논문 17-42-10-22 The Journal of Korean Institute of Communications and Information Sciences '17-10 Vol.42 No.10
https://doi.org/10.7840/kics.2017.42.10.2012

신호증폭공격 방어를 위한 AP 목록 기반 자동차 원격 키 인증 방식

신 우 주◆, 손 규 식*, 남 승 엽°

Vehicle Remote Key Authentication Scheme based on AP List for Preventing Amplification Attack

Shin Woo Joo ◆, Kyu-Seek Sohn*, Seung Yeob Nam°

요 약

본 논문에서는 AP 목록을 위치 파악 정보로 이용하여 기존의 스마트키를 신호증폭공격으로부터 보호하는 새로운 인증 방식을 제안한다. 신호증폭공격은 스마트키와 차량 사이의 양방향 통신에서 신호를 추출하고 증폭하여 차량을 탈취하는 공격이다. 본 논문에서 제안하는 AP 목록을 이용한 방식은 차량과 스마트키 주변에서 측정되는 AP 목록의 정보를 이용하여 서로의 위치의 근접성을 확인하여 사용자에게 안전한 서비스를 제공한다. 제안된 AP 목록 인증 방식의 성능은 시뮬레이션 및 실험을 통해 평가한다.

Key Words : vehicle, amplification attack, authentication, security, AP (Access Point)

ABSTRACT

In this paper, we propose a new authentication system using Access Point (AP) list as the position information of car to prevent amplification attack on remote key entry system. Amplification attack can be used to open a car using the signal between a car and the corresponding smart key. The attacker catches the signal, amplifies and then replays the signal. In this paper, we propose a new authentication scheme, by which a vehicle can authenticate the corresponding smart key using AP list while mitigating amplification attack between them. The proposed scheme is evaluated through simulation and experiment.

Ⅰ. 서 론

현재 빠르게 성장하고 있는 정보통신기술의 발달로, 다양한 분야에서 IT 기술이 적용된다. 정보통신과 관련된 분야들뿐만 아니라 급격하게 변화하고 있는 자동차 산업에서도 이러한 IT 기술이 결합되고 있는 추세이다. 예를 들어, 가장 흔하게 사용되고 있는 내비게이션은 일반적으로 차량에 부착된 GPS 정보를 얻어 사용자에게 위치와 주변 지도 등의 정보와 목적지에 이르는 경로나 최단 거리 등을 알려줄 때 사용되

※ 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2017-2016-0-00313). 이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(2015R1D1A1A01058595).

◆ First Author : Yeungnam University, Department of Information and Communication Engineering, tlsdnwn1004@naver.com, 학생회원

° Corresponding Author : Yeungnam University, Department of Information and Communication Engineering, synam@ynu.ac.kr, 종신회원

* Hanyang Cyber University, Department of Hacking and Security, kssohn@hycu.ac.kr, 정회원

논문번호 : KICS2017-08-219, Received August 21, 2017; Revised September 5, 2017; Accepted September 6, 2017

고, 최근엔 주변 도로의 길 막히는 현상까지 파악하여 유류비 절감과 시간 단축 효과를 가져다주어 사용자에게 편리함을 제공하고 있다. 이러한 자동차 기술과 정보통신기술의 융합이 자동차 산업에도 많은 영향을 끼치고 있다. 편리함뿐만 아니라 안정성의 면에서도 많은 연구와 개발이 이루어지고 있다.

사용자에게 편리함을 주기 위해 개발된 제품 중 하나로, 현재 출시되는 차량에서 다양하게 나오고 있는 스마트키(smart key)가 있다. 스마트키는 차량과 양방향 통신을 하며, 키를 몸에 지니는 것만으로도 잠금장치를 해지할 수 있고 시동까지 걸 수 있는 최첨단 시스템이다. 벤츠 S클래스에서 처음으로 적용 됐으며, BMW, 아우디, 렉서스 등의 고급 차종을 위주로 적용되다가, 현재는 현대, 기아차 등 한국산 자동차를 포함한 대부분의 브랜드가 기본적인 사양으로 채택하고 있는 추세이다. 스마트키 시스템은 자동차 센서가 신호를 보내고 이 신호를 받은 스마트키가 응답 신호를 돌려보내는 방식으로 동작을 한다. 스마트 키는 ECU, Receiver, 실내 안테나, 실외 안테나로 구성되어 있으며, 소비자가 선택할 수 있도록 많은 기능을 접목 시키고 있다[1].

이러한 스마트키의 양방향 통신 시스템을 이용하여 악의적인 공격을 하려는 시도가 최근 발생하고 있다. 스마트키가 보내는 신호를 증폭하여 자동차 센서에 신호를 보내 실사용자가 잠금 해제를 시도한 것처럼 보이게 하는 신호증폭공격(Amplification attack)에 대한 사례가 증가하고 있다.

신호증폭공격이란, 서로 먼 거리에 떨어져 있는 자동차 센서와 스마트키 사이에서 각 장치가 발생시키는 신호를 증폭하여 상대편에 전달함으로써 운전자가 차량 근처에 있는 것처럼 위장하여 절도하는 공격이다[2-4].

예를 들어, Fig. 1에서, 자동차의 실소유주는 몸에 스마트키를 지닌 채 카페에서 커피 한잔을 시켜 자리에 앉아 책을 읽고 있다고 가정한다. 공격자 A는 차량 실소유주의 근처로 가서 스마트키에서 나오는 신호를 녹음할 준비를 하고 있고, 공격자 B는 자동차의 옆에 가서 대기하고 있다. 공격자 A가 소유주의 스마트키에서 나오는 신호를 추출하여 증폭한 후 공격자 B에게 전송하면, 신호를 받은 공격자 B는 이 신호를 재생하게 되고, 신호를 받은 차량은 실소유주가 잠금 해제를 시도한다고 판단하게 되어 인증을 허가한다. 그렇게 되면, 공격자 B는 차량 탈취에 성공하게 된다.

