A Method of Misbehavior Detection with Mutual Vehicle Position Monitoring

Shuntaro Azuma
Computer and Information Science
Graduate School of Science and Engineering
Doshisha University
Kyoto, Japan
email:syuntaro.azuma@nislab.doshisha.ac.jp

Manabu Tsukada
Graduate School of Information
Science and Technology
Tokyo University
Tokyo, Japan
email:tsukada@hongo.wide.ad.jp

Kenya Sato
Computer and Information Science
Graduate School of Science and Engineering
Doshisha University
Kyoto, Japan
email:ksato@mail.doshisha.ac.jp

***Abstract*—Due to the development of vehicle-to-vehicle (V2V) communication, safe driving support such as collision prevention and adaptive cruise control has been achieved. In addition, vehicle-to-infrastructure (V2I) communication as well as communication with a cloud server using mobile lines (vehicle-to-cloud communication) have been developed in recent years. These communications are altogether called vehicle-to-everything (V2X) communication. Through V2X communication, a vehicle's peripheral information can be shared with other vehicles on a cloud server. However, the problem of masquerade attacks on the cloud must be addressed. By faking vehicle information on a cloud server, an adversary may deliberately cause traffic congestion and/or accidents. In this research, we proposed a method that detects misbehavior (masquerade data) from aggregated data on a cloud server using V2X communication by utilizing the surrounding vehicle information. We also analyzed possible threats and requirements for data that are sent to cloud servers, and evaluate the proposed method's implementation. Using the proposed method, we detected 93% of the masquerade data, improved the detection rate by 100% by increasing the threshold value of the proposed method, and enhanced the effect of guaranteeing the data's reliability. Furthermore, we evaluated the false positives of the proposed method and its execution processing time, examining the method's feasibility.**

***Keywords*–vehicle security; V2X communication; detecting masqueraded data.**

I. INTRODUCTION

This paper is based on ”A Method of Detecting Camouflage Data with Mutual Vehicle Position Monitoring” published in VEHICULAR 2017[1]. This paper consists of 6 sections. We describe the background of this research in section II. In section III, we compare existing research and analyze the threat of vehicle spoofing to clarify the novelty and goal of this research. We show our proposed method in section IV, and we describe its evaluation and consideration in section V. Considering the evaluation, we offer insight to our future work in section VI, and summarize this research in the final section VII.

II. BACKGROUND

In recent years, research on autonomous driving and vehicle-to-vehicle (V2V) communication are being conducted in the Intelligent Transport Systems (ITS) field. In addition to providing V2V communication using the Vehicular Ad hoc Network (VANET), vehicles can engage in vehicle-to-infrastructure (V2I) communication with roadside aircraftst and vehicle-to-pedestrian (V2P) communication with tablets owned by pedestrians. Vehicles can also do vehicle-to-cloud (V2C) communication with cloud servers using mobile lines. These communication methods listed above are generally referred to as vehicle-to-everything (V2X) communication. When vehicles perform V2X communication, cloud servers can collect various kinds of information, and we can create a Local Dynamic Map (LDM) [2] for cooperative driving from the collective management of road and vehicle information. This type of communication sometimes is referred as probe information systems [3] or floating car data (FCD) [4]. In addition, various systems and services can be provided, which includes simplification of management tasks such as summarizing operation results, analyzing operation trends, summing up tasks, and simplifying the input of daily reports.

On the other hand, in a system using a cloud server, masquerade data transfer to a cloud influences a system. Attacks against safe driving support services using a cloud pose a threat because the intentional transfer of masquerade data to a cloud are on the rise. Attackers can block roads or cause traffic congestion by sending fake traffic accident information to a cloud server. Various masquerade techniques of vehicle disguise have been identified, such as faking driving and position information as well as a vehicle ’s condition. In this research, we focus on masqueraded position information among all of the data received by a cloud server from vehicles, and we attempt to detect them by mutually monitoring the position information of vehicles using V2X communication.

III. RELATED WORK

There are previous work researching the detection of malicious vehicles in V2X communication [5] [6], but in reality, the definition of a malicious vehicle is ambiguous. In this section, we analyze attacks on vehicle communication and clarify what kind of malicious vehicles to be solved in this research.

