|  |
| --- |
| **PX4-Autopilot 으로 보는 UAV Security**  **요 약**  최근 드론 기술이 발전함에 따라 여러 분야에 드론의 사용이 시도되고 있다. 정보의 중요성이 강조되는 분야에 있어 드론의 보안은 중요한 문제로 자리잡는다. 하지만 드론의 무선 주파수 대역은 기존의 무선 통신의 취약점을 가지고 있으며, 일반적인 드론의 경우 보안을 고려하지 않은채 설계된다. 이에 UAV에 대한 두 방면의 보안 문제가 대두된다. 드론 자체의 하드웨어적 보안과 드론 외부의 네트워크적 보안이다. 본 문서는 PX4-Autopilot 네트워크 통신 과정에서 발생하는 외부적 보안 문제에 대한 분석과 해결방안을 다룬다. |

**1. 서론**

**1.1. 연구배경**

최근 Amazon , Samsung 과 같은 기업들은 드론을 활용하여 다양한 산업에 활용하고 있다. 기업뿐만 아니라 최근에는 민간에서 까지 드론을 사용하고 있는 추세이다. 현재 민간용 드론에 사용하는 대부분의 Drone은 Ground Control System (이하: GCS) 와 통신을 위해 mavlink protocol 을 사용하고 있다.

드론에서는 복잡한 연산을 수행 할 수 있는 compute 능력이 부족하기 때문에 mavlink protocol은 복잡한 암호화 알고리즘을 사용하지 않고 있다. 즉, mavlink protocol 은 경령화된 통신에 초점을 둔 프로토콜이기 때문에 보안적으로 결점이 있는게 현 상태이다. 또한 드론은 무선 환경에서 통신을 하기 때문에 외부에 전파들이 노출되는 상황이기 때문에 쉽게 외부적인 위협에 맞닿게 된다. 실제 드론 2013년 이라크 작전에 사용됐던 미국의 드론들은 이라크 무장단체에 의해 해킹당하는 사례가 있었으며, 보안 컨퍼런스인 2016 PacSec 에서는 Icarus 라는 해킹 시스템이 등장하여 드론 보안에 대한 중요성이 강조되었다. 이에 따라 오픈소스인 PX4 를 통해서 UAV 의 작동방식 및 통신을 살펴보고 보안의 취약점을 파악하고 이를 보완하고자 하였다.

**1.2. 연구목표**

해당 연구에서는 첫번째로, 오픈소스인 PX4 와 QGoundControl 를 사용하여 드론의 비행을 직접 시연해보고자 한다. 이를 통해 현재 UAV의 작동 방식, UAV 와 GCS 의 통신방법에 대해 연구 할 것이다.

두번째로, 직접 시뮬레이션 상에서 외부접근을 구현하여 UAV가 해킹에 취약하다는 사실을 입증하고자 한다. 이 때 해킹 공격 이후의 기존 통신의 상태에 따라 두가지 상황을 구현하여 각각의 상황을 표현하고자 한다.

세번째로, 만약 실제 UAV가 외부의 공격에 의해 다양한 문제점이 발생하게 된다면, 이에 대한 대응책 및 개선점을 만들어 취약점을 보완하고자 한다.

**2. 관련연구**

**2.1. Signal interrupt**

**2.1.1. Spoofing**

드론의 이동은 위성의 GPS 받아 진행된다. 위성의 GPS신호는 저출력이며 보안이 약하다는 특징을 갖고 있다. 위성 신호에 비해 더 강한 신호를 드론에게 송출하면 드론에게 조작된 GPS 신호를 전달할 수 있다. 조작된 신호를 전달 받은 드론은 사용자가 원하는 경로를 이탈 시키거나, 조작자가 원하는 장소에 위치시킬 수 있다.

**2.1.2. Jammer**

드론은 무선 주파수를 통해 통신하여 사용자로 부터 목적지에 대한 정보를 전달 받게된다. 이 때 전파를 교란하는 신호를 드론에게 송출하면 드론-사용자, 드론-위성신호 간의 정보 교환이 원활하게 이루어지지 못한다. 정보의 소실로 드론의 추락, 강제 착륙, 강제 귀환을 유도한다.

