https://doi.org/10.14400/JDC.2017.15.8.195

무인기 군집 비행 보안위협 및 보안요구사항 연구

김만식*, 강정호**, 전문석*
숭실대학교 컴퓨터학과*, 숭실대학교 평생교육원 정보보안학과**

A study on the security threat and security requirements for multi unmanned aerial vehicles

Mansik Kim*, Jungho Kang, Moon-seog Jun***
Dept. of Computer Science & Engineering, Soongsil University*
Dept. of Information Security, Soongsil University Lifelong Education Institute**

요 약 Unmanned Aerial Vehicle (UAV)는 군사적 목적으로 주로 이용되었지만 ICT의 발전과 저렴해진 제작비용으로 인해 다양한 민간 서비스에서도 점차 이용되고 있다. UAV는 앞으로 스스로 임무를 수행하는 자율비행을 할 것이라 기대되고 있는데, 복잡한 임무를 수행하기 위해서는 군집 비행이 필수적이다. UAV 군집 비행은 기존 UAV 시스템과 네트워크 및 인프라 구조가 달라 국내외에서 많은 연구가 이루어지고 있지만, 아직 안전한 UAV 군집 비행을 위한 보안위협 및 보안요구사항에 대한 연구가 이루어지지 않고 있다. 본 논문에서는 이러한 문제점을 해결하기 위하여 UAV 자율비행기술을 미 공군 연구소와 미국 육군 공병대를 기반으로 정의하고 UAV 군집비행기술 및 보안위협을 분류하였다. 그리고 각 UAV 군집비행기술의 보안위협에 따른 보안요구사항을 정의하여 비교 분석함으로써 향후 안전한 UAC 자율비행 기술 발전에 기여할 수 있도록 하였다.

주제어 : 드론, 무인기, 보안, 자율비행, 군집비행

Abstract Unmanned Aerial Vehicles (UAV) have mostly been used for military purposes but with the progress in ICT and reduced manufacturing costs, they are increasingly used for various private services. UAVs are expected to carry out autonomous flying in the future. In order to carry out complex tasks, swarm flights are essential. Although the swarm flights has been researched a lot due to its different network and infrastructure from the existing UAV system, There are still not enough study on security threats and requirements for the secure swarm flights. In this paper, to solve these problems, UAV autonomous flight technology is defined based on US Army Corps of Engineers (USACE) and Air Force Research Laboratory (AFRL), and swarm flights and security threat about it are classified. And then we defined and compared security requirements according to security threats of each swarm flights so as to contribute to the development of secure UAC swarm flights in the future.

Key Words : Drone, Unmanned Aerial Vehicle, Security, Autonomous Control, Swarm Flight

Received 23 June 2017, Revised 24 July 2017
Accepted 20 August 2017, Published 28 August 2017
Corresponding Author: Moon-seog Jun
(Dept. of Computer Science & Engineering, Soongsil University)

Email: mjun@ssu.ac.kr
ISSN: 1738-1916

1. 서론

Unmanned Aerial Vehicle (UAV)는 군사적 목적으로 주로 이용되었지만 ICT의 발전과 저렴해진 제작비용으로 인해 다양한 민간 서비스에서도 점차 이용되고 있다. [1,2,3] 한 예로 중국의 UAV 개발 업체인 DJI는 2015년에 약 1조 1,500억원의 매출을 달성하였으며, 미국의 Teal Group는 전세계 UAV 시장이 2024년에 147억 달러 규모가 될 것이라 예상하였다[4]. UAV는 앞으로도 계속 연구 및 발전되어 최종적으로 인간의 제어를 받지 않고 스스로 임무를 수행하는 자율비행을 할 것이라 기대되고 있다[5]. 그러나 컴퓨팅 자원이 부족한 UAV가 자율적으로 복잡한 임무를 수행하기 위해서는 군집 비행이 필수적인데, 대부분의 UAV 보안 연구는 단독 UAV 제어에 초점이 맞추어져 있다. 본 논문에서는 이러한 문제를 해결하기 위하여 UAV 군집 비행의 형태를 분류하고 보안 요구사항을 정의하였다.

