https://doi.org/10.7840/kics.2022.47.10.1629

신호 · 프로토콜 · 메시지 차원의 드론 무선통신 통합보안 연구

전 승 현◆, 김 도 희*, 서 민 재*, 황 병 우°

A Study on the Integrated Security of Drone Wireless Communication in Terms of Signal, Protocol and Message

Seung-hyeon Jeon◆, Do-hee Kim*, Min-jae Seo*, Byung-woo Hwang°

요 약

본 논문은 드론 무선통신에서의 취약점에 대한 통합보안에 대해 연구한다. 우선 상용 드론을 활용하여, 시나리오 기반의 취약점 테스트를 진행하였다. 그 결과, 복합적 공격이 들어옴에 따라, 단일 보안만 적용된 드론들의 경우 무력화되는 것을 확인할 수 있었다. 이에 따라 실제 드론 공격 시나리오들을 체계적으로 분석하였고, 세 관점으로 나누어 보안 방안을 설계하였다. 이렇게 각 관점별로 설계한 보안 방안을 바탕으로 단일 관점에서 테스트를 진행하고, 이후 통합보안을 적용시켜 복합적 공격에 내성을 갖는 드론 통신 모델을 제안한다. 나아가 결과물을 바탕으로 정부에서 발표한 '드론 사이버보안 가이드'의 한계를 보완하여, 드론 무선통신 보안 발전에 기여할 수 있을 것이라 예상한다.

키워드 : 드론, 무선통신 보안, 재밍, 암호화, Wi-Fi
Key Words : Drone, Wireless Communication Security, Jamming, Cryptography, Wi-Fi

ABSTRACT

In this paper, we study the collaborative security measures to redeem vulnerabilities of drone wireless communication. Primary, vulnerability tests were conducted using commercial drones based on the scenario. Thus, found out that when complex attacks were implemented, the drones with single security were neutralized. Therefore precisely analyzing the actual scenarios to hijack drones, we were able to design security measures in 3 aspects. For each aspect, tests were done from a single perspective based on the security measures. Then by applying triple-layer security, a drone communication model which is resistant to complex attacks becomes tolerant to those attacks. Furthermore, based on the results, it is expected that it will be able to contribute to the development of drone wireless communication security supplementing the limitations of the 'drone cybersecurity guide' announced by the government.

※ 본 연구는 KITRI - Best of the Best 내부 프로젝트 지원 및 관리로 수행되었습니다.
◆ First Author : KITRI - Best of the Best , jsh302204@gmail.com, 학생회원
° Corresponding Author : KITRI - Best of the Best, sp9512@naver.com, 정회원
* KITRI - Best of the Best, smj100394@gmail.com; dohui7557@g.skku.edu
논문번호 : 202205-076-C-RE, Received April 30, 2022; Revised July 11, 2022; Accepted July 12, 2022

Ⅰ. 서 론

Bureau of Investigative Journalism에서 드론 공습으로 인해 받은 피해를 정리한 표, 하단의 [그림 1]에 [1] 따르면 세계 각국에서 드론을 활용한 공격이 꾸준히 증가하고 있음을 확인할 수 있다.

또한, 해당 자료는 드론으로 인해 다방면으로 피해가 발생하고 있고, 사람의 목숨까지 위협하고 있음을 보여준다. 이러한 상황과 더불어 드론에 대한 수요가 폭발적으로 증가하는 지금, 이제는 드론 보안 위협에 대한 대응이 필요한 시점이다.

드론은 물리적으로 제어할 수 없는 거리에서 작동한다는 특성을 갖기에 어떠한 위협에도 영향을 받지 않고 기존 컨트롤러와 안정적으로 연결되어야 한다는 특성을 갖는다. 해당 특성을 보완하기 위해 상용 드론들에서 리턴 투 홈(RTH) 또는 호버링(Hoborring)과 같은 기능들을 적용하고 있지만, 현재 적용된 기능들로는 공개된 공격 벡터들도 막아내지 못하는 것이 현실이다. 이에 따라 복합적인 공격들로부터 드론의 안정적인 통신을 보장할 수 있는 통합보안 모듈에 관하여 연구하고자 한다.

