CAMEO: ROS 2 Callback 단위 보안을 위한 중재 및 집행 오버레이

최윤서*, 이승수**

*,**인천대학교 (학부생, 교수)

CAMEO: Callback-Aware Mediation and Enforcement Overlay

Yunseo Choi*, Seungsoo Lee**

*,**Incheon National University(Undergraduate student, Professor)

요 약

ROS 2는 분산 로봇 시스템의 핵심 통신 미들웨어이며, SROS2는 DDS Security 기반의 Participant 및 Topic 단위 접근제어를 제공한다. 그러나 동일 Node의 Callback은 독립적인 권한 단위로 구분되지 않아, 특정 Topic 권한을 실제로 사용한 Callback을 식별하기 어렵다. 이러한 한계를 해결하기 위해 본 논문은 DDS Sample을 원본 Callback에 귀속시키고 Cross-Domain 전달 과정에서 Callback 단위 최소 권한을 집행하는 CAMEO를 제안한다. CAMEO는 Callback-Topic Allowlist 생성, 런타임 provenance 기반 권한 판정, 보호 Domain 직접 우회 차단을 결합하여 Callback별 전달 권한을 제어한다. TurtleBot3 기반 평가에서 CAMEO는 정상 발행을 유지하면서 비인가 발행과 직접 우회를 차단하였으며, 생성된 Allowlist는 Ground Truth와 일치하였다. 또한 Secure DDS Router 대비 median latency와 평균 CPU 사용량이 각각 38.3%와 37.4% 낮음을 확인하였다.

I. Introduction

Robot Operating System 2(ROS 2)는 연구용 로봇을 넘어 자율주행, 물류, 서비스 로봇 등 다양한 실제 로봇 시스템에 활용되는 대표적인 로봇 소프트웨어 플랫폼이다[1]. ROS 2에서는 분산된 소프트웨어 구성요소가 메시지를 통해 센싱, 인지, 계획, 제어 기능을 연계하며, 일부 메시지는 로봇의 물리적 동작을 직접 결정한다. 따라서 침해된 구성요소의 비인가 메시지 생성과 전달을 제한하는 것은 ROS 2 시스템의 보안과 안전을 위해 필수적이다.

ROS 2의 기존 보안 체계인 Secure ROS 2 (SROS2)는 Data Distribution Service(DDS) Security를 기반으로 Participant 인증과 Topic 단위 접근제어를 제공한다. 그러나 동일 Node의 Callback은 독립적인 권한 단위로 구분되지 않아 security identity와 Topic 권한을 공유하며, 특정 Topic 발행의 원본 Callback을 식별하기 어렵다. 정적 분석 기반의 기존 ROS 2 보안 정책 생성 연구도 런타임 DDS Sample의 원본 Callback을 식별하지 않아 Callback 단위 권한을 집행하지 못한다. 이러한 한계로 인해 변조된 Callback은 다른 Callback에 허용된 발행 권한을 이용할 수 있을 뿐 아니라, 보호 Domain으로 비인가 명령이 전달될 수 있다.

이를 해결하기 위해 본 논문에서는 DDS Sample의 원본 Callback을 식별하고 Callback별 최소 권한에 따라 Cross-Domain 전달을 제어하는 CAMEO를 제안한다. CAMEO는 정상 프로그램의 Callback-Topic 관계로 최소 권한 Allowlist를 생성하고, 비동기 DDS 송신에서 Sample의 출처를 추적하여 전달 권한을 판정하며, 비신뢰 프로세스의 보호 Domain 직접 송신을 차단한다. 평가에서 CAMEO는 정상 Sample을 모두 허용하고 공격 Sample과 직접 우회 전송을 모두 차단하였으며, Secure DDS Router 대비 median latency와 평균 CPU 사용량이 각각 38.3%와 37.4% 감소하였다.

본 논문의 주요 기여는 다음과 같다.

- DDS 비동기 송신에서 Sample과 원본 Callback의 provenance를 유지하여 Cross-Domain 권한을 집행하는 Callback-Aware Authorization을 제안한다.
- 정상 ROS 2 프로그램의 Callback-Topic 관계를 기반으로 Callback별 최소 권한 Allowlist 생성 방법을 제안한다.
- 보호 Domain 직접 송신을 차단하여 정책 집행 경로의 우회를 제한하는 Bypass-Resistant Mediation을 제안한다.