2. UAV 자율비행기술

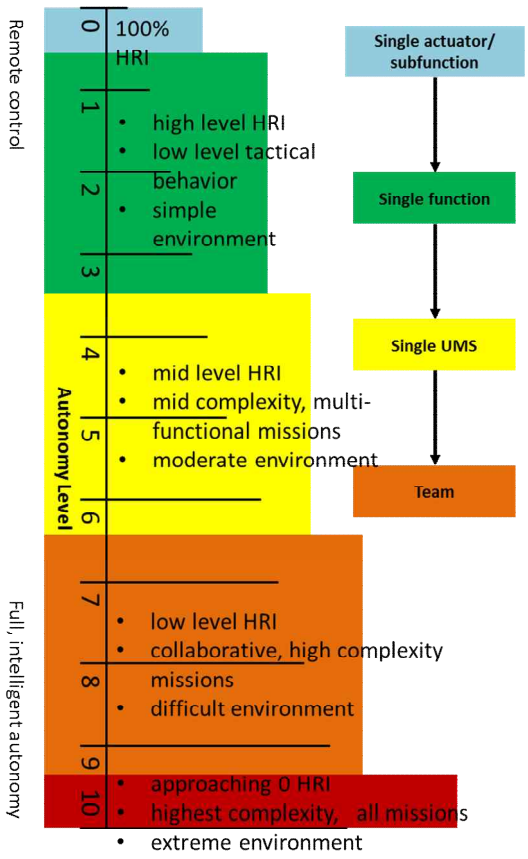
UAV 자율비행기술은 인간의 개입 없이 UAV가 임무를 수행하기 위해 자율적으로 비행하는 기술이며, UAV 자율성에 따라 여러 등급으로 나눌 수 있다. 미 공군 연구소 (AFRL, Air Force Research Laboratory)는 자율성 (Autonomy)을 외부의 명령 없이 스스로 목표를 설정하는 능력과 자유 의지라 정의하였다[6]. 그리고 UAV의 자율비행기술 레벨을 Remotely Piloted, Remotely Operated, Remotely Supervised, Fully Autonomous을 기준으로 <Table 1>과 같이 level 0 부터 10 까지 분류하여 Autonomous Control Level (ACL) chart를 제시하였다.

<Table 1> Final ACL Chart

Level	Level Description
10	Fully Autonomous
9	Battlespace Swarm Cognizance
8	Battlespace Cognizance
7	Battlespace Knowledge
6	Real Time Multi-Vehicle Cooperation
5	Real Time Multi-Vehicle Coordination
4	Fault/Event Adaptive Vehicle
3	Robust Response to Real Time Faults/Events
2	Changeable Mission
1	Execute Preplanned Mission
0	Remotely Piloted Vehicle

ACL chart에서 level 0은 파일럿이 원격으로 UAV를 조종하는 가장 낮은 기술 단계이며 level 10은 UAV가 마치 사람처럼 동작하는 가장 높은 기술 단계로 level이 높아질수록 UAV의 자율성이 높아진다.

미국 육군 공병대 (USACE, US Army Corps of Engineers)는 Unmanned Ground Vehicle (UGV)이나 Unmanned Aerial Vehicle (UAV), Unmanned Maritime Vehicle System (UMVS) 등과 같은 intelligent Unmanned Systems (UMS)의 자율성을 [Fig. 1]와 같이 level 0에서 level 10까지 Autonomy Level (AL)으로 분류하였다[7].