본 논문에서는 실제 드론 무력화 및 탈취 시나리오를 기반으로 Wi-Fi 환경에서 통신하는 DJI 사의 Tello 드론과 Parrot 사의 Anafi 드론의 취약점 테스트를 진행한다. 분석한 시나리오 및 테스트 결과를 바탕으로 신호, 프로토콜 그리고 메시지 차원에서의 보안 방안을 각각 구현하고, 나누어진 보안 방안들을 한 모듈에 적용함으로써 통합보안 모듈을 제작한다. 그리고 제작한 모듈과 기존 상용 드론에 동일한 복합적 공격 테스트를 진행하여, 보안성을 검증한다. 검증을 통해, 제작한 통합보안 모듈 연구의 필요성 및 중요성에 대해 강조하고 나아가 해당 연구 결과의 활용 방안까지 제안할 것이다.

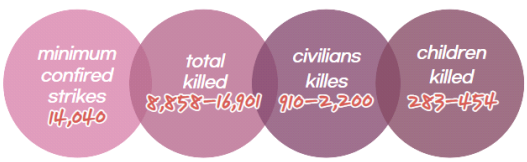

그림 1. 드론 공습 피해 통계 자료
Fig. 1. Drone Airstrike Damage Statistics

Ⅱ. 관련 연구 동향

KISA의 드론 사이버 보안 가이드[2]를 포함하여 드론 보안의 최근 동향을 담고 있는 논문들에서 여러 시나리오를 토대로 도출된 드론 무선통신 관련 취약점들을 찾아볼 수 있다. 이러한 취약점들을 발생 위치 기반으로 새롭게 분류하게 되면 아래의 표와 같이 표현할 수 있고, 새로운 접근이 가능해진다.

표에 분류된 신호, 프로토콜, 메시지 카테고리에서 신호 차원의 취약점이란 물리적인 전파 위치에서 발생하는 문제이며 프로토콜 차원의 취약점은 드론이 사용하는 프로토콜의 위치에서 발생하는 문제로 프로토콜 자체가 가지는 취약점을 의미한다. 마지막으로 메시지 차원의 취약점은 드론이 통신하는 상황에서 교환하는 실질적인 데이터, 즉 메시지 상에서 발생할 수 있는 문제점이다. 분류된 카테고리별로 본 논문에서 다루는 주된 취약점과 관련된 연구들은 다음과 같다.

먼저 신호 차원의 관련 연구[3]에서는 재밍에 대응하기 위하여 공격을 지속적으로 탐지하고 송신 신호를 재밍 신호와 직교하게 만드는 방식의 반복적인 채널 추정 알고리즘을 제안한다. 프로토콜 차원의 관련 연구[7]에서는 Wi-Fi로 통신하는 드론에 대한 취약점을 분석한다. 메시지 차원 관련 연구[12]에서는 드론이 통신 데이터 즉 메시지에 대해 발생할 수 있는 문제점에 관해 서술하고 이를 보완할 수 있는 암호 모듈을 제안한다. 소개한 연구 외에도 카테고리별로 드론의 무선통신 취약점 및 보안 방안에 관한 논의가 활발히 진행되고 있다.

기존 연구를 토대로 발행된 KISA의 드론 사이버 보안 가이드[2] 경우 공격 가능한 단일 시나리오들을 토대로 보안 항목들을 구분하여 개별 보안 방법을 기술한 형태로 작성돼 있다. 하지만 이는 취약점들의 특성에 따라 복합적으로 보완되어야 하는 통합보안의 중요성은 기술하지 못하고 있다. 그러나 본 논문에서 소개하는 신호, 프로토콜 그리고 메시지 차원으로 분류한 체계에 대한 검증이 가능하다면, 기존 가이드라

표 1. 드론 주요 취약점 분류
Table 1. classification of major drones vulnerabilities

Category	Vulnerability	Related research
Signal	Jamming	[3], [4]
	Signal Replay Attack	[5], [6]
Protocol	Deauthentication Attack	[7], [8]
	Bluetooth Impersonation Attacks	[9]
Message	Unencrypted Data	[10], [11], [12]
	Spoofing	[13]

인의 한계점을 보완한 드론 무선통신 보안 시스템을 구축할 수 있다고 판단된다.

Ⅲ. 취약점 분석 및 보안 방안 설계

본 장에서는 복합적인 공격에 대해 내성을 갖는 통합 보안 모듈을 구현하기 위해 먼저, 취약점 분석을 진행한 후 각 취약점에 대한 보안 방안을 설계한다. 취약점 분석의 경우 사전 분석한 공격 시나리오를 바탕으로 '신호 차원', '프로토콜 차원' 그리고 '메시지 차원'으로 나누어 연구를 진행한다.

