선박용 복합통신 게이트웨이의 Non-IP 디바이스 연동방안에 관한 연구

구형서, 한병욱, 김민준, 유대승*
주식회사 한컴유비마이크로, *한국전자통신연구원
{control, bwhan, mjkim1}@hancomum.com, *ooseyds@etri.re.kr

A Study on Integration Methods for Non-IP Devices in a Shipboard Multi-Communication Gateways

Koo Hyeong Seo, Han Byoung Wook, Kim Min Jun, Yoo Dae Seung*
HancomUbimicro Co., Ltd, *ETRI

요 약

본 연구는 선박용 복합통신 게이트웨이가 기존의 ModbusRTU, NMEA 등 유선기반 통신뿐 아니라, Bluetooth, Zigbee, VHF, LoRa 등 무선기반 통신을 포함한 이종 Non-IP 디바이스를 IP기반 시스템에 통합 시 직면하는 연결복잡도 증가, 데이터 비표준화, 디바이스 상태 관리의 어려움 등의 문제점을 해결하기 위한 다양한 연결 모델을 검토한다.

기존의 연결 모델은 게이트웨이가 Non-IP 디바이스를 직접 연결하였기에 높은 결합도와 비효율성을 초래한다. 이를 해소하기 위해 본 논문은 대리자(Agent) 연결 모델을 제안한다. 이 모델은 Agent 내부의 추상화 계층이 Non-IP 디바이스의 연결, 데이터 송수신, 프로토콜처리, 상태 관리 등을 전담한다. 이는 디바이스별 프로토콜 복잡성으로 인한 관리 오버헤드, 데이터 비표준화로 인한 데이터 처리의 비효율성, 높은 결합도로 인한 의한 비유연성, 각 디바이스의 상태관리의 어려움, 데이터 보안 관리의 취약점을 개선하는 방안이 될 수 있다. 이로써 복합통신 게이트웨이는 연결의 복잡성과 비표준화로부터 해방되며 이기종 디바이스의 연결성과 디바이스의 상태관리의 편의성이 확보된다.

Ⅰ. 서 론

1. 연구 배경 및 필요성

ModbusRTU, NMEA와 같은 유선기반 프로토콜과 Bluetooth, Zigbee, VHF, LoRa와 같은 무선기반 기술을 포함하는 Non-IP 디바이스들은 선박과 같은 개별적이고 폐쇄된 환경에서 이미 오랜 기간 운용되어 왔다. 최근 중앙 집중식 데이터 수집, 원격 모니터링, 통합제어 시스템 구축의 사례가 늘어나면서, 기존의 Non-IP 디바이스들도 IP 시스템에 연결되어 통합관리하기 위한 요구가 증대되고 있다. 이에 따라 복합통신 게이트웨이가 이종 통신환경을 통합하고 표준화하는 핵심 매개체로서 그 역할이 자리매김하는 추세이다.

특히 선박환경에서 복합통신 게이트웨이는 항통 장비, 기관실 제어장비, 안전환경 센서 등 다양한 종류의 데이터 통합을 담당한다. 따라서 복합통신 게이트웨이는 Non-IP 디바이스들의 연결 및 관리에 대한 편의성을 높이고, 유지보수 비용을 절감하는 등 유연성과 안정성뿐만 아니라, 국제표준 준수와 보안 신뢰성 등을 확보하는 것이 필수적이다.

2. 문제 제기 및 연구 목표

기존 복합통신 게이트웨이가 Non-IP 디바이스와 연결하는 방식은 게이트웨이의 운영체제(OS)나 핵심 프레임워크가 통신연결 및 프로토콜 처리를 직접 관리하는 방식이다. 이러한 직접 관리 방식은 다음과 같은 몇 가지 문제를 초래하며, 복합통신 게이트웨이의 기술적 및 운영적 한계를 유발한다.

