Journal of Digital Convergence
Vol. 18. No. 3, pp. 163-169, 2020

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2020.18.3.163

사용자의 이동정보를 활용한 클라이언트 인증 기반의 임베디드 보안 컨트롤러 설계

홍석원
경남도립거창대학 교무처 기획평가팀장

Design of Embedded Security Controller Based on Client Authentication Utilizing User Movement Information

Suk-Won Hong
University of Gyeongnam Geochang Ademic Afairsoffice Head of Planning Evaluation

요 약 스마트키는 다양한 임베디드 환경에서 활용하고 있지만 사용자의 위치에서 신호의 증폭을 통한 원격지 공격이 발생하고 있음을 알 수 있다. 방어 기법에 대한 기존 연구는 다수의 센서를 사용하거나 인증 속도의 개선을 위한 해시 함수를 사용한 경우가 있는데 이는 전력 소모를 증가시키거나 1종 오류가 발생할 가능성을 가지고 있다. 이에 본 논문에서는 컨트롤러와 호스트 장치간의 인증 방식을 개선하여 사용자의 이동 정보와 클라이언트 인증 기반의 임베디드 보안 컨트롤러 모델을 제안하고자 한다. 제안하는 모델에 대하여 아두이노 보드와 GPS 및 블루투스를 이용한 통신을 위하여 암호화 알고리즘을 적용하였으며 인증을 위하여 사용자의 이동 정보를 사용하여 경로 분석을 통해 인증을 수행하였다. 그리고 제안하는 모델을 사용하여 동작 수행을 하더라도 작동 편이성에 큰 영향을 미치지 않았음을 암호화 및 복호화 시간 측정을 통하여 확인하였다. 제안하는 모델의 임베디드 보안 컨트롤러는 이륜차와 같은 리모트 컨트롤러와 이동 또는 고정형 호스트 장치를 가지고 있는 시스템 구조에서 적용할 수 있으며 연구 과정에 암호화 및 복호화 시간이 각각 100ms 이내에 처리를 수행할 수 있음을 확인하였으며 향후 경로 데이터 관리 방법에 대한 추가연구 및 암호화 및 복호화 소요 시간과 데이터 통신 시간을 줄일수 있는 프로토콜에 대한 연구가 더 필요할 것으로 판단된다.

주제어 : 임베디드시스템, 클라이언트인증, 암호화, GPS, 퍼스널모빌리티보안, 아두이노

Abstract A smart key has been used in a variety of embedded environments and there also have been attacks from a remote place by amplifying signals at a location of a user. Existing studies on defence techniques suggest multiple sensors and hash functions to improve authentication speed; these, however, increase the electricity usage and the probability of type 1 error. For these reasons, I suggest an embedded security controller based on client authentication and user movement information improving the authentication method between a controller and a host device. I applied encryption algorithm to the suggested model for communication using an Arduino board, GPS, and Bluetooth and performed authentication through path analysis utilizing user movement information for the authentication. I found that the change in usability was nonsignificant when performing actions using the suggested model by evaluating the time to encode and decode. The embedded security controller in the model can be applied to the system of a remote controller for a two-wheeled vehicle or a mobile and stationary host device; in the process of studying, I found that encryption and decryption could take less then 100ms. The later study may deal with protocols to speed up the data communication including encryption and decryption and the path data management.

Key Words : Embedded system, Client authentication, Encryption, GPS, Personal mobility security, Arduino

*Corresponding Author : Suk-Won Hong(okapple1@naver.com)
Received November 21, 2019 Revised February 17, 2020
Accepted March 20, 2020 Published March 28, 2020