3.1 신호 차원

3.1.1 신호 차원 취약점

비면허대역의 주파수를 활용하여 통신하는 드론의 특성상 방해전파 신호로 인한 통신 무력화는 반드시 해결해야만 하는 과제 중 하나이다. 정부에서는 이러한 특성을 역이용하여 불법 드론 무력화에 재밍을 활용하여 성과를 거두고 있다. 그러나 최근 SDR이 공공연하게 사용됨에 따라, 신호를 제작하여 송수신하는 것이 비교적 쉬워졌고, 전문가가 아니어도 재밍 신호를 제작할 수 있게 되었다. 이것은 불법 드론뿐만 아니라 정상적인 드론들 또한 악의적인 재밍으로 인해 무력화될 수 있음을 시사한다. 따라서 드론이 신호 차원에서 재밍을 통해 위협받을 수 있음을 인지하고 미리 대비하여야만 한다.

서론에서 언급된 상용 드론들을 바탕으로 재밍을 활용한 무력화 시나리오를 작성하고 그 결과를 확인해보았다. 결과적으로, 드론과 컨트롤러 사이의 통신이 강한 노이즈 신호들로 인해 무력화됨을 확인할 수 있었다. 그렇게 무력화된다는 전제하에 재밍을 회피하여, 안전하게 통신상태를 유지 가능한 방법이 무엇일지 고민해보며, 아래와 같은 아이디어를 고안해낼 수 있었다. 하단의 [그림 2]는 재밍이 발생하였을 때, 기존에 사용하던 인터페이스의 통신상태가 불안정해지게 되면, 더 상태가 원활한 다른 인터페이스로 통신 채널을 변경하는 방식을 보여주고 있다.

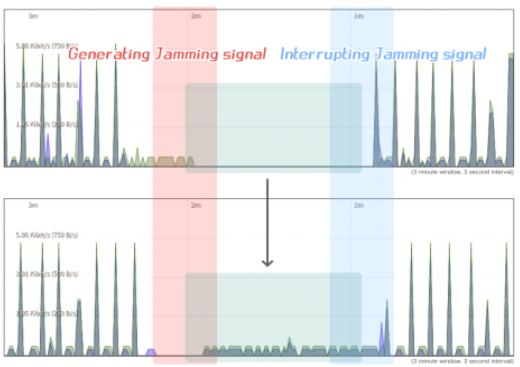

그림 2. 재밍 회피 아이디어, 다중 연결을 활용한 인터페이스 변경
Fig. 2. Jamming Avoidance Ideas, Changing Interfaces Using Multiple Connections

3.1.2 사용하는 기술개념

네트워크 본딩이란 네트워크 인터페이스를 논리적으로 묶어, 하나의 인터페이스로 결합하는 것을 말한다. 본딩을 제어하는 드라이버는 NIC(Network Interface Card)로 전송되는 데이터를 관리하는 방식으로 작동한다. 즉, 이번 장에서는 이러한 본딩 드라이버가 본딩된 NIC에게 상황에 따라 적절한 패킷을 분배하는 원리를 활용한다.

3.1.3 보안 방안 설계

인공지능과 센서를 이용한 관성항법 시스템 등 안티 드론의 대처 방법들이 존재하지만, 그로 인해 통신이 무조건 복구되는 것이 아니므로, 통신이 완전히 끊기지 않을 방법으로 본딩 기술을 이용한 채널 스위칭을 하단의 [그림 3]과 같이 설계해보았다.

각각 다른 채널을 사용하여 통신하고 있는 가상 인터페이스를 생성하고, 하단의 [표 2]과 같은 옵션들을 설정한다.

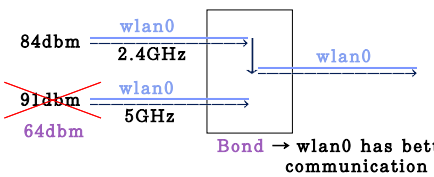

그림 3. 본딩의 Active-Backup policy를 활용한 보안 방안
Fig. 3. Security method using Active-Backup policy of Bonding

표 2. 본딩 인터페이스 설정
Table 2. Setting of bonding interface.

