초음파 센서를 이용한 거리 기반 인증 시스템의 설계 및 분석

(Design and Analysis of an Authentication System based on Distance Estimation using Ultrasonic Sensors)

박 진 오 † 이 문 규 †† 임 철 수 †††
(Jin O Park) (Mun-Kyu Lee) (CheolSu Lim)

요 약 본 논문에서는 거리 확인 및 공유 키 기반의 challenge-response를 통하여 사용자를 인증하는 인증 시스템을 제안한다. 인증장치는 전파와 초음파 신호의 도달시간의 차를 이용하여 사용자가 소유한 인증토큰이 유효 거리 이내에 있는지 확인하는 동시에, 인증장치가 송신한 challenge에 대해 인증토큰이 키를 기반으로 정확한 응답을 보내는지를 확인한다. 본 논문에서는 이와 같은 인증시스템을 실제로 구현하고 인증장치와 인증토큰의 초음파 센서 방향과 위치의 변화에 따른 인증 성공률을 분석하였다. 실험 결과에 따르면 인증장치와 인증토큰의 방향이 크게 어긋나 있지 않은 상황에서는 대부분 100%에 가까운 인증 성공률을 보임을 확인할 수 있었다.

키워드 : 인증, 거리, challenge, nonce, 초음파센서

Abstract We introduce a user authentication system using distance estimation and a simple challenge response protocol based on a pre-established key. Using the time difference of arrival between an RF signal and an ultrasonic signal, an authenticator verifies if a user's authentication token is within its threshold distance, and it also verifies if the token's response to its random challenge is valid. We implement our authentication system and we analyze the success rates for authentication according to the variations in the distances and facing angles between the authenticator and the token. Our experimental results show that the token is authenticated with very high probability in reasonable settings.

Key words : Authentication, distance, challenge, nonce, ultrasonic sensor

1. 서 론

인증시스템은 사용자를 인증하고 시스템의 접근권한을 주는 시스템이다. 컴퓨터와 KIOSK 단말기, 은행단말기(ATM) 등을 사용하는 데 있어 사용자 신원 확인을 위해 전통적으로 사용되는 방법 중 대표적인 것으로 패스워드를 이용한 인증방식이 있는데, 이것은 미리 공유한 패스워드를 확인하여 시스템의, 접근권한을 주는 방식이다. 하지만, 컴퓨터에서는 키보드 해킹의 우려가 있으며, ATM이나 KIOSK에서는 사용자가 패스워드를 입력하는 순간 공격자가 어깨너머로 슬쩍 엿보는 것만으로도 패스워드를 알아내는 'shoulder surfing' 공격이 가능하다[1]. 또한 패스워드를 이용한 인증방식은 사용자가 패스워드를 기억하지 못해 인증을 실패하는 경우가 있다는 단점이 있기 때문에 패스워드 방식 이외에 여러 가지 인증 방식들이 고안된 바 있는데, 일례로 바이오인식(biometrics) 방법은 개인의 고유한 생물학적

· 본 연구는 지식경제부 및 정보통신연구진흥원의 IT핵심기술개발사업의 일환으로 수행하였음[2008-F-045-02. 장애인 및 고령자를 위한 Digital Guardian 기술개발]

† 학생회원 : 인하대학교 컴퓨터정보공학부
mojaick@gmail.com
†† 종신회원 : 인하대학교 컴퓨터정보공학부 교수
mklee@inha.ac.kr
(Corresponding author임)
††† 정 회 원 : 서경대학교 컴퓨터공학과 교수
cslim@skuniv.ac.kr

논문접수 : 2008년 8월 27일
심사완료 : 2008년 12월 14일

특성을 이용하여 신원을 검증하는 방식이다. 이 방식은 키보드 해킹으로 인한 패스워드의 유출이나 기억을 못 함에 따른 불편은 없으나, 개인의 고유한 생물학적 특성은 불변하기 때문에 패스워드를 변경하는 것이 어렵고 일단 패스워드의 정보가 유출된다면 위험성이 매우 커지는 단점이 존재한다[2]. 따라서 사용자가 몸에 지니고 다니면서 시스템으로부터 인증을 받고 접근권한을 얻을 수 있도록 해주는 물리적 토큰을 이용하는 방식 또한 이용되고 있는데, 보통은 메모리 토큰에 하나 이상의 IC를 추가하여 메모리 토큰의 기능을 확장시킨 형태인 스마트 토큰을 쓰는 경우가 많다. 스마트 토큰이 동작하도록 하기 위해서는 스마트 토큰을 컴퓨터나 단말기의 특정 슬롯에 삽입하고 패스워드나 PIN 번호를 입력하여야 하는데[3], 이러한 방식은 사용자로 하여금 많은 불편함을 초래할 수 있다. 따라서 사용자 입장에서 인증을 받을 때 사용이 편리하며 안정성을 보장 받을 수 있는 형태로서 무선 통신을 활용한 인증방식이 제안된 바 있다[4-6]. 그러나 이 방식 또한 무선이라는 특성상 타 인증장치와의 간섭이나 도청, 위조 등의 위험성이 크다는 문제점이 있다.