1. 서론

ADAC(독일자동차연맹)는 릴레이 기법에 의한 스마트키 차량 보안테스트를 237종의 스마트 키 차량을 테스트 했는데 3종을 제외하고 이 기법에 취약하다는 것을 발견했다[1]. 이 공격은 스마트 키의 신호를 증폭하여 스마트키가 차량에 인접하고 있는 착오에 빠지게 하여 인증을 통과하는 공격 방법이다. 이러한 공격에 대한 대응 방안의 연구에서 GPS 센서와 지자기 센서를 활용하여 신호 증폭 공격의 검출을 통한 보안 인증 방식을 제안하기도 하였다[2]. 이 연구는 스마트 키와 차량 간의 위치 정보를 검증하는 방법을 사용하는데 유사한 위치에 있을 경우는 검증 값이 유사하다는 것을 이용하여 인증을 수행한다. 그리고 이 연구를 개선하여 인접 AP(Access Point) 목록 정보를 활용한 인증 방식에 대한 연구도 있었다[3]. 이 연구는 GPS 좌표를 현재 위치를 확인하는데 주로 활용하고 인접하고 있는 위치에 있다면 AP 목록이 유사할 것이라는데 전제 조건을 두고 연구를 수행하였다. 그러나 AP의 목록은 동일한 위치에 있어도 스마트 키와 차량이 서로 다르게 인식할 수 있는 가능성이 높고 AP 목록을 검증하기 위하여 해시 함수를 사용하는데 이 경우 1종 오류의 발생 가능성을 내포하고 있다. 또한 이들 연구는 공통적으로 스마트 키에 다수의 센서를 사용하는 방법으로 스마트 폰을 사용하면 된다는 전제 조건을 가지고 있다. 이들 연구의 문제점은 다수의 센서를 사용하면 전력 소모의 문제가 발생할 수 있으며 스마트 폰을 사용하지 않는 경우는 별도의 컨트롤러가 있어야 한다는 점에 착안하여 본 논문에서는 기존 연구에서 사용하는 다양한 센서를 줄이고 GPS 좌표를 취득하고 이를 이용하여 사용자의 이동 정보를 활용한 클라이언트 인증 기반의 임베디드 보안 컨트롤러를 설계하였다. 그리고 아두이노를 활용하여 설계를 구현하였으며 이 과정에 대칭키 암호화 기법을 적용하여 제안하는 모델에 대한 실험을 수행하고 암호화 기법을 적용한 경우의 임베디드 보안 컨트롤러의 활용 가능성을 검증하였다. 이를 통하여 제안하는 임베디드 보안 컨트롤러가 현실적으로 사용에 불편함이 크지 않음과 경량화의 가능성을 확인할 수 있었다.

2. 관련연구

2.1 스마트 키

2.1.1 개요

스마트 키 시스템은 차량과 스마트 키의 통신을 433MHz 의 RF 주파수를 사용하는 경우와 125/134.2kHz 의 LF 주파수를 사용할 수 있다[4]. 이러한 RF 또는 LF 주파수를 사용하는 경우의 단점은 릴레이 기법을 이용한 인증 통과가 쉽게 발생할 수 있다는 점이다.

2.1.2 스마트 키 보안 연구 동향

스마트 키의 보안 성능을 향상하기 위해 GPS와 지자기 센서를 이용하여 위치 정보로 활용하는 경우에 대한 연구가 있다[2]. 이 연구는 클라이언트와 서버로 구성한 환경에 GPS와 지자기 정보를 각각 저장하여 비교하는 인증과정을 수행하여 유사한 위치에 있는가를 판단하는 연구이다.

또 다른 연구에서는 AP의 목록 정보를 활용하여 인증하는 방식으로 클라이언트 서버 측의 각각의 주변 AP를 스캔하여 양측의 AP목록과 비교하여 일치하는 정도에 따라 인증을 수행하는 연구도 있다[3].

또한 관점별로 다양한 보안 이슈에 대응하여 보안 요구사항은 기본 보안 기능이라는 용어를 사용하여 기밀성, 무결성 및 가용성을 나타내며 이들은 기본 보안 기능이 제공하는 사용자 또는 호스트 인증 메커니즘뿐만 아니라 생체 인식 및 액세스 제어와 같은 다른 메커니즘을 사용할 수 있다[5]. 이를 정리하면 Table 1과 같다.

Table 1. Security Requirement

Requirement	Description
Confidentiality	Authorized user can access to property
Integrity	Authorized user can modify information in accredited way
Availability	Accessible in valid time

임베디드 시스템은 광범위한 영역에서 존재하므로 연구 분야도 매우 다양하다. 본 논문의 연구 분야인 클라이언트 또는 호스트 인증 메커니즘의 경우는 최근 NFC를 이용한 보안 요구 충족에 대한 연구를 진행하는 경우도 있다[6,7].

