한모코(HMC) 학습일지

이름	서영재	학번	20195178
날짜	2022.10.12		

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 329, 350, 370, 430, 440, 545, 690이다.

학습 내용

* 해당 데이터셋 파일(csv)을 CAN 프레임(TimeStamp, CAN ID, DCL, DataField, Temp) 기준으로 인덱싱 후, TimeWindow와 TimeInterval 컬럼을 추가해주었다.

* TimeStamp 값을 상대시간으로 표현하고 TimeStamp 값의 차이를 계산해주는 함수 작성을 한 뒤, TimeStamp 상대시간 값을 TimeWindow에, TimeStamp의 차이 값을 TimeInterval에 넣었다.

- 여기서 TimeStamp 값을 상대시간으로 표현하는 코드는

```
loss = df.loc[i, 'TimeStamp']- df.loc[1, 'TimeStamp']
```

이와 같다.

- TimeStamp 값의 차이(TimeInterval)를 계산해주는 코드는

```
df.loc[i, 'TimeInterval']= df.loc[i-1, 'TimeInterval']+ loss
```

이와 같다.

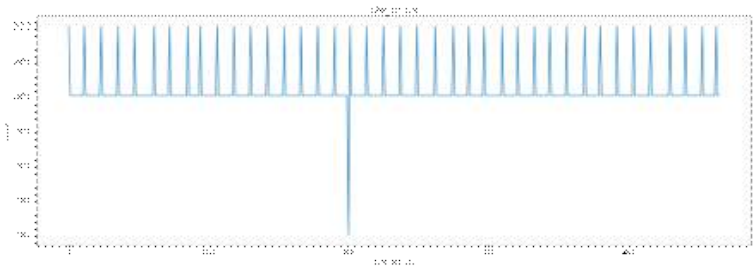
< csv 파일을 불러와서 데이터에 인덱싱을 해준 후, 새로운 컬럼 추가 및 계산해준 값을 나타낸 화면 >

	Unnamed: 0	index	TimeStamp	CAN_ID	DLC	DataField	TimeWindow	TimeStack
0	0	5	1.513924e+09	2B0	5	E9 FF 00 07 22	0.000000	0.000000
1	1	11	1.513924e+09	18F	8	FE 49 00 00 00 3C 00 00	0.003490	0.003490
2	2	13	1.513924e+09	2A0	8	60 00 72 1D 0B 05 E3 00	0.000460	0.003950
3	3	16	1.513924e+09	2C0	8	14 00 00 00 00 00 00 00	0.001385	0.005335
4	4	19	1.513924e+09	1F1	8	00 C5 00 00 00 00 00 00	0.003366	0.008701
...	...	...	...	...	...	...	...	...
164761	164761	928821	1.513924e+09	18F	8	FE 3C 00 00 00 50 00 00	0.003043	351.287880
164762	164762	928824	1.513924e+09	2A0	8	20 00 77 1D 0B 05 E3 00	0.000724	351.288604
164763	164763	928836	1.513924e+09	1F1	8	00 3C 55 50 05 55 50 05	0.002966	351.291570
164764	164764	928847	1.513924e+09	2B0	5	53 FF 02 07 21	0.002764	351.294334
164765	164765	928849	1.513924e+09	2C0	8	14 00 00 00 00 00 00 00	0.000559	351.294893