Slave Interfaces	wlan0	wlan1
Bonding Policy	Active-Backup policy	
Primary Slave	wlan0 or wlan1	
Reselection policy for primary slave	Option 1	
Set same MAC Address to all slaves	Yes (none, 0)	

3.2 프로토콜 차원

3.2.1 프로토콜 차원 취약점

통신하기 위해서는 수많은 프로토콜이 필수적이다. 특히 무선 통신 프로토콜의 경우 통신 거리나 환경, 기기의 특성에 따라 프로토콜이 Bluetooth, Zigbee, Wi-Fi, RFID, NFC 등 다양하게 존재한다. 본 논문에서는 다양한 무선 통신 프로토콜 중 드론이 주로 사용하는 무선 통신 프로토콜 중 하나인 Wi-Fi 프로토콜에 대해 분석을 진행하였다.

Wi-Fi 프로토콜은 데이터의 기밀성과 인증을 위해 WPA, WPA2 등 다양한 프로토콜을 제공한다.[14] 하지만 관리 프레임에 대해서는 인증과 검증이 미흡하여 이를 보안하기 위한 802.11w가 제정되었다.[15] 이러한 상황에도 불구하고 실제 802.11w를 적용하고 있는 제품은 많지 않다. 그에 따라 802.11w가 적용되어 있지 않은 제품의 경우 관리 프레임의 인증과 검증의 미흡으로 인해 Access Point(AP)와 Station(STA) 간 연결을 강제로 해제하는 Deauthentication Attack 즉, Deauth Attack이 가능하다는 취약점을 갖는다.[16]

실제 Deauth Attack을 시중에서 판매 중인 DJI의 Tello 드론과 Parrot 사의 Anafi 드론에 대해 시도해 보았으며 그 결과는 다음과 같다.

실험 결과 Anafi 드론의 경우 드론과 전용 컨트롤러에 802.11w가 적용되어 해당 공격이 무력화되는 모습을 확인할 수 있었다. 하지만 802.11w가 적용되어 있지 않은 Tello 드론의 경우 Deauth Attack에 취약한 모습을 확인할 수 있다.

이러한 Deauth Attack이 발생하면 컨트롤러가 드론에 대한 제어권을 잃을 수 있으며 이후 Wi-Fi 패스워드 크래킹이나 드론 탈취 등의 위협으로 이어질 수 있다. 따라서 본 장에서는 Deauth Attack에 대한 보안 방안을 설계해보고자 한다.

3.2.2 보안 방안 설계

Deauth Attack의 근본적인 원인은 관리 프레임에 대한 인증 부분이 빠져 있다는 것이다. 따라서 공격을 방어하기 위해 리눅스 커널에서 무선 네트워크 코드 중 Deauth Frame 관련 소스 코드를 수정하여 기존의

표 3. DJI Tello 드론 Deauth Attack 결과
Table 3. DJI Tello Drone Deauth Attack Results

Direction / Controller	AP→ALL	AP→STA	STA→AP
smartphone controller	O	O	O

표 4. Parrot Anafi 드론 Deauth Attack 결과
Table 4. Parrot Anafi Drone Deauth Attack Results

direction / controller	AP→ALL	AP→STA	STA→AP
smartphone controller	X	O	X
Dedicated controller	X	X	X

Deauth Frame에 인증 필드를 추가하였다. 하단의 [그림 4]는 기존의 Deauth Frame과 인증 필드가 추가된 Deauth Frame을 나타낸다.

또한, Deauth Frame이 수신되었을 때 호출되는 API를 수정하여 해당 인증 데이터가 없는 프레임의 경우에는 'Drop'하고 올바른 인증 데이터가 있는 경우에는 정상적으로 'Accept' 하여 세션 연결을 해제하도록 설계하였다.

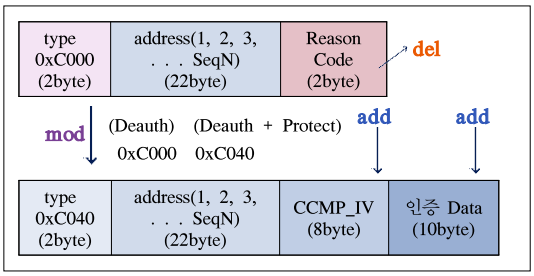

그림 4. 기존의 Deauth Frame과 인증 필드가 추가된 Deauth Frame
Fig. 4. The original Deauth Frame and the Deauth Frame to which the authentication field is added.