본 논문에서는 이러한 문제점들을 해결하기 위하여, 서버와 사용자 사이에 미리 공유된 정보 이외에 추가적으로 초음파를 이용한 거리 측정에 기반하여 인증을 수행하는 인증 시스템을 제안한다. 본 논문에서 제안하는 시스템은 서버가 생성한 challenge에 대해 사용자의 토큰이 올바른 응답을 한다고 해도 어느 한계치 이상의 거리에 존재하고 있다면 인증에 실패하는 특성을 부여함으로써, 간섭이나 위조의 위험성을 크게 줄일 수 있다. 본 논문에서는 이러한 인증 시스템의 실용성을 확인하기 위해 버클리 대학에서 설계하고 Cross bow사에서 제작한 Cricket 모트 상에서 RF(Radio Frequency)신호 및 초음파신호를 이용한 인증시스템을 설계 및 구현하였다. 본 논문의 구성은 다음과 같다. 2장에서는 센서간 통신 및 위치인식 기술 및 이에 기반한 인증 방식의 동향을 살펴보고, 3장에서는 제안하는 인증시스템에 대해 설명한다. 4장에서는 설계된 인증 시스템을 구현하여 실험을 수행하고 결과를 분석하며, 5장에서는 결론 및 향후 계획을 기술한다.

2. 관련연구

위치 측정 방식으로 현재 가장 널리 쓰이는 것 중 하나인 GPS(global positioning system) 방식은 많은 응용을 가지고 있으나, 실내용 위치 측정 시스템으로 사용하기에는 정밀도나 신호 수신 문제 등으로 인해 사용이 부적합하다. 때문에 실내용 위치 측정 시스템으로는 적외선, RF를 비롯한 전파, 초음파 등을 이용한 시스템이 가장 일반적으로 사용되고 있다. 적외선을 이용한 시스템의 한 예로 1992년 AT&T 캠브리지 연구소에서 개발한 액티브 배지(Active Badge)가 있는데, 이는 주기적으로 고유의 아이디 정보를 가진 적외선 신호를 송신하는 송신기와 천정에 부착된 수신기로 구성되며, 수신기는 특정한 아이디를 가진 송신기가 현재 범위 이내에 있음을 통해서 송신기의 위치를 결정하는 시스템이다[7]. 그러나 햇빛이나 형광등 등의 간섭이 심하다는 단점과 적외선 신호의 충돌이 일어날 수 있다는 점 때문에 문제를 가지고 있다. 전파를 이용하는 시스템의 예로는 1997년 미국 마이크로소프트 연구소에서 제안된 RADAR(Radio Detection and Ranging)[8]와 1999년 미국 워싱턴 대학에서 제안된 SpotON[9] 등이 있는데, 이러한 종류의 시스템들은 신호 세기를 기반으로 거리를 측정하므로 신호 출력을 조정함으로써 거리를 조작할 수 있다는 단점이 있다. 일례로, 블루투스(BlueTooth)의 경우 신호의 세기를 조절하여 거리를 속이는 공격이 알려진 바 있다[10,11]. 예를 들어 두 시스템 간에 신호 세기를 기반으로 인증하는 경우, 정상적인 신호 수신 범위 바깥에 있는 공격자가 정상 시스템보다 수신 능력이 월등한 고성능 안테나로 미약한 신호를 수신하고 고출력 전송장치로 이 신호를 전달(relay)할 경우 정상적인 시스템과 구분이 어려우므로 중간자공격(man-in-the-middle attack)이 가능하게 된다.

한편, 초음파는 0.1~10M 정도의 거리에서 신호의 도착 시간차를 이용한 측위방식(TODA: Time Difference Of Arrival)을 이용하여 거리를 구할 수 있는데, 초음파의 도착 시간은 물리적으로 조작이 불가능하므로 위조의 위험 없이 거리를 안전하게 측정할 수 있다[5,6,12]. 최근에는 초음파를 거리 측정 뿐 아니라 데이터 전달에 이용하여 안전하게 키를 교환하는 "Integrity region" 기법이 제안된 바 있다[13]. 즉, 사용자가 눈으로 확인할 수 있는 거리(integrity region) 안에 두 개의 시스템을 위치시키고 Diffie-Hellman 키 공유 프로토콜을 수행하는 방식인데, 각 시스템은 키 공유 메시지를 전송한 상대방의 위치를 초음파를 이용하여 파악할 수 있으므로 중간자공격을 사전에 방지할 수 있는 방식이다.