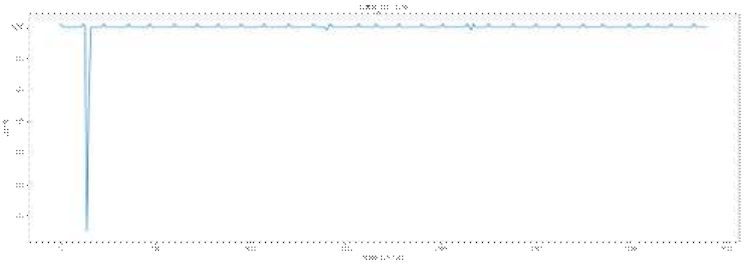
164766 rows × 8 columns

< CAN ID ‘329’의 데이터 >

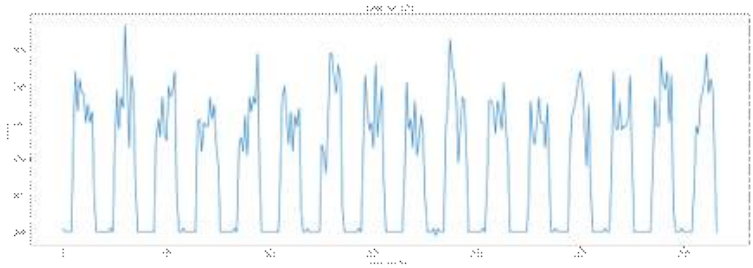
● Free 상태 시각화



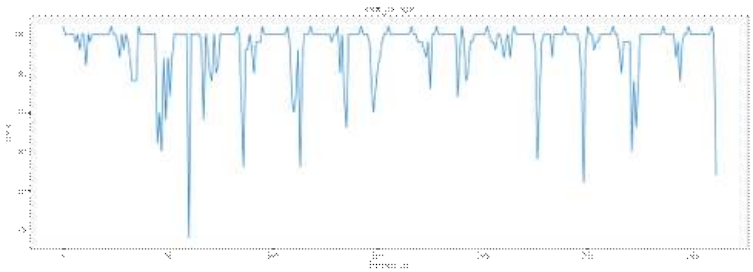
● Dos 공격 상태 시각화



● Fuzzy 공격 시각화

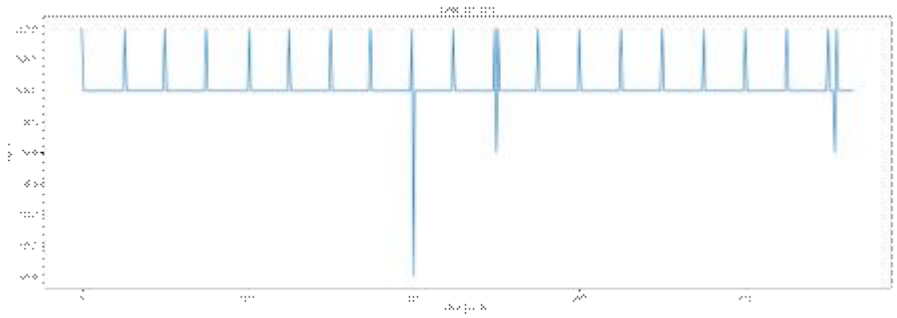


● MalFunction 상태 시각화