3.3 메시지 차원

3.3.1 메시지 차원 취약점

드론의 통신은 신호가 전 방향으로 방사되는 무선 통신을 활용하기에 스니핑에 취약하다. 만약 메시지가 암호화되어 있지 않을 경우, 공격자가 평문으로 통신되는 패킷을 스니핑하여 통신 내용을 분석할 수 있다. 또한, 분석된 정보를 바탕으로 추가적인 공격이 가능하며 그 결과 최악의 경우 드론이 탈취당할 수 있다는 보안 위협이 존재한다.[17]

Tello 드론과 Anafi 드론을 대상으로 실제 스니핑을 시도해 보았으며 수집된 패킷을 바탕으로 제어 구조를 분석한 결과 각각의 드론별로 메시지 차원의 취약점이 실제로 존재함을 확인할 수 있었다.

Tello 드론은 이미 제어 패킷의 구조가 하단의 [표 5]와 같이 이미 알려져 있었으며 이러한 구조에 맞춰 제어 패킷을 생성 후 드론에 송신하면 공격자가 원하

는 방향으로 드론제어를 수행할 수 있었다.

Anafi 드론 또한 제어 패킷의 데이터 부분이 하단의 [그림 5]와 같이 암호화가 진행되어 있지 않아 스니핑을 통해 제어 패킷의 구조를 유추할 수 있었으며 패스워드 같은 민감정보 역시 평문으로 송수신 중인 모습을 확인할 수 있었다.

이러한 결과를 통하여 실제 드론들이 스니핑과 같은 공격에 취약하며 이러한 취약점을 방어하지 않는다면 추가적인 공격의 시작점이 될 수 있음을 알 수 있었다.

이에 따라 본 논문에서는 제조사가 직접 제작한 프로토콜 및 표준 프로토콜을 사용할 때 스니핑에 대응할 수 있도록 LEA 암호 알고리즘을 이용한 드론의 암호화 통신을 설계하려고 한다.

표 5. Tello 드론의 제어 패킷 구조
Table 5. Control Packet Structure of a Tello Drone

Bytes	Contents
1 Byte	Header[Magic_num (0xCC)]
2 Byte	Packet Size
1 Byte	CRC-8
1 Byte	Packet Type
2 Byte	Message ID
2 Byte	Sequence
. . .	Payload
2 Byte	CRC-16

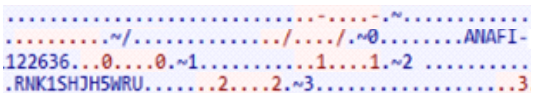

그림 5. Anafi 드론의 제어 패킷 데이터
Fig. 5. Control packet data for Anafi drone

3.3.2 사용하는 암호 알고리즘

LEA(Lightweight Encryption Algorithm)는 프로세서가 기본적으로 제공하는 연산인 ARX(Addition, Rotation, XOR)를 사용하고, 비선형 치환 테이블을 배제하여 경량 환경에서 사용할 수 있는 블록 암호 알고리즘이다.[18] 이번 장에서는 스니핑 위협에 대응하기 위해, 유한체 곱셈 연산과 메시지 인증 코드를 결합한 구조를 가진 LEA GCM(Galois/Counter Mode) 모드를 사용하였다.

3.3.3 보안방안 설계

먼저 LEA를 사용하는 데 필요한 인자 값을 암/복호화하기 위해 ECDH를 기반으로 설계하였으며, 실질적인 제어 패킷 데이터를 암/복호화하기 위해 LEA를 이용하였다.

암호화 통신 설계구조는 상단의 [그림 6]과 같다. 컨트롤러 측에서 임의의 nonce 값 및 비대칭 키를 생성한 후 공개키와 nonce 값을 드론에 전달한다. 이후 드론 측에서 lea key 및 부가 인증 데이터(aad) 값을 생성한다. 생성된 비밀키와 부가 인증 데이터를 공개키로 암호화하여 드론 측에서 컨트롤러 측으로 전송한다. 전송된 데이터를 컨트롤러 측에서 개인키를 통해 복호화하여 드론과 컨트롤러는 동일한 lea key 값과 aad 값을 공유한다. 또한, 드론과 컨트롤러 간 시간 동기화 시점을 기반으로 hash 알고리즘을 사용하여 부가 인증 데이터값을 주기적으로 동일한 값으로 변경하여 OTP 개념까지 추가하여 암호화 통신을 설계하였다.

