디바이스 상 측정되는 Wi-Fi 신호강도를 이용한 디바이스 DNA 생성 제안

홍은기*, 김제인*, 오미경**, 강유성**, 서승현*
*한양대학교 전자공학과
**한국전자통신연구원
e-mail: heg0403@gmail.com

Device DNA Development Using Wi-Fi RSSI Measured on Device

Eungi Hong*, Jane Kim*, Mi-Kyoung Oh**, Yousung Kang**, Seung-Hyen Seo*
*Dept. of Electronic Engineering, Hanyang University
**Electronics and Telecommunications Research Institute

요 약

IoT 기술은 대규모의 IoT 네트워크가 디바이스들로부터 수집되는 데이터들을 이용해 서비스를 제공하는 기술이다. 이러한 IoT 네트워크는 디바이스 상호 간 연결되어 있어 네트워크에 포함 되어있는 하나의 디바이스가 가지고 있는 취약점을 이용하면 IoT 네트워크 전체가 공격받을 수 있다. 따라서, IoT 디바이스는 사양의 높고 낮음에 관계없이 전체 네트워크의 보안 수준에 맞추어 보안 강도를 보장받아야 한다. 본 논문에서는 근래에 새롭게 제시된 “디바이스 DNA”를 이용하여 새로운 디바이스 인증 기술을 개발하는 것에 초점을 맞추어, “디바이스 DNA”로 디바이스 상에서 측정되는 Wi-Fi 신호강도(RSSI; Received Signal Strength Indication)를 사용할 수 있는 가능성을 보인다.

1. 서론

IoT 는 현재 홈, 가전, 의료, 교통 등 실제생활 영역에 적용되면서 생활의 효율성 및 편의성을 증대하고 있다. 그러나 IoT 디바이스들의 접근 통제나 인증 기술의 부재로 인해 카메라가 탑재된 디바이스를 이용한 사생활 침해부터 자율형 차량의 적합하지 않은 사용자에 의한 엔진 통제까지 다양한 보안 위험에 노출되어 있다. 또한 IoT 네트워크는 디바이스 상호 간에 연결되어 있어 취약점을 가진 한 디바이스가 공격을 받으면 네트워크에 포함되어 있는 다른 디바이스들 또한 공격받기 쉬워진다. 따라서 IoT 디바이스들은 전력이나, 메모리, CPU 등의 성능격차에 관계없이 IoT 디바이스 간 인증이나 통신 보안 기술들에 대한 연구가 필요하다. 이러한 디바이스 간 인증을 위해 최근 “디바이스 DNA”라는 개념이 새롭게 등장하였다. “디바이스 DNA”는 생체인식에 이용되는 사람의 생체 데이터와 같이 디바이스에서도 개별적으로 하드웨어적 특성을 반영하는 특정 정보를 추출할 수 있고 그 정보가 불변성과 고유성을 충족하는 데이터를 말한다[1]. 무인 환경에서 운영되고 있는 IoT 디바이스는 사용자가 게이트웨이를 통한 인증을 하는 방식은 적합하지 않다. 이 환경에 맞는 보안솔루션에 구축하는데 디바이스가 자체적으로 고유하게 얻을 수 있는 데이터인 “디바이스 DNA”를 사용한다면, 안전성을 보장받는 보안 솔루션을 구축할 수 있을 것이다. PUF(Physically Unclonable Function)가 대표적인 “디바이스 DNA”로 제안되었지만, 이는 디바이스마다 PUF 칩을 장착해야 하는 한계가 있다. 또한 무인 환경에서 운용되고 있는 IoT 디바이스는 디바이스의 탈취 등 물리적인 공격을 받았을 때 무방비하다. 따라서 디바이스가 주변 환경에 상호작용하여 얻을 수 있는 데이터를 “디바이스 DNA”로 이용하여 보안 솔루션을 구축한다면, 사용자의 개입 없이 인증이 가능하고, 고정된 위치에서 운용하는 IoT 디바이스의 탈취되었을 때 동작을 불가능하게 하는 등의 대응이 가능할 것이다. 본 논문에서는 디바이스가 무선 네트워크 인프라(Infrastructure)로서 구축된 AP 의 신호강도를 이용하여 얻을 수 있는 Wi-Fi 신호강도(RSSI; Received Signal Strength Indication)를 분석하여 유일성과 불변성을 갖추고 있는지 확인하고, 이를 “디바이스 DNA”로서 사용할 수 있는 가능성을 보인다.