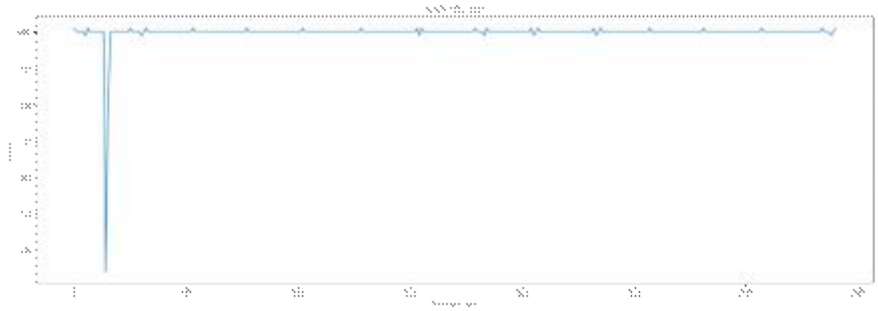


< CAN ID ‘350’의 데이터 >

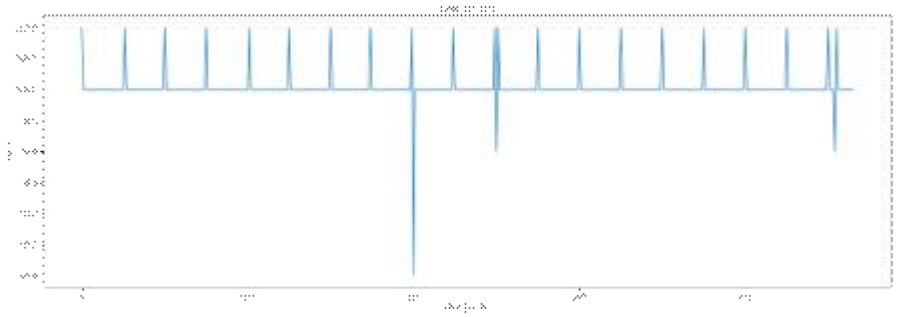
● Free 상태 시각화



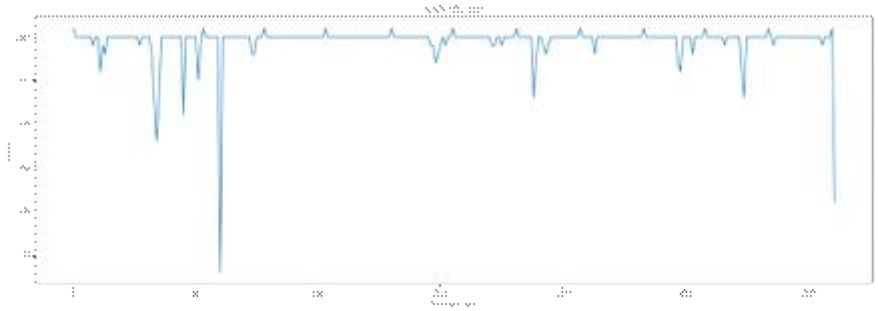
● Dos 공격 상태 시각화



● Fuzzy 공격 시각화

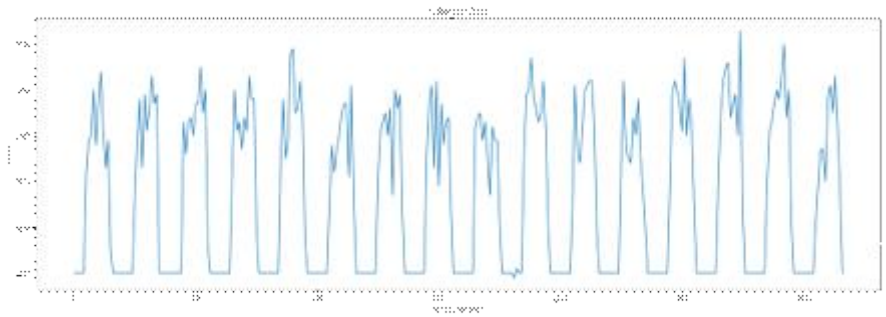


● MalFunction 상태 시각화

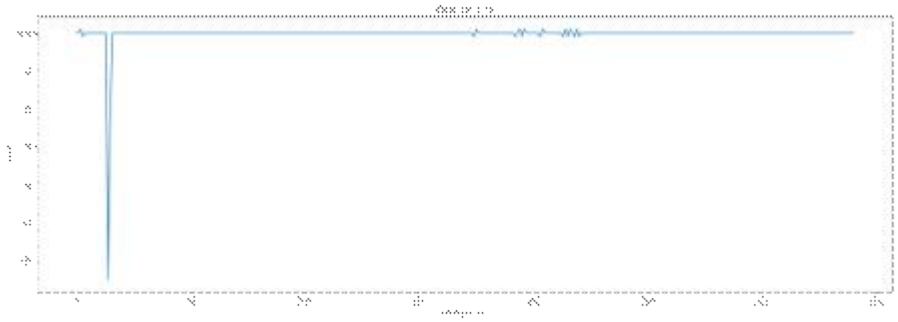