3. 인증시스템 설계

본 논문에서는 초음파를 데이터 전달과 거리 측정의 두 가지 목적으로 동시에 활용하는 [13]의 아이디어를 사용자 인증에 적용하였다. 즉, 두 시스템 간에는 이미 적절한 방법에 의해 키 공유가 완료되어 있다고 가정하고, 이 공유된 키를 기반으로 한 challenge에 대해 상대방이 적절한 응답을 할 수 있는지를 확인하는 것이 목적이다. 본 논문에서는 이러한 challenge-response 프

로토콜을 설계하고 이를 구현하여 성능을 평가하였다. 일반적인 환경에서는 대개 단방향 사용자 인증이 필요한 경우가 많으므로, 본 논문에서는 두 개의 시스템 중 하나는 인증장치(authenticator)로, 나머지 하나는 인증토큰(authentication token)으로 동작하는 상황을 가정한다. 단, 필요에 따라 양방향 인증이 가능하도록 시스템을 변형하는 것도 가능하다.

3.1 인증시스템 요구사항

인증장치와 인증토큰은 서로 공유되어 있는 키를 가지고 있고, 인증장치는 인증할 대상인 인증토큰의 리스트를 가지고 있는 것으로 가정한다. 키 공유를 위해서는 관리자의 직접 설정이나 유선 설정 등 다양한 방식을 이용할 수 있으며, [13]의 무선 키 공유 방식을 이용하는 것도 가능하다. 인증 시에 인증토큰은 인증장치로부터 유효거리 안에 위치하여야 하며, 유효거리를 벗어날 경우 인증이 되지 않아야 한다. 또한, 인증장치는 인증토큰을 무선 통신을 통해서 올바른 인증대상자인지를 판단하여야 하는데, 구체적으로 인증장치는 인증토큰에게 무작위값을 보내고 받은 인증토큰의 응답을 인증장치와 인증토큰간에 공유되어 있는 키를 이용하여 자체적으로 생성한 값과 비교하여 인증대상인지를 판단할 수 있어야 한다.

3.2 인증시스템 설계

그림 1은 위와 같은 요구사항에 근거하여 설계된 인증 프로토콜을 나타낸다. 먼저, 인증장치는 인증토큰으로부터 사용자 ID를 받고서 인증토큰이 인증장치의 리스트에 있는 합법적인 사용자이면 인증과정을 시작한다. 인증장치는 새로운 인증 세션마다 인증토큰에게 새로운 무작위값 C를 생성하여 보내고 응답을 받음으로써 재사용 공격(replay attack)을 피할 수 있다. 인증토큰은 이렇게 무작위로 생성되어 전송된 인증장치의 challenge에 대해 공유키 K 기반의 연산을 통해 적절한 응답 R′을 생성하여야 하며, 인증장치는 인증토큰과 동일한 연산을 수행하여 얻는 결과값 R을 인증토큰으로부터 온 응답 R′과 비교함으로써 인증토큰의 유효성을 판단할 수 있다. 그러나 인증토큰이 R′을 계산 후 바로 인증장치로 이를 전송하고 인증장치가 R과 R′을 직접 비교하게 할 경우 정확한 시간 측정이 어려워지는 문제가 발생하게 된다. 즉, 인증장치는 인증토큰의 거리를 측정하기 위해 응답 R′을 초음파 신호로 전송받고 C의 발신부터 R′의 수신 시점까지의 시차를 측정해야 하는데, R′의 계산은 안전성 보장을 위해 연산 시간이 많이 소모되는 의사난수함수(pseudorandom function, 이하 PRF)를 이용하여야 하므로 측정된 시간 안에 초음파 신호 전송 시간 뿐 아니라 이러한 연산 시간이 오차로 포함되는 문제가 발생한다.

따라서 그림 1의 프로토콜은 R과 R′을 직접 비교하는 것이 아니라 인증장치가 무작위로 생성하고 전송한 nonce N과의 XOR 연산 결과값인 X와 X′을 통해 간접적으로 비교하도록 설계되어 있다. 이는 XOR 연산이 초음파 신호 전송 시간에 비해 소요시간이 거의 무시할 수 있는 정도인 간단한 연산이므로 시간 측정 상의 오차를 최소화할 수 있다는 점에 기반한 것이다.

인증장치는 무작위값 N을 인증토큰으로 보내는 시점 T_R과 X′을 받은 시점 T_U 사이의 시간 차이를 측정하여 이를 기반으로 거리를 계산한다. 이때 N은 초음파가 아닌 RF 채널로 전송되므로 인증장치에서 인증토큰까지 N이 도달하는 시간은 0으로 가정할 수 있다. 위에서 설명한 바와 같이 X′의 생성 시간도 거의 0으로 가정할 수 있으므로, 시간 ($T_U - T_R$)는 X′이 초음파 채널을 통해 전송되는 데 소요된 시간으로 볼 수 있다. 이 시차를 이용하여 계산된 인증토큰의 거리가 유효거리보다 크면 인증토큰은 인증에 실패하게 된다. 만약 유효거리 이내로 계산되면 인증장치는 X와 수신된 X′를 비교하여, 일치하면(X=X′) 인증하고 일치하지 않으면(X≠X′) 인증하지 않는다.