2. Wi-Fi 를 이용한 디바이스 DNA 구성 제안

Wi-Fi 의 신호는 AP 의 케이블과 커넥터에 의해 감소할 수 있고, 성능이 좋은 안테나(high-gain antenna)를 사용하면 신호 강도의 크기 또한 커진다. 또한 AP 로부터 신호가 송출될 때 주파수와 거리에 따라 강도가 낮아지며, 장애물에 반사 혹은 굴절되기도 한다. 이에 따라 특정 환경에 고정 되어있는 IoT 디바이스가 주변 AP 의 Wi-Fi 신호를 측정하면 다른 위치의 기기는 이와 같은 신호를 측정할 수 없다. 이를 이용하여 IoT 디바이스 간에 효과적인 비밀 키를 생성(Key

establishment)하거나 인증하는 방안에 대해 활발한 연구가 진행되고 있다. Wi-Fi 의 신호를 이용한 방식들은 대표적으로 신호강도와 채널상태 정보(CSI; Channer State Information)를 사용한다.

● 신호강도 RSSI

신호강도 RSSI 는 잡음이 포함된 무선 신호 강도에 대한 일반적인 명칭이다. Wi-Fi 신호강도는 거리가 증가하면 감소하는 특징이 있어, Wi-Fi fingerprint 를 이용한 위치파악(Localization)에 많이 사용된다. 권혁찬은 2016 년에 Wi-Fi 신호를 이용해 위치를 특정하는 Wi-Fi fingerprint 를 이용해 자율형 차량에 대한 정당하지 않은 디바이스가 접근하는 것을 방지하는 방식을 제안하였다[5]. 또한 Zi-Li 는 2018 년에 Wi-Fi 거리에 따라 신호강도가 변하는 것을 이용하여 같은 움직임을 보이는 두 기기가 유사한 파장의 변화를 측정해 비밀키를 생성하는 방안을 제안하였다[3].

● 채널상태 정보 CSI

채널상태 정보 CSI 는 위치에 기반한 고유한 채널의 측정 값이다. RSS 와 비교해 정보를 직교성이 있는 부반송파(Sub-carrier)를 포함하여 보내기 때문에 더 많은 데이터를 포함하고 있다. Wei Xi 는 2016 년에 이 채널 상태 정보의 위치에 기반한 동일함을 이용하여 하나의 디바이스가 키를 결정한 후 물리적으로 근접한 거리에 있는 장치들이 키를 합의할 수 있는 TDS(The Dancing Signals) 프로토콜을 제안하였다[2]. Syed W. Shs 는 2018 년에 사용자가 키를 입력할 때 동작하는 패턴에 따라 채널상태 정보가 변하는 것에 따라 정당한 사용자를 인증을 하는 것을 제안했다[4].

이 밖에도 현재 Wi-Fi 의 무선 네트워크 인프라(Infrastructure)가 널리 구축되어 있는 장점과, IoT 디바이스들이 이러한 네트워크에 접속할 수 있는 특징으로 Wi-Fi 의 신호를 이용하여 보안성을 보장받는 방식에 대한 연구들이 활발히 진행 중이다. “디바이스 DNA”로의 활용 가능성을 평가해 보면, 채널상태 정보는 위치에 기반한 데이터이기 때문에 다른 기기여도 매우 근접한(약 6cm)에 있어도 유사한 데이터를 생성하기 때문에 고유성을 충족시키지 못한다. 따라서 본 논문에서는 RSSI 에 초점을 맞추어 “디바이스 DNA” 생성해 각각의 AP 가 갖고 있는 공개된 고유의 데이터(MAC 주소, SSID 등)을 결합하여 Hash 화하여 Digital Fingerprint 를 구성하는 방안을 제안한다.

3. 디바이스 DNA 의 요구조건에 따른 Wi-Fi 신호강도 분석

본 연구에서는 Wi-Fi 신호강도 데이터의 불변성과 고유성을 평가하여 “디바이스 DNA”로 이용할 수 있는 가능성을 보기 위해 실험을 진행하였다.

● 불변성

데이터의 변하지 않는 성질, 디바이스에서 생성할 수 있는 값으로 어느 상황에도 변하지 않아야 인증 솔루션의 유효성이 높아진다.

● 고유성

데이터의 고유한 성질, 특정 디바이스가 다른 디바이스는 생성하지 못하는 값을 생성할 수 있어야 인증 솔루션의 부인방지가 가능하다.