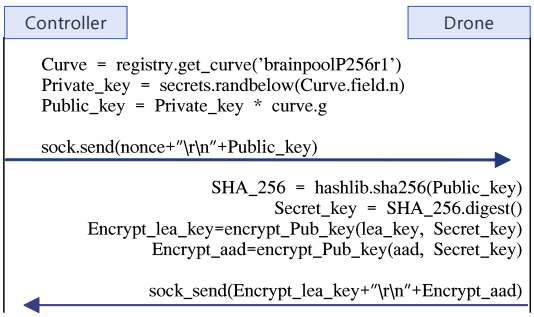

그림 6. 드론과 컨트롤러 간 키 교환 과정
Fig. 6. Key exchange process between drone and controller

Ⅳ. 보안 방안 테스트 결과

4.1 신호 차원의 보안 방안 테스트 결과

정확한 실험 결과를 얻기 위해 테스트 외의 신호 간섭을 막는 간이 전파 차단 챔버 안에서 검증을 시행하였다.

Active-Backup policy의 세부 옵션 중 신호 감도가 더 좋은 쪽을 택하는 1번 옵션까지 적용해 테스트를 진행해 보았다. 결과적으로, 통신 중인 채널에 재밍을 걸어보니, 노이즈 신호가 채널에 수신되면서 기존 채널에 이상을 감지하고 더 통신상태가 안정한 인터페이스로 옮겨가는 결과를 보였다. 하단의 [표 6], [표 7]은 검증을 진행할 때, 노이즈 신호를 수신하여 증가하는 신호 전력의 수치와 그에 따라 변경되는 인터페이스 연결 상태를 표로 표현한 것이다.

표 6. 재밍 : wlan0
Table 6. Jamming(primary slave): wlan0

	Normal	Attacked	Interface
wlan0	-82dbm	-62dbm	wlan0 → wlan1
wlan1	-90dbm	-91dbm	

표 7. 재밍 : wlan1
Table 7. Jamming(primary slave): wlan1

	Normal	Attacked	Interface
wlan0	-82dbm	-82dbm	wlan1 → wlan0
wlan1	-90dbm	-66dbm	

4.2 프로토콜 차원의 보안 방안 테스트 결과

하단의 사진들은 AP와 STA가 세션 연결 상태를 보여주는 GUI 환경이다. 하단의 [그림 7], [그림 8]은 'Drop' 또는 'Accept' 하여 정상적으로 세션이 유지, 해제되는 모습을 보여준다.

위와 같은 테스트를 통하여 인증 데이터가 없는 프레임과 인증 데이터가 있는 프레임을 송신시키고 실제로 세션 연결이 끊어지는 것을 확인할 수 있다.

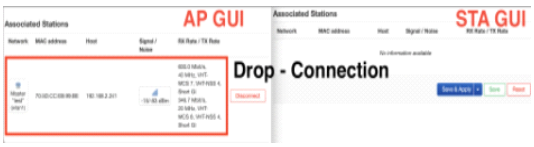

그림 7. 인증 필드 없는 Frame Drop
Fig. 7. Drop the frame doesn't have authentication field

그림 8. 인증 필드 있는 Frame Acceptt
Fig. 8. Accept the Frame does have authentication field

4.3 메시지 차원의 보안 방안 테스트 결과

LEA 알고리즘을 통해 12바이트의 제어 패킷을 암호화하게 되면 하단의 [표 8]와 같은 결과를 얻을 수 있으며, 스니핑 위협에 대해 대응할 수 있다.

표 8. 특정 제어 패킷을 LEA 암호화 진행
Table 8. LEA encryption of the specific control packet

	Hex
Plain text	cc 60 00 27 68 55 00 77 01 00 7b fb
Encrypted	1f 84 60 25 ba 43 a8 b7 83 66 eb 7b 1b 20 fc 9b 20 e5 a7 fb 90 de 06 69 63 5e 59

V. 통합보안 모듈 중요성 제시

재밍을 우회할 수 있는 보안 모듈만 탑재된 드론에 재밍과 Wi-Fi Deauth Attack을 동시에 진행했을 때, 재밍은 방어하나 Deauth Attack은 방어할 수 없었다. 결국, 드론의 세션 연결은 해제되었고, 대응책을 탑재하였음에도 통신 유지에 실패하였다. 이렇듯 실제 드론 보안을 위해 통합보안 모듈 연구가 필수적임을 보였다. 이에 따라 본 장에서는 앞서 구현한 세 가지 관점에서의 보안 방안을 한 통신 모듈에 구현하여 검증을 진행한다.

