Journal of KIIT. Vol. 23, No. 8, pp. 87-95, Aug. 31, 2025. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2025.23.8.87

UGV 환경에서 운용 가능한 경량 룰셋 기반 탐지 기법

이화성*[1], 정영기*[2], 허선동*[3], 박무성*[4], 유찬곤*[5]

Lightweight Rule-based Detection for Operation in UGV Environments

Hwaseong Lee*[1], Youngki Jung*[2], Seondong Heo*[3], Moosung Park*[4], and Changon Yoo*[5]

요 약

무인지상차량(UGV, Unmanned Ground Vehicle)의 자율 주행 기능은 ROS(Robot Operating System)를 기반으로 다양한 센서 및 제어 모듈 간 실시간 데이터 교환에 의해 운용된다. 그러나 ROS는 개방형 구조로 인해 공격에 취약하며, 이는 시스템의 안정성에 위협이 된다. 본 논문은 ROS 1과 ROS 2 기반 무인지상차량을 대상으로 룰셋 기반 침입 탐지기법을 개발하고 실험적으로 검증하였다. 주요 공격은 악의적 노드의 생성 및 정상 노드에 특정 시그널을 주입해 조향, 센서 데이터, 상태정보 토픽을 비정상적으로 발행/구독하도록 유도하는 방식으로 구성되었다. 제안 기법은 경량 구조로 설계되어 효과적인 이상행위 탐지가 가능함을 실제 환경에서 입증하였고, 본 논문을 통해서 자원이 제한된 무인체 환경에서 보다 안전한 무인체 개발이 기대된다.

Abstract

Autunomous driving in Unmanned Ground Vehicle (UGVs) relies on real-time data exchange between various sensors and control modules, commonly supported vy the Robot Operating System (ROS). However, the open architecture of ROs makes it vulnerable to attacks, which can compromise the stability and safety of the system. This study develops rule-based detection methods for ROS 1 and ROS 2 environments, tested on real UGVs. The attacks include creating malicious nodes or injectin signals into normal nodes to trigger abnormal pulibhsing or subscribing of critical topics such as steering, sensor data, and system status. Experimental results demonstrate that the proposed lightweight detection system effectively identifies abnormal behaviors in actual robotic environments. This paper presents the necessity and research outcomes of lightweight anomaly detection techniques applicable to resource-constrained ummaned systems, contributing to the development of safer unmanned platforms.

Keywords

unmanned ground vehicle, robot operating system, rule-based detection, attack

* 국방과학연구소 연구원(*[1] 교신저자)
- ORCID[1]: https://orcid.org/0009-0007-9302-4456
- ORCID[2]: https://orcid.org/0009-0003-1245-5600
- ORCID[3]: https://orcid.org/0000-0002-7050-7208
- ORCID[4]: https://orcid.org/0000-0003-0760-5072
- ORCID[5]: https://orcid.org/0000-0003-1878-2162

· Received: May 15, 2025, Revised: Jun. 02, 2025, Accepted: Jun. 05, 2025
· Corresonding Author: Hwaseong Lee
Agency for Defense Development, Korea
Tel: + 82-2-3400-2646, Email: mail.hslee@gmail.com

Ⅰ. 서 론

자율주행 기반의 무인지상차량(UGV, Unmanned Ground Vehicle)은 정찰, 경로 안내, 재난 대응 등 다양한 현장 중심의 응용 분야에서 빠르게 확산 되고있다. 이러한 시스템은 카메라, LiDAR, GPS 등의 복수 센서와 경로 계획, 제어, 통신 기능이 유기적으로 연결되어 있으며, 복잡한 소프트웨어 아키텍처를 기반으로 실시간으로 동작한다. 특히 UGV는 ROS(Robot Operating System)를 중심으로 구성되는 경우가 많으며, 개방형 구조와 메시지 기반 통신의 특성상 공격에 취약하다[1]-[3]. 예를 들어 공격자가 새로운 노드를 삽입하거나, 정상 노드의 동작을 교란하여 잘못된 명령을 유도할 수 있다. 이는 시스템 전체의 안정성에 심각한 영향을 줄 수 있으며, 물리적 사고나 임무(Mission) 실패로 이어질 수 있다.

이러한 보안 위협에 대응하기 위한 다양한 이상 탐지 기법들이 제안되고 있다. 특히, 네트워크 기반 침입 탐지 시스템(NIDS), 머신러닝 기반 이상탐지 모델, ROS 전용 보안 미들웨어 등이 대표적이다[4][5]. 그러나 대부분의 기법은 복잡한 학습 절차나 비정형 데이터 처리를 포함하고 있어 연산 자원이 제한된 임베디드 환경, 특히 실시간 자율 주행 시스템에는 적용이 어렵다는 한계가 있다.

