# CAN Bus 보안 강화를 위한 Sequence와 Time interval 기반 침입 탐지 및 공격 분류

김형선* , 강도희 * , 곽병일 * *
*, * * 한림대학교 소프트웨어학부 ( 학부생, 교수 )

DCRL Data-driven Cybersecurity Research LAB

## 연구 개요 및 목적

현대 차량은 전자 제어 장치(Electronic Control Unit, ECU)을 사용하여 차량 내부 시스템 관리 및 제어한다. 이러한 ECU는 Controller Area Network (CAN) 통신 프로토콜을 사용하여 정보를 교환한다. 하지만, CAN Bus는 메시지 암호화, 인증과 같은 보안 기능을 제공하지 않아, 사이버보안 위협에 노출되어 있다.

본 연구는 CAN Bus에서의 발생 가능한 공격 탐지 및 식별 방법을 제안한다. 이를 위해 연속된 CAN Dataframe Sequence 및 Time interval을 기반으로 피처를 추출하였으며, XGBoost 알고리즘을 적용하여 성능을 평가하였다.

## 피처 추출

기존 데이터의 Arbitration ID (AID)와 Byte Data를 10진수로 변환하여 CAN Bus 데이터의 순서와 주기성을 고려한 총 9개의 피처를 추출하였다.

### 1. Sequence 계열 피처

현재 CAN 데이터를 기준으로 하여 이전 AID 5개를 추출하여 Sequence로 추가하였다. 해당 피처를 통해 CAN 데이터의 순서에 대한 정보를 제공한다.

### 2. Time interval 기반 피처

AID와 DLC를 고려하여 4가지 피처를 추출했다. 먼저, Time Interval 피처는 현재 데이터와 직전 데이터의 Timestamp 차를 계산하였고, 나머지 3가지의 피처는 아래 Fig.1과 같이 추출되었다.

- **AID Gap Time Interval** : Fig.1-(a)와 같이 동일한 AID를 가지는 데이터끼리의 Time Interval을 구하였다.
- **DLC Time Delta** : Fig.1-(b)와 같이 동일한 DLC를 가지는 데이터 간의 Time Interval을 계산하였다.

