 구동부 2 (Power Driver 2)를 교번적으로 동작시킨다. 이 동작으로 수신된 태그 ID는 포락선 검파와 필터를 거친 후 마이크로 콘트롤러가 인식할 수 있는 신호로 변환되며, 컨트롤러에 태그의 ID를 입력하게 된다.



(a) Multi-reader



(b) Active Tag

그림 2. 개념도 1에 대한 블록 다이어그램
Fig. 2 Block diagram for fig. 1

그러나 인증을 위한 태그의 ID는 이 시스템을 동작되는 동안 지속적으로 입력되는 것이 아니며, 약 100ms 마다 한 번씩 인식하도록 한다. 포락선 검파기는 태그의 ID 데이터 수신하면 태그와 리더기의 안테나 사이의 거리에 따라 파의 진폭이 매우 달라진다. 왜냐하면 거리에 따라 파의 세기는 지수 함수적으로 감소하기 때문이다. 이때 컨트롤러 안에 내장되어 있는 A/D를 통하여 2진으로 계수화 하여 서로 비교한다. 만약 그림 2에서 두 안테나 사이의 정 중앙 점에 태그가 존재 한다면 두 안테나에서 수신된 파형의 진폭은 같을 것이다. 그러나 태그가 안테나 1에 근접해 있다면 안테나 1에 연결된 포락선 검파기의 진폭은 안테나 2에 비해 상대적으로 매우 큰 값을 가진다. 이로 인해 컨트롤러는 태그가 안테나 1의 위치에 있다는 것은 알게 된다. 만약에 태그가 안테나 1에서 안테나 2의 위치로 옮겨 간다면 컨트롤러는 태그의 진행 방향을 알 수 있게 된다. 이로서 태그를 소유하고 있는 물체가 움직일 때 컨트롤러는 좌우로 움직이는 방향을 인지하여 모터(motor)를 이용하여 방향을 전환한다. 또한 이 물체와 일정한 거리를 유지하기 위해서 초음파 센서를 부착한다. 이 거리는 30cm에서 1m까지 가능하도록 컨트롤러에 설정한다. 혹은 외부 에서 입력시킬 수 도 있다.

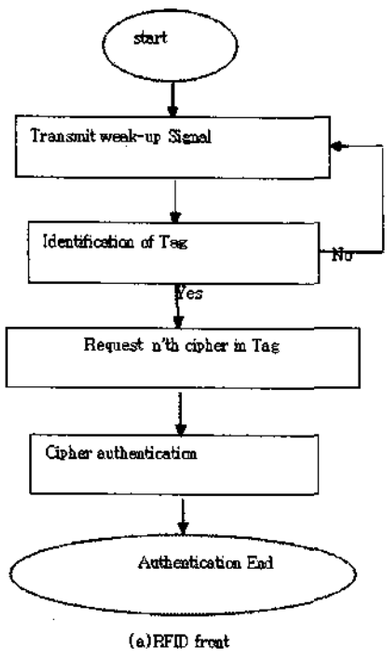
2.1 하드웨어 구성

하드웨어 구성은 RFID 전단부와 컨트롤러 부분이 있다. 그리고 거리의 인식을 위해 초음파(ultrasonic) 부분이 있다. RFID 전단부는 전력 구동부 (power driver), 신호 발생기 및 분배부 (signal generator and divider), 포락선 검파부 (envelop detector), 그리고 펄스 정형화부 (pulse shaping)로 구성된다. 전력 구동부는 데이터를 안테나로 보내는 역할을 한다. 이 회로의 구성은 FET로 만들어 진다. 만약 태그를 소유하고 있는 물체가 2m 이상이 떨어져 있으면 반송파 출력을 높이기 위하여 여러 개의 FET를 사용해야 한다. 만약 근거리 일 때는 출력을 감쇠시키기 위해서 감쇠기를 사용해야 한다. 포락선 검파기의 구성은 다이오드, 콘덴서 그리고 저항을 사용한다. 이검파기는 태그에서 들어온 파형 세기를 측정하기 위한 것이다. 그림 2 (a)에서 보였듯이 2개의 RFID 전단부의 검파기 출력은 컨트롤러로 들어가 전파의 세기를 비교하게 된다. 13.56MHz 안테나는 콘덴서와 안테나 코일이 필요하다. 이것은 LC 동조회로이며, 데이터는 이 동조 회로를 통해 공간으로 전파된다. 반송파 발생은 13.56MHz 발진기를 사용하여 반송파가 발생되며, 이 반송파는 마이크로 프로세스와 전력구동부로 연결된다.