ROS 기반 UGV 시스템에서는 제한된 계산 자원 내에서 자율주행, 센서 데이터 처리, 보안 탐지 기능이 모두 동시에 수행되어야 하며, 과도한 자원 사용을 요구하는 보안 기법은 시스템의 실시간성이나 임무 수행 능력을 저해할 수 있다. 따라서 탐지 기법은 반드시 경량화되어야 하며, 시스템에 부하를 주지 않으면서도 필수적인 보안 기능을 효과적으로 수행할 수 있어야 한다.

한편 최근에는 룰셋 기반 탐지(Rule-based detection)가 다시 주목받고 있다[6]. 이는 복잡한 학습 없이도 미리 정의된 정상상태와의 비교를 통해 이상을 탐지할 수 있어, 처리 부화가 적고 해석 가능성도 높기 때문이다. 특히 ROS 환경에서는 노드 구성, 발행/구독 관계, 통신 등록 요청 등과 같은 정적인 시스템 구조를 탐지 기준으로 삼을 수 있어, 효율적인 보안 모듈 구현이 가능하다. 하지만 대부분의 룰 기반 기법은 시뮬레이션 환경에서만 평가되었거나 ROS 1에 한정되어 있으며, 실제 UGV 플랫폼에서 탑재 가능한 경량 탐지기 형태로 구현된 사례는 매우 제한적이다.

본 논문에서는 이러한 문제를 해결하기 위해, UGV 실험 환경에서 동작 가능한 경량 룰셋 기반 탐지 기법을 설계하고 ROS 1과 ROS 2 기반 플랫폼에 각각 적용하였다. 본 기법은 학습이나 통계 기반 모델 없이, 미리 정의된 정상상태 룰셋과 수집된 정보를 비교함으로써, 노드 삽입, 토픽 발행/구독 구조 변형 등과 같은 구조적 이상을 실시간으로 탐지한다. 또한 탐지기는 수집기로부터 전달받은 JSON/CSV 기반 시스템 정보를 실시간으로 룰셋과 비교하는 방식으로 경량화되어 있으며 실제 UGV에 NVIDIA Jetson Orin을 탑재하여 실험적 평가를 수행하였다. 이를 통해 본 논문은 구조 기반 탐지 방식의 실효성뿐만 아니라 실제 시스템 적용 가능성(Deployability)을 실험을 통해 검증하였다.

Ⅱ. 탐지 기법 구조 및 구현

본 논문은 ROS 기반의 UGV 환경에서 실시간으로 적용 가능한 경량 탐지 기법을 구현하기 위해, ROS 1과 ROS 2 환경에 모두 적용 가능한 탐지 모듈을 설계하였다. 전체 시스템은 수집기, 탐지기, 룰셋으로 구성되며, 각 구성 요소는 자율주행 임무 수행 중 발생 가능한 이상 행위를 최소한의 지원으로 탐지하도록 경량화되었다. 특히 ROS 1과 ROS 2는 구조적으로 차이가 크므로, 각 버전에 맞게 탐지 방식과 수집 정보의 종류가 구분되며, 이를 위해 모듈별 설계 전략을 독립적으로 구성하였다.

2.1 탐지 기법 요구사항 및 설계 개요

본 탐지 기법의 주요 설계 목표는 다음과 같다. 첫째, 실시간 동작이 가능해야 한다. UGV는 자율주행 중 지속적으로 센서 데이터를 처리하고 경로를 계획하므로, 탐지 모듈이 시스템의 실시간성을 저해하지 않도록 경량 설계가 필수적이다[7]. 따라서 탐지기는 별도의 비동기 프로세스로 동작하며, 일정

주기마다 필요한 정보만 선택적으로 수집하여 탐지를 수행한다.

둘째, 이식성과 확장성이 확보되어야 한다. 그림 1처럼 ROS 1은 마스터 기반 중앙 집중형 통신을 사용하는 반면, ROS 2는 DDS(Data Distribution Service) 기반의 분산 통신 구조를 채택하고 있기 때문에 각 환경에 맞는 탐지 방식이 필요하지만, 전체적인 설계는 유사한 구조를 따르도록 구성하여 상호 확장이 가능하도록 한다[8][9].

셋째, 정적인 룰셋 기반 탐지 방식을 채택한다. 이는 복잡한 학습 없이도 미리 정의된 정상상태의 정보만으로 이상을 판별할 수 있으므로, 자원 소비를 최소화할 수 있으며, 해석 가능성도 높다.

넷째, 실험적 검증을 통해 실제 UGV 임무 수행 중 탐지 모듈이 정상적으로 작동할 수 있음을 보여야 한다. 이를 위해 UGV에 NVIDIA Jetson Orin을 부착하여 탐지 모듈을 탑재하고, 다양한 공격 시나리오 하에서의 탐지 성능 및 시스템 자원 사용량을 측정하였다.