TABLE I. THREATS ANALYSIS ABOUT TRANSMISSION DATA

THREAT		REQUIREMENT	COUNTERMEASURE
Eavesdropping		Confidentiality	Encryption
Falsification		Completeness	Encryption
Spoofing	Vehicle impersonation	Node reliability	PKI
	Data masquerade	Date reliability	**Target of this research**

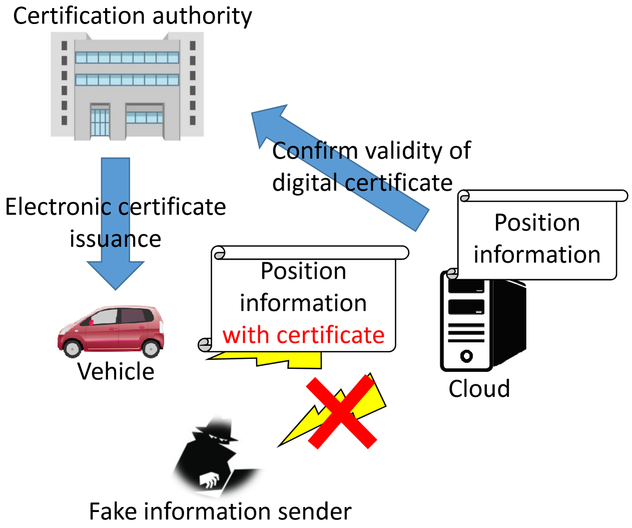

Certification authority
Electronic certificate issuance
Confirm validity of digital certificate
Position information
Position information with certificate
Vehicle
Cloud
Fake information sender

Figure 1. PKI to adapt to vehicles

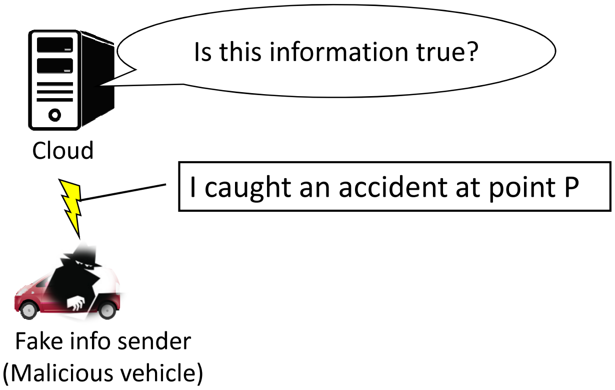


Figure 2. Problem of settling by this research

A. Threat Analysis of Transmission Data

Table I shows the threat analysis of data transmitted to a cloud server. These threats include eavesdropping attacks, falsifications, and spoofing. Spoofing attacks are divided into vehicle impersonation and data masquerade. Vehicle impersonation means that attackers pretend to be other vehicles. For example, even though one vehicle does not have any trouble, an attacker pretends to be another vehicle and then calls the police lying that it had an accident. An example of data masquerade is when a vehicle's own position information or status is masked.

Security requirements regarding these threats include confidentiality, completeness, node reliability, and data reliability. To supply confidentiality and completeness, data encryption is proposed and can be done by a secret key or an ID base cipher. Node reliability identifies vehicles that are pretending to be other vehicles. The Public Key Infrastructure (PKI) method, which is adapted by the vehicles, is one good resolution because certificates guarantee vehicles. Data reliability prevents attackers from masquerading data. However, this is not effective for all spoofing acts.

B. Difference Between Node and Data Reliability

Node reliability means that a cloud server trusts a particular vehicle and believes that it is not pretending to be a different vehicle. The previous section showed that the PKI method can be adapted by vehicles to resolve the problem. A cloud may be able to verify the electronic certification and confirm the transmitter's information by the mechanism shown in Figure 1.

On the other hand, this research focuses on data masquerade, as described in Figure 2. Since data encryption and PKI do not confirm whether the received data are masqueraded, data masquerade is inherently different from node reliability which can be resolved by these methods. We will propose a method that can handle such example, which guarantees the reliability of the data.

IV. PROPOSAL

In this section, we will propose a method to detect misbehavior from data transmitted to a cloud.

A. Outline

Vehicles can use V2X communication. When they send their position information to a cloud server, they also send other information in addition to their position. In this research, a cloud server detects masqueraded data from transmitted data by using the relay base station information in V2C communication and peripheral vehicles in V2V communication. We will explain separately them to simplify our proposing method.

B. Presuppositions

1) A safe channel has been secured by relationships of mutual trust among all vehicles and cloud servers
2) Vehicles and cloud servers have been mutually certified beforehand.
3) Relationships between cloud servers and base stations have been built.

C. Definition of Terminology in Proposed Method

- Vehicle ID

This ID is used by vehicles in V2V communication, and this is a different public ID for each vehicle.

