Relatório da Atividade de Laboratório 04 - Setup experimental de redes intraveiculares baseadas em Ethernet automotiva

Karen S. B. Silva[1], Luiz Henrique B. A. Silva[1]

[1]Centro de Informática – Universidade Federal de Pernambuco (UFPE)
Caixa Postal 7851 – 50732.970 – Recife – PE – Brazil

{ksbs@cin.ufpe.br, lhbas@cin.ufpe.br}

Abstract. *In this study, we present an Ethernet-based Intrusion Detection System (IDS) designed to enhance cybersecurity in vehicular networks. The IDS utilizes supervised and unsupervised machine learning algorithms to analyze Ethernet traffic, specifically targeting packet modification attacks. Our contributions include the development of experimental setups for simulating and detecting various attack scenarios, leveraging Python libraries for real-time packet analysis. Results demonstrate the efficacy of our approach in accurately identifying and mitigating threats in vehicle communication networks.*

Resumo. *Este estudo apresenta um Sistema de Detecção de Intrusões (IDS) baseado em Ethernet, desenvolvido para fortalecer a cibersegurança em redes veiculares. O IDS utiliza algoritmos de aprendizado de máquina supervisionado e não supervisionado para analisar o tráfego Ethernet, focando especialmente em ataques de modificação de pacotes. Nossas contribuições incluem o desenvolvimento de cenários experimentais para simulação e detecção de diversos tipos de ataques, além da utilização de bibliotecas Python para análise em tempo real de pacotes. Os resultados demonstram a eficácia de nossa abordagem na identificação precisa e mitigação de ameaças em redes de comunicação veiculares.*

1. Introdução

A rede Ethernet automotiva é uma tecnologia desenvolvida especificamente para atender às demandas do setor automotivo, sendo uma adaptação da tecnologia Ethernet tradicional. Seu objetivo é proporcionar comunicação eficiente entre os sistemas dos veículos modernos, oferecendo alta largura de banda, flexibilidade e custo-efetividade, superando as limitações de outras redes automotivas, como as redes CAN, LIN e FlexRay.

No entanto, além dessas características, a Time-Sensitive Networking (TSN) desempenha um papel crucial na evolução das redes automotivas. O TSN é um conjunto de padrões em desenvolvimento pelo grupo de trabalho IEEE 802.1 TSN, que visa fornecer comunicação determinística e de alta confiabilidade em redes Ethernet. Ele inclui recursos como sincronização de tempo, priorização de tráfego e controle de latência, tornando-o adequado para aplicações industriais, automotivas e outras que exigem transmissão precisa e previsível.

Ao todo, este relatório detalha as atividades de laboratório realizadas durante a criação de um setup experimental de redes intra veiculares baseadas em Ethernet automotiva utilizando dispositivos da TSN Systems, especializada em oferecer suporte

para a transição efetiva para o mundo TSN. O objetivo principal foi desenvolver um sistema de detecção de intrusão (IDS) para redes Ethernet automotivas e realizar testes de ataques simulados para avaliar a eficácia do sistema.

2. Trabalhos Relacionados

A detecção de intrusões em redes veiculares é crucial para garantir a segurança cibernética automotiva, especialmente com a crescente conectividade dos veículos modernos. Atualmente, existem alguns métodos tradicionais, como Snort e Suricata, que utilizam conjuntos de regras baseados em texto para monitorar o tráfego de rede e identificar atividades suspeitas. No entanto, essas soluções não são ideais para os microcontroladores embarcados em veículos devido às suas limitações de recursos e à complexidade crescente das redes Ethernet automotivas, particularmente com a introdução do Time-Sensitive Networking (TSN). Para abordar essas limitações, Zihan et al. (2021) propuseram o ETH-IDS, um sistema de detecção de intrusões baseado em Ethernet, otimizado para microcontroladores embarcados. O ETH-IDS converte regras de Snort e Suricata para um formato binário, o que aumenta a eficiência de armazenamento e processamento. Além disso, o ETH-IDS é compatível com a especificação AUTOSAR, melhorando a detecção de ataques Ethernet em redes veiculares.

O trabalho de Zihan et al. destaca a importância de um sistema eficiente de IDS em redes Ethernet automotivas, especialmente considerando as especificações de TSN que exigem comunicação determinística e de alta confiabilidade. Eles desenvolveram um modelo abrangente de avaliação para o ETH-IDS, considerando desempenho, funcionalidade e aplicabilidade. Em conclusão, os experimentos mostraram que o ETH-IDS oferece melhor utilização da CPU e da memória em comparação com o Suricata, validando sua eficácia em ambientes embarcados.

