Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

Analysis on the Security Requirements for the Aviation-IT Convergence

Seong-Jong Kim*

Department of Aviation-IT Convergence, Far-East University

ABSTRACT

In the age of fourth industrial revolution, convergence in various industries is inevitable. The convergence of the aviation industry and the IT industry sector is rapidly moving into one of the major industries and technologies to facilitate international standardization efforts. In this paper, for stable operation of the drone, analyzed vulnerability through various types of reported accidents and propose requirements for the necessary security requirements. Conventional use methods, such as spoofing and jamming attack, which are used to examine the frequency bands, have proven that they are no longer able to secure GPS safely. And in this paper, limited to low-cost industrial drone operation, suggesting a new set of algorithms that take account of the operational goals of the drone. The proposed algorithm improved reliability by suggesting a technique for separating data collected by the external data required for navigation and by the captured data. Further, it has increased stability compared to costs, resulting in a double security structure that lets them distinguish against wrong signals that has open the corresponding network only when needed and the random values depending on time. The algorithm presented in this paper does not significantly change the existing hardware and most processes operated by software, expect that will contribute to the efficient operation of low-cost industry drone.

Ⓒ 2017 KKITS All rights reserved

KEYWORDS: Convergence, Aviation industry, IT(Information technology) industry, GPS, Security requirements, Spoofing, Jamming, Low-cost Industrial drone

ARTICLE INFO: Received 13 March 2017, Revised 3 April 2017, Accepted 7 April 2017.

*Author is the Department of Aviation-IT Convergence, Far-East University, 76-32 Daehak-Gil Gamgok-myeon, Eumseong-gun, Chung-buk, Korea

E-mail address: ksj@kdu.ac.kr

www.kci.go.kr

1. 서론

1-1 연구의 필요성

4차 산업혁명의 시대로 빠르게 변화하고 있는 현대 사회에서 여러 산업분야에서의 융합은 필연적인 것이라 할 수 있을 것이며, 항공 산업분야와 IT(Information Technology) 산업분야의 융합도 빠르게 진행되고 있다. 미래창조과학부는 2016년 하반기까지 드론 보안 가이드라인을 마련할 계획이라고 하였으나 아직 제시되지 않은 상태이며, 그 사이 군사적 목적의 드론과 택배산업 등 관련 산업들도 하루가 다르게 발전하고 있다.[1][2][3][4] 본 논문에서는 최근 여러 분야에서 사업화 논의와 구현이 활발하게 이루어지고 있는 무인항공기(UAV ; Unmanned Aerial Vehicle) 분야 중 드론(Drone)의 안정적인 운영을 위해 필요한 여러 보안 요구사항들에 대한 취약점들을 분석하고, 저비용 산업용 드론을 위한 효율적인 운영 알고리즘을 제시하고자 한다.

1-2 관련시장 동향 및 규모

무인항공기는 가격이나 효용 가치 등의 측면에서 효율적인 면이 많아 최근 군사적인 목적 이외에도 다양한 민간 분야에서 활용되고 있다. 무인항공기 중 드론의 대표적인 사용용도를 살펴보면 다음과 같다. 먼저 여러 종류의 센서(Sensor)와 카메라를 활용하여 다양한 주변 환경의 요소들을 감지하거나 감시하는 데 사용할 수 있는데, 예를 들면 산불을 감시하거나 고속도로 전용차선 위반 단속에 드론을 사용하고 있다. 또한 드론을 이용한 택배나 방송 촬영은 일반화 되어가고 있는 추세이며 치안, 광물 탐사, 재해 구호, 과학 연구와 아직 시장의 대부분을 차지하고 있는 군사적인 목적 그리고 수색 및 구조에도 드론이 폭넓게 활용되고 있다. 드론에 대한 관심은 일반 소비자들에게도 높아 2015년 1월에 미국 라스베가스에서 열린 국제가전박람회(CES ; Consumer Electronics Show)에 최초로 드론 제품 전시 구역이 설치되어 뜨거운 반응을 보였으며, 민간용 드론 시장만 고려해도 규모면에서 연평균 20% 이상의 성장을 보여 2023년에는 약 22억 달러에 이를 것으로 전망되고 있으며, 방위 산업 분야에서도 2022년까지 약 114억 달러 규모로 증가할 것으로 예상하고 있다.[5][6]