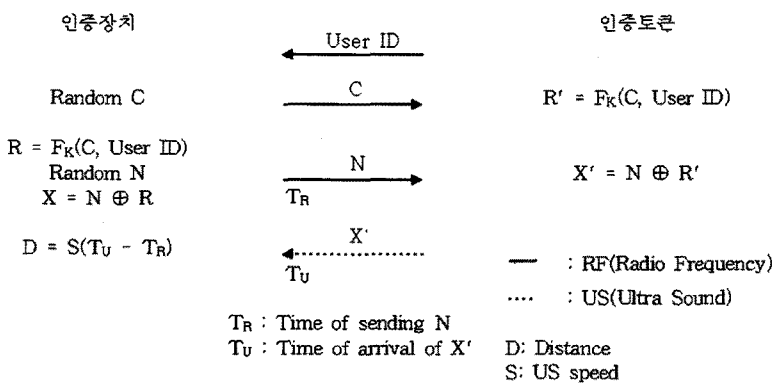

그림 1 인증토큰에 대한 인증과정

무작위 challenge C와 nonce N의 생성, 응답 R 및 R′의 계산을 위해서는 PRF를 이용하게 되는데, 그림 1에서는 이를 F로 표시하였다. 인증장치와 인증토큰이 각각 인증값 R과 R′을 생성하기 위해서는 C와 User ID를 덧붙인 값과 공유키 K를 이용하여 F를 실행하게 되며, C와 N을 생성하기 위해서는 무작위 seed 값을 이용하여 F를 실행하면 된다. PRF에 대해서는 다음 절에서 자세히 설명한다.

3.3 Pseudorandom Function

다양한 국제 표준에서 많은 PRF의 구현들이 있고, 대부분이 해쉬함수를 이용하거나 블록 암호를 이용한다. 본 논문에서는 이 두 종류의 스킴을 구현하고 비교하여 인증시스템에 적합한 PRF를 찾고자 하였다. 이 절에서는 해쉬기반 메시지 인증코드(HMAC, Hash-based Message Authentication Code) 및 블록 암호기반 인증코드(CBC-MAC, Cipher Block Chaining-Message Authentication Code)를 살펴보고, 이들에 대한 비교결과를 제시한다.

먼저, 그림 2는 HMAC의 전 과정을 보여준다. 용어들을 정의하면 다음과 같다.

H : 표준 해쉬함수(예를 들면, MD5, SHA-1 등)

M : HMAC에 들어가는 입력 메시지(내장된 해쉬함수에서 정해진 패딩 포함)

Y_i : M의 i번째 블록, $0 \le i \le L-1$, L : M에 있는 블록 수

b : 블록 내에 있는 비트 수

n : 내장 해쉬함수에 의해 만들어진 해쉬 코드의 길이

K : 비밀키, 만약 키의 길이가 b보다 크면, 그 키는 n비트 키를 생성하기 위한 해쉬함수의 입력이 된다. 권고하는 길이는 n이상이다.

K^+ : b 비트 길이가 되도록 왼쪽을 0으로 채운 K

ipad : 00110110을 b/8 번 반복, opad : 01011100을 b/8 번 반복

HMAC은 다음과 같이 표현된다. ||은 덧붙임의 기호이다.

$HMAC_K(M) = H[(K^+ \oplus opad) \,||\, H[(K^+ \oplus ipad) \,||\, M]]$

다음에, CBC-MAC은 블록 암호를 메시지 인증용으로 활용하는 방법이다. 키 K는 블록 암호의 키로 사용된다. CBC-MAC의 아이디어는 CBC모드로 메시지 M을 암호화하는 것이다. 그림 3은 블록 암호로 AES(Advanced Encryption Standard)를 이용한 CBC-MAC을 구성한 것을 보여준다. 메시지 M은 각 블록 M_1, M_2,…, M_n을 덧붙여 놓은 것이다. 각각의 메시지 블록 M_i는 128bit 크기이다. 마지막 블록 M_n이 128bit 크기가 되지 않는다면 블록 M_n은 10…0으로 부족한 비트만큼 덧붙여진다.

PRF를 구성하기 위해서 본 논문에서는 SHA-1(Secure Hash Algorithm 1)을 이용한 HMAC인 HMAC-SHA1과 AES를 이용한 CBC-MAC인 AES-CBC-MAC을 고려하였고, AVR Studio에서 인증 시스템 테스트 환경인 Cricket mote의 ATMEGA128 마이크로컨트롤러로 설정하여 함수의 실행시간과 메모리 사용을 측정하였다. HMAC-SHA1의 경우 출력이 160 비트이므로 본 논문의 인증 프로토콜에서 challenge C, nonce N, 응답 R, 인증값 X 등은 모두 160 비트가 되며, AES-CBC-MAC을 이용할 경우 위 값들은 128 비트가 된다. 표 1을 보면, HMAC-SHA1과 AES-CBC-MAC을 비교하였을 때 시간과 메모리 사용 측면에서 AES-CBC-MAC이 더 효율적인 것을 확인할 수 있으며, 따라서 본 논문에서는 AES-CBC-MAC을 PRF로 이용하기로 결정하였다.

