소닉 커뮤니케이션 기반 사용자 식별 방법 연구

임윤규, 서재학, 김대천, 박예찬, 염상길, 추현승
성균관대학교 정보통신대학
e-mail: oewi, forget1026, daecheon, dpcks001, sanggil12, choo@skku.ecu

User Identification Method based on Sonic Communication

Yoon-gyu Lim, Jaehak Seo, Daecheon Kim, Yechan Park, Sanggil Yeom, Hyunseung Choo
Dept of Computer Engineering, Sungkyunkwan University

요 약

최근 스마트기기 사용량이 증가함에 따라 NFC나 Bluetooth 등 다양한 근거리 통신 서비스가 제공되고 있다. 그러나 이들 통신방식은 별도의 통신 모듈을 필요로 하는 단점이 있다. 이러한 단점을 해결하기 위해 비가청주파수 대역을 이용한 통신이 연구되고 있다. 비가청주파수 대역은 18kHz~22kHz 사이의 사람에게 들리지 않는 주파수 대역으로 마이크와 스피커만 있으면 비가청주파수 통신이 가능하다. 기존 연구는 특정 사용자를 식별하여 데이터를 보안상 안전하게 전송하는 방식이 없다. 본 논문에서는 통신에 사용되는 두 기기가 본 논문에서 제안한 공유키를 활용하여 3단계의 과정을 거쳐 사용자를 식별하는 방법을 제안한다. 또한 식별 과정에서 만들어진 값은 메시지를 암호화하는데 사용되어 보안을 강화한다. 이 식별 방법은 비가청주파수 통신을 IoT 등 다양한 분야에 활용하는데 사용할 수 있다.

1. 서론

최근 스마트기기가 널리 사용되고 있고 다양한 근거리 통신 서비스가 제공되고 있다. 현재 널리 사용 중인 근거리 통신 종류는 NFC(Near Field Communication), Bluetooth, IR(Infrared) 통신 및 RF(Radio Frequency) 통신이다. 그러나 위의 통신방식은 별도의 통신 모듈이 필요하고 이는 기기 생산 시 추가비용을 요구한다[1]. 이러한 단점을 해결하기 위해 대부분 스마트기기에 스피커와 마이크가 내장된 점을 착안하여, 스피커와 마이크만으로 데이터의 송수신이 가능한 비가청주파수 통신이 연구되고 있다[2][3]. 비가청주파수 통신은 사람 대다수가 듣지 못하는 18kHz~22kHz 사이의 주파수 대역을 사용하며, Chirp Binary orthogonal keying 방식을 사용한다면, 97%의 통신 성공률로 25m 거리까지 초당 16 bits의 데이터를 전송할 수 있다[4]. 하지만 기존 비가청주파수 통신 연구는 특정 사용자를 식별하여 데이터를 보안상 안전하게 전송하는 방식을 규정하고 있지 않다.

본 논문에서는 비가청주파수 통신을 이용하는 기기들이 사용자를 식별하고 안전하게 데이터를 전송하는 방법을 제안한다. 사용자는 자신이 가지고 다니는 스마트폰 등의 기기와 자신을 식별할 필요가 있는 기기에(ex. 도어락)서 128 bits 이상의 공용키를 넣는다. 사용자는 버튼을 통해 식별을 요청할 수 있다. 이때 두 기기는 32 bits의 임의로 값을 생성하고 공용키와 조합하여 비밀키를 만든다. 임의로 만들어진 값과 비밀키는 3단계의 식별단계를 거친다. 이 단계를 통해 서로의 공용키가 같다면 식별이 성공적으로 마무리 되고 공용키가 다르다면 식별은 실패하게 된다.

2. 관련연구

논문 [5]는 비가청주파수 대역인 18kHz ~ 23kHz 중 20kHz~23kHz 대역에서 데이터를 전송한다. 데이터 전송방법은 송신전력의 조정을 통해서 소리가 나지 않는 상태와 높은 주파수 상태를 증폭시켜 bit 데이터를 전송한다. 수신자는 A/D컨버터를 통해서 수신 받고 필터를 통해서 시작점과 끝나는 점을 구분한다. 그 후 normalize를 통해서 비트 데이터를 검출하여 출력한다. 단, 위의 방법을 사용하게 되는 경우 전송거리가 80cm ±10으로 제한되어 있고 데이터 전송 중 송신자 또는 수신자가 장비를 움직일 경우 전송이 중단 되거나 데이터를 받지 못하는 단점이 존재한다.

논문 [6]은 공연 중에 사용할 수 있는 비가청주파수 통신을 설명한다. 공연자와 관람객 사이에서 공연에 관한 정보가 들어 있는 웹 사이트 주소를 전송하기 위한 새로운 방식을 제안한다. 무대에서 공연이 진행되다가 관객과의 상호작용을 위해서 공연을 하는 도중에 무대 스피커에서 음향이 나올 뿐만 아니라 공연 데이터가 포함된 비가청주파수도 나온다. 그리고 이것을 휴대용 디바이스의 마이크가 인식을 해서 비가청주파수에 담겨진 데이터를 해석해서 해당 웹사이트로 접속하게 해준다.

이와 같은 공연자와 관람자의 상호작용을 통해서 공연자는 좀 더 쉽게 자신의 공연에 대한 이해를 도울 수 있다. 그러나 고유의 인증방식이 없어서 데이터를 1 대 1 전송이 아닌 1 대 다수 전송 형태로 만들어서 특정인을 대상으로 전송을 할 수 없다. 또한 데이터에 대한 보안이 되지 않아서 해킹의 위험성이 있다.