II. Background

2.1 ROS 2와 DDS 통신

ROS 2는 Node 내부의 Subscription Callback과 Publisher를 통해 Topic 기반 통신을 수행하며, Robot Middleware(RMW) 계층을 통해 이를 DDS 통신으로 변환한다. Callback에서 Publisher를 통해 발행된 데이터는 DDS DataWriter의 Sample로 등록되므로, 발행 경로는 Callback → Publisher → DDS DataWriter → DDS Sample로 구성된다. DDS는 Domain을 기준으로 통신 참여자를 구분하며, 서로 다른 Domain 간 메시지 전달에는 두 Domain을 연결하는 Router 또는 Relay를 사용할 수 있다.

또한, ROS 2는 RMW 계층을 통해 다양한 DDS 구현체를 지원하며, Fast DDS는 ROS 2에서 널리 사용되는 DDS 구현체 중 하나이다. 본 연구는 Fast DDS의 비동기 발행 경로를 대상으로 하며, 이 경우 Callback을 실행하는 Executor Thread와 실제 네트워크 송신을 수행하는 DDS Sender Thread가 분리될 수 있다. 따라서 DataWriter에 등록된 Sample은 이후 별도의 Sender Thread에서 송신될 수 있으며, Sample 생성과 네트워크 송신이 서로 다른 실행 문맥에서 수행될 수 있다.

2.2 SROS2와 DDS 보안

ROS 2는 DDS 통신에 보안 기능을 적용하기 위해 DDS Security 기반의 SROS2를 지원한다. SROS2에서는 ROS 2 Enclave에 DDS security identity와 permissions를 부여하고, 이를 기반으로 Participant 인증과 Topic 단위 publish/subscribe 접근제어를 수행한다. 따라서 publish/subscribe 권한은 DDS Participant의 security identity와 대상 Topic을 기준으로 정의되며, 동일 Node 내부의 Callback은 동일한 Node 수준의 보안 컨텍스트를 공유한다.

III. Problem Statements

3.1 Cross-Domain 통신에서의 Callback 단위 권한 집행 부재

동일 Node 내부의 여러 Callback은 하나의 security identity와 Topic 권한을 공유하므로, 기존 Node/DDS Participant 수준의 권한 정보만으로는 DDS Sample을 생성한 Callback을 구분할 수 없다. 이에 따라 특정 Callback이 동일 Node에 허용된 Publisher 또는 Topic 권한을 사용하더라도 기존 권한 모델에서는 이를 정상 발행과 구별하기 어렵다. Fig. 1과 같이, 정상적으로 /diagnostics만 발행하는 Callback A가 변조되어 /cmd_vel을 발행하더라도, 해당

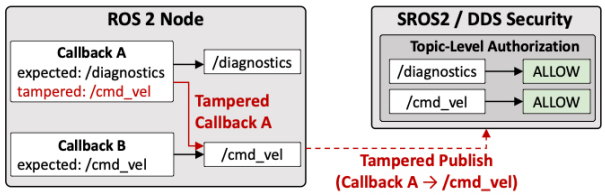


Fig. 1. Callback-Level Authorization Gap under Topic-Level Access Control

Topic이 동일 Node에 허용되어 있다면 SROS 2/DDS Security는 이를 Callback B의 정상 발행과 구분할 수 없다. 이러한 한계는 Cross-Domain 통신에서도 동일하게 나타나며, 보호 Domain으로 전달되는 Sample의 원본 Callback을 식별할 수 없는 경우 중재자는 Callback별 발행 권한을 구분하여 집행할 수 없다.

3.2 Callback 단위 최소 권한 정책의 부재

기존 연구에서는 정적 분석을 통해 ROS 2 프로그램의 통신 관계를 분석하고 보안 정책을 자동 생성하는 방법이 제안되었다. 그러나 이러한 방법은 Node와 Topic 수준의 통신 관계를 기반으로 정책을 생성하며, Node 내부의 개별 Callback이 사용하는 출력 Topic까지 구분하지 않는다. 따라서 기존 정책 생성 방식으로는 Callback별 실제 발행 관계를 반영한 세분화된 최소 권한 정책을 생성할 수 없다.