이런 문제에 대한 해결책으로 전문가들이 제안하는 것은 키의 신호가 사라지면 시동을 꺼버리는 방법을 제안하고 있다. 신호증폭의 한계가 있기 때문에 범위를 벗어나면 시동을 꺼버리자는 의견은 정상적인 스마트키의 배터리 방전과 고장의 경우 시동이 꺼져 버리게 되면 문제가 될 수도 있기 때문에 이러한 방법도 쉽지 않다. ADAC (Allgemeiner Deutscher Automobil-Club)에서 다양한 제조사의 차량에 테스트를 하였고, 24개의 차종에 이와 같은 절도 방법이 동작하는 것을 확인했다[5,6].

본 논문에서는 이러한 위험에 대응하기 위해 보안성을 향상시키는 해결 방안으로 새로운 인증 방식을 제안한다. 신호증폭공격은 스마트키가 인증을 시도할 때 스마트키가 실제 물리적으로 차량에 가까이 있는지 확인할 수 있으면 물리적으로 근접한 경우에만 인증을 허용함으로써 문제가 해결될 수 있다. 따라서 본 연구에서는 자동차의 위치정보와, 소지하고 있는 스마트키의 위치 정보를 활용하고자 한다.

본 논문에서는 사용자와 자동차의 위치정보로써 주변 AP (Access Point) 정보를 활용하는 방식을 제안한다. AP 목록 정보 비교에 기반한 시스템은 자동차 주변에서 측정되는 AP와 사용자의 스마트키 주변에서 측정되는 AP의 목록을 비교하여 서로 공통되는 AP가 많으면 가까운 거리에 있다고 판단할 수 있다. 서로 원거리에 있는 경우, 서로 공통되는 AP가 적기 때문에 서로 멀리 있다고 판단한다. 즉, 공격자가 인증을 시도 하고 있다고 판단하여 인증을 종료하게 된다. AP 목록을 비교하는 방법은 실외뿐만 아니라 실

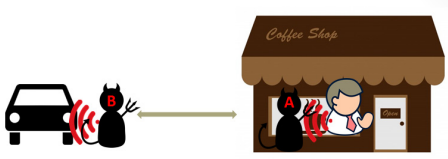


그림 1. 신호증폭공격의 예
Fig. 1. Example of amplification attack

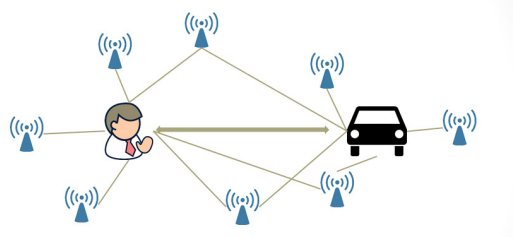


그림 2. AP 목록을 이용한 인증
Fig. 2. Authentication using AP list

내에서도 사용이 가능하며, 야외 주차장뿐만 아니라 실내 주차장에서 까지 사용할 수 있으므로 매우 유용하다(Fig 2).

본 논문은 다음과 같이 구성된다. 2장에서는 배경 지식에 대해 설명하며 AP 목록 기반 인증 방식에서 사용하는 Bloom Filter에 대해 설명한다. 3장에서는 GPS, 지자기를 이용한 기존 인증 프로토콜에 대해 설명하고, 4장에서는 AP 목록 기반 인증 방식에 대해 서술하며, 5장에서는 실험 결과 및 분석을 통해 기존 연구와 AP 목록 기반 인증 방식을 비교한다. 마지막으로 6장에서는 결론을 서술한다.

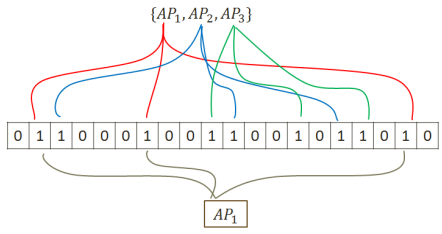
Ⅱ. 배경 지식

신호증폭공격에 대응하기 위해 사용자의 차량과 스마트키 사이의 위치정보를 비교하기 위해서 AP 목록 기반 인증 프로토콜에서 사용하는 블룸 필터(Bloom filter)에 대해 설명한다.

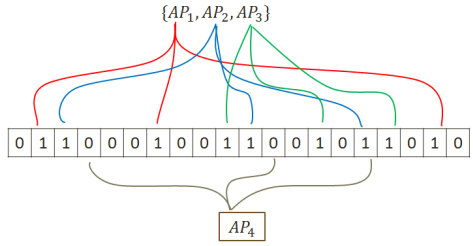
2.1 블룸 필터 (Bloom Filter)

블룸 필터는 특정 원소가 주어진 집합에 속하는지 여부를 검사하는데 사용되는 확률적 자료구조이다. m 비트 크기의 비트 배열 구조를 가지며, k 개의 서로 다른 해시 함수를 사용하여 입력된 원소에 대해 k 개의 해시 값을 균등한 확률로 출력한다. 블룸 필터에 데이터를 추가 하는 경우, 추가하려는 데이터에 대해 k 개의 해시 값을 계산한 다음, 각 해시 값에 대응하는 비트를 1로 설정한다. 블룸 필터에서 데이터를 검색하는 경우, 검색하는 데이터에 대해 k 개의 해시 값을 계산한 다음, 각 해시 값에 대응되는 비트가 전부 1이면 속한다고 판단하고 나머지의 경우에는 속하지 않는다고 판단한다[7,8].

예를 들어, Fig. 3에서 AP_1, AP_2, AP_3는 블룸 필터 bitmap(m=20, k=3)에 추가한 데이터이다. 검색하고자 하는 경우에는 검색하고자 하는 데이터에 대해서 k개의 해시 값을 계산한 후, k개의 해시 값에 해당하는 위치의 비트가 모두 1이라면 이미 등록이 되어있다고 판단한다. Fig. 3a를 보면, AP_1에 해당하는 3가지 해시 값이 1, 6, 19이므로 이에 해당하는 위치의 비트를 1로 설정한다. 찾고자 하는 데이터는 AP_1이고, 해당하는 모든 위치의 bit가 1이므로 이미 등록되어 있다고 판단한다. Fig. 3b의 경우에는 AP_4의 해시 값들에 대응하는 위치의 bit가 모두 1이 아니기 때문에 속하지 않는다고 판단한다.



