무인항공기 환경에서 Wi-Fi 취약점 보완 방안 연구

김택중*, 홍남수*, 김형주**, 강정호*, 전문석*
*숭실대학교 컴퓨터학과
**KT R&D Center
e-mail:kimmycode23@ssu.ac.kr

A Study of Wi-Fi Vulnerability Supplementation Method in Unmanned Aerial Vehicle Environment

Taekjung Kim*, Namsu Hong*, Hyungjoo Kim**, Jung-Ho Kang*,
Moon-Seog Jun*
*Dept of Computer Science & Engineering, Soongsil University
**KT R&D Center

요 약

무인항공기의 시장이 성장하면서 많은 무인항공기 수요와 개체 증가가 이루어지고 있다. 그에 따라 무선네트워크 해킹 위협에 대한 우려가 높아지고 있다. 실제로 판매되고 있는 소비자용 무인항공기가 해킹에 취약하다는 사례가 발생하면서 무인항공기의 네트워크 보안성을 높이는 것이 필요하다고 판단하였다. 본 논문에서는 기존 Wi-Fi는 가상AP의 비밀번호를 이용해 네트워크에 접속한 것과 다르게 사용자의 디바이스 정보를 활용하여 본인의 디바이스 정보를 이용한 접근이 아니면 네트워크에 접속할 수 없는 방안을 제안한다.

1. 서론

최근 정부가 26억 달러 규모의 무인항공기 시장이 10년 내에 4배 이상의 시장으로 성장할 것으로 예측하면서 국토교통부에서는 무인항공기산업 육성과 발전을 위해 '무인항공기 규제혁신 및 지원 방안'을 추진하고 있다 [1].

무선 네트워크 환경을 기반으로 하고 있는 무인항공기에 대한 해킹 위협이 무인항공기 수요 및 개체 증가로 인하여 높아지고 있다. 2015년도 라스베이거스에서 열린 보안관련 컨퍼런스 '데프콘(DefCon)'에서 소비자용 무인항공기가 해킹에 취약하다는 사실을 공개하여 무인항공기를 강제로 추락시킬 수 있다는 것을 보여주었다.

기존 무인항공기 통신 방식은 크게 블루투스, 셀룰러 시스템, 위성통신, Wi-Fi로 나눌 수 있다. 본 논문에서 활용될 Wi-Fi는 하나의 채널로 제어신호와 함께 실시간 영상 전송이 가능한 장점을 지니고 있다. 하지만 출력이 제한되어 있어 무인항공기를 제어할 통신범위에 대한 제약이 존재하는 단점이 있다. 국내 무인항공기 대부분은 비면허 Industrial Scientific Medical Band(ISM) 대역인 2.4 GHz 혹은 5.8 GHz 사용한다. 이를 최근 정부 지원 방안으로 2015년 12월에 WRC-15에서 무인항공기 지상제어 전용으로 분배 된 5,030~5,091 MHz의 61MHz 대역을 국내에서 이용할 수 있도록 개정하였다. 이를 통해 10mW로 제한되었던 출력세기가 10W까지 허용하는 결과를 얻게 되었고 높아진 출력세기를 통해 조종거리가 늘어나게 되었기에 Wi-Fi를 활용한 환경을 사용한다.

기존 Wi-Fi 네트워크 연결 방식을 사용자마다 전용의 가상 Access Point(AP)를 할당하는 방식을 활용하여 가상 AP가 오직 한 사용자 기기의 속성에 맞출 수 있게 함으로써 네트워크의 보안성을 높일 수 있다[2].

본 논문의 구성은 다음과 같다. 2장에서는 기존 무인항공기가 사용하고 있는 통신 방식에 대해 서술하였고 3장에서는 해킹으로 인한 피해를 미연에 방지하기 위한 개인 네트워크 방식에 대해 작성하였다. 4장에서는 논문에 대한 결론과 향후 계획에 대해 작성하였다.

2. 관련 연구

2.1 블루투스

블루투스(Bluetooth)는 근거리(10m 이내)에서 PC 주변기기나 가전기기 등을 무선으로 손쉽게 연결하며 데이터를 주고 받을 수 있는 근거리 무선기술표준이다[3]. 블루투스의 사용 주파수대역은 ISM대역인 2400~2483.5 MHz를 사용한다. 총 79개의 채널을 사용하기 때문에 주파수 간섭 문제에 대한 방안으로 주파수 호핑 기법을 사용한다. 주파수 호핑은 Direct Sequence(DS)와 Frequency Hopping(FH) 방식으로 나눌 수 있고 DS방식은 의사랜덤성 부호계열에 의해 반송파를 직접 변조하는 방식이며

※ This work was supported by the ICT R&D program of MSIP/IITP. [R0112-14-1061, The analysis technology of a vulnerability on an open-source software, and the development of Platform]

FH는 정해진 패턴에 따라 불연속적으로 반송파 주파수를 편이 시키는 것이다. 이 중에서 FH방식을 무인항공기에서 주로 이용하고 있다. 일반적으로 데이터 전송이 많이 필요하지 않은 무인항공기 제어에는 적합하지만 영상정보에 데이터와 사진 등에 있어서 자료전송이 힘들다는 단점이 있다.

