드론 운용의 보안 위협과 대응 방안

류해원*, 최성한*, 하일규*
*경일대학교 컴퓨터학과
e-mail:riddkdk@kiu.kr

Security Treats and Countermeasures in Drone Operation

Hae-Won Ryu*, Sung-Han Choi*, Il-Kyu Ha*
*Dept of Computer Engineering, Kyungil University

요 약

최근 무인항공기는 국내뿐만 아니라 전 세계적으로 활용에 대한 관심이 높아지며 다양한 분야에서 사용되고 있다. 드론은 독립적으로 외부로부터 정보를 수집하는 임무를 수행하거나, 군집을 이루어 데이터를 주고받으며 특정한 임무를 수행하게 된다. 지금까지의 드론에 관한 연구는 신속하고 정확한 임무의 수행에만 초점을 두어왔고, 드론 자체 또는 드론 군집에서 주고받는 데이터의 보안과 안전에 관한 연구는 비교적 소홀히 다루어져 왔다. 따라서 본 연구는 드론 운용에 있어서 구성요소별 보안 취약점을 분석하고 취약점을 해결할 수 있는 대응방안을 설명한다. 특히 드론의 가장 중요한 임무 중 하나인 지상의 목표물 탐색에 있어서 발생할 수 있는 보안위협 요소와 이에 대한 해결방안을 제시한다.

1. 서론

최근 드론은 국내뿐만 아니라 전 세계적으로 관심이 높아지고 있는 추세다. 처음 드론은 군사 분야에서 무기로 사용되었으나, 기술이 발전함에 따라 드론의 크기가 다양해지고 가격이 저렴해지면서 일반인들에게도 쉽게 접할 수 있는 제품이 되었고, 여가생활로 드론을 사용하는 모습도 자주 볼 수 있다. 무인항공기에 카메라 이외에도 여러 가지의 기능을 가진 센서를 부착하고 IT 기술을 응용하여 활용 범위의 폭을 넓혀 군사 분야와 민간분야 외에도 농업, 택배 운송, 항공촬영, 기업 홍보 등 산업분야에서도 다양한 용도로 사용되고 있다. 드론의 핵심 기술은 위성항법장치(GPS, Global Positioning System)와 영상처리 기술이라고 할 수 있으며, 정확한 위치 파악 기술 덕분에 드론이 단시간에 상용화될 수 있었다고 할 수 있다[1][2].

무인항공기는 각종 사업에 다양하게 활용되는 만큼 보안성이 중요한데 드론의 경우는 무선으로 정보를 교환하는 점과 다양한 통신채널을 이용하기 때문에 보안에 있어 매우 취약하다. 보안성이 낮을 경우 악의적인 해킹이나 공격에 노출되기 쉽다. 특히 군사 분야에서 사용되고 있는 무인항공기의 경우 군사에 관련된 정보 유출, 정보 손상 및 변경, 경로 이탈, 침해 등은 국가 안보에 막대한 피해를 입힐 수 있다. 실제적인 예로 2008년 이라크의 'shiite' 무장단체들이 미군 무인항공기의 영상 정보가 암호화되지 않은 것을 알고 실시간 비디오 영상을 해킹하기도 하였다. 이 비디오 영상은 무인항공기의 소프트웨어에 대한 사이버 공격을 통해 얻을 수 있었다[3]. 군사 분야이외에도 민간분야와 산업분야에서도 보안성은 중요하다. 민간분야의 경우 민간용 GPS에 대한 의존도가 높으나 민간용 GPS는 암호화가 되어 있지 않아 보안성이 취약하여 사생활 침해가 우려되기 때문에 민간분야 무인항공기의 보안성도 매우 중요하고 할 수 있다.

무인항공기가 군사 분야뿐만 아니라 넓은 분야에서 주목 받고 있는 만큼 보안성에 대해서도 관심이 높아지고 있다. 최근 무인비행기의 보안 및 취약성에 파악하여 대응방안을 제시하고 있는 연구들이 진행되고 있으나, 무인항공기가 중심이 되는 시스템의 구성요소별 보안 취약 요소를 정확하게 분류하고, 이에 대한 대응방안을 제시한 연구는 많지 않다.