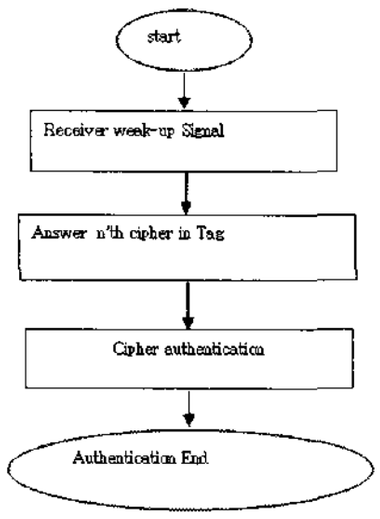
2.2 소프트웨어 구성

그림 3 (a)는 RFID 전단부 동작 운용 알고리즘이며, 태그로 동작신호를 보내어 태그를 확인하는 과정이다. 만약 확인이 되지 않으면 다시 동작 신호를 보내어 확인하려고 하는 태그를 찾을 때까지 반복한다. 만약 태그가 확인되면, 태그 안에 있는 n' 번째 인증 암호를 호출하게 된다. 이 암호는 이 시스템의 동작이 완료할 때까지 지속적으로 인증 절차를 갖는다.

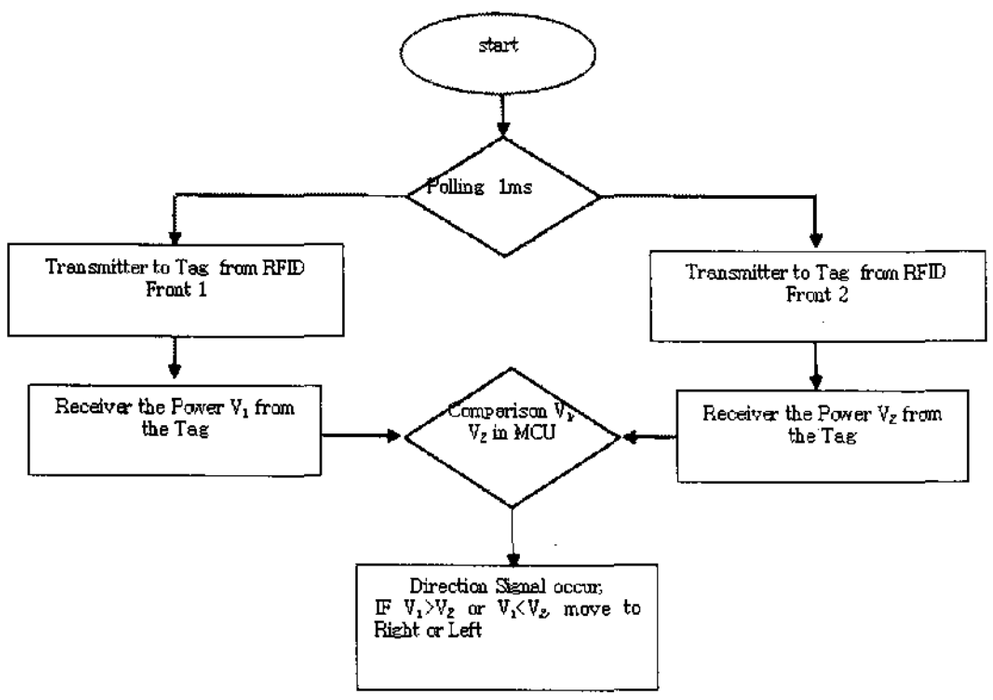
그림 3 (b)는 태그의 ID 인증 동작 알고리즘이다. 리더에서 태그내의 n 번째 ID를 요구 하면 태그는 그 ID를 전송한다. 그리고 리더와 태그는 상호 인증을 완료하게 된다. 그림3 (c)는 2개의 전단부에서 반송파를 송신 및 수신하는 방법을 보였다. 그리고 수신된 신호의 크기로 태그 의 좌우 위치를 판단할 수 있는 알고리즘을 제시하였다.



