자율주행 통신 환경을 위한 침입 탐지 모델의 거짓양성률 기반 성능 비교 분석

김민수, 이태양, 박한영, 최지웅
대구경북과학기술원

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

Perofrmance Comparison of Intrusion Detection Models Based on Low False Positive Rate in Autonomous Driving Communication Environments

Minsu Kim, Taeyang Lee, Hanyoung Park and Ji-Woong Choi
Daegu Gyeongbuk Institute of Science and Technology (DGIST)

요 약

본 연구에서는 대표적인 기계학습 및 딥러닝 기반 모델을 대상으로 False Positive Rate (FPR)이 0.01 이하인 구간에서의 탐지 성능과 처리 효율성을 정량적으로 비교하였다. CIC-IDS2017 데이터를 기반으로 Long Short-Term Memory (LSTM), Neural Network (NN), Random Forest (RF), Decision Tree (DT) 모델을 학습하고, 정확도, Area Under Curve (AUC), 훈련 시간, 추론 시간 등을 측정하였다. 실험 결과, LSTM 은 최고 성능을 보였으나, 처리 지연이 커 실시간성에 제약이 있었다. 반면, Random Forest (Top 6 Feature 기반)는 True Positive Rate (TPR) 0.999 를 유지하면서도 빠른 추론 속도를 보여 실환경 적용 가능성이 높았다. 본 연구는 정확도 중심의 평가를 넘어 실시간 시스템 관점에서의 탐지 모델 비교 기준을 제시하였다.

Ⅰ. 서 론

자율 주행 차량은 다양한 무선 통신 기술들을 기반으로 주행 환경을 인식하고 판단을 수행하지만, 외부 침입에 의한 통신 교란에 매우 민감하다 [1]. 이에 따라 통신 기반 자율 주행 시스템에서는 높은 정확도를 가진 Intrusion Detection System (IDS)이 필수적이며, 이를 위해 다양한 머신 러닝 및 딥러닝 기반의 탐지 모델이 제안되어 왔다. 기존 연구들은 대체로 정확도, 정밀도, Area Under Curve (AUC)와 같은 통합 지표를 중심으로 모델 성능을 평가하고 비교하는데 집중하였다 [2]. 실제 자율 주행 시스템은 초저지연성과 실시간 경보 신뢰도를 요구하기 때문에 단순 정확도 외에도 False Positive Rate (FPR)에 대한 고려가 필수적이다. 특히 FPR 이 0.01 이하인 환경에서도 탐지 민감도를 유지할 수 있는지 여부는 실제 시스템 적용 측면에서 핵심적인 요소이지만, 해당 구간에 대한 세부적인 분석은 기존 연구들에서 충분히 고려되지 않았다 [3].

본 논문에서는 이러한 한계를 보완하고자, 대표적인 머신러닝 및 딥러닝 기반 탐지 모델을 대상으로 FPR 이 낮은 구간(≤ 0.01)에서의 True Positive Rate (TPR) 유지 능력을 핵심 지표로 설정하여 정량적인 비교 분석을 수행하였다. 또한 각 모델의 훈련 시간과 단일 샘플 기준 추론 시간까지 함께 측정하여 자율 주행 통신 환경에 실시간 적용 가능성에 대해서도 종합적으로 평가하였다.

Ⅱ. 본론

본 연구에서는 자율주행 통신 환경에서 발생 가능한 다양한 침입을 탐지하기 위해, LSTM 기반의 순환 신경망, NN, RF, DT 등 총 다섯 가지 기계학습 기반 분류 모델을 비교하였다. 각 모델은 동일한 데이터셋(CIC-IDS2017)을 기반으로 학습되었으며, 정확도, AUC, 훈련 시간, 테스트 시간, 샘플 당 추론 시간 등 주요 성능 지표를 기준으로 정량적 비교를 수행하였다. 학습에 사용된 파라미터들은 표 1 과 표 2 에 나타나 있다.