(a) Search of AP_1 in Bloom filter, where AP_1,AP_2 and AP_3 are registered



(b) Search of AP_4 in Bloom filter, where AP_1,AP_2 and AP_3 are registered

그림 3. 블룸필터에서 데이터의 등록 및 검색
Fig. 3. Data addition and search of data in Bloom filter

블룸필터의 데이터 추가와 검사에 걸리는 시간은 $O(k)$로, 집합에 포함되어 있는 원소 수와 무관하다. 블룸 필터에서 데이터를 검사할 때 없는 데이터가 있다고 판단될 확률(false positive)은, 다음과 같이 계산할 수 있다. 데이터를 n개 추가 했을 때, 특정 비트가 0일 확률이 $(1-\frac{1}{m})^{kn}$이다. 따라서 원소를 검사할 때 k개의 해시 값이 모두 1이 될 확률은 $(1-(1-\frac{1}{m})^{kn})^k$가 되며, 이 값은 대략적으로 $(1-e^{\frac{kn}{m}})^k$가 된다[9,10].

블룸 필터에서 false positive가 일어날 확률은 비트 배열의 크기인 m이 클수록, 데이터 개수인 n이 작을수록 낮다. 해시 함수의 개수 k의 경우에는 일정 수준으로 증가할 때 까지는 false positive가 일어날 확률이 낮아지지만, 일정 수준 이상이 되면 false positive가 일어날 확률이 높아진다.

$$P_{err} = (1-P_0)^k = (1-(1-\frac{1}{m})^{kn})^k \approx (1-e^{-\frac{kn}{m}})^k \quad (1)$$

수식 (1)에서, P_{err}는 $k=\frac{m}{n}ln2$에 대해 최소화된다. 본 논문에서는 해시 함수로 SHA-256을 사용한다[11].

Ⅲ. 기존 연구

Shin[12]은 GPS, 지자기 센서를 이용하여 신호증폭 공격에 대한 문제를 해결하는 방안을 제시하였다. 이 방식에서는 차량과 스마트키에서 측정하는 GPS 값과 지자기 센서값을 위치 정보로 활용한다. 실외에서만 측정이 가능한 GPS를 보완하기 위해 지자기 센서를 결합하여 사용하였다(Fig 4).

Fig. 5는 GPS-지자기 인증 프로토콜을 나타내며, 다음과 같이 단계별로 동작한다. K_s는 사용자의 스마트키(client)와 차량(server) 간에 공유되는 대칭키를 의미하고, 차량 제조사의 의해서 미리 설정된다고 가정한다.

1) client에서 server로의 인증 시도를 위해, 난수(nonce) N_1과 스마트키 고유의 ID 정보를 전송하여 인증 절차를 시작한다.

2) server가 client의 인증 요청 신호를 받은 후 sever에서 난수 N_2를 생성한 후 N_1과 N_2를 암호화해서 $E_{K_s}(N_1,N_2)$를 전송한다. 여기에서 E는 암호화 연산을 의미하고, D는 복호화 연산을 의미한다.

그림 4. GPS 센서와 마그네틱 센서를 이용한 인증
Fig. 4. Authentication using GPS and magnetic sensors

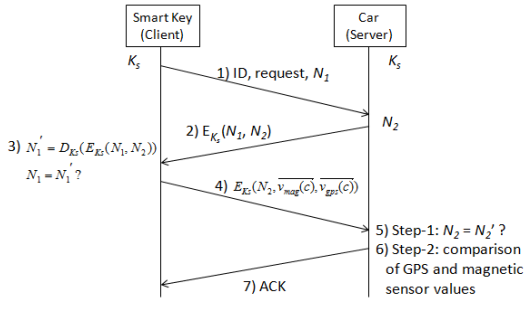


그림 5. GPS와 마그네틱 센서를 이용한 인증 프로토콜
Fig. 5. Authentication protocol using GPS and magnetic sensors

3) server로부터 받은 암호화된 N_1를 client가 가지고 있는 대칭키 K_s를 이용하여 아래와 수식(2)와 같이 복호화 하여 client에서 가지고 있는 N_1 과 같은지 비교한다.

$$(N_1',N_2')=D_{K_s}(E_{K_s}(N_1,N_2)) \tag{2}$$

4) 3단계 인증이 완료된 후, client는 server로부터 받은 N_2값과 client의 GPS 센서 값($\overrightarrow{v_{gps}(c)}$)과 지자기 센서 값($\overrightarrow{v_{mag}(c)}$)을 아래와 같이 암호화해서 server로 전송한다.

$$E_{K_s}(N_2,\ \overrightarrow{v_{gps}(c)},\overrightarrow{v_{mag}(c)}) \tag{3}$$

5) 서버 인증 1단계: server에서는 client로부터 전송된 정보가 정당한 정보인지를 확인하기 위해 client로부터 받은, 수식 (3)에 의해 암호화된 결과를 K_s을 이용하여 다음과 같이 복호화 한다.

$$D_{K_s}(E_{K_s}(N_2,\overrightarrow{v_{mag}(c)},\overrightarrow{v_{gps}(c)})) \tag{4}$$

수식 (4)을 통해 얻은 N_2의 값이 server에 저장한 N_2의 값과 동일한 값이라면 1단계 인증에 통과한 것이며, 이 경우에만 다음 인증 단계로 넘어간다.

