Detecção de Intrusões em Redes CAN com Machine Learning  
 precision recall f1-score support

BENIGN 0.99955 0.96077 0.97978 200000

DoS 0.94556 1.00000 0.97202 132437

Fuzzy 0.99782 0.99911 0.99846 98369

RPM 0.99999 1.00000 1.00000 130980

gear 0.99995 1.00000 0.99997 119450

accuracy 0.98835 681236

macro avg 0.98857 0.99198 0.99005 681236

weighted avg 0.98896 0.98835 0.98840 681236

Gráfico, Gráfico de linhas

O conteúdo gerado por IA pode estar incorreto.

Gráfico, Gráfico de linhas

O conteúdo gerado por IA pode estar incorreto.

Gráfico

O conteúdo gerado por IA pode estar incorreto.

Gráfico, Gráfico de linhas, Gráfico de dispersão

O conteúdo gerado por IA pode estar incorreto.  
  
Vou ter dizer oque eu fiz e vc me da sugestão das coisas.

Eu peguei esse dataset 'Car-Hacking Dataset'

Abstract

As modern vehicles have lots of connectivity, protecting in-vehicle network from cyber-attacks becomes an important issue. Controller Area Network (CAN) is a de facto standard for the in-vehicle network. But, lack of security features of CAN protocol makes vehicles vulnerable to attacks. The message injection attack is a representative attack type which injects fabricated messages to deceive original ECUs or cause malfunctions. Thus we open our datasets to the public to foster further car security research.

Que tem esses ataques:

Attack Type # of messages # of normal messages # of injected messages

DoS Attack 3,665,771 3,078,250 587,521

Fuzzy Attack 3,838,860 3,347,013 491,847

Spoofing the

drive gear 4,443,142 3,845,890 597,252

Spoofing the

RPM gauze 4,621,702 3,966,805 654,897

GIDS: Attack-free

(normal) 988,987 988,872 -

e adicionei os ataques de DOS e normal desse dataset 'CIC IoV dataset 2024'  
The main goal of this research is to propose a realistic benchmark dataset to support the development of new cybersecurity solutions for internet of vehicles (IoV) operations. To accomplish this, five attacks were executed against the fully intact inner structure of a 2019 Ford car, complete with all Electronic Control Units (ECUs). However, the vehicle was rendered immobile and incapable of causing any potential harm or injuries. Hence, all attacks were carried out on the vehicle without endangering the car's driver or passengers.

These attacks are classified as spoofing and Denial-of-Service (DoS) and were carried out through the CAN-BUS protocol. This effort establishes a baseline complementary to existing contributions and supports researchers to propose new IoV solutions to strengthen the overall security using different techniques (e.g., Machine Learning - ML).

Depois de juntar os dois fazendo todo o processamento dos dados, treinei um modelo de mlpo do skit learning. E consegui esses resultados:

precision recall f1-score support

BENIGN 0.99955 0.96077 0.97978 200000

DoS 0.94556 1.00000 0.97202 132437

Fuzzy 0.99782 0.99911 0.99846 98369

RPM 0.99999 1.00000 1.00000 130980

gear 0.99995 1.00000 0.99997 119450

accuracy 0.98835 681236

macro avg 0.98857 0.99198 0.99005 681236

weighted avg 0.98896 0.98835 0.98840 681236