표 2 LSTM 및 NN 모델의 학습 파라미터 설정

	Epoch	Batch Size	Optimizer	Hidden Layer
LSTM	50	32	Adam	(64, 32)
NN	50	64	Adam	(128, 64)

표 1 Tree 기반 모델의 설정 및 사용 Feature

	Criterion	Number of Trees	Max Depth	Feature used
RF	Gini	100	10	All
RF (Top6)	Gini	100	10	Top 6
DT	Entropy	-	10	All

본 논문에서 사용된 CIC-IDS2017 데이터셋은 캐나다 사이버보안연구소 (CIC)에서 제작한 공개 데이터셋으로, 다양한 날짜의 Distributed Denial-of-Service(DDoS), PortScan, Web Attack, Infiltration, Botnet, Brute Force 등 다양한 유형의 실제 네트워크 공격 시나리오와 정상적인 흐름의 데이터가 포함된다. 데이터셋은 흐름 기반으로 구성되며, 각 흐름은 약 80 여 개의 네트워크 및 트래픽 관련 Feature 로 구성되어 있다. 전처리 과정에서는 문자열 형태의 IP 주소와 Timestamp 를 각각 정수형으로 변환하고, 학습에 사용된 Feature 는 모두 수치형으로 정규화하여 모델 입력에 적합하도록 구성하였다.

본 실험의 훈련 시간 및 추론 시간은 동일한 환경에서 측정되었으며, 이는 사용된 시스템 사양에 따라 달라질 수 있다. 실험은 Intel Core i7-6700K CPU, 32GB RAM, NVIDIA GTX 960 GPU 기반 환경에서 수행되었다.

Figure 1 은 각 모델별 Receiver Operating Characteristic (ROC) 곡선을 시각화한 것으로, 임계값 변화에 따른 TPR 과 FPR 의 관계를 나타낸다. 표 3 에는 각 모델의 훈련 시간, 테스트 시간, 정확도가 정리되어 있다. 이를 통해 모델 간 처리 성능 및 효율성을 직관적으로 비교할 수 있다.

LSTM 모델은 시계열 기반 패턴 학습 능력으로 인해 AUC 0.9998, 정확도 99.67%로 가장 높은 공격 분류 성능을 나타냈으며, 이는 자율주행 차량 내부의 패킷 흐름과 같이 연속적 의존성을 가지는 데이터 특성을 효과적으로 반영한 결과로 해석할 수 있다. 그러나 LSTM 은 50 epoch 기준으로 약 3,126s 의 훈련 시간이 소요되었으며, 샘플 당 평균 1.056ms 의 처리 시간이 소요되었다. 이는 실시간성이 중요한 자율주행 통신 시나리오에서는 부담이 될 수 있는 처리 지연으로 판단된다.

한편, Random Forest 모델은 전체 Feature 를 활용한 경우 정확도 99.74%, AUC 0.9995 를 기록하였으며, 주요 상위 6 개 Feature 만을 활용한 경우 정확도는 99.86%로 향상되었고 AUC 역시 0.9997 로 향상되었다. 특히, Random Forest(Top 6) 모델은 샘플 당 테스트 시간 0.0114ms 수준으로 매우 빠른 응답 속도를 보였으며, 훈련 시간 또한 395s 로 LSTM 대비 약 8 배 이상 짧았다. 이는 모델 경량화 및 추론 시간 단축 측면에서 실시간 시스템 적용이 가능함을 의미한다.

Decision Tree 모델은 AUC 0.9962, 정확도 99.47%로 상대적으로 낮은 성능을 보였으나, 단일 샘플 예측 시간은 약 0.00063ms 로 가장 짧았다.

신경망 기반 모델 중 Neural Network 모델은 정확도 99.36%, AUC 0.9970 로 5 가지 모델 중 가장 낮은 정확도를 기록하였고, 검출 시간 역시 샘플 당 1.33ms 로 효율성 역시 가장 떨어지는 것으로 분석되었다.