6) 서버 인증 2단계: 1단계 인증에 성공한 client가 정상적인 사용자인지, 신호증폭공격을 하는 공격자인지 구별하기 위하여 client와 server의 GPS와 지자기 정보를 비교하는 2단계 인증을 시행한다. server의 GPS와 지자기($\overrightarrow{v_{mag}(s)},\overrightarrow{v_{gps}(s)}$)정보는 미리 server의 데이터베이스에 저장되어 있다고 가정한다. 아래 수식 (5)가 만족이 되면 사용자와 차량이 물리적으로 가까운 것으로 판정하며, 이 경우에 서버 인증 2단계가 통과한 것으로 판정한다.

$$\alpha_1\times|\overrightarrow{v_{gps}(c)}-\overrightarrow{v_{gps}(s)}| + \alpha_2\times|\overrightarrow{v_{mag}(c)}-\overrightarrow{v_{mag}(s)}|<\epsilon \tag{5}$$

server와 client가 가까운 곳에 위치한 경우 GPS 센서 값과 지자기 센서 값이 모두 서로 유사한 범위에 있을 확률이 높다. 따라서 수식 (5)에서 α_1, α_2, ϵ의

값을 적절히 설정하면 정상적인 사용자의 원격 키는 서버 인증 2단계를 통과할 수 있게 된다. 그렇지만, 해커가 원거리에 있는 사용자와 차량 간에 신호 증폭 공격을 하는 경우 원격키와 차량 간의 위치 차이로 인해서 GPS 센서 값과 지자기 센서 값이 모두 큰 차이를 보일 확률이 높아지기 때문에, 신호 증폭 공격의 경우에 수식 (5)에 기반한 서버 인증 2단계는 통과하기 어렵게 된다.

GPS의 정보를 실내에서는 활용할 수 없다는 단점을 가지고 있다. 지자기 센서는 주변의 환경에 따라 결과값의 차이가 크다는 점이 장점이 될 수도 있으나, 가까운 위치에도 불구하고 측정값이 크게 차이가 나는 경우도 있어 가까운 거리에서 인증이 통과되지 않을 확률이 존재하는 단점이 있다.

Ⅳ. 제안하는 AP 목록 기반 인증 방식

본 논문에서 제안하는 AP 목록 기반 인증 방식은 사용자의 스마트키와 자동차에서 측정하는 AP의 목록을 비교하여 인증하는 방식으로, 위치에 따라서 측정되는 AP들이 다르다는 점을 이용하여 신호증폭공격을 해결한다.

AP 목록을 비교할 때 비교 속도를 높이기 위하여 Bloom filter 방식을 사용한다. Bloom filter 방식을 사용하기 위해서, 최적화된 Bloom filter의 bitmap size와 해시 함수의 개수를 실험을 통해 얻는다.

본 논문에서 제안하는 AP 목록 기반 인증 방식은 자동차와 스마트키가 공유하고 있는 대칭키를 이용한 인증 뿐 아니라, 이에 추가로 자동차와 사용자의 스마트키의 위치 정보를 이용하기 위해 주변 AP를 각각 측정하여 상대편의 AP 목록과 비교하여 일치하는 정도에 따라 상대편을 검증하는 방법을 추가로 사용하는 방식이다. 자동차의 잠금을 해제하기 위한 시스템이므로 가능한 짧은 시간에 비교를 진행하여 사용자에게 편의성을 제공하며 보안성 있는 비교를 통해 안정성을 지향한다. 위치에 따라 측정되는 AP들이 다르다는 점을 이용하여 통신 프로토콜을 구축하고, 실험을 통해 판단에 대한 문턱값(threshold)을 구한다.

4.1 AP 목록 기반 인증 프로토콜

제안하는 프로토콜은 nonce에 기반해서 challenge-response 방식으로 대칭키를 이용한 인증을 사용한다는 점에서 3장에서 설명한 기존 방식과 유사하나, 다음과 같은 차이가 있다.

0) 제안하는 방식에서는 스마트키, 즉, client와 차량, 즉, server가 각각 주변에 있는 AP를 관측하여 목록으로 만든다는 점이 다르다. client가 관측한 AP의 목록을 $APlist_c$라고 하고, server가 관측한 AP의 목록을 $APlist_s$라고 한다. 스마트키에서의 AP 목록 측정은 스마트폰이 스마트키의 역할을 하는 경우에 대부분의 스마트폰이 이미 무선랜카드를 내장하고 있기 때문에, 쉽게 실현이 될 수 있다.

1) Fig. 5와 같이 스마트키가 인증을 시작하는 경우 스마트키가 인증 시작 신호를 주기적으로 전송하게 되면 스마트키의 배터리가 빨리 소모될 가능성이 있기 때문에, 제안하는 방식에서는 Fig. 6과 차량이 wake-up 신호를 보내서 스마트키가 wake-up 신호를 받으면 인증절차를 진행하도록 한다.

Fig. 6의 2), 3) 단계는 Fig. 5의 1), 2) 단계와 동일하다. Fig. 6의 4)에서 Fig. 5의 3)과 마찬가지로 client가 가지고 있는 N_1의 값과 server에서 받아 복호화한 N_1'이 동일한 값임을 확인하였다면 client의 AP 목록인 $APlist_c$를 server로부터 받은 N_2와 함께 암호화하여 server로 전송한다. 전송받은 데이터를 server에서 수식 (6)에 따라 복호화 하여, 2단계의 인증 방식을 적용한다.

$$D_{k_s}(E_{k_s}(N_2, APlist_c)) \tag{6}$$

6) 1단계 인증 : client로부터 받은 데이터를 수식 (6)에 따라 복호화 하여 client로부터 받은 N_2의 값이 server의 N_2의 값과 같은지를 확인하고 값이 같다면 인증이 성공한 것으로 판단하여 2단계 인증으로 넘어

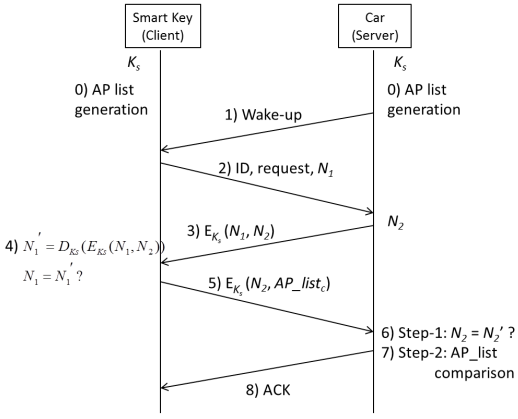


그림 6. AP 목록 기반 스마트 키 인증
Fig. 6. AP list-based smart key authentication

가게 된다. 만약 두 값이 같지 않다면 잘못된 인증자로 인식을 하여 실행을 종료한다.