- *프로토콜 복잡성 및 관리부담* : 복합통신 게이트웨이는 이종 Non-IP 디바이스와 연결하기 위해 다양한 프로토콜 스택(Modbus, NMEA, BLE 등)을 내부에 유지해야 하며, 이는 소프트웨어의 복잡도와 관리의 부담을 기하급수적으로 증가시킴.
- *데이터 비표준화 문제* : Non-IP 디바이스별로 상이한 데이터 포맷(Raw Bytes, ASCII, Big/Little-Endian 등)이 게이트웨이 코어로 직접 유입되어, 데이터 처리 및 정규화 작업이 비효율적임.
- *높은 결합도와 비유연성* : 새로운 통신 기술이 등장하거나 디바이스가 추가될 때마다 복합통신 게이트웨이의 메인 프레임워크를 수정하고 재배포해야 함.
- *디바이스 상태 관리의 어려움* : 수백 대의 Non-IP 디바이스에 대한 실시간 연결 상태, 헬스 체크, 오류 감지 등을 게이트웨이가 직접 비동기적으로 관리하는데 부하가 큼.
- *보안 취약점 확산 위험* : 자체 보안이 없는 Non-IP 프로토콜 인터페이스가 게이트웨이의 핵심 시스템과 직접 연결되어 잠재적인 보안 취약점이 IP 네트워크 전체로 확산될 위험이 큼.

본 연구는 이러한 직접 연결 방식의 한계를 극복하고, 다양한 Non-IP 디바이스에 대해 높은 확장성, 유연성 및 보안성을 제공할 수 있는 최적화된 통신 구조를 분석하고 제안하는 것을 목표로 한다. 이를 위해 대리자(Agent) 기반 모델을 중심으로 연구를 진행한다.

Ⅱ. 본론

1. 선박환경에서 운용 중인 Non-IP 디바이스들

복합통신 게이트웨이가 처리해야 하는 Non-IP 디바이스의 유형은 물리 계층부터 통신 방식까지 광범위하게 다양하다. 특히 선박에서는 안정적인 관리와 제어를 위해 유선통신과 IoT 무선통신이 복합적으로 존재한다.

<표 1> 선박 환경의 Non-IP 디바이스

통신방식 / 프로토콜	주요 특징
ModbusRTU	▪ RS-485 Modbus호환성 ▪ PLC제어, 센서모니터링, 보안 취약
NMEA	▪ 항통 장비(레이더, 해도, GPS) ▪ 정형화된 데이터 메시지
Bluetooth (BT/BLE)	▪ 근접 환경 및 개인 장치 ▪ 비인가 접속 위험
LoRa, LoRaWAN	▪ 장거리, 저대역폭 ▪ 화물 추적, 환경 모니터링, 원격 제어
VHF	▪ GMDSS, AIS ▪ 가시거리통신, 해상교통관제

이러한 이종 디바이스들을 효과적으로 통합하고 중앙 집중식으로 관리하기 위해서는 다음과 같은 세 가지 주요 기술적 처리가 필수적으로 요구되며, 이는 복합통신 게이트웨이 설계의 핵심 과제이다.

- *프로토콜 변환 (Protocol Translation)* : 유선기반의 Modbus, NMEA 및 무선기반의 BLE, LoRa 등 다양한 전송계층(Transmit Layer) 및 네트워크 계층(Network Layer) 프로토콜을 공통의 IP 기반 프로토콜(예: CoAP, MQTT)로 매핑하는 과정. 이종 프로토콜의 특성과 구조(예: 동기/비동기, 마스터/슬레이브)를 이해하고 이를 IP 통신 환경에 맞게 상호변환하는 복잡한 로직이 요구됨.
- *데이터 포맷 정규화 (Data Format Normalization)* : Non-IP 디바이스에서 수집된 원시데이터(Raw Data)는 Binary, ASCII 문자열, 고정 길이필드 등 비표준화된 다양한 형태로 존재함. 이처럼 이질적인 데이터를 상위시스템이 이해할 수 있도록 JSON, XML과 같은 표준화된 구조와 데이터 타입으로 변환하고 정제하는 과정이 요구됨.
- *연결 상태 관리 (Connection State Management)* : 수백 대에 이르는 Non-IP 디바이스들의 실시간 연결 상태와 가용성을 안정적으로 모니터링해야 함. 특히 배터리 기반의 무선 디바이스나 불안정한 유선 연결의 경우, 주기적인 헬스체크(Health Check), 타임아웃 감지, 오류 감지 및 재연결 로직 등 고신뢰성 상태 관리 메커니즘이 요구됨.

2.Non-IP디바이스연결방식연구

2.1직접관리모델

직접관리 모델은 Non-IP 드라이버나 프로토콜 스택을 게이트웨이의 OS 커널 영역에 직접 구현하는 방식이다.