(a)RFID front



(b) Tag



(c) Detection of Tag position from Reader

그림 3. 구동을 위한 알고리즘
Fig. 3 Algorithms for implementation

잡음이 많은 무선네트워크에서는 블록 암호의 **OFB** (output feedback mode) 모드를 적용하는 것이 유리하다. **OFB** 모드를 적용할 경우 **ECB**(electronic codebook mode) 모드를 적용하는 것보다 에러에 덜 민감하며 에러 관리가 용이하다. 본 논문에서는 **DES** 알고리즘의 암호학적 취약점에 따라, 표 1에서와 같이 **FIPS-197** 미연방 표준으로 개선된 **AES** 암호 알고리즘 **[20]**, **T-DES** (Triple-DES) 알고리즘, 그리고 국내 표준암호인 **ARIA** 알고리즘 **[21]** 과 **SEED** 알고리즘 **[22]**을 적용하여 **RFID** 암호화에 적용하는 방법을 제시하였다.

전술한 바와 같이 무선 통신을 위하여 블록 암호는 **OFB** 모드를 적용하여야 하며, 이 때 **OFB** 모드는 **PN** (pseudo-noise)-발생기와 같은 작용을 하며, 일부 출력은 암호화를 위한 **XOR** 연산으로 입력하고 나머지 출력은 블록암호의 입력 버퍼로 이동하여 입력시킨다. 최종적으로 평문은 **PN** 출력과 함께 **XOR** 연산되어 암호화된다.

표 1. 암호 적용 방법
Table 1. Security algorithms

Items	Secure Algorithm	
	Confidentiality algorithm	Authentication algorithm
Block mode (고비도, 고전력형)	AES[20], ARIA[21], SEED[22], T-DES, IDEA	SHA-1[27], HAS-160[28], MD5, AES-CBC, SEED-CBC, ARIA-CBC
Stream mode (고비도, 저전력형)	PingPong[23], LILI-II[24], Dragon[25], Parallel-LM[26]	

스트림 암호 알고리즘으로 제시된 **PingPong[23]**, **LILI-II[24]**, **Dragon[25]**, 및 **Parallel LM[26]**는 출력 모드와 관계없이 무선 통신에 적합한 암호학적 특징을 갖는다. 이 들은 암호학적으로 안전성과 고속 처리성, 그리고 더욱 빠른 암호학적 적용을 위한 병렬형 구현이 가능하다. 또한 휴대성을 위한 저전력형, 하드웨어 구현 효율성이 부수적으로 지원된다. 그림 8에서 보여준 **PingPong [23]**은 두 개의 **LFSR** 레지스터, 두 개의 클럭 조절 함수 (clock-control functions) fa & fb, 두 개의 귀환 함수 (feedback functions) fc & fd, 그리고 하나의 출력 함수 (output function) fz.로 구성되어 있다.:

$$f_a(L_a) = 2L_{a42}(t) + L_{a85}(t) + 1 \quad (1)$$

$$f_b(L_b) = 2L_{b43}(t) + L_{b86}(t) + 1 \quad (2)$$

$$c_j = f_c = a_j b_j \oplus (a_j \oplus b_j) c_{j-1} \quad (3)$$

$$d_j = f_d = f(a_j, b_j, d_{j-1}) = b_j \oplus (a_j \oplus b_j) d_{j-1} \quad (4)$$