7) 2단계 인증 : 수식 (6)에 따라 복호화 된 데이터 $APlist_c$를 server의 $APlist_s$와 비교하는 작업을 시행한다. 각 AP 목록을 비교하여 AP 목록간 일치율이 일정 수준 (threshold) 이상이면, 인증에 성공한 것으로 판단한다.

더 구체적으로는 공통 AP 비율, 즉 CAR(Common AP ratio)를 다음과 같이 정의하여 사용한다. S_c를 client, 즉, 스마트키에서 측정한 AP의 집합으로 정의하고, S_s를 server, 즉, 차량에서 측정한 AP의 집합으로 정의한다. 그러면, 스마트키와 차량 간 공통 AP의 비율인 CAR은 다음과 같이 정의할 수 있다.

$$\text{CAR} = \frac{|S_c \cap S_s|}{|S_c \cup S_s|} \quad (7)$$

CAR의 값이 특정 문턱값 δ를 넘는 경우에는 차량과 스마트키가 충분히 근접한 것으로 판단하여 인증을 통과시키고, CAR값이 δ를 넘지 않는 경우에는 차량과 스마트키가 멀리 떨어진 것으로 판단하여 인증을 통과시키지 않는 단계가 바로 제 2 인증 단계이다. δ의 값은 많은 실험을 통하여 0.4로 설정하였으며, 원거리와 근거리 판단 기준은 10m로 잡았다.

Fig. 7은 CAR 인증 방식을 설명하기 위하여 client와 server에서 측정한 AP 목록의 예를 보여준다. 그림에서 $S_c \cap S_s = \{AP_1, AP_3, AP_6\}$이고, $S_c \cup S_s = \{AP_1, AP_2, AP_3, AP_4, AP_5, AP_6, AP_7\}$이기 때문에, CAR의 값은 $|S_c \cap S_s| / |S_c \cup S_s| = 3/7 = 0.43$이 된다. 이 값은 $\delta = 0.4$보다 크기 때문에 제 2 인증 단계는 차량과 사용자의 스마트키가 가깝다고 판정하게 된다.

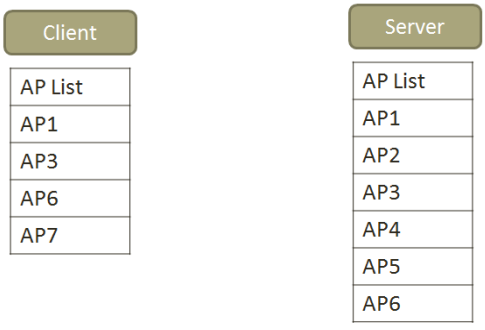


그림 7. 클라이언트(스마트 키)와 서버(차량)에서 측정한 AP 목록의 예
Fig. 7. Example of AP lists for a client and a server

제안하는 인증 방식의 안전성은 간략하게 다음과 같이 분석할 수 있다. 먼저 기존에 잘 알려진 재전송 (replay) 공격의 경우 Fig. 6에서 보는 것과 같이 client가 생성하는 난수 N_1과 server가 생성하는 난수 N_2를 서로 확인하므로 단순한 재전송 공격은 성공이 어렵게 된다. 또한, 신호증폭공격의 경우 스마트키가 자동차로부터 멀리 떨어져 있을 때 자동차쪽에 위치한 해커가 자동차 주변의 AP 목록을 미리 파악하여 일치도를 높이려는 시도를 생각해 볼 수 있다. 그렇지만, 자동차 주변의 AP 목록을 미리 파악하였다 할지라도 그러한 AP의 목록이 스마트키를 통하지 않으면 차량이 받아들이지 않는다. 그 이유는 인증 단계에 비밀키 기반 인증이 포함되어 있기 때문이다. 따라서, 미리 파악한 AP의 목록 정보를 스마트키에 입력할 수 없다면 이러한 공격도 유효한 공격이 될 수 없다. 스마트키 시스템을 대상으로 직접적인 해킹 공격은 이 논문의 범위를 벗어나며, 이 논문에서는 스마트키와 차량간 신호증폭공격 문제로 범위를 한정한다.

4.2 Bloom filter 방식과 binary search 방식의 비교

제안하는 방식에서는 스마트키와 차량 간 근접성 확인을 위해서 스마트키가 관측한 AP의 목록과 차량이 관측한 AP의 목록을 비교한다. 이 때, 서로 다른 AP 목록간 비교를 위해 잘 알려진 binary search 방법을 고려할 수 있으나, 본 논문에서는 비교시간을 줄이

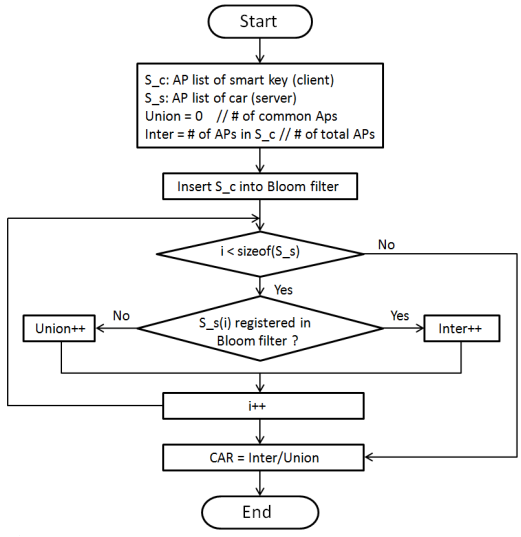


그림 8. 블룸필터를 이용한 와 의 비교에 기반한 CAR 값의 계산
Fig. 8. CAR calculation based on comparison of and using Bloom filter

기 위해서 Bloom filter 기반 방법을 사용한다.

Fig. 8에서 S_c의 AP 목록을 Bloom filter bitmap에 저장하고, S_s의 AP 목록을 bitmap과 비교하여 CAR을 구하는 알고리즘을 보여준다.

