Scientific Research Publishing

Journal of Transportation Technologies, 2021, 11, 284-295
https://www.scirp.org/journal/jtts
ISSN Online: 2160-0481
ISSN Print: 2160-0473

Misbehavior Detection Method by Time Series Change of Vehicle Position in Vehicle-to-Everything Communication

Toshiki Okamura, Kenya Sato

Computer and Information Science, Graduate School of Science and Engineering, Doshisha University, Kyoto, Japan
Email: toshi.okamura@nislab.doshisha.ac.jp

How to cite this paper: Okamura, T. and Sato, K. (2021) Misbehavior Detection Method by Time Series Change of Vehicle Position in Vehicle-to-Everything Communication. *Journal of Transportation Technologies*, **11**, 284-295.
https://doi.org/10.4236/jtts.2021.112018

Received: March 23, 2021
Accepted: April 26, 2021
Published: April 29, 2021

Abstract

In recent years, research has been conducted on connected vehicles (CVs) that are equipped with communication devices and can be connected to networks. CVs share their own position information and surrounding information with other vehicles using Vehicle-to-Everything (V2X) communication. CVs can recognize obstacles on non-line-of-sight (NLoS), which cannot be recognized by autonomous vehicles, and reduce travel time to a destination by cooperative driving. Therefore, CVs are expected to provide safe and efficient transportation. On the other hand, problems of security of V2X communication by CVs have been discussed. Safe and efficient transportation by CVs is on the basis of the assumption that correct vehicle information is shared. If fake vehicle information is shared, it will affect the driving of CVs. In particular, vehicle position faking has been shown that it can induce traffic congestion and accidents, which is a serious problem. In this study, we define position faking by CV as misbehavior and propose a method to detect misbehavior on the basis of changes in vehicle position time series data composed of vehicle position information. We evaluated the proposed method using four different misbehavior models. F-measure of misbehavior models that CV sends random position information detected by the proposed method is higher than one by a related method. Therefore, the proposed method is suitable for detecting misbehavior in which the position information changes over time.

Keywords

Connected Vehicle, V2X Communication, Security, Misbehavior Detection, Anomaly Detection

1. Introduction

In recent years, expectations for connected vehicles (CVs) equipped with communication devices have increased, and studies for their widespread use have been widely conducted. CVs communicate with other vehicles and a cloud by vehicle-to-anything (V2X) communication between multiple CVs. CVs share their own position information and surrounding information with other vehicles using V2X communication. By sharing position information and surrounding information, CVs can recognize obstacles on non-line-of-sight (NLoS), which cannot be recognized by autonomous vehicles, and prevent accidents [1]. Moreover, CVs can change lanes safely [2] and reduce travel time to a destination [3] by cooperative driving. Therefore, CVs are expected to provide safe and efficient transportation.

However, the connection of CVs to networks is expected to cause security problems.

Possible CVs security problems include vehicles being hijacked on the basis of hacking from outside the vehicle [4], intentional traffic congestion due to vehicle camouflage [5] and Sybil attacks [6]. Therefore, CVs security is very important because attacks on CVs directly endanger the lives of drivers and pedestrians. Conventional vehicle security methods are not sufficient because they do not take into account that the vehicles are connected to networks. Hence, a security countermeasure method that assumes the use case of the attacks on CVs is necessary. Past research focused on position faking among the attacks against CVs. However, position faking is difficult to prevent position faking by not only conventional vehicle security methods, but also by network security methods such as pre-shared key (PSK) authentication and public key infrastructure (PKI) [7]. In addition, position faking has various negative impacts such as traffic accidents, partial occupation of roads, and traffic congestion and significantly impacts an intelligent transportation system (ITS).

In this study, we define position faking by CVs as misbehavior and propose a method to detect misbehavior on the basis of changes in vehicle position time series data.

