JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 26, No. 5: 793~801, May. 2022

NBAS: NFT를 활용한 블루투스 장치 인증시스템

황성욱[1] · 손성무[1] · 정성욱[2*]

NBAS: NFT-based Bluetooth Device Authentication System

Seong-Uk Hwang[1] · Sung-Moo Son[1] · Sung-Wook Chung[2*]

[1]Student, Department of Computer Engineering, Changwon National University, Changwon, 51140 Korea
[2*]Associate Professor, Department of Computer Engineering, Changwon National University, Changwon, 51140 Korea

요 약

블루투스 이어폰과 같은 대부분의 블루투스 장치는 무선이라는 편리성으로 다양하게 사용되지만 소형 무선기기라는 특성으로 자주 분실되는 단점이 있다. 그러나 대부분의 블루투스 장치에서는 합법적인 소유자에 대한 인증 기능 제공이 미흡하며, 분실된 블루투스 장치를 습득한 제 3자는 해당 기기를 손쉽게 자신의 스마트기기 등에 연결하여 사용할 수 있다. 본 논문에서는 분실이 잦은 블루투스 장치에서 NFT를 이용하여 합법적인 소유자를 인증하는 NBAS(NFT-based Bluetooth Device Authentication System)에 대해서 제안하였다. NBAS는 탈중앙화된 네트워크인 이더리움 블록체인을 활용하여 이더리움상에 디지털 지갑을 생성하고, 디지털 지갑에 블루투스 장치의 MAC 주소를 이용하여 NFT를 생성하고 보관한다. 지갑의 소유자는 개인키를 사용하여 NFT의 소유를 증명함으로써 블루투스 장치의 합법적인 소유자임을 인증하게 된다. NBAS는 평균 10.25sec의 초기 페어링 시간을 보였으며 재연결 시간은 0.007sec로 기존 방식과 비슷하며, 미승인 사용자에 대한 페어링 거절 시간은 평균 1.58sec로 측정되었다. 따라서 제안하는 NBAS는 미승인된 블루투스 장치의 연결을 방지하여 기존의 보안성이 약한 블루투스 인증 방식을 효과적으로 개선함을 보여준다.

ABSTRACT

Most Bluetooth devices are commonly used in various ways these days, but they can be often lost due to small-size devices. However, most Bluetooth protocol do not provide authentication functions to legitimate owners, and thus someone who obtains the lost Bluetooth device can easily connect to their smart devices to use it. In this paper, we propose NBAS can authenticates legitimate owners using NFT on lossy Bluetooth devices.NBAS generates a digital wallet on the blockchain using the decentralized network Ethereum blockchain and facilitating the MAC address of the Bluetooth device in the digital wallet. The owner of the wallet uses a private key to certify the Bluetooth device using NFT. The initial pairing time of NBAS was 10.25 sec, but the reconnection time was 0.007 sec similar to the conventional method, and the pairing rejection time for unapproved users was 1.58 sec on average. Therefore, the proposed NBAS effectively shows the device authentication over the conventional Bluetooth.

키워드 : NBAS, NFT, 인증시스템, 블루투스 장치, IoT

Keywords : NBAS, NFT, Authentication, Bluetooth, IoT

Received 12 April 2022, **Revised** 16 April 2022, **Accepted** 19 April 2022

*** Corresponding Author** Sung-Wook Chung(E-mail: swchung@changwon.ac.kr, Tel: +82-55-213-3819)
Associate Professor, Department of Computer Engineering, Changwon National University, Changwon, 51140 Korea

Open Access http://doi.org/10.6109/jkiice.2022.26.5.793 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

근거리 무선통신기술인 블루투스는 전력 효율이 뛰어나고 고품질 데이터를 지속적으로 전송하는데 최적화된 통신 기술이다. 오늘날 블루투스는 노트북, 휴대폰, 이어폰, 마우스, 키보드, 헬스기기 등의 다양한 휴대기기 분야에서 광범위하게 적용되고 있다. 애플, 삼성, 샤오미 등 다양한 IT 기업들은 무선이어폰 시장을 장악하기 위해 경쟁하고 있으며, 헬스케어와 피트니스 기업들은 블루투스 기술이 적용된 센서를 활용하여 사용자의 생체 데이터와 운동 데이터를 수집한 후 스마트폰으로 전송하는 웨어러블 기기들을 선보이고 있다. 그림 1은 블루투스 기술의 다양한 활용 분야를 보인 것이다.

블루투스 기기는 대부분 소형의 휴대장치 형태로 인하여 분실이 자주 발생하는 문제점이 있다. 무선 이어폰의 경우 많은 사용자들이 분실을 경험하게 되는데 분실된 블루투스 이어폰을 습득하는 경우 간단한 초기화를 통해서 사용이 가능하여 습득자가 사용하거나 중고거래 시장에 판매하는 경우가 빈번하다. 특히 해외 제조사인 경우, 국내에서 블루투스 기기의 위치추적 기능을 제공하지 않고 있어 분실대책이 전무한 상태이다. 국내 제조사의 경우, 블루투스 무선 이어폰을 분실할시 위치 추적기능을 지원한다. 그러나 평소 해당 기능이 활성화되어 있어야 하며, 잃어버린 기기 주변에 위치 추적 기능이 활성화된 같은 제조사의 다른 제품이 있어야 분실 기기의 추적이 가능하다. 또한 위치 추적 이전에 제3자가 습득할 경우에는 분실 대책으로서 한계가 있다[1].