- V2C Vehicle ID

This ID is used for a unique key in V2C communication. This secret ID is not available to others. V2C Vehicle ID and Vehicle ID is uniquely related.

- Via Base Station (BS) ID

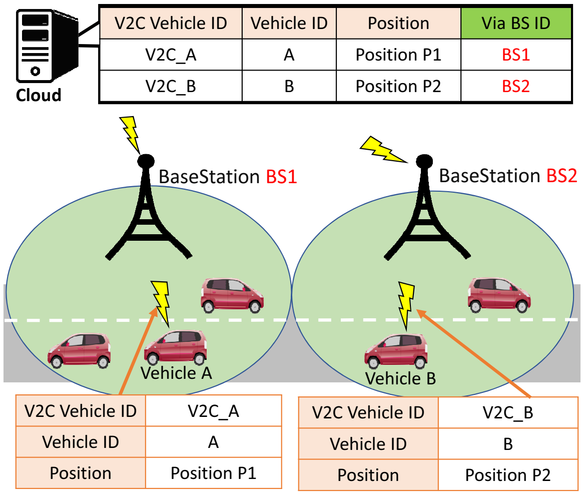
This ID is used in V2C communication, and this is a different ID for each base station.

- Peripheral Vehicle (PV) ID

This ID is a received vehicle ID from other vehicles in V2V communication.

D. Use of Base Station's Information in V2C Communication

When sending position information in V2C communication, vehicles attach V2CVehicleID to their position information, and send it to a cloud. A relay base station on the V2C communication attaches its own ViaBSID to information which was sent from vehicles and encapsulates it. V2CVehicleIDs of all vehicles are registered in cloud servers, and cloud servers can be known from which vehicles inquiry when they confirm these IDs. A possible communication range covered by



V2C Vehicle ID	Vehicle ID	Position	Via BS ID
V2C_A	A	Position P1	BS1
V2C_B	B	Position P2	BS2

V2C Vehicle ID	V2C_A
Vehicle ID	A
Position	Position P1

V2C Vehicle ID	V2C_B
Vehicle ID	B
Position	Position P2

Figure 3. Use example of base station's information in V2C communication

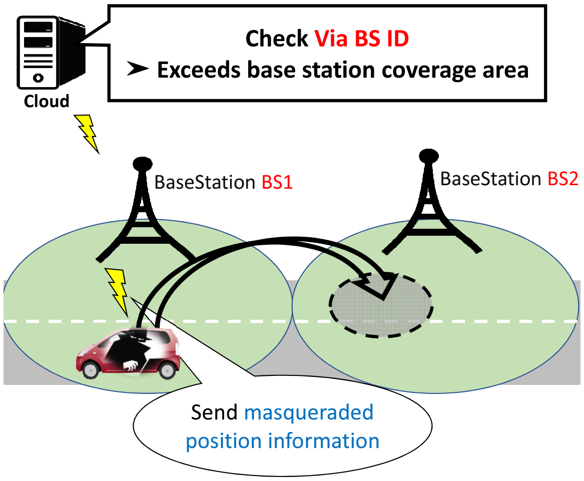

Cloud
Check Via BS ID
➤ Exceeds base station coverage area
BaseStation BS1
BaseStation BS2
Send masqueraded position information

Figure 4. Advantage of using base station's information

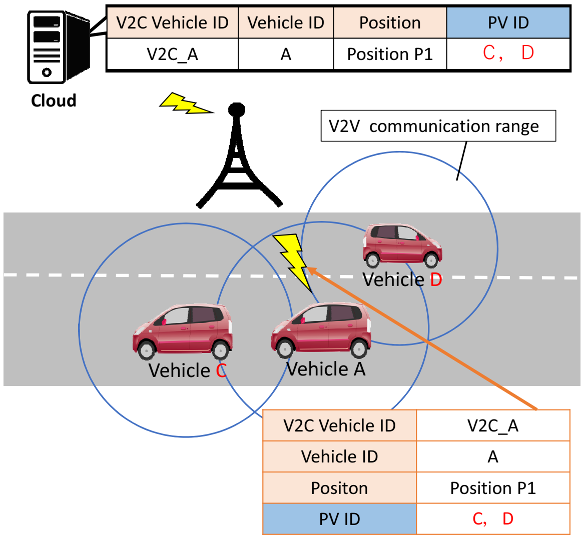
base station's area and ViaBSIDs are also registered in cloud servers.