2. Related Works

2.1. Detection of Malicious Nodes in VANETs Algorithm Method

Detection of malicious nodes in VANETs (DMN) algorithm has been proposed [8]. It is designed to isolate the nodes showing abnormal behavior as well as enhancing the network performance. This method is to detect malicious vehicles that drop or duplicate packets sent from other vehicles. Therefore this attack is not included in the attack that we want to detect.

2.2. Machine Learning Method

A misbehavior detection method using machine learning has been proposed [9]. Specifically, the misbehavior detection uses position information of senders and

receivers of vehicle-to-vehicle (V2V) communication and received signal strength indicator (RSSI) as features, and performs unsupervised machine learning. For the machine learning model, they proposed a new model based on Deep Autoencoder and used it. As a result, when the ghost vehicle is 100 m away from the real vehicle, the detection rate for the proposed model is nearly 100%.

However, when the ghost vehicle is less than 30 m away from the real vehicle, or when the RSSI values of the ghost vehicle and the real vehicle are close, the masqueraded position data is difficult to detect.

In another study, an ensemble method that combines the results of individual classifiers, such as Native Bayes, Adaboost 1, and so on, into one final result in order to achieve higher detection accuracy is proposed [10]. In this experiment, misbehavior on a highway is assumed. Our method is subject to misbehavior in a city scenario. Therefore this study is not included in our study.

A misbehavior classifier with a set of features by using artificial neural network (ANN) techniques is also proposed [11]. The classifier is trained using feed-forward back-propagation ANN with one hidden layer after collection of enough data. This method needs to train the model before detecting misbehavior. In our study, we focused on a misbehavior detection without learning beforehand.

2.3. Heartbeat Message Method

A misbehavior detection method using heartbeat messages has been proposed [12]. The specific procedure is shown below.

1) A reporting vehicle periodically broadcasts its positional and kinematics information through their heartbeat message.

2) An observing vehicle running a misbehavior detection scheme receives heartbeat messages from the reporting vehicles.

3) The observing vehicle predicts the current position of the reporting vehicle on the basis of the information acquired at the previous time.

4) The misbehavior detection determines whether the reporting vehicle is misbehaving or not on the basis of its expected current position.

Through a simulation, high precision and recall were measured in a highway scenario without intersections, but low precision and recall were measured in a city scenario with intersections. There is also the problem that the reporting vehicle outside the observing vehicle's dedicated short range communication (DSRC) can misbehave.

2.4. Mutual Position Monitoring Method

A misbehavior detection method has been proposed on the basis of the mutual vehicle position monitoring using V2X communication [13]. The specific procedure is shown below.

1) Vehicles exchange vehicle IDs with nearby vehicles using V2V communication.

2) Vehicles send its position information and IDs of peripheral vehicles ob-

tained in 1 to a cloud. Then the base station adds the base station ID to the packet.

3) The cloud checks whether the vehicle's position is within the possible V2V communication area of the peripheral vehicles. When the position information is outside the possible V2V communication area, the cloud determines that the received position information has been camouflaged.

This method can detect masqueraded position data from malicious vehicles.

However, it has two problems with this method. First, misbehavior of a vehicle that has no peripheral vehicles cannot be detected. Second, the method may not be able to detect misbehavior if the misbehavior is performed in a short distance from the vehicle's actual position. That is because that position information can be disguised within a range in which peripheral vehicles and the V2V communication range are possible.

3. Proposed Method

3.1. System Architecture

One problem with conventional methods for misbehavior detection is that misbehavior is difficult to detect on maps that include intersections or when misbehavior is a short distance away. Therefore, to solve the problems of conventional methods, we verify a misbehavior detection method that focuses on changes in position time series data.

Figure 1 shows the system structure of the proposed method. We introduce a cloud and CVs in the system. The cloud is a server on networks that communicates with CVs. In an ITS, the cloud can aggregate vehicle information and pedestrian data to provide a dynamic map [14]. In this study, the cloud obtains vehicle position information from all CVs. Then, the cloud creates position time series data for each vehicle and uses it to detect misbehavior.

