무인기 기반의 IoT 통신 구조의 보안 기술 동향

왕기철 김대호* 이병선** 안재영***
한국전자통신연구원 선임연구원
한국전자통신연구원 책임연구원 *
한국전자통신연구원 그룹장 **
한국전자통신연구원 본부장 ***

최근 들어 무인기 관련 기술이 급격히 발전하고 다양한 무인기들이 출시됨에 따라 다양한 IoT 장치들과 통신기술을 무인기에 탑재하고 적절한 타이밍에 의도된 위치에서 IoT 장치들을 제어함으로써 다양한 부가가치를 창출하고자 하는 시도가 늘어나고 있다. 이러한 무인기 기반의 IoT 통신은 무인기, 무선통신기술, IoT 서비스 사용자, 그리고 사용자의 요구와 무인기 서비스를 연결하는 시스템으로 구성되며, 구성요소간 통신에서 다양한 보안 위협에 노출된다. 본 고에서는 무인기 기반의 IoT 통신의 구조를 제시하여 이 구조의 잠재적인 응용들을 보여주고, 또한, 무인기 기반 IoT 통신에 대한 보안위협, 공격 유형, 그리고 공격 유형별 대응 방안을 제시하며, 마지막으로 무인기의 비행경로 이탈에 대응하기 위한 방안과 무인기가 범행에 이용될 경우에, 이를 효과적으로 추적하기 위한 방안을 살펴본다.

Ⅰ. 서론

무인기는 과거에 군에서 적진감시 및 정찰, 목표물 추적, 군용물품 배달, 필요 시 정밀 타격과 같은 용도로 이용되어 왔으나 무인기 관련 기술이 급격히 발전함에 따라 무인기를 민간영역에서 이용하고자 하는 요구도 지속적으로 증가되어 왔다. 이에 발 맞추어서 최근에 무인기는 택배, 통신 인프라 구조 확장 및 대체, 재난대처 임무, 정밀농법, 기상측정, 지도맵핑 등과 같은 다양한 임무에 활용되어 우리의 생활을 편리하게 해줄 것으로 기대되고 있다.

무인기 기술이 지속적으로 발전되면서 무인기들은 다양한 IoT(Internet of Things) 장치들을

* 본 내용은 왕기철 선임(☎ 042-860-1377, gcwang@etri.re.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP 의 공식적인 입장이 아님을 밝힙니다.
***본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음[R0126-17-1005, 고신뢰성 다종 무인이동체 통신 및 보안 SW 기술 개발]

<자료> N. H. Motlagh, M. Bagaa, T. Taleb, "UAV-Based IoT Platform: A Crowd Surveillance Use Case", IEEE Communications Magazine, vol.55, no.2, 2017. 2, pp.128-134.

[그림 1] IoT 서비스를 위한 무인기 구조

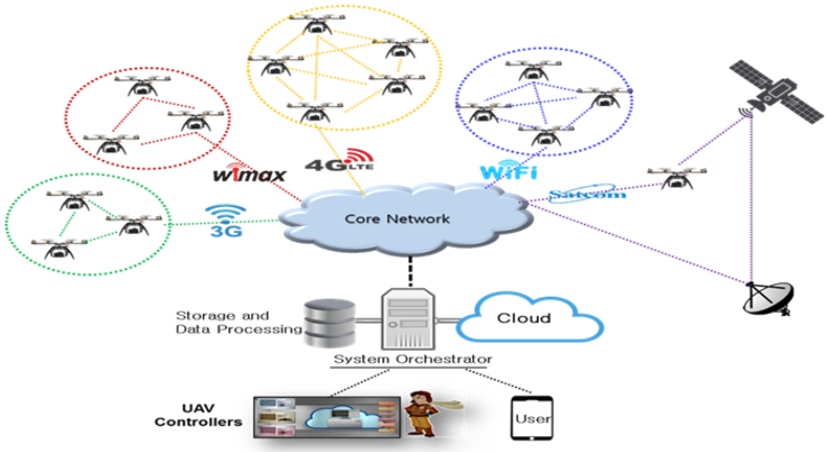
장착하고 운영할 수 있게 되었으며, 이들을 적절한 시간에 의도된 위치에서 특정한 이벤트가 있을 때 원격으로 제어함으로써 무인기들을 이용한 부가가치 서비스들을 제공할 수 있게 되었다[1]. IoT 장치들에 의해 수집된 데이터는 해당 IoT 데이터의 계산에 필요한 에너지량 및 IoT 작업의 긴급성에 따라 무인기 자체적으로 혹은 원격서버로 보내져 처리될 수 있다. 또한, 다양한 통신 네트워크로의 접근이 가능하게 함으로써 언제 어디서나 IoT 장치들로부터 수집된 데이터를 전송하고, 때로 기반구조를 이용한 통신이 불가할 때는 무인기들 간의 애드 혹 네트워크(Flying Ad hoc NETwork: FANET)을 형성하여 지속적인 연결성을 보장할 수 있다[2]. [그림 1]은 다양한 IoT 장치들과 통신장치들이 결합되어 있는 IoT 서비스를 위한 무인기 구조를 보여준다.