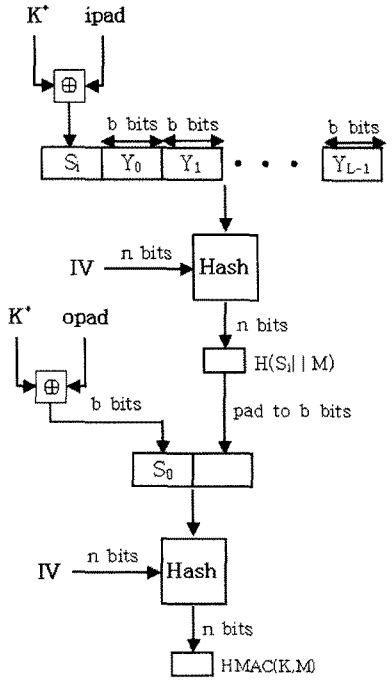

그림 2 HMAC Structure

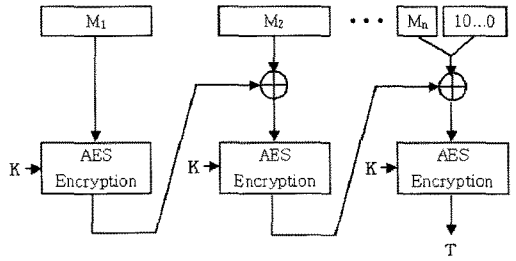

그림 3 AES-CBC-MAC_K(M)

표 1 HMAC과 AES-CBC-MAC의 실행시간 비교와 메모리 사용 측정(메시지 크기는 각각 1블록)

	측정시간(msec)	Program
HMAC-SHA1	46.1	7720 bytes
AES-CBC-MAC	7.3	7110 bytes

4. 실험결과 및 분석

4.1 실험개요

본 논문의 인증시스템 프로토타입은 두 개의 모트(mote)와 하나의 PC로 구성된다. 먼저 인증장치는 첫 번째 모트를 호스트 PC와 유선으로 연결하여 구성하였는데, 이때의 모트는 인증토큰을 인증하고 인증 결과를 호스트 PC로 전송해 주는 역할을 한다. 나머지 하나의 모트는 그 자체로 인증토큰이 된다.

본 논문에서는 인증시스템을 위한 모트로 RF와 초음파 통신이 가능한 UC Berkeley의 Cricket mote(그림 4)를 이용하였다. Cricket 모트는 ATMEGA128 마이크로컨트롤러를 탑재하고 있으며, 7.3728MHz로 동작한다. ATMEGA128은 32개의 8비트 범용레지스터를 가지고 있으며, 128KB In-System Programmable(ISP) 플래시 메모리와 4KB 내부 SRAM을 가지고 있다. Cricket 모트의 초음파 송수신부는 Kobitone 제품으로, 40 KHz로 동작하고 대역폭은 2 KHz이다. RF 송수신부는 CC1000 chip을 이용하고 있다[14-16]. 운영체계는 무선 센서네트워크를 위한 컴포넌트 기반의 Tiny OS를 사용하였다.

거리 측정을 위해서는 초음파의 속도를 설정하여야 하는데, 온도와 습도에 따라 약간의 차이가 있지만 상온 15°C 온도에서의 속도가 약 340m/sec라고 알려져 있으므로 이 값을 이용하였다. 또한, 본 논문에서 측정 대상으로 삼는 거리는 1m 이내의 가까운 거리이므로 cm 단위의 거리측정을 위해서 μs단위의 시간계산이 필요하여, TinyOS의 System컴포넌트를 사용하였다. 인증시스템의 거리계산은 RF신호와 초음파의 도착시간 차이를 이용하기 때문에 프로세서의 명령어 처리 시간을 고려하여 프로그램상에서 명령어 처리가 최소화되는 부분에서 발수신 시간을 측정하였다. 이를 위해서 인증시스템의 시간측정은 Cricket 모트의 초음파 신호를 감지하는 최하단 컴포넌트인 usTransceiver 컴포넌트에서 하였다. Cricket 모트에서 초음파 채널로 데이터를 전송할 때에는 1 cycle이 1bit로 구성된 8개의 cycle 단위로 전송하는데, 이러한 8개의 cycle을 하나의 pulse로 정의하고 있다. 즉, 1 pulse 당 1 바이트를 전송할 수 있다. 1개의 cycle은 25μs에 해당되며, 하나의 cycle 내에 초음파를 감지하면 1로 정의하고 감지하지 못하면 0으로 정의한다.