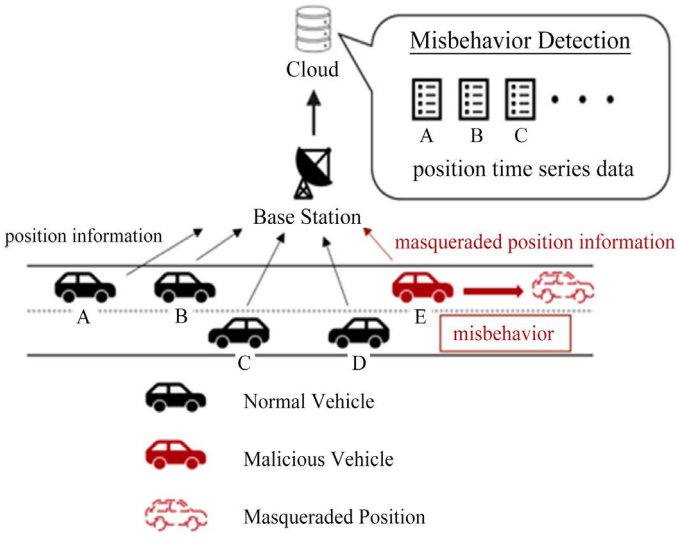

Figure 1. Proposed method to detect misbehavior.

Position time series data is a vector whose elements are vehicle position information at each time. This time, the position information is added to the time series data every time a cloud communicates with the CVs. When the cloud communicates in 1 s cycles, position information is added every 1 s. Furthermore, the position information is the data that represents the area where the cloud can communicate in the Cartesian coordinate system (x, y).

Next, we describe CVs, which can communicate with the cloud using cellular networks, and with CVs using DSRC or long-term evolution (LTE) direct. In this study, the CV transmits the vehicle position information to the cloud. CVs usually send the exact position information of their vehicles. However, for criminal purposes, CVs send masqueraded position information to the cloud, which is different from the vehicle position. Thus, an act of a CV sending masqueraded position information to the cloud is misbehavior.

3.2. Anomaly Detection

Anomaly detection is a method for detecting anomaly samples from a population in statistics [15]. In this study, the population is the position information and the anomaly samples are masqueraded position data. In addition, an anomaly score is defined by singular spectrum transformation (SST). SST is independent of a distribution of time series data, applicable to various types of data, and robust to noise introduced into the data.

3.3. Singular Spectrum Transformation

Equations (1) to (7) represents SST. In Equation (1), D is position time series data, whose elements are position information $\xi(t)$ of a vehicle at time t.

First, Equation (1) is transformed into Equation (2). Equation (2) is a Hankel Matrix. x is a time series data with M elements as shown in Equation (3). From the time series data D, a history matrix $X(t)$ with a window size M and the number of columns n and a test matrix $Z(t)$ with a lag L and the number of columns k are generated as in Equations (4) and (5). The window size is the number of elements of x, which is an element of the matrix.

$$D = \left\{ \xi^{(1)}, \xi^{(2)}, \ldots, \xi^{(T)} \right\} \tag{1}$$

$$D = \left\{ x^{(1)}, x^{(2)}, \ldots, x^{(N)} \right\} \tag{2}$$

$$x^{(1)} = \left(\xi^{(1)}, \xi^{(2)}, \ldots, \xi^{(M)} \right), x^{(2)} = \left(\xi^{(2)}, \xi^{(3)}, \ldots, \xi^{(M+1)} \right), \ldots \tag{3}$$

$$X^{(t)} = \left[x^{(t-n-M+1)}, \ldots, x^{(t-M-1)}, x^{(t-M)} \right] \tag{4}$$

$$Z^{(t)} = \left[x^{(t-k+L-M+1)}, \ldots, x^{(t-M+L-1)}, x^{(t-M+L)} \right] \tag{5}$$

As a result of singular value decomposition of $X(t)$ and $Z(t)$, matrices of left-singular vectors are obtained as shown in Equations (6) and (7). Both u and q are left singular vectors with M elements, where r and m are the numbers of columns in each matrix.