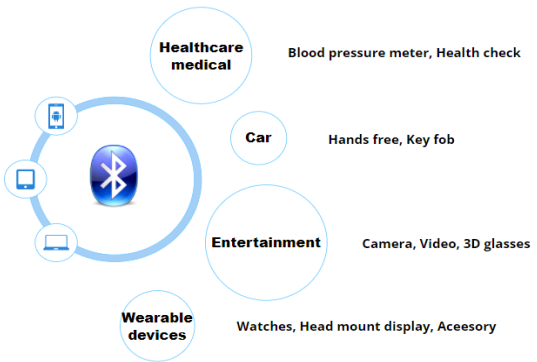

Fig. 1 Bluetooth utilizations

이러한 문제점을 해결하기 위하여 본 연구에서는 블루투스 기기에서 NFT(Non-Fungible Token)를 이용하여 합법적인 사용자를 인증하는 시스템을 제안하였다. 기존의 중앙화된 형태의 인증 방식으로는 다양한 기업에서 만든 블루투스 기기들을 통합하고 인증하는데 어려움이 존재한다. 제안하는 시스템에서 사용자는 블루투스 기기를 기기의 고유 정보인 MAC Address를 기반으로 탈중앙화된 형태의 이더리움[2] 블록체인상에 등록하고, 등록된 블루투스 기기는 최초 페어링 과정에서 개인키의 소유 유무를 확인하도록 하여 보안성을 강화하도록 하였다. 따라서 새로운 기기에서 분실된 기기를 사용하는 경우에 개인키 인증 절차를 거친 후 페어링이 가능하므로 제3자에 의한 분실된 블루투스 기기의 재사용을 방지하도록 하였다. 그리고 블루투스 기기를 분실했을 때 소유자가 분실 메시지를 이더리움에 등록하는 기능을 제공하여 습득자가 분실 메시지를 활용하여 사용자에게 되돌려 줄 수 있도록 하였다. NFT를 이용하는 인증 방식은 중앙화된 형태의 기존 인증 방식에 비하여 다양한 블루투스 기기들이 존재하는 환경에서도 별도의 관리 체계를 필요로 하지 않는다는 장점이 있다. 이더리움에서 NBAS(NFT-based Bluetooth Device Authentication System)의 평균 페이링 시간은 10.25sec로 마스터 장치와 슬레이브 장치간에 최초 페어링때 한번만 등록하고 그 후에는 재연결 기능을 사용한다. 재연결 평균시간은 0.00741sec로 기존 블루투스 장치의 재연결시간과 유사하다. NBAS에서 미등록 장치에 대한 거절시간은 1.58sec로 측정되었다.

본 논문의 구성은 다음과 같다. 2장에서는 블루투스 장치에서의 기존의 인증 기법에 대해서 소개한다. 3장에서는 NFT를 활용한 블루투스 인증시스템에 대해서 설명하고, 4장에서는 실제로 구현한 NBAS와 이를 활용한 실험 결과를 제시한다. 그리고 5장에서 결론을 맺는다.

Ⅱ. 관련연구

2.1. Bluetooth Authentication

블루투스 장치의 보안 모드는 비보안 모드, 서비스 수준 강제 보안 모드, 링크 수준 강제 보안 모드로 나뉜다. 보안 기능을 제공하지 않는 비보안 모드를 제외한 두 가지 보안 모드에서는 그림 2에서와 같이 마스터 장치와 슬레이브 장치 간에 일차적으로 키 공유 과정을 통하여 링크키를 공유하여 상호 간에 인증 및 암호화 기능을 제

공하게 된다. 키 공유 후 인증을 요구한 기기에서 제공한 128비트 난수값과 블루투스 주소값, 공유된 링크키를 이용하여 128비트 난수값을 생성하여 32비트는 인증에 활용하고 나머지 96비트(Authenticated Ciphering Offset)는 암호 키 생성에 활용한다[3].

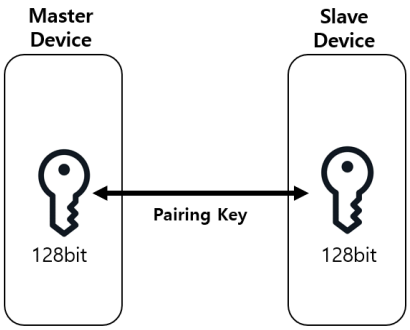

Fig. 2 Authentication method in Bluetooth

2.2. Motorcycle Authentication system using HC-05

Nenny Anggraini 외 5명은 오토바이 사용자의 키분실 대비책으로 블루투스를 활용하는 SA-RT(Situation Awareness Rating Technique)방식을 적용한 오토바이 2차 인증 시스템을 구축하였다. 해당 시스템은 아두이노 기반 HC-05와 SIM800L 모듈을 사용하여 열쇠 분실 문제를 해결하고 열쇠가 분실된 오토바이를 확보 할 수 있도록 하였다. 그림 3은 SA-RT 시스템에서 데이터 흐름과 제어 흐름을 나타낸 것이다[4].

