**Proceedings of 2017 IEMEK Symposium on Embedded Technology**
**(ISET 2017)**
*Hotel Grand Haeundae, Busan, Korea,* 18-*19 May, 2017.*

# Sensor Attack Detection and Classification via CNN and LSTM

Jongho Shin[*] Youngmi Baek[*] Sang Hyuk Son[*]

[*]Department of Information and Communication Engineering
DGIST, Daegu, Republic of Korea
E-mail: {shinhapp1, ymbaek, son}@dgist.ac.kr

## Abstract

In recent years, security of autonomous vehicles is emerging as popular research topics. Especially, autonomous vehicles are equipped with many sensors such as GPS, IMU, wheel encoders and some of them are vulnerable to the attack, such as spoofing. Our objective is to detect and classify attacks of the right encoder sensor by using variables of GPS, IMU, two wheel encoder sensors. We also analyze classification accuracy and computational cost when the data are applied to Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM).

**Keywords:** sensor attack, classification, CPS, CNN, LSTM.

## 1. Introduction

Cyber-Physical Systems (CPS) are vulnerable to attacks on hardware and cyber-attacks on data management and network. Attacks including all of the deliberate attempts or actions to change, reject or insert data are conducted from outside the system by adversaries. CPS has been applied to autonomous vehicles. The modern automobiles utilize many sensors such as GPS, IMU, ultrasonic sensor, camera, and wheel encoders. These sensors can be targets of various attacks. For instance, if an attacker spoofs an encoder of an autonomous vehicle, a catastrophic accident or environmental damage could happen since it cannot provide exact information about the speed of the vehicle. It is, therefore, necessary to detect an attack of a sensor to ensure the safety of people as well as vehicles as components of transportation systems.

Redundancy technology should be selected first to address attack problems as shown in Figure 1 [1]. The technique can be classified into two major types: hardware and analytical redundancy. Hardware redundancy detects sensor attacks by using multiple sensors to measure the same physical variable. In analytical redundancy, the difference between a sensor value and an estimated value is exploited to detect the attack of the sensor. We exploit analytical redundancy because hardware redundancy has some problems such as cost, weight, space and power. Analytical redundancy is divided into a data-based method and a model-based method. The data-based method requires a number of data in order to train the model of a given system. Although both Principle Component Analysis (PCA) and Neural Network (NN) are kinds of it, these machine learning technologies do not consider the correlation between features. The model-based method including a Kalman Filter (KF) and an observer-based method requires dynamics and modeling of a system. In order to make the automobile robust against sensor attacks and control it, it is important to express nonlinearity of sensor data. Note that nonlinearity increases while the velocity of the vehicle is suddenly changeable and road surfaces are uneven. The model-based method is suffering from nonlinearity problem. Therefore, in this work, we apply CNN and LSTM that consider the correlation between features and express nonlinearity well into attack detection and classification. We focus on a novel way to detect and classify attacks of a right encoder sensor from the variables of GPS, IMU and two wheel encoder sensors of autonomous vehicles. We also analyze computational costs and accuracy of CNN and LSTM under a simple condition to choose an adequate deep learning model for a more complex condition in the future.

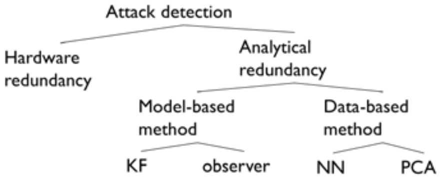

Figure 1. Attack detection approaches.

Table Ⅰ. Test accuracy and the number of parameters of CNN and LSTM

| | Test accuracy | The number of parameters |
|---|---|---|
| CNN1 | 98.4127% | 48568 |
| LSTM | 96.0317% | 5324 |
| CNN2 | 75.3968% | 3784 |

## 2. CNN and LSTM

The data were obtained on 220 meter straight road at the several (0.4, 0.7, 1.0, 1.3, 1.6 m/s) by driving mobile robot platform called Jackal. The data consists of 50400 training data and 12600 test data. Input data consists of 11 channels (altitude, latitude and longitude from GPS, angular velocity x/y/z and acceleration x/y/z from IMU and left/right velocity from left/right wheel encoders). Attacks of the right encoder sensor were detected and classified into 4 classes such as normal operation, constant bias attack, small and large additive attack after 11 variables were normalized by Min-Max normalization. Constant bias attack made the right encoder sensor read a constant bias 1.5 m/s regardless of sensor values. Small and large additive attack added each 0.11 m/s and 0.22 m/s to the right velocity.

Same data were applied to each CNN and LSTM. At first, the architecture of CNN1 consists of 1-D convolution 2 layers and Fully Connected (FC) 2 layers. ReLu was used as the activation function. Dropout was set to be 0.5 and Softmax classifier and Adam was exploited. In this case, learning rate, epoch and batch size were each 0.001, 150 and 32. In the case of LSTM, the architecture of LSTM has LSTM 2 layers and FC layer. Dropout was set to 0.2 and Softmax classifier was exploited. Optimizer, learning rate, and batch size were same as CNN and epoch was 100. Table Ⅰ. shows that the accuracy of CNN1 is higher than that of LSTM but the number of parameters of CNN1 is about 9 times higher than that of LSTM. The number of parameters of CNN2 that have the same architecture of LSTM is very low but that of accuracy is 75.3968%.

## 3. Conclusions and Future Work

In our results, they have classified into normal operation and three kinds of attacks after data of the right encoder have been processed in each CNN and LSTM. Both CNN and LSTM designed to classify attacks have high accuracy. In terms of the computational complexity, LSTM can be superior to CNN since the number of parameters required to perform the classification is much lower than that. We plan to experiment on diverse conditions such as stop, left turn, right turn, and traveling at from 0 to 1.85 m/s. We will design a new system using LSTM to recover an attacked sensor in the presence of noises.

### Acknowledgement

This research was supported in part by Global Research Laboratory Program (2013K1A1A2A02078326) through NRF, DGIST Research and Development Program (CPS Global Center) funded by the MSIP, and Institute for Information & communications Technology Promotion (IITP) grant funded by the Korean government (MSIP) (No. B0101-15-0557, Resilient Cyber-Physical Systems Research).

### References

[1] Mehranbod, Nasir, Masoud Soroush, and Chanin Panjapornpon. "A method of sensor fault detection and identification." *Journal of Process Control* 15.3 (2005): 321-339.
[2] LeCun, Yann, Yoshua Bengio, and Geoffrey Hinton. "Deep learning." *Nature* 521.7553 (2015): 436-444.