휴리스틱과 XGBoost 를 활용한 비정상 CAN 메시지 탐지

김세린 [1], 윤범헌 [1], 조학수 [2]
[1] 호서대학교 컴퓨터공학부 학부생
[2] 호서대학교 컴퓨터공학부 교수

kimserin48@gmail.com, ybh7159@naver.com, marius1406@gmail.com

Anomaly CAN Message Detection Using Heuristics and XGBoost

Se-Rin Kim[1], Beom-Heon Youn[1], Hark-Su Cho[2]
[1]Student, Dept. of Computer Engineering, Hoseo University
[2]Professor, Dept. of Computer Engineering, Hoseo University

요 약

최근 자동차의 네트워크화와 연결성이 증가함에 따라, CAN(Controller Area Network) bus 의 설계상 취약점이 보안 위협으로 대두되고 있다. 이에 대응하여 CAN bus 의 취약점을 극복하고 보안을 강화하기 위해 머신러닝을 활용한 침입 탐지 시스템에 대한 연구가 필요하다. 본 논문은 XGBoost 를 활용한 비정상 분류 방법론을 제안한다. 고려대학교 해킹 대응 기술 연구실에서 개발한 데이터 세트를 기반으로 실험을 수행한 결과, 초기 모델의 정확도는 96%였다. 그러나 추가적으로 TimeDiff(발생 간격)과 DataDiff(바이트의 차분 값)을 모델에 통합하면서 정확도가 3% 상승하였다. 본 논문은 향후에 보다 정교한 머신러닝 알고리즘과 데이터 전처리 기법을 적용하여 세밀한 모델을 개발하고, 업체의 CAN Database 를 활용하여 데이터 분석을 보다 정확하게 수행할 계획이다. 이를 통해 보다 신뢰성 높은 자동차 네트워크 보안 시스템을 구축할 수 있을 것으로 기대된다.

1. 서론

자동차 네트워크의 활발한 연결 증가는 최신 자동차에서 CAN(Controller Area Network) 버스 기술의 확대로 이어지고 있다. 이는 자동차 내의 다양한 전자 기기 및 시스템 간에 정보를 교환하고 제어하는 데 사용되는 표준 통신 프로토콜로, 자동차의 성능과 편의성을 향상시키는 데 중요한 역할을 한다. 그러나 이러한 연결성의 증가는 자동차 네트워크 보안에 대한 중요성을 더욱 부각시키고 있다. 외부 공격자들이 자동차에 침입하여 제어를 획득하거나, 중요한 데이터를 탈취하는 위협은 개인 정보 침해, 자동차의 안전성에 직접적인 위협을 가하고 있다. 이에 따라, 자동차 네트워크 보안의 강화는 중요한 과제로 대두되고 있다. 본 논문에서는 자동차 네트워크의 보안성을 향상시키기 위한 연구 방향과 XGBoost 기반의 비정상 분류 방법론을 제안하고자 한다.[1]

Received(04.23.2024), Accepted(05.08.2024)
본 연구는 과학기술정보통신부와 정보통신기획평가원의 SW 중심대학사 업의 연구결과로 수행되었음 (2019-0-01834)

2. 관련 논문

CAN 프로토콜의 취약성에 대응하기 위해 ZBCAN 방어 시스템은 메시지 타이밍을 활용하여 공격을 방어한다. 주요 공격에 대해 100%의 예방률을 달성하며, 실제 차량에서도 효과적으로 적용될 수 있음이 확인되었다.[1]

차량의 CAN 버스에서 이상 및 공격을 감지하기 위한 포괄적인 시스템인 Controller Area Network Attack Detection Framework (CAN-ADF)을 소개한다. 이 시스템은 규칙 기반과 Recurrent Neural Networks (RNN)을 결합하여 공격을 탐지한다. KIA Soul 과 Hyundai Sonata 에서 수집된 7,875,791 개의 차량 CAN 패킷을 사용하여 알고리즘의 정확도를 평가한 결과, 평균 99.45%의 정확도를 달성하였다.[2]

차량 네트워크 보안에 중점을 두고, 특히 Controller Area Network (CAN)의 취약성을 해결하기 위해 동적 ID 가상화 방법을 제안한다. 이 방법은 고정된 ID 를 사용하는 CAN 의 취약성을 보완하고, 메시지 전송 시 ID 를 무작위로 변경하여 공격자의 유효한 메시지 주입을 방지한다. 제안된 방법의 보안성은 유효 메시지 주입 공격에 대해 분석되었고, 실제 차량 네트워크에 미치는 영향을 평가하였다.[3]

3. 방법론

3.1 데이터 세트 분석

본 연구에서는 고려대학교 해킹 대응 기술 연구실에서 개발한 주행 및 주차 정보로 이루어진 데이터 세트를 활용하였다. 이 데이터 세트는 현대 아반떼 CN7의 CAN Message 를 기반으로 하며, 정상, Flooding, Fuzzing, Replay, Spoofing 으로 분류되어 있다.[4]

CAN 메시지 중 데이터 필드를 분석한 결과, 모든 CAN 메시지에 대해 DBC 데이터를 수집하는 것은 비정상 분석에 도움이 될 수 있다. 하지만 DBC 파일 입수와 데이터 디코딩에 관련된 문제가 있다. 이러한 문제로 인해 Rule-based 방식으로 비정상 탐지하는 한계가 발생하였다. 따라서, 본 연구에서는 머신러닝을 활용하여 정상과 비정상을 학습하고 분류하는 것이 필요하다.

