V2X 네트워크 침입 탐지 시스템의 발전 및 연구 동향 조사

이태양 [1], 김민수 [1], 박한영 [2], 최지웅 [2]
[1] 대구경북과학기술원 기초학부
[2] 대구경북과학기술원 전기전자컴퓨터공학과

{sunny626, excel2001, prkhnyng, jwchoi}@dgist.ac.kr*

A Study on the Evolution and Trends of V2X Intrusion Detection Systems

Taeyang Lee[1], Minsu Kim[1], Hanyoung Park[2], Ji-Woong Choi[2]

[1]School of Undergraduate Studies , DGIST,
[2]Department of Electrical Engineering & Computer Science, DGIST

요 약

V2X(Vehicle-to-Everything)는 차량·인프라·보행자·네트워크가 안전·협력 주행 정보를 교환하는 핵심 통신 기술로, 저지연, 고신뢰 요구가 강화되고 있다. 하지만 인증 인프라만으로는 비정상행위를 충분하게 차단하기 어려워 IDS(Intrusion Detection System)가 각광받고 있다. 본 논문에서는 이러한 IDS 에 대한 최신 연구 동향을 소개한다.

Ⅰ. 서 론

Vehicle-to-Everything(V2X) 통신기술은 차량·도로 인프라·보행자·네트워크가 주행 관련 정보를 교환하여 협력 주행과 안전 서비스를 구현하는 핵심 기술이다 [1]. V2X 는 고이동성 환경에서 저지연·고신뢰 통신을 목표로 하며, 다양한 계층에서 요구사항과 연구 과제가 정리되어 왔다 [1],[2]. 그러나 V2X 는 safety-critical 메시지를 개방형 무선 채널로 광범위하게 전파하는 특성상, 공격 표면이 넓고 가용성 저하가 곧 안전 기능의 성능 저하로 이어질 수 있다 [3]. 이를 완화하기 위해 인증서 기반 자격증명 관리 체계가 도입되었지만 [4], DoS(Denial of Service)와 같은 가용성 공격이나 합법 노드에 의한 비정상 행위는 인증만으로는 충분히 차단하기 어렵다 [3],[5]. 이러한 배경에서 V2X 보안에서는 기반 인증 인프라와 더불어, 네트워크/엣지 관점에서 공격을 탐지·대응하는 IDS(Intrusion Detection System)가 중요해지고 있다 [3],[5]. 다만 V2X 환경은 차량·지역·시간대에 따라 트래픽 분포가 크게 변하고, 라벨링된 공격 데이터 확보가 제한적이며, 실시간 운용을 위한 경량성과 프라이버시 요구까지 동시에 만족해야 한다. 본 논문에서는 이러한 배경에서 V2X 환경에서 요구되는 IDS 의 역할을 정리하고, 기술의 발전 흐름을 중심으로 핵심 설계 고려사항과 최신 연구 동향을 소개한다.

Ⅱ. 본론

초기 V2X 보안은 사람이 설계한 규칙이나 임계값 기반의 판단 방식이 주를 이루었다. 이는 복잡한 무선 환경의 요구사항을 반영한 퍼지 로직 기반 자원 할당 기술 등으로 나타났다 [6]. 규칙 기반 방식은 계산 복잡도가 낮고 동작 원리가 명확하나, 공격 기법이 고도화됨에 따라 변칙적인 패턴 탐지에 한계를 보였다. 이를 보완하기 위해 규칙 기반으로 이상을 1 차 선별하고, 복잡한 패턴은 딥러닝으로 식별하는 하이브리드 구조가 제안되었다 [7]. 또한 내부 의사결정 과정을 파악하기 어려워 결과의 근거를 알 수 없는 딥러닝의 '블랙박스' 문제를 해결하기 위해 학습된 결정 경계에서 이해 가능한 규칙을 추출하여 활용하는 연구도 진행되었다 [8]. 정해진 규칙만으로 포착하기 어려운 공격이 증가함에 따라, 사전에 정의된 조건 대신 데이터로부터 스스로 경계를 학습하는 머신러닝 기반 접근법이 확산되었다. 머신러닝 기반 접근법은 특징추출과 분류기 설계를 통해 공격을 식별하며, 다양한 기법의 성능 비교를 통해 적용 조건이 체계화되었다 [9]. 차량 환경에서는 여러 계층의 정보를 통합하는 다계층/하이브리드 구조의 IDS 로 확장되었다 [10]. 머신러닝 기반 접근법은 특징 설계 과정에서 높은 도메인 지식 의존도를 보이며, 차량의 이동성이나 네트워크 상태 변화와 같은 복잡한 시공간적 상관관계를 수작업 특징만으로 충분히 반영하기 어렵다는 한계가 있다. 또한 데이터의 규모와 다양성이 증대됨에 따라 특징 기반 모델의 일반화 성능이 저하될 수 있다는 점 역시 주요한 과제로 남아있다.

