An LSTM-based Forgery Detection Method for V2X Messages*

Kyung-Mo Sung[1], WonSeok Choi[1†], Laihyuk Park[2], Woongsoo Na[3]
[1] Telecommunications Technology Association, Korea
[2] Dept. of Computer Science and Engineering, Seoul National University of Science &Technology, Korea
[3] Department of Software, Kongju National University, Korea.
{skm, wschoi}@tta.or.kr, lhpark@seoultech.ac.kr, wsna@kongju.ac.kr

Abstract

This paper proposes an algorithm to detect abnormal packets in Basic Safety Messages (BSMs) used for vehicular communication, utilizing information such as latitude, longitude, speed, acceleration, and heading. The method adapts the conventional LSTM Autoencoder by training it on sequences of normal BSMs, while also separately calculating and incorporating the delta values of the packet's detailed features (e.g., latitude, longitude, speed, acceleration). An experiment was conducted to verify its ability to detect sequences containing 3,500 arbitrarily inserted abnormal packets and to evaluate its false positive rate. The test results showed a detection rate of 91.2%.

1 Introduction

As autonomous driving technology has recently become a major topic, extensive research is underway. Efforts are being made to utilize various technologies, such as ADAS (Advanced Driver-Assistance Systems), which use sensors inside and outside the vehicle to provide warnings or actively control the vehicle to avoid hazardous situations like collisions. Fundamentally, this control is based on sensor information. However, sensors have limitations in environmental perception, especially in situations like blind spots caused by buildings or structures, or severe weather such as dense fog. V2X (Vehicle to Everything) technology has emerged as an alternative to address this. V2X refers to the technology where a vehicle exchanges or shares information with surrounding vehicles and road infrastructure via wireless networks. Representative messages used in V2X communication include BSM (Basic Safety Message), SPaT (Signal Phase and Timing), MAP (Map Data), and TIM (Traveler Information Message). The BSM is a message that announces a vehicle's presence and status, making it the most fundamental safety message. BSMs are designed to be broadcast at a 10Hz frequency. They periodically transmit data including a Vehicle ID (a temporary identifier changed periodically for privacy), latitude, longitude, altitude, current speed, heading (direction of travel), and acceleration (longitudinal/lateral). These characteristics allow BSMs to be used for various warning and safety services, such as Forward Collision Warning (FCW) and Intersection Movement Assist (IMA). For these reasons, the security of BSM messages in V2X technology is critical, as it is directly linked to

* Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-64, December 16-18, 2025, Sapporo, Japan.
† Corresponding author: Intelligent Network Dept., Telecommunications Technology Association, Bundang-gu, Seongnam-city, Gyeonggi-do, 13591, Korea, Email: wschoi@tta.or.kr

safety. In this paper, we developed an AI model based on an LSTM (Long Short-Term Memory) Autoencoder, utilizing the periodicity of BSMs and their location information, time information, and vehicle IDs. We conducted experiments by directly capturing and training on BSMs transmitted from V2X terminals.

2 Proposed algorithm and Experimental results

LSTM, a type of RNN, is advantageous as it specializes in learning patterns from time-ordered (time-series) data. This strength was expected to yield excellent performance in remembering a vehicle's previous movements and predicting its next ones. An Autoencoder is an unsupervised learning model that learns the patterns of 'normal' data. It is trained to compress (Encode) and then reconstruct (Decode) data, and it has been repeatedly demonstrated that it can restore normal data almost perfectly. Therefore, this paper utilizes an LSTM-Autoencoder to learn normal data, for which the data preprocessing was performed through the following steps. First, the data is filtered and sorted by vehicle using the Source address within the BSM message. This division by vehicle (using the Source address) is necessary because if the data were only sorted generally, the model might mistakenly learn that a vehicle "jumping" from the final position of vehicle A to the initial position of vehicle B is normal behavior.

Second, for the data divided by vehicle, it is necessary to structure the changed features (feature engineering), in addition to the basic location information (latitude, longitude, speed). Features such as the change in latitude, change in longitude, calculated speed (based on position change), acceleration, and rate of heading change are extracted and structured for model training. Finally, to make the data suitable for a time-series model like LSTM, the data is divided into fixed time intervals (e.g., 10 seconds) to be input as single sequences, rather than just using a fixed number of data points. After this, a normalization process is applied, and the training begins. For the experiment, training was performed using a total of 3,860,000 packets, which were automatically used to generate sequences with a 1-second size. During training, MinMaxScaler was applied to learn the normal range of data based only on the maximum and minimum values. The model was trained for 30 epochs with a batch size of 64. For validation, the reconstruction error (MAE) was calculated for each sequence. The 99th percentile of these errors was set as the threshold for anomaly detection. To verify the trained model, 100,000 packets were used to generate sequences in the same manner as the training process. If a sequence's reconstruction error exceeded the threshold, it was classified as abnormal; otherwise, it was classified as a normal packet. This validation set of 100,000 packets included approximately 3,500 forged packets, which had been modified with anomalous latitude, longitude, and speed values, to test the model's performance. The test results showed a detection rate of 91.2%, successfully identifying 3,192 out of 3,500 abnormal packets. Additionally, it demonstrated a false positive rate of 0.68%, incorrectly classifying 655 out of 96,500 normal packets as abnormal.

Acknowledgments

This research was supported by the MSIT (Ministry of Science and ICT), Korea, and supported by the IITP (Institute of Information & communications Technology Planning & Evaluation). (No.2022-0-00979, Development of technology and test criteria for evaluating the security of self-driving vehicle data and V2X communication network.).

References

[1] Hochreiter, S. and Schmidhuber, J., "Long short-term memory," Neural computation, Vol. 9, No. 8, pp. 1735-1780, 1997.