ROS 기반 신뢰성 및 이상 탐지 방법론의 micro-ROS 적용 방안에 대한 연구

김경환[1], 강정환[2], 권동현[3]
[1]부산대학교 정보컴퓨터공학부 학부생
[2]부산대학교 정보융합공학과 박사과정
[3]부산대학교 정보컴퓨터공학부 교수 (교신저자)
{kyounghwankim, jeonghwan, kwondh}@pusan.ac.kr

Feasibility Study of Applying ROS-Based Reliability and Anomaly Detection to micro-ROS

Kyoung-Hwan Kim[1], Jeong-Hwan Kang[2], Dong-Hyun Kwon[1]
[1]School of Computer Science and Engineering, Pusan National University
[2]Dept. of Information Convergence Engineering, Pusan National University

요 약

ROS (Robot Operating System)는 로봇 소프트웨어의 효율적인 개발과 확장을 가능하게 하며, 많은 산업 및 연구 현장에서 표준 인터페이스로 자리잡고 있다. 최근에는 마이크로컨트롤러 (MCU)에도 적용 가능한 micro-ROS가 등장함에 따라 임베디드 환경에서도 널리 사용되고 있다. 그러나 micro-ROS의 초경량 통신 계층인 XRCE-DDS는 암호화를 포함한 DDS Security 기능을 완전히 지원하지 못해 잠재적인 보안 취약점이 존재한다. 따라서 본 논문에서는 ROS 1 및 ROS 2에서 수행된 대표적인 신뢰성 및 이상 탐지 연구들을 분석하고, 그 결과를 micro-ROS 환경에 이식했을 때의 적용 가능성과 한계를 평가한다. 이러한 접근은 micro-ROS 기반 로봇 시스템에서의 신뢰성과 안전성을 높이는 데에 기여할 것이며, 다양한 산업 분야에서의 응용 가능성 확대에 핵심적인 역할을 할 것으로 기대된다.

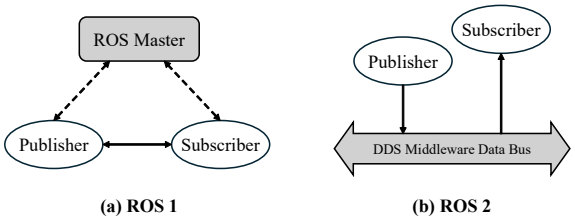
1. 서론

현대 로봇 시스템의 발전과 함께, ROS (Robot Operating System)는 다양한 분야에서 중요한 역할을 수행한다. 특히, 로봇 소프트웨어의 효율적인 개발과 확장을 가능하게 하며, 많은 산업 및 연구 현장에서 표준 인터페이스로 자리잡고 있다. 최근에는 기존 ROS의 장점을 계승하고 임베디드 환경에 최적화된 경량화 버전인 micro-ROS[1]가 널리 사용되고 있다.

micro-ROS는 마이크로컨트롤러 (MCU)에서 실행될 수 있도록 설계된 초경량 로봇 운영체제이다. 통신 계층으로 XRCE-DDS (eXtremely Resource Constrained Environment DDS)를 채택해 패킷 크기와 메모리 오버헤드를 최소화하고, 정적 메모리 기반 런타임으로 실시간성·결정성을 확보한다. 또한, MCU가 DDS와 QoS 스택 전체를 자체 처리하기 어려운 한계를 보완하기 위해, micro-ROS 노드는 ROS 2 Agent를 통해 ROS 2 네트워크와 메시지를 주고받는다. 이러한 분산형 구조 덕분에 엣지 디바이스에서도 ROS 2와의 상호 운용성이 보장된다.

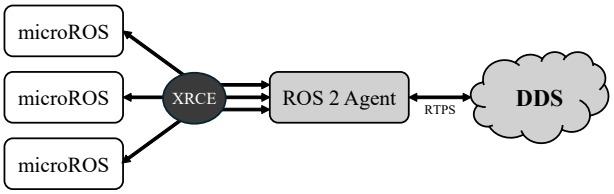
그러나 micro-ROS에서 사용하는 초경량 통신 계층인 XRCE-DDS는 암호화, 인증 및 세분화된 QoS 제어 등 DDS Security 기능을 완전히 지원하지 못해 위·변조나 서비스 거부(DoS)와 같은 공격에 노출될 수 있다. 따라서, 본 논문에서는 ROS 1과 ROS 2에서 진행된 신뢰성 및 이상 탐지 연구들을 분석하고, micro-ROS 환경에의 적용 가능성과 그 한계를 분석하고자 한다. 이러한 접근은 micro-ROS 기반 로봇 시스템의 신뢰성과 안전성을 높이는 데 기여할 것이며, 더 나아가 다양한 산업 분야에서의 응용 가능성을 확대하는 데 핵심적인 역할을 할 것으로 기대된다.

