uORB 메시지 기반 내부 이상 탐지 프레임워크

하영빈*, 장우현**, 김연재**, 허재원**, 박기웅†

세종대학교 SysCore Lab. (대학원생)

LIG넥스원 (연구원)

***세종대학교 정보보호학과 (교수†)

uORB Message-based Internal Anomaly Detection Framwork

Young-Bin Ha*, Woo-Hyun Jang**, Yeon-Jae Kim**, Jae-Won Heo**, Ki-Woong Park†

*SysCore Lab., Sejong University

**LIG Nex1

***Dept. of Computer and Information Security, Sejong University

(Graduate Student*, Researcher**, Professor†)

요 약

현대 무기체계는 비행 제어, 항법, 자율 임무 수행 등을 위해 다수의 센서, 통신 모듈이 상호 연동되어 동작하는 복잡한 제어 구조를 갖추고 있다. 이러한 시스템 구조는 더 많은 기능을 효율적으로 수행할 수 있도록 하지만, 동시에 내부 파라미터 조작이나 펌웨어 변조와 같은 템퍼링 공격에 노출될 가능성이 있다. 이에 본 연구는 비행 제어 소프트웨어 내부의 미들웨어를 통해 전달되는 데이터를 검증하는 방식으로 시스템에서 발생하는 이상을 탐지하는 프레임워크를 제안한다. 해당 프레임워크는 PX4 오픈소스 비행 제어 시스템에서 미들웨어를 담당하는 uORB를 기반으로 하여 각 모듈 간 교환되는 메시지의 정보를 실시간으로 모니터링하도록 구현하였다. 이를 통해 이상의 경계가 모호한 실질적 데이터가 아닌 데이터의 시간적 일관성 및 논리적 특성 등을 검증함으로써 이상 징후를 탐지하고자 한다.

I. 서론

현대 무기체계는 비행 제어, 항법, 여러 센서 데이터에 기반한 자율적 의사결정 등을 수행하기 위해 복잡한 소프트웨어 구조로 발전하고 있다. 이러한 무기체계는 다양한 센서 및 통신 모듈 등의 장치를 연결하여 실시간으로 데이터를 교환하며 동작하는데, 이와 같은 구조는 임무를 수행함에 있어 효율성과 유연성을 높이지만, 파라미터 변경과 펌웨어 변조와 같은 템퍼링(Tampering)에 취약하다[1, 2]. 임베디드 환경에서 공격자는 네트워크 및 전자 공격 [3]등 외부 채널을 통해 시스템 탈취를 시도할 뿐만 아니라 하드웨어적으로 침투하여 접근이 가능한데, 이러한 상황에서 외부 요소에 대한 모니터링만으로는 위협 상황을 식별하기 어렵다. 따라서 시스템 내부의 데이터 흐름과 모듈 간 상호작용을 직접 관찰할 수 있는 구조적 접근이 하나의 방안이 될 수 있으며[4], 운영체제와 응용 프로그램 사이에서 서로 다른 시스템 간의 데이터 전달, 통신 등의 역할을 수행하는 중간 계층 소프트웨어인 미들웨어 계층의 동작을 모니터링함으로써 이를 수행하고자 한다.

미들웨어에는 ORB(Object Request Broker)라는 분산 객체 시스템에서 객체 간의 호출을

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

이 논문은 2022년 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임(KRIT-CT-22-051)

지원하는 미들웨어 유형이 있으며, PX4는 ORB의 개념을 기반으로 RTOS 환경에서 내부 모듈 간 고성능·저지연 메시지 통신을 지원하는 uORB(micro Object Request Broker)를 사용한다[5, 6].

본 연구는 이러한 PX4 내부 메시지 미들웨어인 uORB에서 발생하는 토픽과 각 토픽의 메타데이터를 실시간으로 모니터링하여, 공격자가 시스템을 탈취하거나 제어 권한을 확보하는 과정에서 발생할 수 있는 펌웨어 변조 등 템퍼링 행위를 실시간으로 탐지하기 위한 실시간 경량 검증 기법을 제안한다.

본 논문의 구성은 2장에서는 관련 연구를 기술하고, 3장에서는 실험 환경 및 구현한 프레임워크에 대해 서술한다. 끝으로 4장에서 결론 및 향후 연구를 언급하며 마무리하고자 한다.

II. 관련 연구

Abdullahi Sani Shuaibu 외 5인은 DDS(Data Distribution Service) 미들웨어의 publish-subscribe 구조를 이용해 각 모듈로부터 전압, 전류, 전력 등의 전기적 데이터를 실시간으로 수집하고, 이를 사전에 학습된 DNN 기반 모델에 전달하여 분석함으로써, 스파이크나 단기간 전력 소비량의 비정상적 변동과 같은 시스템의 이상을 탐지하였다[7].