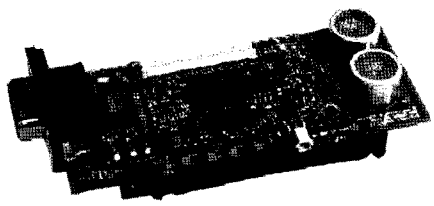

그림 4 Cricket Mote, MCS410CA

한편, 본 논문에서 제안하는 인증시스템은 데이터 전송 시에 초음파, 즉 일종의 소리를 이용하기 때문에 이를 주위 환경에서 자연적으로 발생하는 잡음과 구별하는 것이 필요하다. 이를 위해 초음파 데이터를 보낼시 시작 부분에 0xAA, 0xAA를 인위적으로 추가하여 자연신호와 구별되도록 하였다. 0xAA는 10101010의 이진수로 표현되며 소리가 일정한 시간 간격으로 발생하고 중단되는 것의 규칙적인 반복이기 때문에 자연적으로 발생하는 소리에서 이러한 신호가 연속적으로 발생하는 것은 어렵다. 본 인증시스템에서는 초음파 데이터를 수신시에 0xAA, 0xAA 신호가 연속적으로 감지된 이후 들어오는 신호를 데이터 값으로 사용하였다.

본 논문에서는 위와 같이 설계된 인증시스템 프로토타입 및 인증 프로토콜을 기반으로, 실내에서 센서간 거리측정과 인증값 확인 실험을 수행하였다. 인증장치는 중앙에 위치되었으며, 인증토큰은 인증장치를 바라보는 각도와 거리를 달리하여 배치되었다. 즉, 그림 5와 같이 각도 Θ는 인증토큰이 인증장치의 중심선상에서 얼마나 빗겨난 방향에 있는지를 나타내는 각도이며, 중심 위치가 0°, 왼쪽으로 -45°, -90°, 오른쪽으로 45°, 90°로 설정되었다. 각도 α는 인증토큰이 자체회전한 각도로서, 인증토큰의 중심선이 정확히 인증장치쪽을 바라보고 있을 때 0°로 하고, 왼쪽으로 -45°, -90°, -135°, 오른쪽으로 45°, 90°, 135°로 설정하였다.

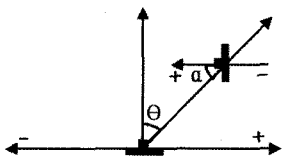

그림 5 인증토큰의 위치 및 각도 설정

4.2 거리와 각도에 따른 인증결과

표 2와 표 3, 그림 6과 그림 7은 거리와 각도 변화에 따른 측정 거리와 인증률 변화를 나타내고 있다. 본 실험에서는 인증장치와 인증토큰 간의 거리를 70cm와 90cm에 놓은 상태로 실험하였으며, 인증기준 거리는

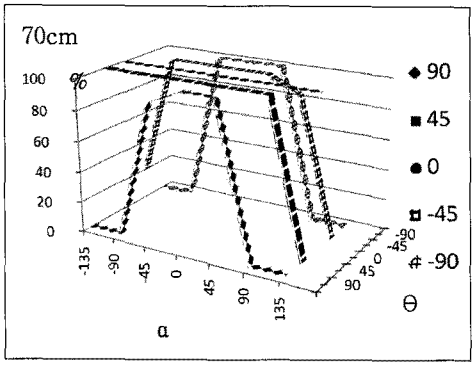

그림 6 70cm에서 각도에 따른 인증률

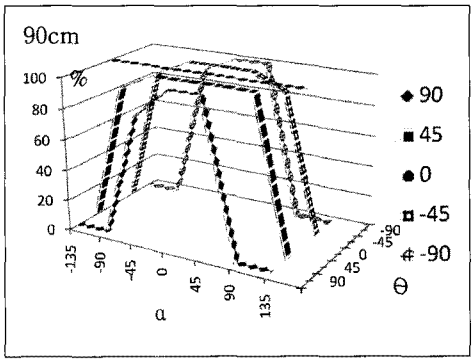

그림 7 90cm에서 각도에 따른 인증률

표 2 70cm에서의 Θ, α값에 따른 인증률

Θ \ α	-135°	-90°	-45°	0°	45°	90°	135°
90°	0	0	90	100	100	0	0
평균거리	-	-	74.7	74.5	74.5	-	-
45°	100	100	100	100	100	100	0
평균거리	77.8	74.3	74.0	72.5	73.1	76.7	-
0°	100	100	100	100	100	80	100
평균거리	75.7	74.2	76.6	71.5	72.7	75.7	78.4
-45°	20	100	100	100	100	90	0
평균거리	81.0	75.6	75.2	72.8	72.5	75.7	-
-90°	0	0	100	100	100	0	0
평균거리	-	-	75.2	73.6	76.7	-	-