Finally, an anomaly score a is defined by (8). σ_1 is the largest singular value of $U_r^{(t)^T} Q_m^{(t)}$.

The anomaly score indicates the magnitude of the difference between the history matrix and the test matrix. If the anomaly score is greater than or equal to a predefined anomaly threshold h, the test matrix is recognized as different from the history matrix and is judged to be anomalous.

3.4. Misbehavior Models

In this study, we evaluate four types of misbehavior models based on the research of So [16] to determine which misbehavior model the proposed method is suitable for detecting.

Figure 2 shows four types of misbehavior models. The red vehicles in the figure are malicious vehicles, and the blue dots are masqueraded positions by the malicious vehicles.

The details of the misbehavior models are described below.

Model 1 CV sends position information of a specific place (300, 100)

Model 2 CV sends position information 200 m away from the vehicle's position in the x- and y-axes directions.

Model 3 CV sends random position information in the map

Model 4 CV sends random position information 200 m away from the vehicle's position in the x- and y-axes directions.

3.5. Misbehavior Detection Procedure

Figure 3 shows a procedure of misbehavior detection by a cloud.

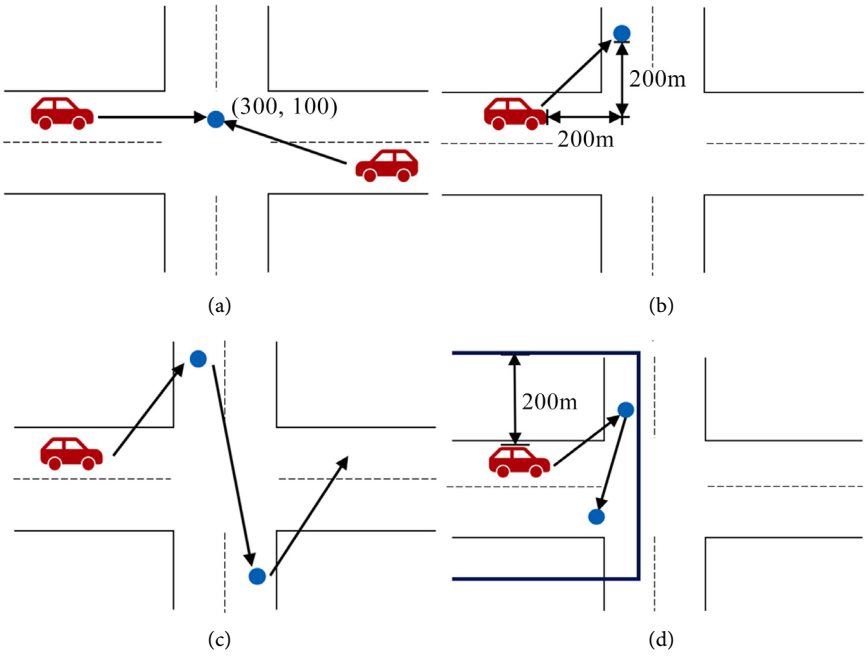

Figure 2. Misbehavior models to be detected by the proposed method. (a) Model 1; (b) Model 2; (c) Model 3; (d) Model 4.