2.2 위치 기반의 인증 시스템

위치 기반의 인증 시스템은 위치 정보의 측위 기술과 인증 기술로 분류할 수 있는데 측위 기술은 실외에서는 위성항법 시스템과 실내의 경우는 실내 무선 측위 기술로 분류할 수 있으며 인증 기술은 사용자의 물리적 위치 정보를 이용한다[8]. 측위 기술에서 GPS는 위성 항법 시스템의 한 종류로 GPS 위성에서 송신하는 신호를 수신하여 삼변측량[9]의 방법으로 수신자의 위치를 측정한다. GPS 수신기는 반송파의 해석을 통하여 NMEA 메시지를 배포하는데 이를 사용하기 위하여 해당 메시지의 타입을 확인하고 맞는 프로토콜로 해석하는 과정을 수행해야 한다[10]. GPS 좌표 정보의 해석을 통하여 사용자의 이동 거리나 위치를 계산할 수 있다.

2.3 암호화

암호화 알고리즘은 크게 세 가지로 분류할 수 있다. 이는 대칭키 암호화와 비대칭키 암호화 및 단방향 암호화 알고리즘으로 분류 할 수 있다[11,12]. 대칭키 암호화는 비밀키 암호화, 비 대칭키 암호화는 공개키 암호화라고 한다. 또한 단방향 암호화는 해시 알고리즘이라고 한다.

대칭키는 암호화 키와 복호화 키가 동일한 경우를 말하며 비 대칭키는 키가 서로 다른 경우를 말한다.

대칭키 암호화는 키 배송을 안전하게 수행할 수 없는 단점이 있으며 비 대칭키 암호화는 대칭키 암호화에 대비하여 안전하기는 하지만 암/복호화가 상당히 느리다는 단점을 가지고 있다.

본 논문에서는 이러한 스마트 키와 유사한 유형의 임베디드 시스템이 다양한 종류의 자동차와 이륜자동차들 및 전자 제품에 사용되고 있으며 이들에 대한 보안 환경이 공격에 취약하다는 점과 임베디드 시스템에 사용되는 센서와 암호화 알고리즘에서는 경량화가 중요하다는 점에 착안하여 사용자 이동 정보를 활용한 클라이언트 인증 기반의 임베디드 보안 컨트롤러를 제안하고자 한다.

3. 제안 모델

3.1 시스템 설계

3.1.1 구조

제안하는 모델은 클라이언트 인증 방식을 사용하며 암호화 키는 일반적인 통신 환경에서 많이 사용하는 대칭키 인증을 사용한다. 제안하는 모델의 구조는 Fig. 1.과 같다.

Fig. 1에서 호스트는 클라이언트 인증을 위한 challenge를 컨트롤러에 보내고 컨트롤러는 이를 수신하면 보유하고 있는 이동 좌표 정보와 수신한 challenge를 암호화해서 이들 값을 호스트로 보낸다. 호스트는 수신한 데이터를 검증하는 과정으로 구분할 수 있다.

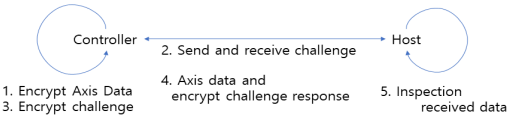

Fig. 1. structure of proposed model

3.1.2 제안 모델의 다이어그램

제안하는 솔루션에서 사용하는 파라미터는 Table 2.와 같다.

Table 2. Parameter of Challenge Response Authentication

Label	Definition
challenge	challenge value for embedded system
response_r	response message of remote_controller
encAxis	encrypt trace axis
secret_key	encrypt symmetric key

제안하는 모델에서 인증과정은 클라이언트 인증을 사용하며 호스트에서 전송하는 challenge를 컨트롤러가 수신하면 미리 교환한 대칭키인 secret_key를 이용하여 암호화 과정을 수행하여 response_r메시지를 생성한다. 또한 encAxis는 컨트롤러가 기록한 자신의 이동 GPS 좌표를 암호화한 정보이다.

Table 2에서 제시한 Label을 이용하여 표현한 제안 모델의 시퀀스 다이어그램은 Fig. 2와 같다.