3.3 보호 Domain 중재 경로의 우회

Callback 단위 정책을 Trusted Mediator에서 집행하더라도, 비신뢰 프로세스가 Mediator를 거치지 않고 보호 Domain으로 직접 DDS 송신을 수행할 수 있다면 해당 정책 집행 경로는 우회될 수 있다. 이 경우 Mediator의 Callback 단위 권한 판정과 관계없이 Sample이 보호 Domain으로 전달될 수 있다.

IV. System Design

4.1 위협 모델 및 범위

CAMEO는 배포 후 ROS 2 Node의 Application Logic이 변조되어, 공격자가 동일 Node에 허용된 Publisher를 비인가 Callback에서 사용하거나 Trusted Mediator를 우회해 보호 Domain으로 직접 송신할 수 있다고 가정한다. 반면 공격자는 root 권한을 갖지 않으면, 정책 생성에 사용된 정상 소스 코드와 정책, CAMEO 구성 요소, Kernel과 extended Berkeley Packet Filter(eBPF) 프로그램 및 map, ROS 2/Fast DDS Runtime은 신뢰한다. 구현 및 평가는 Fast DDS의 UDP 통신 경로를 대상으로 한다.

4.2 전체 구조 및 동작 흐름

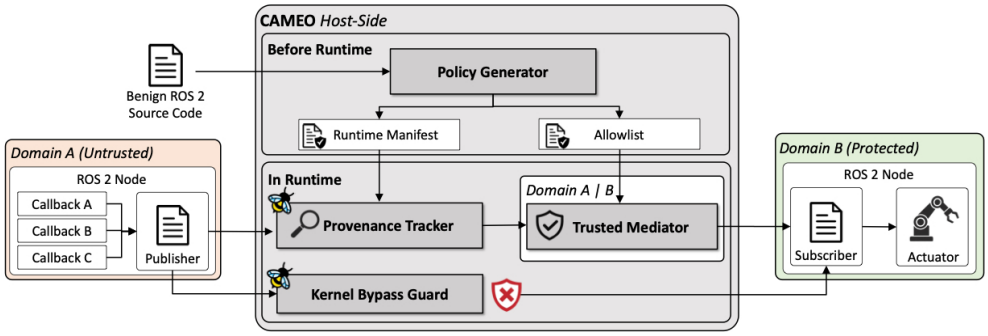


Fig. 2. CAMEO Overall Architecture

Fig. 2와 같이 CAMEO는 Policy Generator, Provenance Tracker, Trusted Mediator 및 Kernel Bypass Guard로 구성된다. Policy Generator는 소스 코드에서 Runtime Manifest와 Callback-Topic Allolist를 생성한다. 런타임에는 Tracker가 DDS Sample의 원본 Callback을 추적하고, Mediator가 Allolist를 적용하며, Guard가 Domain B 직접 송신을 차단한다.

4.3 Callback 단위 권한 집행

§3.1의 Callback 단위 권한 집행 문제를 해결하기 위해 CAMEO는 eBPF uprobe 기반 Provenance Tracker로 DDS Sample과 원본 Callback을 연결한다. Manifest의 Callback 식별자(CID)를 런타임 Callback에 바인딩하고, Callback의 진입과 반환 시 Thread별 실행 문맥을 설정·삭제하여 동시 실행되는 Callback을 구분한다.

Fast DDS의 비동기 발행에서는 Callback을 실행하는 Executor Thread와 실제 송신을 수행하는 Sender Thread가 분리되므로, 송신 시점의 Thread 정보만으로 원본 Callback을 식별할 수 없다. 이에 Tracker는 자기 보고 값이 아닌, Callback 실행 경로와 DDS Writer 경로에서 관찰한 이벤트를 결합하여 Sample 식별자(Writer GUID, Sequence Number)를 (CID, TopicID)와 연결한 provenace를 생성한다. Fig. 3에서 C1이 T2의 Sample을 생성하면 (W1, 42) → (C1, T2)가 기록되며, Sender Thread가 달라져도 Sample 식별자를 통해 provenance를 추적할 수 있다.