$$z_j = f_z = a_j \oplus b_j \oplus c_{j-1} \oplus d_{j-1} \quad (5)$$

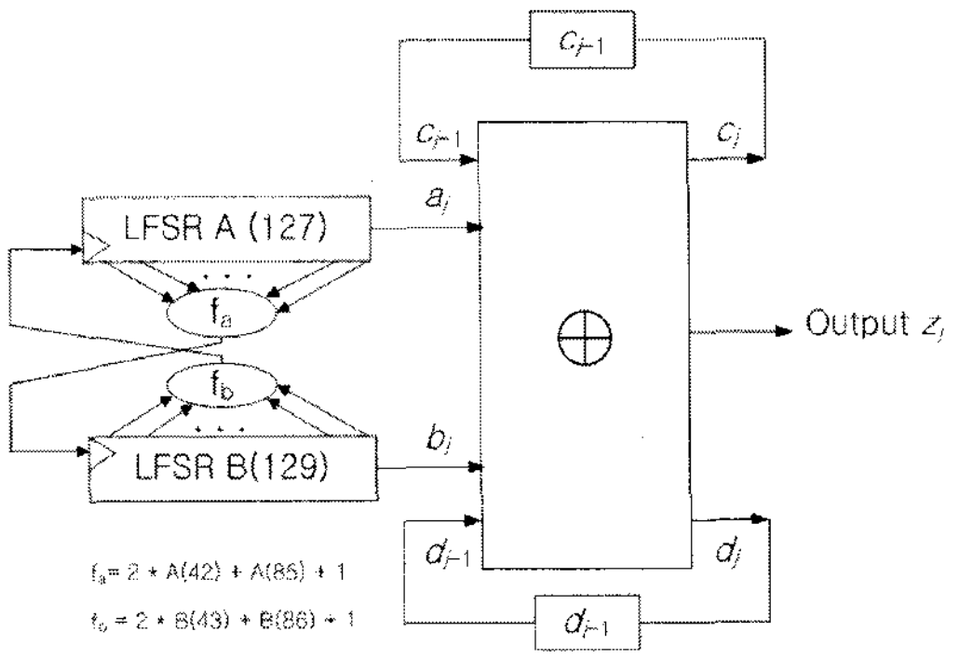
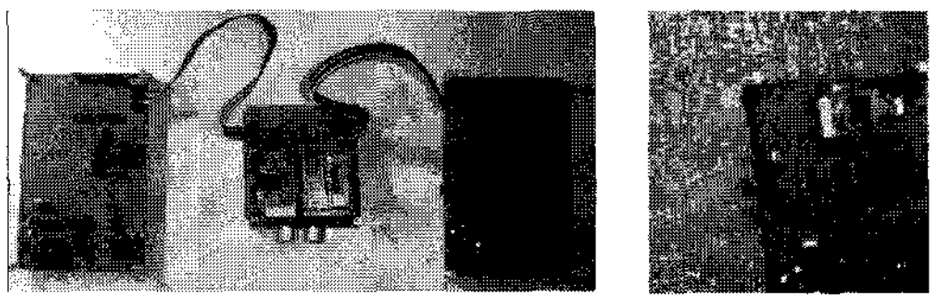


그림 4. Ping-Pong 키수열 발생기 (스트림 암호)
Fig 4. Ping-Pong keystream generator (stream cipher)

결과적으로, Ping-Pong은 암호 알고리즘의 안전성이 높고, 구성이 간단하며, 하드웨어 또는 소프트웨어 구현이 용이하기 때문에 RFID 전송 시스템에 적용할 때 경량 암호로 적합한 스트림 암호 형태이다.