본 고는 먼저 Ⅱ 장에서 무인기 기반의 IoT 통신 구조를 살펴보고, 이 통신 구조의 응용사례를 분야별로 분류한 뒤에 대표적인 응용들을 설명한다. Ⅲ 장에서는 무인기 기반의 IoT 통신 구조에 대한 잠재적인 보안위협을 식별하고 이에 따른 공격 유형 및 공격 성공시의 결과를 보여준다. 또한, 이러한 무인기 기반 IoT 통신 공격들에 대한 대응 방안들을 공격 유형별로 제시한다. Ⅳ 장에서는 이전 장에서는 다루지 않았지만 무인기 기반 IoT 통신의 보안성을 향상시키기 위해 필요한 기술 요소를 제시한다.

Ⅱ. 무인기 기반의 IoT 통신 구조 및 응용

1. 무인기 기반의 IoT 통신 구조

일반적으로 무인기 기반의 IoT 통신 구조는 무인기들과 무선통신기술, 시스템 조정자(System Orchestrator: SO), 사용자로 구성된다[3]. 먼저, 무인기는 [그림 1]과 같은 다양한 IoT 장치들을 보유하고 요구에 따라 그 IoT 장치들을 이용하여 정보를 수집하고 이를 무선통신기술을 통해 전송한다. 다음으로, 무선통신기술은 무인기와 지상통제소 간의 통신, 무인기와 무인기 간의 통신, 그리고 무인기와 SO 와의 통신을 수행하기 위해 필요하다. 즉, 무인기들은 그 이동성이 어떤 통신 노드보다도 높기에 향상된 통신범위 제공, 안정적인 연결 보장, 충분한 처리율과 같은 신뢰성 요소들이 중요하다. 따라서, 기본적으로는 4G LTE 나 5G 와 같은 고속의 무선통신기술을 이용해야 하고, 이들에 대한 보완기술로써 WiMax 나 WiFi 가 이용될 수 있다. 또한, 무인기들이 BLoS(Beyond Line of Sight)에 위치하여 직접적인 통신이 불가할 때를 대비하여 위성 통신(Satellite Communication)을 이용해야 될 때도 있다. SO 는 무인기들과 그들의 IoT 장치들의 운영을 조정하여 사용자들의 IoT 서비스 요구들이 신속하게 처리되도록 한다. 또한, SO 는 무인기들이 상호 간에 충돌 없이 안전하게 운행하도록 운행경로를 설정한다. 사용자는 무인기를 이용하여 활용 가능한 서비스들 중에서 원하는 서비스를 SO 에게 요구하고, 해당 서비스에 대한 응답을 SO 를 통해 제공 받는다. [그림 2]는 무인기 기반의 IoT 통신 구조를 보여준다.



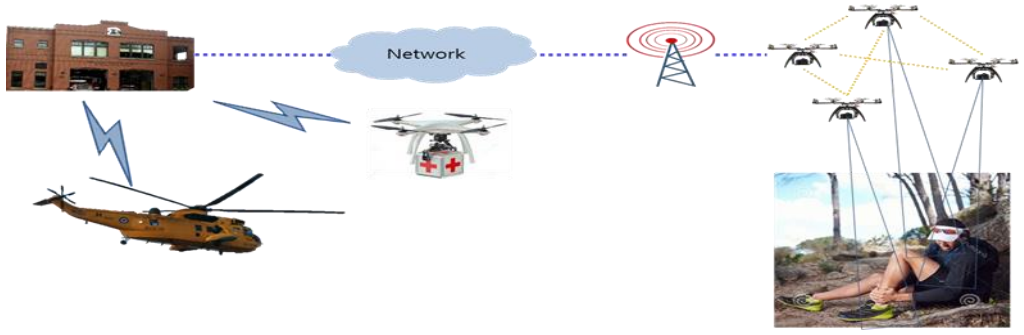
<자료> N. H. Motlagh, T. Taleb, O. Arouk, "Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives", IEEE Internet of Things Journal, vol.3, no.6, 2016. 12, pp.899-922.