검증에 사용한 시나리오는 다음과 같다. 우선, Deauth Attack을 통해 컨트롤러와 세션을 끊는다. 그 다음 연결이 끊긴 컨트롤러와 드론 간 재연결을 위한 EAPOL패킷을 스니핑 후 패스워드 사전공격을 통하여 Wi-Fi 해킹을 진행한다. 세 번째로, 세션 재연결이 된 컨트롤러와 드론 간 통신하는 메시지를 스니핑하여 메시지의 구조를 알아낸다. 마지막으로 재밍을 통해 드론과 컨트롤러 간 통신을 마비시킨 뒤 알아낸 메시지 구조를 이용하여 위조 메시지를 만들어 드론 탈취를 성공시킨다.

그 결과, Tello 드론, Anafi 드론, 그리고 통합보안 모듈을 탑재한 제작 드론 중 제작 드론만 전반적인 보안에 성공하는 모습을 보였다. 앞선 Tello, Anafi 드론의 경우 실제 시나리오에서 무력하였고, Tello 드론의 경우 탈취까지 이어짐을 확인하였다. 하단의 [그림 9]는 통합보안 모듈을 도식화한 것이다.

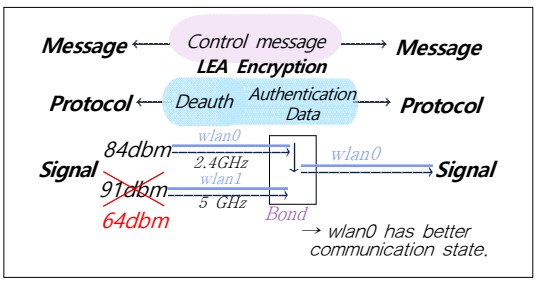

그림 9. 다계층 보안 모델
Fig. 9. Multi-layered security model

VI. 결 론

비행하는 드론의 특성상 무선 통신을 활용하는 것은 필수 불가결하다. 또한, 무선 통신이 공격 벡터의

시발점이 될 수밖에 없기에 복합적인 공격으로 이루어지는 드론 공격 시나리오에 대해 본 논문에서는 신호, 프로토콜 그리고 메시지 차원의 세 관점으로 나누어 보안 방안을 연구하였다. 또한, 각 관점으로 나누어진 드론 보안 방안들을 통합하고 검증함으로써, 통합보안 모듈의 중요성을 강조했다.

도출된 결과물은 KISA에서 발표한 '드론 사이버보안 가이드'에서[2] 대응 방안의 구체적 구현방안 및 해결방안을 연계한 통합보안의 중요성 부분에서 본 논문이 보완책으로 활용이 가능할 것으로 판단된다. 현재 대한민국이 드론 국제표준 프로토콜 제작 과제를 수행하고 있는 가운데[19], 기술의 안정화가 진행된 후에 보안 모듈 설계가 필수 불가결할 시점이 올 것이다. 설계를 진행하면서 가이드라인과 함께 본 연구 내용을 적용한다면, 높은 보안성을 가진 드론 보안 모듈을 설계할 수 있을 것이다.

References

[1] J. Serle and J. Purkiss, *Drone wars: The full data*(1970), Retrieved Jan. 3, 2022, from https://www.thebureauinvestigates.com/stories/2017-01-01/drone-wars-the-full-data.

[2] KISA, *Cyber Security Guide for Drone*(2020), Retrieved Jan. 3, 2022, from https://www.kisa.or.kr/2060205/form?postSeq=9&lang_type=KO.

[3] J. H. Jung, Y. M. Hwang, K. H. Cha, J. S. Lee, Y. Shin, and J. Y. Kim, "Iterative channel estimation algorithm for anti-jamming in MIMO communication systems," *J. Satellite, Inf. and Commun.*, vol. 11, no. 3, pp. 32-36, 2016.

[4] C.-M. Choi, "GPS anti-jamming using beamforming technique," *J. Korea Inst. Inf. Commun. Eng.*, vol. 20, no. 2, pp. 451-456, Feb. 2016. (https://doi.org/10.6109/jkiice.2016.20.2.451)

[5] H.-J. Kim and I.-Y. Lee, "A study on secure and improved single sign-on authentication system against replay attack," *J. KIISC*, vol. 24, no. 5, Oct. 2014. (https://doi.org/10.13089/JKIISC.2014.24.5.769)

[6] Y.-J. Maeng and D.-H. Nyang, "An analysis of replay attack vulnerability on single sign-on solutions," *J. KIISC*, vol. 18, no. 1, pp. 103-114, Feb. 2008. (https://doi.org/10.13089/JKIISC.2008.18.1.103)

[7] J. Malimban, B. R. Payne, and T. T. Abegaz, "Drone hacking: Applying the cyber kill chain to hijack unmanned aerial systems," *Quart. Rev. Busin. Disciplines*, vol. 8, no. 3, pp. 213-228, Nov. 2021.