**2.2. PX4**

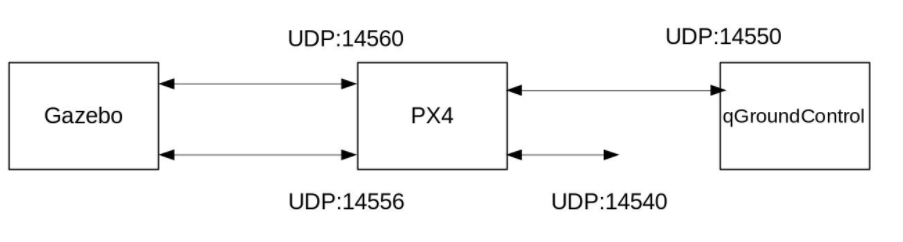
PX4는 쿼드콥터같은 무인항공기의 원격조정 및 자율주행을 위해 설계된 NuttX 운영체제 기반의 소프트웨어로 이루어진 플라이트 컨트롤 보드에서 작동하는 완전한 플랫폼이다.

**2.2-1 QGroundController**

PX4 프로젝트에서 제공하는 오픈소스로 GCS 의 역할을 담당한다. PX4 및 Ardupiot 혹은 MAVLink 를 사용하는 기타 조종 장치들에대해 비행을 지원하며 자율 비행을 위한 임무 계획 기능을 지니고 있다.

**2.2-2 SITL (Software In The Loop)**

순수 소프트웨어 기반의 시뮬레이션으로서 하드웨어 없이 원하는 환경을 실험 할 수 있는 시스템이다 . PX4는 jMAVsim 과 Gazebo 라는 시뮬레이션을 사용하며 해당 연구에서는 jMAVsim 을 사용한다.



**[그림 1] PX4 프로젝트의 구성도**

**2.2-3 Publish-Subscribe Model**

PX4 의 module들은 Publish-Subscribe Model 을 사용함으로써 컴포넌트화 되어 있다는 특징을 가지고 있다. publish 와 subscribe는 PX4의 미들웨어인 uORB 가 관장하고 있다.

**2.3 MAVLink**

MAVLink는 매우 가벼운 드론용 메시지 프로토콜이다. 이 중 MAVLink 2는 14바이트의 크기를 가진다. MAVLink는 추가 프레이밍이 필요가 없기 때문에 통신 대역폭을 상당히 제한하는 여건에서 사용한다.



**[그림 2] MAVLink V2 의 Frame 구조**

**2.4. 기존 연구의 문제점 및 해결 방안**

**2.4.1. 연구의 문제점**

- 드론과 사용자, 드론과 위성 신호간의 통신 과정에서의 문제가 발생한다.

- 위성 신호의 저출력이나 보안적 취약성은 개인이 해결할 수 없는 문제이다.

- 드론이 탈취 당한 경우 일부 정보 유출은 불가피하다.

- 위 세가지 기술적 문제를 유지한채 드론의 보안 성능을 향상 시키기 위한 방안을 제시해야 한다.

**2.4.2. 해결 방안**

**2.4.2.1. 드론 내부에 위성 신호 저장**

드론 내부에 탑재된 GPS 신호를 주기적으로 받아 드론의 이동 경로를 파악한다. 미션에 대한 예상 이동 경로에서 이탈 할 경우 또는 지체 될 경우 사용자에게 경고 신호를 전달 한다. 초기 명령자에게 이후 미션 수행에 대한 인가를 요청한다. 사용자 설정에 따라 인가 대기 시간 동안 드론의 복귀 또는 고정 비행 상태를 유지한다. 비인가의 경우 드론의 강제 복귀 및 기존의 명령 강제 수행을 진행한다. 인가의 경우 드론의 최종 목적지에 대한 정보를 수정한다. Jamming 방지된다.

**2.4.2.2. AI 를 사용한 IDS 구축**

이상탐지 방식으로 IDS 를 구축하여 실시간으로 사용자의 행위에 대한 검증을 할 수 있는 시스템을 만든다. 오용탐지가 아닌 이상탐지를 이용하는 이유는 알려지지 않은 공격에 대한 대비 또한 가능하기 때문이다. 중점으로 다루어야 할 부분은 공격이 아닌 패턴을 공격으로 패턴하는 False Positive 문제이다. 이 문제를 해결하기위해 AI를 통해 공격패턴과 정상패턴을 학습시켜 오탐률을 낮추려고 한다.