Trusted Mediator는 Sample 식별자로 provenance를 조회한 뒤 즉시 삭제하여 재사용을 방지한다. 이후 복원된 (CID, TopicID)가 Allowlist에 존재할 때만 Sample을 Domain B로 재발행한다. Fig. 3의 (C1, T2)는 C1에 허용된 관계이므로 전달되며, 비허용 관계나 provenance를 확인할 수 없는 Sample은 fail-closed로 차단한다.

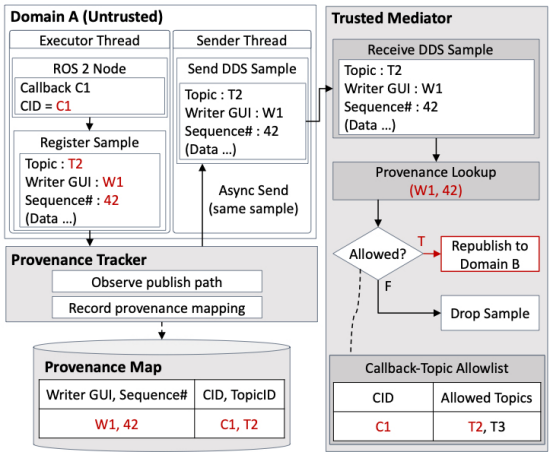


Fig. 3. Callback Provenance Authorization Flow

4.4 Callback 단위 최소 권한 정책 생성

§3.2의 Callback 단위 정책 생성 문제를 해결하기 위해 Policy Generator는 Clang Abstract Syntax Tree(AST) 기반 정적 분석으로 정상 ROS 2 프로그램의 Callback-Topic 관계를 추출하여 Runtime Manifest와 Allowlist를 생성한다. Allowlist에는 정상 소스 코드에서 확인된 관계만 포함되어 각 Callback에는 실제 발행에 필요한 Topic 권한만 부여된다.

4.5 보호 Domain 직접 송신 우회 차단

§3.3의 중재 경로 우회 문제를 해결하기 위해 CAMEO는 eBPF Linux Security Modules (LSM) 기반 Kernel Bypass Guard를 사용한다. Guard는 socket_sendmsg에서 Trusted Mediator의 정상 송신은 허용하고, 등록된 비신뢰 프로세스의 보호 Domain 대상 IPv4 UDP 직접 송신은 차단한다. 이를 통해 지원되는 Fast DDS/UDP 경로에서 중재 경로의 우회를 제한한다. TCP, IPv6 및 Shared Memory Transport는 현재 범위에서 제외한다.

V. Evaluation

5.1 평가 환경 및 방법

평가는 Fig. 4(A)에 제시한 Raspberry Pi 4

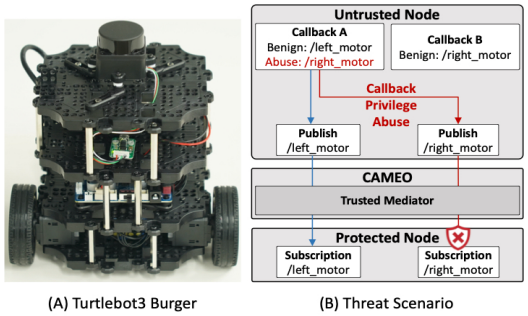


Fig. 4. Evaluation Enviroment

>_ Benign Action	>_ Tampered Action
[Node] Callback A publish /left_motor	[Node] Callback A publish /right_motor
[MEDIATOR] CID=1, TID=/left_motor	[MEDIATOR] CID=1, TID=/right_motor
[MEDIATOR] allowlist match -> ALLOW	[MEDIATOR] allowlist miss -> DENY
[RESULT] authorized action delivered	[RESULT] unauthorized callback use blocked

Fig. 5. Enforcement Results

기반 TurtleBot3 Burger 모델에서 ROS 2 Jazzy와 Fast DDS 2.14.6을 사용하여 수행하였다. 실험 환경은 비신뢰 작업 영역인 Domain A와 보호 영역인 Domain B로 구성하였다. 동일 환경에서 권한 집행·악용, 직접 우회 및 정책 생성을 검증하고 지연 시간, CPU, 부하 및 장시간 안정성을 측정하였다.

