화생방 정찰 드론의 군집비행 시 사이버전자전 취약점 및 대응방안 분석★

김 지 원*, 박 상 준**, 이 광 호***, 정 찬 기***

요 약

5대 게임 체인저는 적의 비대칭 위협에 대응해 전시 국민 피해를 최소화하고 최단시간 내 전쟁을 승리로 이끄는 지상작전 수행개념이다. 이 중에서 드론봇(드론+로봇) 운용을 위한 네트워크 구성방안 연구는 육군이 창설하는 여러 개의 드론봇 전투단을 ICT를 통해 유기적으로 연결해 통합 C4I체계를 갖춤으로써 통합작전을 수행하는 핵심이 되는 연구이다. 본 연구에서 제시하는 드론봇의 한 형태인 화생방 정찰 드론의 군집비행 운용은 차량 및 인간을 대신하여 화생방 물질 탐지와 신속한 상황 공유를 가능하게 한다. 그럼에도 불구하고 화생방 정찰드론의 군집비행에 대한 연구와 그에 대한 사이버전자전의 취약점에 대한 연구는 아직 부족한 실정이다. 그러므로 본 연구에서는 화생방 정찰 드론을 군집비행 운용 시 취약점과 대응방안을 제시하여 미래전 연구의 토대를 마련하고자 한다.

A Study on Vulnerability of Cyber Electronic Warfare and Analysis of Countermeasures for swarm flight of the NBC Reconnaissance Drones

Jee-won, Kim*, Sang-jun Park**, Kwang-ho Lee***, Chan-gi Jung***

ABSTRACT

The 5 Game changer means the concepts of the army's operation against the enemy's asymmetric threats so that minimize damage to the public and leads to victory in war in the shortest time. A study of network architecture of Dronebot operation is a key study to carry out integrated operation with integrated C4I system by organically linking several drones battle groups through ICT. The NBC reconnaissance drones can be used instead of vehicles and humans to detect NBC materials and share situations quickly. However, there is still a lack of research on the swarm flight of the NBC reconnaissance drones and the weaknesses of cyber electronic warfare. In this study, we present weaknesses and countermeasures of CBRNs in swarm flight operations and provide a basis for future research.

Key words : National defense, drone, NBC, swarm flight, network, cyber electronic

접수일(2018년 5월 31일), 게재확정일(2018년 6월 20일)

★ 본 논문은 2018년 화랑대연구소 지원에 의하여 연구되었음.

* 육군사관학교 컴퓨터과학과
** 육군사관학교 전자공학과
*** 아주대학교 NCW학과

1. 서 론

게임 체인저(game changer)란[1] 기존의 시장에 엄청난 충격을 가할 정도로 혁신적인 아이디어를 가진 사람을 가리키는 용어로 사용된다. 2017년 육군총장 부임 이후 제시한 5대 게임 체인저는 적의 비대칭 위협에 대응해 전시 국민 피해를 최소화하고 최단시간 내 전쟁을 승리로 이끄는 지상 작전 수행개념으로, 전천후·초정밀·고위력 미사일 3종과 공지기동부대, 특수임무여단, 드론봇(드론+로봇) 전투체계 등이 핵심 구성요소이다. 이 중에서 드론봇 운용을 위한 네트워크 구성방안 연구는 육군이 창설하는 여러 개의 드론봇 전투단을 ICT를 통해 유기적으로 연결해 통합 C4I체계를 갖춤으로써 통합작전 수행의 핵심이 되는 연구이기도 하다.[1].

이러한 드론봇의 한 형태인 화생방 정찰 드론은 측정 장비를 탑재하여 차량 및 인간을 대신하여 화생방 물질을 탐지하고 신속한 상황 공유를 가능하게 할 수 있다. 특히 군집형태(swarm)의 초소형 드론을 운용할 경우 보다 다양한 정보를 획득할 수 있을 것으로 예상된다. 그럼에도 불구하고 국내에서는 초소형 드론의 비행체의 비행 기술은 많이 연구되고 있으나 군집비행을 하는 드론들의 네트워크 구성 및 임무 수행 방법과 사이버전자전에 대한 연구는 아직 부족한 실정이다[2].

그러므로 본 논문에서는 군집비행을 하면서 화생방 정찰임무를 수행하는 화생방 정찰 드론 운용 간 사이버전자전에 대한 취약점을 파악하고 그 대응 방안을 제시하고자 한다.