[Fig. 1] ALFUS summary model overall concept

level 0은 UAV가 인간과 로봇간의 상호작용하는 Human-Robot Interaction (HRI) 기술에 100%에 의존하는 가장 낮은 기술 단계이고 level 10은 UAV가 HRI에 전혀 의존하지 않는 가장 높은 단계로 ACL처럼 level이

높아질수록 UAV의 자율성이 높아진다. 미 공군 연구소와 미국 육군 공병대는 모두 UAV의 자율성 단계가 높아질수록 복잡한 임무를 수행할 수 있다고 정의 하였으며, 각각 ACL과 AL에서 level 5와 level 6에서부터 UAV간에 협업이 가능하다고 하였다. 일반적으로 UAV는 무게가 가볍고 무선으로 작동하기 때문에 배터리나 컴퓨팅 자원 등이 많이 부족하여 수행할 수 있는 임무에 한계가 있기 때문에, 복잡한 임무를 수행하기 위해서는 UAV간의 협업이 필요하다[8]. 현재 많은 연구가 진행되고 있는 UAV 군집비행기술은 UAV 협업 기술 중 하나로, 여러 UAV가 하나의 유기체처럼 서로간의 충돌 없이 상호 작용하며 비행하는 기술이다. 한 예로 David 등 4명은 바람 등과 같은 불안정한 환경에서 효율적으로 군집비행을 할 수 있는 충돌탐지 기법을 제안하였고, Ugur Cekmez 등 3명은 UAV 군집비행의 최적경로를 산출하기 위하여 Compute Unified Device Architecture(CUDA) 기반의 h Parallel Genetic Algorithms을 이용하였다[9,10]. 이와 같이 군집비행기술에 따라 UAV간에 통신하는 구조와 인프라가 기존 UAV 시스템과 달라지지만, 현재 대부분의 연구는 단일 UAV 시스템에 집중되어 있기 때문에 안전한 UAV 군집비행을 하기 위해서는 UAV 군집비행기술을 분류하고 군집비행에 따른 보안 위협을 분석하여 보안 요구사항을 정의 할 필요가 있다.

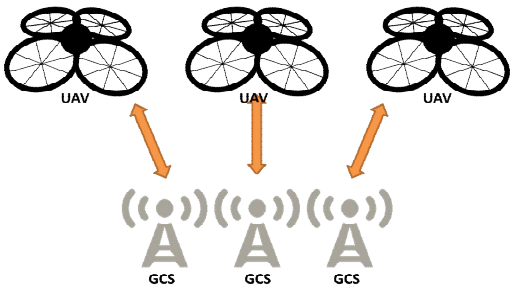
3. UAV 군집비행기술 및 보안위협

3.1 UAV 군집비행기술

본 논문에서는 다음과 같이 UAV 군집비행기술을 1:1 제어 기술과, 리더-팔로워 제어 기술, Airborne Control Center (ACC) 기반 군집 제어 기술, 복합 UAV 군집 비행 제어 기술로 분류하였다.

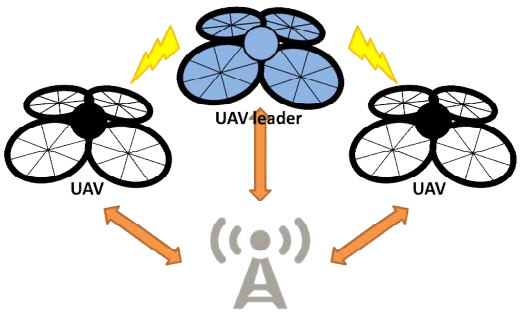
3.1.1 1:1 군집 제어 기술

1:1 제어 기술은 [Fig. 2]와 같이 군집 UAV에서 각 UAV는 GCS와 1:1로 대응하여 커뮤니케이션을 한다. 각 UAV는Ground Control Center (GCS)와 1:1로 대응되어 직접 GCS로부터 임무를 부여 받고 제어되며 수집한 데이터를 전송한다[11]. 같은 군집에 속하는 UAV는 모두 동등한 지위를 가지며 같은 임무를 수행하거나 서로 정보를 교환 할 수 있지만, 각 UAV를 제어하는 GCS의 허가 없이는 서로에게 접근할 수 없다. 각 UAV를 제어하기 쉽고 다른 UAV로부터 영향을 받지 않지만, 모든 UAV에게 GCS를 할당해야 하기 때문에 자원과 인력이 많이 소모 되며, 각 UAV가 따로 제어되기 때문에 실질적으로 군집제어라 보기 어렵다.