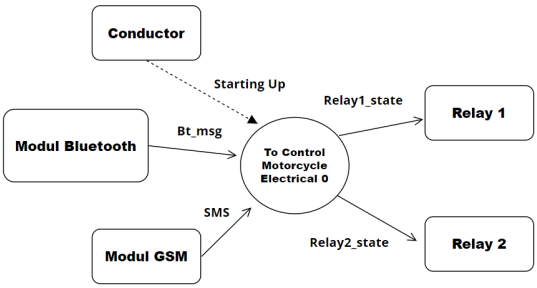

Fig. 3 SA-RT Motorcycle system

2.3. IoT Device NFT using PUFs

NFT는 블록체인 네트워크의 기술적 장점인 신뢰성과 무결성을 활용한 기술이다. NFT는 자산에 대한 특징을 블록체인 네트워크에 기록함으로써 자산에 대한 원본 보장이 가능하다. NFT는 블록체인 네트워크의 계정에 의해 발급된다. NFT를 발급하는 생성자 계정은 토큰을 발급하는 트랜잭션에 디지털 서명을 한다. 이때 디지털 서명은 블록체인 기술의 측면에서 계정의 소유자가 개인키를 활용하여 트랜잭션에 서명하였는지를 확인할 수 있음을 의미한다. 이렇게 디지털 서명된 트랜잭션은 서명에 사용된 암호화 알고리즘으로 인하여 조작이 불가능하다. 그림 4는 NFT 생성 과정을 보인 것이다[5].

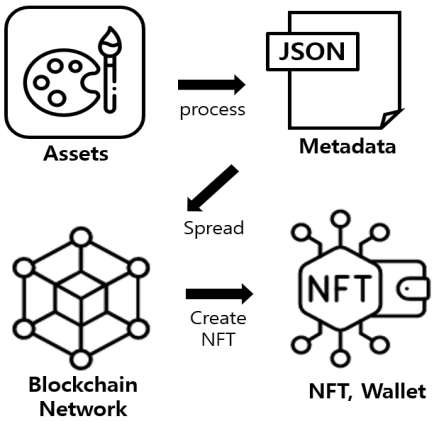

Fig. 4 Create NFT process

그림 5에서는 IoT장치에 기기 고유의 NFT를 생성하여 저장하는 방식으로 IoT장치의 하드웨어와 소프트웨어에 대한 신뢰성을 제공하는 방식을 보인 것이다. 제조사는 IoT장치에 내장된 SRAM PUFs(Physical unclonable functions)를 사용하여 스마트 NFT를 생성하고 장치를 프로그래밍한다. 제조부터 최종 사용자 적용까지 IoT장치의 하드웨어와 소프트웨어 신뢰성을 보장하여 사용자 BCA(BlockChain Account), 장치의 작동 모드와 관련된 상태, 공개, 소유자 및 사용자와 공유하는 비밀과 관련된 데이터 등의 정보들을 스마트 계약 기능과 가스 소비를 통해 제공한다[6].

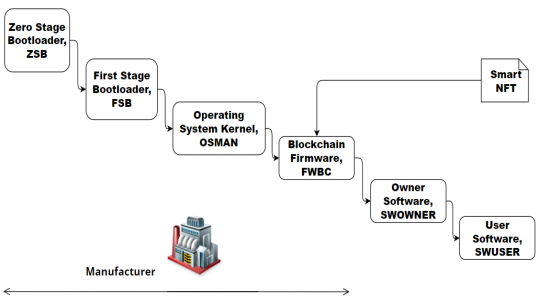

Fig. 5 NFT creating-process in PUF

Ⅲ. NBAS 구조

3.1. NBAS 구성요소

NBAS 기본 구성 요소는 그림 6과 같다. 사용자는 자신의 마스터 장치(스마트폰)를 소지한다. 마스터 장치는 슬레이브 장치(무선 이어폰)와 페어링 된다. 사용자는 페어링 과정에 마스터 장치를 통해 슬레이브 장치의 NFT를 지갑에 생성하게 된다. 공개키와 개인키를 쌍으로 생성하여 마스터 장치 내부에 개인키를 저장한다. 이때 슬레이브 장치의 NFT는 장치에 내장된 고유한 MAC 주소를 포함한다.

일반적으로 1명의 사용자는 다수의 블루투스 장치를 소유할 수 있다. 그림 7은 1명의 사용자가 다수의 슬레이브 장치를 소지하는 경우의 NBAS 구성도를 나타낸 것이다. 슬레이브 장치들은 사용자의 지갑 내부에 NFT 리스트로 저장되며 페어링 단계에서 마스터 장치에 저장된 개인키를 통해 인증되게 된다.

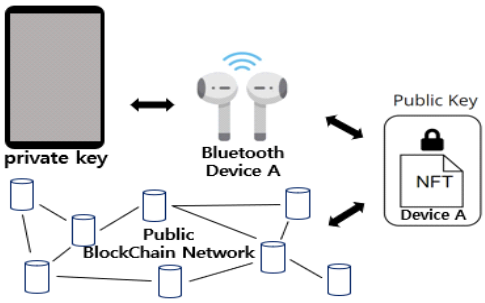

Fig. 6 Fundamental architecture in NBAS

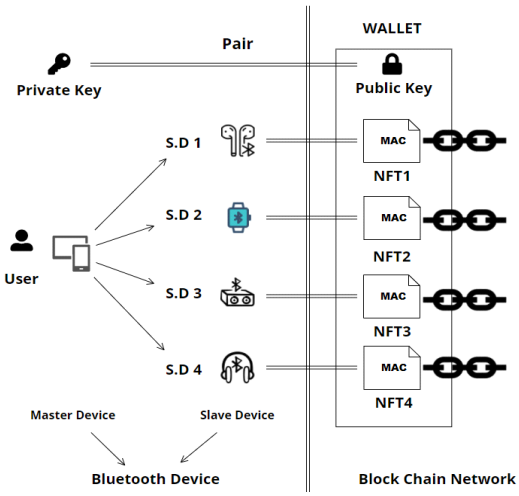

Fig. 7 Multi-devices authentication in NBAS

3.2. NBAS 인증 방식

NBAS의 인증 절차는 개인키와 공개키 쌍을 검증하는 과정으로 그림 8에서와 같이 이루어진다. 개인키는 Web3 Secret Storage Definition에서 정의한 표준 양식 PBKDF2-SHA-256을 활용하여 마스터 장치에 저장된다. 마스터 장치는 이더리움에서 제공하는 API를 사용하여 노드와 통신한다. 각 노드들은 분산 원장에 저장되어 있는 장부를 통하여 NFT의 존재 유무를 검증하는 방식으로 인증하게 된다.