3. 제안 아이디어

3.1. 사용자 식별 3단계 구성

사용자 식별 과정은 그림1에서 볼 수 있듯이 크게 3단계로 이루어져 있다. 식별 과정에서 사용되는 값은 기기A가 생성한 임의의 값 RA, 기기B가 생성한 임의의 값 RB, 기기A가 RA와 공유키를 조합하여 생성한 값 KA, 기기B가 RB와 공유키를 조합하여 생성한 값 KB, 기기A가 RB와 공유키를 조합하여 생성한 값 CA, 기기B가 RA와 공유키를 조합하여 생성한 값 CB이다. 다음 시나리오는 사용자가 기기A를 이용하여 기기B에게 식별을 요청하는 상황이며, 같은 공유키가 두 기기에 미리 넣어져 있는 상황을 가정한다.

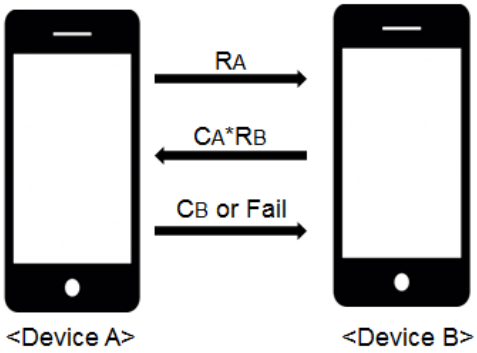

그림 1. 사용자 식별의 3단계

3.2. 사용자 식별 방법

첫째, 사용자가 기기A를 이용하여 식별을 요청한 경우 기기A는 32bits의 임의의 값 RA를 생성한 후 기기B로 전송한다. 그 후 RA와 공유키를 조합하여 32 bits의 비밀키 KA를 생성한다. 비밀키를 생성하는 과정은 Rijndael key schedule[7] 같은 키 생성 방식을 응용할 수 있다.

둘째, 기기B는 상시 비가청주파수 대역 통신을 대기하고 있는 상태이다. 기기B는 기기 A로부터 RA를 전송 받으면 RA와 자신의 공유키를 조합하여 32 bits의 CA를 생성한다. 기기B는 기기A와 마찬가지로 32 bits의 임의의 값 RB를 생성하고 CA와 같이 전송한다. 그 후 RB와 공유키를 조합하여 32 bits의 비밀키 KB를 생성한다.

셋째, 기기A는 기기B로부터 CA*RB를 전송받는다. 두 기기가 같은 공유키를 공유하고 있는 상태에서 같은 임의의 값으로 조합하였다면 KA와 CA는 서로 같다. 만약 이 값이 다르면 기기A는 기기B로 fail message를 전송한다. 값이 같은 경우 기기A는 RB와 자신의 공유키를 조합하여 32 bits의 CB를 생성한다. 성공적으로 CB를 생성한 기기A는 기기B로 데이터 전송을 시작한다. 이 때 전송하는 데이터는 CB와 32bit block단위로 XOR 연산을 통해 암호화 과정을 거친다. 모든 데이터를 전송했다면 기기A는 CB를 전송한다. 기기B는 기기A로부터 전송받은 데이터를 XOR 연산을 통해 해독과정을 거친다. 일정시간동안 메시지를 받지 못하거나 XOR 연산 결과 값이 0일 경우 통신을 종료한다.

4. 결론 및 향후 연구

본 논문에서는 18kHz~22kHz 사이의 비가청주파수 대역 통신을 이용하여 사용자를 식별하는 방안에 대해 제안하였다. 각 기기는 2^32개의 키를 생성하여 식별하고 데이터 전송 시 XOR 연산을 통해 암호화된 메시지를 전달한다. 이 방식을 통해 식별과 동시에 공격에 안전한 통신을 할 수 있다. 향후 연구로 적은 주파수 대역으로 다량의 데이터를 안정적으로 전송할 수 있는 비가청주파수 통신 방식을 고안한다. 또한 본 논문에서 제안한 방법을 구체적으로 적용한 시스템을 개발 및 테스트하고 나아가 홈 IoT에 적용할 수 있는 방법을 고안한다.

ACKNOWLEDGEMENT

이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2010-0020210).

참고문헌

[1] D Luke, "Inaudible sound as a covert channel in mobile devices," 8th USENIX Workshop on Offensive Technologies (WOOT 14). 2014.

[2] G. Bang, M. C, and I. K, "Data communication method based on inaudible sound at near field," ICACT, 2016.

[3] S. Park, Y. Do, J. Park, D. S. Kim, and H. Choo, "Inaudible Dual Tone Data transmission for home appliancesm," 2014 IEEE Fourth International Conference on Consumer Electronics Berlin (ICCE-Berlin), IEEE, 2014.

[4] H. Lee, T. H. Kim, J. W. Choi, and S. Choi, "Chirp Signal-Based Aerial Acoustic Communication for Smart Devices," International conference INFOCOM 2015, 2014.

[5] Arentz, W. Archer, and U, Bandara, "Near ultrasonic directional data transfer for modern smartphones," Proceedings of the 13th international conference on Ubiquitous computing, ACM, 2011.

[6] J. Jeon, C. Chae, E. J. Lee, and W. S. Yeo, "TAPIR Sound Tag: An Enhanced Sonic Communication Framework for Audience Participatory Performance," NIME, 2014.

[7] J. Daemen, and V. Rijmen, "Specification for the Advanced Encryption Standard (AES)," 2002.