한모코(HMC) 학습일지

이름	서영재	학번	20195178
날짜	2022.10.31.		

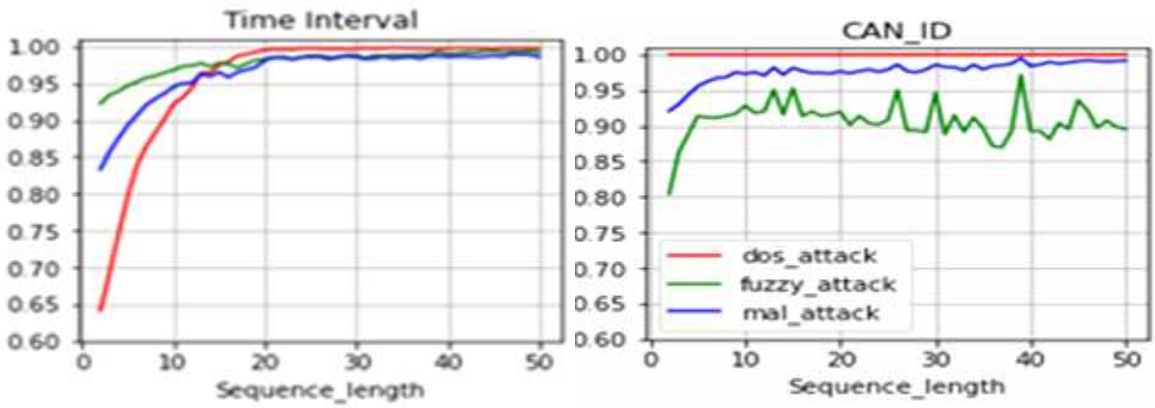
학습 계획

< 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.
- Time Interval Sequence + CAN ID Sequence 피처들에 대한 AUC Score을 구했다.
- Sequence 길이를 2부터 50까지 지정하여 각 길이에 따른 데이터 구축

학습 내용

- Sequence 길이를 2부터 50까지 지정하여 각 길이에 따른 데이터 구축하였다.
- 지난 주에 한 Time Interval Sequence + CAN ID Sequence 피처들에 대한 성능과 비교하기 위해, Time interval Sequence 및 CAN ID Sequence를 단일 피처로 적용하여 AUC 성능을 보았다.



- **Time interval Sequence 단일 적용**

  공격이 주입될 시, Time Interval의 값이 낮아지고 확인 결과 정상 데이터와 공격 데이터 값 차이가 일반적으로 발생하므로 학습이 가능. 이때 Sequence 길이 20부터 높은 탐지성능을 달성함.

- **CAN ID Sequence 단일 적용**

  DoS 공격의 경우 4.4.1에 기술한 이유로 AUC score가 약 1.0으로 가장 높은 성능을 달성함

  Malfunction 및 Fuzzy 공격은 특정한 CAN ID를 번갈아 설정하거나 랜덤한 CAN ID 와 Date Field value를 설정하기 때문에 DoS공격보다 AUC 성능이 낮음을 확인함.

  Malfunction 공격의 경우 CAN ID Sequence가 Fuzzy 공격 에서보다 유사한 경우가 많아서 Fuzzy 공격에서의 침입 탐지성능보다 높음을 확인함.