Haocheng Meng 외 5인은 PX4 비행 제어 시스템의 uORB 미들웨어를 통해 교환되는 센서 데이터를 이용하여 IMU에 대한 공격을 탐지하는 기법을 제안하였다. 해당 모듈이 공격받거나 비정상 값을 출력할 경우, 각속도와 가속도를 추력과 토크로 대체하여 상태를 추정하는 기법을 적용하였으며, Gazebo 시뮬레이터 환경에서 평가를 수행하였다[8].

III. 실험 환경 및 프레임워크

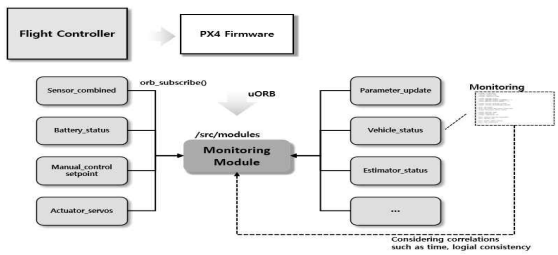
3.1 실험 환경 구성

본 연구의 실험은 PX4 오픈소스 비행 제어 알고리즘과 내부 미들웨어인 uORB의 동작을 실제 환경과 유사하게 재현하기 위해 SITL(Software In The Loop) 환경에서 수행하였다. 또한 비행 환경 시뮬레이터인 jMAVSim과 SITL을 연동하여 센서 데이터, 자세, 배터리 상태 등의 정보가 상호 교환되는 과정을 모사함으로써, 내부 데이터 흐름을 관찰할 수 있는 환경을 구축하였다[9].

3.2 uORB를 활용한 이상 탐지 프레임워크

본 논문에서 제안하는 이상 탐지 프레임워크를 구현하기 위해, PX4 펌웨어의 모듈들이 위치한 경로에 감시 모듈을 추가하였으며, 해당 모듈은 uORB 기반 메시지 전달 방식을 통해 동작한다. 추가된 감시 모듈은 PX4의 빌드 시스템 내에 정상적으로 컴파일 및 실행될 수 있도록 모듈의 경로와 소스 파일 등록, 설정 항목을 추가하여, 사용자가 해당 모듈의 활성화 여부를 선택할 수 있도록 하였다.

스레드 및 프로세스 간 비동기식 메시지 교환 구조를 따르는 uORB는 각 모듈이 게시한 정보를 다른 모듈이 구독하여 실시간으로 참조할 수 있도록 한다. 이러한 구조적 특성을 이용하여 식별하기 힘든 사용자의 의도적인 조작과 공격자의 악의적 변조에서 나타나는 내부 데이터의 변화에 초점을 맞추는 것이 아닌, 시스템 동작 과정에서 필연적으로 남는 행위 기반의 흔적인 메타데이터 정보를 모니터링 함으로써, 시스템의 상태를 실시간으로 검증할 수 있도록 하였다. 아래의 (그림 1)은 앞서 제안한 프레임워크의 아키텍처를 나타낸다.

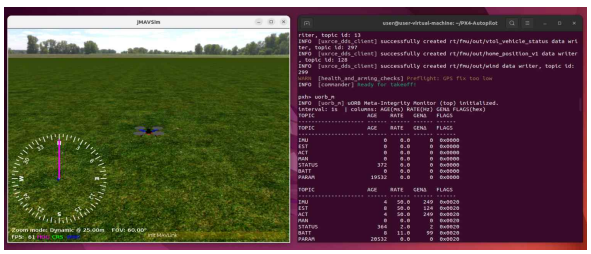


(그림 1) uORB 기반 제안 프레임워크 아키텍처

감시 모듈은 메인 루프 내에서 주기적으로 각 토픽의 갱신 상태를 확인한다. 이 과정에서 Subscribe API를 통해 각 토픽의 핸들을 가져오며, 이러한 핸들은 사용자 입력으로부터 생성된 명령, 센서, 비행 상태 등의 데이터를 포함

하는 토픽들을 인자로 입력받는다. 각 토픽이 게시될 때 해당 데이터가 언제, 어떤 순서로 시스템 내에서 전달되었는지 등과 같은 메타데이터를 메시지 구조체 필드에 포함하는데, 이를 탐지 요소로 활용하여 모듈 간의 데이터를 시계열적으로 분석함으로써 재생(Replay) 혹은 자원 고갈 공격 등으로 인한 태스크 지연이나 파라미터 및 제어 신호 변조 등의 비정상적인 변화를 탐지할 수 있다.

