

데이터 무결성을 보장하는 ROS 기반 무인 항공 시스템

이효준, 윤지영, 박경준
대구경북과학기술원

{hj.lee; hailey_yoon; kjp} @dgist.ac.kr

ROS-based Unmanned Aerial Systems for Ensuring Data Integrity

Hyojun Lee, Jiyoung Yoon, Kyung-Joon Park
Daegu Gyeongbuk Institute of Science & Technology (DGIST)

요 약

최근 활용도가 높아지는 UAV(Unmanned Aerial Vehicles)는 단순한 조종뿐 아니라 자율비행과 군집비행 등 용도에도 쓰인다. 이를 위해 소프트웨어 프레임워크인 ROS(Robot Operating System)를 UAV와 함께 사용하며 이는 UAV와 센서, 그리고 지상 관제소와의 통신의 중심에 위치한다. 이때 비행에 영향을 미치는 대량의 데이터가 UAV에 전송된다. 본 논문에서는 ROS 내 통신 문제점으로 인한 UAV의 취약성에 대해 서술하고 해당 문제점을 해결할 수 있는 방법을 제안한다.

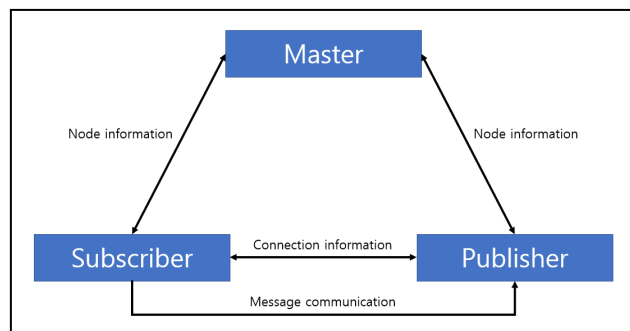
I. 서론

드론이라 불리는 UAV(Unmanned Aerial Vehicles)는 레저, 미디어 엔터테인먼트, 인명 구조 활동, 군사 목적 등 점점 더 많이 이용되고 있다. 이런 상황에서 상용 드론의 확산은 더욱 늘어날 전망이다. 미국 연방항공청(FAA)은 최근 2019~2039년 상업용 및 비상업용 드론의 수를 예측한 예측 보고서 'FAA 항공 전망 2019-2039'를 발표했다. 상업용 드론 시장이 예상보다 빠르게 성장하고 있는 것으로 나타났으며 2023년까지 3배 이상 늘어날 전망이다. 또한 드론은 CPS(Cyber Physical System)의 중요한 분야 중 하나로 떠오르고 있다.[1, 2]

드론의 활용도는 증가하고 있으며 단순한 RC 조종뿐만 아니라 자율비행, 군집비행 등 용도에도 쓰인다. 이러한 기능을 위해 Robot Operating System (ROS)과 드론이 함께 UAS(Unmanned Aerial Systems)로 구축되어 사용된다. ROS는 로봇 소프트웨어 개발을 위한 소프트웨어 프레임워크로 나사의 Robonaut 등 많은 로봇 플랫폼에서 점점 더 많이 사용되고 있다. 드론은 ROS를 이용해 여러 개의 센서를 장착해 군집을 제어 비행하거나 자율적으로 비행하는 등 응용된 비행을 할 수 있게 된다.

ROS는 다음 그림 1과 같이 master, publisher, subscriber의 세 가지 유형의 node로 구성된다. Master node는 서로 데이터를 교환하려는 publisher와 subscriber 사이의 연결고리 역할을 한다. Topic은 데이터의 방향성에 사용되며, publisher는 원하는 subscriber에게 특정 topic(센서 값 또는 명령)을 전달한다. Subscriber는 해당 topic에 대한 값을 받아 후속 로봇 활동에 필요한 프로세스를 실행한다.