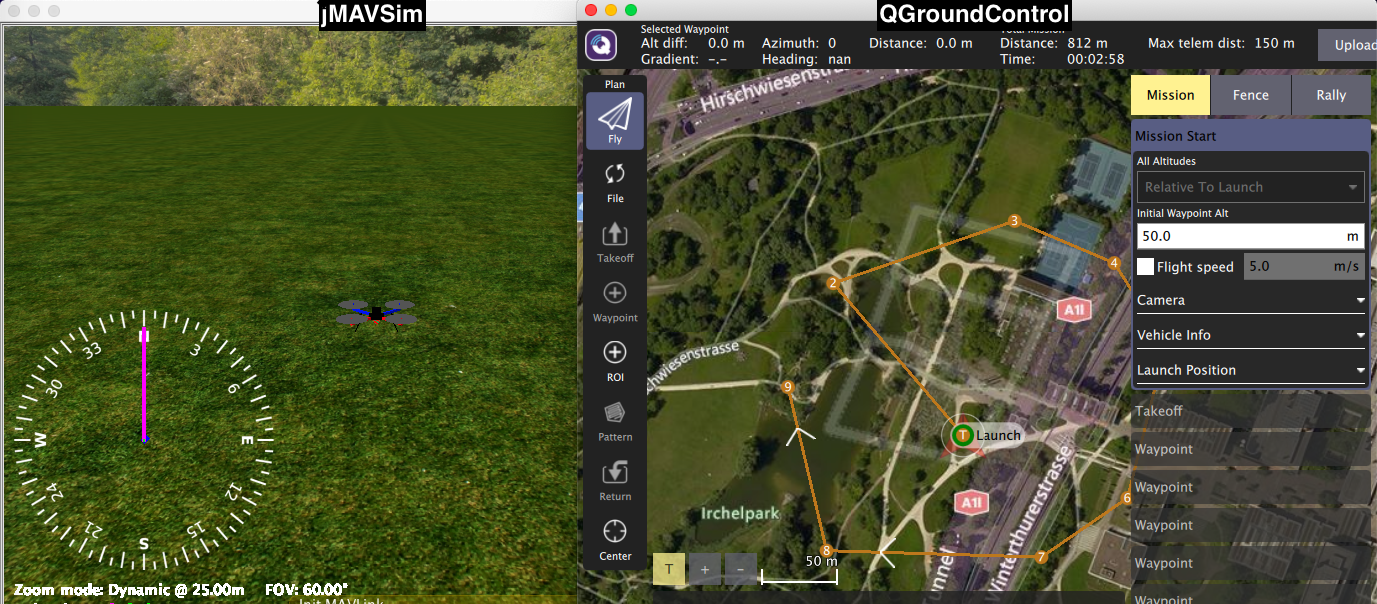
**2.4.2.3. 드론의 목적지 고정**

최초 명령의 전달 이후 GPS로 부터 받은 신호를 드론 내부에 고정적으로 저장한다. 이후 위조된 신호 또는 정상적인 신호를 무시하여 중간에 변동 없이 초기 지시된 수행을 마무리할 수 있도록 강제한다. 미션에 대한 유동성이 떨어지지만 드론의 탈취 및 외부로 부터의 간섭을 최소화 할 수 있을 것이라 생각된다. Spoofing 방지될 듯 싶다.

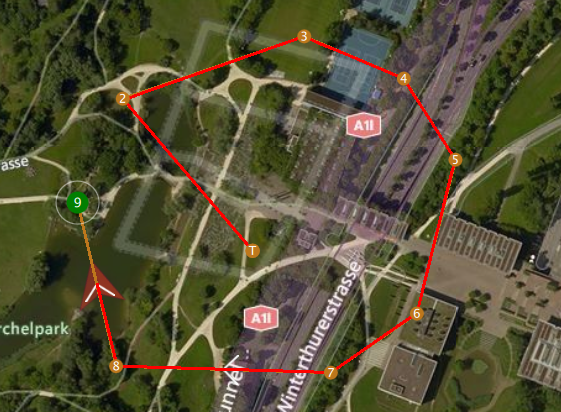
**3. 프로젝트 내용**

**3.1. 시나리오**

**3.1.1. PX4 기반 시뮬레이션 작동**

 **[그림 3] jMAVSim (좌) 과 QGroundControl 의 interface**

[그림 3]은 PX4 Project의 QGroundControl 화면과 SITL 프로그램인 jMAVSim의 화면이다. QGroundControl 의 좌측 상단을 보면 톱니바퀴의 설정모양이 있다.