따라서, 본 연구에서는 무인항공기 보안 및 취약성과 대응방안에 대한 기존 연구를 바탕으로 무인항공기 응용시스템의 구성요소별 보안 취약점을 분석하며, 그러한 취약점을 보완할 수 있는 대응방안을 제시하고자 한다. 2장에서는 관련 연구에 대해서 설명하고, 3장에서는 드론 응용시스템의 구성요소별 보안 취약점에 대하여 논하고, 각 요소별 보안 해결책을 설명한다. 4장에서는 드론의 목표물 탐색에 있어서 보안위협요소와 그 해결 방법에 대하여 기술하며, 5장에서 결론을 언급한다.

2. 관련연구

2.1 드론 보안관련 연구 분석

다양한 직종에서 널리 쓰이고 있는 드론은 보안성이 취약하여 이에 관련된 연구들이 최근 들어 활발히 진행되고

있다. 표1은 드론의 보안과 관련된 연구들을 정리한 것이다. 연구 [2]의 경우 2008년부터 2014까지 일어난 무인항공기 보안사고 사례를 정리한 뒤 드론의 구성요소와 정보 흐름을 기준으로 보안 취약점에 대하여 논하고 있다. 또한 드론에 대한 보안 공격 포인트들 정리하고 무인항공기만의 독특한 취약점에 대하여 서술하고 있다. 연구 [3]에서는 무인항공기의 무선통신과 관련한 문제와 잠재적 위협 및 가능한 해결책을 제시하고 있다. 연구 [4]는 드론 기술 및 보안 위협을 식별한 뒤 보안 요구 사항 나열하며 해결점을 제시하였다. 연구 [5]는 UAV 시스템에 전반적인 시스템의 세부적인 분석을 통하여 설계자와 사용자를 구별하고 취약성을 식별하여 대응 및 복구에 도움을 주는 방법을 제안하고 있다. 연구 [6]은 드론에 대한 보안 및 비디오 피드에 취약성과 그 영향에 대한 예비조사를 실시하고, 해결방안을 제시한 연구이다. 연구 [7]은 드론에 대한 기존 취약성 연구를 바탕으로, 보안 취약성을 분석한 후 보안성을 평가하기 위해 보호프로파일을 제시하였다. 드론에 위협이 될 요소들을 식별하고 이를 바탕으로 무인 비행기에 적용 가능한 공격 시나리오를 도출하여 보호프로파일을 개발하여 무인 비행체의 안전성을 평가하기 위한 기준을 제안하고 있다. 연구 [8]은 기존에 알려진 보안 위협 요소들을 정리하여 보안 위협 부재로 인한 문제점을 제시하고 국내 사이버 공격 대응 체계와 국외 사이버 공격 대응체계를 정리하고 있다.

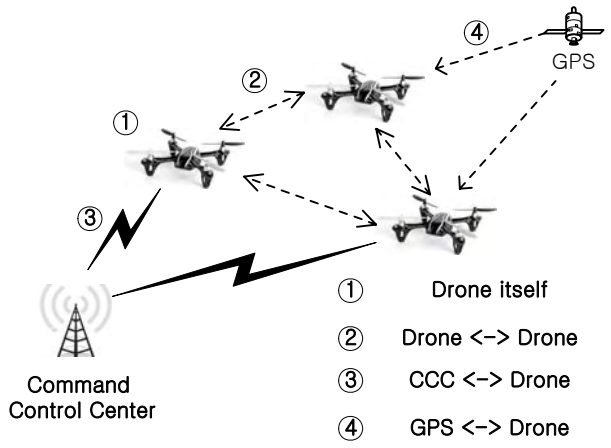
<표 1> 드론 보안 관련 연구

연구	내용
[2]	드론의 사이버 보안 사고사례를 살펴보고, 드론의 구성요소에 따른 보안 취약성을 분석함.
[3]	드론 무선 관련 문제, 잠재적 위협 및 가능한 해결책을 제시함.
[4]	보안위협을 분류하고 각 드론의 보안위협에 따른 보안요구사항을 정의하여 비교 분석함.
[5]	드론 시스템에 대한 다양한 보안 위협을 분석하고 사이버 보안 위협 모델을 통해 공격 경로를 파악함.
[6]	네트워크 보안 관점에서 드론의 작동에 미치는 보안 취약성과 그 영향에 대한 예비조사를 함.
[7]	드론의 보안 취약성을 분석하고, 이를 바탕으로 드론의 안전성을 평가하기 위한 기준을 제안함.
[8]	드론 보안위협 분류 및 무인항공기 보안위협 적용방안을 제시함