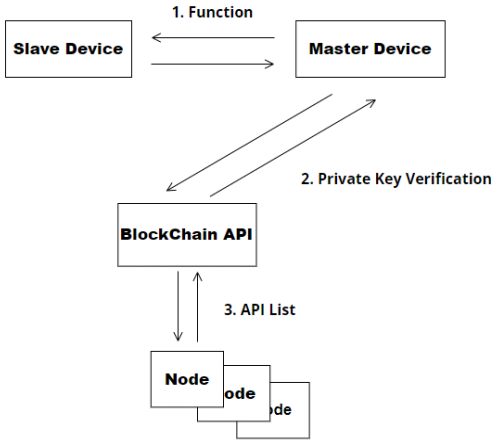

Fig. 8 Authentication process in NBAS

이더리움에서 공개키는 개인키와 쌍을 이루며 사용자의 지갑을 생성한다. 지갑 내부에는 개별 장치에 대응되는 NFT들이 리스트로 존재하며 개인키를 이용하여 소유를 증거하게 된다. 그림 9는 NFT 내부 데이터 구조를 보인 것으로, 슬레이브 장치의 MAC 주소가 포함되며 사용자가 정의한 데이터가 포함된다.

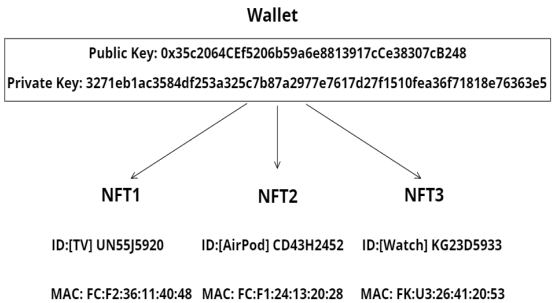

Fig. 9 NFT data structure in NBAS

3.3. NBAS 기능

NBAS는 장치 등록, 장치 연결, 장치 양도, 초기화 등의 4가지 기능을 제공한다. 그림 10은 NBAS에서 제공하는 4가지 기능들에 대한 흐름도를 나타낸 것이다. 장치 등록은 사용자가 구매한 슬레이브 장치를 최초로 페어링하는 과정에서 NFT를 생성하는 기능이다. 동일한 MAC 주소가 존재할 경우 NFT 생성이 거절된다. 장치 연결은 마스터 장치와 페어링 후 재연결을 위한 기능이다. 재연결시에는 개인키를 확인하지 않고 페어링만 되어 있다면 마스터 장치와 즉시 연결한다. 장치 양도는 사용자가 다른 사용자에게 슬레이브 장치를 양도하는 경우 다른 사용자의 지갑으로 NFT를 전송하는 기능이다. 장치 초기화는 블루투스 장치 사용 중 장치에서 오류가 발생하는 경우에 장치 초기화를 제공하는 기능이다. 초기화를 진행하여도 이미 등록된 MAC 주소를 통해 NFT와 연결되며 개인키 확인 과정없이 초기화를 진행한다.

장치 등록과 장치 양도 기능에서는 마스터 장치에 저장된 개인키 확인 과정을 거치게 된다. 장치 재연결은 페어링이 완료되었다면 이후로는 마스터 장치와 자동 연결되기 때문에 추가적인 인증 프로세스를 거치지 않는다. 그림 11은 블루투스 장치를 이더리움에 등록하는 절차를 그림으로 보인 것으로 세부 절차는 다음과 같다.

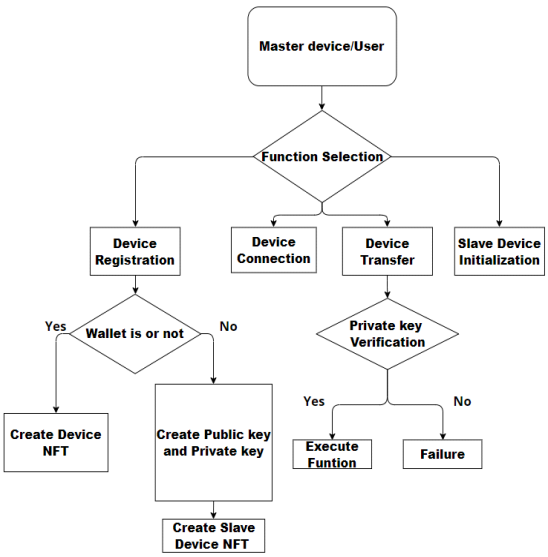

Fig. 10 NBAS function diagram

먼저 마스터 장치에서 슬레이브 장치를 검색하고, 검색된 슬레이브 장치는 자신의 MAC 주소를 마스터 장치로 전송한다. 마스터 장치는 이더리움에 지갑생성을 요청한다. 이더리움은 지갑을 생성하고 개인키를 마스터 장치에게 전달한다. 지갑 생성 후 마스터 장치는 이더리움에 슬레이브 장치 MAC 주소를 기반으로 하는 NFT 생성을 요청한다. 어떤 지갑에 NFT를 생성할지 결정하기 위해 개인키를 요청한다. 개인키를 전달한 후 이더리움에서 NFT를 생성한다.