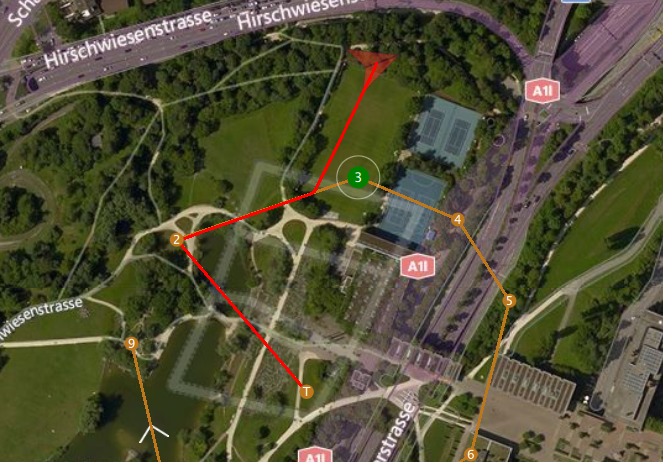


**[그림 4] mission에 따라 비행을 수행하는 드론**

이 설정을 통하여 [그림 4] 와 같이 waypoint들을 만들어 드론이 수행할 mission 을 지정해준다. 위와 같은 mission 이 지정되어있으면 그림 1의 비행 버튼을 클릭하여 실제 jmavsim 과 QGroundControl 에서 해당 드론이 비행함을 볼 수 있다.

**3.1.2. 대응방안이 없을 때의 해킹 시연**

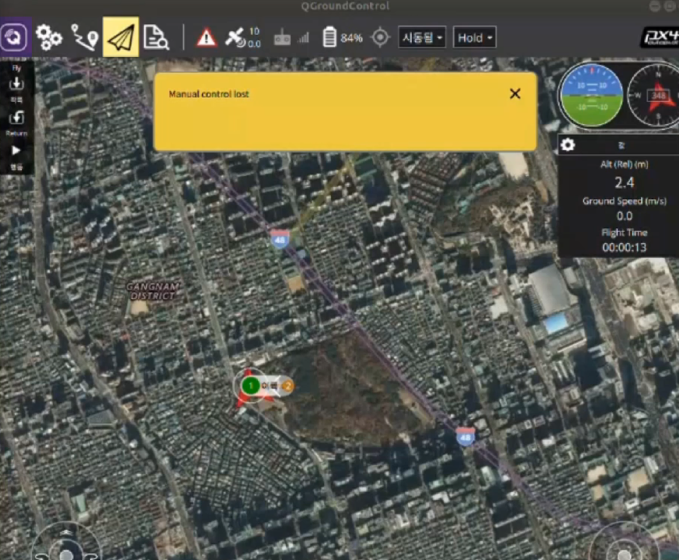
**3.1.2-1 기존의 통신이 유지된 채로 해킹을 당했을때**

****

**[그림 5] 기존의 통신이 유지된 채 외부 공격으로 경로 바뀐 상황**

3.1-1 환경에서 외부 접근을 통해 GCS 와 UAV 간의 통신을 가로채 UAV에게 기존 mission 과는 다른 명령을 전달하여 기존의 경로가 아닌 다른 경로로 UAV를 유도하고자 한다. [그림 5]는 [그림 4]에서 보인 경로에서 외부 공격에 의해 mission 이 아닌 길을 가고 있는 상황이다. Qgroundcontrol 상에서 확인을 할 수 있다. 이처럼 기존 통신이 연결되어있다면 실시간으로 경로의 변경을 파악 할 수 있다는 특징이 있다.

**3.1.2-2 외부 공격으로 인해 통신이 단절된 경우**



**[그림 6] 외부 공격으로인해 통신이 단절 된 상황**

[그림 6] 의 경우는 외부 공격에 인해 통신이 단절되어 오른쪽 상단에 ‘Manual control lost’ 라는 경고문이 나온 상태이다. 이 상황이 된다면 UAV에 대한 모든 control 이 불가능한 상황이 된다.

**3.1.3. 대응방안이 들어간 후 해킹 시연**

3.1-2 의 두가지 해킹 상황을 해결하게 된다면 외부공격이 오더라도 [그림 4] 의 mission 을 그대로 진행하게 된다. 대응방안이 적용된 시스템은 외부의 공격이 있었음을 사용자에게 알리고 경고를 주는 형태로 사용자에게 상황을 전달하고자 한다.

**3.2. 요구사항**

**3.2.1. PX4 기반시뮬레이션 에 대한 요구사항**

PX4 기반 시뮬레이션을 사용하기 위해서는 PX4 Tool Chain 을 사용하여 관련 프로그램들을 설치하여야한다. 해당 과정은 linux ubuntu 18.04f를 기준으로 한다.