ROS의 publisher와 subscriber 사이의 통신은 평문으로 이루어지며, 공격 대상 드론이 ROS를 이용하는 것을 알고 있는 공격자는 포트 스캔을 통해

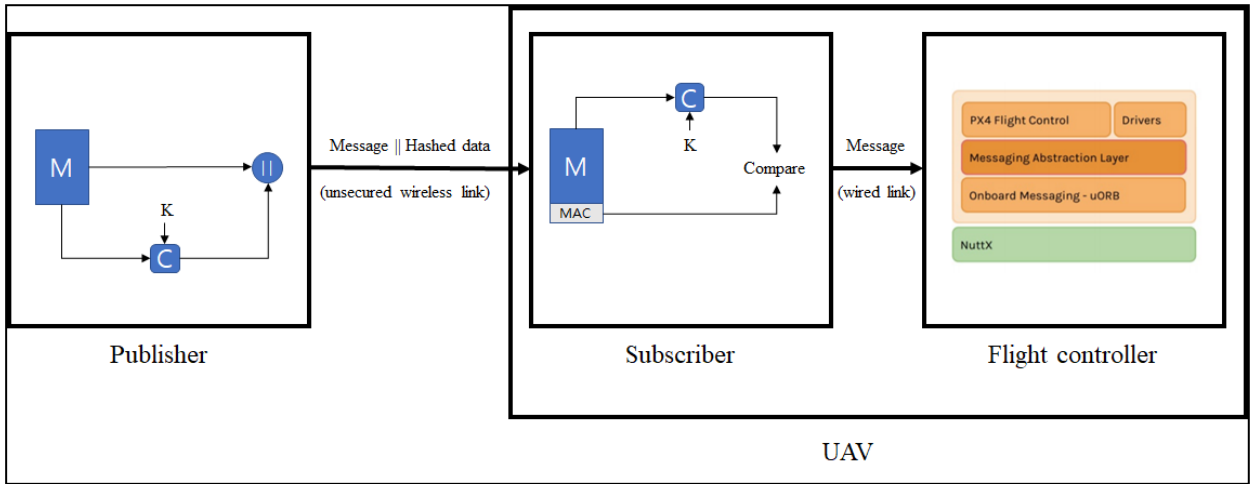


<그림 1> ROS 개념도.

master가 실행되는 컴퓨터의 IP 주소를 알아낼 수 있다. 이후 드론 시스템에서 사용하는 topic에 publisher와 subscriber를 연결해 비정상적인 센서 데이터 또는 명령을 전달하거나 시스템에서 주고받는 데이터를 도청하는 것이 가능하다. Publisher를 연결해 데이터를 sniffing하는 공격자는 시스템에서 상대적으로 민감한 공격이 아니다. 하지만 publisher를 연결하고 비정상적인 데이터를 주입하면 드론 비행에 큰 영향을 미칠 수 있다. 그래서 우리는 ROS 내 통신에서 데이터 무결성을 보장하는 UAS를 제안한다.

II. 본론

ROS에서 공격자는 시스템 내의 데이터에 대한 sniffing 및 injection 공격을 간단한 방법으로 수행할 수 있다. 공격자가 ROS가 동작하는 네트워크에 침입할 수 있는 경우, master node에 publisher node로 등록하여 원하는 subscriber node에게 데이터를 전송할 수 있다. 우리는 이러한 ROS 취약점을 해결하기 위해 ROS 통신에 Message Authentication Code(MAC)를 구현한 시스템을 제안한다.