이후 딥러닝 기반 IDS 는 이러한 한계를 완화하기 위해 복잡한 시공간 패턴을 자동으로 포착하고 특징을 직접 학습함으로써 탐지 성능과 일반화 가능성을 높이는 방향으로 발전하였다. 특히 엣지/포그 컴퓨팅과의 결합은 네트워크 변화에 능동적으로 대응하는 실시간 지능형 탐지를 가능케 했다 [11]. 최근에는 실제 환경 재현을 위한 디지털 트윈 기반 보안 분석이 시나리오 검증 측면에서 주목받고 있으나, 실시간성 확보는 여전히 과제로 남아있다 [12]. 아울러 safety-critical 시스템의 신뢰성을 확보하기 위해 탐지 결과에 근거를 제시하는 설명가능한 AI(eXplainable Artificial Intelligence; XAI) 결합형 연구가 활발히 진행 중이다 [13].

마지막으로 최근 V2X 보안의 패러다임은 연합학습 기반 IDS 로 이동하고 있다. V2X 데이터는 차량과 RSU(Road Side Unit) 등에 분산되어 있어 원시 데이터를 공유할 경우 프라이버시 침해 및 통신 부하가 발생하기 때문이다. 연합학습은 데이터 공유 없이 모델을 업데이트함으로써 이러한 제약을 완화하는 현실적 대안으로 제시된다 [14]. 특히 5G/6G 환경의 제로데이 공격 탐지나 엣지 컴퓨팅 기반의 분산 IDS 구현 사례는 연합학습의 실용성을 입증한다 [15]. 최근 연구는

VANET(Vehicular Ad Hoc Network) 환경에서의 경량화와 지연 시간 단축에 집중하고 있다 [16]. 다만, 통신 오버헤드와 데이터 불균형, 중독(Poisoning) 공격 등은 향후 해결해야 할 주요 과제이다 [5],[14].

Ⅲ. 결론

본 논문에서는 V2X 보안 내 IDS 의 도입 배경을 고찰하고, 실질적인 운용 제약을 반영한 기술적 발전 방향을 체계적으로 정리하였다. V2X 환경은 고이동성 및 고변동성이라는 특성상 단순 탐지 정확도 확보를 넘어 실시간 지연 및 연산 자원 제약, 데이터 공유 시의 프라이버시 보호 등 다각적인 설계 변수를 동시에 고려해야 한다. 그렇기에 향후 IDS 연구는 단순 분류 성능 향상을 넘어, 동적인 환경 변화와 지능화되는 공격 패턴에 유연하게 대응할 수 있는 강건한 학습 및 추론 구조를 정립하는 데 집중해야 한다. 먼저 차량 밀도나 도로 유형에 따른 데이터 분포의 가변성을 극복하기 위한 일반화 기법이 핵심적이다. 이를 위해 도메인 적응, 증분 학습, 자기지도 학습 기반의 제로데이 공격 대응 기술이 필수 요소로 통합되어야 한다. 차량 및 RSU 의 자원 제약 하에서 실시간성을 보장하기 위한 추가적인 경량화 기법의 도입 또한 필요하다. 특히 안전 필수 시스템상 오탐 대응 비용이 막대하므로, 모델의 불확실성을 정량화하는 리스크 스코어링 체계가 병행되어야 한다. 마지막으로 연합학습 기반 IDS 의 실용성을 높이기 위해 데이터 불균형에 따른 수렴 저하와 모델 중독공격 등의 보안 과제를 해결해야 한다. 이를 위해 개인화 연합학습, 강건 집계, 통신 효율화 기술이 유기적으로 결합된 분산 학습 아키텍처가 요구된다. 결론적으로, 차세대 IDS 는 강건성, 경량 추론, 보안성이 확보된 분산 학습 체계를 동시에 만족하는 통합 프레임워크를 지향해야 하며, 이러한 기술적 완성도는 미래 협력 주행 서비스의 신뢰성을 담보하는 결정적인 토대가 될 것이다.