2.2 드론 보안 분야

드론은 광대역 컴퓨터 네트워크 상에 무선으로 연결되어 있는 하나의 노드이다. 넓은 범위에서 무선으로 통신이 가능하다는 장점을 가지고 있으나 이것은 곧 단점이 된다. 무선으로 연결된 곳을 주파수 신호로 공격을 하거나 암호화되지 않은 부분을 찾아 정보 유출 및 정보 손상을 일으킬 수 있다. 또한 드론의 경우 실시간으로 정보를 주고받는 형식으로 상시 열린 상태를 유지하기 때문에 공격에 노출되기 쉬우며, 전자기 신호에 민감하고 취약하다.

그림 1은 드론을 활용한 응용 네트워크를 나타낸 것이며, 각 구성요소별 보안 위협분야를 표 2에서 정리하였다.



(그림 1) 드론을 활용한 응용 네트워크와 보안 요소

<표 2> 드론 보안 분야

구분	보안 위협분야
드론 자체	-지상관제소와 드론 사이에 정보 -GPS와 정보교류 -드론과 정보를 공유하는 통신장치
드론-드론	-드론과 드론사이 -드론과 CCC(Command Control Center) -드론과 GPS
CCC-드론	-드론과의 정보교류
GPS-드론	-GPS와 드론사이에 무선통신 -암호화가 걸려있지 GPS -위치정보

3. 드론의 보안 위협과 개선 방안

3.1 드론 자체

드론은 조작에 의한 비행보다는 자율적인 판단에 의해 임무를 수행하는 자율비행이 대부분이다. 특히 자율비행에 있어서 드론 자체의 구성요소는 상호 의존적인 측면이 있어서 어느 한 요소에서 공격을 받게 되면 비행경로와 제어에 타격을 받아 임무 수행에 큰 차질을 빚게 된다. 가장

흔하게 발생할 수 있는 보안 위협은 외부로부터 중요한 데이터를 수신 받아야 하는 경우, 잘못된 정보가 삽입되는 경우이다. 이러한 경우 드론의 동작에 심각한 영향을 줄 수 있다.

이에 대한 개선 방안은 드론이 교환하는 통신채널마다 기밀성을 보장하기 위한 암복호화와 키를 이용하여하고, 데이터 변조 및 조작, 오류에 대해서 대처할 수 있는 변경 감지코드(MDC,Modification Detection Code)를 전송 데이터에 덧붙여야 하며, 인증이 필요한 경우에는 메시지 인증 코드(MAC, Message Authentication Code)를 추가해야한다. 또한 드론 내부에는 부품 간의 데이터 주입 공격을 방지하기 위한 이상 징후를 확인하는 경량소프트웨어도 필수적이다[4][6].

3.2 드론-드론

드론 군집에서 각 드론은 무선으로 네트워크를 형성하여 데이터를 송수신 또는 공유하기 때문에 어느 한 노드의 드론이 해킹되어도 모든 드론에게 영향을 끼칠 수 있다. 이에 따라 드론 군집에 임무수행이 불가능해지거나 차질을 빚게 된다.

이를 개선하기 위해서는 드론에 사이에 주고 받는 데이터에 대한 암호화가 필수적이다. 또한 드론마다 변경 감지 코드를 덧붙여 보안성을 강화하고, 메시지 인증 코드를 추가하여 외부 공격에 대비해야한다.

3.3 CCC-드론

지상관제소(CCC, GCS)는 드론을 통제하고 임무를 할당하는 장소이며 드론으로부터 파악된 정보를 수집하고 분석하는 장소이다. 지상관제소와 드론은 비교적 원거리이므로 전송 데이터 보안에 더욱 취약할 수 있다. 지상관제소가 공격을 당하여 드론에 잘못된 임무 전달하거나, 원하는 데이터를 드론으로부터 전달받지 못하는 일을 초래할 수 있다. 따라서 이를 사전에 예방하고 해킹 위협으로부터 대비를 할 수 있어야 한다. 지상관제소에 가능한 공격으로는 Virus, Malware, Keyloggers, Trojans, Hacking 등이 가능하다[5].