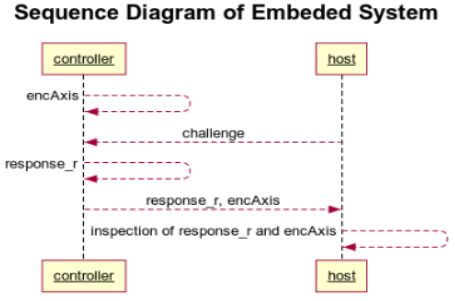

Fig. 2. Sequence Diagram for Proposed Model

Fig. 2 의 동작은 아래의 절차로 진행한다.
step1. 컨트롤러의 이동 정보를 암호화
step2. challenge 송수신
step3. challenge를 기반으로 response_r생성
step4. 이동정보와 response_r을 송수신
step5. 이동 정보와 response_r을 복호화
step6. 이동 정보와 response_r을 검증

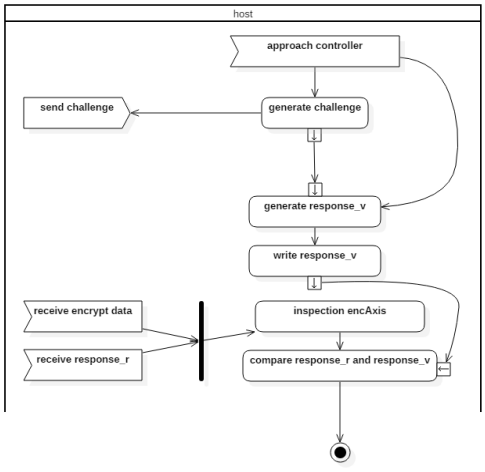

Fig. 3. activity diagram of host

제안 모델의 액티비티 다이어그램은 Fig. 3및 Fig. 4와 같다.

Fig. 3은 호스트에서의 동작을 나타내는 다이어그램으로 컨트롤러가 호스트에 접근하면 블루투스 페어링으로 상호 인식하며 호스트는 challenge를 생성하여 컨트롤러로 전송한다. 그리고 생성한 challenge는 1회성 난수이므로 차후 비교를 위하여 response_v로 저장한다. Fig. 4는 컨트롤러에서의 동작을 나타내는 다이어그램으로 컨트롤러는 GPS 좌표를 수신하여 이동 정보를 저장하는 과정을 수행하다가 호스트에 접근하면 수신을 중단하고 저장해 둔 이동 정보를 읽어 들인다. 그리고 이를 암호화하여 저장하는 과정을 수행한다. 또 그 과정에 challenge를 수신하면 이를 암호화하여 response_r을 생성하고 암호화 해 둔 encAxis와 response_r을 호스트로 전송한다. 이후 Fig. 3에서 호스트는 수신한 encAxis와 response_r을 복호화 한 후 encAxis는 검증을 하고, response_r은 저장해둔 response_v와 비교하는 과정을 통하여 인증과정을 수행한다.

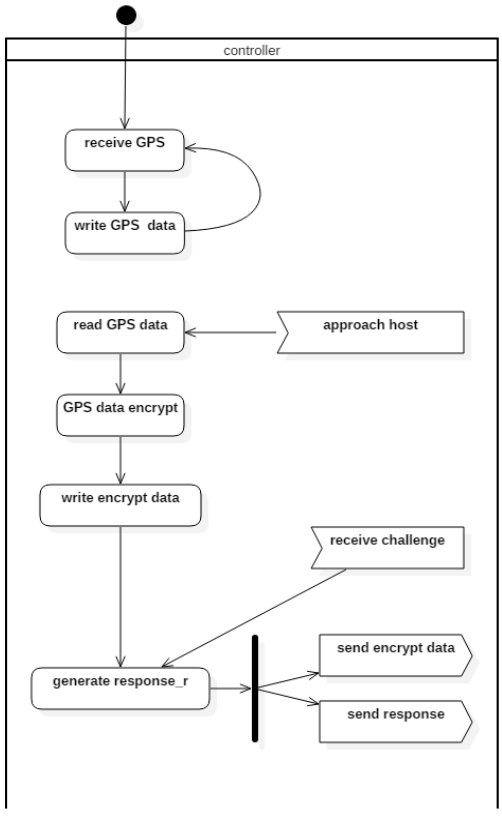

Fig. 4. activity diagram of remote_controller

4. 구현 및 평가

4.1 실험 환경

제안하는 모델은 임베디드 시스템의 경량화에 적합한 아두이노를 사용하여 실험한다. 본 모델의 컨트롤러의 결선도는 Fig. 5 및 Fig. 6과 같다. Fig. 5는 컨트롤러에 대한 결선도이며 Fig. 6은 호스트에 대한 결선도이다.