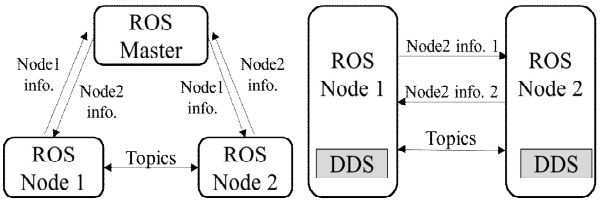

그림 1. ROS 1(좌)과 ROS 2(우)의 통신 방식 비교
Fig. 1. Comparison of communication architectures in ROS 1(left) and ROS 2(right)

2.2 ROS 1 기반 탐지 모듈

ROS 1 기반 탐지 모듈은 수집기와 탐지기로 구성되어 있다. 수집기는 주기적으로 시스템 정보를 수집하여 JSON 혹은 CSV 형식의 정제된 데이터로 저장하고, 탐지기는 해당 폴더에 신규 파일이 생성될 때마다 자동으로 룰셋과 비교하여 이상 여부를 판단한다. 이를 통해 실시간성을 유지하면서 탐지 모듈의 부하를 최소화하였다.

• 수집기: 주기적(예: 5초)으로 rosnode list 명령어를 실행하여 현재 활성화된 노드 목록을 수집한다. 동시에 ROS 마스터에 대한 XML-RPC(XML Remote Procedure Call) 요청 흐름을 tcpdump를 기반으로 수집한다. 수집된 결과 중 노드 생성/삭제 및 서비스 생성/종료와 관련성이 있는 정보만 선별하여 JSON 혹은 CSV 파일로 저장한다.

• 탐지기: 탐지기는 지정된 폴더를 모니터링 하고 있다가, 새로운 JSON/CSV 파일이 생성되면 해당 파일과 정상상태를 정의한 룰셋(JSON파일)과 비교한다. 탐지 항목은 다음과 같다.

- 노드목록 비교: 수집된 노드 리스트가 정상 룰셋과 정확히 일치하는지 확인하고, 삭제 노드 또는 미정의 신규 노드가 존재하면 이상으로 간주한다.

- XML-RPC 요청 분석: MethodCall에 한해서 MethodName과 파라미터 목록(예: 노드명, 토픽명, 서비스명 등)을 추출하여 MethodName 별로 룰셋에 정의된 정상 구조와 다를 경우 탐지한다.

이러한 설계는 실제 UGV의 ROS 1 기반 운영 환경에 부하를 거의 주지 않으며, JSON 기반 비교 구조는 디버깅과 재현에도 용이하다.

2.3 ROS 2 기반 탐지 모듈

ROS 2 기반 탐지 모듈 또한 수집기와 탐지기로 구성되며, ROS 2는 중앙 마스터가 없는 분산 구조로 CLI(Command-Line Interface) 기반으로 수집하고, 수집된 정보를 정제하여 JSON 파일로 저장한 뒤 탐지를 수행한다. 특히 R-UGV의 실험 환경에서는 동일한 노드명을 가진 중복 노드가 동시에 생성될 수 있는 특징이 있으며, 이는 공격자가 기존 노드를 대체하지 않고, 추가 노드를 생성하여 공격할 가능성이 있다. 따라서 ROS 2 기반 탐지에서는 노드별 발행/구독 구조 분석과 함께 동일 노드명의 수(Count)도 중요한 탐지 기준으로 활용된다.

• 수집기: 수집기는 CLI 명령어를 이용하여 분산된 시스템 상태 정보를 주기적으로 수집하고, 이를 정형화된 JSON 형태로 저장한다. 주요 수집 항목은 다음과 같다.

- ros2 node list: 현재 실행 중인 노드 목록을 수집하고 각 노드명을 기준으로 동일 노드명의 중복 개수를 계수한다.

- ros2 topic info /<topic>: 노드별 발행/구독 관계

를 구성하여 구조적 연결 정보를 생성한다.

수집기는 위 정보를 전처리하여 각 시간 시점에 존재하는 노드-토픽 관계, 중복 노드 여부 등을 포함한 JSON 파일로 저장하며, 탐지기가 이 파일을 기반으로 이상 여부를 판단할 수 있도록 한다.

• 탐지기: 탐지기는 지정된 폴더 내 JSON 파일을 감지하며, 새롭게 저장된 수집 결과를 정상상태 룰셋(JSON)과 비교하여 이상을 탐지한다. ROS 2의 분산 특성상, 마스터 기반의 직접적인 호출 감시(XML-RPC)가 불가능하다.

- 노드목록 비교: 수집된 노드명 목록이 정상 노드 목록에 포함되는지 여부 확인한다. 노드가 삭제되었거나 신규 노드명이 존재할 경우 이상으로 판단한다.

노드-토픽 발행/구독 구조 비교: 각 노드가 발행/구독으로 토픽 구조가 정상상태 룰셋과 일치하는지 확인한다. 특정 노드가 예상치 못한 토픽을 발행하거나 구독하는 경우 이상 탐지한다.