< CAN ID ‘370’의 데이터 >

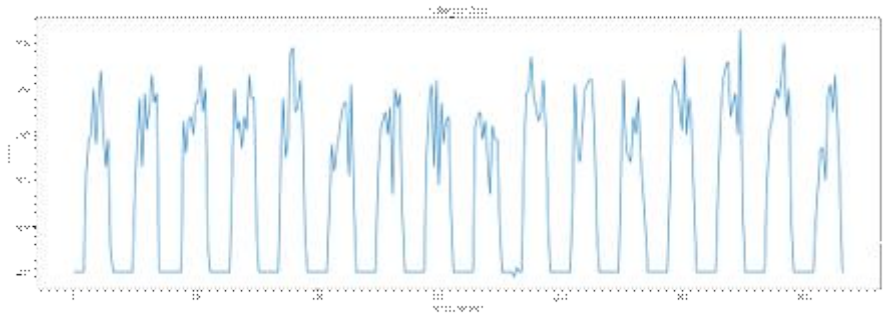
● Free 상태 시각화



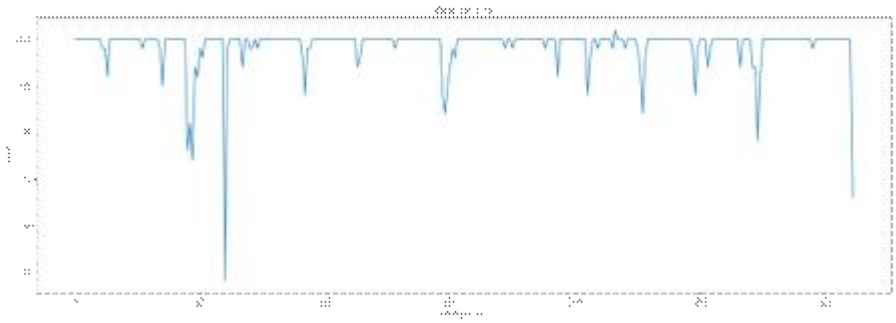
● Dos 공격 상태 시각화



● Fuzzy 공격 시각화

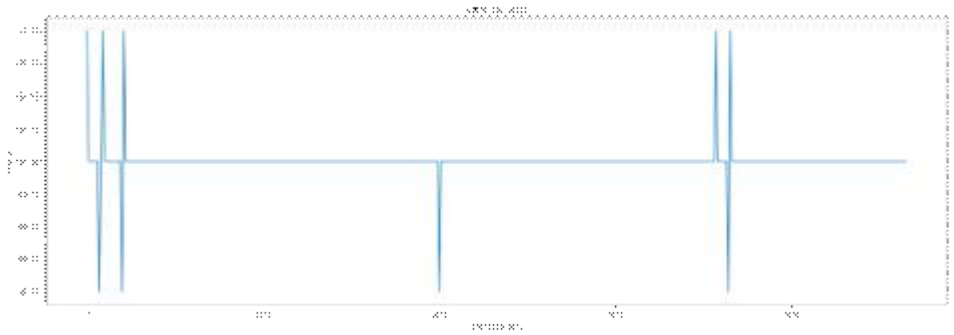


● MalFunction 상태 시각화

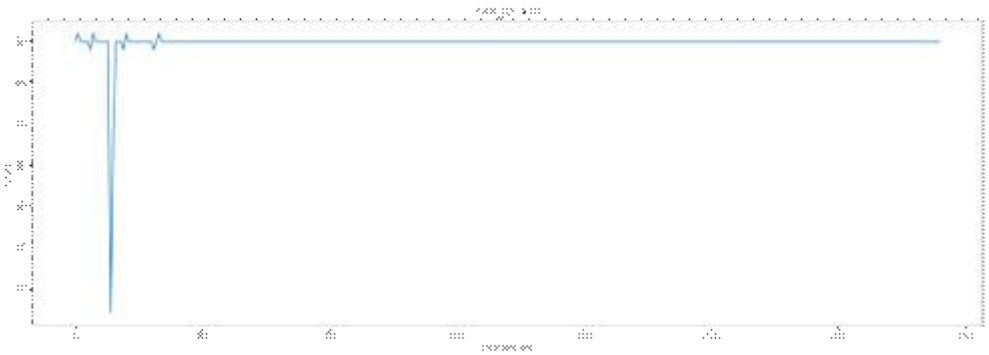


< CAN ID ‘430’의 데이터 >