[Fig. 2] 1:1 multi-UAV control

3.1.2 리더-팔로워 군집 제어 기술



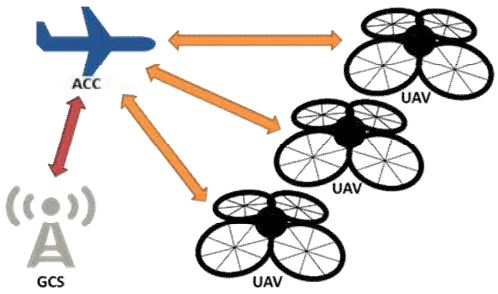
[Fig. 3] Leader-Follower multi-UAVcontrol

[Fig. 3]는 UAV 군집에서 리더를 선출하여 UAV 리더만 GCS와 커뮤니케이션 하는 리더-팔로워 구조를 보여준다. UAV 군집에서 오직 UAV 리더만 GCS로부터 임무를 부여 받거나 제어되며, 나머지 UAV는 UAV 리더에게 제어 되거나 맹목적으로 따른다[12]. 각 UAV로부터 수집된 데이터는 개별적으로 GCS에게 전송하거나 UAV 리더가 수집하여 GCS에게 전송할 수 있다. UAV 리더만 제어하면 군집을 이루는 나머지 UAV도 한꺼번에 제어가 되기 때문에, 1:1 제어 방법보다 적은 자원과 인력이 필요하다. 그러나 UAV 리더에게 이상이 생겼을

때 군집에 대한 통제권을 잃을 수 있으며 UAV 리더를 제외한 나머지 UAV는 항상 UAV 리더와 네트워크로 연결이 되어 있거나 시야(카메라, 적외선 등) 안에 있어야 한다.

3.1.3 ACC 기반 군집 제어 기술

[Fig. 4]는 ACC를 기반으로 한 UAV 군집 비행 제어 구조를 보여준다.

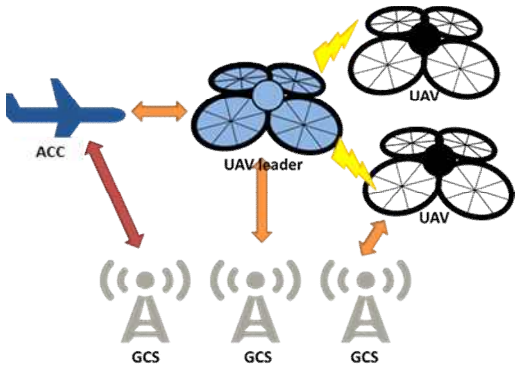


[Fig. 4] ACC based multi-UAV control

UAV 군집은 GCS와 직접 커뮤니케이션 하지 않고, 네트워크 및 시야가 닿는 ACC와 커뮤니케이션 한다. ACC는 공중에서 GCS로부터 받은 제어 신호나 임무를 UAV에게 전달하며, UAV 군집으로부터 받은 데이터를 GCS에게 전달한다[13]. 일반적으로 ACC는 UAV 보다 월등한 성능을 가지고 있어 리더-팔로워 구조에서 GCS 리더가 하지 못했던 복잡한 연산을 수행 할 수 있으며 UAV가 GCS와 커뮤니케이션을 할 수 없는 곳에서도 원활하게 UAV 군집을 제어할 수 있다. 그러나 ACC가 필수적으로 리더-팔로워 구조보다 많은 비용을 발생시킬 수 있으며 여전히 각 UAV 가 ACC 시야 안에 있어야 하며 ACC에게 이상이 생겼을 때 ACC 군집을 통제하기 어렵다는 문제점이 있다.