Figure 3 indicates an example of base station's information in V2C communication. Vehicles possess own V2CVehicleID; base stations also possess own ViaBSIDs. V2CVehicleIDs shall be V2C_A or V2C_B, and ViaBSIDs shall be BS1 or BS2 to explain simply. When vehicles perform V2C communication, a cloud can obtain not only VehicleID or vehicle's position information but also ViaBSID and V2CVehicleID.

Figure 4 shows a countermeasure example of position data masquerade. We can detect masqueraded position information toward another base station using relay base station's information in V2C communication.

E. Use of Peripheral Vehicle's Information in V2V Communication

Vehicles exchange VehicleIDs with nearby vehicles in V2V communication. We define that peripheral vehicles are traveling vehicles within V2V communication coverage area, and PVID is received vehicleID from a peripheral vehicle. In our proposed method, only VehicleID is exchanged in V2V communication.



V2C Vehicle ID	Vehicle ID	Position	PV ID
V2C_A	A	Position P1	C， D

V2C Vehicle ID	V2C_A
Vehicle ID	A
Positon	Position P1
PV ID	C, D

Figure 5. Use example of peripheral vehicle information in V2V communication

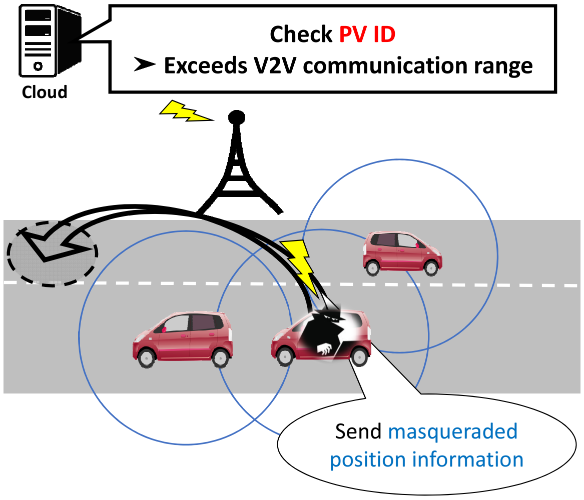
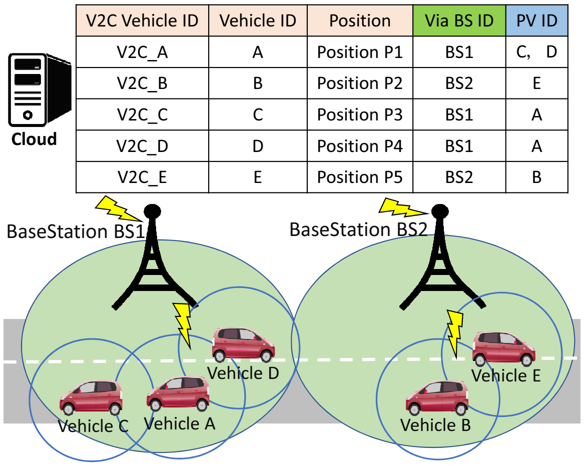

Cloud
Check PV ID
➤ Exceeds V2V communication range
Send masqueraded position information

Figure 6. Advantage of using peripheral vehicle information

When vehicles send their position information to a cloud, these information include V2CVehicleID, VehicleID, and received PVIDs in V2V communication. PVIDs show a guarantee that nearby vehicles exist in V2V communication coverage area. Figure 5 shows an example of peripheral vehicle's information in V2V communication. Vehicle A communicates with the vehicle C and D which are traveling in V2V communication coverage area, and acquires those vehicle IDs. Vehicle A handles acquired VehicleIDs as PVIDs, and a cloud use PVIDs to check Vehicle A's position information with peripheral Vehicles C and D.

Figure 6 shows a countermeasure example of position data masquerade. We assume that a malicious vehicle masquerades its own position information. A cloud confirms PVIDs sent from a vehicle and compares received position information with peripheral vehicle's positions which are relevant to PVIDs. When a cloud finds that transmitted position information is outside V2V communication coverage with peripheral vehicles, the cloud determines that the received position information has been masqueraded. However when this information



V2C Vehicle ID	Vehicle ID	Position	Via BS ID	PV ID
V2C_A	A	Position P1	BS1	C, D
V2C_B	B	Position P2	BS2	E
V2C_C	C	Position P3	BS1	A
V2C_D	D	Position P4	BS1	A
V2C_E	E	Position P5	BS2	B

Figure 7. Use example of peripheral vehicle information in V2X communication

does not exceed the coverage area, the cloud trusts the received position information. Vehicles acquire peripheral vehicle information in V2V communication and mutually monitor them. This helps cloud servers detect masqueraded data.