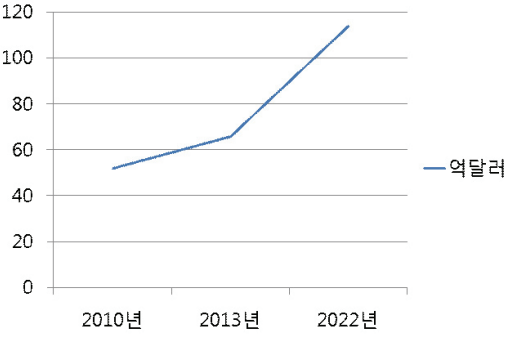

그림 1. 드론 시장 규모 예측(방위 산업)
Figure 1. Drone market scale prediction(Defence Industry)

2. 드론을 위한 안전과 보안 고려사항

2.1 안전(Safety) 고려사항

모든 항공기의 안전운항에서 충돌회피는 기본적인 사항이다. 무인항공기의 충돌회피를 위한 See & Avoid 기능은 가격적인 문제와 전력소모 및 하중의 문제의 해결을 위한 연구가 진행 중에 있다. 시스템의 신뢰성의 경우 유·무인 항공기의 주 사용목적과 소모용 여부에 차이가 있어 유인항공기와 비교가 적절하지 않지만 높은 신뢰성에 저비용

www.kci.go.kr

의 시스템을 구현하기 위한 노력도 설계의 단순화, 인증된 부품의 사용 등 다 방면에서 진행 중에 있다. 무인항공기의 경우 사람에 의한 사고 비율은 유인항공기에 비해 낮다는 것이 일반적인 보고이나 최근 다양한 유형의 드론의 등장과 한 사람이 여러 대를 조정하는 시점에 이르러 조종에 대한 자격증 부여의 필요성도 대두되고 있다. 그 밖에 기상문제에 따른 안전도 역시 고려 대상이기는 하나 비용과 드론의 사용 목적 한정 등으로 크게 문제 시 되고 있지는 않은 실정이다.

2.2 보안(Security) 고려사항

드론은 그 특성 상 무선망의 이용과 여러 입력 센서들 그리고 직렬적인 안정성 구조를 갖기 때문에 사이버 공격으로 인한 보안사고 위험이 매우 높으며, 시스템을 구성하는 한 유닛의 침해에도 전체 시스템의 안전과 보안을 보장할 수 없게 된다. 대표적인 보안 위협 공격 요소들로는 이미 여러 차례 보고된 공격 방식인 GPS 스푸핑(spooling)과 재밍(Jamming), 데이터와 영상 정보에 대한 해킹(Hacking), 물리적인 기체 탈취, 컴퓨터 바이러스를 이용한 공격 등을 들 수 있다. 보안사고 사례를 살펴보면 2011년 전파 재밍을 통한 GPS 시스템 공격으로 추정되는 미국 무인정찰기의 이란에 의한 포획 사건이 있다.[7][8][9][10] 이 밖에도 비디오 영상 데이터 해킹, 드론의 바이러스 감염 사례등도 보고되었으며, 우리나라에서도 북한으로 추측되는 GPS(Global Positioning System) 교란 공격으로 해군 무인기가 추락하는 등 항공기들과 선박들의 GPS 관련 동작에 문제가 발생했던 것으로 보고되었다.[11][12]

3. 취약점 분석 및 효율적 운영 방안

3.1 보안 취약점 분석

드론은 여러 가지 기능의 구성요소들이 연결된 형태로 구조적으로 외부로부터 노출에 자유로울 수 없는 시스템이라 할 수 있다. 드론은 그 운영 특성 상 외부에서 들어오는 입력 자료들에 의해 그 동작이 영향을 받으며, 사이버 보안에 취약점을 갖는 무선통신방식의 여러 입력 채널(Channel)들을 제공해야만 하는 단점이 있다.