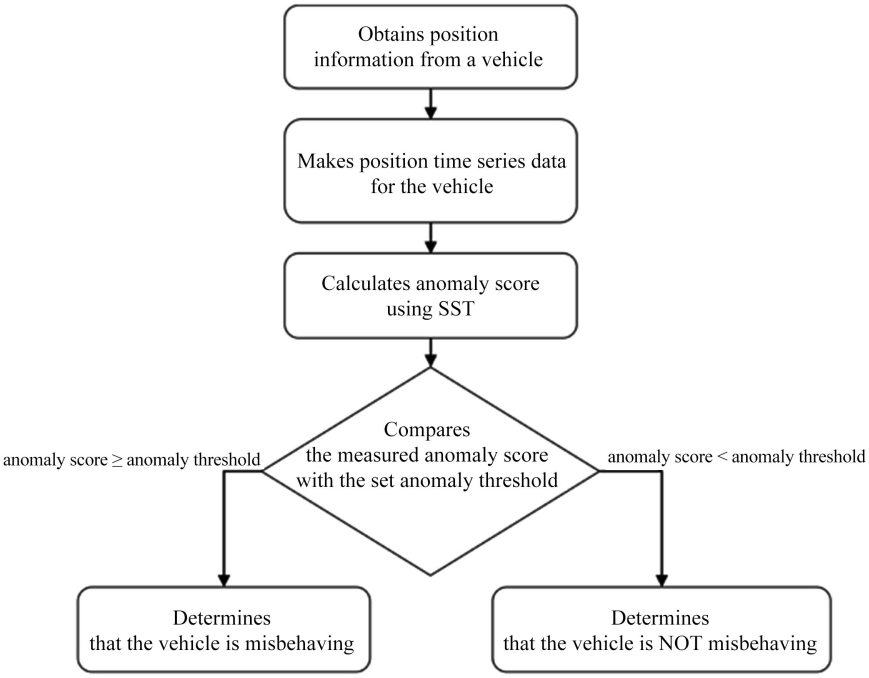

Figure 3. Flowchart of misbehavior detection by cloud.

First, the cloud obtains the position information of the CVs that is sent periodically. The cloud keeps storing the vehicle position time series data. First, the cloud creates history matrices. Once the number of data to which SST can be applied is stored, the cloud applies SST to the position time series data and obtains left-singular vectors. Next, the cloud creates test matrices in the same way, using the position time series data with a time lag L shifted from the history matrices, and obtains left-singular vectors. The cloud calculates the anomaly score using left-singular vectors, and if the anomaly score is greater than or equal to the anomaly threshold, the cloud determines that the vehicle has been misbehaving.

4. Evaluation Experiment

4.1. Evaluation Environment

We use a simulator to evaluate a detection rate of misbehavior detection of the proposed method. For the evaluation, CVs, base station, and cloud were reproduced using Scenargie [17], a network simulator developed by Space-Time Engineering (STE).

We used a Manhattan model with roads of 1 km^2 and intersections every 200 m in both the x- and y-axis directions of the map. We used a geographic information system (GIS)-based random waypoint [18], which is a model of random movement on the road on the basis of the random-waypoint mobility model.

The simulation was performed for 10 minutes on the basis of the related methods. We assumed that the malicious vehicles would misbehave for a total of 2 minutes, from 120 s to 180 s and from 420 s to 480 s. Because malicious vehicles

are unlikely to misbehave all the time, we set up the malicious vehicles to misbehave for one minute in both the first and second halves of the simulation.

Table 1 shows the simulation environment and communication method.

It is highly probable that a misbehaving vehicle may not misbehave all the time. Therefore, we set up the misbehaving vehicle to misbehave for one minute in each of the first and second halves of the simulation.

We calculated anomaly scores by SST with the following parameters. A window size M is 20. The history matrix and test matrix contain 10 columns. We used only one left-singular vector to calculate anomaly scores. Therefore, both r and m are 1. The lag L between the history matrix and the test matrix is 10.

In this study, we focused on misbehavior while driving. Therefore, there is assumed to be no misbehaving at the start of driving. In addition, we do not consider the noise of the position information when the vehicle acquires its own position information.

4.2. Evaluation Method

We used precision, recall, and F-measure as evaluation methods for the proposed method. Precision and recall are basic metrics that can evaluate detectors. Precision and recall are in a trade-off relationship experimentally, and F-measure shows the balance between precision and recall.

Each equation is as follows. True positive (TP) is the number of times the cloud correctly judged that misbehavior had taken place, false positive (FP) is the number of times that the cloud misjudged that misbehavior had taken place, and false negative (FN) is the number of times that the cloud did not recognize that misbehavior had taken place. F-measure is the harmonic mean of precision and recall.

Table 1. Simulation parameters.