Ⅲ. 실험 및 성능

그림 5에서 RFID를 탑재한 실험 시스템을 보인다. 그림 5 (a)는 2개의 RFID 전단부와 중앙에 마이크로 콘트롤러로 구성되어 있다. 마이크로 콘트롤러는 Atmega 128을 사용하였으며, 그림 4 (b)는 태그의 구성이다. 이 태그 내에도 역시 128 마이크로 콘트롤러를 가지고 있다.



(a) (b)

그림 5. 실험 시스템 (a) 2개의 RFID front와 마이크로 콘트롤러 (b) Active Tag
Fig. 5 Experimental system (a) two RFID front and microcontroller (b) Active Tag

표 2. 태그의 거리와 위치에 따른 전압 차이
Table 2. Voltage differences for distance and for position of tag

Position of Tag	Left side	Middle	Left Side	
state of V_1 and V_2	$V_1 > V_2$	$V_1 = V_2$	$V_1 < V_2$	
D > 1.5m	60mv Value of $\|(V_1 - V_2)\|$	0mv Value of $\|(V_1 - V_2)\|$	60mv Value of $\|(V_1 - V_2)\|$	stability
1m < D < 1.5m	100mv Value of $\|(V_1 - V_2)\|$	0mv Value of $\|(V_1 - V_2)\|$	100mv Value of $\|(V_1 - V_2)\|$	Relative stability
D < 1m	300mv~150mv Value of $\|(V_1 - V_2)\|$	0mv~40mv Value of $\|(V_1 - V_2)\|$	300mv~150mv Value of $\|(V_1 - V_2)\|$	unstability

D: Distance between Front and Tag, V_1 : Voltage of Front 1, V_2 : Voltage of Front 2

실험에서 능동형 태그의 사용으로 거리에 따라 진폭이 매우 급격하게 변화함을 얻을 수 있으며, 이 변화를 이용하여 태그의 위치를 알 수 있다. 표 2에서 태그의 위치가 두 전단부의 왼쪽과 오른 쪽에 위치할 때 전단부에서 측정한 전압 값을 보인다.

표 2의 측정 조건은 그림 6에 보인다.

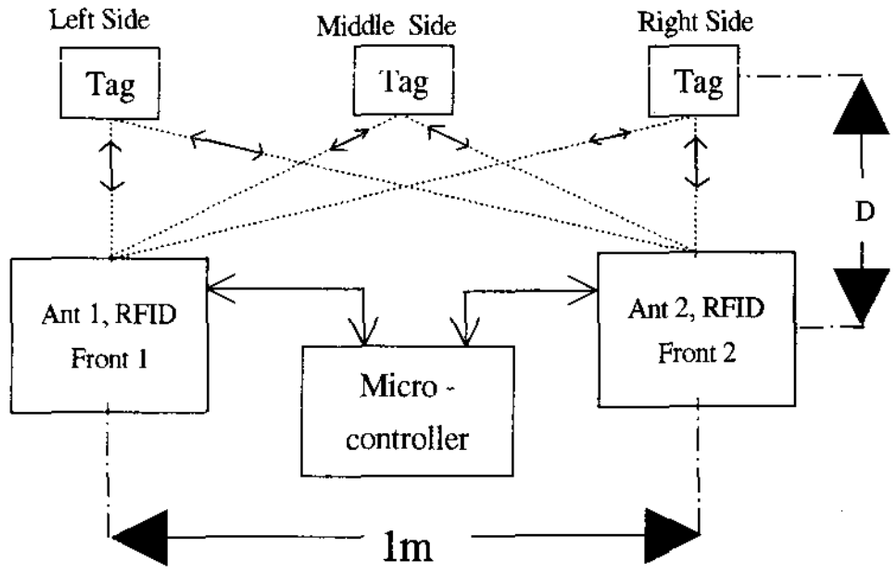


그림 6. 시스템 측정시 배치도
Fig. 6 Arrangement for measuring instruments

그림 6에서 태그는 왼쪽, 중앙 그리고 오른쪽에 두었다. 그리고 RFID Front 1과 2의 사이는 약 1m이다. RFID Front와 태그의 사이는 표 2와 같이 3가지 다른 거리에서 측정하였다. 지면에서 높이는 약 20cm이다.