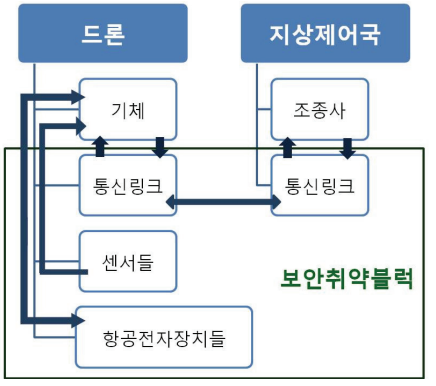

그림 2. 드론 시스템
Figure 2. Drone system

그림 2.에서 보안에 가장 취약한 부분들을 분석해보면, 드론과 지상 제어국의 통신 링크들 사이에 양방향 정보 통신 지점과 외부로부터 각 종 센서들로 전달되는 단방향 정보 통신 지점이라 할 수 있다. 이러한 지점들은 다양한 형태와 방법으로 신호가 왜곡 및 조작될 수 있기에 높은 신뢰성을 갖아야만 할 것이다. 또한 드론의 항공-IT 융합적인 측면에서 보안 상 취약점들을 구체적으로 살펴보면 다음과 같다. 먼저 항공학적인 면으로는 비행체의 자율 비행과 연관된 GPS, GCS(Geographic Coordinate System), 관성측정장치(IMU; Inertial Measurement Unit) 자이로스코프 등은 드론 외부의 신호나 드론 내부의 센서들로부터 필요한 정보

www.kci.go.kr

를 제공 받게 되는데 이때 신호가 왜곡되거나 악의적인 목적의 이상 신호를 전달받게 되면 드론의 안전 운항에 치명적 영향을 미칠 수 있다. 이와 관련해서 2015년 KAIST(Korea Advanced Institute of Science and Technology)에서 드론에 장착된 자이로스코픽 센서(Gyroscopic Sensors)들에 의도적인 소음을 사용한 주파수 교란을 시도하여 드론의 정상 동작을 방해하는 실험을 수행하여 드론이 무력화 될 수 있음을 증명하였기도 하였다.[13] 다음으로 IT 측면에서 보안 취약점들을 살펴본다면, 드론도 무선 네트워크 상 움직이는 하나의 노드로 볼 수 있기 때문에 다양한 해킹 기법들을 통하여 드론 내부의 각종 정보나 드론에 의해 수집된 중요 데이터의 약탈 그리고 통신 프로토콜의 취약성을 이용하여 변조된 명령에 의한 드론 자체의 탈취 등이 발생할 수 있으며 앞에서 기술하였듯이 이미 여러 사례들이 보고되고 있다.

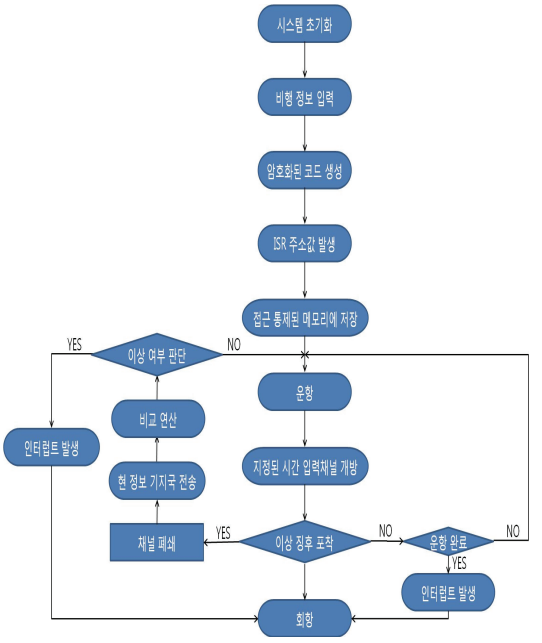

그림 3. 제안된 알고리즘
Figure 3. Proposed Algorithm

3.2 제안된 알고리즘

드론의 안전 운항을 위해 주파수 대역을 검사하는 등의 기존에 사용하던 스푸핑과 재밍 공격 방어 방법들은 더 이상 GPS를 안전하게 보호할 수 없음이 증명되었다.[14][15] 현재 군사용 드론의 경우 관련 업체들은 외부 신호에 무관하게 드론을 운항할 수 있도록 하여 GPS를 대체할 수 있는 높은 신뢰성을 갖는 기술과 새로운 암호화 기법을 적용하여 GPS를 안전하게 보호하려는 연구들이 진행되고 있는데 이는 막대한 비용과 시간이 필요한 실정이다.