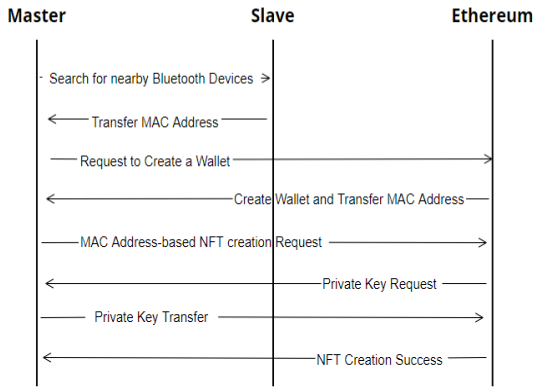

Fig. 11 Device registration process in NBAS

블루투스 장치의 최초 등록 및 페어링 과정이 끝나면 사용자는 장치를 재연결한다. 장치의 재연결은 이더리움 네트워크과 통신하지 않고 페어링이 완료된 후라면 개인키 확인없이 자동으로 재연결하게 된다.

블루투스 슬레이브 장치를 양도(hand-over)하는 경우에는 양도할 장치의 NFT를 수신할 상대방의 공개키 주소를 필요로 한다. 그림 12는 장치 양도 절차를 그림으로 보인 것으로 세부 절차는 다음과 같다. 마스터 장치에서 소유 중인 블루투스 장치의 NFT 전송을 요청한다. 전송 대상은 장치를 양도받을 사용자 마스터 장치의

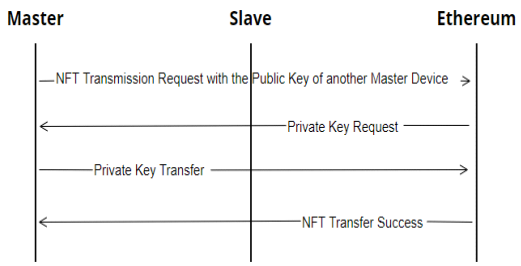

Fig. 12 Device hand-over process in NBAS

공개키이다. 이더리움에서 개인키를 요청하고, 개인키를 이더리움에 전달한다. 공개키의 개인키가 맞다면 입력된 공개키 주소로 NFT를 전송한다.

NBAS에서 슬레이브 장치의 초기화는 블루투스 연결 과정에서 생기는 오류나 사용자가 기기 초기화를 원하는 경우에 블루투스 통신을 위한 페어링 쌍을 초기화하는 기능이다. NBAS에서의 초기화는 기존의 블루투스 장치에서 초기화와 달리 MAC 주소를 초기화하지 않는다.

표 1에서는 기존 블루투스 장치에서의 초기화 기능과 NBAS에서의 초기화 기능의 차이점을 비교 제시한 것이다. 제안하는 NBAS 시스템은 MAC 주소를 인증 시스템의 요소로 활용하기 때문에 초기화를 하여도 이더리움에 저장된 MAC 주소는 초기화되지 않고 유지되게 된다.

Table. 1 Initialization comparison

Bluetooth	NBAS
Pairing Key Pair	Pairing Key Pair
Do not Use of MAC Address	Use of MAC Address

Ⅳ. 실험 및 실험결과

4.1. 실험 환경

본 연구에서는 그림 13과 같은 NBAS 모의 실험 환경을 구축하고 다양한 실험을 수행한다. 모의 실험 환경은 합법적인 블루투스 장치 소유자 스마트폰 A(사용자 마스터 장치), 미등록 스마트폰 B(미등록 마스터 장치)와 블루투스 장치 C(슬레이브 장치)로 구성된다. 이더리움에서의 노드 개수가 증가하면 속도가 저하될 수 있으나

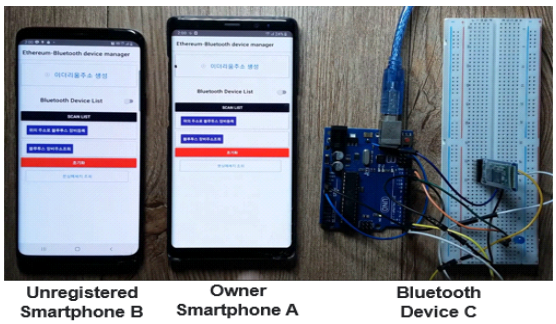

Fig. 13 Test environment

[7], 본 연구에서는 NBAS에서 블루투스 장치의 인증 보안의 효용성을 확인하기 위한 테스트베드를 구성하여 성능을 측정한다.

표 2에서는 실험 환경 구축에 사용된 언어 등 세부 구현 환경을 제시한다. 자바스크립트를 사용해 모의 시스템을 구축하고 솔리디티를 통해 스마트 컨트랙트를 배포한다. 구축 환경으로 리액트 네이티브, 트러플, 노드 JS를 사용한다.

Table. 2 Implementation environments

Environment	React-native, Truffle, Nodejs
Library	Ethereumjs-tx.js, Ethereumjs-wallet.js, Ethereumjs-util 6.0.0, Ethers 4.0.23, React 16.6.3, React-native-bluetooth-serial 1.0.0, React-native-secure-key-store 2.0.0
Language	Javascript, Solidity

Node-bluetooth.js 라이브러리를 사용하여 블루투스 세부 기능을 구현한다. 마스터 장치는 블루투스 장치 검색, 페어링된 장치 출력, 블루투스 연결, 데이터 통신등의 역할을 수행한다. 마스터 장치는 내부적으로 개인키를 저장하며 사용자가 지정한 암호문으로 암호화 된다. 개인키를 통해 사용자를 증명하고 이더리움과 통신한다.

web3.js는 HTTP, IPC 또는 WebSocket형태로 로컬 또는 원격 이더리움 노드와 상호작용할 수 있는 용도로 사용한다. 데이터를 주고받는 형태는 JSON 형태이며 기능에 따라 직렬화를 진행한다.