5.2 보안 효과 검증

Callback 단위 권한 집행·권한 악용 차단. security identity와 Topic 권한을 공유하는 동일 Node의 Callback을 대상으로 CAMEO와 SROS2를 비교하였다. Fig. 4(B)와 같이 Callback A가 Callback B의 /right_motor 권한을 사용하는 시나리오에서, Fig. 5와 같이 CAMEO는 정상 동작을 유지하면서 비인가 명령을 모두 차단하였다. 또한 Callback 오귀속은 발생하지 않았으며 provenance를 확인할 수 없는 Sample도 fail-closed로 차단하였다. 반면 SROS2에서는 동일 Node에 허용된 Topic 권한을 이용한 비인가 발행이 모두 전달되어 Callback별 권한을 구분하지 못하였다.

중재 경로 우회 차단. Trusted Mediator를 통한 정상 전달과 비신뢰 프로세스의 보호 Domain 직접 송신을 각각 수행하여 Kernel Bypass Guard의 우회 차단 효과를 검증하였다. 그 결과 Guard는 정상 전달을 유지하면서 Domain B로의 직접 송신을 모두 차단하였다. 이를 통해 Callback 단위 권한 판정과 별개로 발생할 수 있는 중재 경로의 직접 우회를 제한할 수 있음을 확인하였다.

최소 권한 정책 생성. 정상 소스 코드를 수동 분석하여 각 Callback에 필요한 출력 Topic 관계를 Ground Truth로 구성하고, 이를 Policy Generator가 생성한 Callback-Topic Allowlist와 비교하였다. 두 평가 프로그램에서 30회 반복한 결과, 생성된 Allowlist는 누락 및 추가 관계 없이 Ground Truth와 모두 일치하였으며, 정상 프로그램에 존재하지 않는 관계도 포함되지 않았다. 이를 통해 평가 범위에서 정상 동작에 필요한 권한만을 포함하는 Callback 단위 정책이 정확하게 생성됨을 확인하였다.

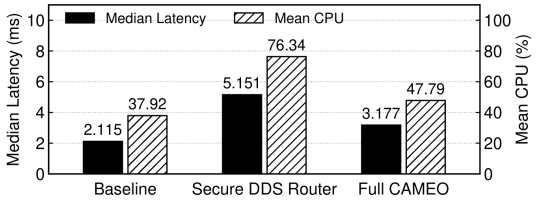


Fig. 6. Cross-Domain Performance Comparison

5.3 Cross-Domain 성능 및 안정성

성능 평가에서는 동일한 Cross-Domain topology에서 최소 relay인 Baseline, DDS Security 기반 Secure DDS Router, Full CAMEO를 비교하였다. Fig. 6과 같이 CAMEO는 Baseline 대비 median latency와 평균 CPU 사용량이 각각 50.2%, 26.0% 증가한 반면, Secure DDS Router 대비 각각 38.3%, 37.4% 감소하였다. 10-200 Hz에서도 정상 전달과 차단을 유지했고, 100 Hz에서 1시간 동안 360K개 Sample을 처리해 중단 없이 99.929%의 종단 간 전달률을 기록하였다. 결과적으로 CAMEO의 추가 권한 집행 비용에도 불구하고 Secure DDS Router보다 낮은 지연시간과 CPU 사용량으로 Cross-Domain 권한 집행을 유지함을 보여준다.

VI. Conclusion

본 논문은 DDS Sample의 원본 Callback을 추적하여 Cross-Domain 환경에서 Callback별 권한을 집행하는 CAMEO를 제안하였다. CAMEO는 Callback-Topic 최소 권한 정책, provenance 기반 판정 및 Kernel Bypass Guard를 결합하여 권한 악용과 중재 경로 우회를 제한한다. 향후에는 다양한 ROS 2/DDS 버전과 전송 방식으로 적용 범위를 확장할 예정이다.

ACKNOWLEDGEMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. RS-2025-16069415).

[참고문헌]

[1] Macenski, S., Foote, T., Gerkey, B., Lalancette, C., & Woodall, W. (2022). Robot operating system 2: Design, architecture, and uses in the wild. Science robotics, 7(66), eabm6074.