이를 위해 지상관제소로 부터 드론에 전달되는 데이터는 암호화하여 보안성을 높이고 드론에는 변조된 데이터를 복구할 수 있는 기술이 필요하다. 또한 지상관제소에 snoop server기술 등을 적용하여 네트워크를 통해 전송되는 모든 데이터와 요청에 접근과 감시가 이루어지도록 한다.

3.4 GPS-드론

민간용 GPS 신호는 군사용과 다르게 전혀 암호화되지 않으며, GPS 공격방법에 관한 기술 문서들이 널리 공개되어 보안성이 매우 낮다. GPS 입력 신호의 제어권이 해킹되면 원하는 목적지로 드론을 이동시킬 수 있으며, 이에 따라 지상관제소의 통제를 벗어날 수 있게 된다.

이에 대한 해결점은 GPS를 대체할 수 있는 기술로 위치 신호 없이도 운행을 수행할 수 있도록 하는 방법이 연구되고 있다. 지형의 시각적 이미지, 별 추척(star-tracking), 양방향 시간전송(2-way time transfer) 방법 등이 활용될 수 있고, 기존의 GPS를 개량하여 GPS의 약한 신호 때문에 발생되는 스푸핑과 재밍에 대비하기 위한 거짓 신호로부터 진짜 신호를 구별 할 수 있는 암호화 기술을 개선하는 방법이 있다[2].

4. 목표물 탐색에서의 보안 위협과 대응 방안

본 절에서는 드론을 이용한 지상의 목표물 탐색에서 보안 위협요소와 이에 대한 대응 방안을 설명한다. 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability) 측면에서 위협요소를 구별하고 해결책을 제시한다.

4.1 드론 자체의 보안 위협과 대응 방안

드론의 목표물 탐색 수행을 위해서는 드론, GPS, 지상관제소 등과 상호작용하면서 임무를 수행하게 된다. 드론과 드론 이외의 장치들과의 보안 위협요소 이외에도 드론 자체의 보안 위협요소를 구별하고 이에 대한 대응 방안을 모색하는 작업이 기본적으로 이루어져야 한다. 기밀성 측면에서 인가되지 않는 접근이나 정보 탈취 공격으로부터 드론 자체를 보호하여야 한다. UAV에 가해질 수 있는 가장 흔한 보안 위협은 Hacking이다. 무결성 측면에서 자연재해등에 의해 의도하지 않은 데이터의 무결성 위협이 발생할 수 있으며, 악의를 가진 공격자에 의한 jamming, retransmitting, distortion 등 다양한 공격이 가능하다. 가용성 측면에서도 Dos(Denial of Service) 또는 DDos (Distributed DoS) 공격에 의하여 정보의 사용이 제한될 수 있다[5].

이러한 문제점들을 해결하기 위해서는 인가되지 않은 침입으로부터 드론 자체를 보호할 수 있는 암호화 장치가 필요하며, 정보 생성 및 변조를 막기 위하여 데이터에 대한 변경 감지코드를 만들어 무결성을 높인다. 정보 누출을 막기 위해서는 데이터 변조를 시도하는 상대방 컴퓨터에 대량의 데이터를 주어 접속 불가능 상태로 만들어 해킹에 대한 위험도를 낮춘다.

4.2 드론과 드론 간의 보안 위협과 대응 방안

여러 대의 드론이 군집으로 목표물 탐색을 수행할 경우에는 공격경로가 다양해지므로 드론이 한 대일 때보다 해킹에 대한 위험도가 높아지며, 보안에 있어서 더욱 취약해질 수 있다. 여러 대 드론이 무선 네트워크를 사용하므로 각 연결마다 위협을 받을 수 있으며, 전달되는 정보 또한 공격에 취약하다. 기밀성 측면에서 다양한 공격에 의한 통신 링크의 단절이 가능하다. identity spoofing, Hijacking, 프로토콜 기반 공격 등이 가능하다. 무결성 측면에서 통신

링크에 악의적인 코드를 삽입하거나 jamming, retransmitting 등의 공격이 가능하다. 가용성 측면에서도 jamming, Dos, DDos, 제어 신호의 위변조 등의 공격이 가능하다[5].