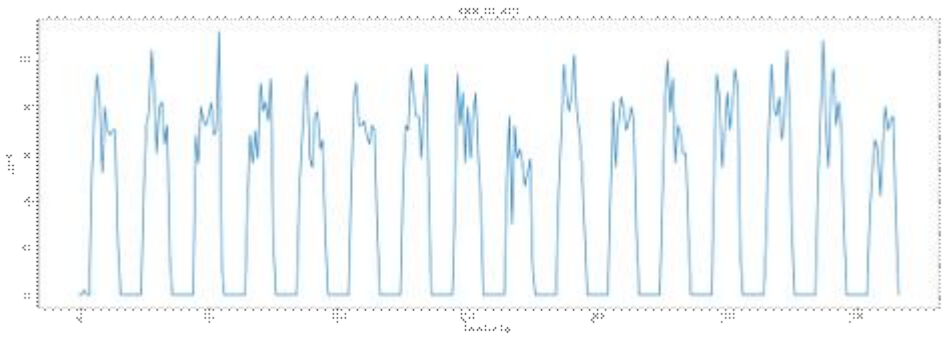
● Free 상태 시각화



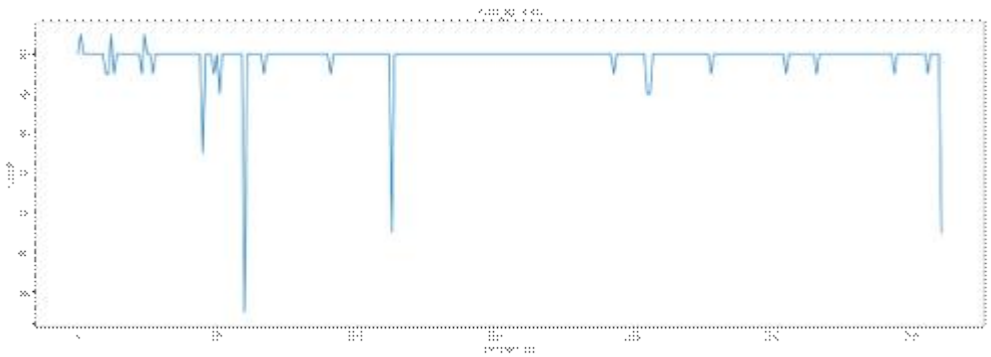
● Dos 공격 상태 시각화



● Fuzzy 공격 시각화

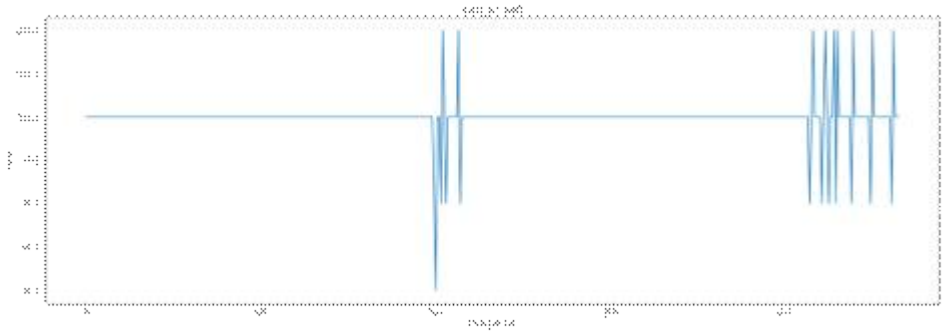


● MalFunction 상태 시각화

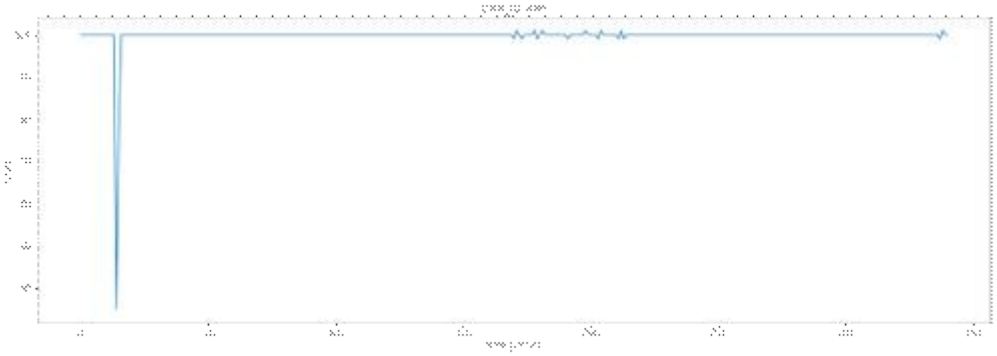


< CAN ID ‘440’의 데이터 >

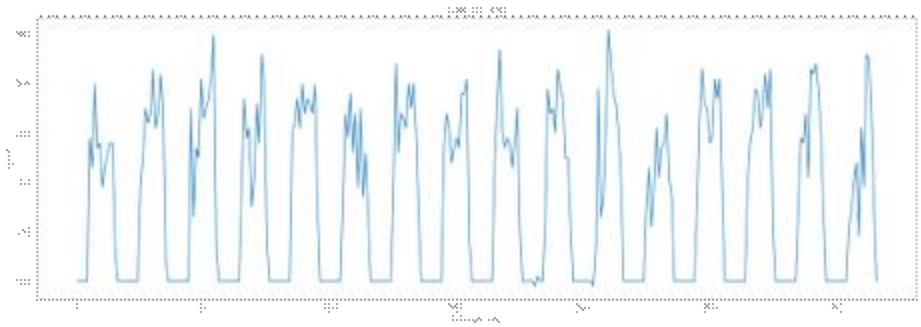