3.1.4 복합 UAV 군집 비행 제어 기술

[Fig. 5]는 앞서 언급한 3가지 UAV 군집 비행 제어 방안의 장점을 결합한 복합 UAV 군집 비행 제어구조이다[14]. 복합 UAV 군집 비행 구조에서는 각 UAV들이 부여 받은 임무에 따라 GCS에게 개별 제어 받거나 UAV 리더로부터 제어 받는다. UAV 리더는 UAV 군집의 나머지 UAV를 제어하면서 GCS와 커뮤니케이션을 하지만 GCS와의 통신거리가 닿지 않거나 긴급한 상황인 경우 가까이 있는 ACC와 커뮤니케이션을 하여 임무를 수행한다. ACC는 GCS와 UAV 군집 사이에서 정보를 전달하며 UAV 리더에게 이상이 생겼거나 임무에 필요한 경우 리더를 재지정하여 UAV 군집이 원활하게 임무를 수행할 수 있도록 할 수 있다. 복합 구조에서는 다양한 구성요소들이 유기적으로 연결되어 있으므로, 수행하는 임무나 비용 및 자원에 따라 구조를 변경 할 수 있으며, 긴급한 상황에도 대처 할 수 있다.



[Fig. 5] Composite multi-UAV control

3.2 UAV 보안위협

UAV에 대한 보안 위협은 <Table 2>와 같이 무선 네트워크의 보안 위협인 기밀성 (Confidentiality), 무결성 (Integrity), 가용성 (Availability)에 대한 공격으로 나눌 수 있다[15, 16].

<Table 2> UAV System Cyber-Security Threat

Threat	Description
Confidentiality	Interception of Information(Transfer/Loss)
Integrity	Fabrication of Information
	Modification of Information
Availability	Communication Interruption

● 기밀성 위협

기밀성에 대한 위협은 주로 인가되지 않은 접근이나 중간에 정보를 탈취하려고 하는 공격으로 주로 GCS나, UAV, 통신 링크, 사람을 대상으로 공격한다.

● 무결성 위협

무결성에 대한 위협은 기존 정보나 새로운 정보를 조작하려고 하는 공격으로 전송되고 있는 데이터나 저장되어 있는 데이터를 변경한다[17, 18]. 주로 번개나 태양광 등과 같은 자연재해나 재밍과 같은 악의적인 공격을 통해 위협 받는다.

● 가용성 위협

가용성에 대한 위협은 UAV의 통신을 방해하는 공격으로 무결성 위협과 같이 주로 자연재해나 악의적인 공격을 통해 위협받는다[19, 20].

4. UAV 군집비행 보안요구사항

UAV가 안전하게 군집비행하기 위해서는 군집비행 기술 종류 마다 기밀성, 가용성, 무결성 위협에 대하여 보안요구사항을 만족해야 한다. <Table 3>은 기존 UAV 비행과 UAV 군집비행의 보안요구사항을 보여준다.

<Table 3> Multi UAV System Cyber-Security Requirements

UAV System	Confidentiality	Integrity	Availability
1:1 control or existing UAV control	Data encryption between UAV and GCS	MDC and MAC between UAV and GCS	UAV and GCS resources
Leader-Follower control	Data encryption between leader UAV and follower UAVs, including 1:1 control condition	MDC and MAC between leader UAV and follower UAVs, including 1:1 control condition	leader UAV resources, including 1:1 control condition
ACC based control	Data encryption between GCS and ACC, and ACC and UAVs	MDC and MAC between GCS and ACC, and ACC and UAVs	ACC resources, including 1:1 control condition
Composite control	Including 1:1 control, Leader-Follower control, and ACC based control condition	Including 1:1 control, Leader-Follower control, and ACC based control condition	Including 1:1 control, Leader-Follower control, and ACC based control condition

4.1 1:1 군집 제어 기술 보안 요구사항

● 기밀성 보안요구사항

UAV가 교환하는 데이터는 UAV 군집에서 각 해당 UAV와 1:1로 통신하는 GCS에게만 송수신 되어야 하므로, 각 UAV-GCS 통신마다 기밀성을 보장하기 위하여 다른 키를 이용하여 암복호화 되어야 한다. UAV간의 협업을 위한 데이터 교환은 GCS단에서 수행함으로써 기밀성을 유지하면서 군집 제어를 할 수 있다.

● 무결성 보안요구사항

UAV 군집에서 각 UAV-GCS마다 개별 데이터 및 제어 명령을 송수신하기 때문에 제 3자의 도움 없이 데이터 변조 및 조작, 에러에 대해서 대처할 수 있도록 중요한 통신 데이터에 대하여 변경 감지 코드 (MDC, Modification Detection Code)를 덧붙여야 하며, 인증이 필요한 경우에는 메시지 인증 코드 (MAC, Message Authentication Code)를 추가해야한다.