본 논문에서는 저비용 산업용 드론의 운영으로 국한하여, 드론의 운영 목적에 의해 발생하는 여러 특징적인 사항들을 고려한 새로운 알고리즘을 제시하고자 한다.

운항 목표지점과 소요시간 등을 미리 파악할 수 있는 경우, 실제 운항 시 필요한 지리적 데이터, 위치 정보 등과 목표 지점에 따라 예상되는 경로 그리고 거리 등의 주요 데이터를 운항 전 미리 산출하여 보안에 취약한 입력 채널들로부터 제공받아야 하는 데이터의 양을 최소화한다. 산출된 데이터들은 드론에 탑재된 마이크로컨트롤러의 보호된 메모리의 지정된 영역에 저장하도록 하며, 하드웨어적인 인터럽트 기능을 적용하여 고정된 메모리 참조만으로 드론의 운영하여 비용 대비 보안성을 높일 수 있다. 또한 각종 센서 등을 통해 수집되는 원시 데이터와 운항에 필수적인 데이터들은 구별하여 처리하고, 후자의 경우 필요시에만 해당 망을 오픈하여 운영하며, 시간에 따라 랜덤하게 변화하는 지정된 간단한 암호화 변수 값을 통해 잘못된 신호 여부를 판별하게 하는 이중 보안 구조를 갖도록 함으로써 비용에 비해 안정성을 높이도록 하였다.

www.kci.go.kr

4. 결 론

드론은 그 운영 특성 상 오픈되어 있는 무선망의 이용과 여러 입력 센서들 그리고 직렬적인 안정성 구조를 갖기 때문에 외부 공격으로 인한 보안사고 위험이 매우 높다. 외부에서 들어오는 입력 자료들은 드론의 각 종 동작에 영향을 미치게 되는데, 보안에 가장 취약한 부분들은 드론과 지상 제어국 사이와 외부로부터 각 종 센서들로 전달되는 통신 지점이라 할 수 있다.

본 논문에서는 저비용 산업용 드론의 운영으로 국한하여, 운영 목적에 의해 발생하는 여러 특징적인 사항들을 고려한 새로운 알고리즘을 제시하였다. 제안된 알고리즘은 미리 산출하여 최소화된 운항 정보와 암호된 정보에 의해 개방되는 입력 채널의 운영 그리고 이중 보안 구조를 갖도록 하여 비용에 비해 안정성을 높였다. 또한 외부 신호에 의한 재밍 등의 사고에 어느 정도의 효과가 기대되며, 해킹 등에 공격에도 대처할 것으로 기대한다. 제안된 알고리즘은 기존의 하드웨어를 크게 변경하지 않으며 대부분의 처리가 소프트웨어적으로 수행됨에 따라 저비용 산업용 드론의 효율적 운영에 기여할 것으로 기대한다.

마지막으로 정부 관련 부처와 국내 관련업체들도 드론의 사업화에 필요한 법적 제도적 보완 사항들을 정리하여 조속히 입법화 하여야 할 것이며, 본 논문의 향후과제는 국제 표준화 동향을 고려한 알고리즘의 개발과 구현이 될 것이다,

References

[1] Unmanned Aerial Vehicle Operations in U.K. Airspace-Guidance, CAP 722, Section 2.1, Directorate of Airspace Policy, CAA, 2002.

[2] FAA Draft Advisory Circular, *Unmanned aerial vehicle design criteria,* Section 6. J, 15 Jul. 1994.

[3] http://www.wired.com, *Exclusive: Computer Virus Hits U.S. Drone Fleet,* 07. 10. 2011.