1. Tool-chain 설치 스크립트 생성

* + sudo apt-get install git
  + git clone <https://github.com/PX4/Firmware.git> --recursive
  + cd Firmware
  + bash ./Tools/setup/ubuntu.sh
  + sudo reboot now

2. QGroundControl 설치

- sudo apt-get remove modemanager -y

- sudo apt install gstreamer1.0-plugins-bad gstreamer1.0-libav

gstreamer1.0-gl -y

* wget https://s3-us-west-2.amazonaws.com/qgroundcontrol/latest/QGroundControl.AppImage

3. QgroundControl & jmavsim 실행

- chmod +x ./QGroundControl.AppImage

- ./QGroundControl.AppImage

**3.2.2. 해킹에 대한 요구사항**

**-** 해당 연구에서는 UAV와 GCS 간의 통신에 사용되는 Mavlink protocol 쪽의 해킹 공격에

대응하고자한다. (UAV 와 GPS 간의 통신, UAV의 악성 펌웨어 사전 설치 배제)

- 3.1-2 에서 언급한 바와 같이 기존의 통신이 유지된 상황과 기존의 통신이 끊긴 두가지 상황을

구현한다.

**3.2.3. 대응책에 대한 요구 사항**

**3.2.3-1 외부 공격 후 통신이 유지된 상황**

**-** 드론의 비행 경로를 GPS를 통해 지속적으로 추적한다.

- 실제 이동 경로와 예상 경로를 비교한다.

- 예상 경로의 반경 50m 이상 이탈한 순간을 목적지 변경 시점으로 인지한다.

- 목적지 변경에 대한 경고를 최초 사용자에게 전달한다.

- 외부 간섭을 최소화하기 위해 목적지 변경에 제약을 준다.

- 한번 요구된 목적지는 끝까지 수행되도록 고정한다.

- IDS 를 구성 할 경우, False Positive를 줄이기 위해서 AI 를 통한 학습이 필요하다.

- 이 때 , 학습될 데이터의 양이 적기 때문에 비지도 학습법을 통한 학습이 필요하다.

**3.2.3-2 외부 공격 후 통신이 단절된 상황**

**-** 통신이 단절된 경우 UAV에게 명령을 줄 수 없는 상황이기에 UAV 자체에서 제어를 해야한다는

한계가 있다.

**-** UAV에는 실시간 판단 명령어를 주기에는 어려움이 있으므로 오용탐지 기법을 사용한 경량화된

IDS 기법을 적용하여 이상 명령어가 들어 왔을 경우 복귀하거나 이전 통신을 재연결하는 형식을

구축하여야 한다.

- IDS 기술을 적용하지 않을 시에는 기존의 연결 세션에 대한 특징을 UAV에 저장하고 이 변경사항이

발생하는 즉시 UAV는 명령을 받아들이지 않고 위와 동일한 조치를 취해야 한다.

**4. 향후 일정 및 역할 분담**

-px4-autopilot 구성 파일 분석

- 해킹 방식 조사 및 분석

- jMAVSim을 통한 드론 해킹 모의 실험

- 고안한 보안 방식 구현 및 적용

- 보안 성능 확인 및 평가

- 문제 분석 및 피드백

**5. 결론 및 기대효과**

해당 연구를 통해서 PX4 Project를 사용한 드론 운용에 대한 이해를 높일 수 있다고 본다. 위치, 법 등 다양한 제약조건 상황에 영향을 받지 않고 원하는 형태로 드론을 운용함으로서 드론에 대한 여러 문제점을 파악할 수 있게 될 것이다.

두번째로, 드론의 보안 문제를 파악함으로 드론 운용자들(기업 및 민간)에게 드론 해킹에 대한 경각심을 일깨워 줄 수 있으며, PX4 사용자들에게도 시각적인 자료를 제공할 수 있게 될 것이다.

세번째로 드론의 보안 문제에 대한 해결책을 마련함으로써 해킹에 대한 위협에 다소 자유로워 질 것이며, PX4 오픈소스에 이를 언급 및 공유 함으로써 해당 커뮤니티에 기여를 할 수 있다.

마지막으로, 해당 연구의 과정을 공유함으로써 기존의 부족했던 드론 입문자들을 위한 자료가 생성 될 것이다.

**6. 참고문헌**

[1] PX4 AutoPilot Github : https://github.com/PX4/PX4-Autopilot.git

[2] PX4 AutoPilot User Guide : https://docs.px4.io/master/en/

[3] 조승민, “드론 보안에 적용된 암호기술 현황”, 정보보호학회지 vol.30-2 , 2020.4

[4] A. Koubâa, "Micro Air Vehicle Link (MAVlink) in a Nutshell: A Survey," in *IEEE Access*, vol. 7, pp.

87658-87680, 2019

[5] 류해원, 최성한, 하일규, “드론 운용의 보안 위협과 대응 방안", 한국정보처리학회, 2018.10