● 가용성 보안요구사항

UAV 군집에서 각 UAV는 하나의 GCS와 통신을 하기 때문에 UAV나 GCS에게 많은 자원이 필요하지 않다. 그러나 악의적인 공격자가 가용성 공격을 시도하거나 자연재해로 인하여 컴퓨팅 자원이 고갈 될 수 있기 때문에, 자원이 고갈되었을 때 대처할 수 있는 여분을 항시 남겨놔야 한다.

4.2 리더-팔로워 제어 기술 보안 위협

● 기밀성 보안요구사항

리더 UAV를 제외한 각 UAV는 리더 UAV로부터 제어 데이터를 전달받기 때문에 리더 UAV와 군집의 나머지 UAV간에 암호화 통신이 필수적이다. 각 UAV는 리더 UAV와 독립적으로 기밀성을 유지하기 위해서는 각 통신 마다 다른 키를 이용하여 보안통신을 해야 한다. UAV와 GCS간의 기밀성 유지는 1:1 군집 제어 통신과 보안 요구사항이 같다.

● 무결성 보안요구사항

GCS로부터 리더 UAV에게 전달되는 데이터와 더 UAV로부터 나머지 UAV에게 각 전달되는 데이터의 무결성이 보장되지 않는다면, UAV 군집의 제어 데이터가 조작 및 변경 되어 군집 비행이 적절하게 이루어지지 않을 수 있다. 'GCS-리더 UAV-UAV'간의 통신에서 데이터의 무결성을 보장할 수 있도록 MDC, MAC등의 데이

터 무결성 보장 기술을 적용해야한다.

● 가용성 보안요구사항

리더 UAV는 나머지 UAV보다 많은 데이터를 송수신하기 때문에 더 많은 컴퓨팅 자원을 가지고 있지만, 리더 UAV의 자원이 고갈되면 전체 군집이 제대로 비행하지 못하기 때문에 악의적인 공격자로부터 가용성 공격을 당할 확률이 높다. 리더 UAV는 항시 여분의 자원을 확보해 놔야 하며, 필요시 작업을 다른 UAV에게 배분할 수 있어야 한다.

4.3 ACC 기반 군집 제어 기술 보안 위협

● 기밀성 보안요구사항

ACC 기반 군집 제어에서 통신 구간은 크게 GCS-ACC와 ACC-UAV 군집으로 나뉜다. ACC는 일반적으로 복잡한 연산을 할 수 있고 UAV 군집의 각 UAV에 대한 데이터를 GCS로부터 전달 받으므로 기존 환경에서 이용하는 기밀성 보장 보안 통신 기법을 이용해야 하고, GCS와 각 UAV 간에도 데이터 기밀성을 위하여 경량화된 보안 통신 기법을 이용해야 한다.

● 무결성 보안요구사항

앞서 언급한 군집 제어 기술과 같이 MDC, MAC 등의 데이터 무결성 보장 기술을 각 GCS-ACC와 ACC-UAV 군집 통신 구간에 적용해야 하고, GCS-ACC 구간에서는 ACC에서 즉각적인 처리를 하기 위하여 데이터 변조 탐지뿐만이 아니라 변조된 데이터를 자가 수복할 수 있는 기법을 이용해야 한다.

● 가용성 보안요구사항

GCS 뿐만이 아니라 ACC는 UAV 군집 제어의 가용성 공격 대상이 될 수 있다. ACC의 가용 자원은 GCS에서 항시 실시간으로 모니터링 하여 UAV 군집을 제어하는데 이상이 없도록 하여야 하고, 만약 가용자원이 없을시 GCS에서 직접적으로 UAV 군집을 컨트롤 하거나 다른 매체를 통해 통신할 수 있는 방안을 마련해야 한다.