2.2 셀룰러 시스템

셀룰러 시스템이란 기지국을 공간적으로 확장하여 주파수 자원을 효율적으로 활용하는 서비스를 제공하는 것으로 주파수 자원 부족을 해소할 수 있는 장점이 있다[5]. 게다가 국내에서는 촘촘한 망이 존재하기에 장소에 구애를 받지 않는 통신이 가능하다. 하지만 셀룰러 시스템을 이용하기 위해서는 통신사와 연계를 해야 하며 그에 따른 통신료가 청구된다는 점, 공중에서 사용하기엔 셀룰러 망이 개설되어 있지 않다는 것 때문에 고도에 따른 제한이 있는 무인항공기통신에 적용하기 어렵다.

2.3 위성통신

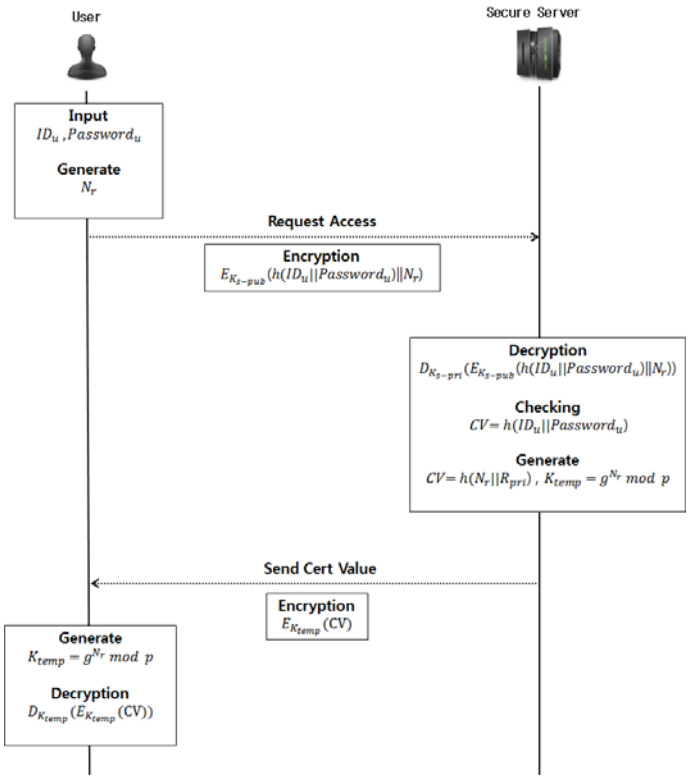
위성통신은 인공위성을 이용하여 1~30 GHz 정도의 넓은 대역폭 범위에서 작동하는 통신이다. 위성통신은 통신을 할 때 특정국가 전역 등을 통신 권역으로 할 수 있기 때문에 광대역성을 지니고 있으며 1 GHz 이상의 높은 마이크로파를 이용하기에 고품질의 특징을 가지고 있을 뿐만 아니라 재해의 발생에도 제약을 받지 않는 내재해성까지 지니고 있다. 하지만 전파의 왕복시간이 발생하기에 음성통신을 할 때 전송이 지연된다는 단점과 전력원으로 태양전지를 이용하기 때문에 태양간섭에 따른 기후에 영향을 받아 순간적인 통신두절 현상이 나타날 수 있다.

2.4 Wi-Fi

Wi-Fi는 컴퓨터 네트워킹 기술을 무선화한 것으로 High Fidelity(Hi-Fi)를 활용하여 무선 환경에서도 유선랜과 같은 수준으로 데이터 통신이 가능하도록 한다[4][5]. 미국의 IEEE 802.11 표준을 준수하고 있으며 Internet of Things(IoT)환경에 다양하게 적용되고 있다. 비면허 대역인 ISM 대역을 이용하는데 해당하는 대역은 2.4 GHz, 5 GHz 대역의 주파수이다. 장점으로는 하나의 채널을 통해 제어 신호와 함께 실시간으로 고속으로 데이터 전송이 가능하다는 점이 있다. 단점으로는 Wi-Fi 모듈의 출력제한이 존재하기 때문에 통신범위의 제약이 존재한다는 것이지만 최근 정부의 출력세기 제한이 완화되면서 통신범위가 넓어졌다. 또 다른 단점은 비면허 대역인 ISM 대역을 활용하기에 통신범위가 넓어질 경우 같은 채널을 사용하는 기기들 간 간섭문제가 발생할 수 있다는 점이다.