중복 노드 감시: 동일 노드명이 여러 인스턴스로 존재하는 경우, 허용된 최대 개수(보통 1)을 초과하면 이상으로 판단한다.

이와 같은 탐지 방식은 ROS 2 환경에 적합한 구조로, 공격자가 기존 노드명을 도용하여 중복된 발행/구독 노드를 생성하거나, 정상 노드가 공격에 의해 비정상적인 토픽을 추가로 발행/구독하도록 변경된 경우를 모두 탐지할 수 있도록 설계되었다.

2.4 룰셋 구성 및 비교 방식

본 논문에서 정의한 룰셋은 노드 목록 혹은 노드별 토픽 발행/구독 구조를 정적으로 정의한 규칙 정보이며, 이는 시스템의 정상상태를 기술하는 참조 역할을 한다. 그림 2는 자율주행 노드와 하드웨어 간 인터페이스로서 중요한 역할 수행하는 WmMotionControlerNode에 대한 정상 룰셋에 대한 예시로, 해당 노드의 발행(pub)/구독(sub) 노드 정보를 확인할 수 있다. 탐지기는 실제 수집된 노드의 토픽 발행/구독 목록과 참조 룰셋을 비교하여 불일치 여부를 점검하며, 불일치 시 이상 행위로 판단한다.

```
"ros2_rule": [
{
    "rule_type": "set",
    "rule_name": "NodePubSubValidation",
    "set": [
        {
            "node_name": [
                "/WmMotionControllerNode"
            ],
            "pub":[
                "/parameter_events",
                "/rtt_odom"
            ],
            "sub": [
                "/can/control_hardware",
                "/cmd_vel",
                "/control/mode"
                "/drive/can/emergency"
            ]
        },
```

그림 2. ROS 2 룰셋 샘플(JSON 형식)
Fig. 2. Sample JSON format of a ROS 2 rule

2.5 탐지 흐름도

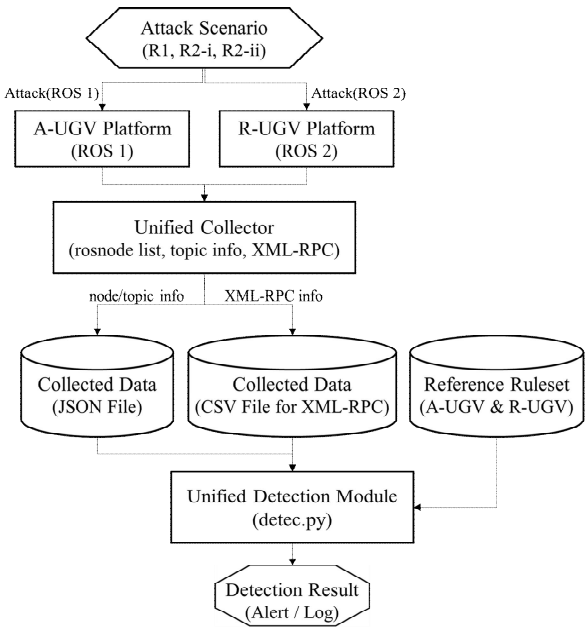

그림 3. 공격 시나리오 기반 탐지 흐름도
Fig. 3. Attack scenario-based detection flowchart

공격자는 UGV 내부네트워크에 접근하여 노드를 삽입하거나 토픽 발행/구독 구조를 변경한다. 수집기는 주기적으로 시스템 상태를 수집하여 JSON/CSV 형태로 저장하고, 탐지기는 해당 데이터를 사전 정의된 정상 룰셋과 비교하여 이상 여부를 판단하고 탐지 결과를 가시화 화면에 표시하고 관

련 로그를 DB(Database)에 저장한다(그림 3). 탐지기의 동작은 실시간성을 유지하기 위해서 JSON 비교 방식으로 경량화되었으며, 탐지 시에는 이상 노드명, 토픽명, 탐지 사유 등을 로그에 남긴다. 이 구조는 향후 디버깅에도 용이하다.

III. UGV 기반 실험 구성 및 공격 시나리오

3.1 실험 환경 및 장비 구성

본 논문은 실제 ROS 기반 UGV에 경량 탐지 모듈을 탑재하고, 실외 자율주행 미션을 수행하는 동안 공격 시나리오를 주입하여 탐지 효과를 검증하였다. 실험에는 두 종류의 UGV가 사용되었으며, 각각 ROS 1과 ROS 2 환경에서 동작한다.