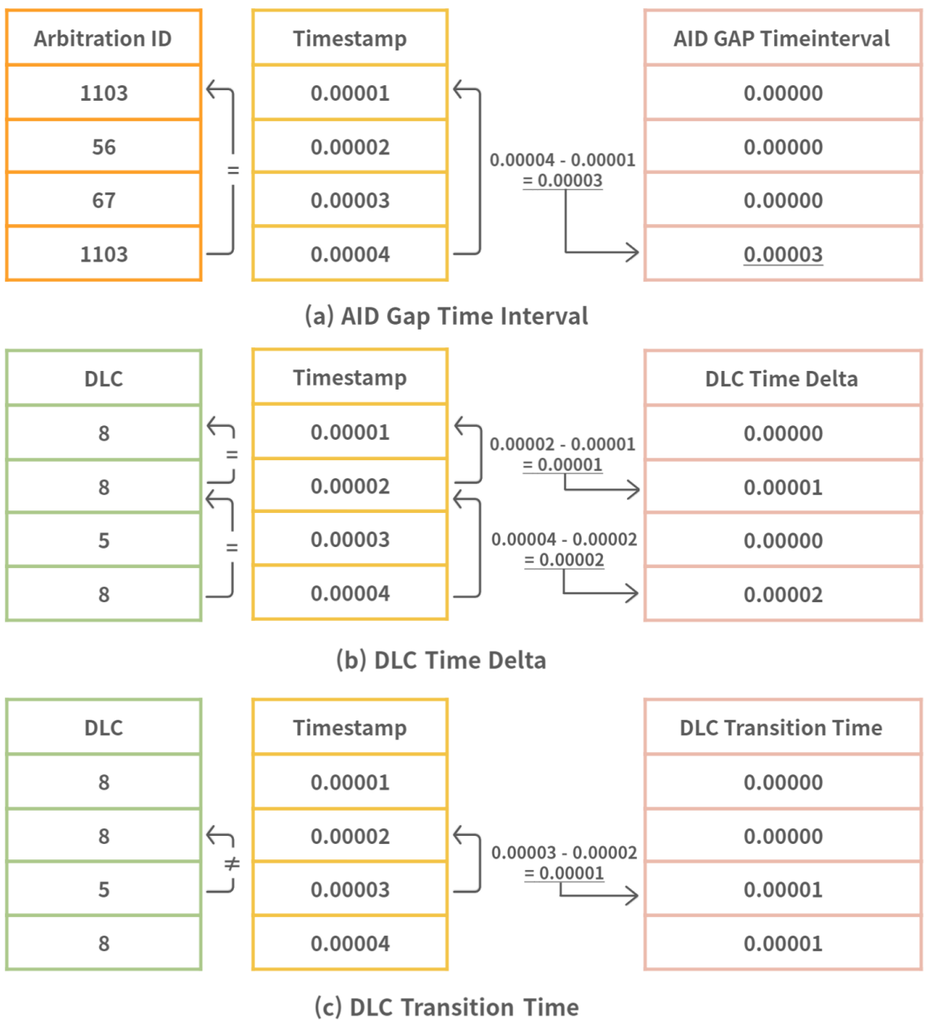


Fig.1 Time Interval Based Feature Extraction

- **DLC Transition Time** : Fig.1-(c)와 같이 DLC 값이 변할 때, 이전 데이터와 현재 데이터 간 Time Interval을 계산하였다.

Fig.2는 Time Interval 기반 피처 값들을 정상과 공격이 섞여 있는 전체 데이터에 대해 나타낸 그래프이다. Fig2-(a)는 각 공격에 대한 위치를 표시했으며, 그래프를 통해 해당 피처들이 정상과 4가지 공격 사이의 값 변화를 명확하게 나타내는 것을 확인할 수 있다. 특히, Fig.2-(b)와 Fig.2-(e)는 Replay 공격 패턴을 두드러지게 나타낸다.

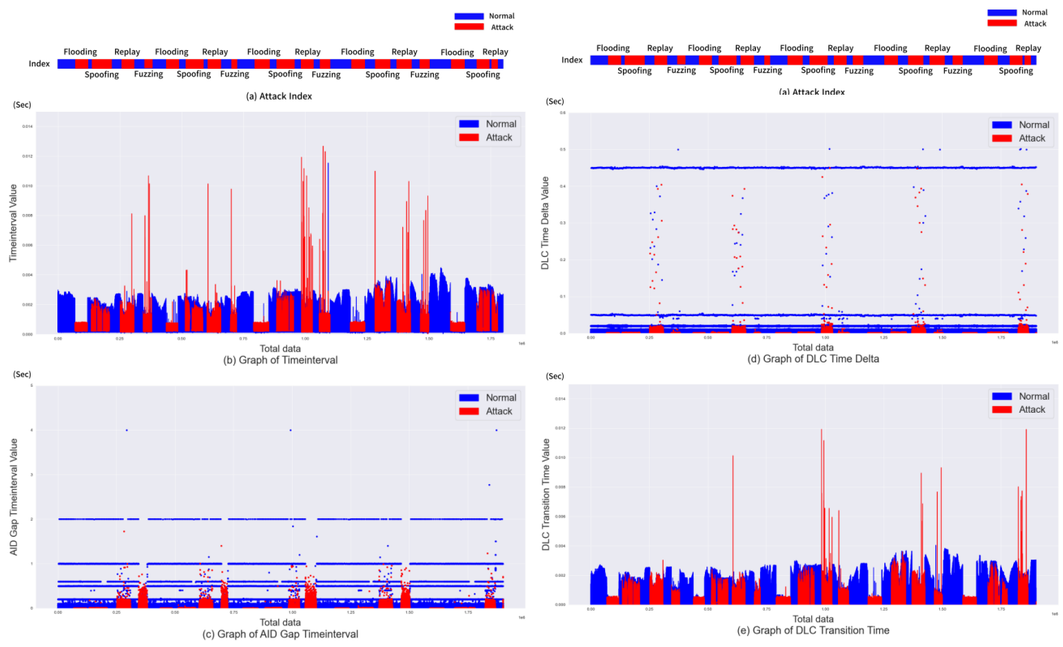


Fig.2 Graph of Time Interval Based Feature

## 실험 및 평가

4가지 공격(Spoofing, Fuzzing, Flooding, Replay)을 공격으로 구분하였을 때를 True Positive (TP)로 설정한 뒤 계산한 정확도(Accuracy)와 F1-Score를 Table.1에 나타냈다.