Ⅳ. 결론

RFID 시스템은 다양하게 응용되고 있으며, 호스트 컴퓨터에 태그 ID 데이터를 전송하는 방법도 다양하다. 본 논문에서는 RFID를 응용한 시스템 중에 2개의 RFID를 사용하여 태그의 위치를 인지하는 시스템을 제안하였고, 이를 구현하여 성능을 분석하였다. 이는 자율 운반체와 운반체의 인식 기능이 주된 기술이며, 한편으로 이 시스템은 무선으로 데이터를 송수신하므로 노이즈에 매우 민감하다. 또한 사용자 인증을 강화하기 위하여 암호화 기능을 사용하였다.

제안된 시스템의 구현 결과, 태그와 리더기의 거리에 따라 수신 전압 차이가 매우 심하다는 사실을 확인하였다. 1.5m 이상에서는 거리에 따른 전압 값이 일정한 패턴으로 변하지만, 1m 이내에서는 수신 전압 값의 편차가 매우 크게 나타났다. 이러한 문제를 해결하기 위하여 초

음파를 이용한 일정 거리 유지 장치를 추가하였다. 또한 데이터 암호 및 사용자 인증을 위하여 Ping-pong 알고리즘을 적용하였다. Ping-Pong 암호 알고리즘은 RFID와 같은 경량, 저전력형 시스템에 적합한 알고리즘이다. 제안 시스템은 태그의 소유자만을 따르는 자율 로봇 등에 응용이 가능함을 실험적으로 확인하였다.

감사의 글

This research was supported by University IT Research Center Project of Korea and by the Program for Training of Graduate Students in Regional Innovation.

참고문헌

[1] Chipcon Tech. Support, "User Manual Rev. 2.0", Chip AS, (2004), www.chipcon.com.

[2] Hwang-Hae Kyun, Sung-Jun Bae, "I love ATMEGA128", Bok-Du Verlag, (2005)

[3] Duck-Yong Yun , "AVR ATmega128 Master", (2004)

[4] Klaus Finkenzeller, " RFID Handbook", John Wiley & Son, LTD, (1999)

[5] Jonathan Collins, "FTC Asks RFID Users to Self-Regulate", RFID Journal, Mar. 10, (2005)

[6] E. Kaasinen, "User Acceptance of MobileServices-Value. Ease of Use, Trust and Ease of Adoption," doctoral dissertation, VTT 566, VTT Publication,(2005)

[7] Vinay Deolalikar, Malena Mesarina, John Recker, Salil Pradon,"Perturbative time and frequency allocations for RFID reader networks" (2006) USN

[8] Kyung-Hyup Lee, Yoon-Young An, Hee-Dong Park, You-Ze Cho," A Data-centric Self-organization Schema for Energy-Efficient Wireless Sensor Networks" (2006) USN (USN 2006 in Seoul).

[9] Soo-Cheol Kim, Sang-Soo Yeo, Sung Kwon Kim, "MARP: Mobile Agent for RFID Privacy Protection", 7th Smart Card Research and Advanced Application IFIP Conference (CARDIS '06), Lecture Notes in Computer Science, vol.3928, pp.300-312, April 2006.

[10] "FIPA Agent Management Specification," FIPA 2004 Specification, Foundation for Intelligent Physical Agents, March 2004. <URL: http://www.fipa.org/specs/fipa00023/SC00023k.pdf>

[11] W. Jansen, T. Karygiannis, "NIST Special Publication 800-19 - Mobile Agent Security, <URL: http://csrc.nist.gov/publications/nistpubs /800-19/sp800-19.pdf>

[12] W. Stalling, Cryptography and Network Security (4th edition), Prentice-Hall, 2006.