A-UGV은 방산업체에서 개발한 ROS 1 기반 6륜 전기식 다목적 무인 지상 차량으로 보병 작전 지원을 위해 개발하였다. 그 외 군수품 운송, 부상자 후송, 감시/정찰, 근접 전투 지원 등 다양한 임무를 수행 가능하며 원격 조정과 자율주행 기능을 모두 갖추고 있다. R-UGV(Research-UGV)는 자체 개발한 플랫폼(그림 4)으로 차량 샤시 중량은 250kg(허용 중량 500kg)이고 플랫폼 컨트롤러(Nuc)의 CPU는 Phantom Canyon i7-1165G7이다. 또한 ROS 2 Foxy 기반으로 구성되었고 표 1과 같은 센서가 부착되어 있다. ROS 2는 DDS-Security 기반의 보안 기능을 지원하지만, R-UGV는 실시간성을 보장하고 한정된 연산 자원을 고려하여 평문 통신으로 구성하였다. 이는 성능 저하 없이 동작 하기 위함이며, 기존 연구에서도 ROS 2 보안 기능 활성화 시 성능 저하가 발생할 수 있음이 발표되었다[10]-[12].

R-UGV는 실외 환경에서 SLAM(Simultaneous Localization and Mapping)을 이용해 주행 지도를 생성하였고, 이후 생성된 지도상에 Waypoint를 지정하면 Global Path를 설정하였다. 자율주행 시에는 SLAM 기반 위치 추정과 실시간 센서 데이터를 이용하여 현재 위치를 추정하고, Local planner가 장애물을 회피하거나 최적의 Local path를 생성하는 방식으로 경로를 추종하였다[13].

그림 4. R-UGV 외형
Fig. 4. Physical R-UGV

표 1. R-UGV의 센서 스펙
Table 1. Sensor Spec. in R-UGV

Sensor	Spec.	Comm.
LiDAR (3D)	- Detection Range/Accuracy: 100m/3cm - Vertical FoV: 30° - Vertical Resolution: 2°(16채널) - Horizon FoV: 360° - Horizontal Resolution: 0.1°~0.4°	Ethernet
GPS	- Positioning Accuracy: 1.0cm (based on RTK) - Support Systems: GPS, GLONASS etc	Serial
IMU	- Gyroscope Speed Max (X-Axis, Y-Axis): ± 400°/s - Gyroscope Speed Max(Z-Axis): ± 300°/s	USB

각 UGV는 외부 통제기에서 무선으로 접속된 제어기와 연동되어 원격으로 관리되며, 탐지 모듈 또한 해당 통제기에서 실시간으로 실행된다. 탐지기는 NVDIA Jetson Orin 장비에서 동작한다(CPU: ARM Cortex A78AE v8.2 12 Core, GPU: Ampere with 2048 CUDA cores, 메모리:64GB). 그림 5는 R-UGV의 시스템 구성도이고 A-UGV도 이와 동일하다.

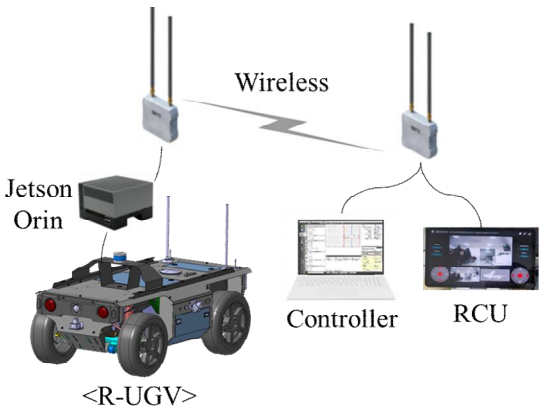

그림 5. R-UGV의 시스템 구성도
Fig. 5. System architecture of R-UGV

3.2 공격 시나리오 설계

본 논문은 공격자가 시스템 내부에 이미 침투하여 특정 수준의 권한을 확보한 상태로 임무 실패를 유도하기 위해서 ROS 메시지를 조작하는 방식으로 시스템을 교란하는 것을 가정한다. 정상 노드와 유사한 형태로 토픽을 발행하거나 구독 구조를 변경함으로써, 시스템은 외형상으로는 정상 동작하지만 실제 주행 판단에 오류를 유도할 수 있다. 이러한 형태의 공격은 물리적 이상 없이도 임무 실패나 정보 노출을 발생시킬 수 있어 실효성이 높으며, 시스템 운영자 입장에서 원인을 추적하기 어렵다는 특징이 있다. 이에 따라, 탐지 대상은 UGV 내부네트워크(In-vehicle network)상에서 발생하는 구조적 이상 행위에 한정한다.

ROS 1과 ROS 2의 구조적 차이를 고려하여 공격 시나리오를 각각 구성하였으며, 실험에서는 실제 노드 생성 및 토픽 발행이 가능한 범위 내에서 안전을 고려하여 실험하였다.