3. 제안 내용

3.1 User 등록



(그림 1) 사용자 등록 절차

Step1. User의 ID, Password를 입력하고 N_r 난수를 생성한다.

Step2. ID, Password를 해시하고 N_r 난수를 연접하여 Secure Server의 공개키로 암호화하여 전송한다.

Step3. Secure Server는 개인키로 복호화 하여 ID, Password의 해시값과 N_r 을 얻는다.

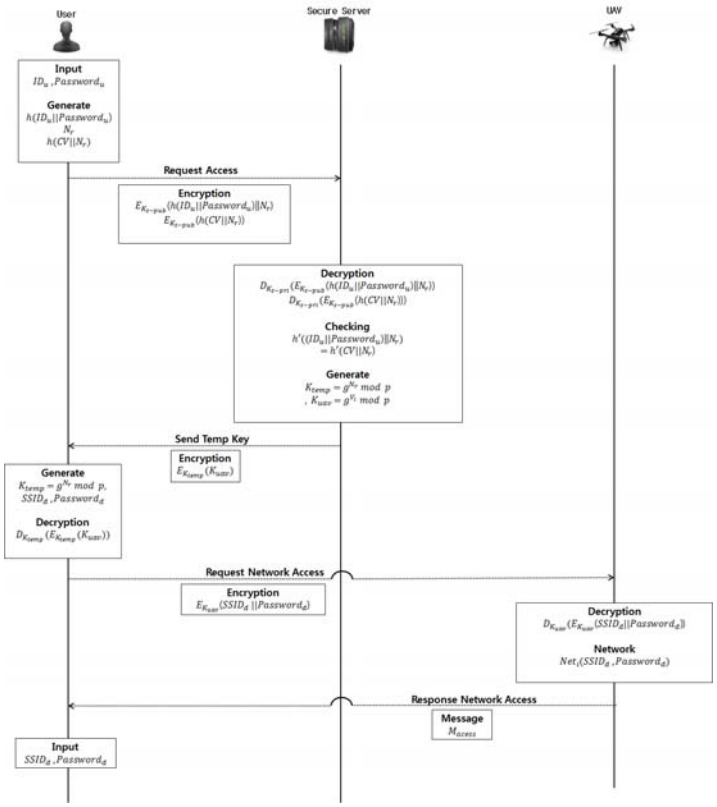
Step4. ID, Password의 해시값을 통해 등록된 유저인지 확인하고 아닐 경우 인증값 CV를 생성한다.

Step5. $K_{temp} = g^{N_r} \bmod p$ 를 이용해 임시키를 만들어 인증값 CV를 암호화하여 User에게 전송한다.

Step6. User는 N_r 난수를 이용해 임시키를 생성하고 이를 복호화하여 인증값 CV를 얻는다.

3.2 개인 네트워크 설정

Step1. User의 ID, Password의 해시값을 생성하고 새로 생성한 N_r 난수와 연접하여 한 번 더 해시를 한다. 기존 등록된 User가 맞는지 확인하기 위해 발급받은 CV값과 N_r 값을 연접하여 해시값을 만들고 이를 Secure Server의 공개키로 암호화하여 전송한다.



(그림 2) 네트워크 생성 연결

Step2. Secure Server는 CV값을 이용해 N_r값을 얻어 CV값과 N_r을 계산하여 전송받은 $h(ID_u||Password_u)||N_r$값과 일치하는지 비교한다. 기존 등록된 User일 경우 $K_{temp} = g^{N_r} \bmod p$를 이용해 임시키를 생성하고 무인항공기의 키 $K_{uav} = g^{V_i} \bmod p$를 임시키로 암호화하여 User에게 전송한다.

Step3. User는 N_r 난수를 이용해 임시키를 생성하고 이를 복호화하여 무인항공기 키 값 K_{uav}을 얻는다.

Step4. User는 디바이스의 SSID와 Password를 무인항공기 키로 암호화하여 무인항공기에 전송한다.

Step5. 무인항공기는 전송받은 SSID와 Password를 복호화하여 SSID와 Password를 이용해 Wi-Fi 네트워크를 생성한다.