Binary search의 경우에는 데이터를 정렬하지 않으면 사용할 수 없기 때문에 Quick sorting을 이용하여 데이터를 정렬하였다. 반면, Bloom filter 방식은 데이터 정렬을 필요로 하지 않는다.

Fig. 9는 binary search 방식과 Bloom filter 방식 간 비교 연산 시간을 data의 개수에 따라 시뮬레이션으로 분석한 결과를 보여준다. 두 비교 연산을 분석해 보았을 때, binary search의 경우에는 데이터를 정렬하여야 비교, 검색을 할 수 있기 때문에 데이터가 증가하면 할수록 실행에 걸리는 시간이 AP 개수의 제곱 속도로 증가한다. Bloom filter의 경우에는 Fig. 8에 나타난 것과 같이 데이터를 정렬할 필요가 없고, 해쉬 함수 연산 시간이 짧아 AP 목록 비교 시간이 수 μs 정도로 binary search 방식에 비해서 매우 짧은 것을 확인할 수 있다.

따라서, AP 목록을 비교하기 위한 방법으로는 Bloom filter가 연산 시간 측면에서 binary search에 비해 좋다는 사실을 알 수 있다.

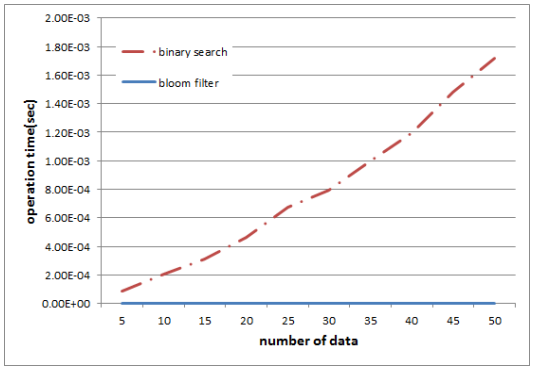


그림 9. 블룸필터를 이용한 AP 목록 비교 시간과 이진 탐색을 이용한 AP 목록 비교 시간의 비교
Fig. 9. Comparison of matching time between Bloom filter and binary search

4.3 Bloom filter 최적화

본 논문에서 블룸 필터를 사용하기 위하여 최적화된 bitmap size와 해시 함수의 개수(k)를 구하고자 한다. 충돌 확률은 0.1% 이하로 설정하였다. 해시 함수는 SHA-256을 사용한다[13,14].

Fig. 10은 해시 함수의 증가에 따라 연산 시간을 측정한 결과를 보여준다. 예측할 수 있는 것처럼 해시

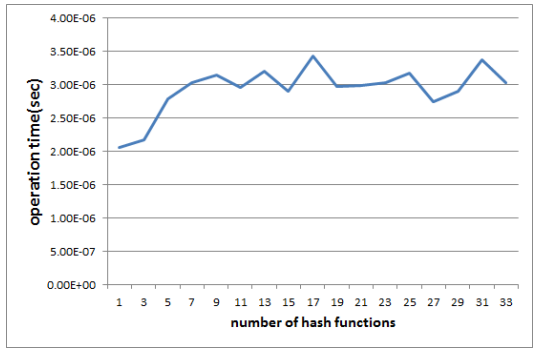


그림 10. 해쉬 함수 개수의 증가에 따른 연산 시간의 변화
Fig. 10. Calculation time for various numbers of hash functions

함수의 개수가 증가할수록 연산 시간이 증가하는 경향이 있는 것을 알 수 있다.

Fig. 11에서는 Bloom filter에 50개의 AP를 등록하는 경우에 주어진 해시 함수의 개수(k)에 대해서 충돌 확률을 0.001로 유지할 수 있는 최소의 bitmap size (m)을 수식 (1)에 따라서 계산한 결과를 보여준다. 해시 함수의 개수가 1일 때에는 필요한 bitmap size는 크지만 점차 감소하여 5부터는 비교적 감소 이득이 크지 않음을 알 수 있다.

AP의 MAC 주소는 48bit이다. n개의 AP 정보를 개별적으로 저장하려면 48n bit의 공간이 필요하다. AP 정보를 Bloom filter에 저장하는 경우에 Bloom filter의 bitmap 크기(m)가 개별적으로 저장할 때 필요한 공간보다 크다면 Bloom filter를 사용할 필요가 없어지기 때문에 다음과 같은 m에 대한 제약 조건을 얻을 수 있다.

$$m \leq 48n \tag{8}$$

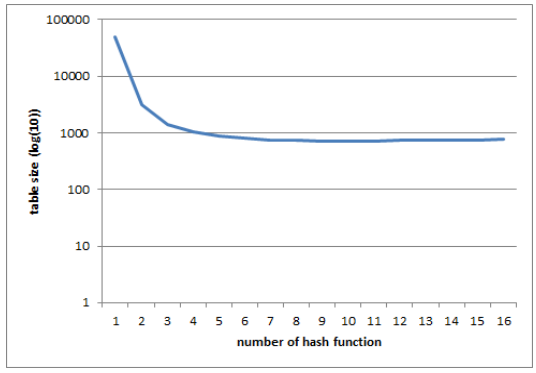


그림 11. 해시 함수 개수의 증가에 따른 충돌 확률을 유지할 수 있는 블룸필터의 최소 크기
Fig. 11. Bitmap size as a number of hash function

하나의 장소에서 관측할 수 있는 AP의 개수가 50을 넘지 않는다고 가정하면 $n \leq 50$ 이고, 이 조건과 수식 (8)을 결합하면 다음 조건을 얻을 수 있다.

$$m \leq 48 \times 50 = 2400$$

Fig. 11에 따르면 $m \leq 2400$ 조건을 만족하는 해시 함수의 개수(k)의 범위는 $k \geq 3$가 된다.