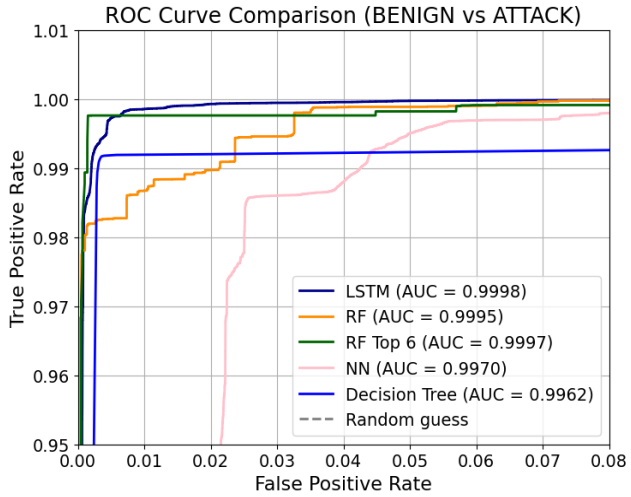

그림 1 모델에 따른 ROC Curve

표 3 모델에 따른 훈련 및 검출 시간과 정확도

	Train Time (s)	Test Time (ms)	Accuracy (%)
LSTM	3126.61	1.056	99.67
RF	881.19	0.0149	99.74
RF (Top 6)	395.68	0.0114	99.86
NN	1193.66	1.33	99.36
DT	84.55	0.00063	99.47

자율주행 통신 시스템은 실시간성과 알람 신뢰도가 가장 핵심적이다. 이에 따라 본 논문에서는 탐지 정확도뿐 아니라 FPR 0.01 이하의 저위험 구간에서의 성능을 중점적으로 분석하였다. Sridhar 등은 스마트 그리드 환경과 같은 실시간 사이버물리 시스템에서는 FPR 이 0.005 이상일 경우 알람의 실효성이 급격히 저하되어 시스템 신뢰도 유지가 어렵다고 했으며[4], 자율주행 통신 환경 역시 이와 유사한 실시간 요구 조건을 가진다. 본 실험에서 LSTM, Random Forest (Top 6)는 FPR 0.01 이하의 구간에서도 TPR 0.999 이상을 유지하며 우수한 정밀 탐지 능력을 확인하였다. 반면, NN 과 Decision Tree 모델은 해당 구간에서 상대적으로 완만한 TPR 곡선을 보여 초기 탐지 민감도 측면에서는 한계를 보였다.

Ⅲ. 결론

본 논문에서는 자율 주행 통신 환경을 고려해 다양한 기계학습 기반 탐지 모델들의 성능을 정량적으로 비교하였다. 정확도와 AUC 뿐만 아니라 실시간성의 기준이 되는 샘플 당 추론 시간과 FPR 0.01 이하 구간에서의 TPR 유지 능력을 함께 분석하였다. 그 결과, 정확도 기준으로는 LSTM 이 가장 우수한 성능을 보였으나, 실시간성과 시스템 효율성을 함께 고려할 경우 Random Forest (Top 6 Feature) 모델이 가장 균형 잡힌 성능을 나타냈다. 또한 초저지연 응답이 요구되는 환경에서는 Decision Tree 기반 모델의 적용도 유효할 수 있다. 본 연구는 단순한 분류 성능 비교를 넘어서, 실제 자율 주행 시스템에서의 적용 가능성을 반영한 평가 기준을 제시하였다는 점에서 기존 연구와 차별성을 가진다. 향후 연구에서는 자율 주행 시뮬레이션 환경에서의 실시간 연동 실험으로의 확장을 제시하고자 한다.

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. Sommer and V. Paxson, “Outside the Closed World: On Using Machine Learning for Network Intrusion Detection,” *IEEE Symposium on Security and Privacy*, pp. 305– 316, 2010.

[2] X. Lin, R. K. Li, and X. Lin, “Security and Privacy for the Internet of Vehicles: Challenges and Opportunities,” *IEEE Communications Magazine*, vol. 56, no. 10, pp. 62– 68, Oct. 2018.

[3] F. Buczak and E. Guven, “A Survey of Machine Learning Techniques for Cyber Security Intrusion Detection,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153– 1176, 2016.

[4] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber–physical system security for the electric power grid: A survey,” *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 1– 9, Mar. 2012.