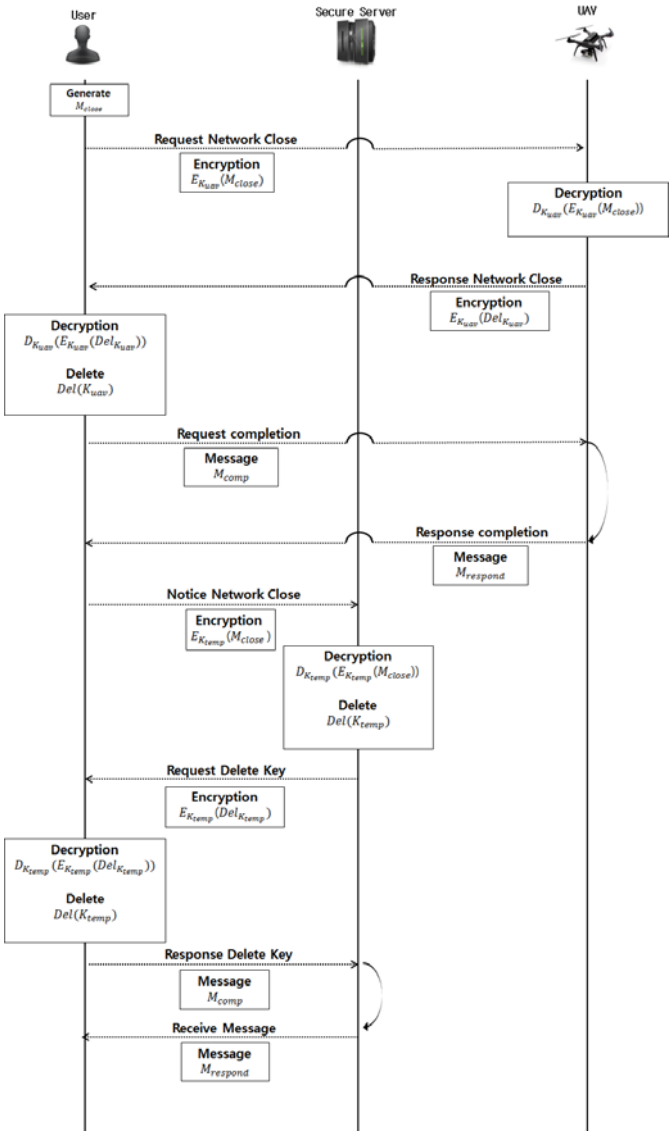
Step6. 생성된 네트워크에 접근할 수 있음을 알리는 메시지를 User에게 전송하면서 User 디바이스와의 개인 네트워크 연결이 확립된다.

3.3 연결 종료

Step1. User는 연결을 종료하겠다는 메시지를 무인항공기에게 요청한다.

Step2. 무인항공기는 메시지를 복호화하여 확인하고 응답메시지로 K_{uav}키 폐기를 요청한다.

Step3. User는 키 폐기 요구에 따라 K_{uav}를 폐기하고 무인항공기에게 키폐기를 완료했다는 메시지를 전송한다.



(그림 3) 네트워크 연결 종료

Step4. 무인항공기는 수신을 완료했다는 메시지로 응답한다.

Step5. 무인항공기의 수신완료 메시지를 받은 User는 Secure Server에게 무인항공기와의 네트워크 종료를 알리는 메시지를 전송한다.

Step6. Secure Server는 사용된 임시키 K_{temp}를 폐기하고 User에게도 임시키를 폐기하라는 메시지를 전송한다.

Step7. User는 메시지에 따라 임시키를 폐기하고 완료했다는 메시지를 Secure Server에게 전송한다.

Step8. Secure Server가 키 폐기에 대한 응답을 확인하고 연결 종료를 선언함으로써 Wi-Fi 네트워크 연결과정이 종료된다.

4. 결론

본 논문에서는 무인항공기 해킹 위협 증가에 따른 해결책으로 기존 Wi-Fi 네트워크 연결 방식을 User 디바이스의 속성에 맞춰 전용의 가상 AP를 할당하는 방식을 활용함으로써 네트워크의 보안성을 높일 수 있는 방안을 제시하였다.

향후 필요한 연구는 Wi-Fi의 환경에서 비정상적인 연결종료가 발생했을 때 네트워크에 재접속하기 위해 새로운 임시키 값을 생성하여 무인항공기와 연결하는 것이 아닌 기존에 활용한 임시키 값을 통해 빠르게 Wi-Fi 환경을 복구하는 방안이 필요하다.

참고문헌

[1] 손성화, 강진혁, 박경준 “드론 무선통신의 개요 및 이슈,” 한국통신학회 2006.01.

[2] 이남세, 이주호, 정충교 “PS-Net : 개인별 보안 Wi-Fi 네트워크”, 한국통신학회, 2015.03

[3] Bluetooth SIG, “Specification of the Bluetooth System”, Core v1.1, 2001.

[4] IEEE COMPUTER SOCIETY LAN MAN STANDARDS COMMITTEE, “Wireless LAN Medium Access Control(MAC) and physical layer(PHY) specification”, 1997.

[5] 신수복, 예홍진, 김강석 “무선 네트워크 환경에서 모바일 디바이스 기반 효율적인 사용자 인증 기법”, 한국정보보호학회, 2013.