드론과 드론사이의 보안 강화를 위해서는 정보의 훼손과 변경을 막기 위하여 데이터의 암호화가 필수적이고, 데이터 변조 및 조작에 대처할 수 있는 변경감지코드(MDC, Modification Detection Code)가 필요하며, 인증이 필요한 경우 메시지 인증 코드(MAC, Message Authentication Code)가 필요하다[4].

4.3 드론과 CCC 간의 보안 위협과 대응 방안

일반적으로 드론의 목표물 탐색 정보는 최종적으로 지상관제소에 전달된다. 지상관제소와의 통신라인이 위협받게 되면 정보의 무결성 측면에서 심각한 타격을 입게 된다. 따라서 드론 응용 시스템의 구성요소 중 어느 요소보다 중요한 부분으로 다루어져야 한다. 기밀성 측면에서 지상관제소에는 Virus, Malware 등으로부터 위협받을 수 있으며 드론과의 통신 링크에서도 hijacking, 프로토콜 기반 공격 등으로부터 정보 손실이 발생할 수 있다. 무결성 측면에서도 악성코드의 삽입, 신호의 왜곡 등 악의적인 공격에 의한 보안 위협이 있을 수 있다. 가용성 측면에서도 jamming, Dos, DDos 등에 의하여 위협을 받을 수 있다.

이를 위해서는 지상관제소와 드론간의 암호화 통신이 필수적이며, 침입자로부터 공격을 당하였을 때 변조된 데이터를 복구 할 수 있는 기술이 필요하며, snoop server기술을 활용하여 침입자의 행동을 감시하도록 한다.

4.4 드론의 실제 운영에서 보안 대책 적용

위에서 제시한 보안 위협은 드론의 독립적 또는 군집 임무수행에서 일반적으로 고려해야할 보안 위협요소와 대응방안을 제시한 것이다. 드론의 실제 운용에서는 각 구성요소별 보안위협요소를 표로 정리하고 각 요소에 대한 위협정도, 중요도, 대응책 등을 파악하고 보안 우선순위, 영향도 등을 파악하여 보안 위협에 대응하여야 한다.

5. 결론

본 연구에서는 드론의 임무 수행에서 가장 중요한 요소 중 하나인 보안 위협을 다루었다. 즉 드론 운용에서 보안적인 측면에서 취약해질 수 있는 위협요소를 드론 응용체계의 구성요소별로 설명하였고, 이에 대한 대응 방안도 설명하였다. 특히, 드론의 가장 일반적인 임무 중 하나인 목표물 탐색에서 고려해야할 보안 위협요소를 구분하였고, 각 위협요소별 대응 방안을 제안하였다. 향후 대응 방안의 실제 적용을 위한 보안 점검 리스트의 작성과 보안 적용 사례 연구를 수행해나갈 계획이다.

※이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No.2017R1D1A1B03029895).

참고문헌

[1] 김사웅, “무인항공기 기반 빅데이터 처리 시스템의 프로토타입 설계,” 스마트미디어저널, 제5권, 제2호, pp.51-58, 2016.

[2] 박태규, 김영준, 김소연, 이승엽, 이지환, “무인항공기 사이버 보안 사고사례와 보안 취약성,” 정보통신기술진흥센터, pp.1-12, 2015.

[3] D. Rudinskas, Z. Goraj, J. Stankūnas, “Security analysis of uav radio communication system,” Aviation, Vol.13, No.4, pp.116-121, 2009.

[4] 김만식, 강정호, 전문석, “무인기 군집 비행 보안위협 및 보안요구사항 연구,” 디지털융복합연구, 제15권, 제8호, pp. 195-202, 2017.

[5] A. Javaid, W. Sun, V Devabhaktuni, M. Alam, “Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System,” in Proceedings of the 2012 IEEE Conference on Technologies for Homeland Security (HST), pp.585-590, 2012.

[6] E. Rivera, R. Baykov, G. Gu, “A Study On Unmanned Vehicles and Cyber Security,” Texas, USA, 2014.

[7] 전웅렬, “무인비행기의 보안취약성 분석 및 공통평가기준 기반 보호 프로파일 개발,” 정보기술아키텍처연구, 제13권, 제4호, pp.663-672, 2016.

[8] 이홍한, “통합보안위협 분류기준 및 무인항공기 적용방안 연구,” 석사학위논문, 동국대학교 국제정보대학원, 2015.