INFURA를 사용하여 이더리움 노드와 통신하고 ethereumjs-tx.js라이브러리를 사용해 서명 및 스마트 컨트랙트 함수를 호출한다. 퍼블릭 블록체인의 종류는 비트코인, 이더리움, 폴리곤 등이 있다[8]. 이 중 본 연구에서는 개발 환경이 우수하고 다양한 라이브러리를 지원하는 이더리움을 사용하였다. 일반적인 블록체인 기술에서는 토큰이 대체 가능한 형태이다. 하지만 NFT는 대체 불가능한 토큰이기 때문에 고유한 원본성과 소유권을 나타내는데 사용 될 수 있는 장점이 있다[5]. 따라서 제안하는 NBAS에서 MAC address를 NFT에 저장함으로서 원본성 및 소유권을 나타낼 수 있다. 스마트 컨트랙트는 솔리디티를 사용하여 이벤트, 구조체, 배열, 7개의 매핑 및 메서드로 구현하며, ERC721에서 권장하는 인터페이스를 따른다. 배포는 트러플을 사용하고 주소는 0xf1fe23dd1a73663e07b7ceffccbbc7dfe6197529이다.

그림 14는 NBAS의 전체적인 개발구성을 나타낸다.

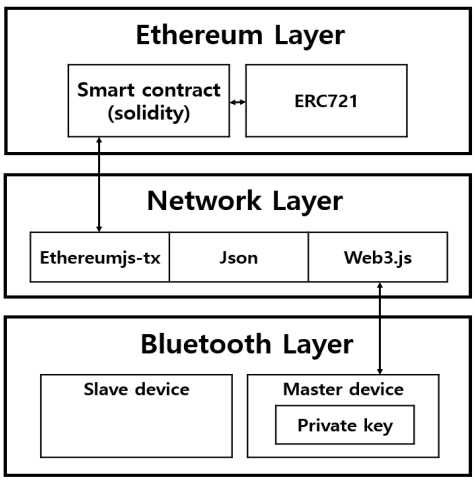

Fig. 14 Development structure in NBAS

그림 15는 모의 실험 환경 구축에 활용된 지갑생성을 위한 공개키와 개인키, MAC 주소, 아두이노 장치 슬레이브 블루투스 장치의 이름을 나타낸다.

```
Choose execution : 5
Account : 0x35c2064CEf5206b59a6e8813917cCe38307cB248
Private key : 3271eb1ac3584df253a325c7b87a2977e7617d27f1510fea36f71818e76363e5
Choose execution : 2
Found : (FC:F1:36:11:4D:48)[TV]UN55J5920
```

Fig. 15 Public address, Private Key, MAC address

제안하는 시스템을 통해 슬레이브 블루투스 장치의 NFT생성 트랜잭션은 그림 16과 같다. NFT를 생성한 후 다른 사용자에게 자신의 사용권을 양도하는 트랜잭션 내용은 그림 17과 같다.

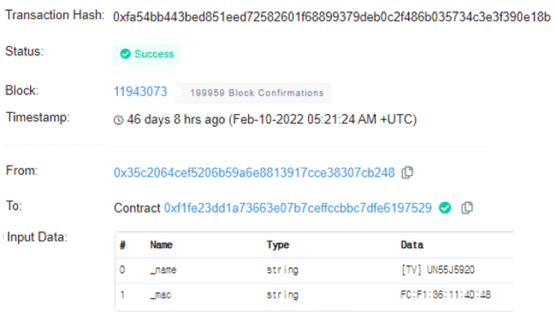

Fig. 16 NFT creation

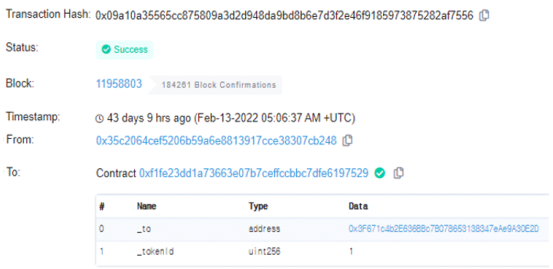

Fig. 17 Device hand-over in NBAS

미등록 스마트폰 B가 소유자 스마트폰 A의 블루투스 슬레이브 장치 아두이노에 페어링을 시도하면 개인키 검증을 통해 소유자를 확인하고 소유자가 아니라면 그림 18과 같이 경고 메시지가 팝업된다.

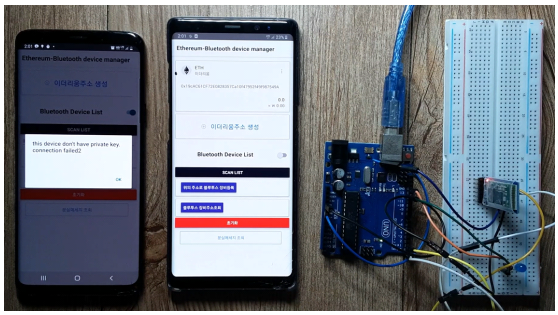

Fig. 18 Trial of unregistered user connection

소유자 스마트폰 A를 통해 아두이노 블루투스 장치의 분실메세지를 등록할 수 있고 분실메세지가 등록되면 분실물을 습득한 사용자의 미등록 스마트폰 B를 통해 그림 19와 같은 분실 메세지를 확인한다.