각 피처를 단일로 추가했을 때와 종합적으로 추가했을 때 모두 기존 데이터(AID, Byte Data)만 모델의 입력 데이터로 설정했을 때보다 높은 성능을 보였다. 특히, 종합 피처 적용 시 Replay에 대한 F1-Score가 26.62% 향상되었다.

| Feature | Accuracy (%) | F1-Score (%) |
|---|---|---|
| AID, Byte Data | 99.04 | 92.66 |
| AID Sequence | 99.58 | 97.25 |
| Time Interval | 99.56 | 96.95 |
| AID Gap Timeinterval | 99.39 | 95.84 |
| DLC Time Delta | 99.46 | 96.04 |
| DLC Transition Time | 99.25 | 94.49 |
| Total Feature | 99.88 | 99.27 |

Table.1 Accuracy and F1-score by Feature

## 결론

본 연구는 차량의 CAN Bus에서 발생할 수 있는 4가지 공격 유형에 대한 침입 탐지 및 분류 방법을 제안하였다. CAN 데이터의 순서와 주기성을 고려하여 Sequence 및 Time Interval 기반 피처 9개를 추출하였다. 해당 피처를 단일 및 종합적으로 적용하여 성능을 평가한 결과, 기존 데이터(AID, Byte Data)에 비해 분류 정확도 및 F1-Score가 향상되었음을 확인하였다. 이를 통해 제안된 피처 기반 방법이 유용하게 작용함을 입증하였다.

# CAN Bus 보안 강화를 위한 Sequence와 Time interval 기반 침입 탐지 및 공격 분류

김형선* , 강도희 * , 곽병일 * *
*, * * 한림대학교 소프트웨어학부 ( 학부생, 교수 )

DCRL Data-driven Cybersecurity Research LAB

## Background & Purpose

현대 차량은 전자 제어 장치(Electronic Control Unit, ECU)을 사용하여 차량 내부 시스템 관리 및 제어한다. 이러한 ECU는 Controller Area Network (CAN) 통신 프로토콜을 사용하여 정보를 교환한다. 하지만, CAN Bus는 메시지 암호화, 인증과 같은 보안 기능을 제공하지 않아, 사이버보안 위협에 노출되어 있다.

본 연구는 CAN Bus에서의 발생 가능한 공격 탐지 및 식별 방법을 제안한다. 이를 위해 연속된 CAN Dataframe Sequence 및 Time interval을 기반으로 피처를 추출하였으며, XGBoost 알고리즘을 적용하여 성능을 평가하였다.

## Feature Extraction

기존 데이터의 Arbitration ID (AID)와 Byte Data를 10진수로 변환하여 CAN Bus 데이터의 순서와 주기성을 고려한 총 9개의 피처를 추출하였다.

### 1. Sequence 계열 피처

현재 CAN 데이터를 기준으로 하여 이전 AID 5개를 추출하여 Sequence로 추가하였다. 해당 피처를 통해 CAN 데이터의 순서에 대한 정보를 제공한다.

### 2. Time interval 기반 피처

AID와 DLC를 고려하여 4가지 피처를 추출했다. 먼저, Time Interval 피처는 현재 데이터와 직전 데이터의 Timestamp 차를 계산하였고, 나머지 3가지의 피처는 아래 Fig.1과 같이 추출되었다.

- **AID Gap Time Interval** : Fig.1-(a)와 같이 동일한 AID를 가지는 데이터끼리의 Time Interval을 구하였다.
- **DLC Time Delta** : Fig.1-(b)와 같이 동일한 DLC를 가지는 데이터 간의 Time Interval을 계산하였다.