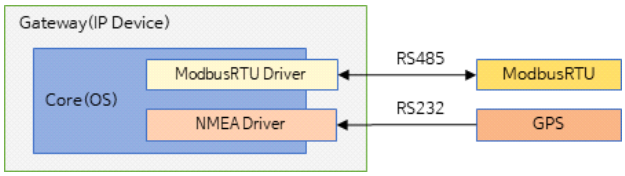

그림 1 직접 관리 모델

- *장점* : 데이터 처리 지연 시간이 짧고(Low Latency) 효율적임.
- *단점* : 결합도(Coupling)가 매우 높고, 새로운 디바이스 타입 추가 시 게이트웨이의 시스템을 재컴파일 및 풀테스트를 수행해야 하며, 보안 취약점 발생 시 시스템 전체로 확산될 위험이 큼.

2,2 대리자(Agent) 기반 모델

대리자 기반 모델은 복합통신 게이트웨이와 Non-IP 디바이스 사이에 독립적인 중개SW(Agent)를 배치하는 방식이다. 이 Agent는 Non-IP 디바이스의 프로토콜을 처리한 후, IP 기반 프로토콜(예: MQTT, CoAP)로 변환하여 복합통신 게이트웨이 메인에 전달한다.

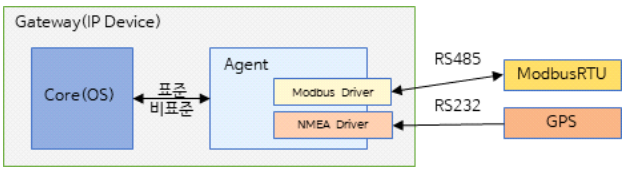

그림 2 Agent 모델

- *장점* : 느슨한 결합(Loose Coupling) 달성. Non-IP 디바이스 추가 시, 복합통신 게이트웨이 본체가 아닌 해당 Agent만 수정 및 배포하면 되어 확장성과 유지보수 용이성 극대화.

2.3 단순 프로토콜 변환 게이트웨이 (Simple Translator Gateway)

이 방식은 2.1의 직접연결 방식의 한계를 인지하고, 최소한의 기능만을 수행하는 경량 프록시를 도입한 형태이다.

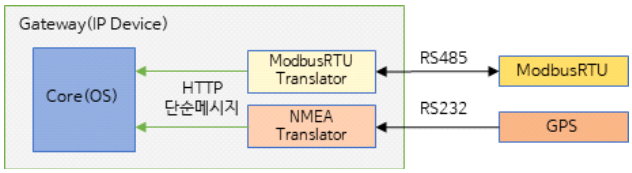

그림 3 단순 프로토콜 변환 모델

- *주요 기능* : Non-IP 프로토콜(예: Modbus RTU)의 원시 데이터(Raw Data)를 단순한 IP 기반 메시지 포맷(예: MQTT 페이로드)으로 1:1 변환하는 역할.
- *한계* : 디바이스의 상태 관리, 펌웨어 업데이트, 보안 인증 등 고수준의 서비스 관리 기능은 복합통신 게이트웨이가 직접 처리해야 함. 즉, 단순한 통신 매핑은 해결하지만, 복잡한 관리 업무는 해결하지 못함.

2.4 OS 기반 드라이버 프록시 모델 (Driver Proxy Model)

이 방식은 Non-IP 디바이스와의 통신을 위한 '드라이버'를 메인 OS의 커널 영역이 아닌 사용자 영역(User Space)에서 독립적인 프록시로 분리하여 실행한다. 이는 드라이버의 안정성을 높이고, 특정 드라이버 오류가 메인 시스템에 영향을 미치지 않는다.

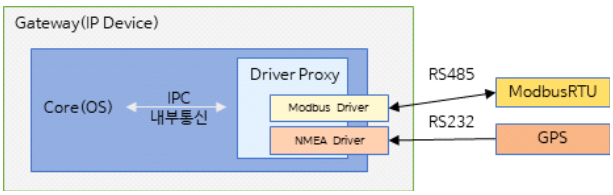

그림 4 OS기반 Driver Proxy 모델

- *Non-IP 드라이버 Proxy의 역할* : Non-IP 디바이스의 물리적인 연결 및 프로토콜 처리 전담.
- *Agent와의 차이점* : 이 모델은 OS 내부 통신(IPC)에 의존하며, 표준화된 IoT 서비스 계층의 추상화 및 관리 기능이 부족함. 즉, 운영의 유연성은 개선되지만 표준기반의 상호 운용성은 확보되지 않음.

