# Federated Learning for Securing Smart Vehicles

Sadaf MD Halim[1], Md. Delwar Hossain[2], Latifur Khan[1], Hideya Ochiai[3], Hiroyuki Inoue[4], Kevin W. Hamlen[1], Anoop Singhal[5], Youki Kadobayashi[2]

[1]The University of Texas at Dallas, [2]Nara Institute of Science and Technology [3]The University of Tokyo
[4]Kyoto Sangyo University [5]National Institute of Standards and Technology

## Abstract:

Smart vehicles are susceptible to a variety of attacks through signals from malicious entities. As more and more aspects of a smart car become automated, it becomes increasingly important to safeguard these systems against any vulnerabilities. Machine learning approaches are a popular choice for detecting such attacks based on the information in the payload. As with any machine learning approach, access to a large amount of data is absolutely imperative. However, with manufacturers independently gathering this data, it is impractical to expect all the available data in one place. As such,in this work, we explore federated solutions for increased smart vehicle security. We investigate a variety of different federated settings for such attacks and explore the benefits of the larger set of data that we gain access to when training such a model collaboratively.

## Challenges:

- Variety of attacks and severe class-imbalance
- Extreme scenarios involving complete absence of a class

We address class imbalance via triplet mixup:

$$\hat{x} = \lambda_i x_i + \lambda_j x_j + (1 - \lambda_i - \lambda_j) x_k$$

where: $\lambda_i, \lambda_j \sim Uniform(0, \alpha)$

Using triplet mixup, we can make arbitrarily many attack labels from the given labels. We scale up each attack count to **match the benign class count.** The original dataset distribution is show in Figure 3. Figure 2 shows the columns.

.

We perform a reference study in a centralized setting, where we assume all data is in one central location and the entire model is trained there. This is not realistic since data usually exists in a disparate manner. In a centralized setting, we are able to obtain an accuracy of 99.5%. This centralized accuracy gives us an upper bound on the accuracy that we can achieve with the federated model. We expect the federated model to perform worse than the centralized model, but we expect this to be still better than the real-life alternative, where nodes will only actually contain a fraction of the data that we see in the centralized data, and where their local models would miss new attack labels entirely without the aid of federated learning. Results from Federated experiments are in Figure 4. Figure 1 shows our overall architecture.