Simulator	Scenargie 2.2
Simulation Time	600 (s)
Simulation Area	1000 (m) × 1000 (m)
Simulation Environment	Manhattan Model
Time for Misbehavior	120 - 180, 420 - 480 (s)
Vehicle Speed	0 - 30 (km/h)
Mobility Model	GIS-Based Random Waypoint
Communication Model	LTE
Use Frequency Band	2.5 (GHz)
Communication Interval	1.0 (s)
Radio Spread Model	LTE-Micro

4.3. Comparison with Conventional Method

To clarify whether the proposed method is effective, we created models on Scenargie on the basis of the mutual position monitoring method. The road environment, the number of vehicles, and the communication method are the same as in the proposed method. The communication method of V2V communication is ARIB STD T109, and the communication period is 100 ms. The radio spread model of V2V communication is ITU-R P.1411. The number of peripheral vehicles necessary for a cloud server to trust is 20 % of the number of vehicles at the base station where the vehicle communicates.

5. Results and Discussion

Precision, Recall, and F-Measure of Misbehavior Detection

Figures 4-6 shows the precision, recall, and F-measure for misbehavior detection by the proposed method. In all models, lowering the anomaly threshold

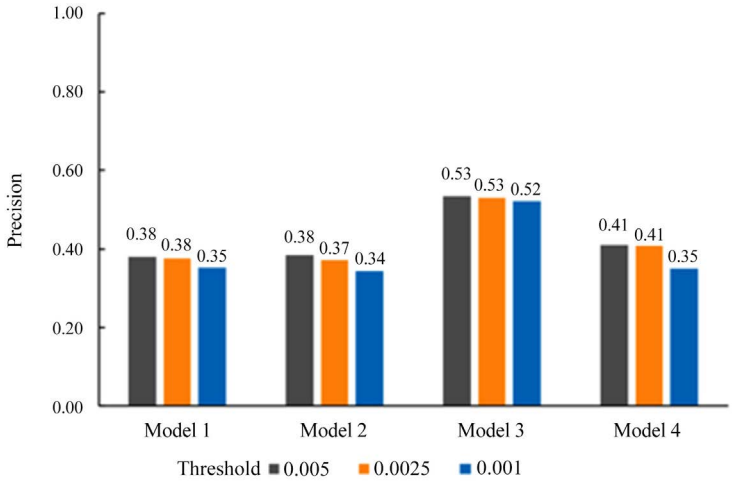

Figure 4. Simulation results for threshold value of anomaly score to estimate the precision.

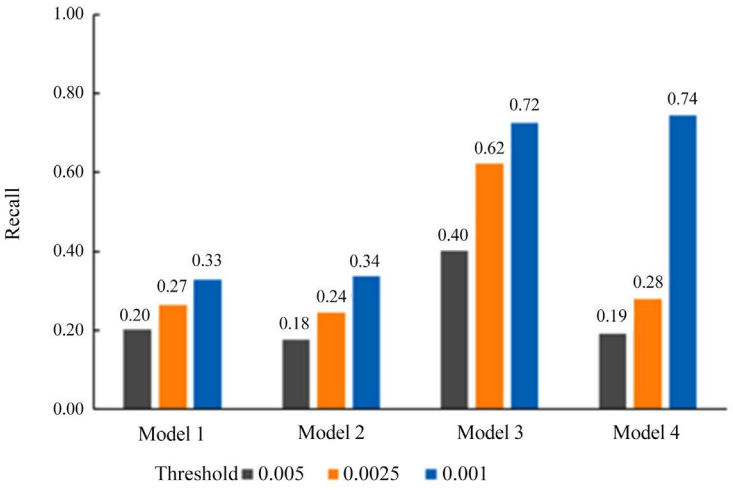

Figure 5. Simulation results for threshold value of anomaly score to estimate the recall.