2.5 서비스 기반 Agent 아키텍처 (제안 모델)

본 연구는 앞선 직접통합 및 드라이버 프록시 모델(2.1~2.4)이 해결하지 못한 표준기반 서비스 추상화 및 관리기능 부재라는 한계를 극복하고, 느슨한 결합을 극대화하여 Non-IP 디바이스의 다양성과 변화에 대응할 수 있는 서비스 기반 Agent 아키텍처를 제안하며, 핵심 구성 요소는 다음과 같다.

- *Protocol Abstraction Layer (PAL) 도입* : Agent 계층에서 각 Non-IP 디바이스의 원시(Raw) 프로토콜을 처리함. 상위 복합통신

게이트웨이 코어에는 통일된 추상화된 데이터 모델만 제공하여, 복합통신 게이트웨이 코어의 복잡도를 낮춤.

- *동적 로딩(Dynamic Loading) 기반 모듈화* : 각 Non-IP 통신드라이버를 플러그인 형태의 독립적인 모듈로 분리함. 복합통신 게이트웨이 동작 중 OS 또는 Proxy 계층에서 새로운 모듈을 동적으로 로딩/언로딩하여 시스템 중단 없이 확장성을 확보함.
- *Agent의 상태 관리 기능 강화* : Agent가 연결된 Non-IP 디바이스의 연결 상태, 배터리 잔량, 펌웨어 버전 등의 정보를 자체적으로 관리하고 복합통신 게이트웨이 코어에 보고함으로써 복합통신 게이트웨이의 관리 부하를 줄임.

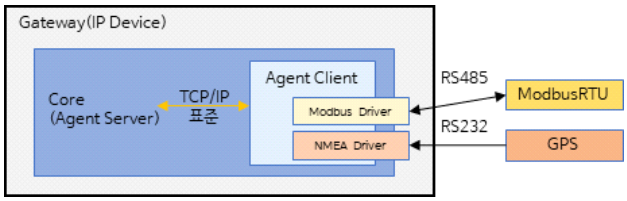

그림 5 서비스 Agent를 통한 추상화 모델

3. 관련 표준 및 기술 동향 검토

3.1 OneM2M

OneM2M은 다양한 IoT 애플리케이션과 이종 통신 네트워크 간의 상호운용성을 제공하기 위해 서비스계층(Service Layer)과 공통서비스기능(CSFs)을 정의한다.

- *개요* : OneM2M은 수직적(Vertical)으로 분산된 IoT 애플리케이션들을 수평적(Horizontal) 플랫폼으로 통합하는 것을 목표로 함. Agent 아키텍처에서는 이 표준을 통해 디바이스 관리 기능을 추상화하여 게이트웨이 코어의 복잡도를 낮춤.
- *주요 CSF 및 활용* : Agent는 CSFs를 활용하여 Non-IP 장치를 표준화된 리소스(Resource) 형태로 추상화함. 주요 CSF인 Registration (디바이스 등록), Security(인증/권한), Group Management 등은 Agent의 핵심 관리 기능과 일치함.

3.2 OMA LwM2M

OMA LwM2M(Lightweight M2M)은 제약이 심한 IoT 디바이스를 효율적으로 관리하기 위해 설계된 경량 프로토콜이다. Agent 아키텍처에서 LwM2M은 Non-IP 데이터를 표준화된 리소스로 변환하는 PAL의 실질적인 구현 수단으로 기능하며, 복합통신게이트웨이 코어(LwM2M 서버)와 통신하는 핵심 프로토콜이 된다.

- *객체 모델 기반 추상화* : Non-IP 디바이스에서 수집된 센서 데이터 및 디바이스 정보(배터리 잔량, 펌웨어 버전)를 /객체 ID/인스턴스 ID/리소스 ID 구조의 통합 관리용 표준 데이터 모델로 캡슐화함.
- *서비스 추상화 계층 구조* : Agent 내에서 LwM2M 객체는 OneM2M CSFs와 연동하여 최종 서비스 계층을 구성함.

3.3 OPC UA

OPC UA는 산업 자동화 분야에서 널리 사용되는 플랫폼 독립적인 서비스 지향 아키텍처(SOA) 기반의 표준이다.