[4] A. Kim, B. Wampler, J. Goppert, and I-S. Hwang, Proc. of AIAA 2012, *Cyber attack vulnerabilities analysis unmanned aerial vehicles*, Jun. 2012.

[5] https://twitter.com/BIIntelligence, Dec. 2014.

[6] http://www.tealgroup.com/, Dec. 2014.

[7] *U.S. military sources: Iran has missing U.S. drone,* Fox News, Published, Dec. 5, 2011.

[8] K. Hartmann, and C. Steup, *The vulnerability of UAVs to cyber attacks-an approach to the risk assessment*. Proc. of 5th International Conference on Cyber Conflict, 2013.

[9] The Christian Science Monitor, *Iran hijacked US drone, says Iranian engineer(Video)*, Dec. 5, 2011.

[10] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, *On the requirements for successful GPS spoofing attacks,* Proc. of the 18th ACM conference on Computer and communications security, pp. 75-86, 2011.

[11] E. Rivera, R. Baykov, and G. Gu, *A study on unmanned vehicles and cyber security*, 2014.

[12] D. A. Dulo, *Unmanned aerial insecurity*, Cyber West 2015, Mar. 26, 2015.

[13] Y-M. Son, Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim, *Rocking drones with intentional sound noise on gyroscopic sensors*, Proc. of the 24th USENIX Security

www.kci.go.kr

Symposium, pp. 881-896, Aug. 12-14 2015.
[14] Military Avionics R&D: Spending Dips But Opportunities Soar, Avionics Today, Oct. 1, 2014.
[15] INFOSEC Institute, Hack-Proof Drones Possible with HACMS Technology, Posted in General Security on Jun. 3, 2014.

항공-IT 융합을 위한 보안 요구사항 분석

김성종
극동대학교 항공-IT 융합학과

요 약

4차 산업혁명의 시대를 맞이하여 여러 산업분야에서의 융합은 필연적인 것이라 할 수 있다. 항공 산업분야와 IT 산업분야의 융합도 주요한 미래 산업 중 하나로 관련 연구들과 기술 개발 및 국제 표준화 시도가 빠르게 진행되고 있다. 본 논문에서는 드론의 안정적인 운영을 위해, 보고된 여러 사고유형들을 통하여 필요한 보안 요구사항들에 대한 취약점들을 분석하였다. 주파수 대역을 검사하는 등의 기존에 사용하던 스푸핑과 재밍 공격 방어 방법들은 더 이상 GPS를 안전하게 보호할 수 없음이 증명되었다. 그리고 본 논문에서는 저비용 산업용 드론의 운영으로 국한하여, 드론의 운영 목적에 의해 발생하는 여러 특징적인 사항들을 고려한 새로운 알고리즘을 제시하였다. 제안된 알고리즘에서는 운항에 필요한 외부 데이터와 드론에 의해 수집되는 데이터를 분리 처리하는 기법을 제시하여 안정성을 높였다. 또한 필요시에만 해당 망을 오픈하여 운영하며, 시간에 따라 랜덤하게 변화하는 암호화 변수 값을 통해 잘못된 신호 여부를 판별하게 하는 이중 보안 구조를 갖도록 하여 비용에 비해 안정성을 높였다. 본 논문에서 제시한 알고리즘은 기존의 하드웨어를 크게 변경하지 않으며 대부분의 처리가 소프트웨어적으로 수행됨에 따라 저비용 산업용 드론의 효율적 운영에 기여할 것으로 기대한다.

감사의 글

This work was supported by the 2016 Far East University Research Grant (FEU2016R09)

Seong Jong Kim received the bachelor's degree in the Department of Electronics from the DanKook University in 1987. He received the M.S. degree and the Ph.D. degree in the Department of Electronics from DanKook University in 1989 and 1998, respectively. He was a professor in the Department of Ubiquitous IT at FarEast University since 1998. His current research interests include IoT, EoT, Security of IT and embedded system. He is a member of the KKITS.
E-mail address: ksj@kdu.ac.kr

www.kci.go.kr