Fig. 10에 따라서 연산 시간은 해시 함수의 개수(k)에 따라 증가하기 때문에 수식 (8)의 조건을 만족하면서 연산 시간을 최소화할 수 있는 k의 값은 3이 되고, 이 때 bitmap size(m)은 Fig. 11에 의해 1423bit가 된다. 따라서 본 논문에서는 bitmap size(m)을 1423으로 설정하고, 해시 함수의 개수(k)를 3으로 고정한다.

V. 실험 결과 및 분석

GPS, 지자기를 이용하는 방식과 본 논문에서 제안하는 AP 목록 기반 방식의 성능을 시뮬레이션을 통해 비교 및 평가 한다. 두 방식의 성능은 근거리 탐지 오차율과 원거리 탐지 오차율에 관해서 평가한다.

AP 목록 기반 방식의 측정은 차량 센서와 스마트키를 두 개의 라즈베리 파이보드에 구현하여 실험하였고, 라즈베리 파이의 버전은 3이다. 라즈베리 파이에서 운영체제는 리눅스이며, python을 활용하여 AP 목록을 수집하였다. 사양은 Intel(R) Core(TM) I5-4590 CPU, 메모리 8GB, 64비트 운영체제이다.

AP 목록은 2초간 수집하며, 반복 실험을 위해서 2초가 지나면 측정한 자료를 기록하고, 목록을 지우도록 했다. 실험은 초기 10m 이내의 근거리 실험과 10m 이상의 원거리 실험으로 나누어 진행하였다.

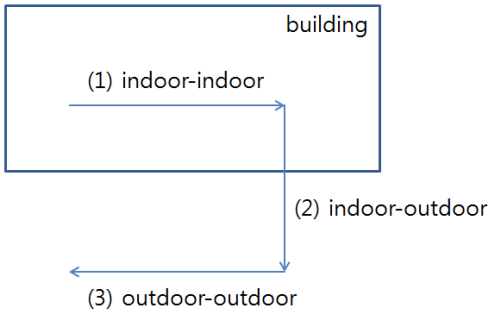


그림 12. 차량과 스마트 키 사이의 상대적인 위치 및 거리를 고려한 다양한 실험 환경
Fig. 12. Diverse experiment scenarios describing the relative positions between a car and a smart key

Fig. 12는 세 가지 서로 다른 실험 환경을 보여준다. (1)은 차량과 스마트키가 모두 실내에 있는 경우를 나타내고, (2)는 차량과 스마트키 가운데 하나는 실내, 하나는 실외에 있는 상황, (3)은 차량과 스마트키가 모두 실외에 있는 상황을 나타낸다.

근거리의 경우 오차의 개념은 차량과 스마트키 사이의 거리가 가깝다고 인식이 되어야하나 원거리로 인식될 경우이며, 원거리의 경우는 차량과 스마트키 사이의 거리가 멀다고 인식이 되어야하나 근거리로 인식 되는 경우 오류가 된다.

5.1 근거리에 대한 실험 결과

Server와 client 노드 사이의 거리가 근거리의 경우 각 방식들의 오차율을 비교 분석한다. 실험은 Fig. 12의 (1), (2), (3)의 경우에 대해 차량 노드와 스마트키 노드의 간격을 1m부터 5m까지 1m씩 증가시키면서 진행하였다.

1~5m의 근거리에서는 AP 목록을 비교했을 때 자동차와 스마트키 사이의 거리가 가깝다고 인식을 하여야 올바른 판단이 된다. 즉, 제안하는 방식에서는 높은 CAR이 나와야 정상이고, CAR 값이 0.4보다 작을 때 오류가 된다.

Table 1~3에서 AP list 기반 방식이 GPS-지자기 센서를 이용하는 방식에 비해서 낮은 오차율을 나타내는 것을 확인할 수 있다.

표 1. 근거리 실험에서의 오차율(indoor-indoor)
Table 1. Error probability of AP-list-based and GPS-Magnetic-based methods for short distances (indoor-indoor scenario)

Distance	AP list method	GPS-Magnetic method
1m	0%	0%
2m	0%	50%
3m	0%	10%
4m	0%	50%
5m	0%	100%

표 2. 근거리 실험에서의 오차율(indoor-outdoor)
Table 2. Error probability of AP-list-based and GPS-Magnetic-based methods for short distances (indoor-outdoor scenario)

Distance	AP list method	GPS-Magnetic method
1m	0%	0%
2m	0%	0%
3m	0%	20%
4m	0%	80%
5m	0%	90%

표 3. 근거리 실험에서의 오차율(outdoor-outdoor)
Table 3. Error probability of AP-list-based and GPS-Magnetic-based methods for short distances (outdoor-outdoor scenario)

Distance	AP list method	GPS-Magnetic method
1m	0%	0%
2m	0%	20%
3m	0%	20%
4m	0%	100%
5m	30%	100%

5.2 원거리에 대한 실험 결과

Server와 client 노드 사이의 거리가 원거리의 경우 각 방식들의 오차율을 비교 분석한다. 실험은 Fig. 12의 (1), (2), (3)의 경우에 대해 차량 노드와 스마트키 노드의 간격을 10m부터 50m까지 10m씩 증가시키면서 진행하였다.

10~50m의 원거리에서는 AP 목록을 비교했을 때 자동차와 스마트키 사이의 거리가 멀다고 인식을 하여야 올바른 판단이 된다. 즉, 제안하는 방식에서는 낮은 CAR이 나와야 정상이고, CAR 값이 0.4 이상이면 오류가 된다.

Table 4~6에서 AP list 기반 방식이 GPS-지자기 센서를 이용하는 방식에 비해서 차량 노드와 스마트키 노드가 멀리 떨어진 경우에도 대체로 더 낮은 오류율을 보임을 확인할 수 있다.