● Free 상태 시각화



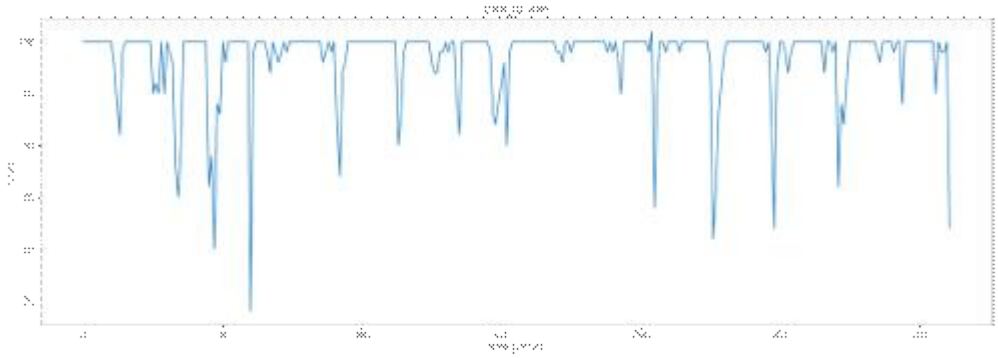
● Dos 공격 상태 시각화



● Fuzzy 공격 시각화

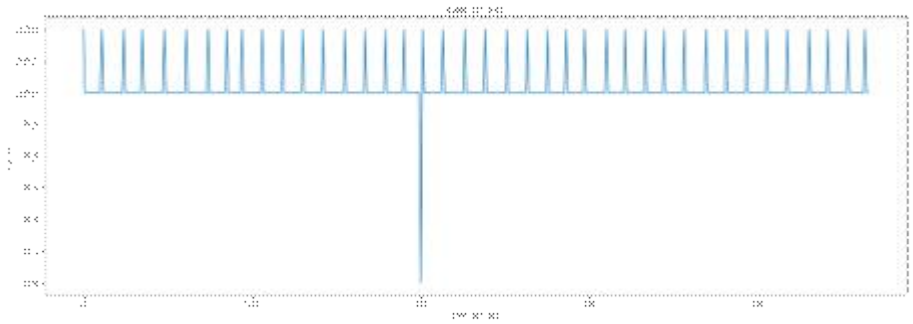


● MalFunction 상태 시각화

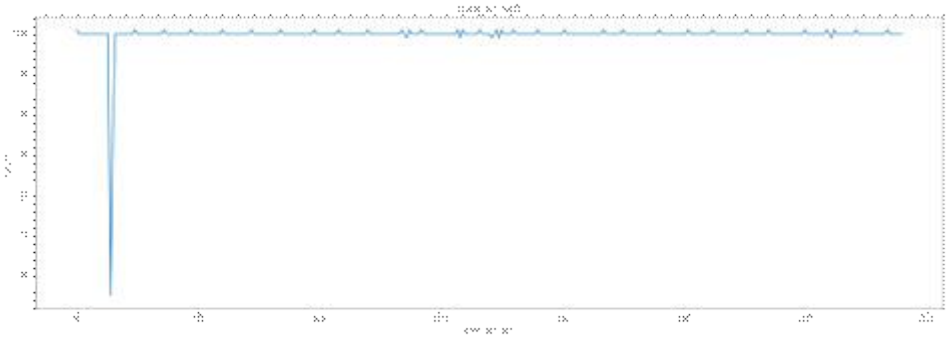


< CAN ID ‘545’의 데이터 >

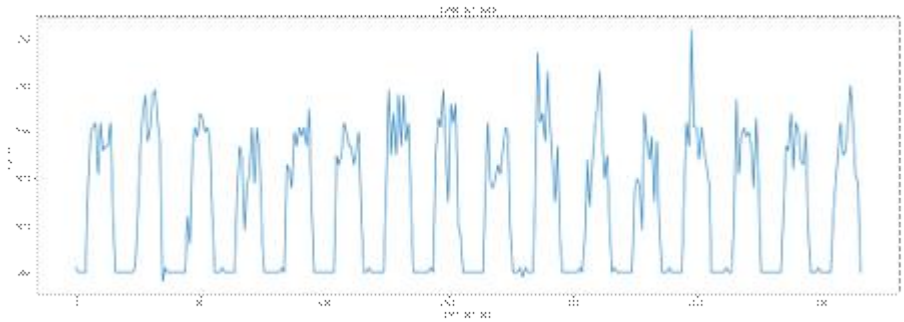
● Free 상태 시각화



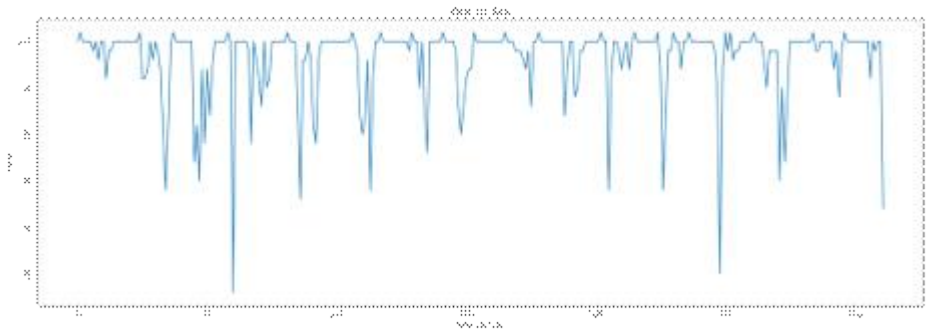
