**사이버 보안 챌린지 2020**

**자동차 해킹 공격/방어”**

**예선 데이터셋 설명**

**목차**

[1 챌린지 문제 3](#_Toc50740676)

[2 차량 내부 네트워크 데이터셋 3](#_Toc50740677)

[2.1 기본정보 3](#_Toc50740678)

[2.1.1 파일 정보 3](#_Toc50740679)

[2.1.2 추출 환경 3](#_Toc50740680)

[2.1.3 정상 파일 4](#_Toc50740681)

[2.1.4 공격 종류 4](#_Toc50740682)

[2.1.5 공격 영향 5](#_Toc50740683)

[2.2 학습용 데이터셋 - CAN data 5](#_Toc50740684)

[2.2.1 학습용 데이터셋의 파일 및 SubClass별 row 수 6](#_Toc50740685)

[2.3 제출용 데이터셋 및 탐지결과 제출 양식 6](#_Toc50740686)

[2.3.1 제출용 데이터셋의 파일 및 row 수 7](#_Toc50740687)

# 챌린지 문제

온라인 평가플랫폼에 접속하여 제시된 차량 내부 네트워크(CAN) 데이터 셋을 분석하여 공격 탐지 결과(csv)를 제시하는 것이 주요 목표입니다. 이를 위해, 공격을 탐지할 수 있는 알고리즘을 개발해야 하며, 알고리즘은 머신 러닝, AI 기반 등 형태에 제한은 없으나, 프로그램으로 구현 및 자동화가 가능해야 합니다.

# 차량 내부 네트워크 데이터셋

## 기본정보

### 파일 정보

데이터셋은 학습용과 제출용으로 나누어져 있으며, 학습용 데이터셋의 경우 대회에서 선정한 2020 아반떼 CN7 차량에 대해, 정차(S) 중 추출한 3개 파일과 주행(D) 중에 추출한 3개 파일로 구성됩니다. 제출용 데이터셋은 레이블링 (Class)을 제외한 내용으로 이뤄지며, 정차와 주행 중에 추출한 2개 파일로 구성됩니다. 압축 해제 시 학습용 데이터셋은 213 MB, 제출용 데이터셋은 198 MB입니다.

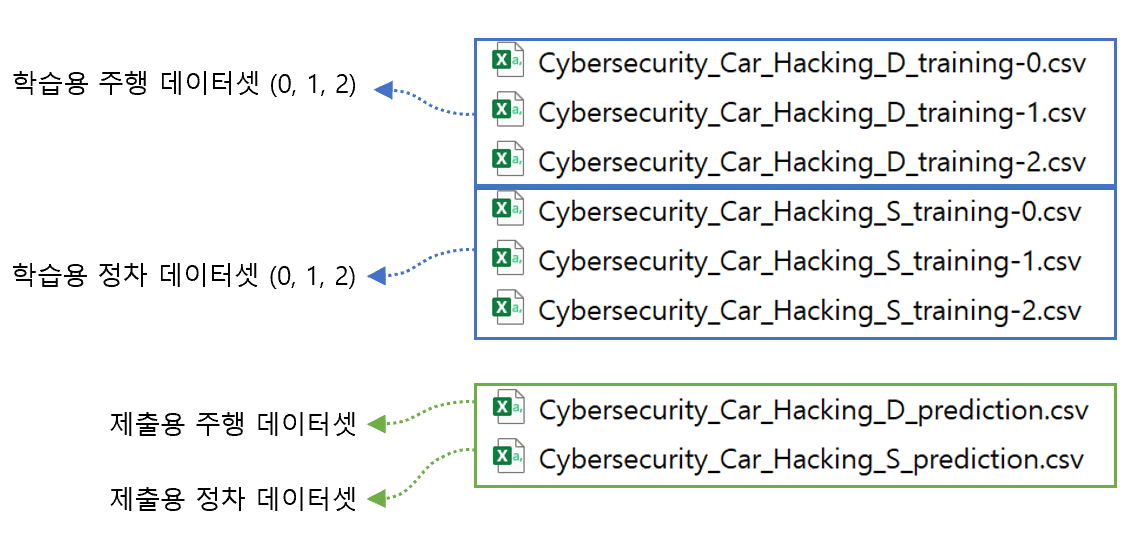
****

Figure . 데이터셋 파일 구성

### 추출 환경

차량의 정차 상태와 주행 상태의 정의는 다음과 같습니다.