표 4. 원거리 실험에서의 오차율(indoor-indoor)
Table 4. Error probability of AP-list-based and GPS-Magnetic-based methods for long distances (indoor-indoor scenario)

Distance	AP list method	GPS-Magnetic method
10m	20%	100%
20m	0%	100%
30m	0%	0%
40m	0%	0%
50m	0%	0%

표 5. 원거리 실험에서의 오차율(indoor-outdoor)
Table 5. Error probability of AP-list-based and GPS-Magnetic-based methods for long distances (indoor-outdoor scenario)

Distance	AP list method	GPS-Magnetic method
10m	0%	0%
20m	0%	0%
30m	0%	0%
40m	0%	0%
50m	0%	0%

표 6. 원거리 실험에서의 오차율(outdoor-outdoor)
Table 6. Error probability of AP-list-based and GPS-Magnetic-based methods for long distances (outdoor-outdoor scenario)

Distance	AP list method	GPS-Magnetic method
10m	0%	0%
20m	20%	10%
30m	0%	0%
40m	0%	0%
50m	0%	0%

Ⅵ. 결 론

신호 증폭 공격은 차량 실소유주와 차량이 멀리 떨어져 있을 때, 스마트키와 자동차 간 인증 신호를 증폭해 전달함으로써 인증단계를 해킹하는 방식이다.

본 논문에서는 이러한 신호 증폭 공격을 해결하기 위해 새로운 인증 방식을 제안하였다. 자동차와 사용자의 스마트키의 위치 정보를 고려하여 위치가 가깝지 않다고 판단되면 실소유주가 아님을 판단하도록 하였다. 본 논문에서는 위치정보 추정을 위하여 AP 목록을 이용하였다.

Bloom filter를 이용하여 차량의 AP 목록과 스마트키의 AP 목록을 더 빠르게 비교할 수 있는 방법을 제안하였으며, 실험을 통하여 제안하는 방식이 기존의 다른 방식에 비해 근거리 또는 원거리 환경 모두 더 낮은 오류율로 신호증폭 공격을 방어할 수 있음을 확인하였다.

추후 연구로는 좀 더 현실적인 테스트 환경, 즉, 자동차 ECU 기반 인증 시스템 및 스마트키 환경에서 실험을 통하여 추가 검증을 수행하고, AP목록 전송으로 인한 추가 트래픽 부하를 분석하고자 한다.

References

[1] Mroczkowski RS, Ritchie LT, *Smart key system*, US Patent 5,157,244, 1992.

[2] A. Greenberg, *Radio attack lets hackers steal 24 different car models*, Retrieved Aug. 21, 2017, from https://www.wired.com/2016/03/study-finds-24-car-models-open-unlocking-ignition-hack/.

[3] S. W. Lee, *Smart key exposed in remote hacking system*, Retrieved Aug. 21, 2017,

from http://techholic.co.kr/archives/51169.

[4] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlides, “Lock it and still lose it-on the security automotive remote keyless entry systems,” *25th USENIX Secur. Symp.*, Austin, Texas, Aug. 2016.

[5] A. Francillon, B. Danev, and S. Capkun, “Relay attacks on passive keyless entry and start systems in modern cars,” *NDSS*, San Diego, CA, Jan. 2011.

[6] B. S. Baek, *Smart-key car, easy to be stolen*, Retrieved Aug. 21, 2017, from http://m.zdnet.co.kr/news_view.asp?article_id=20170504090559.

[7] M. Ripeanu and A. Iamnitchi, *Bloom Filters - Short tutorial*, Retrieved Aug. 21, 2017, from http://people.cs.uchicago.edu/~matei/PAPERS/

[8] K. M. Yoo, H. S. Sang, E. H. Kyeong, H. S. Won, Y. S. Kim, and Y. C. Kim, “Efficient bloom filter based destination address monitoring scheme for DDoS attack detection,” *J. KICS*, vol. 33, no. 3, pp. 152-158, 2008.

[9] J. H. Jin, T. J. Lee, and S. Y. Nam, “DDoS defense using address prefix-based priority service,” *J. Korea Soc. Simulation*, vol. 18, no. 4, pp. 207-217, Dec. 2009.

[10] M. Mitzenmacher, “Compressed bloom filters,” *IEEE/ACM Trans. Netw.*, vol. 10, no. 5, pp. 604-612, Oct. 2002.

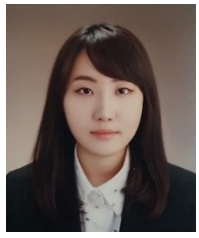
[11] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, Y. Markov, A. P. Bianco, and C. Baisse, *Announcing the first SHA1 collision*, Retrieved Sept. 5, 2017, from https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html

[12] W. J. Shin, S. J. Baek, S. Djuraev, Y. M. Jeon, S. G. Yoon, and S. Y. Nam, “Authentication scheme to prevent amplification attack on vehicle remote key entry system,” in *Proc. KICS Winter Conf.*, pp. 1180-1181, Jan. 2017.

[13] A. Pagh, R. Pagh, and S. S. Rao, “An optimal bloom filter replacement,” in *Proc. 16th Annu. ACM-SIAM Symp. Discrete Algorithms*, pp. 823-829, Vancouver, British Columbia, Jan. 2005.

[14] C. Jeong and Y. Kim, “Implementation of efficient SHA-256 hash algorithm for secure vehicle communication using FPGA,” in *Proc. Int. SoC Design Conf.*, pp. 224-225, Jeju, Korea, Nov. 2014.

신 우 주 (Shin Woo Joo)



2015년 2월 : 영남대학교 정보통신공학과 학사

2017년 8월 : 영남대학교 정보통신공학과 석사

<관심분야> 네트워크 보안, 통신공학, 보안

손 규 식 (Kyu-Seek Sohn)

1982년 2월 : 한양대학교 전자공학과 학사

1984년 2월 : 한양대학교 전자통신공학과 석사

2003년 8월 : KAIST 전기 및 전자공학과 박사

2004년 3월~현재 : 한양사이버대학교 해킹보안학과 부교수

<관심분야> IoT 보안, 네트워크 보안, 정보보호

남 승 엽 (Seung Yeob Nam)

2004년 8월 : KAIST 전기 및 전자공학과 박사

2007년 3월~2013년 2월 : 영남대학교 정보통신공학과 조교수

2013년 3월~현재 : 영남대학교 정보통신공학과 부교수

<관심분야> 네트워크 보안, 미래 인터넷, IoT 보안