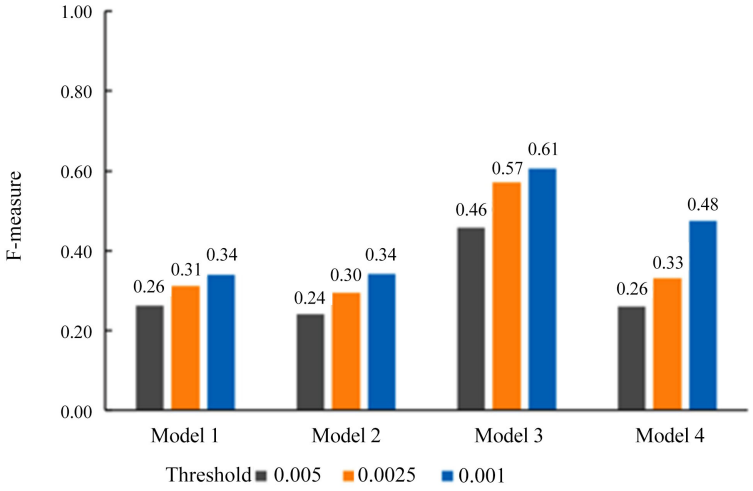

Figure 6. Simulation results for threshold value of anomaly score to estimate the f-measure.

improved recall but reduced precision, whereas the F-measure improved because the recall improved more than the precision. Since the highest F-measure is in Figure 6 when the anomaly threshold was 0.001, the anomaly threshold was fixed at 0.001 in the subsequent evaluations.

In addition, in both precision and F-measure, the best value is shown in model 3 for all anomaly threshold values. Even in recall, the best value is shown in model 3 except when the anomaly threshold value is 0.001. From this result, the proposed method is suitable to detect the misbehavior of model 3. On the other hand, there is no significant difference between models 1 and 2.

6. Conclusions

Misbehavior of position information using vehicle-to-anything (V2X) communication by connected vehicles (CVs) can induce traffic congestion and significantly affect intelligent transportation system (ITS). Therefore, to prevent misbehavior, a method to detect misbehavior is necessary.

In this study, we proposed a method for a cloud to detect misbehavior by detecting changes in position time series data by anomaly detection. In the proposed method, we defined an anomaly score in singular spectrum transformation (SST) and prepared four types of misbehavior models. The proposed method is implemented using the simulator Scenargie. We presented the precision, recall, and F-measure when varying the anomaly threshold and when comparing the proposed method with a related method, the mutual position monitoring method. The results demonstrated that the proposed method can detect misbehavior. In addition, it is verified that the proposed method is more suitable than the mutual position monitoring method for detecting misbehavior in which the position information changes dynamically over time. In this study, the evaluation condition was that CVs did not misbehave at the start of operation. In the future, we need to devise a method to enable misbehavior to be detected at the

start of operation with the proposed method. In addition, we need to investigate the effect of time-lag on software used after misbehavior detection.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Sun, C., Zheng, S., Ma, Y., Ma, Y., Chu, Chu, D., Yang, J., Zhou, Y., Li, Y. and Xu, T. (2020) An Active Safety Control Method of Collision Avoidance for Intelligent Connected Vehicle Based on Driving Risk Perception. *Journal of Intelligent Manufacturing*. https://doi.org/10.1007/s10845-020-01605-x

[2] Kamal, M.A.S., Taguchi, S. and Yoshimura, T. (2015) Efficient Vehicle Driving on Multi-Lane Roads Using Model Predictive Control under a Connected Vehicle Environment. *Proceedings of* 2015 *IEEE Intelligent Vehicles Symposium* (*IV*), Seoul, 28 June-1 July 2015, 736-741. https://doi.org/10.1109/IVS.2015.7225772

[3] Kimura, K., Azuma, S. and Sato, K. (2018) Evaluation of Safety and Efficiency Simulation of Cooperative Automated Driving. *Proceedings of* 7*th International Conference on Advances in Vehicular Systems*, *Technologies and Application* (*VEHICULAR*), Venice, 24-28 June 2018, 66-71.