3. Arquitetura Proposta

Neste trabalho, desenvolvemos um sistema de Detecção de Intrusões (IDS) para redes Ethernet veiculares, utilizando uma abordagem baseada em redes neurais LSTM (Long Short-Term Memory). A arquitetura do sistema é composta por estas seguintes etapas fundamentais:

- Condução dos ataques de modificação de pacote no tráfego Ethernet: Os ataques foram conduzidos utilizando modificadores de fluxo de pacotes que simulam erros típicos em sistemas TSN. Os tipos de ataques incluídos foram:
    1. Drop: Simulação de queda de pacotes na rede Ethernet.
    2. Delay: Introdução de atrasos na transmissão dos pacotes.
    3. Out-of-Sequence: Troca da ordem de pacotes na transmissão.
    4. Transmit Timestamp Jitter: Adição de ruído aleatório aos tempos de transmissão dos pacotes.
- Coleta de Dados: Inicialmente, realizamos a coleta de dados a partir dos dispositivos Ethernet distribuídos pela rede veicular. Utilizamos o TSN Tools para captura e gravação dos pacotes Ethernet, essenciais para a análise subsequente.
- Pré-processamento: Os dados coletados passaram por um processo de

pré-processamento que incluiu uma normalização para garantir consistência nos dados e a segmentação adequada para facilitar o treinamento dos modelos.

- Construção e Treinamento dos Modelos LSTM: Implementamos modelos LSTM supervisionados e não-supervisionados. Esses modelos foram projetados especificamente para analisar o tráfego de rede Ethernet veicular e identificar comportamentos anômalos que possam indicar ataques. O treinamento dos modelos foi realizado utilizando conjuntos de dados separados para treino, validação e teste.
- Avaliação dos Modelos: Após o treinamento, os modelos foram avaliados utilizando métricas como acurácia, precisão e recall. Essas métricas foram essenciais para avaliar o desempenho na detecção de intrusões em ambiente controlado.

4. Metodologia e Validação Experimental

4.1 Datasets

Para avaliar o sistema de Detecção de Intrusões (IDS) proposto, geramos cinco conjuntos de dados que representam diferentes tipos de tráfego na rede Ethernet veicular. Esses dados incluem um tráfego benigno e quatro tráfegos maliciosos, um para cada tipo de ataque, cobrindo uma variedade de cenários de ataque identificados anteriormente.

4.2 Pré-processamento e Dados de Treinamento, Validação e Teste

Os dados foram pré-processados usando a técnica de normalização MinMaxScaler para garantir que todas as características estivessem dentro do mesmo intervalo, facilitando o treinamento dos modelos LSTM. Posteriormente, os dados foram divididos em janelas de tempo fixas para capturar a sequência temporal do tráfego Ethernet. Os conjuntos de dados foram divididos da seguinte maneira:

Para o Modelo Supervisionado:

- Treinamento: 75% dos dados totais, usados para ajustar os parâmetros do modelo.
- Validação: 12.5% dos dados, utilizados para ajustar hiperparâmetros e evitar overfitting.
- Teste: 12.5% dos dados, usados para avaliar o desempenho final do modelo. A distribuição das classes foi equilibrada para evitar viés.

Para o Modelo Não-Supervisionado:

Foram exploradas duas configurações de proporções durante os treinamentos, cada uma aplicada a diferentes experimentos:

- Primeira proporção:
  - Treinamento: 40% dos dados benignos.
  - Validação: 10% dos dados benignos.
  - Teste: 50% dos dados benignos + 100% dos dados maliciosos.
- Segunda proporção:
  - Treinamento: Aproximadamente 76% dos dados benignos.

- Validação: Aproximadamente 19% dos dados benignos.
- Teste: Cerca de 5% dos dados benignos + 100% dos dados maliciosos.

4.3 Estrutura do Modelo e Experimentos Realizados

Para o Modelo Supervisionado utilizamos uma LSTM com 50 unidades, seguida por camadas de Dropout, BatchNormalization e uma camada densa com regularização L2. O modelo foi treinado com o otimizador Adam, utilizando uma taxa de aprendizado de 0.004 e a função de perda MSE.

Já para o Modelo Não-supervisionado implementamos um autoencoder LSTM composto por uma LSTM para codificação, seguida por RepeatVector e uma LSTM para decodificação. O modelo também inclui camadas de Dropout e BatchNormalization. Além disso, ele foi treinado com o otimizador Adam, usando a função de perda MSE.