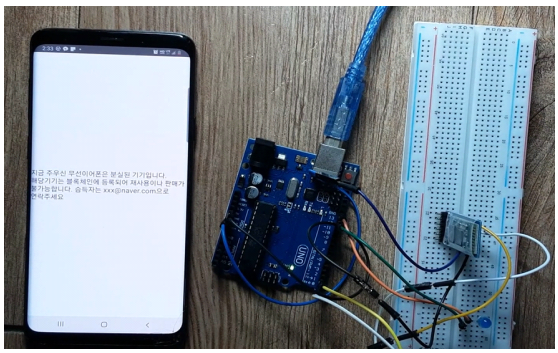

Fig. 19 Lost message of missing device

4.2. 실험 결과

일반적으로 블루투스 장치의 페어링 시간은 0.8sec~0.9sec로 알려져 있다[9]. 그러나 해당 연구는 NS2를 이용한 시뮬레이션 환경으로 실제 물리적 환경에서의 PIN을 이용한 기존 블루투스의 페어링 시간보다 측정시간이 작을 것으로 판단된다. 본 연구에서 실제 물리적 환경에서 측정한 기존 블루투스 장치의 평균 페어링 시간은 2.52sec으로 측정되었다.

4.2.1. NBAS 페어링 시간

NBAS에서 장치간 페어링 단계에서 개인키와 공개키 쌍을 생성하고 NFT를 생성한다. 키쌍을 생성하면 개인키는 마스터 장치에 PBKDF2-SHA-256방식으로 저장되며 키쌍을 생성하고 복호화 하는 평균 시간은 7.285sec가 소요되었다. 그리고 NFT생성시간[10]은 이더리움에 트랜잭션을 요청하는 시간을 측정하였다. NFT 트랜잭션 생성 시간은 평균 0.474sec으로 측정되었다.

$$P_t = K_t + N_t + P_{dt} \quad (1)$$

식 (1)과 같이 NBAS 페어링 시간(P_t)은 키 쌍 생성 및 복호화 시간(K_t), NFT생성시간(N_t), 초기 페어링 시간(P_{dt})의 합으로 나타낼 수 있다. 따라서 NBAS의 최초 페어링 시간은 평균 10.25sec가 소요되는 것으로 계산되었다. 이는 실험결과 기존 블루투스 페어링 시간과 비교하여 평균 7.72sec 정도가 추가로 소요되는 것으로 나타났다. 그러나 이것은 NFT를 사용하기 위한 추가시간으로 분실된 장치에 대한 보안성 보장을 위한 오버헤드로 이해할 수 있다.

그림 20은 전체 100회 수행하였을 때, 기존 블루투스 장치의 페어링 시간과 NBAS 페어링 시간을 비교한 것이다.

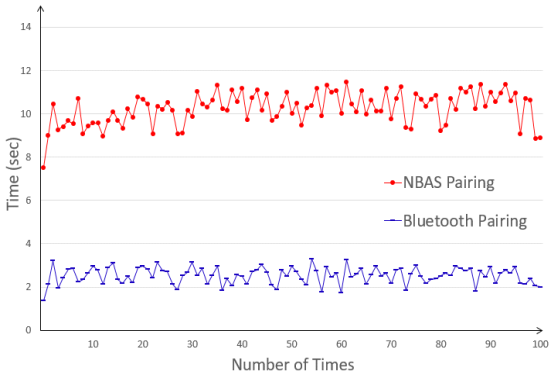

Fig. 20 Comparison of pairing time

4.2.2. NBAS Reconnection 시간

그림 21의 기존 블루투스 장치 재연결 시간은 평균 0.007sec로 측정되었다. NBAS의 경우 최초 페어링 이후 재연결시에는 마스터 장치 내부에 NBAS를 통한 기존 페어링 장치들의 정보가 저장됨으로 추가적으로 이더리움 네트워크상에 접속할 필요가 없다. 따라서 NBAS에서도 재연결될 때 시간은 기존의 블루투스 장치의 재연결 시간과 비슷하게 측정되었다.

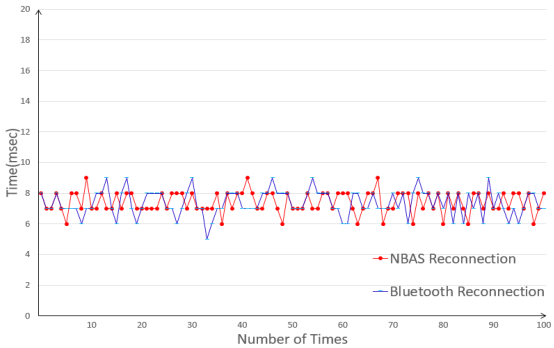

Fig. 21 Comparison of reconnection time

4.2.3. 미등록 장치의 NBAS Rejection 시간

NBAS는 NFT를 활용하여 미승인된 장치의 승인을 거절함으로써 기존 블루투스 장치의 분실, 도난에 대한 보안성을 제공한다. 그림 22에서처럼 미승인된 장치에서 이더리움에 등록된 슬레이브 장치에 페어링을 요청하는 경우 미승인 장치의 접근은 페어링이 제한되며 NBAS의 거절 시간은 평균 1.58sec로 측정되었다. 이는 NBAS와 기존 블루투스 페어링을 구분짓는 중요한 특징으로 NBAS는, 미승인 장치의 페어링을 효과적으로 제한함을 보여준다.