구성한 실험 환경은 아래 그림 1 과 같으며, 라즈베리파이를 각 장소에 배치해 실험을 진행했다. 건물 내에 위치한 AP 가 다수 있어서 한 장소에서 기기가 수신하는 Wi-Fi 신호가 -75dB 이상으로 측정되는 AP 또한 10 개 이상이었다. 따라서 측정되는 데이터 중 유의미한 크기로 균일하게 측정되는 것을 토대로 분석하였다.

그림 1. 실험 환경

다음의 그림 2 은 특정한 장소 Place 1 에서 디바이스#1(라즈베리파이)이 1000 회 연속적으로 측정한 Wi-Fi 신호강도이다. Wi-Fi 신호강도는 파장의 진폭이 있고, 일정한 크기를 보이지 않는다. 하지만 한 위치에서 측정하게 되면 진폭에 차이는 있지만 크기의 수준이 유지된다는 것을 확인 할 수 있다. 따라서 데이터 그대로 이용하기에는 불변성과 고유성이 있다고 보기 어려웠다. 따라서 디바이스에서 추출해 낸 데이터에 적절한 가공이 필요했으며, 간단한 결과를 위해 100 회씩 평균을 내어 비교하였다.

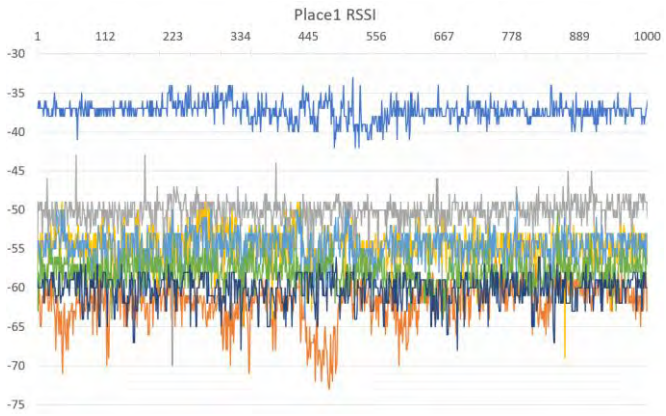

그림 2. Place1 에서 1000 회 연속적으로 측정된 Wi-Fi 신호강도

3.1 불변성 판단

"디바이스 DNA"로 사용하기 위해선 데이터가 불변성을 갖추고 있어야 한다. 그를 위해선 특정한 디바이스가 같은 위치에서는 항상 같은 데이터를 추출할 수 있어야 하며, 이를 확인하기 위해 같은 장소에서 시간이 흐른 뒤에도 기존에 측정했던 결과와 같은 결과를 얻을 수 있는지에 대한 실험을 진행했다. 그림 3 은 그림 2 와 같이 디바이스#1 이 Place 1 에서 측정된 신호강도를 100 회 단위로 평균을 그래프화 한 것과 시간이 흐른 뒤 같은 조건에서 같은 기기로 측정한 것을 그래프화 한 것에 대한 비교이다. 비교를 확인해보면 위치가 일정하면 측정되는 AP 별 Wi-Fi 신호강도가 ±3dB 이내로 일정하다는 것을 확인할 수 있다. 이를 토대로 불변성을 완전하게 갖추고 있지는 않지만 데이터의 가공을 통해 일정하게 맞출 수 있다면 충분한 불변성을 갖출 수 있을 것으로 보인다.

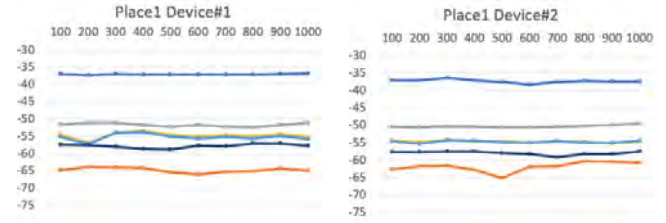

그림 3. 시간에 따른 신호강도 비교 실험

3.2 고유성 판단

"디바이스 DNA"의 고유성을 판단하기 위해 본 연구에서는 다른 위치에서 같은 기기가 같은 값을 생성할 수 없는지에 대한 실험과 같은 위치에서 다른 기기가 같은 값을 생성할 수 없는지에 대한 실험을 진행했다. 다음의 그림 4 는 디바이스#1 이 Place 1 에서 측정한 신호강도와 같은 디바이스가 Place 2 에서 측정한 신호강도에 대한 비교이며, 그림 5 는 디바이스#1 이 Place 3 에서 측정한 신호강도와 디바이스#2(라즈베리파이)가 같은 장소에서 측정한 신호강도에 대한 비교이다. 실험 결과를 보면 같은 기기와 같은 장소가 아니라면 AP 별 Wi-Fi 신호강도의 유사성이 없어진다는 것을 확인할 수 있으며, 이를 토대로 고유성을 갖추고 있다고 보인다.