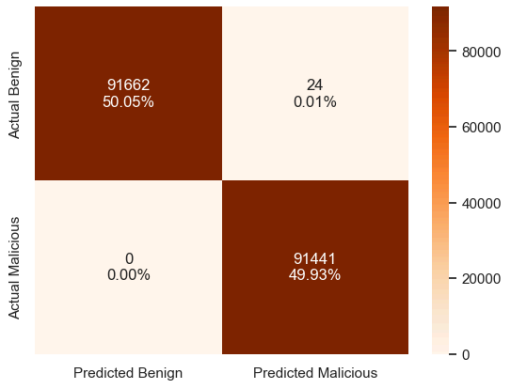
No geral, ambos os modelos foram configurados com callbacks para Early Stopping visando evitar overfitting durante o treinamento.

5. Resultados e Discussões

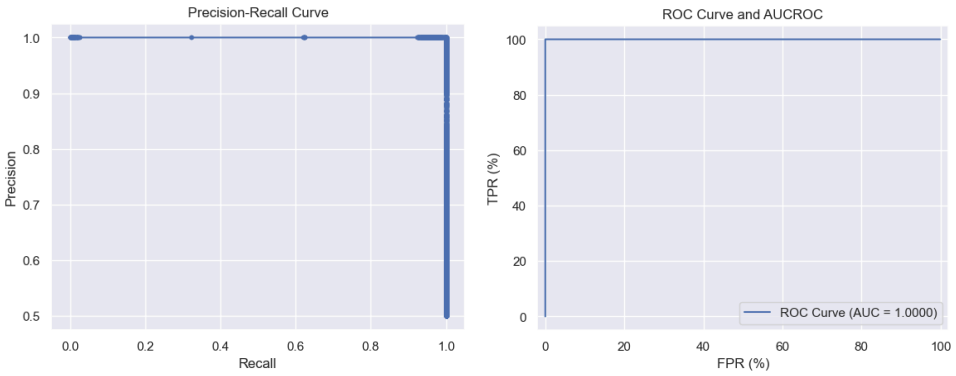
O modelo supervisionado foi avaliado utilizando a função get_overall_metrics(test_labels, predicts_1d), e os resultados obtidos foram os seguintes:

- Acurácia (acc): 0.999868943410857
- Taxa de Verdadeiro Positivo (TPR): 1.0
- Taxa de Falso Positivo (FPR): 0.0002617629736273804
- Precisão: 0.9997376045481878
- F1-Score: 0.999868785058992

Esses resultados indicam um desempenho quase perfeito do modelo supervisionado, com uma taxa de verdadeiros positivos e precisão extremamente altas. A taxa de falso positivo, embora muito baixa, ainda é não-nula, o que sugere que o modelo pode ocasionalmente classificar incorretamente alguns pacotes legítimos como ataques.



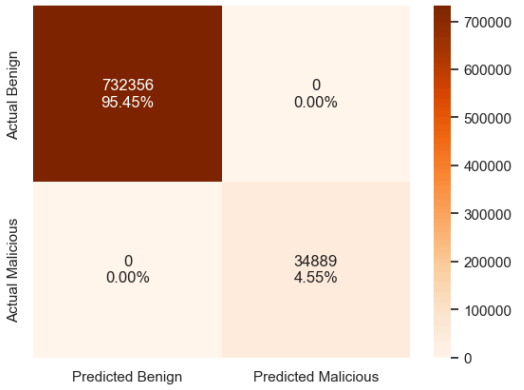
Além disso, também geramos os gráficos de Curva Recall e ROC:

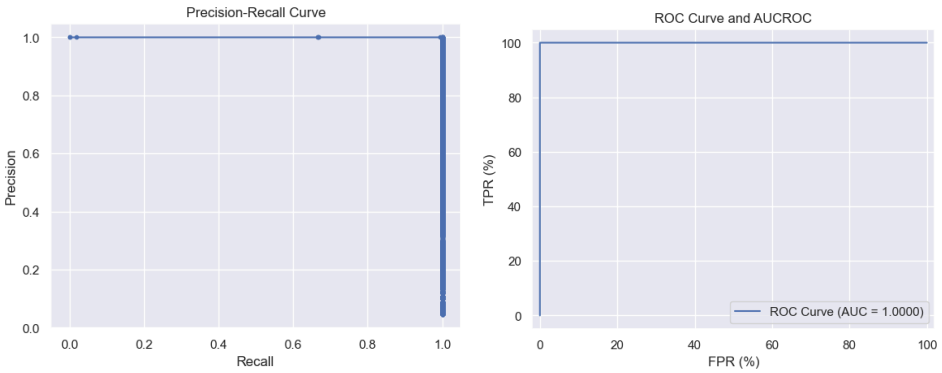


O modelo não-supervisionado foi avaliado utilizando a função get_overall_metrics(test_data_2_labels, reconstruction_errors_rounded), e os resultados obtidos foram os seguintes:

- Acurácia (acc): 1.0
- Taxa de Verdadeiro Positivo (TPR): 1.0
- Taxa de Falso Positivo (FPR): 0.0
- Precisão: 1.0
- F1-Score: 1.0

Os resultados deste modelo sugerem que ele consegue identificar todos os ataques corretamente, sem nenhum falso positivo. Além disso, as curvas Recall e ROC indicam sua eficácia na detecção de anomalias sem erros.





Comparativamente, ambos os modelos apresentam um desempenho extremamente alto na detecção de ataques. No entanto, o modelo supervisionado pode

ser mais facilmente ajustável para diferentes tipos de ataques específicos devido à disponibilidade de dados rotulados. Isso permite que o modelo supervisionado aprenda características específicas de cada tipo de ataque, tornando-o potencialmente mais robusto em cenários variados.

Em contrapartida, o modelo não-supervisionado não requer dados rotulados para o treinamento, o que é uma vantagem significativa em ambientes onde a rotulagem é impraticável ou demorada. Além disso, o modelo não-supervisionado mostrou-se capaz de detectar anomalias com perfeição no conjunto de testes fornecido, sugerindo uma excelente capacidade de generalização.

Em conclusão, o modelo supervisionado apresentou uma leve taxa de falso positivo, que pode ser minimizada com técnicas de balanceamento de dados ou ajuste de hiperparâmetros. Já no modelo não-supervisionado, a validade dos resultados perfeitos deve ser confirmada com testes adicionais em diferentes cenários de ataque e em datasets mais variados.

6. Conclusão e Trabalhos Futuros

Neste trabalho, nós desenvolvemos e avaliamos um Sistema de Detecção de Intrusões (IDS) baseado em redes neurais para redes veiculares Ethernet, focando na detecção de ataques por modificação de pacotes. Utilizamos modelos supervisionados e não supervisionados, que demonstraram alta eficácia na identificação de intrusões.

Os modelos supervisionados apresentaram métricas de desempenho notáveis, como precisão, taxa de verdadeiros positivos e taxa de falsos positivos. Da mesma forma, os modelos não supervisionados mostraram uma performance robusta, alcançando altos índices de detecção de ataques sem a necessidade de rótulos nos dados de treinamento.

Contudo, reconhecemos a necessidade de ampliar o conjunto de dados, incorporando mais cenários de ataque e realizando testes em ambientes de tráfego real para validação adicional.

Para trabalhos futuros, pensamos em explorar diferentes configurações e parâmetros dos modelos utilizados. Além disso, há também a integração com outras técnicas de segurança que podem ser investigadas para fortalecer ainda mais a proteção das redes veiculares. Esses avanços podem contribuir para melhorar a segurança cibernética em veículos, garantindo a detecção eficiente e precisa de intrusões em diferentes condições operacionais.

Referências

Araújo, R., & Silva, M. (2023). Automotive Ethernet: Architecture and Security Challenges and Technologies. International Journal of Electrical and Computer Engineering (IJECE), 13(5), 5209-5221. http://dx.doi.org/10.11591/ijece.v13i5.pp5209-5221.

P. Hank, S. Müller, O. Vermesan and J. Van Den Keybus, "Automotive Ethernet: In-vehicle networking and smart mobility," 2013 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 2013, pp. 1735-1739,

doi: 10.7873/DATE.2013.349.

R. Duo, X. Nie, N. Yang, C. Yue and Y. Wang, "Anomaly Detection and Attack Classification for Train Real-Time Ethernet," in IEEE Access, vol. 9, pp. 22528-22541, 2021, doi: 10.1109/ACCESS.2021.3055209.

Z. Zihan, C. Lirong, Z. Haitao and Z. Fan, "Research on Intrusion Detection Technology Based on Embedded Ethernet," 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 2021, pp. 587-600, doi: 10.1109/ICCWAMTIP53232.2021.9674069.