- *개요* : OPC Classic의 한계(Windows 의존성, 보안 취약성)를 극복하고, 강력한 보안 기능과 정보 모델링 기능을 통합하여 데이터 상호 운용성을 제공.
- *활용 및 동향* : 복합통신게이트웨이 환경에서 OPC UA는 특히 ModbusRTU와 같은 유선 산업 제어 장치들의 데이터를 표준화된 방식으로 수집하는 데 중요한 역할을 함. Agent는 OPC UA 클라이언트 역할을 수행하여 Non-IP 데이터를 수집하거나, 자신이 수집한 데이터를 상위 시스템에 OPC UA 서버 형태로 제공하여 게이트웨이 코어의 산업연동 확장 가능. OPC UA는 LwM2M이 경량 디바이스 관리에 중점을 둔다면, 산업용 데이터의 정보 모델링과 수직적 통합에 강점을 가짐.

4. 데이터 보안 및 메시지 보호 대책 연구

4.1 Agent 기반 구조에서의 보안 책임 분리

Agent 기반 아키텍처는 보안 책임을 복합통신 게이트웨이에서 Agent 계층으로 분리한다. 각 Agent는 자신이 담당하는 Non-IP 통신 구간의 보안을 전담하며, 복합통신 게이트웨이와의 통신 구간에 대한 메시지 보안을 책임진다.

4.2 Non-IP 구간 보안 강화

- *무선 구간 (BLE, LoRaWAN)* : BLE의 링크 계층 AES-128 암호화 및 LoRaWAN의 NwkSKey/AppSKey 분리를 통해 데이터 기밀성 및 무결성을 보장
- *유선 레거시 구간 (ModbusRTU, NMEA)* : 자체 보안 기능이 없는 프로토콜의 경우, Agent는 데이터를 수집하는 즉시 데이터 출처인증 및 무결성검증을 수행하고, 암호화된 터널을 통해 복합통신게이트웨이 코어로 전송

4.3 Agent-복합통신게이트웨이 간 메시지 보안 (End-to-End)

Agent와 복합통신 게이트웨이 코어 간의 IP 통신(CoAP 또는 MQTT)에는 반드시 전송계층 보안(TLS/DTLS)을 적용해야 한다.

- *TLS (Transport Layer Security)* : TCP/IP 통신에서 데이터의 기밀성, 무결성, 상호 인증을 제공하는 핵심 프로토콜
- *DTLS (Datagram Transport Layer Security)* : TLS의 보안 기능을 UDP 기반 환경으로 확장한 프로토콜로, UDP의 비신뢰성에도 불구하고 메시지의 기밀성 및 무결성을 보장.

Ⅲ. 결론

본 연구는 복합통신 게이트웨이경에서 이종 Non-IP 디바이스 연결 시 발생하는 소프트웨어 복잡성, 데이터 비표준화, 디바이스 관리의 어려움이라는 핵심적인 문제를 해결하기 위한 연구를 진행하였다. 연구 결과, 기존의 직접 관리 및 단순 프록시 방식은 이 문제를 해결하기에 부족함을 알 수 있다.

서비스 기반 Agent 아키텍처가 이종 Non-IP 디바이스 연결에 대한 적절한 방안이라고 볼 수 있다. Agent는 OMA LwM2M 객체 모델을 통해 데이터를 표준화하고, 상태 관리 기능을 전담하며, Non-IP 통신 스택을 게이트웨이 코어로부터 완전히 분리(Loose Coupling)한다. 이로써 복합통신게이트웨이는 유연한 확장성을 확보하며, Agent-코어 간 DTLS/TLS 보안을 통해 고신뢰성이 요구되는 데이터의 안전성 요구사항을 충족하여 선박이라는 폐쇄적인 환경에서 안전성이 요구되는 환경에서 최적의 대안이 될 수 있을 것으로 기대한다.

ACKNOWLEDGMENT

본 논문은 2025년도 해양수산부 재원으로 해양수산과학기술진흥원의 지원을 받아 수행된 연구임(20220544, 실해역 성능검증 기반기술 개발)

참고문헌

[1] “SmartM2M; Study for OneM2M; Discovery and Query solution analysis & selection”, ESTI (2020)

[2] “oneM2M”, onem2m.org

[3] “OMA LwM2M”, https://en.wikipedia.org/wiki/OMA_LWM2M

[4] “OSI”, https://en.wikipedia.org/wiki/OSI_model

[5] “이종 홈네트워크 기기 간 상호호환성 제공 시스템 구축 방법“, ETRI, 박호진. 특허청

[6] ”Industrial Protocol Gateway“, Advantech