3.2.1 ROS 1 기반 공격 시나리오

- [R1] 신규 노드 생성 및 토픽 발행 공격:

공격자는 시스템에 존재하지 않는 신규 노드명을 사용하여 노드를 생성한 후, 정상 시스템에서 사용하는 것과 동일한 토픽명과 자료형에 맞춰 토픽을 발행하고 대신 Payload(실제 토픽 메시지)는 조작한다. 예를 들어 조향 방향을 반대로 변경하거나, LiDAR 센서값을 수정해 장애물이 있음에도 회피하지 못하게 만들거나, 장애물이 없음에도 비상 정지를 유도하는 등 임무 실패를 유도할 수 있다. 탐지 대상은 노드 목록과 XML-RPC 기반 등록 요청이며, 정상상태 룰셋에는 없는 노드 생성/해제 및 서비스 생성/종료를 탐지 기준으로 한다.

3.2.2 ROS 2 기반 공격 시나리오

- [R2-i] 신규/기존 노드 기반 토픽 발행 공격:

공격자는 기존 시스템에 존재하지 않은 신규 노드명 또는 이미 존재하는 정상 노드명과 동일한 이름으로 노드를 생성한 후, ROS 1과 동일하게 정상적인 토픽명과 자료형에 맞춰 공격 토픽을 발행한다[14]. 이는 토픽 발행/구독 구조가 정상상태와 달라지고, 동일 노드명의 인스턴스 수가 기준치를 초과하는 이상상태를 발생시킨다. 탐지기는 노드 목록과 토픽 구조 비교를 통해 이상을 판단한다.

- [R2-ii] 정상 노드 기반 조건부 비정상 동작:

공격자는 정상 노드의 소프트웨어를 변경하여, 특정 Signal이 입력되었을 때만 비정상적인 토픽을 구독하도록 구성할 수 있다. 예를 들어 GPS 토픽을 구독하지 않던 노드가 특정 Signal 수신 이후 /ublox/fix 토픽(GPS 값 포함)을 구독하게 되고, 이를 통해 특정 위치 정보를 내부에 저장하거나 외부로 유출할 수 있다.

Ⅳ. 실험 결과 및 분석

본 장에서는 제안한 경량 룰셋 기반 탐지 기법을 ROS 1과 ROS 2 기반 UGV 환경에 각각 적용하여 수행한 결과를 정리한다. 실험은 실제 자율주행 중 공격 시나리오에 따라 공격하고, 탐지기의 반응 여부와 시스템 자원 사용률, 탐지 시간 등을 측정하였다. 탐지 성공률과 시나리오별 대응 효과는 아래와 같으며, 시스템 성능 분석은 탐지기의 실시간 운용 가능성을 중심으로 평가하였다.

4.1 탐지 가능성 및 시나리오별 탐지 결과

탐지기는 각 공격 시나리오에 대해 룰셋과의 구조 비교를 통해 탐지 가능 여부를 평가하였다(표 2). ROS 1의 경우, 신규 노드가 삽입되면 rosnode list와 XML-RPC 요청 변화가 발생하여 명확한 탐지가 가능하였다. ROS 2의 경우, 노드 중복 생성과 토픽 발행/구독 구조 변경이 탐지 기준에 해당되므로, 공격 시도 시 룰셋 위반이 감지되었다. 특히 시나리오 R2-ii처럼 정상 노드의 내부 코드가 조건부로 변경된 경우에도 토픽 발행/구독 구조의 실시간 변경을 기반으로 이상 여부를 탐지할 수 있었다. 이러한 결과는 룰셋 기반의 구조적 명확성과 실시간 반응 가능성을 보여준다.

표 2. 공격 시나리오별 탐지 결과
Table 2. Detection result by attack scenario

ID	ROS ver.	Attack type	Items to be detected	Detect-ability
R1	ROS1	New node with topic pub	Node list, XML-RPC	Detectable
R2-i	ROS2	New or duplicated node with topic pub	Node list, Pub/sub relation, Duplicated node #	Detectable
R2-ii	ROS2	Abnormal behavior of a normal node under specific conditions	Pub/sub relation	Detectable

4.2 시스템의 성능 분석

탐지기는 실시간 자율주행 시스템에 부담을 주지 않아야 하므로, CPU 사용률(%), 메모리 점유율(RSS, %MEM), 탐지 처리 시간(s) 등의 시스템 성능 지표를 측정하였다. CPU 사용률은 탐지 모듈이 시스템 연산 자원을 얼마나 소모하는지를 나타내며, RSS(Resident Set Size)는 해당 프로세스가 실제 물리 메모리(RAM)에서 차지하는 용량(KB)를 의미한다. 반면 메모리 사용량(%)은 해당 프로세스가 차지한 물리 메모리(RSS)를 시스템 전체 메모리 용량과 비교하여 계산한 비율로, 전체 메모리 중 어느 정도를 해당 프로세스가 사용하고 있는지 나타낸다. 표 3은 ROS 1/2 환경에서 탐지 모듈 실행 시 측정된 평균 자원 사용률을 정리한 것이고 표 4는 평균 탐지 시간을 정리한 것이다. CPU/메모리 사용량은 pipstat를 이용해 측정하였고 공격 시나리오별로 1초 간격으로 1분 이상 개별적으로 사용량을 측정하여 평균값을 계산하였다. 탐지 시간 역시 공격에 대해서 JSON/CSV 파일 생성(수집) ~ 탐지까지 시간을 측정하였다.