[그림 2] 무인기 기반의 IoT 통신 구조

2. 무인기 기반의 IoT 통신 구조의 응용

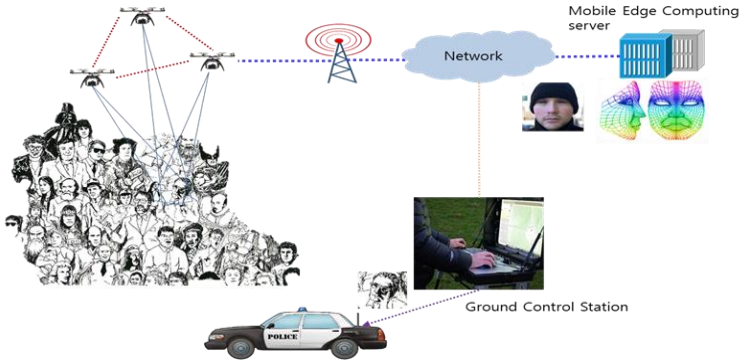
무인기 기반의 IoT 통신 구조는 다양한 분야에서 이용될 수 있다. 먼저, 지능형 수송체계(Intelligent Transportation Systems: ITS)에서 무인기는 높은 고도의 운용환경을 통해 전방의 교통사고를 미리 인지할 수 있으며, 이를 신속히 노변장치 및 교통관리체계 서버로 전송할 수 있다[4]. 이러한 선제적 알림 서비스는 기존의 V2V 통신과 더불어 사고예방 효과를 높이고 현장의 위치 및 상황을 정확하게 전달하여 신속한 구급 활동이 이루어지도록 할 수 있다. 또한, 무인기는 도로상에서 긴급하게 진행되고 있는 공사 등을 높은 고도에서 신속히 인지하여 교통관리체계 서버에 전송할 수 있다. 교통관리체계 서버는 무인기들로부터 수집되는 정보를 종합적으로 판단하여 후방 차량들이 공사상황을 정확히 인지하도록 하고 우회할 수 있도록 도울 수 있다[4].

또 다른 무인기 기반의 IoT 통신의 응용은 재난구조이다. 먼저, 지진이나 해일과 같은 자연재해가 발생하였을 때 해변에 위치한 원자력 발전소는 큰 위험에 처하게 된다. 이때 무인기들을 이용하면 원자력발전소의 주변상황들을 높은 고도에서 점검할 수 있으며 신속한 후속조치가 가능하게 된다. 즉, 방사능 누출 수준에 따라 방제작업을 신속히 시작하고 주변 주민들의 신속한 대피를 유도하며 대피소로 필요한 물품을 배달할 수 있다[3]. 만일, 급격한 기상악화로 인해 산악 실종자 및 부상자가 발생한 경우에도 무인기는 그 위력을 발휘할 수 있다. 즉, 실종자의 주변에 무인기를 띄워서 실종자를 수색하고, 부상을 입었을 경우에는 부상자의 이미지를 촬영해서 구조센터에 전송할 수 있다. 이러한 이미지들을 바탕으로 구조센터는 구조헬기나 구조대를 신속히 파견할 수 있으며, 때로는 구호약품을 먼저 무인기를 통해 전송함으로써 인명피해를 최소화 할 수 있다[5]. [그림 3]은 무인기 기반의 산악 재난 구조를 보여준다. 사실 무인기가



<자료> ETRI 자체 작성

[그림 3] 무인기 기반의 산악 재난 구조

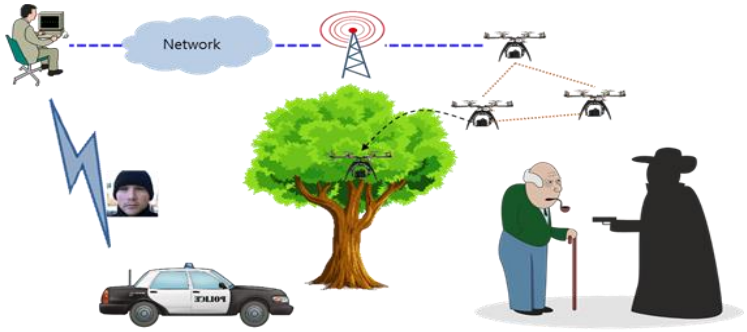


<자료> N. H. Motlagh, M. Bagaa, T. Taleb, "UAV-Based IoT Platform: A Crowd Surveillance Use Case", IEEE Communications Magazine, vol.55, no.2, 2017. 2, pp.128-134.

[그림 4] 무인기 기반의 테러 감시

초기에 사용되기 시작한 것은 주로 목표가 되는 영역이나 표적을 감시하고 그 상태를 점검하기 위한 목적이었다. 그래서 무인기 기반의 IoT 통신도 그 주요한 응용 중 하나가 감시이다. 특히, 최근 전세계 곳곳에서 테러가 자주 발생하는 것을 고려해 볼 때, 군중이 운집하는 곳에서 테러 활동을 감시하여 선제적으로 테러리스트를 색출하고 그 위험성을 제거하는 것은 매우 중요한 일이다. 무인기를 이용하면 높은 고도에서 위험인물의 영상을 촬영하여 치안센터 등으로 전송하고, 치안센터에서는 수집된 영상의 얼굴인식을 통해 테러리스트를 감지한다. 이를 통해 신속한 테러리스트 색출 및 검거를 수행함은 물론 군중이 운집한 곳에서 경찰인력 배치의 부담을 크게 줄일 수 있다[1]. [그림 4]는 위에서 설명한 무인기 기반의 테러 감시를 보여 준다.