[13] W. Trappe & L. Washington, Introduction to Cryptography with coding theory (2nd edition), Prentice-Hall, 2006.

[14] NIST, "Announcing the Advanced Encryption Standard (AES)", FIPS-197, Nov. 2001.

[15] Daesung kwon, Jaesung Kim, Sangwoo Park, Soohak Sung, Yaekwon Sohn, Junghwan Song, Yongjin Yeom, E-Joong Yoon, Sangjin Lee, Jaewon Lee, Seongtaek Chee, Daewan Han, and Jin Hong, "New Block Cipher: ARIA," LNCS 2971 - ICISC2003, pp.432-445, Springer, 2004.

[16] KISA, Development of SEED, the 128-bit block cipher standard, Oct, 1998. (http://www.kisa.or.kr)

[17] A. Clark, E. Dawson, J. Fuller, J. Golic, Hoon-Jae Lee, W.Millan, Sang-Jae Moon, L. Simpson, "The LILI-II Keystream Generator," LNCS 2384, pp.25-39, Jul. 2002 (ACISP'2002)

[18] Kevin Chen, M. Henrickson, W.Millan, J. Fuller, A. Simpson, Ed Dawson, Hoonjae Lee, Sangjae Moon, "Dragon: A Fast Word Based Stream Cipher," LNCS (ICISC'2004)2004.12.2-12.3

[19] Hoonjae Lee, Sangjae Moon, "Parallel Stream Cipher for Secure High-Speed Communications," Signal Processing, Vol.82,No.2,pp.259-265, Feb, 2002.

[20] Federal Information Processing Standards (FIPS) Publication 180-1, Secure Hash Standard (SHS), U.S. DoC/NIST, Aug. 1, 2002.

[21] TTAS.KO-12.0011/R1, "Hash Funtion Standard - part 2: Hash Function Algorithm Standard (HAS-160)," Dec. 20, 2002. (http://www.tta.or.kr)

[22] R.C.Joshi and Shashikala Tapaswi, "Frame Sliced Parallel Signature Files for Fast Colored Image Retrieval", JCIT:Journal of Convergence Information

Technology, Vol.2 No.2, pp.5-9, 2007.
[23] Sanjay Raghani, Durga Toshniwal and R. C. Joshi, "Distributed Certification Authority for Mobile Ad Hoc Networks - A Dynamic Approach", JCIT:Journal of Convergence Information Technology, Vol.2 No.2, pp.10-21, 2007

저자소개

박 철 민 (Chul-Min Park)

2002년 3월 ~ 현재 : 동서대학교 컴퓨터정보공학부 재학중
※관심분야 : RFID 시스템, 무선통신, HW 설계

조 형 국(Heung-Kuk Jo)

1973년 2월 : 동아대학교 전자공학과 졸업(학사)
1979년 2월 : 동아대학교 전자공학과 졸업(석사)
1990년 2월 : 베를린공과대학교 음향전자연구소 졸업 (박사)
1990년 2월~1993년2월 : 삼성전자 기술총괄 선임연구
1993년 3월~현재 : 동서대학교 컴퓨터정보공학부 부교수
※관심분야 : RFID 시스템, 무선통신, HW 설계

이 훈 재(HoonJae Lee)

1985년 2월 : 경북대학교 전자공학과 졸업(학사)
1987년 2월 : 경북대학교 전자공학과 졸업(석사)
1998년 2월 : 경북대학교 전자공학과 졸업(박사)
1987년 2월~1998년1월 : 국방과학연구소 선임연구원
1998년 3월~2002년2월 : 경운대학교 조교수
2002년 3월~현재 : 동서대학교 컴퓨터정보공학부 부교수
※관심분야 : 암호이론, 네트워크보안, 부채널공격