4.3 복합 UAV 군집 비행 제어 기술 보안 위협

● 기밀성 보안요구사항

복합 UAV 군집 비행 제어 기술은 GCS, ACC, 리더 UAV등을 복합적으로 이용하여 다양한 위협이나 예외상황에 대해서 대처할 수 있지만, 통신 구간이 다양해져 기밀성 공격대상이 많아진다. 기밀성을 보장하기 위하여 각 통신 구간에 앞서 언급하였던 군집 비행 제어 기술에서 요구 하였던 기밀성 보장 기법들을 갖춰야 한다.

● 무결성 보안요구사항

기밀성과 마찬가지로 다양한 통신구간으로 인해 공격자가 데이터를 변조할 수 있는 구간이 다양해져 무결성을 보장하며 각 구간에서 데이터를 교환하기 위해서는 각 통신 데이터에 대하여 무결성 보장 코드 및 자가에러 수복 기법을 환경에 맞게 적용시켜야 한다.

● 가용성 보안요구사항

복합 UAV 군집 비행 제어 기술은 사용할 수 있는 가용자원이 UAV 뿐만이 아니라 리더 UAV, ACC, GCS 등 다양하게 분포되어 있다. 그러나 각각 중간 요소가 가용자원이 다 소모되면 전체 UAV 군집이 제어되지 않기 때문에 반드시 GCS에서 가용자원을 모니터링 해야 한다.

5. 결론

UAV는 주로 군용으로 연구 및 개발 되었지만, ICT 기술 발전으로 인해 이제 많은 민간 서비스에서도 이용되고 있다. UAV는 지속적으로 성장하여 자율성을 가지고 임무를 수행할 것이라 기대되는데, 복잡한 임무를 수행하기 위해서는 많은 컴퓨팅 자원을 확보하기 위하여 UAV 군집 비행이 필수적이다. 안전한 UAV 군집 제어를 위해 보안 위협과 요구사항을 분석해야 하지만 기존 대부분의 UAV 보안 연구는 단독 UAV 제어에 맞추어져 있다는 문제점이 있다. 본 논문에서는 UAV 군집 비행을 분류 하고 각 UAV 군집 비행마다 필요한 보안요구사항을 정의 하여 향후 UAV 자율비행 발전에 기여할 수 있도록 하였다.

REFERENCES

[1] Pan-Seop Shin, Sun-Kyung Kim, and Jung-Min

Kim. "Intuitive Controller based on G-Sensor for Flying Drone." Journal of Digital Convergence, Vol. 12, No. 1, pp.319-324, 2014.

[2] Keun-Wang Lee and Joon-kyu Park, "Construction and Analysis of Geospatial Information about Submerged District Using Unmanned Aerial System ", Journal of Digital Convergence, Vol. 14, No. 12, pp.225-230, 2016.

[3] Jeong-Pil Lee, Jae-Wook Lee, Keun-Ho Lee, "A Scheme of Security Drone Convergence Service using Cam-Shift Algorithm", Journal of the Korea Convergence Society, Vol. 7, No. 5, pp29-34, 2016.

[4] A. L. Lee, "Drone market and industry trend", Weekly TIP, Vol. 53, Convergence Research Policy Center, 2017.

[5] Ryan, A., Zennaro, M., Howell, A., Sengupta, R., and Hedrick, J. K., "An overview of emerging results in cooperative UAV control." Decision and Control, 2004. CDC. 43rd IEEE Conference on. Vol. 1. IEEE, 2004.

[6] Clough, Bruce T. "Metrics, schmetrics! How the heck do you determine a UAV's autonomy anyway", AIR FORCE RESEARCH LAB WRIGHT-PATTERSON AFB OH, 2002.

[7] Huang, H. M., Pavek, K., Albus, J., and Messina, E. "Autonomy levels for unmanned systems (alfus) framework: An update.", Defense and Security. International Society for Optics and Photonics, Vol. 27, pp.439-448, 2005.

[8] Gaudiano, P., Shargel, B., Bonabeau, E., and Clough, B., "Control of UAV swarms: What the bugs can teach us.", 2nd AIAA Unmanned Unlimited Conf. and Workshop & Exhibit, pp.6624-6624, 2003.