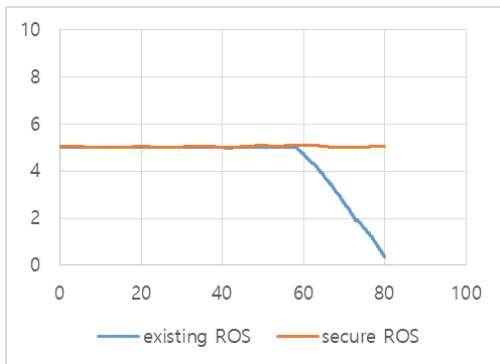
<그림 2> MAC이 적용된 ROS 기반 UAV 개념도

ROS는 오픈소스 시스템이라 소스에 접근할 수 있었고, ROS의 무결성을 확보하기 위해 소스 코드로 MAC을 구현했다. ROS의 MAC 구현은 그림 2에 나타나 있으며, publisher와 subscriber가 그 기능을 수행한다. 그 과정의 세부사항은 다음과 같다. publisher가 원본 메시지와 원본 메시지를 hash 함수를 통해 변환한 데이터인 MAC을 subscriber에게 전달한다. subscriber는 데이터를 수신하고, MAC과 원본 데이터를 분리한 다음, 원본 데이터를 hash 함수로 변환한다. 그런 다음 수신된 MAC을 이전 단계의 hash 값과 비교하여 데이터가 손상되었는지 확인한다. 데이터가 변조되었다고 판단하면 수신된 데이터를 무시하고, 그렇지 않다면 비행 제어를 담당하는 flight controller에게 데이터를 전달한다.

위와 같은 기능의 구현을 위해 publisher와 subscriber에 hash 함수를 구현했다. MAC의 안정성은 hash 알고리즘의 안전성에 좌우되기 때문에 hash 알고리즘은 SHA-256을 사용했다. SHA-256은 빠른 출력 속도의 장점을 가지고 있으며 블록체인에 가장 널리 채택되어 사용되고 있다.

우리는 Software in the Loop(SITL) 환경에서 실험을 진행하였다. 실험에서 ROS의 topic은 센서 값이 아닌 명령어로 간주된다. 우리의 실험 환경은 다음과 같다. 우리는 드론 보드에는 Pixhawk2를 사용하고 펌웨어에는 PX4를 사용한다. 그리고 ROS는 Raspberry pi의 Ubuntu MATE에 설치되어 있다. 그리고 Raspberry pi는 Pixhawk2에 연결되며 ROS publisher가 받은 데이터를 전달한다. 실험에 사용되는 ROS topic은 확장된 ROS 패키지인 MAVROS의 setpoint_position/local이다.

먼저 기존의 시스템에서의 드론이 비행할 때 공격에



<그림 3> 시간에 따른 드론 고도 변화

대한 영향을 실험했다. 정상적인 이용자는 5m 고도에서 최대 80 초까지 드론을 제어하려고 하였으나 공격자는 58 초 지점에서 악의적인 publisher를 이용해 드론에게 접근했다. 그 결과 그림 3과 같이 드론이 80 초에 이를 때까지 서서히 고도를 낮추는 것을 볼 수 있다.

두 번째 실험은 MAC을 적용한 시스템에서 드론의 움직임을 분석하였다. 앞선 실험과 같이 정상적인 사용자가 드론을 5m 고도로 조종하면 공격자가 드론을 0m 고도로 비행하도록 방해한다. 그림 3은 실험 결과를 보여준다. Subscriber가 공격자의 악의적인 publisher로부터 생성된 데이터를 받아들이지 않고 드론은 5m 고도에서 80 초 간 비행한다. 이 두 실험을 통해 ROS에서의 MAC 알고리즘 사용이 무결성이 보장된 데이터의 전송을 가능하게 한다는 것을 확인할 수 있었다.

III. 결론

자율 비행, 군집 비행과 같이 응용된 UAV의 비행을 위해 사용하는 ROS가 탑재된 드론의 데이터는 무결성에 취약하다. 이러한 문제는 드론의 비행에 매우 치명적인 위험을 줄 수 있다. 이를 해결하기 위해 SHA-256 알고리즘을 이용한 MAC을 ROS에 적용한 시스템을 제안한다. 또한 이 방법이 ROS의 데이터의 무결성을 보장할 수 있다는 것을 두 가지 실험을 통해 입증했다.

ACKNOWLEDGMENT

본 연구는 방위사업청과 국방과학연구소가 지원하는 군집형 무인 CPS 특화연구실 사업의 일환으로 수행되었습니다.

(UD190029ED)

참고 문헌

- [1] K.-J. Park, R. Zheng, and X. Liu, "Cyber-physical systems: Milestones and research challenges," Computer Communications, vol. 36, issue 1, pp. 1-7, December 2012.
- [2] K.-J. Park, J. Kim, H. Lim, and Y. Eun, "Robust path diversity for network quality of service in cyber-physical systems," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2204-2215, November 2014.