[4] Takefuji, Y. (2018) Connected Vehicle Security Vulnerabilities [Commentary]. *IEEE Technology and Society Magazine*, **37**, 15-18. https://doi.org/10.1109/MTS.2018.2795093

[5] Bißmeyer, N. (2014) Misbehavior Detection and Attacker Identification in Vehicular Ad Hoc Networks. Ph.D. Thesis, Technical University of Darmstadt, Darmstadt.

[6] Upadhyaya, A.N. (2018) Attacks on VANET Security. *International Journal of Computer Engineering & Technology* (*IJCET*), **9**, 8-19.

[7] Yi, S. and Kravets, R. (2002) Key Management for Heterogeneous Ad Hoc Wireless Networks. *Proceedings of 10th IEEE International Conference on Network Protocols*, Paris, 12-15 December 2002, 202-203.

[8] Khan, U., Agrawal, S. and Silakari, S. (2014) Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks. *Proceedings of International Conference on Information and Communication Technologies*, Kochi, 3-5 December 2014, 965-972. https://doi.org/10.1016/j.procs.2015.01.006

[9] Wang, X., Mavromatis, I., Tassi, A., Santos-Rodriguez, R. and Piechocki, R.J. (2019) Location Anomalies Detection for Connected and Autonomous Vehicles. *Proceedings of* 2019 *IEEE* 2*nd Connected and Automated Vehicles Symposium* (*CAVS*), Honolulu, 22-23 September 2019, 1-5. https://doi.org/10.1109/CAVS.2019.8887778

[10] Grover, J., Laxmi, V. and Gaur, M.S. (2012) Misbehavior Detection Based on Ensemble Learning in VANET. In: Thilagam, P.S., Pais, A.R., Chandrasekaran, K. and Balakrishnan, N., Eds., *Advanced Computing, Networking and Security*, Vol. 7135, Springer, Berlin, 602-611. https://doi.org/10.1007/978-3-642-29280-4_70

[11] Ghaleb, F.A., Zainal, A., Rassam, M.A. and Mohammed, F. (2017) An Effective Misbehavior Detection Model Using Artificial Neural Network for Vehicular Ad Hoc Network Applications. *Proceedings of* 2017 *IEEE Conference on Application, Information and Network Security* (*AINS*), Miri, 13-14 November 2017, 13-18. https://doi.org/10.1109/AINS.2017.8270417

[12] Barnwal, B.P. (2012) Heartbeat Message Based Misbehavior Detection Scheme for Vehicular Ad-Hoc Networks. *Proceedings of* 2012 *International Conference on Connected Vehicles and Expo*, Beijing, 12-16 December 2012, 29-34. https://doi.org/10.1109/ICCVE.2012.14

[13] Azuma, S., Tsukada, M. and Sato, K. (2018) A Method of Misbehavior Detection with Mutual Vehicle Position Monitoring. *Proceedings of International Journal on Advanced in Internet Technology*, **11**, 82-91.

[14] Watanabe, Y., Sato, K. and Takada, H. (2018) DynamicMap 2.0: A Traffic Data Management Platform Leveraging Clouds, Edges and Embedded Systems. *International Journal on Intelligent Transport Systems Research*, **18**, 77-89. https://doi.org/10.1007/s13177-018-0173-7

[15] Chandola, V., Banerjee, A. and Kumar, V. (2009) Anomaly Detection: A Survey. *ACM Computing Surveys*, **41**, Article No. 15. https://doi.org/10.1145/1541880.1541882

[16] So, S. (2019) Self-Reliant Misbehavior Detection in V2X Networks. M.S. Thesis, Boston University, Boston.

[17] SPACE-TIME Engineering Scenargie. https://www.spacetime-eng.com/jp/products

[18] Koga, D., Ikeda, M. and Barolli, L. (2016) Impact of Delayed Acknowledgment for Message Suppression in Vehicular-DTN. In: Barolli, L., Xhafa, F. and Yim, K., Eds., *Advances on Broad-Band Wireless Computing, Communication and Applications*, Vol. 2, Springer, Cham, 199-208. https://doi.org/10.1007/978-3-319-49106-6_18