2. 드론 기술 동향

드론의 정의는 조종사가 비행체에 탑승하지 않고 원격조종(Remote Piloted) 또는 사전에 정의된 프로그램에 의해 자동비행(Auto Piloted), 반자동비행(Semi-Auto Piloted) 방식으로 자율비행 하는 비행체로 정의할 수 있다. 드론은 인공지능 기반으로 자율 판단하는 비행체, 비행체를 통제하는 지상통제장치(Ground Control Station), 통신장비(Data Link), 지원장비 (Support Equipment) 등으로 구성되어 있다[3]. 항공 무인분야는 민간 및 국방에서 활발히 개발되고 있으나 국방 분야의 무인전투기/공격기, 장기체공 정찰 무인기 등이 최신 기술의 집약체로서 기술진보를 선도하고 있으며, 민간에서는 택배용 드론 등 실용적 드론 개발을 진행 중이다.

2.1 국 내

국내에서는 아직 초소형 무인기에 대한 연구는 활발하지 않으나, 단일 무인기를 이용한 공간정보 획득에 필수적인 Mapping시스템 및 무인항공기 충돌회피 기술연구 등이 진행 중이다[2].

2.2 국 외

국외에서는 2000년 중반 10~20Cm급 비행체를 개발하였으며 초소형 무인기 네트워크의 민간이용에 대한 연구는 2010년 중반부터 학계에서 발표되고 있다. 또한, 군집형 정찰플랫폼 영상획득기술을 별도로 연구 및 개발 중이다. 현재는 한 명의 조종사가 조종이 가능한 무인기의 개수를 늘리기 위한 연구를 수행하고 있으며, 뇌파를 이용한 조종기술 연구도 진행 중이다[2].

2.2.1 Perdix 군집무인기

2013년 MIT Lincoln Laboratory Beaver Works Center에서 Perdix micro surveillance UAV 개발을 착수로 2014년 F-16에서 Perdix 공중 사출을 처음으로 수행하였다. 2015년 알래스카에서 90회의 임무 비행연습 수행하여 2017년 미 국방부의 Strategic Capabilities Office는 670대 이상의 Perdix AV 비행을 보고하였으며, 추후 1,000대 이상의 운용을 중이며 현재 는 영상획득용으로 운용 중이다[2].

2.2.2 이항(eHang) 드론 쇼

최근 중국 드론 기업에 의한 드론 공연이 활발하게 진행되고 있는데, 중국의 대표적인 드론 제조 회사인 이항(eHang)이 중국 광저우시에서 드론 1000대에 대한 동시 제어 기술을 활용한 드론 쇼를 공연하였다. 이 공연에서는 290m × 19m 공간에 드론 1000대를 1.5미터 간격으로 배치하였다. 통신 시스템, 비행 안전 시스

1) 네이버 시사용어 사전(검색일: 18‘ 05. 27)

템이 제대로 동작되는 상태에서 한 대의 중앙제어 컴퓨터로부터 1000대의 드론이 제어됨을 확인하였고 세계 기록을 수립하였다[4].

2.2.3 평창올림픽 슈팅스타 드론

92개국의 선수들이 모인 2018년 평창 동계올림픽 개막식에서 인텔社가 1,200개가 넘는 슈팅스타 드론으로 최신 기네스 세계 기록을 갱신하였다[5]. 특히, 1,200개의 비행체를 3D로 동사에 제어하고 구성하며 물리적 구간의 실제 센싱 수치를 실시간으로 적용하는 기술은 빠르고 정확한 계산이 요구되는 기술이다. 특히, 1,200여개의 통신 채널 구성과 이를 실시간으로 제어하기 위한 대역폭 기술, 드론이 일정한 시간을 유지하기 위한 GPS기반 위치 지정 기술, 바람이라는 변수를 극복하기 위한 개별 모터동력 균형제어 기술이 핵심이 되었고 이런 기술을 모두 한 사람의 조종사가 조종하였다.

이와 같이 군집비행의 최근 기술들은 군집개체를 모두 개별로 조정하는 능동형으로 하는 방식과 하나의 송신 플랫폼에 다수의 수신기를 군집으로 하는 반 능동형이 있다. 반 능동형의 경우 소형화, 항재밍(anti-jamming), 스텔스 기능이 우수하여 많이 쓰이는 추세이다.

