네트워크기반함정에서의정보보안강화를위한MDM설계

최영두*
해군사관학교
chododo78@navy.ac.kr

DesignofanMDMArchitectureforEnhancingInformationSecurityinNetworkedNavalPlatforms

Choi Young Doo
ROK Navy Academy

요 약

현대 해군 함정은 네트워크 중심의 전투체계 운영으로 인해 고도화된 연결성과 함께 사이버 위협에 대한 취약성이 증가하고 있다. 본 연구는 이러한 문제에 대응하기 위해 스마트센서 기반 신뢰도 평가, 생성형 인공지능(GAN)을 활용한 이상 탐지, 그리고 블록체인 기반 정책 무결보장을 결합한 모바일 기기 관리(MDM) 아키텍처를 제안한다. 제안 시스템은 해군 운용 환경을 모사한 시뮬레이션을 통해 구현되었으며, 92% 이상의 탐지 정확도, 정책 반영 지연 5초 이내, 블록체인 처리속도 100TPS 수준의 성능을 달성하였다. 이를 통해 본 논문은 실시간 대응성과 분산 신뢰를 요구하는 네트워크 기반 함정 환경에서의 정보보안 강화를 위한 차세대 MDM 구조의 실효성을 입증한다.

Ⅰ. 서 론

기존의 모바일 기기 관리(Mobile Device Management, MDM) 체계는 주로 중앙 집중형 구조와 기기 제어 중심의 정책 적용에 초점이 맞추어져 있어 실시간 이상 탐지, 신뢰 기반 정책 적용, 데이터 무결성 검증 등의 기능을 수행하는 데 한계가 있다[1] 또한 해상 전장이라는 특수한 운용 환경에서는 고정된 인프라 없이도 보안 정책이 자율적이고 분산적으로 실행될 수 있는 능동적 보안 체계가 요구된다. 이에 따라 기존 MDM 체계의 한계를 보완하고 함정 내 네트워크 기반 보안을 강화하기 위한 새로운 접근이 필요하다.

Ⅱ. 본론

본 논문에서 제안하는 MDM 아키텍처는 크게 세 가지 구성요소로 이루어진다. 스마트센서 기반 신뢰도 평가 모듈, GAN 기반 이상 탐지 엔진, 블록체인 기반 정책 기록 및 검증 모듈이다.

이들은 상호 연동되어 단말기의 상태를 지속적으로 감시하고, 이상 징후 발생 시 즉시 정책을 적용하며, 모든 행위를 불변의 형태로 기록한다.

센서로부터 수집된 물리 계층 통신 정보(예: RSSI, 통신 주기, 패킷 크기 등)를 통계적으로 분석하여 각 단말기의 신뢰 점수를 계산한다. 신뢰 점수가 임계값 이하일 경우, 해당 단말은 의심 대상으로 분류되며, 접근 제어 정책이 강화된다[2].

정상 시나리오로 학습된 GAN 생성기를 활용해 입력 데이터의 재구성 오차를 기반으로 이상도를 산출한다[3]. 생성기의 출력값과 실제 측정값 간의 차이를 이용하여 이상 여부를 판단하고, 탐지된 이상은 정책 트리거로 활용된다.

MDM 시스템 내에서 발생한 모든 정책 변경 이력, 접속 로그, 이상 탐지 결과는 블록체인 노드에 기록된다. 각 블록은 SHA-256 해시를 기반으로 연결되며, 외부 감사자가 검증할 수 있도록 설계되었다[5],[6]. 이로써 함정 내 보안정책 이력의 위조·삭제 위험이 방지된다.

MATLAB R2024b 기반으로 시뮬레이터를 구성하고, GUI 환경에서 실시간 이상 탐지, 시각화, 경고창, 블록체인 로그 기록 모듈을 통합 구현하였다. 테스트 환경은 3개의 센서 데이터를 기반으로 구성되며, 각 센서는 이상 패턴을 임의 삽입하여 탐지 성능을 평가하였다.

정상 패턴 학습은 3개 센서의 정상 데이터를 GAN 생성기로 학습한다. 이상 패턴 삽입은 각 센서에 일정 구간 이상값 주입 탐지 및 정책 적용, 이상 감지 시 경고 발생, 로그 기록 수행 무결성 확인: 블록체인 상의 블록 연결 구조와 해시값 확인한다.

실험 결과는 이상 탐지 정확도: 92.3% (F1-score 기준), 정책 반영 지연: 평균 4.8초, 블록체인 처리량 100 TPS 달성하였다.

Ⅲ. 결론

본 논문에서는 네트워크 기반 함정 환경에서 증가하는 정보보안 위협에 효과적으로 대응하기 위한 새로운 MDM 아키텍처를 제안하였다. 기존의 중앙 집중형 MDM 체계가 해상 전장 환경에서 가지는 한계를 극복하고자, 본 연구는 스마트센서를 활용한 물리 계층 기반 신뢰도 평가, 생성형 인공지능(GAN)을 이용한 이상 탐지, 그리고 블록체인 기술을 통한 정책 무결성 보장 기능을 통합 설계하였다.

ACKNOWLEDGMENT

This work was supported by the Naval Academy Ocean Research Institute's 2025 Academic Research Program Grant.

참 고 문 헌

[1] 박정훈 외 3인, “군용 IoT 환경에서의 MDM 기술 동향과 적용 방안,” 국방정보통신연구, 제48권 제3호, pp. 40-51, 2021.

[2] 이재원, 김상배, “함정 기반 무선 통신 보안 취약점 분석 및 대응방안,” 정보보호학회논문지, 제29권 제1호, pp. 15-23, 2019.

[3] S. Goodfellow et al., “Generative Adversarial Nets,” in Advances in Neural Information Processing Systems (NeurIPS), 2014.

[4] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and Solutions,” Computer Communications, vol. 120, pp. 10 - 29, 2018.

[5]조승현, “군 전장환경에 적합한 블록체인 보안 기술 연구,” 사이버군사과학지, 제12권 제2호., pp. 33-47, 2022.