2. ROS 관련 연구 분석



(그림 1) ROS 1과 ROS 2의 통신 방식

ROS 1은 그림 1의 (a)에서 볼 수 있듯이 Master 노드 기반의 중앙 집중식 구조이다. 이로 인해 대부분의 ROS 1 환경에서의 연구가 중앙 집중형 네트워크 트래픽 기반의 이상 탐지 연구들[2][3]이다. 이러한 연구들은 ROS 1에서의 TCPROS/UDPROS 트래픽 데이터를 실시간으로 수집해 SVM, CNN 등의 머신러닝 모델을 사용하여 이상 지점을 탐지하는 방법론을 제안한다. 또한, ROSRescue[4]는 ROS 1의 Master 노드의 단일 실패 지점 문제를 해결하기 위해 가벼운 장애 복구 기능을 도입한 연구이다. 최소한의 메타데이터를 Master 노드에서 관리하여 낮은 오버헤드로 여러 노드를 동시에 관리할 수 있음을 보여준다. 하지만, ROS 2 기반의 micro-ROS에는 그림 1의 (b)와 같은 분산형 구조로, Master 노드와 같은 지점이 없고 노드들이 DDS와 직접 통신하며 패킷이 흩어지기 때문에 네트워크 트래픽 등 특정 데이터를 수집 및 분석하기 어렵다. 이러한 이유로 ROS 1에서 수행된 이상 탐지 및 장애 복구 기능을 바로 적용하기가 어렵다.



(그림 2) micro-ROS와 ROS 2 Agent 간의 통신 시각화

이러한 ROS 2 환경에서 수행된 이상 탐지 연구로는 Watch Your Callback[5]이 대표적이다. 해당 연구에서는 ros2_tracing 프레임워크를 통해 수집한 ROS 2 어플리케이션의 이벤트 로그를 분석하여 이상 지점을 탐지하는 방법론을 제안한다. 이를 통해 분산형 구조에서도 노드 내부의 실행 정보를 이용해 효과적으로 이상을 탐지할 수 있음을 보여준다. 하지만, micro-ROS에는 ros2_tracing 계측 지점이 존재하지 않아 MCU 상에서의 추적은 불가능할 수 있다. 그러나, micro-ROS 환경에서의 노드는 통신 및 동작을 위해 그림 2처럼 ROS 2 Agent와의 통신이 필수적으로 수행된다. 따라서 이러한 구조를 활용하면 ROS 2 기반 Agent에서의 간접적인 추적은 가능할 것으로 보인다. 즉, micro-ROS 환경에서도 ROS 2 기반의 이벤트 로그를 분석 지점으로 삼는 접근이 효과적일 수 있다.

3. 결론 및 향후 연구 방향

본 논문에서는 ROS 1·2 환경에서 제안되었던 신뢰성 향상 및 이상 탐지 기법을 검토하고, 이를 micro-ROS 환경에서의 적용 가능성과 한계를 분석하였다. micro-ROS는 MCU 기반의 임베디드 환경에서도 ROS 2 생태계와의 상호 운용성을 제공하지만, XRCE-DDS가 DDS Security를 온전히 지원하지 못한다는 보안적 취약성과 분산형 구조로 인해 관측할 수 있는 정보가 제한적이라는 가시성 문제를 동시에 안고 있다. 따라서, micro-ROS 기반의 환경 위에서 보안을 강화하고 신뢰성과 안전성을 높이는 연구가 지속적으로 추진될 필요가 있다.

사사문구

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. RS-2023-00217689).

참고문헌

[1] Belsare, Kaiwalya, et al. "Micro-ros." Robot Operating System (ROS) The Complete Reference (Volume 7). Cham: Springer International Publishing, 2023. 3-55.

[2] Antunes, Rodrigo Abrantes, Bruno L. Dalmazo, and Paulo LJ Drews. "Detecting data injection attacks in ROS systems using machine learning." 2022 Latin American Robotics Symposium (LARS), 2022 Brazilian Symposium on Robotics (SBR), and 2022 Workshop on Robotics in Education (WRE). IEEE, 2022.

[3] Santoso, Fendy, and Anthony Finn. "Trusted operations of a military ground robot in the face of man-in-the-middle cyberattacks using deep learning convolutional neural networks: Real-time experimental outcomes." IEEE Transactions on Dependable and Secure Computing 21.4 (2023): 2273-2284.

[4] Kaveti, Pushyami, and Hanumant Singh. "ROS rescue: fault tolerance system for robot operating system." Robot Operating System (ROS) The Complete Reference (Volume 5) (2021): 381-397.

[5] Kang, Jeonghwan, Kyounghwan Kim, and Donghyun Kwon. "Watch Your Callback: Offline Anomaly Detection using Machine Learning in ROS 2." IEEE Access (2025).