3. 화생방 드론 활용

화생방 작전은 부대 규모를 막론하고 전군 모든 부대에서 운영하고 있는 작전개념이다. 화생방 작전에서 드론을 활용해야 하는 이유는 높은 고도에서 운용되기에 지상에서보다 정찰임무가 가시적이고 신속하기 때문이다. 화생방 작전 특성상 오염탐지, 제독 등의 작전수행은 국지적으로 실시되기 때문에 화생방 드론의 운용가능 제대는 군단급 이하의 전술제대가 될 것이다.

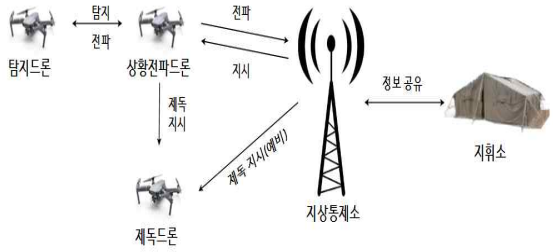
또한, 화생방 드론의 경우는 <표 1>과 같은 이유로 군집으로 이루어져야하며 탐지드론, 제독드론, 상황전파 드론으로 구성되어야 하며 드론의 기능별로 주 예비로 구분하여 최소 6대의 드론이 한 팀이 되어 운용되어야 한다.

화생방 드론의 구성요소와 전파체계는 (그림 1)과 같다. 탐지 드론은 장착된 탐지지를 통해 오염종류와

<표 1> 단일 UAV와 군집 UAV의 비교

특 징	단일 UAV	군집 UAV
고장시 영향도	영향이 크며, 임무지속 수행 제한으로 실패	영향이 작으며, 시스템 재구성시 임무수행 가능
확장성	제 한	높 음
생존성	제 한	높 음
임무수행 속 도	제 한	협동 임무 수행으로 신속수행
비행체 비 용	높 음	저 렴
통 신 대역폭	광대역	중계통신으로 대역소요량 감소
안테나	(무)지향성	지향성
제 어 복잡도	낮음	높음

오염지역 범위를 신속히 파악하고 상황전파 드론은 지상통제소에 탐지된 정보를 전파하면 지휘소에서 실시간 정보가 공유되어 제독 여부를 판단할 수 있는 시스템으로 운용된다. 제독의 경우는 전파체계를 이중으로 두어 상황전파 드론이 불가용 하거나 상황이 급박할 시 지상통제소에서 직접 제독 드론에게 제독을 지시할 수 있다. 이와 같은 상황 전파체계는 군집형태로 한 팀이 되어서 움직여야만 신속한 정보공유와 오염지역을 파악할 수 있다.



(그림 1) 화생방 드론의 구성 및 전파체계

3.1 군집비행 시 정보전송체계

적의 화생방 공격이 예상되거나 이동하려고 하는 작전지역이 이미 화생방 오염이 되었을 것으로 예상될 경우 오염예상 지역으로 화생방 드론들을 투입하여 화생방 오염 여부를 신속히 탐지한다. 탐지결과는 상황

전파드론에 의해 지상통제소로 실시간 전송하며 이를 확인한 지상통제소에서는 제독 등의 임무를 지시한다. 오염종류 및 오염지역 범위 등을 확인한 지상통제소는 지휘통제체계 및 전술정보통신체계를 통해 전군으로 전파하여 전 부대에서 화생방 피해상황에 대한 정보를 실시간으로 공유한다. 제독지시를 받은 제독드론은 오염지역의 정보(지형정보, 풍향, 풍속 등)를 고려하여 오염범위 및 지형에 따라 오염범위가 적을 경우에만 제독을 실시하고 광범위한 지역이 오염되었을 경우에는 별도의 제독차량을 투입하여 제독을 실시한다. 제독 임무가 끝나면 다시 탐지 드론을 보내 재탐지를 실시한다. 이 모든 상황을 상황전파 드론이 영상 및 기타 방법으로 기록하여 실시간 전부대가 실시간 공유할 수 있도록 한다. 만약, 지상 지휘소가 이동을 하게 된다면 화생방 드론은 지휘소가 이동하기 전 오염지역의 통로를 개척하는 등에 관한 정보를 제공하는 용도로 활용되고 정찰 및 제독이 완료된 이동구간을 통해 지휘소가 이동할 수 있도록 한다[4].