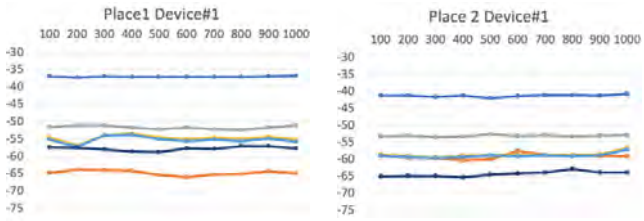

그림 4. 장소별 신호강도 비교 실험

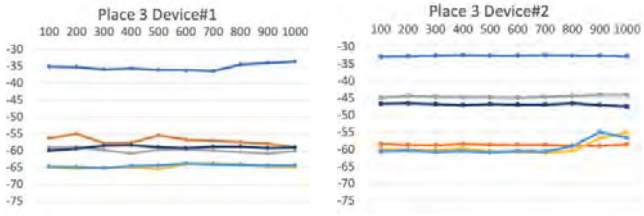

그림 5. 기기별 신호강도 비교 실험

실험 결과에 비추어 디바이스는 Wi-Fi 신호 강도를 일정하게 측정하지만 디바이스 마다 동일하지 않게 측정해 낸다는 것을 알 수 있다. 이는 "디바이스 DNA"의 고유성을 충족시키는 것을 뜻하며, 신호강도 데이터의 가공을 통해 불변성을 개선하여 "디바이스 DNA"로 사용될 수 있다.

4. 결론 및 향후 연구

현재 스마트 디바이스의 보안 솔루션으로 생체 인식이 널리 사용되고 있다. 그러나 무인 환경에서 운용되는 IoT 디바이스들은 이러한 생체 인식 기술을 보안 솔루션에 적용하기 어려워 디바이스가 디바이스의 환경과 상호작용하여 잡음 데이터를 생성해내는 "디바이스 DNA"를 추출하는 것이 중요하다. 본 논문에서는 현대 사회에 흔하게 사용하고 있는 무선 네트워크의 핵심인 Wi-Fi 의 신호강도를 이용하여 디바이스 DNA 를 생성할 수 있는 가능성을 보인다. 현재까지 Wi-Fi 의 신호를 이용한 보안 솔루션들은 여러 디바이스가 공유하는 키를 생성하거나 합의할 때, 같은 시점에 동시에 측정해야 되고, Wi-Fi 신호강도를 수신하는 소자의 상태에 따라서 측정되는 파장이 달라질 수 있다는 한계가 있다. 따라서 향후에는 3 장에서 보인 디바이스가 정해진 위치에서 신호강도의 수준이 유지된다는 점을 이용하여 "디바이스 DNA"화 하기 위한 데이터 가공방식을 분석 및 연구할 예정이며, 이렇게 생성된 "디바이스 DNA"를 이용한 보안 솔루션 및 프로토콜을 개발할 예정이다.

참고문헌

[1] 최두호, 강유성, 오미경, 이상재, 김태성, “IoT 보안을 위한 디바이스 DNA 개념,” 정보보호학술지, Vol.28, No.5, pp 15-19, 2018

[2] Wei Xi, Chen Qian, Jinsong Han, Kun Zhao, Sheng Zhong, Xiang-Yang Li, Jizhong Zhao, “Instant and Robust Authentication and Key Agreement among Mobile Devices,”’16 Proceedings of the 2016 ACM SIGSAC conference on CCS, pp 161-627, Oct. 2016

[3] Zi Li, Qingqi Pei, Ian Markwood, Yao Liu, Haojin Zhu, “Secret Key Establishment via RSS Trajectory matching Between Wearable Devices,” IEEE Transactions on Information Forensics and Security, Vol.13, No. 3, pp 802-817, Mar. 2018

[4] Syed W. Shah, Salil S. Kanhere, “Wi-Access: Second Factor User Authentication leveraging WiFi Signals,” 2018 IEEE International Conference on Pervasive Computing and Communications Workshops, Mar. 2018

[5] Hyeokchan Kwon, Sokjoon Lee, Byung-ho Chung “Wi-Fi Fingerprint-based Approach to Securing the Connected Vehicle Against Wireless Attack,” Netcom, NCS, WiMoNe, GRAPH-HOC, SPM, CSEIT – 2016, pp 211-217, 2016