최근 들어 우리 사회가 급격한 핵가족 시대로 접어들고 있으며, 이로 인해 가족과 떨어져서 혼자 사는 독거인들이 증가하고 있어 사회적 약자를 상대로 한 묻지마 범죄도 증가하고 있는



<자료> ETRI 자체 작성

[그림 5] 무인기 기반의 범죄 예방

추세이다. 특히, 사회적 약자가 CCTV 의 사각지대에서 흉악범을 만났을 경우에, 이들의 공격에 무방비로 노출되고 늦게 발견되어 생명을 잃는 경우도 자주 발생하게 된다. 무인기를 이용하면 이러한 CCTV 사각지대에서 현장을 선회하며 비행함으로써 범죄를 예방하고, 범행이 발생하는 경우에는 범행 발생을 신속히 치안센터에 알려 경찰의 출동을 유도함은 물론 범행현장 촬영을 통해 사후 범인검거에 도움을 줄 수 있다. [그림 5]는 무인기 기반의 범죄 예방 시나리오를 보여 준다.

[표 1]은 위에서 설명한 무인기 기반의 IoT 통신의 응용들과 기타 다른 응용들을 목적에 따라 구분하고 각각의 응용 시나리오를 설명한다.

[표 1] 무인기 기반의 IoT 통신의 응용들

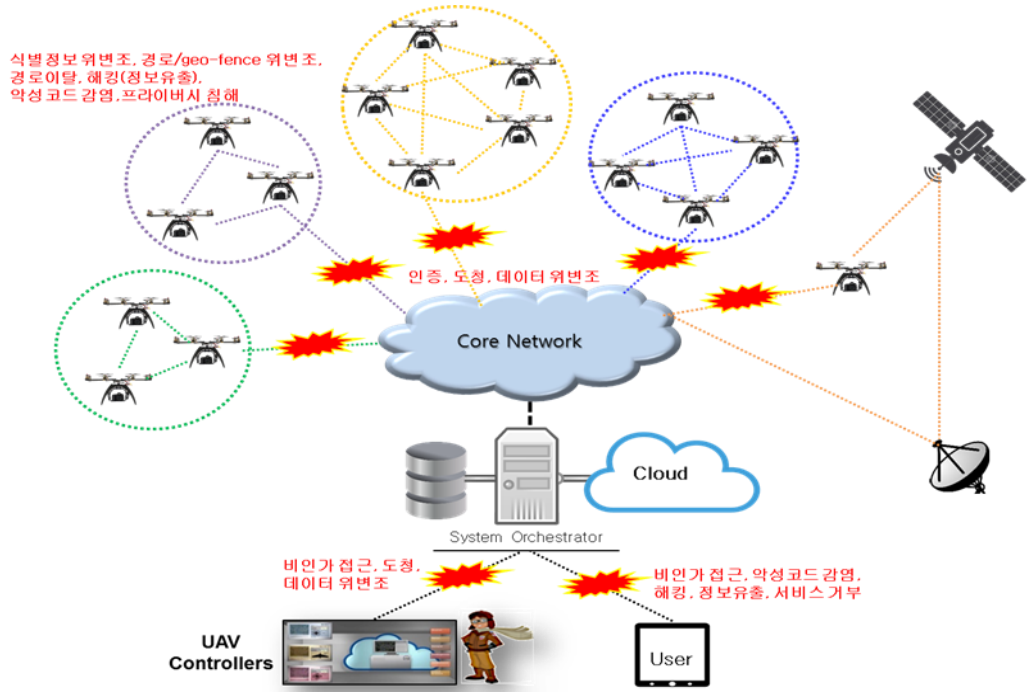
구분		시나리오
지능형 수송체계	교통사고 보고	무인기가 높은 위치에서 교통사고를 미리 인지하고 상황전파를 통해 사고 예방
	교통안전 노변장치	무인기가 도로 공사, 긴급상황 등을 미리 인지하여 알리고 후방 차량의 선제적 조치 추동
	교통안전 경찰	도로 상의 불법운행차량 정보를 미리 획득하여 경찰의 선제적 안전확보 활동 지원
재난구조	재난 발생시 신속대피 지원	지진이나 해일 발생 시 원자력 발전소의 상황을 감시하여 신속한 대피 및 물품 지원
	해양오염사고 대응 지원	해양에서 약품이나 기름 유출 사고 발생 시 상황을 정확히 전달하여 신속한 조치 및 대응 지원
	산악 재난 구조	산악 실종자의 상태와 건강상황 등을 판단하여 신속한 수송 및 약품 지원 수행
감시	재난 감시	기반구조, 산불, 화학약품, 기름 유출 등을 무인기를 통해 선제적 감시 및 조치
	테러 감시	무인기를 통해 테러 위험 인물 및 테러 위험의 선제적 식별 및 조치
치안 및 복지	범죄 예방	CCTV 사각지역에서의 범죄 현장 촬영 및 알리미 역할 수행
	사회적 약자 도우미	사회적 약자들의 신변에 비상사태 발생 시 신속한 알림 및 조치