* 정차: 주차된 상태에서 시동을 켠 상태로, 차량의 바퀴가 움직이지 않는 상태 (핸들 움직임이나 기어 변화 등은 포함될 수 있음)
* 주행: 운전을 하여 차량이 움직이고 있는 상태

차량에서 추출한 데이터는 CAN(Controller Area Network)에 흐르는 메시지입니다. CAN은 국제 표준 규격으로 채택되어 차량용 통신으로 널리 쓰이는 네트워크 시스템입니다. 차량 내부에서 CAN은 설계에 따라 C-CAN, B-CAN, CCP-CAN 등 여러 개의 네트워크로 구성될 수 있습니다. 본 예선 데이터셋은 아반떼 CN7 차량의 **C-CAN**에 흐르는 메시지를 추출한 것입니다. C-CAN에는 다음과 같은 제어기가 연결되어 있습니다.

* 계기판
* 차선 이탈 방지 보조 유닛
* 운전자 주차 보조 제어기 유닛
* MDPS 유닛
* 에어백 컨트롤 모듈
* 후측방 충돌 경고 유닛
* 후방 카메라
* VDC 모듈
* 전방 충돌 방지 보조 유닛

### 

### 정상 파일

* 차량 CAN bus의 공격 상황과 비교를 위해, 정상 CAN bus traffic을 제공합니다. 학습용 0번 파일(“\*\_training-0.csv”) 2개가 이에 해당합니다. 각각 약 1분 ~ 1분 20초 정도의 트래픽을 정차/주행 상태에서 추출하였습니다.

### 공격 종류

* Flooding Attack
  + CAN bus는 여러 개의 제어기들이 CAN 메시지를 송신할 때, Arbitration ID의 우선순위를 통해 송신하는 CAN 메시지를 선택하게 됩니다. (Arbitration ID의 우선순위는 그 값이 낮을 경우, 더 높은 우선순위를 가지게 됩니다.)
  + 이를 악용하여 높은 우선순위의 CAN 메시지를 대량 전송하는 공격입니다.
* Spoofing Attack
  + Spoofing Attack은 차량의 특정 Arbitration ID를 대상으로 수행하게 됩니다.
  + 공격자는 사전에 Arbitration ID을 자동차 기능에 대해 리버싱하여, 공격자가 원하는 기능을 수행하도록 CAN 메시지를 생성하여 주입하는 공격입니다.
* Replay Attack
  + 특정 시간 동안 CAN bus의 정상 CAN traffic을 추출하여, CAN bus에 그대로 주입하는 공격입니다.
* Fuzzing Attack
  + 차량의 정상 Arbitration ID 중 임의로 선택한 ID에 무작위 값을 매번 설정하여 주입하는 공격입니다.
  + 공격의 목적은 차량의 이상을 일으키기 위한 것으로, 차량의 특정 기능에 대한 공격이 아니기 때문에, 무작위로 CAN 메시지를 주입합니다.

### 공격 영향

* Flooding Attack
  + Flooding Attack 수행 시, 공격의 영향으로 CAN bus의 네트워크 대역폭에 대한 점유율을 높여, 정상 CAN 메시지의 전송을 방해합니다.
* Spoofing Attack
  + Spoofing Attack 수행 시, 공격의 영향으로 실험용 차량의 계기판에 “공장 모드” 출력과 “RPM” 부분의 변화가 일어납니다. (제출용 데이터셋에는 이 외에 다른 액션을 유도하는 공격이 포함되어 있습니다.)
* Replay Attack
  + Replay Attack 수행 시, 공격의 영향으로 계기판의 경고등이 점멸하며, 차량 주행 시 정상 상태와는 다른 주행감이 나타납니다.
* Fuzzing Attack
  + Fuzzing Attack 수행 시, 공격의 영향으로 계기판의 많은 경고등이 점멸하며 주행에 영향을 줄 수 있는 이상현상이 발생합니다.

## 학습용 데이터셋 - CAN data

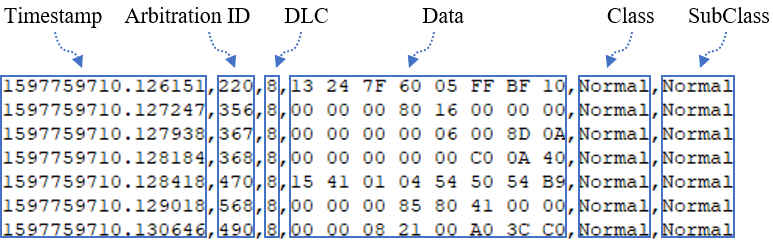


Figure 2. CAN traffic – 학습용

**Timestamp** : CAN Data 덤프 시, 해당 CAN 메시지가 로깅되는 시간

**Arbitration\_ID** : CAN 메시지의 식별 ID

**DLC** : CAN 메시지의 Data field의 크기

**Data** : CAN 메시지의 데이터가 적재된 필드

**Class** : 해당 CAN 메시지의 정상(Normal) 또는 공격(Attack)을 나타내기 위한 필드

* 본 대회에서 제시할 탐지 알고리즘이 분류해야 하는 값

**SubClass** : 공격의 종류를 나타내기 위한 필드

* SubClass는 공격을 구분할 수 있도록 ‘Normal’, ‘Flooding’, ‘Spoofing’, ‘Replay’, ‘Fuzzing’으로 구성됨
* 특성 분석을 위해 추가적으로 제공하는 값으로, 탐지 알고리즘은 Class까지만 분류 가능하도록 구현