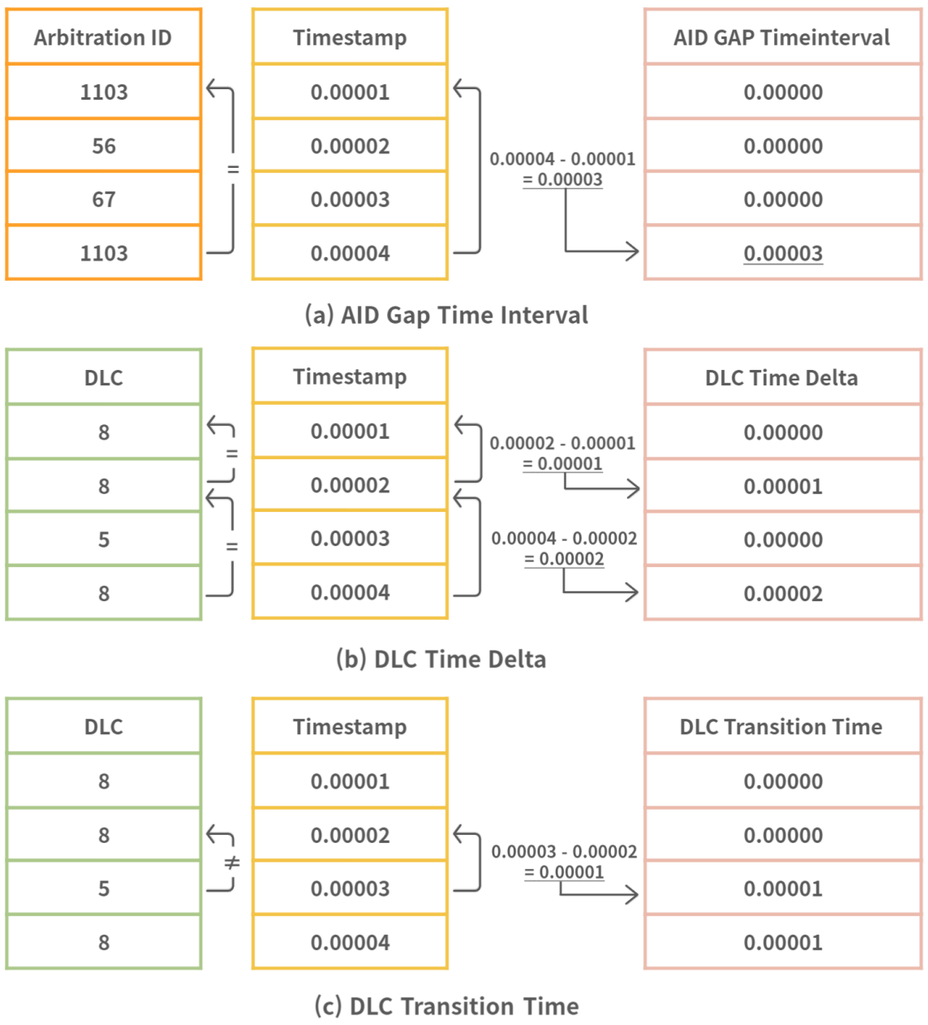


Fig.1 Time Interval Based Feature Extraction

- **DLC Transition Time** : Fig.1-(c)와 같이 DLC 값이 변할 때, 이전 데이터와 현재 데이터 간 Time Interval을 계산하였다.

Fig.2는 Time Interval 기반 피처 값들을 정상과 공격이 섞여 있는 전체 데이터에 대해 나타낸 그래프이다. Fig2-(a)는 각 공격에 대한 위치를 표시했으며, 그래프를 통해 해당 피처들이 정상과 4가지 공격 사이의 값 변화를 명확하게 나타내는 것을 확인할 수 있다. 특히, Fig.2-(b)와 Fig.2-(e)는 Replay 공격 패턴을 두드러지게 나타낸다.