<자료> ETRI 자체 작성

Ⅲ . 무인기 기반의 IoT 통신의 보안 위협 및 대응 방안

1. 무인기 기반의 IoT 통신의 보안 위협

무인기 기반의 IoT 통신구조에서 보안 위협은 무인기 자체에 대한 보안 위협, 무인기의 통신에 대한 보안 위협, 시스템과 조종사 간 인터페이스 보안 위협, 시스템과 사용자간 인터페이



<자료> ETRI 자체 작성

[그림 6] 무인기 기반의 IoT 통신의 보안 위협

스 보안 위협으로 구분된다. [그림 6]은 이러한 무인기 기반의 IoT 통신의 보안 위협을 보여준다.

먼저, 무인기 자체에 대한 보안 위협은 무인기 내에 저장되어 있는 고유식별정보, 경로 정보, 영상 정보, 기타 SW 등이 유출되거나 위조 및 변조되어 문제 혹은 이상 행위를 일으키는 것을 말한다. 무인기의 고유식별정보가 위/변조되면 무인기의 악의적인 행위를 추적하기 어려워지게 된다. 만일 공격자가 무인기의 경로정보를 위/변조할 수 있게 되면 공격자는 다음과 같은 이점을 취한다. 공격자는 경로정보 위/변조를 통해 특정경로를 배타적으로 독점할 수 있게 된다. 공격자는 보호구역에 무단으로 침입하여 촬영하는 등의 정보노출 활동을 할 수 있다. 또한, 공격자는 범죄를 저지른 후에 자신의 경로정보 변조를 통해 범죄사실을 은폐할 수 있다. 마지막으로 공격자는 무인기가 소프트웨어 등을 업데이트할 때 악성코드를 삽입하여 무인기가 제어되지 않거나 이상행위를 하도록 할 수 있다.

무인기 통신에 대한 보안 위협은 무인기-조종사 간의 통신, 무인기-SO 간 통신, 무인기 간의 통신에서 통신 당사자의 신뢰성이나 교환되는 데이터의 기밀성 및 무결성이 훼손되기 쉽다는 것이다. 무인기-조종사 간의 통신 보안이 훼손되면, 무인기와 조종사 간에 전달되는 데이터

가 노출되고 위/변조될 뿐만 아니라 타인에게 무인기의 제어권을 잃을 수도 있게 된다. 무인기와 SO 간의 통신 보안이 훼손되면, 잘못된 정보로 인해 무인기간 충돌이 발생하고, 신뢰할 수 없는 정보의 홍수로 인한 무인기 운행 방해 및 시스템 운영 혼란이 초래된다. 또한, 무인기간 통신 보안이 훼손되면, 무인기간 전달 데이터의 노출 및 위/변조는 물론 신뢰할 수 없는 정보의 범람으로 인해 무인기 운행 방해 및 충돌이 발생할 수 있다.

시스템과 조종사 간의 인터페이스 보안 위협은 조종사가 시스템에 인가되지 않은 접근을 시도하여 데이터를 도청하고 심지어는 무단으로 위조 혹은 변조하는 위협을 의미한다. 임의의 조종사가 시스템에 인가되지 않은 접근을 성공하게 되면 조종사는 해킹을 통해 시스템의 무결성을 손상시킬 수 있다. 또한, 시스템과 타 조종사 간에 전달되는 데이터를 도청하여 기밀성을 손상시키고, 시스템 내에 저장된 정보를 위/변조하여 그 무결성을 훼손할 수 있다.