4. 취약점 및 대응방안

군집비행 시 화생방 정찰 드론은 비행체 상호간 네트워크를 구성하여 자체 통신을 하며, 상황전파 드론이 지휘소와 통신을 한다. 네트워크 내에서 유통되는 정보는 드론의 위치 및 배터리 등 상태 정보, 화생방 물질의 탐색 결과, 제독 결과, 지휘소와 드론 간 명령 및 상황보고 메시지 등이다. 이러한 정보들이 유통되는 네트워크 내에는 GPS 교란, 도청(eavesdropping), 재밍(jamming), 시빌 공격(Sybil attack) 등의 적의 사이버전자전 수행에 따른 외부요인에 의한 취약점과 제한된 배터리 용량으로 발생하는 자체 취약점이 발생한다. 본 장에서는 군집비행 간 화생방 정찰 드론 네트워크에서 발생하는 이러한 취약점에 대한 대응방안을 논의하고자 한다.

4.1 GPS 교란 시 취약점 대응방안

GPS는 지구 전역을 대상으로 위성을 통해 위치 및 시각정보를 제공하는 범지구 위성항법시스템(GNSS) 중 하나로 1970년대 초 미국 국방부에서 개발하였고 우리나라에서 주로 쓰이고 있는 시스템이다[5]. GPS는 위성에서 보내는 전파신호로 정확한 위치를 파악할 수 있지만 위성이 상공 2만km 밖에 있어 신호세기가 미약하여 전파 방해에 매우 취약하다. 그러므로 같은 주파수 대역에 강력한 방해전파를 이용하여 교란하기가 쉽다. GPS 교란 공격의 대응방안으로는 범지구 위성항법시스템(GNSS, Global Navigation Satellite System)을 복합적으로 사용하는 것이다. 이 시스템은 GPS 하나만 사용하는 일반적인 항법과는 달리 항상 전 지구를 커버할 수 있도록 하여 위성에서 발신한 전파를 이용하여 지구상의 사용자에게 언제 어디서나 누구에게나 위치, 고도, 속도, 시간정보를 제공할 수 있도록 하는 시스템이다[7]. 미국의 GPS, 러시아의 GLONASS, 유럽의 Galileo, 중국의 Beidou, 일본의 QZSS가 대표적이며, 각 시스템별 주파수는 <표 2>와 같다. 이와 같이 다중 GNSS를 사용하면 주파수 교란으로 인한 위치 및 시각 정보의 오차 발생 등에 대응이 용이할 것이다.

<표 2> GNSS 별 주파수

시스템	신호, 주파수 범위(MHz)
GPS	L1:1560~1590, L2:1215~1239, L5:1164~1188
GLONASS	L1:1598~1605, L2:1243~1249, L3:1189~1213
BeiDou	B1:1559~1563, B2:1195~1219, B3:1256~1280
Galileo	E1:1558~1592, E5:1166~1217, E6:1258~1300
QZSS	L1:1560~1590, L2:1215~1239, L5:1164~1188

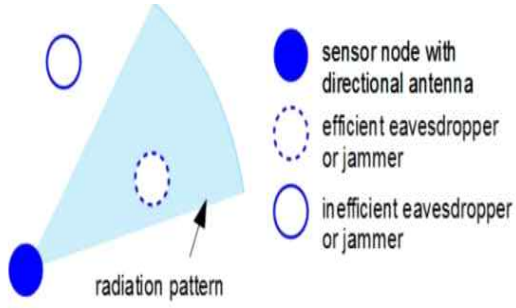
4.2 네트워크 취약점 대응방안

4.2.1 도청(eavesdropping)과 재밍(jamming)

(그림 2)에서 보는 바와 같이 군집비행 시 드론에 대한 도청(eavesdropping)은 비인가 수신자로서 청취하는 형태로 드론 네트워크의 상황전파 및 명령 메시지 등 정보를 빼내는 형태이다. 이에 대응방안은 빅데이터, 클라우드 등 고속 환경 및 모바일기기 등 경량 환경에서 기밀성을 제공하기 위해 개발된 256비트 블

록암호 알고리즘인 LEA(Lightweight Encryption Algorithm)을 사용하는 것이 적합하다.

