한모코(HMC) 학습일지

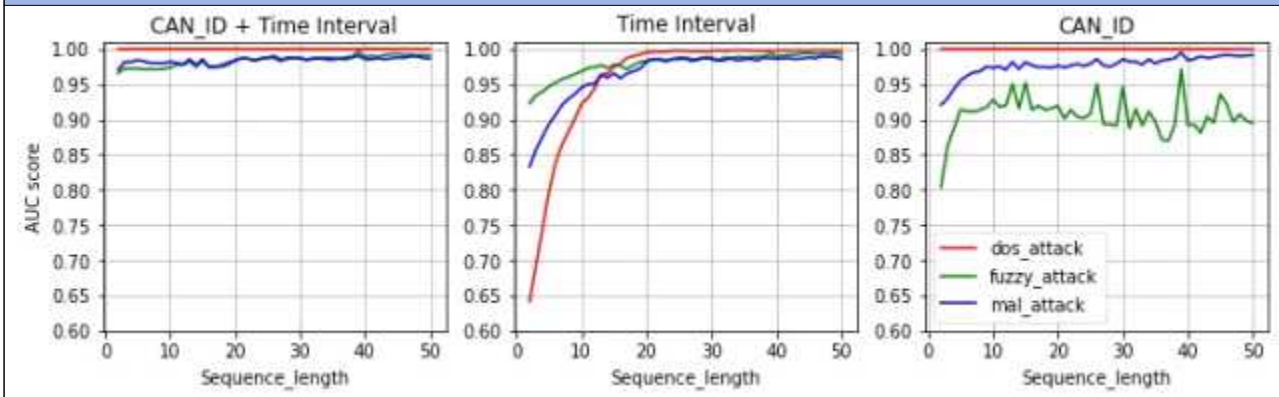
이름	유수경	학번	20205209
날짜	2022.10.31.		

학습 계획

< IVN_Dataset " IVN_HYSonata_Driving " >

- 현대 소나타 차량의 주행 중 공격 데이터셋을 Python 언어로 분석 후 시각화
- DoS, Fuzzy, MalFunction, Free 상태의 차량 주행 데이터를 분석하여 그래프로 시각화하고 각 공격과 공격이 들어오지 않은 상태를 비교하면서 공격 주입 시점을 분석하는 활동을 진행.
- 팀원들끼리 각 CAN ID를 7개씩 맡아 분석을 진행하였다.
- 내가 맡은 CAN ID는 0A0, 0A1, 18F, 1F1, 2A0, 2B0, 2C0 이다.

학습 내용



- CAN ID + Time Interval

DoS 공격

에서는 CAN ID '000'의 존재 여부가 곧 클래스를 의미하므로 탐지 모델 역시 해당 CAN ID '000'이 있는지를 학습하여 Sequence 길이와 상관없이 AUC score가 모두 1.0을 기록.

Malfunction 및 Fuzzy 공격에서는 CAN ID Sequence와 Time interval Sequence를 동시에 사용했을 때, 짧은 Sequence 길이가 3으로 설정되더라도 약 0.98 AUC score에 수렴하는 것을 확인.

- Time Interval

Sequence 길이 20에서부터 높은 탐지 성능을 달성.

Time interval 그래프와 같이 Sequence 길이가 증가할수록 (최대 50) 성능이 지속적으로 증가함을 확인.

- CAN ID

DoS 공격의 경우 AUC score가 약 1.0으로 가장 높은 성능을 달성.

추가로, Malfunction 공격 및 Fuzzy 공격에서는 DoS 공격에서와는 다르게 특정한 CAN ID를 번갈아 설정하여 공격 또는 랜덤하게 CAN ID와 Data Field Value를 설정하기 때문에, AUC 성능이 DoS 공격의 탐지 성능보다 낮음을 확인.

Malfunction 공격의 경우, 공격에서 사용한 CAN ID가 2가지이고, CAN ID Sequence가 Fuzzy 공격에서보다 유사한 경우가 많아서 Fuzzy 공격에서의 침입 탐지 성능보다 높음을 확인하였다.