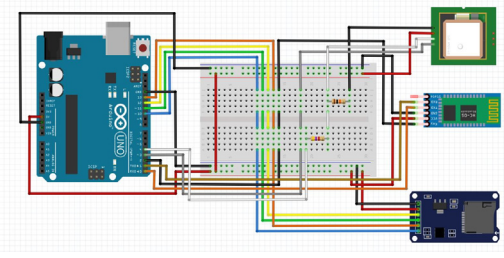

Fig. 5. connection figure of controller

Fig. 5는 아두이노 보드를 사용하여 GPS 수신모듈을 부착하고 호스트와의 통신을 위한 블루투스 모듈을 부착하였다. 블루투스 모듈은 마스터 슬레이브의 설정이 가능한 HC-05를 사용하였다. 그리고 사용자의 이동 정보와 생성 정보의 저장을 위한 SD 카드 모듈도 부착하였다.

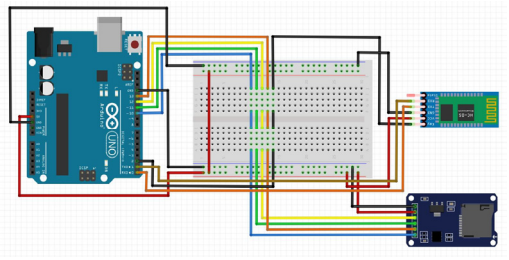

Fig. 6. connection figure of host

Fig. 6은 컨트롤러와 달리 GPS 수신 모듈이 필요하지 않아 제외하고 나머지를 구성하였다.

결선도에 따른 실험을 위하여 구성한 환경은 Fig. 7과 같다. Fig. 7의 좌측 아두이노 보드 측은 호스트를 구성하고 있으며 우측은 컨트롤러를 구성하고 있다. 그리고 실험 환경의 블루투스는 양방향 통신을 위하여 호스트 측을 마스터로 설정하고 컨트롤러 측을 슬레이브로 설정하였다. 다만 이는 통신의 방향과는 특별한 관계는 없다.

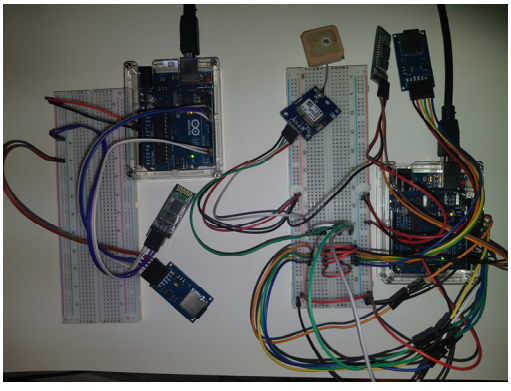

Fig. 7. environment of host and controller

4.2 실험 결과 및 분석

제안 모델의 실험은 컨트롤러가 이동 위치의 GPS 좌표를 수신하고 SD card에 저장한다. 컨트롤러는 부하가 걸리는 동작을 배제하기 위하여 단순 저장의 역할만 수행하였다. 컨트롤러가 호스트로 이동할 경우 블루투스를 이용하여 페어링을 수행한다. 그리고 페어링이 성공했을 때 컨트롤러는 저장한 GPS 데이터를 읽어들인 후 그 값을 암호화 하여 encAxis를 저장한다. 이때 호스트에서는 challenge를 생성하여 컨트롤러에 전송하고 차후 비교를 위하여 response_v로 저장한다.

컨트롤러는 challenge를 수신하면 이를 암호화 한 response_r을 생성하고 저장한 후 미리 생성한 encAxis와 함께 호스트로 전송한다.

호스트는 수신한 encAxis를 복호화 한다. 이동 정보의 분석을 위하여 호스트는 복호화한 GPS 좌표에서 이동 정보를 생성하여 검증한다. GPS좌표는 GPGGA, GPGLL, GPRMC, GPVTG, GPGSA, GPGSV등이 있었으며 GPGGA를 기본으로 이동 정보를 저장하였다. 또한 좌표 정보가 부족한 경우에는 GNSS 정보를 가지고 있는 GPRMC를 추가로 사용하도록 하였다.

실험에서는 10분간 15초 간격으로 40개의 좌표가 각각 인접하고 있는 좌표인지를 검증하였으며 response_r과 저장 해 둔 challenge인 response_v를 비교하여 정상 경로를 사용하여 접근 한 경우 인증을 허용한다.