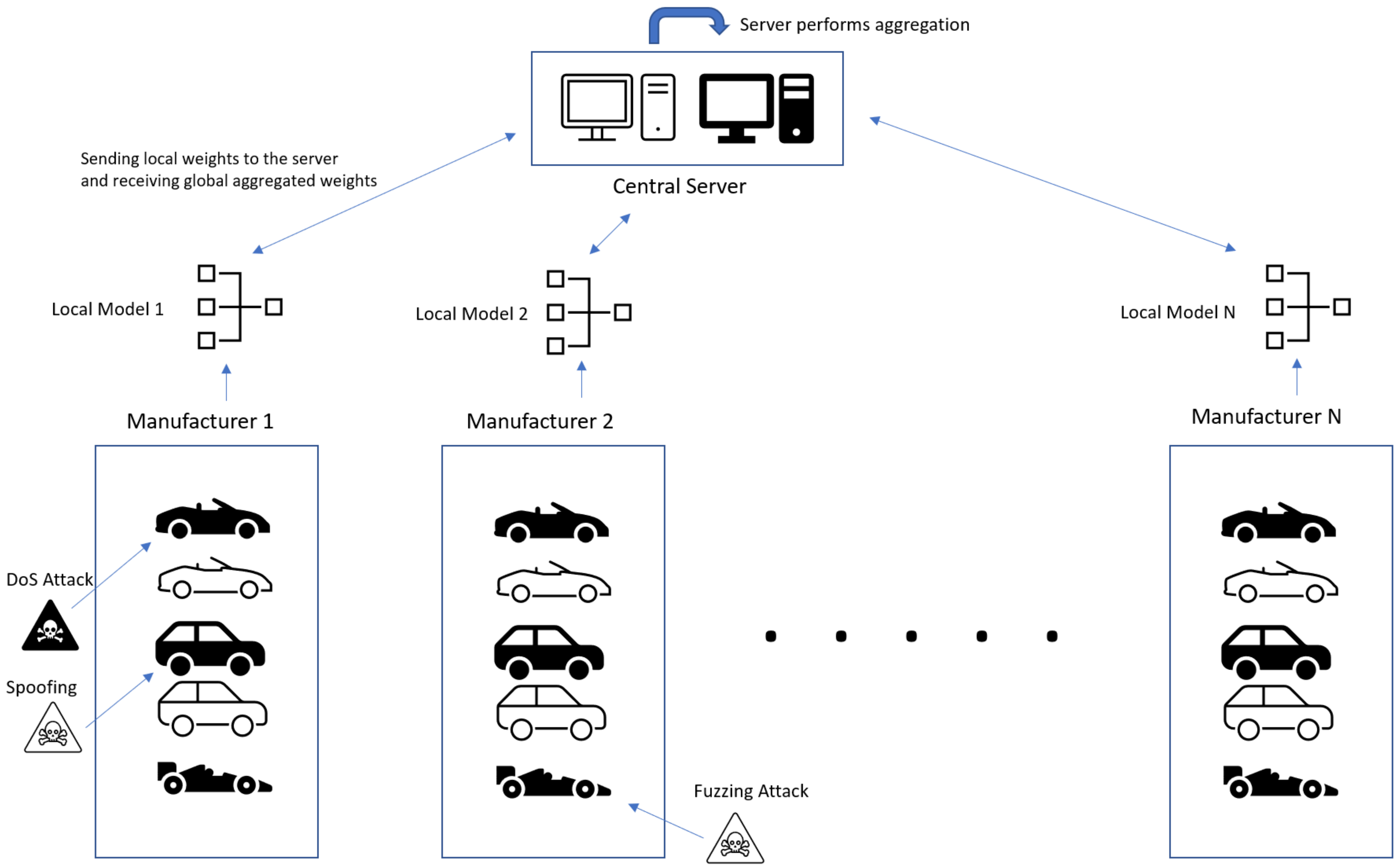
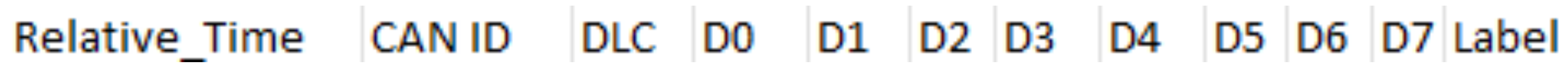


Figure 1: Overview of the system



| Relative_Time | CAN ID | DLC | D0 | D1 | D2 | D3 | D4 | D5 | D6 | D7 | Label |
|---|---|---|---|---|---|---|---|---|---|---|---|