본 실험을 통해 확인 한 결과, 표 3, 표 4와 같이 ROS 1 기반 탐지기는 XML-RPC 요청 분석 기능이 포함되어 있음에도 CPU 점유율이 평균 0.12% 이하이고, 메모리 사용량의 경우 13MB 미만으로 정상 트래픽 뿐 아니라 공격 트래픽 탐지 중에도 메모리 사용률은 0.04% 수준으로 경량성을 유지하였다. ROS 1-2의 명령이 기반 탐지 역시 유사한 실험 결과를 도출하였다. ROS 2 환경에서도 노드-토픽 구조 비교와 중복 노드 분석을 포함한 탐지기가 평균 1.4초 이내에 탐지를 완료하였다. 이는 본 탐지 기법이 실시간 운용 환경에서도 자율주행 성능에 영향을 주지 않고 병렬 실행 가능함을 보여준다.

표 3. 자원 사용
Table 3. Resource usage
(n: normal condition, a: abnormal condition)

Platform	CPU utilization (%)	RSS (KB)	Memory usage (%)
A-UGV (ros)	(n): 0.19 (a): 0.18~0.4	(n): 11,444 (a): 12,368~12,690	(n): 0.04 (a): 0.04
A-UGV (pcap)	(n): 0.06 (a): 0.07~0.12	(n): 11,284 (a): 11,284~12,260	(n): 0.04 (a): 0.04
R-UGV (ros)	(n): 0.07 (a): 0.11	(n): 11,084 (a): 11,084	(n): 0.04 (a): 0.04

표 4. 평균 탐지 시간
Table 4. Average detection time

Platform	Attack type	Average detection time (s)
A-UGV	Status info. spoofing	1.23
A-UGV	Sensor data spoofing	1.12
R-UGV	Status info. spoofing	1.4
R-UGV	Sensor data spoofing	0.6

V. 결론 및 향후 과제

본 논문에서는 ROS 기반 UGV 환경에서 실시간으로 적용 가능한 경량 룰셋 기반 탐지 기법을 제안하고, 실제 ROS 1 및 ROS 2 기반의 두 플랫폼에 적용하여 실험을 수행하였다. 제안 기법은 학습이나 통계 기반의 복잡한 탐지 모델 없이, 사전 정의된 정상 구조를 룰셋과의 비교만으로 이상 여부를 판단하며, 시스템 자원 사용을 최소화하면서도 실시간 탐지가 가능한 구조를 갖는다. 실험 결과, 제안된 탐지기는 노드 삽입, 토픽 발행/구독 구조 변경 등 다양한 공격 시나리오에 대해 효과적으로 대응하였으며, 탐지 시간(1초 내외)과 자원 점유율(CPU 0.4%

이하) 측면에서도 실시간 운용에 어려움이 없음을 확인하였다. 특히 ROS 1과 ROS 2의 구조적 차이를 반영한 탐지 방식을 통해, 다양한 ROS 기반 시스템에서도 확장 가능성을 갖는 경량 보안 솔루션으로 활용될 수 있음을 확인하였다.

향후 연구에서는 제안된 경량 룰셋 기반 탐지 기법의 확장성을 더욱 강화하기 위해, 다양한 공격 시나리오에 대한 자동 대응 체계를 마련하는 것이 필요하다. 장기적으로 자율주행 UGV 뿐만 아니라 다양한 ROS 기반 사이버-물리 시스템에 적용할 수 있는 보안 솔루션으로 발전 할 수 있을 것이다.

References

[1] M. Salah, Q. F. Al-Doori, A. T. Abdullah, and A. A. Abdallah, "Security Vulnerabilities and Threats in Robotic Systems: A Comprehensive Review", International Journal of Safety and Security Engineering, Vol. 13, No. 3, pp. 555-563, Jun. 2023. https://doi.org/10.18280/ijsse.130318.

[2] B. Dieber, B. Breiling, S. Taurer, and S. Kacianka, "Security for the robot operating system", Robotics and Autonomous Systems, Vol. 98, pp. 192-203, Dec. 2017. https://doi.org/10.1016/j.robot.2017.09.017.

[3] A. Botta, S. Rotbei, S. Zinno, and G. Ventre, "Cyber Security of Robots: a Comprehensive Survey", Intelligent Systems with Applications, Vol. 18, May 2023. https://doi.org/10.1016/j.iswa.2023.200237.