3.2 전처리

Data 필드를 8byte 를 각각의 byte 로 분리했으며, CAN_ID Integer 형으로 변환하였다. 또한 Timestamp 값을 0 base 로 값 변환하였다.

3.2 XGBOST

비정상 분류를 위해 투자 시간 대비 효율적인 XGBoost 를 기본 설정으로 선택하여 분석하였다. 이 과정에서 XGBoost 의 하이퍼파라미터 중 n_estimators 를 조정하였다.

4. 실험

4.1 실험 환경

Pre_train_D_1(806,390)를 Train Set 으로 Pre_train_D_2(889,395)를 Test Set 로 사용하였다. 실험 환경은 표 2 와 같다.

(Table 2) Experiment Environment

Environment	Name
Language	Python
Library	XGBoost, scikit-learn, Pandas
CPU	11th Gen Intel®Core™i5-11400F
Memory	16GB

정량화된 성능을 평가하기 위해, 일반적으로 기계학습과 딥러닝 분류 모델에서 사용하는 성능 척도인 정확도, 정밀도, F1-score 를 사용하여 평가를 진행하였다.

4.2 실험 결과

각 모델의 성능은 표 3 와 같다. 초기 모델(X-1)의 학습 결과 정밀도와 F1-score 가 상대적으로 낮았다. 이에 대한 원인을 파악하기 위해 혼동 행렬을 조사한 결과, Replay 공격의 Rpm, 속도, 토크 값이 정상 데이터와의 차이가 크지 않음을 확인하였다. 이로써 데이터의 비정상 분석에 한계가 있음을 인지하였다. 따라서 전체 데이터에 TimeDiff(발생 간격)와 DataDiff(바이트의 차분 값)를 추가한 모델(X-2)을 개발하였다. 이로 인해 성능이 향상되었으며, 추가된 데이터 요소가 모델의 강건성을 향상시키는 데 기여하였다.

(Table 3) Model Performance

Model	Performance		
	Accuracy	Precision	F1
X-1	96.98	80.85	82.02
X-2	99.59	94.84	96.81

5. 결론 및 향후 개선점

최근 자동차와 네트워크의 접목으로 인해 CAN bus 의 보안 문제가 중요성을 더하고 있다. 본 논문에서는 고려대학교 해킹 대응 기술 연구실에서 개발한 데이터 세트를 활용하였으며, XGBoost 를 기반으로 한 비정상 분류 방법론을 제안한다. 초기 모델의 정확도는 96%였으나, 추가된 TimeDiff 와 DataDiff 를 적용한 결과, 모델의 성능이 3% 향상되었다.

향후에는 더욱 정교한 머신러닝 알고리즘과 효과적인 데이터 전처리 기법을 도입하여 정상과 비정상을 더욱 세밀하게 구분할 수 있는 모델을 개발해야 한다. 또한, 데이터 분석을 위한 업체의 CAN Database 를 통한 데이터 분석이 필요하다. 이를 통해 보다 정확하고 신뢰할 수 있는 자동차 네트워크 보안 시스템을 구축할 수 있을 것으로 기대된다.

참고문헌

[1] Khaled Serag, Rohit Bhatia, Akram Faqih, Muslum Ozgur Ozmen, "ZBCAN: A Zero-Byte CAN Defense System", 32nd USENIX Security Symposium, Anaheim, 2023.

[2] Shahroz Tariq, Sangyup Lee, Huy Kang Kim, Simon S. Woo,“CAN-ADF: The controller area network attack detection framework”,Computers & Security, Vol. 94, 101857, 2020.

[3] Hyunjin Sun, Se Young Lee, Kyungho Joo, Hongjoo Jin, Dong Hoon Lee,”Catch ID if You CAN: Dynamic ID Virtualization Mechanism for the Controller Area Network”,IEEE Access,Vol. 7, 2169-3536, 158237 – 158249,2019.

[4] Hyunjae Kang,ByungIl Kwak,YoungHun Lee,Haneol Lee,Hwejae Lee,HuyKang Kim,“Car Hacking: Attack & Defense Challenge 2020 Dataset”, IEEE, 2021.