### 학습용 데이터셋의 파일 및 SubClass별 row 수

(헤더 제외)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 파일명 | Normal | Flooding | Spoofing | Replay | Fuzzing |
| Cybersecurity\_Car\_Hacking\_D\_training-0.csv | 179,346  (100%) | - | - | - | - |
| Cybersecurity\_Car\_Hacking\_D\_training-1.csv | 733,752  (91.0%) | 38,521  (4.8%) | 988  (0.1%) | 10,509  (1.3%) | 22,620  (2.8%) |
| Cybersecurity\_Car\_Hacking\_D\_training-2.csv | 811,532  (91.2%) | 38,852  (4.4%) | 2,891  (0.3%) | 13,266  (1.5%) | 22,854  (2.6%) |
| Cybersecurity\_Car\_Hacking\_S\_training-0.csv | 180,686  (100%) | - | - | - | - |
| Cybersecurity\_Car\_Hacking\_S\_training-1.csv | 727,749  (91.0%) | 38,151  (4.8%) | 988  (0.1%) | 10,525  (1.3%) | 21,879  (2.8%) |
| Cybersecurity\_Car\_Hacking\_S\_training-2.csv | 739,678  (90.5%) | 38,656  (4.7%) | 2,889  (0.4%) | 13,293  (1.6%) | 22,526  (2.8%) |

## 제출용 데이터셋 및 탐지결과 제출 양식

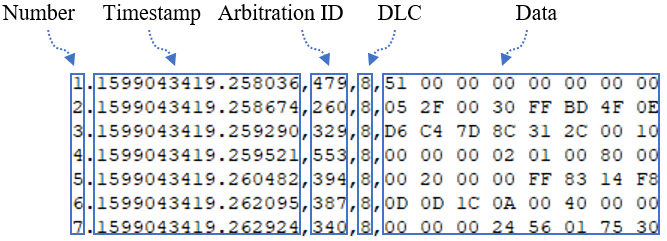


Figure 3. CAN traffic – 제출용

Figure 3과 같이 제출용 데이터셋에는 Class 및 SubClass 필드가 삭제되어 있으며, Timestamp 필드 앞에 각 라인의 번호를 의미하는 ‘Number’ 필드가 추가되어 있습니다. 제출용 데이터셋에 대한 정상/공격 여부를 판단하여, Figure 4와 같이 **‘Number’**와 **‘Class’**를 값을 출력한 탐지결과 파일을 제출하시면 됩니다.

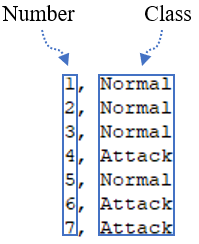


Figure 4. 제출용 데이터셋에 대한 탐지결과 파일

* **‘Number’**는 각 메시지의 식별자이기 때문에 제출용 데이터셋의 ‘Number’와 동일해야 합니다.
* **‘Class’**에는 정상일 경우 **Normal**, 공격일 경우 **Attack**으로 텍스트를 정확히 기재합니다.
* 각 필드가 쉼표(,)로 구분된 CSV 포맷으로 제출해야 하며, 쉼표 앞뒤로 띄워쓰기는 없습니다.
* 제출용 데이터셋은 2개 파일로 구성되어 있지만 답안은 하나의 파일로 합쳐서 제출하여 주시기 바랍니다.

**공격의 세부 유형을 나타내는 SubClass는 탐지결과에 포함하지 않습니다.**즉, 탐지 알고리즘의 출력으로 binary classification을 요구하고 있으며, multiclass classification는 필수적이지 않은 점 유의 바랍니다. 채점 또한 binary classification 기준으로 진행됩니다.

### 제출용 데이터셋의 파일 및 row 수

(헤더 제외)

|  |  |
| --- | --- |
| 파일명 | 전체 (정상 및 공격 데이터 혼합) |
| Cybersecurity\_Car\_Hacking\_D\_prediction.csv | 2,000,733 |
| Cybersecurity\_Car\_Hacking\_S\_prediction.csv | 1,751,313 |