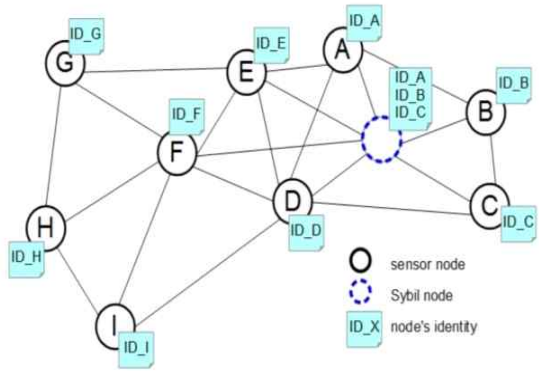
재밍(jamming)은 정상 노드로 가장하여 공격자의 비행체가 마치 아군의 비행체인 것처럼 아군의 드론에 상황전파 및 지시하여 작전임무 수행을 교란하는 것이다. 이에 대한 대응방법으로는 스펙트럼 확산 방식중의 하나인 확산 스펙트럼 변조방식인 주파수 호핑(FH, Frequency Hopping Spread Spectrum) 적용을 통해 적의 재밍으로 인한 피해를 최소화하고 적의 재밍이 발생했음을 인지하는 즉시 지상통제소에 EMI 보고를 하고 즉시 예비주파수로 자동으로 변경할 수 있는 알고리즘을 적용함으로써 적의 사이버전자전 상황에 능동적으로 대처가 가능할 것이다.



(그림 2) 도청과 재밍[9]

4.2.2 시빌 공격(Sybil attack)

시빌 공격(Sybil Attack)은 일종의 네트워크 해킹 공격으로 특정한 목적을 얻기 위해 한 명의 행위를 여러 명의 행위인 것처럼 속이는 공격 형태를 의미한다[8]. 시빌 공격은 실제로 다양한 네트워크 시스템의 기능을 무력화하는데 사용될 수 있는데 공격자가 복수개의 ID를 이용하여 공격대상 네트워크에 가입 및 활동하는 것으로 (그림 3)에서 점선으로 표시한 Sybil node가 ID_A, B, C를 사용하여 공격대상 네트워크에 가입하여 활동하는 것이다. 이러한 시빌 공격에 대한 대응방법으로는 노드들과 P2P네트워크를 형성하지 않고 있는 관리노드가 특정 노드와 연결하여 엄청난 양의 트래픽을 주는 방법이 있다. 군집비행의 노드들은 각각 개별적인 노드이므로 엄청난 트래픽이 주어져도 네트워크 내의 다른 노드의 트래픽에는 영향을 주지 않는다. 하지만 ID를 복사해서 쓰는 시빌 공격 노드는 서로 영향을 받는데 이를 이용하여 노드들의 트래픽 양을 검사하여 공격자의 노드를 찾아내는 방법으로 대응할 수 있다[10].



(그림 3) 시빌 공격 방법[9]

4.2.3 전력소모

드론의 동력원은 엔진을 사용해서 얻는 방법과 배터리를 사용하여 얻는 방법으로 크게 나눌 수 있다. 본 논문에서는 드론의 동력원은 배터리를 사용하는 것으로 가정한다. 화생방 정찰 드론이 군집비행을 하며 임무를 수행하면 탐지 및 제독 임무수행에 따른 전력소모와 드론 상호간 그리고 지휘소와 상황전파 및 명령수령, 정찰 및 제독 결과 등의 데이터 전송 등 통신을 하면서 전력이 소모된다. 예로 살펴보면, IEEE 802.11n, non-MIMO의 경우 모드별 전력 소모량이 TX, RX , Idle, Sleep간 1280 mA, 930 mA, 820 mA, 100 mA가 소모된다. 이는 5,200 mAh 배터리의 경우, 12.5A를 사용하는 소형 UAV를 약 25분간 비행할 수 있는 배터리 용량에 해당한다. 통상적으로 드론의 동력원에서 네트워크 장비의 전력소모 비중은 16%를 차지한다고 한다[7]. 드론의 동력원에서 네트워크 운용으로 발생하는 전력소모를 줄이기 위해서는 비행 동력과 통신 동력을 분리하여 사용하는 방법이 있으며 다른 방법으로는 저전력 장거리 통신기술인 LPWA(Low Power Wide-Area)를 활용하는 것이다. LPWA에서 에너지 소모를 야기하는 원인 중 저전력으로 통신하기 위해서는 에너지 효율적인 MAC 프로토콜이 필수적인데[11] IEEE802.15.4e에서는 이를 제어하기 위한 MAC 계층으로 에너지 소모량을 줄이기 위해 RIT(Receiver Incremental Turning) 동작모드로

동작한다. RIT는 비콘 비활성 모드에서 수신노드의 duty cycle을 줄여서 저전력 통신이 가능하게 하는 방법으로 수신 노드가 wakeup mode와 sleep mode를 주기적으로 자체 반복하여 동작하는 방법이다. RIT를 이용하면 송신노드와 수신노드가 동기를 맞추어 데이터를 송수신할 수 있으며 수신 노드는 duty cycle을 과도하게 늘릴 필요가 없기 때문에 에너지 소모량을 줄일 수 있다[12].