ACKNOWLEDGMENT

본 논문은 2025 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획 평가원의 지원을 받아 수행된 연구임 (No. RS-2024-00442085, 자율주행 차량 서비스 보호를 위한 V2X 무선통신 인프라 보안 핵심기술 개발, No. RS-2024-00398157, AI-Native 응용서비스 지원 6G 시스템 기술개발).

참 고 문 헌

[1] R. Garcia et al., "A Tutorial on 5G NR V2X Communications," IEEE Commun. Surv. Tut., vol. 23, no. 3, pp. 1920-1963, 2021.

[2] E. Ahmed et al., "Wireless Access for V2X Communications: Research, Challenges and Opportunities," IEEE Commun. Surv. Tut., vol. 26, no. 3, pp. 2082-2119, 2024.

[3] J. Herman et al., "Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape Through Systematic Review," IEEE Access, vol. 12, pp. 72871-72895, 2024.

[4] B. Brecht et al., "A Security Credential Management System for V2X Communications," IEEE Trans. Intell. Transp. Syst., vol. 19, no. 12, pp. 3850-3871, Dec. 2018.

[5] S. A. Hakeem et al., "Advancing Intrusion Detection in V2X Networks: A Comprehensive Survey on Machine Learning, Federated Learning, and Edge AI for V2X Security," IEEE Trans. Intell. Transp. Syst., vol. 26, no. 8, pp. 11137-11164, Aug. 2025.

[6] M. Zhang et al., "Fuzzy Logic-Based Resource Allocation Algorithm for V2X Communications in 5G Cellular Networks," IEEE J. Sel. Areas Commun., vol. 39, no. 8, pp. 2501-2513, Aug. 2021.

[7] P. Seong et al., "Enhancing V2X Security Through Combined Rule-Based and DL-Based Local Misbehavior Detection in Roadside Units," IEEE Open J. Intell. Transp. Syst., vol. 5, pp. 109-123, 2024.

[8] M. A. Al-Hajji et al., "Two-Stage Intrusion Detection System in Intelligent Transportation Systems Using Rule Extraction Methods From Deep Neural Networks," IEEE Trans. Intell. Transp. Syst., vol. 23, no. 11, pp. 21612-21626, Nov. 2022.

[9] Y. Zhang et al., "Comparative research on network intrusion detection methods based on machine learning," Comput. Secur., vol. 121, Art. no. 102861, Oct. 2022.

[10] L. Yang et al., "MTH-IDS: A multitiered hybrid intrusion detection system for Internet of Vehicles," IEEE Internet Things J., vol. 8, no. 18, pp. 14532-14547, Sept. 2021.

[11] M. Rihan et al., "Deep-VFog: When Artificial Intelligence Meets Fog Computing in V2X," IEEE Syst. J., vol. 14, no. 4, pp. 2758-2769, Dec. 2020.

[12] Z. Lv et al., "Deep Learning for Security in Digital Twins of Cooperative Intelligent Transportation Systems," IEEE Trans. Intell. Transp. Syst., vol. 23, no. 10, pp. 19249-19259, Oct. 2022.

[13] M. Wazid et al., "Explainable Deep Learning-Enabled Malware Attack Detection for IoT-Enabled Intelligent Transportation Systems," IEEE Trans. Intell. Transp. Syst., vol. 26, no. 3, pp. 3173-3183, Mar. 2025.gkwl

[14] G. Makris et al., "A comprehensive survey of Federated Intrusion Detection Systems: Techniques, challenges and solutions," Comput. Sci. Rev., vol. 56, Art. no. 100688, May 2025.

[15] K. Selamina et al., "Edge Computing-enabled Intrusion Detection for C-V2X Networks using Federated Learning," in Proc. IEEE Glob. Commun. Conf. (GLOBECOM), 2022, pp. 562-567.

[16] X. Chen et al., "Fast and practical intrusion detection system based on federated learning for VANET," Comput. Secur., vol. 143, Art. no. 103912, June 2024.