● Dos 공격 상태 시각화



● Fuzzy 공격 시각화

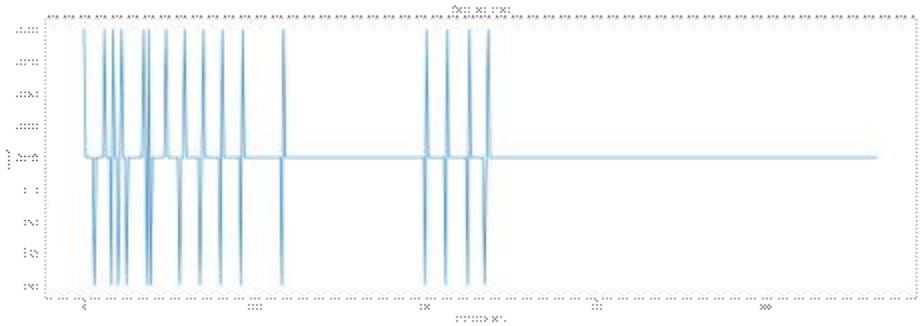


● MalFunction 상태 시각화

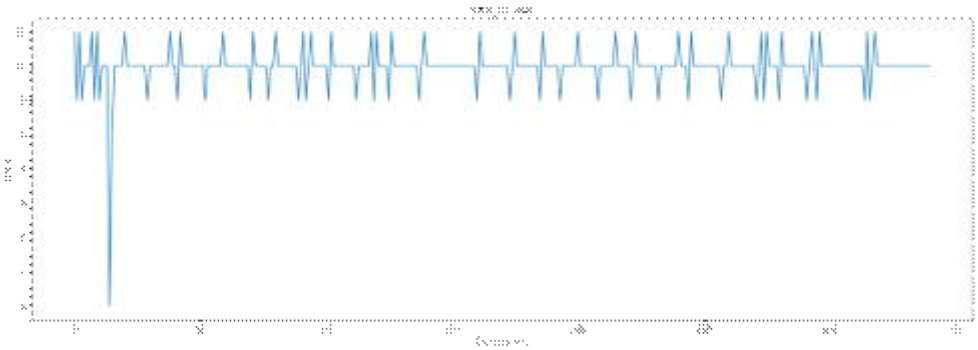


< CAN ID ‘690’의 데이터 >

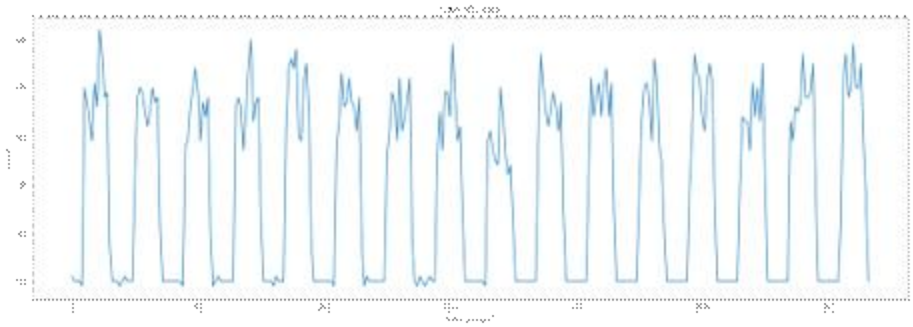
● Free 상태 시각화



● Dos 공격 상태 시각화



● Fuzzy 공격 시각화



● MalFunction 상태 시각화