[8] J. Feng and J. Tornert, *Denial-of-service attacks against the Parrot ANAFI drone*(2021), (Dissertation), Retrieved from http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-303150

[9] D. Antoniol, N. O. Tippenhauer, and K. Rasmussen, "BIAS: Bluetooth impersonation attacks," *2020 IEEE Symp. SP*, pp. 549-562, San Francisco, CA, USA, Jul. 2020. (https://doi.org/10.1109/sp40000.2020.00093)

[10] S. M. Cho, E. Hong, and S. H. Seo, "Random number gererator using sensors for drone," *IEEE Access*, vol. 8, pp. 30343-30354, 2020. (https://doi.org/10.1109/access.2020.2972958)

[11] J. Won, S. H. Seo, and Bertino, "A secure communication protocol for drones and smart objects," in *Proc. 10th ACM Symp. Inf., Comput. and Commun. Secur., ASIA CCS '15*, Singapore, Apr. 2015. (https://doi.org/10.1145/2714576.2714616)

[12] K. Kim and Y. Kang, "Drone security module for UAV data encryption," *2020 Int. Conf. ICTC*, pp. 1672-1674, Jeju, Korea (South), Oct. 2020. (https://doi.org/10.1109/ictc49870.2020.9289387)

[13] K. Wesson, M. Rothlisberger, and T. Humphreys, "Practical cryptographic civil GPS signal authentication," *J. Inst. of Navig.*, vol. 59, no. 3, pp. 177-193, Sep. 2012. (https://doi.org/10.1002/navi.14)

[14] C. He and John C. Mitchell, *Security Analysis and Improvements for IEEE 802.11i*(2005), Retrieved Apr. 29, 2022, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.74.1515&rep=rep1&type=pdf

[15] V. V. Kumari and K. V. K. Raju, *Formal verification of IEEE 802.11w authentication protocol*(2012), Retrieved Apr. 29, 2022, from

https://www.sciencedirect.com/science/article/pii/S2212017312006317. (https://doi.org/10.1016/j.protcy.2012.10.086)

[16] J. Bellardo and S. Savage, *802.11 Denial-of-Service Attacks:Real Vulnerabilities and Practical Solutions*(2003), Retrieved Jan. 3, 2022, from http://users.csc.calpoly.edu/~bellardo/pubs/usenix-sec03-80211dos-html/aio.html.

[17] J. Son, J. Sim, J.-G. Lee, and I.-A. Cheong, "Hijacking attack using wireless network security vulnerability in drone and its countermeasure," in *Proc. KIICS Conf.*, pp. 327-330, Busan, Korea, May 2017.

[18] J. Park, *128-bit Block Cipher LEA and its Modes of Operation*(2016), Retrieved Jan. 3, 2022, from http://www.tta.or.kr/.

[19] S. Choi, *Create an international standard for drone communication protocols*(2020), inews24, Retrieved Jan. 3, 2022, from https://www.inews24.com/view/12 52297.

전 승 현 (Seung-hyeon Jeon)

2017년 3월~현재 : 한국외국어대학교 컴퓨터전자시스템공학부 학사과정

2022년 3월 : BEST OF THE BEST 10기 수료

<관심분야> 무선통신, 통신공학, IoT, 임베디드

[ORCID:0000-0003-3167-3489]

김 도 희 (Do-hee Kim)

2022년 2월 : 서울호서전문학교 사이버해킹보안과 졸업

2022년 3월 : BEST OF THE BEST 10기 수료

2022년 8월~현재 : 성균관대학교 소프트웨어 석사과정

<관심분야> 무선통신, 임베디드, 차량 보안, IoT

[ORCID:0000-0002-8351-2727]

서 민 재 (Min-jae Seo)

2019년 3월~현재 : 중부대학교 소프웨어공학부 정보보호학전공 학사과정

2022년 3월 : BEST OF THE BEST 10기 수료

<관심분야> 무선통신, 인공지능, 보안, IoT

[ORCID:0000-0002-1088-989X]

황 병 우 (Byung-woo Hwang)

2021년 2월 : 홍익대학교 컴퓨터공학과 졸업

2022년 3월 : BEST OF THE BEST 10기 수료

2022년 8월~현재 : (사)금융보안원 재직

<관심분야> 무선통신, 금융보안, IoT, 머신러닝

[ORCID:0000-0002-8931-6188]