[9] Alejo, D., Cobano, J. A., Heredia, G., and Ollero, A. "An Efficient Method for Multi-UAV Conflict Detection and Resolution Under Uncertainties.", Robot 2015: Second Iberian Robotics Conference. Springer, Cham, pp.635-647, 2016.

[10] Cekmez, Ugur, Mustafa Ozsiginan, and Ozgur Koray Sahingoz. "Multi-UAV path planning with parallel genetic algorithms on CUDA architecture." Proceedings of the 2016 on Genetic and Evolutionary Computation Conference Companion. ACM, pp.1079-1086, 2016.

[11] Cummings, M. L., Bruni, S., Mercier, S., and Mitchell, P. J., "Automation architecture for single operator, multiple UAV command and control.", Massachusetts Inst Of Tech Cambridge, 2007.

[12] Rabinovich, Sharon, and Gabriel Elkaim. "Leader-Follower UAVs for Formation Testing." 2016.

[13] Howitt, Sara, and Dale Richards. "The human machine interface for airborne control of UAVs." 2nd AIAA" Unmanned Unlimited" Conf. and Workshop & Exhibit. 2003.

[14] M.S. Kim, H.J. Kim, and M.S Jun, "Classification and Research of Multi-UAV Control Scheme", KIPS, Conf., Apr. 2017.

[15] Rodday, N. M., Schmidt, R. D. O., and Pras, A., "Exploring security vulnerabilities of unmanned aerial vehicles." Network Operations and Management Symposium (NOMS), 2016 IEEE/IFIP. IEEE, pp.993-994, 2016.

[16] Seung-Soo Shin, Gyoo-Soo Chae, Tae-Hyun Lee, "An Investigation Study to Reduce Security Threat in the Internet of Things Environment," Journal of IT Convergence Society for SMB, Vol. 5, No. 4, pp. 31-36, 2015

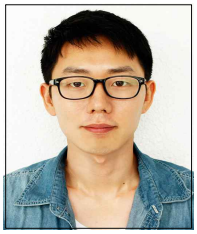
[17] Jeongnyeo Kim, "Security Core Technology Implementation for Hardware-based Smart Devices" Journal of Digital Convergence Vol. 14, No. 11, pp.501-505, 2016.

[18] Jung Hyun Soo, Gyoo-Soo Chae "Detection of Forgery of Mobile App and Study on Countermeasure", Journal of Convergence for Information Technology, Vol. 5, No. 3, pp.27-31, 2015.

[19] Sunghyuck Hong, "Packet attack detection, route security, Distributed denial of service, DDoS detection algorithm, Network" Journal of Digital Convergence Vol. 12, No. 1, pp.423-249, 2014.

[20] Sik-Wan Cho, Won-Jun Jang, Hyung-Woo Lee, "mVoIP Vulnerability Analysis And its Countermeasures on Smart Phone", Journal of the Korea Convergence Society, Vol. 3, No. 3, pp.7-12, 2012.

김 만 식(Kim, Man Sik)



- 2010년 2월 : 안양대학교 컴퓨터공학과(공학사)
- 2012년 6월 : Towson University Computer Science(공학석사)
- 2014년 9월 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정
- 관심분야 : 네트워크 보안, UAV
- E-Mail : mansik@ssu.ac.kr

강 정 호(Kang, Jung Ho)

- 2000년 2월 : 서울과학기술대학교 컴퓨터공학과(공학사)
- 2002년 2월 : 서울과학기술대학교 컴퓨터공학과(공학석사)
- 2013년 12월 : 숭실대학교 컴퓨터공학과 (박사)
- 2013년 ~ 현재 : 숭실대학교 평생교육원 정보보안학과 교수
- 관심분야 : NFC, 시큐어코딩
- E-Mail : kjh@naver.com

전 문 석(Jun, Mun Seog)

- 1989년 2월 : Univ. of Maryland Computer Science(공학박사)
- 1991년 2월 ~ 현재 : 숭실대학교 컴퓨터학과 정교수
- 관심분야 : RFID, PKI 컴퓨터통신
- E-Mail : mjun@ssu.ac.kr