Figure 2: Structure of the Dataset

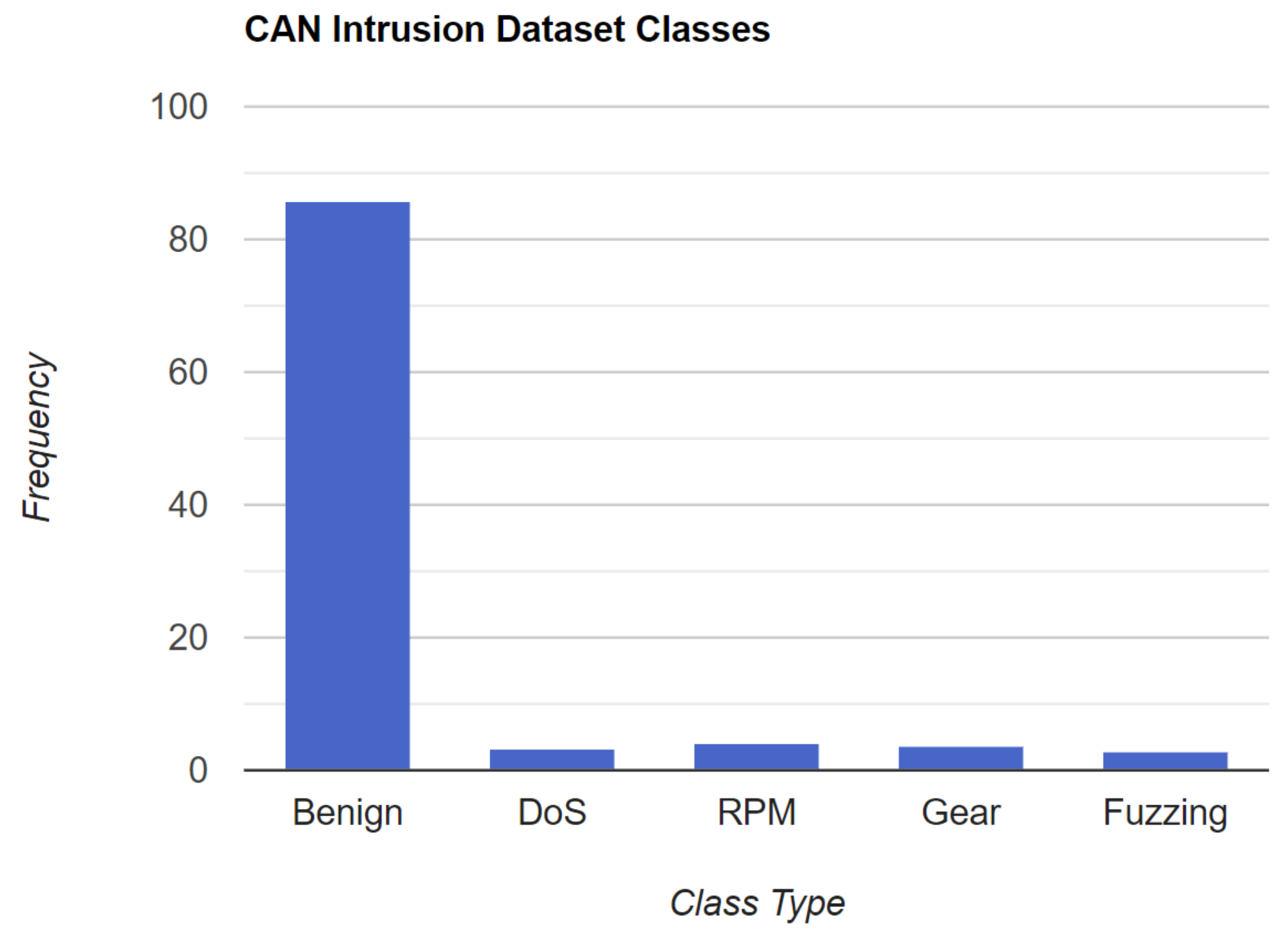


Figure 3: Class imbalance in the dataset – we use triplet mixup to address this

| Experiment Setting | Accuracy | Precision | Recall |
|---|---|---|---|
| All 4 Attacks Present | 89.42% | 89.42% | 89.42% |
| 3 Present, 1 Absent | 89.49% | 89.49% | 89.47% |
| 2 Present, 2 Absent** | 85.92% | 85.92% | 85.92% |
| 1 Present, 3 Absent ** | 85.80% | 85.86% | 85.79% |

Figure 4: Results of initial experimentation

## Acknowledgement:

The research reported herein was supported in part by NSF awards DMS-1737978, DGE-2039542, OAC-1828467, OAC-1931541, DGE-1906630; and an IBM faculty award (Research).
Part of this study was funded by the ICSCoE Core Human Resources Development Program and JSPS KAKENHI Grant Number 22H03572, Japan.