또한 성능 평가를 위하여 데이터를 암호화 하는 과정과 복호화 하는 과정의 시간을 측정하였다. 79회의 실험을 수행한 결과 Fig. 8은 암호화 시간을 나타내며 Fig. 9는 복호화 시간을 나타내고 있다.

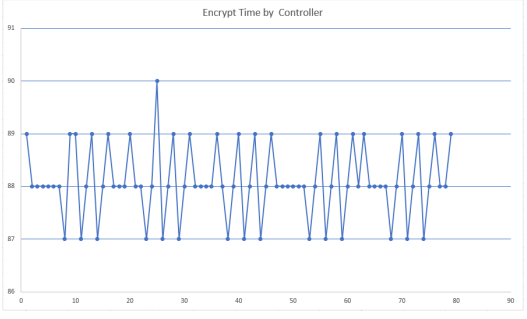

Fig. 8. Encryption time of Controller

컨트롤러가 GPS 좌표를 암호화 하는데 소요되는 시간은 Fig. 8과 같이 87ms에서 90ms가 된다. 또한 컨트롤러가 전송한 데이터를 복호화 하는데 소요되는 시간은 Fig. 9와 같이 95ms에서 100ms였다.

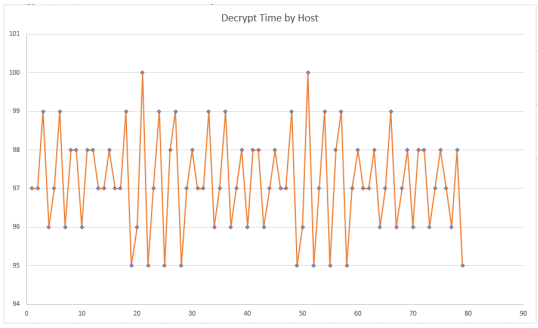

Fig. 9. Decryption Time of Host

이상의 과정을 통하여 사용자 이동 정보와 클라이언트 인증 기반의 임베디드 보안 컨트롤러를 사용하여 호스트와 리모트 컨트롤러간의 데이터 암호화 통신을 사용하여 인증 과정을 수행 할 수 있음을 확인 하였으며, 인증을 위한 암호화 및 복호화를 수행하는 시간이 각각 100ms 이하로 소요됨을 알 수 있었다.

제안하는 모델은 구현을 통하여 임베디드 시스템의 기본 보안 기능의 요구사항에 대하여 기밀성 부분은 컨트롤러의 소유자만 접근 가능하며, 무결성은 암호화 및 복호화와 이동 정보 분석을 통한 정보의 변경이 가능하였다. 그리고 항상 접근이 가능하다는 점에서 가용성도 충족함을 알 수 있었다.

5. 결론

본 논문은 임베디드 시스템 중에서 리모트 컨트롤러와 이동 또는 고정형 호스트 간의 GPS 좌표 정보를 활용한 호스트 인증 기반의 임베디드 보안 컨트롤러 설계를 제안하였다. 기존 연구에서는 다양한 센서를 부착하여 인증 과정을 수행하거나, AP 목록을 이용하는 연구를 수행하였으나 다양한 센서를 사용하거나 AP 목록을 이용하면 전력소모량이 증가하게 되는 문제가 있으며, 더불어 AP 목록을 이용하는 방법에서는 속도 문제가 발생할 수 있다. 그래서 기존 연구에서는 속도 문제를 해결하기 위하여 블룸 필터 방법을 사용하였으나 이 경우 1종 오류가 발생할 수 있다. 그러나 제안하는 모델은 제한된 센서만을 사용하여 경량화된 임베디드 보안 컨트롤러를 설계하였다. 또한 실험을 통하여 제한된 센서만을 사용하더라도 컨트롤러와 호스트간의 인증에 오류가 발생하는 현상은 없었다. 현재까지 많은 리모트 컨트롤러를 이용한 다양한 시스템이 보안 위협에 노출되어 있는 상황에서 본 솔루션은 대칭형 암호화/복호화를 사용하여 보안 위협의 가능성을 줄일 수 있을 것이다. 또한 일반적으로 사용하는 리모트 컨트롤러와 비교하여 암호화/복호화 시간이 각각 100ms 수준으로 실제 사용에서 불편함이 없을 정도의 시간이 소요됨을 알 수 있다. 또한 임베디드 시스템의 기본 보안 기능의 요구 사항을 충족하였다. 본 연구를 수행하는 과정에서 향후 리모트 컨트롤러와 호스트가 장시간 이탈되어 있는 경우 경로 데이터 관리 방법에 대한 연구와 함께 GPS 좌표를 수신 할 수 없는 곳에서의 경로 데이터 관리 방법도 함께 연구가 더 필요할 것으로 판단된다.