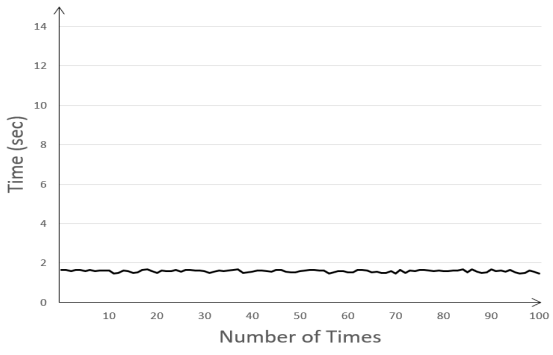

Fig. 22 Rejection time for unauthorized device pairing

Ⅴ. 결 론

본 연구에서는 기존의 블루투스 장치에서 분실 취약점을 해결하기 위한 방안으로 NFT기반으로 블루투스 장치를 인증하는 NBAS를 제안하였다. 블루투스 장치의 초기 페어링 단계에서 슬레이브 장치의 고유정보를 NFT화하여 등록하고 생성한 합법적인 소유자만 해당 NFT에 접근하는 절차를 제안하였다. NBAS의 초기 페어링 시간은 평균 10.25sec이고 재연결 시간은 평균 0.007sec으로 측정되었다. 또한 NBAS는 미등록장치를 평균 1.58sec로 거절함을 보여주었다. 이는 장치 등록 후 다른 소유자 혹은 다른 기기에서 접근을 효과적으로 제한하며 보안성을 강화하였음을 보여준다. 제안하는 시스템은 다양한 형태의 블루투스 장치가 존재하는 환경에서 보안을 강화하고 분실된 블루투스 장치의 무분별한 사용을 방지하는 해결책으로 활용될 수 있을 것으로 기대된다. 또한 신뢰성과 연결성 및 이더넷을 통한 NBAS의 분석을 심화할 예정이다. 후속 연구로는 개인키 보관법, 네트워크 내 데이터 제공자로서의 역할, 다양한 네트워크 및 장치에서 효과적인 추가 보안 강화기법 개발이 기대된다.

ACKNOWLEDGEMENT

This research is financially supported by Changwon National University in 2021~2022.

References

[1] J. Padgette, J. Bahr, M. Batra, M. Holtmann, R. Smithbey, L. Chen, K. Scarfone, "Guide to bluetooth security," *NIST Special Publication*, vol. 800, no. 121, 2017.

[2] H. J. Lee and J. Y. Cho, “A Study on Matters of Crypto-Currency,” *The Jounal of Comparative Private Law*, vol. 25, no. 2, pp. 657-696, May. 2018.

[3] A. I. Mondal and B. K. Mandal, “Architecture of Bluetooth Security for Pairing Key and Better Authentication,” in *Proceeding of the 5th International Conference on Information System and Computer Networks*, Mathura, India, pp. 1-6, 2021.

[4] N. Anggrini, I. M. Shofi, M. Nurzamazami, N. Hakiem, F. Fahrianto, and T. Rosyadi, “Motorcycle Secondary Authentication System Using Arduino-Based HC-05 and SIM8001 Module,” in *Proceeding of the 8th International Conference on Cyber and IT Service Management*, Pangkal, Indonesia, pp. 1-7, 2020.

[5] J. Lee and G. -S. Jo, “Understanding and Utilizing the Latest NFT Technology,” *Korea Institute of Information Technology Magazine*, vol. 19, no. 1, pp. 7-11, Dec. 2021.

[6] J. Arcenegui, R. Arjona, R. Román, and I. Baturone, "Secure combination of IoT and blockchain by physically binding IoT devices to smart non-fungible tokens using PUFs," *Sensors*, vol. 21, no. 9, pp. 3119, 2021, DOI: 10.3390/s21093119.

[7] R. Dennis and J. P. Disso, "An analysis into the scalability of bitcoin and ethereum," in *Proceeding of the third International Congress on Information and Communication Technology*, London, U.K, vol. 797, pp. 619-627, 2019.

[8] F. Irresberger, K. John, P. Muller, and F. Saleh, "The public blockchain ecosystem: An empirical analysis," NYU Stern School of Business: CA, Technical Report, Apr. 2021.

[9] S. Gajbhiye, M. Samta, S. Karmkar, and S. Sharma, “Design, implementation and security analysis of Bluetooth pairing protocol in NS2,” in *Proceeding of the International Conference on Advances in Computing, Communications and Informatics*, Jaipur, India, pp. 1711-1717, 2016.

[10] Ethereum Development Documentation [Internet]. Available: https://ethereum.org/en/developers/docs/blocks/.

황성욱(Seong-Uk Hwang)

2016년 3월 ~ 현재 : 창원대학교 컴퓨터공학과 학사과정

※관심분야 : IoT, 블록체인, NFT, 임베디드 시스템

손성무(Sung-Moo Son)

2019년 3월 ~ 현재 : 창원대학교 컴퓨터공학과 학사과정

※관심분야 : IoT, 블록체인, NFT, 임베디드 시스템

정성욱(Sung-Wook Chung)

2010년 8월 : CISE dept, Univ. of Florida, USA, (Ph.D)

2010년 10월 ~ 2012년 2월 : KT 종합기술원 중앙연구소 선임연구원

2012년 3월 ~ 현재 : 창원대학교 컴퓨터공학과 부교수

※관심분야 : IoT, NFT, HPC, 머신러닝, 실시간 분산 멀티미디어시스템, 홈네트워크