마지막으로, 시스템과 사용자간 인터페이스 보안 위협은 사용자가 시스템에 접속하여 시도

[표 2] 무인기 기반 IoT 통신의 보안 위협별 공격 유형 및 결과

보안 위협	공격 유형	결과
무인기에 대한 보안 위협	무인기 고유식별정보 위조/변조	악의적 행위자 추적 불가
	무인기내 경로정보 위조/변조	보호지역 무단 침입 및 노출, 범죄수사 혼선, 경로독점
	무인기내 경로정보 및 영상정보 유출	개인의 프라이버시 노출
	무인기의 악성코드 감염	무인기의 제어 불가 및 이상 행위
무인기 통신에 대한 보안 위협	무인기-조종사간 통신 보안 훼손	무인기-조종사간 전달 데이터 노출 및 위조/변조, 무인기 제어권 유실
	무인기-SO 간 통신 보안 훼손	시스템 운영에 혼란 초래, 무인기 운영 방해, 무인기 충돌
	무인기간 통신 보안 훼손	무인기간 전달 데이터 노출 및 위조/변조, 무인기 운영 방해, 무인기 충돌
시스템-조종사 인터페이스 보안 위협	조종사의 시스템 비인가 접근	조종사의 시스템 무결성 손상
	조종사의 시스템 데이터 도청	조종사가 시스템과 타 조종사간 전달 데이터의 기밀성 손상
	조종사의 시스템 데이터 위조/변조	조종사가 시스템 내 데이터 무결성 손상
시스템-사용자 인터페이스 보안 위협	사용자의 시스템 비인가 접근	사용자의 시스템 무결성 손상
	시스템의 악성코드 감염	시스템이 악성코드에 감염되어 동작불가 혹은 오동작
	시스템 정보 유출	시스템 내 주요 정보가 외부에 노출
	시스템의 서비스 거부	시스템의 운용가능성이 훼손

<자료> ETRI 자체 작성

하는 모든 악의적인 행위들을[1] 의미한다. 임의의 사용자가 시스템에 인가되지 않은 접근을 성공하게 되면 사용자는 해킹을 통해 시스템의 무결성을 손상시킬 수 있다. 만일 사용자가 시스템에 악성코드를 이식하는 경우에, 시스템의 오동작 유발이나 동작 불가 현상을 유발할 수도 있다. 또한, 시스템 내에 존재하는 주요 정보들을 유출하거나 과부하를 유발하여 서비스 거부가 되도록 할 수도 있다. [표 2]는 무인기 기반 IoT 통신의 보안 위협별 공격 유형과 그 결과를 요약해서 보여 준다.

2. 무인기 기반의 IoT 통신 공격 대응 방안

본 절에서는 앞 절에서 살펴본 무인기 기반의 IoT 통신에 가해지는 공격들을 방어할 대응 방안들을 제시한다. 먼저, 무인기의 고유식별정보에 대한 위조 및 변조 방지는 통신하는 노드 간에 동일한 인증기관이 서명한 고유식별정보의 인증서를 이용하여 통신하고, 상대방은 해당 인증서를 인증기관의 공개키로 검증함으로써 구현할 수 있다. 인증정보를 미리 생성하여 저장하지 않고 즉각적인 고유식별정보를 생성하고 검증하는 PUF(Physically Unclonable Function)[6] 기술을 물리적 복제 방지를 위해 이용할 수도 있다. 만일 SO가 CA(Certification Authority)로 동작한다고 가정하면, SO는 비행경로를 계산하여 자신의 비밀키로 서명한 뒤에 조종사에게 반환함으로써 위조 및 변조로부터 안전한 비행경로가 확보된다. 만일 무인기가 임의의 공격자에게 탈취되면 조종사 및 촬영의 대상에 대한 프라이버시가 노출된다. 이를 막기 위해서는 위치에 따른 카메라 작동이 필요하고, 저장된 정보들은 모두 암호화해서 노출되더라도 쉽게 유출되는 것을 막아야 한다. 또한, 무인기의 SW 를 업그레이드할 때 악성코드가 같이 유입되는 것을 막기 위해서는 체크썸 검사, 화이트 리스트에 있는 SW 만 다운로드, 휴리스틱 기반의 악성코드 탐지 등을 수행한다.

무인기 통신에 대한 보안 위협은 통신 당사자 간의 상호인증 수행, 상호인증 후에 대칭키 수립, 대칭키를 이용한 암/복호화 통신을 통해 해결한다. 무인기와 조종사 간의 통신 보안을 위해서는 IPSec[7]이나 TLS(Transport Layer Security)[8]와 같은 인증서를 이용한 상호인증을 수행하고, 이후에 상호간에 보안능력을 협상하여 대칭키 기반의 암/복호화 통신을 수행한다. 무인기와 SO 간의 통신 보안을 위해서는 IPSec 이나 TLS 와 같은 표준 프로토콜을 사용하여 상호인증

1) 인가되지 않은 시스템 접근, 시스템에 악성코드 유포, 불법 정보유출, 서비스 거부 상태 유발

을 수행한다. 상호 인증이 끝나면 상호 간에 보안 능력을 협상하여 대칭키 기반의 암/복호화 통신을 수행한다. 무인기 간의 통신 보안을 위해서는 인증서 혹은 선분배키(Pre-Shared Key: PSK)를 이용하여 상호인증을 먼저 수행하고 선분배키를 이용하여 대칭키를 설정한다. 이후에 대칭키를 이용하여 암/복호화 통신을 수행한다.

