**Design and Implementation of AI security scheme for Next Generation Autonomous Vehicles**

By

Mohamed Saied Mohamed Abdelrahman

Under supervision of

**Prof Dr Hoda Korashy**

**Dr Khaled Youssef**

**Ain Shams University**

**Introduction**

Autonomous vehicles security is essential for continuous development of safer roads, where vehicles exchange safety messages to prevent collision. Basic Safety Messages are the key for vehicles’ communication with each other or with Infrastructure since communication of Vehicle to vehicle or Vehicle to Infrastructure is done wirelessly this gives a chance of vulnerability and intrusion. Here comes the importance of learning algorithms to learn and then differentiate the real safety message from attacker message.

The Goal of this this paper is to develop a model that should be trained to distinguish attacker messages from real messages using Deep learning method.

So that an Artificial Intelligence algorithm is trained to solve this problem based on neural networks which can be a strong solution for most of complex problems nowadays, the proposed algorithm aimed to classify between the types of attacks which might happen during the exchange of basic safety messages of connected vehicles.

VeReMi Dataset [1] is used in model training, which is a generated dataset for connected vehicles basic safety messages.

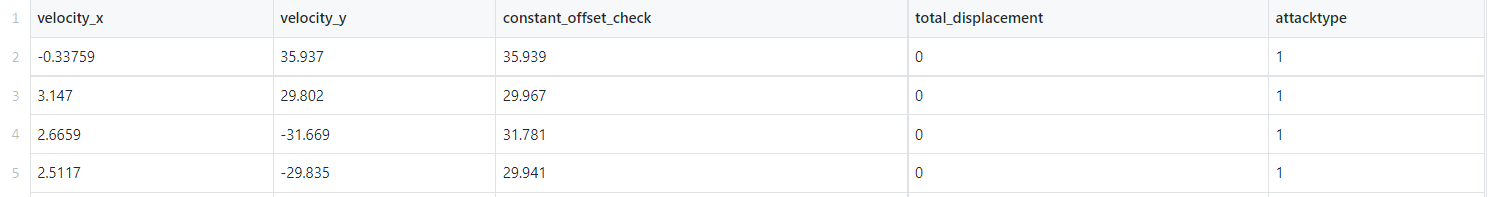


Table 1: sample of the VeReMi Dataset

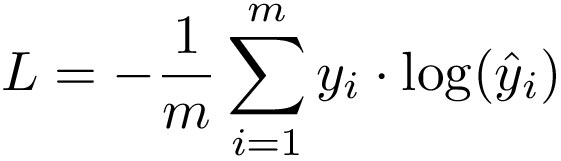
The model is trained on 4 features velocity in two axis, the constant offset and the total displacement.

**Methodology**

Multi-layer perceptron is used to distinguish between the types of attacks.

The model architecture consists of 3 layers including one hidden layer with relu activation, four inputs and six target classes.

Loss is computed using Cross entropy loss function



Cross validation technique is 80% training 20% testing and data is shuffled to increase the randomization.

**Results and Discussion**

Model is developed using Pytorch framework and trained for 100 epochs with learning rate of 1e-2, until reaching the loss of 0. 0704

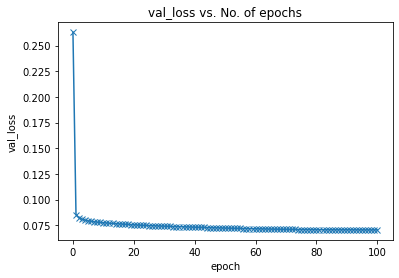
****

Figure 1: Validation Loss vs epoch number for history 1

Training was restarted for 1000 epochs with learning rate of 1e-3

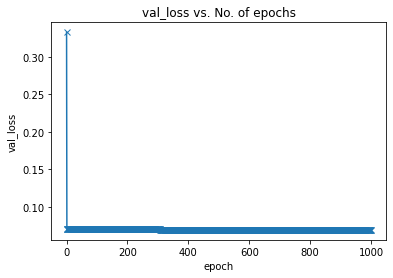


Figure 2: Validation Loss vs epoch number for history 2

**Conclusion**

This was a step towards the goal of safer roads we have future work of putting more features to the network and increase dimension which will need more complex models to solve the problem such as Recurrent Neural Networks.

**References**

[1] S. E. Russell Stewart, "Label-Free Supervision of Neural Networks with Physics and Domain Knowledge."

[2] R. Salazar-Cabrera, Á. Pachón de la Cruz, and J. M. Madrid Molina, "Sustainable transit vehicle tracking service, using intelligent transportation system services and emerging communication technologies: A review," *Journal of Traffic and Transportation Engineering (English Edition),* vol. 7, no. 6, pp. 729-747, 2020/12/01/ 2020, doi: <https://doi.org/10.1016/j.jtte.2020.07.003>.