5. 결 론

화생방 작전 수행 시 각각의 드론은 협업을 통하여 임무를 수행하여야한다. 그러기 위해서 군집비행을 하여야 임무 달성의 성공률을 높일 수 있다는 것과 동시에 군집비행 시 필요한 기술들의 취약점에 관해서도 논의하였다.

이를 통해 본 논문에서는 신속한 정보수집과 전파가 전장의 승리로 귀결되는 미래의 전장 양상에서 화생방 드론의 운용방안과 취약점 및 대응방안을 제시하여 공격자가 화생방 무기를 이용하였을 때 조기무력화가 될 수 있는 토대를 제공하였다.

참고문헌

[1] 국방일보, “육군, 5대 게임체인저에 ICT 적용 본격 연구”, 2018. 2. 06.

[2] 국방기술품질원, ‘4차 산업혁명과 연계한 미래국방기술’, 국방부, 2017. 2.

[3] 임헌영, 박병규 외 3명, “군집비행 제어기술을 기반으로 한 드론 공연의 상설 공연 콘텐츠로서의 실현성에 대한 연구”, 한국영상학회 2018. 2.

[4] eHang, EHang 1000 Drone Light Show Refreshed World Record, Retrieved from http://www.ehang.com/news/249.html, 2017, 02. 11.

[5] Lim, H. Y., Kang. Y. S., Kim, J. W. & Kim, Ch. W.. “Formation control of leader following unmanned ground vehicles using nonlinear model predictive control”, Proceedings of IEEE/ASME Advanced Intelligent Mechatronics, 945-950, 2009.

[4] 국방부, “전술네트워크 기반 무인체계[로봇, 드론] 실증연구”, 2016. 05.

[5] 인텔社 홈페이지, https://www.intel.co.kr/content/www/kr/ko/sports/olympic-games/drones.html

[6] 임덕원, “GPS 전파교란 피해사례와 감시기술 동향”, 항공우주산업기술동향, 제11권 제1호, 2013.

[7] 국립전파연구원, http://spaceweather.rra.go.kr/gnss/html/korean/sub01/sub01_01.jsp.

[8] Gupta, L., et al, “Survey of Important Issues in UAV Communication Networks”, IEEE Communications Surveys & Tutorials 18(2): 1123-1152, 2016.

[9] Curiac, D.-I, Wireless sensor network security enhancement using directional antennas: state of the art and research challenges, Sensors 16(4): 488, 2016.

[10] 류호찬, 이동환, “선택적 자원 소모를 통한 Sybil Attack 노드 그룹 탐지 방법”, 한국정보과학회 학술발표논문집, 1072-1074, 2017.

[11] 이성호 외 6명, “전력 IoT를 위한 LoRa 기반 게이트웨이 및 통신 프로토콜 최적화에 관한 연구”, 대한전기학회 CICS 정보 및 제어 학술대회, 2016. 10.

[12] 임형섭, “IEEE 802.15.4e Non-beacon 모드 RIT의 성능평가”, 고려대학교, 10p, 2016.

[13] 노시춘, “네트워크 보안 효율성 제고를 위한 보안 QoS (Quality of Service) 측정방법론 연구”, 융합보안학회지, 2011.

〔저자소개〕

김 지 원 (Jee-won Kim)
2016년 8월 연세대학교 정보보호 석사
2016년 7월 ~ 현재
육군사관학교 컴퓨터과학과 조교수
2017년 2월 ~ 현재
아주대학교 NCW학과 박사과정
email : jeewonkim@ajou.ac.kr

박 상 준 (Sang-jun Park)
2000년 2월 육군사관학교 학사
2010년 2월
한국과학기술원 정보통신공학 석사
2016년 7월 ~ 현재
육군사관학교 전자공학과 조교수
email : sigpsj13438@gmail.com

이 광 호 (Kwang-ho Lee)
2007년 2월 육군3사관학교 학사
2016년 8월 연세대학교 정보보호 석사
2017년 2월 ~ 현재
아주대학교 NCW학과 박사과정
email : loveney@naver.com

정 찬 기 (Chan-gi Jung)
1986년 공군사관학교 전자공학 학사
1994년 플로리다공대 전산공학 석사
2001년 플로리다공대 전산공학 박사
2007년 3월 ~ 현재
아주대학교 NCW학과 교수
email : ckjung@gmail.com