시스템과 조종사 간의 인터페이스에 대한 보안 위협은 시스템과 조종사 간의 상호인증 후에 양자간 대칭키 수립, 대칭키를 이용한 통신 암/복호화를 통해 해소될 수 있다. 먼저, 조종사가 시스템에 인가되지 않은 접근을 하지 못하게 하기 위해서 IPSec 이나 TLS 를 통해 조종사와 시스템 간에 상호인증을 수행할 수 있다. IPSec 이나 TLS 를 사용하기 곤란한 경우에는 PSK 를 이용하여 상호인증을 수행할 수 있으나, 조종사의 수가 증가하는 경우에 확장성이 떨어지고 복잡도가 증가하는 문제점이 있다. IPSec 이나 TLS 에서 통신 당사자 간에 상호인증이 완료되면 대칭키를 수립할 수 있으며, 이를 이용하여 통신 당사자간 암/복호화 통신을 수행함으로써 데이터 도청이나 위조 및 변조를 예방할 수 있다.

시스템과 사용자 간의 인터페이스에 대한 보안 위협은 시스템과 사용자 간의 상호인증 후에 양자간 대칭키 수립 및 암/복호화 활용을 통해 정보 유출 및 비인가 접근을 예방할 수 있다. 반면에, 시스템의 앞단에 특정 보안기능을 수행하는 정보보호시스템들을 배치하여 악성코드 감염이나 서비스 거부와 같은 보안 위협에 대비할 수 있다. 먼저, 사용자가 시스템에 인가되지 않은 접근을 시도하는 것을 막기 위해서 사용자와 시스템 간에 인증서를 이용한 상호인증(IPSec, TLS) 혹은 PSK 를 이용한 상호인증을 수행할 수 있다. 상호인증을 수행한 후에는 사용자와 시스템 간에 대칭키를 수립하고 이를 이용한 암/복호화 통신을 수행함으로써 시스템의 정보유출을 방지할 수 있다. 일반적으로 사용자는 인터넷과 같은 공용 네트워크를 통해 시스템과 연결되므로 시스템과 연결되는 인터넷은 외부로부터 도래하는 공격의 근원이 된다. 이러한 위협을 해소하기 위해서는 침입차단시스템, 침입방지시스템, 통합보안관리시스템, DDoS 대응장비와 같은 정보보호시스템들을 시스템의 경계부분에 배치한다. 그래서 정상적인 사용자로 가장하여 인터넷으로부터 오는 악성코드 감염이나 서비스 거부 공격 등을 식별하고 이를 조기에 차단한다. [표 3]은 위에서 살펴본 무인기 기반 IoT 통신에 대한 공격 유형별 대응 방안을 요약해서 보여준다.

[표 3] 무인기 기반 IoT 통신에 대한 공격 유형별 대응 방안

보안 위협	공격 유형	대응 방안
무인기에 대한 보안 위협	무인기 고유식별정보 위조/변조	인증서 서명/검증 기반의 고유식별정보 위/변조 방지, 하드웨어 기반의 물리적 복제 방지 기능 (Physically Unclonable Function) 구현
	무인기내 경로정보 위조/변조	인증서 기반의 경로 서명/검증 기술을 통한 위/변조 방지
	무인기내 경로정보 및 영상정보 유출	위치기반의 카메라 작동 제어, 경로정보 및 영상정보의 암호화 저장
	무인기의 악성코드 감염	인가된 SW 의 체크썸 검사를 통해 무결성 검증, whitelist/blacklist 기반의 SW 관리, 휴리스틱 기반의 악성코드 탐지
무인기 통신에 대한 보안 위협	무인기-조종사간 통신 보안 훼손	인증서를 이용한 상호인증 수행(IPSec, TLS), 대칭키 암/복호화 수행
	무인기-SO 간 통신 보안 훼손	인증서를 이용한 상호인증 수행(IPSec, TLS), 대칭키 암/복호화 수행
	무인기간 통신 보안 훼손	인증서 혹은 PSK(Pre-Shared Key)를 이용한 상호인증 수행, 대칭키 암/복호화 수행
시스템-조종사 인터페이스 보안 위협	조종사의 시스템 비인가 접근	인증서(IPSec, TLS) 혹은 PSK(Pre-Shared Key)를 이용한 상호인증 수행
	조종사의 시스템 데이터 도청	대칭키 암/복호화 수행, 비대칭키 암/복호화 수행
	조종사의 시스템 데이터 위조/변조	대칭키 기반 무결성 검증, 비대칭키 기반 무결성 검증
시스템-사용자 인터페이스 보안 위협	사용자의 시스템 비인가 접근	인증서(IPSec, TLS) 혹은 PSK(Pre-Shared Key)를 이용한 상호인증 수행
	시스템의 악성코드 감염	침입차단시스템, 침입방지시스템, 통합보안관리, DDoS 대응장비 등의 정보보호제품 적용
	시스템 정보 유출	대칭키 암/복호화 수행, 비대칭키 암/복호화 수행
	시스템의 서비스 거부	침입차단시스템, 침입방지시스템, 통합보안관리, DDoS 대응장비 등의 정보보호제품 적용