REFERENCES

[1] https://www.bbc.com/korean/news-47030334

[2] Francillon, A., Danev, B., & Capkun, S. (2011). Relay attacks on passive keyless entry and start systems in modern cars. *In Proceedings of the Network and Distributed System Security Symposium (NDSS).*

[3] Kim, G. H., Lee, K. H., Kim, S. S., & Kim, J. M. (2013). Vehicle relay attack avoidance methods using RF signal strength. *Communications and Network*, 5(03), 573-577.
DOI : 10.4236/cn.2013.53b2103

[4] Isa, M. A. M., Hashim, H., Adnan, S. F. S., Marbukhari, N., & Mohamed, N. N. (2017). An automobile security protocol: side-channel security against timing and relay attacks. I*nt. J. Electronic Security and Digital Forensics(IJESDF)*, 9(3), 239-253.
DOI : 10.1504/ijesdf.2017.085194

[5] Shin Woo Joo, Seung Jin Baek, Sirojiddin Djuraev, Youngmin Jeon, Sungkwan Yoon, & Seung Yeob Nam. (2017). Authentication scheme to prevent amplification attack on vehicle remote key entry system. *Proceedings of Symposium of the Korean Institute of communications and Information Sciences.* 1180-1181.

[6] Shin Woo Joo, Kyu-Seek Sohn, & Seung Yeob Nam. (2017). Vehicle Remote Key Authentication Scheme based on AP List for Preventing Amplification Attack. *The Journal of Korean Institute of Communications and Information Sciences, 42(10),* 2012-2021.
DOI : 10.7840/kics.2017.42.10.2012

[7] Jae Oh Bang, Kuk Won Ko, & Chung Eun Yun. (2009). Development of Vehicle Information System using Smartkey Entry System. *Korean Society for Precision Engineering Conference.* 303-304.

[8] Hyung-Jin Mun, Gwang-Houn Choi, & Yooncheol Hwang. (2016). Countermeasure to Underlying Security Threats in IoT communication. *Journal of Convergence for Information Technology, 6(2),* 37-44. DOI : 10.22156/CS4SMB.2016.6.2.037

[9] Taeseok Jin. (2016). Development of Motocycle's Anti-theft Device Based on NFC. *The Transactions of the Korean Institute of Electrical Engineers, 65(1),* 165-170. DOI : 10.5370/KIEE.2016.65.1.165

[10] Hyung-Uk Kim, Hyung-joo Kim, Jung-ho Kang, Moon-seog Jun. (2016). A Study on Analysis and Countermeasure of Security threat in NFC. *Journal of Digital Convergence, 14(12),* 183-191. DOI : 10.14400/JDC.2016.14.12.183

[11] Jung Min Choi, Kwantae Cho, Dong Hoon Lee. (2012). Location-Based Authentication Mechanism for Server Access Control. *Journal of the Korea Institute of Information Security & Cryptology, 22(6),* 1271-1282.

[12] Hyung-Jin Mun, Hee-Young Jeong, Kun-Hee Han. (2016). Improved Trilateration Method on USN for reducing the Error of a Moving Node Position Measurement. *Journal of Digital Convergence, 14(5),* 301-307. DOI : 10.14400/JDC.2016.14.5.301

[13] National Marine Electronics Association. (2002). *NMEA 0183--Standard for interfacing marine electronic devices.* NMEA.

[14] Agrawal, M., & Mishra, P. (2012). A comparative survey on symmetric key encryption techniques. *International Journal on Computer Science and Engineering, 4(5),* 877.

[15] Delfs, H., & Knebl, H. (2007). Symmetric-key encryption. *Introduction to Cryptography.* 11-31. Berlin, Heidelberg. Springer.

홍 석 원(Suk-Won Hong) **[정회원]**

- 2011년 2월 : 경상대학교 컴퓨터과학과(공학박사)
- 1999년 3월 ~ 현재 : 경남도립거창대학 교무처 기획평가팀장
- 관심분야 : 네트워크, 보안, 멀티미디어
- E-Mail : swhong@gc.ac.kr