(그림 2)은 구현한 탐지 프레임워크를 실행한 화면을 나타낸다. 해당 모듈을 실행할 경우, 각 토픽과 해당 토픽의 게시 후 경과 시간, 업데이트 빈도, 누적 발생 횟수 등의 메타데이터가 주기적으로 출력된다. 본 프레임워크는 모니터링 범위를 확장하거나 감시 주기를 조절하는 등 구조적 수정이 간단하며, 수집된 데이터를 DDS로 변환하여 외부 시스템으로 전달할 수 있다는 확장성을 갖는다.



(그림 2) 구현 프레임워크 실행 화면

IV. 결론 및 향후 연구

본 논문에서는 PX4 오픈소스 시스템의 미들웨어인 uORB를 기반으로, 비행 제어 소프트웨어 내부의 데이터 정보를 실시간으로 검증하는 이상 탐지 프레임워크를 제안하였다. 제안한 프레임워크는 미들웨어 계층을 통해 각 모듈 간 교환되는 메시지의 메타데이터를 수집함으로써, 데이터값 자체가 아닌 행위 기반 특성으로 시스템 동작의 이상 징후를 식별할 수 있음을 보였다. 향후 연구에서는 SITL 환경이 아닌 HITL 혹은 실제 기체에, 제안한 모듈 형태의 프레임워크를 적용하고, 공격 시나리오를 설계 및 수행함으로써 오탐, 미탐이 발생하는가에 대한 탐지 성능뿐만 아니라 지연과 오버헤드 등 운영적 측면을 정량적으로 평가하고자 한다.

[참고문헌]

[1] U.S. Government Accountability Office (GAO), Weapon Systems Cybersecurity, GAO-19-128, Washington, D.C., Oct. 2018.

[2] Y.Zhang, Y.Li and Z.Li, Aye: A Trusted Forensic Method for Firmware Tampering Attacks, Symmetry, vol. 15, no. 1, article 145, Jan, 2023, doi: 10.3390/sym15010145.

[3] J-P,Yaacoub, H.Noura, O.Salman and A.Chehab, Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations, Internet of Things (Amst), vol. 11, 100218, May, 2020, doi: 10.1016/j.iot.2020.100218.

[4] S.Gautham, A.Rajagopala, A.V.Jayakumar, C.Deloglos, E.Karincic and C.Elks, Heterogeneous Runtime Verification of Safety Critical Cyber Physical, Systems, arXiv preprint arXiv:2009.09533, Sep, 2020, doi: 10.48550/arXiv.2009.09533.

[5] L.Meier, D.Honegger and M.Pollefeys, PX4: A Node-Based Multithreaded Open Source Robotics Framework for Deeply Embedded Platforms, Proceedings of the IEEE International Conference on Robotics and Automation (ICRA), Seattle, WA, USA, May, 2015, pp. 6235 - 6240, doi: 10.1109/ICRA.2015.7140074.

[6] S.D.Angelo, F.Pagano, F.Longobardi, F.Ruggiero and V.Lippiello, Efficient Development of Model-Based Controllers in PX4 Firmware: A Template-Based Customization Approach, Proceedings of the 2024 International Conference on Unmanned Aircraft Systems (ICUAS), Chania, Crete, Greece, June, 2024, doi: 10.1109/ICUAS60882.2024.10556938.

[7] A.S.Shuaibu, S.U.Haq, B.Almadani,

F.Aliyu, E.Al-Nahari et al., Smart Metering Meets AI: Real-Time Appliance Monitoring and Anomaly Detection over DDS Middleware, IEEE Transactions on Industry Applications, early access, pp. 1 - 18, Sep, 2025, doi: 10.1109/TIA.2025.3608687.

[8] H.Meng, S.Luo, Z.Liang, Q.Huang and A.Khazraei, MARS: Defending Unmanned Aerial Vehicles From Attacks on Inertial Sensors with Model-based Anomaly Detection and Recovery, arXiv preprint arXiv:2505.00924, May, 2025, doi: 10.48550/arXiv.2505.00924.

[9] A.Tullu, S.H.Jung and S.C.Lee, Effects of Model-Specific Parameters on the Developments of Custom Module in PX4 Autopilot Software-int-the-Loop, International Journal of Aerospace Engineering, vol. 2025, Article ID 4886534, pp. 18, Feb, 2025, doi: 10.1155/ijae/4886534.