<자료> ETRI 자체 작성

Ⅳ. 결론

본 고에서는 최근 대중의 큰 관심을 받고 있는 무인기 기반의 IoT 서비스를 위한 무인기 구조를 제시하고, 이에 대응하는 무인기 기반 IoT 통신 구조와 향후에 실현 가능성이 높은 응용사례들을 제시하였다. 또한, 무인기 기반의 IoT 통신 구조가 가지는 보안 취약성과 공격유형 및 이에 따르는 결과를 정리하였다. 이후에 본 고는 해당 보안 취약성 및 공격유형에 대비하기 위한 가용기술들을 공격유형별로 제시하였다.

본 고에서는 무인기 기반의 IoT 통신상의 많은 보안 위협을 다루었지만, 다루어지지 않은

몇 가지 이슈들이 있다. 먼저, 일부 악의적인 조종사들에 의해 무인기가 자신의 비행경로를 이탈해서 비행금지구역으로 진입하거나 충돌을 일으키거나 무단으로 사진을 촬영하거나 행인들을 위협하는 등의 문제를 일으키는 경우에 이에 대한 대응방안이 마련되어야 한다. 즉, 경로를 이탈한 무인기들에 대한 경고 알람이 적기에 방송되어야 하고, 이들의 위치가 정확하게 정상적인 무인기들에게 알려져서 그들이 충돌회피 절차를 진행하도록 유도해야 한다. 또한, 경로이탈 무인기들에 대한 강제착륙 방법이나 절차가 정해져야 한다. 또 다른 이슈는 악의적인 조종사에 의해 제어되는 무인기가 범죄에 활용되는 경우에 이러한 무인기의 행위를 기록하여 나중에 조종사를 추적하기 위한 대응방안이 마련되어야 한다. DJI 에서는 여기에 대한 해결책으로 차량안전통신에서 이용되었던 ELP(Electronic License Plate) 방송의 개념을 무인기에 도입하는 것을 제안하였다[9]. 즉, 무인기가 비행하면서 자신의 고유식별정보를 주기적으로 방송하고 수신자들은 이를 기록함으로써, 필요 시에는 범행에 이용된 무인기의 경로추적은 물론 조종사를 식별하는 것이다. 그러나 이 방법은 프라이버시 침해라는 관련 업계종사자와 조종사, 그리고 대중의 큰 반발을 일으켰고, 이에 따라 기술적용에 앞서 이러한 반발감을 낮추는 조치가 먼저 선행되어야 한다.

[참고문헌]

[1] N. H. Motlagh, M, Bagaa, and T. Taleb, "UAV-Based IoT Platform: A Crowd Surveillance Use Case," IEEE Communications Magazine, Vol.55, No.2, Feb. 2017, pp.128-134.

[2] L. Gupta, R. Jain, and G. Vaszcun, "Survey of Important Issues in UAV Communication Networks," IEEE Communications Surveys and Tutorials, Vol.8, Issue 2, Apr.-Jun. 2016, pp.1123-1152.

[3] N. H. Motlagh, T. Taleb, and O. Arouk, "Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives," IEEE Internet of Things Journal, Vol.3, No.6, Dec. 2016, pp.899-922.

[4] H. Menouar, I. Güvenc, K. Akkaya, A. S. Uluagac, A. Kadri, and A. Tuncer, "UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges," IEEE Communications Magazine, Vol.55, No.3, Mar. 2017, pp.22-28.

[5] T. Andre et al., "Application-Driven Design of Aerial Communication Networks," IEEE Communication Magazine, Vol.52, Issue 5, May 2014, pp.129-137.

[6] S. Guilley, S. Hamaguchi, and Y. Kang, ISO/IEC 20897 WD, "Security requirements, test and evaluation methods for physically unclonable functions for generating nonstored security parameters," 2017.

[7] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," IETF RFC 4301, Dec. 2005.

[8] T. Dierks, "The Transport Layer Security(TLS) Protocol Version 1.2," IETF RFC 5246, Aug. 2008.

[9] DJI, "A Call for a Balanced Identification Approach," A DJI Technology Whitepaper, Mar. 2017.