표 3 90cm에서의 Θ, α값에 따른 인증률

Θ \ α	-135°	-90°	-45°	0°	45°	90°	135°
90°	0	0	80	100	100	0	0
평균거리	-	-	95.4	92.3	93.8	-	-
45°	0	90	100	100	100	100	0
평균거리	-	91.8	92.6	89.1	92.1	94.9	-
0°	100	100	100	100	100	100	100
평균거리	93.6	92.5	90.6	90.6	92.0	93.3	95.1
-45°	0	90	100	100	100	90	0
평균거리	-	94.3	93.2	90.7	92.5	93.4	-
-90°	0	0	90	100	100	0	0
평균거리	-	-	93.0	94.0	95.3	-	-

100cm로 설정하였다. 즉, 측정된 거리가 100cm 이내이면 거리 테스트를 통과하는 것으로 간주하였다. 인증기준 거리를 100cm로 설정한 것은 일반적으로 사용자와 사용 대상 시스템 간의 거리가 수십cm~100cm 정도이기 때문이다. 인증기준 거리를 지나치게 작게 잡으면 정상적인 사용자가 인증에 실패하는 경우가 생길 수 있으며, 크게 잡으면 이웃한 시스템을 사용하는 사용자와 간섭이 일어나는 문제가 발생하게 된다.

실험 결과 70cm일 때와 90cm일 때 거리에 따른 인증률 차이는 거의 없으나, 각도 Θ, α에 따른 인증률은 Θ값이 ±90°, α값이 ±45°를 넘으면 인증률이 현저하게 낮아졌다. 이는 인증토큰의 초음파 발신 장치가 인증장치의 초음파 센서의 수신 각도의 일정부분을 벗어나면 수신율이 떨어지는 현상 때문에 발생한 것으로 판단된다. 단, Θ와 α값이 ±45° 이내인 정상적인 상황에서는 인식률은 항상 100%임을 확인할 수 있다.

좀 더 구체적으로 실험 결과를 살펴보면, Θ가 0° 일 때에는 α의 각도에 상관없이 수신이 잘 되었고, Θ가 커지면 α의 각도에 따라서 초음파 신호가 미약하여 수신이 잘 되지 않는 경우가 발생하였다. 특히, (Θ, α) = (45°, -135°)와 같은 극단적인 경우에는 70cm에서는 수신이 잘 되었지만, 90cm에서는 수신이 안되어 인증률이 0%가 되었다. 이와 같은 현상은, 인증장치와 인증토큰이 서로 마주보지 않은 각도에서는 인증장치가 인증토큰이 발신한 초음파 신호를 회절된 상태로 수신하여야 하는데 인증토큰이 인증장치로부터 멀어짐에 따라 회절된 초음파 신호 세기가 급격하게 감소하기 때문인 것으로 추정된다.

4.3 안전성 분석

제안된 인증시스템은 거리확인과 challenge-response를 통하여 인증대상을 인증한다. 인증시스템이 RF만의 통신으로 구성되어 거리확인과 challenge-response를 통하여 인증대상을 인증하게 되면 통신신호의 세기 조절로 거리를 속일 수 있으므로[10,11] 안전성을 보장할 수 없는 반면, 초음파 통신은 신호의 세기 조절을 하여 먼 곳에서 신호를 보낸다 하더라도 초음파의 도달시간을 조작할 수는 없으므로 거리를 속일 수 없다. 또한, 제안된 인증시스템은 무작위 값을 전송하고 응답을 하였을 때 상호 간에 공유된 키가 없으면 정확한 인증값을 생성할 수 없으므로 인증대상을 속일 수 없다. 3장에서 고려한 AES-CBC-MAC은 128비트의 안전성을 가지는 방법이므로 키를 모르는 공격자가 무작위로 생성한 응답이 인증과정을 통과할 확률은 2^{-128}, 즉 거의 0이라 할 수 있다.

5. 결론 및 향후 계획

본 논문에서는 인증장치와 인증토큰으로 구성된 초음파 기반의 무선 인증시스템을 설계, 구현하고 인증토큰의 각도와 거리 변화에 따른 인증률의 변화를 분석하였다. 제안한 인증시스템은 초음파로 인증값을 전송함으로써, 신호 세기의 강약 조절에 의해 거리를 속이는 공격을 방지할 수 있다.

한편, 인증토큰을 이용하는 인증 방법에 있어 발생할 수 있는 문제점 중 하나는 인증토큰을 지닌 합법적 사용자와 도난 또는 분실 등으로 인증토큰을 획득하게 된 부정 사용자를 구분할 수 없다는 점이다. 따라서 인증토큰은 사용자가 분실시 바로 인지하고 대처할 수 있는 형태여야 하는데, 예를 들어 휴대전화 내장형이나 시각장애인 및 고령자의 지팡이 내장형 등을 고려할 수 있다. 또한, 무선 자동 인증의 편리함과 안전성을 동시에 보장하기 위해서는 본 시스템이 적용될 수 있는 실제 응용의 범위를 좀 더 명확히 정할 필요가 있는데, 예를 들어 [4]에서와 같이 초기의 인증은 패스워드나 PIN과 같은 다른 방법과 병행하여 이중 인증을 수행하고, 이후 같은 세션 동안에 주기적으로 일어나는 재인증(reauthentication)만을 무선 자동 인증으로 하는 방안을 생각해볼 수 있다.