[4] S. Johnson, A. Borah, A. Paranjothi, and J. P. Thomas, "ROS-Lighthouse: An Intrusion Detection System (IDS) in ROS using Ensemble Learning", International Symposium on Wireless Personal Multimedia Communications, pp. 1-6, Nov. 2024. https://doi.org/10.1109/WPMC63271.2024.10863805.

[5] E. Değirmenci, Y. S. Kirca, İ. Özçelik, and A. Yazıcıı, "ROSIDS23: Network intrusion detection dataset for robot operating system", Data in Brief, Vol. 51, pp. 1-12, Dec. 2023. https://doi.org/10.1016/j.dib.2023.109739.

[6] A. Hussain, E. M. Tordera, X. Masip-Bruin, and H. C. Leligou, "Rule-Based With Machine Learning IDS for DDoS Attack Detection in Cyber-Physical Production Systems", IEEE access, Vol. 12, pp. 114894-114911, Aug. 2024. https://doi.org/10.1109/ACCESS.2024.3445261.

[7] T. Kim, "Security Evaluation of ROS-based Robotic Systems", Proc. of ACM CCS Workshop on Cyber-Physical Systems Security and Privacy (CPSS), 2017.

[8] D. Portugal, R. P. Rocha, and J. P. Castilho, "Inquiring the robot operating system community on the state of adoption of the ROS 2 robotics middleware", International Journal of Intelligent Robotics and Applications, Vol. 9, No. 1, pp. 454-479, Oct. 2024. https://doi.org/10.1007/s41315-024-00393-4.

[9] Open Robotics, "ROS 2 Design Overview", https://design.ros2.org/ [accessed, Apr. 2025]

[10] J. Kim, J. M. Smereka, C. Cheung, S. Nepal, and M. Grobler, "Security and Performance Considerations in ROS 2: A Balancing Act", arXiv preprint arXiv:1809.09566, Sep. 2018. https://doi.org/10.48550/arXiv.1809.09566.

[11] H. Lee, H. Lee, S. Heo, M. Park, and C. Yoo, "Experimental Analysis of ROS2 DDS Middleware's Communication Overhead", Journal of KIIT, Vol. 22, No. 2, pp. 93-100, Feb. 2024. https://doi.org/10.14801/jkiit.2024.22.2.93.

[12] Y. Maruyama, S. Kato, and T. Azumi, "Exploring the Performance of ROS2", Proc. of the 13th International Conference on Embedded Software, New York, United States, No. 5, pp. 1-10, Oct. 2016. https://doi.org/10.1145/2968478.2968502.

[13] A. Filotheou, E. Tsardoulias, and A. Dimitriou, A. Symeonidis, and L. Petrou, "Quantitative and Qualitative Evaluation of ROS-Enabled Local and Gloabal Planners in 2D static Environments", Journal of Intelligent & Robotic Systems, Vol. 98, No. 3-4, pp. 567-601, Oct. 2019. https://doi.org/

10.1007/s10846-019-01086-y.

[14] Y. Patel, P. H. Rughani, and D. Desai, "Analyzing Security Vulnerability and Forensic Investgation of ROS2: A Case Study", Proc. of the 8th International Conference on Robotics and Artificial Intelligence, Singapore, pp. 6-12, Nov. 2022. https://doi.org/10.1145/3573910.3573912.

저자소개

이 화 성 (Hwaseong Lee)

2006년 2월 : 고려대학교 정보보호학과(공학석사)
2013년 2월 : 고려대학교 정보보호학과(공학박사)
2013년 9월 ~ 현재 : 국방과학연구소 책임연구원
관심분야 : MUM-T 보안

정 영 기 (Youngki Jung)

2014년 2월 : 서울과학기술대학교 컴퓨터공학과(공학사)
2024년 2월 : 고려대학교 정보보호학과(공학석사)
2024년 3월 ~ 현재 : 국방과학연구소 연구원
관심분야 : 침입탐지 및 대응

허 선 동 (Seondong Heo)

2011년 2월 : 한국과학기술원 전산학과(공학석사)
2017년 2월 : 한국과학기술원 전산학과(공학박사)
2017년 2월 ~ 현재 : 국방과학연구소 선임연구원
관심분야 : 침입탐지 및 대응

박 무 성 (Moosung Park)

1990년 2월 : 서강대학교 전자계산학과(전자계산석사)
2023년 2월 : 세종대학교 컴퓨터공학과(공학박사)
1990년 1월 ~ 현재 : 국방과학연구소 수석연구원
관심분야 : 사이버보안, 사이버훈련, IoT 보안, Robot 보안

유 찬 곤 (Changon Yoo)

1997년 2월 : 충남대학교 전산학과(이학사)
2003년 8월 : South Dakata State University Computer Science(공학석사)
2003년 8월 ~ 현재 : 국방과학연구소 책임연구원
관심분야 : MUM-T 보안