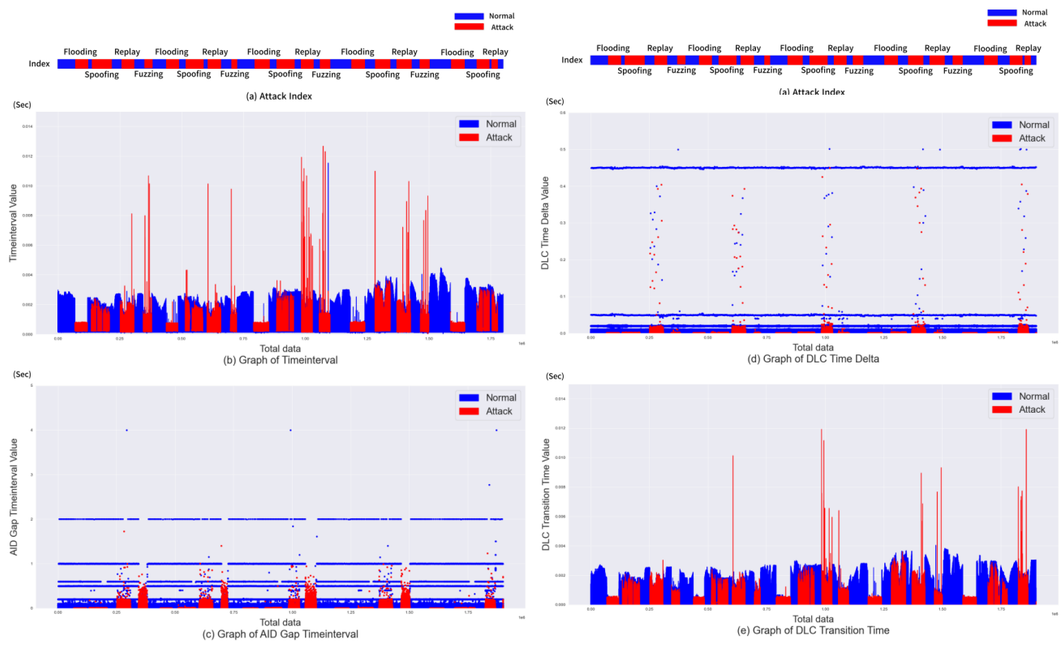


Fig.2 Graph of Time Interval Based Feature

## Experiments & Evaluations

4가지 공격(Spoofing, Fuzzing, Flooding, Replay)을 공격으로 구분하였을 때를 True Positive (TP)로 설정한 뒤 계산한 정확도(Accuracy)와 F1-Score를 Table.1에 나타냈다.

각 피처를 단일로 추가했을 때와 종합적으로 추가했을 때 모두 기존 데이터(AID, Byte Data)만 모델의 입력 데이터로 설정했을 때보다 높은 성능을 보였다. 특히, 종합 피처 적용 시 Replay에 대한 F1-Score가 26.62% 향상되었다.

| Feature | Accuracy (%) | F1-Score (%) |
|---|---|---|
| AID, Byte Data | 99.04 | 92.66 |
| AID Sequence | 99.58 | 97.25 |
| Time Interval | 99.56 | 96.95 |
| AID Gap Timeinterval | 99.39 | 95.84 |
| DLC Time Delta | 99.46 | 96.04 |
| DLC Transition Time | 99.25 | 94.49 |
| Total Feature | 99.88 | 99.27 |

Table.1 Accuracy and F1-score by Feature

## Conclusion

본 연구는 차량의 CAN Bus에서 발생할 수 있는 4가지 공격 유형에 대한 침입 탐지 및 분류 방법을 제안하였다. CAN 데이터의 순서와 주기성을 고려하여 Sequence 및 Time Interval 기반 피처 9개를 추출하였다. 해당 피처를 단일 및 종합적으로 적용하여 성능을 평가한 결과, 기존 데이터(AID, Byte Data)에 비해 분류 정확도 및 F1-Score가 향상되었음을 확인하였다. 이를 통해 제안된 피처 기반 방법이 유용하게 작용함을 입증하였다.