한 가지 추가로 고려할 사항은 초음파의 특성상 인증 메시지를 송수신하는 장치들 사이에 장애물이 있다면 초음파 신호의 수신률이 떨어져 인증률이 낮아질 가능성이 있다는 점이다. 따라서 향후에는 장애물이 있을시 인증시스템의 인증률 변화를 분석하고 이러한 상황에서 인증률을 높이는 방안의 연구가 필요할 것이다.

참 고 문 헌

[1] Kumar, M. and Garfinkel, T. and Boneh, D. and Winograd, T., "Reducing Shoulder-surfing by Using Gaze-based Password Entry," Proceedings of the 3rd symposium on Usable Privacy and security, ACM International Conference Proceeding Series, Vol.229, pp. 13-19, 2007.

[2] Ratha, N.K. and Connell, J.H. and Bolle, R.M., "Enhancing Security and Privacy in Biometrics-based Authentication Systems," IBM Systems Journal(IBMSJ), Vol.40, No.3, pp. 614-634, 2001.

[3] Griswold, C.W and Hedrick, J.R. United States Patent (NO. 6,629,591): Smart token

[4] Nicholson, A.J and Corner, M.D and Noble, B.D, "Mobile Device Security Using Transient Authentication," IEEE Transactions on Mobile Computing, Vol.5, No.11, pp. 149-161, 2006.

[5] Hightower, J. and Borriello, G., "Location Systems for Ubiquitous Computing," IEEE Computer, Vol.34, No.8, pp. 57-66, Aug. 2001.

[6] Priyantha, N.B. and Chakraborty, A. and Balakrishnan, H., "The Cricket Location-Support System," Proceedings of the 6th annual international conference on Mobile Computing and Networking (MOBICOM), pp. 32-43, 2000.

[7] Want, R. and Hopper, A. and Falcao, V. and Gibbons, J., "The Active Badge Location System," ACM Transactions on Information Systems(TOIS), Vol.10, Issue. 1, pp. 91-102, 1992.

[8] Bahl, P. and Padmanabhan, V.N, "RADAR: An In-Building RF-based User Location and Tracking System," Proceedings of the 9th annual joint conference of the IEEE Computer and Communication Societies, INFOCOM 2000, Vol.2, pp. 775-784, 2000.

[9] Hightower, J and Want, R. and Borriello, G., "SpotON: An Indoor 3D Location Sensing Technology Based on RF Signal Strength," UW CSE Technical Report #2000-02-02, 2000.

[10] Jakobsson, M and Wetzel, S., "Security Weaknesses in Bluetooth," CT-RSA 2001, LNCS 2020, pp. 176-191, 2001.

[11] Kügler, D., "Man in the Middle Attacks on Bluetooth," Proceedings of Financial Cryptography, LNCS 2742, pp. 149-161, 2003.

[12] Zhu, L. and Zhu, J., "A New Model and its Performance for TDOA Estimation," IEEE Vehicular Technology Conference 2001, Vol.4, pp. 2750-2753, 2001.

[13] Capkun, S. and Cagalj, M., "Integrity Regions: Authentication Through Presence in Wireless Networks," Proceeding of the 5th ACM workshop on Wireless Security (WiSe), pp. 1-10, 2006.

[14] MCS410 Cricket data sheet, Cricket wireless location system datasheet, Crossbow, http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MCS410_Cricket_Datasheet.pdf

[15] Ultrasound transmitter 255-400ST12 and ultrasound receiver 255-400SR12 datasheet, Mouser Electronics, http://www.mouser.com/catalog/specsheets/KT-400050.pdf

[16] CC1000 data sheet, Chipcon CC1000 single chip transceiver, Texas Instruments, http://focus.ti.com/lit/ug/swru058/swru058.pdf

박 진 오

2007년 인하대학교 컴퓨터공학과 학사

2007년~현재 인하대학교 컴퓨터정보공학부 석사과정. 관심분야는 정보보호, 암호학

이 문 규

1996년 서울대학교 컴퓨터공학과 학사 1998년 서울대학교 컴퓨터공학과 석사 2003년 서울대학교 전기컴퓨터공학부 박사. 2003년~2005년 한국전자통신연구원 (선임연구원). 2005년 3월~현재 인하대학교 컴퓨터정보공학부(조교수). 관심분야는 정보보호, 암호학, 컴퓨터이론

임 철 수

1985년 서울대학교 계산통계학과 학사 1988년 (미)인디애나주립대 컴퓨터과학과 석사. 1995년 서강대학교 전자계산학과 박사. 1988년~1997년 (주)아시아나항공, (주)신세기통신 근무. 1997년 3월~현재 서경대학교 컴퓨터공학과 교수, 산학협력단장. 관심분야는 차세대컴퓨팅, 멀티미디어시스템