F. Detection Method of Misbehavior With V2X Communication

Our proposed method is a combination of two described above by using V2X communication (Figure 7). A cloud receives not only position information or VehicleID but also peripheral vehicle's and relay base station's information. Masqueraded data can be detected through these information, as described in Figure 8.

V2CVehicleID is used in the first step on Figure 8. Cloud servers confirm whether received data is sent from vehicles or not. Second, cloud servers compare ViaBSID with received position information to confirm whether a sending vehicle exists in relay base station's coverage area. When receives position information exceeds this area, we assume that it can't be consistent and that received information was regarded as masqueraded data. This step helps detect data masquerade toward other base station's coverage area. At the third or fourth step, cloud servers detect masqueraded data by using PVIDs. Third, cloud servers search vehicles corresponding to sending vehicle's PVID, and firth, they compare received position information with peripheral vehicle's position corresponding to PVID. If the distance between two vehicle's position exceeds V2V communication coverage, we assume that it can't be consistent and that received information was regarded as masqueraded data. This operation is performed a predetermined number of times. In proposed method, a predetermined number of times means the number of PVIDs which is necessary for cloud servers to trust. This is a so-called threshold value. By setting threshold, we can assure more reliable data.

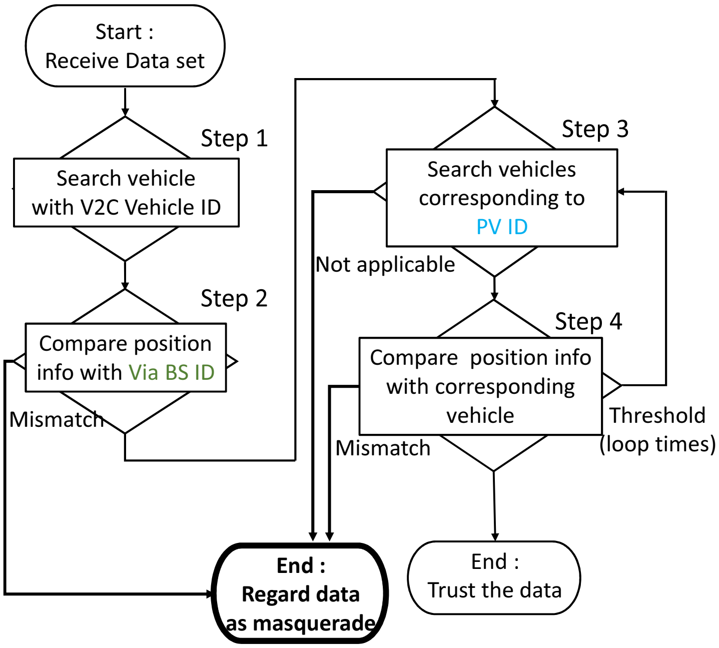


Figure 8. Misbehavior detection procedure to a vehicle send data

V. EVALUATION AND CONSIDERATION

To evaluate the usefulness of our proposed misbehavior detection, we will calculate the evaluation. Then we will consider the practicality of our proposal from the obtained evaluation.

A. Simulator

In this paper we use Scenargie [7] as a simulator to evaluate the performance of our proposed method. Scenargie is a network simulator developed by Space-Time Engineering (STE). By combining expansion modules such as LTE, V2V communication and multi-agent, we can construct a realistic simulation. In addition, since communication systems and evaluation scenarios are becoming more complicated, this ingenious simulation has greatly reduced the effort required to create scenarios.

B. Evaluation Model

For a evaluation environment, we use one square kilometer Manhattan model and use simulation parameters shown in Table II. We set the number of vehicles to 158 [cars] and the range to 1 [km^2] because the average car density in Japan is 158 [cars/km^2]. ITU-R P.1411 model is a radio wave propagation scheme that considers road map information, and radio waves are attenuated based on the shape of the road, so we compared with a two-ray model which includes direct waves and reflected waves from the ground, this model is close to reality. Figure 9 shows one scene when the simulator is active.

TABLE II. SIMULATION PARAMETER

Simulator	Scenargie2.0	
Vehicle number	158 [cars] (five of the send masquerade positions.)	
Area	1000 [m] × 1000 [m]	
Communication mode	ARIB STD T109	LTE
Use frequency band	700 [Mhz]	2.5 [GHz]
Communication interval	100 [ms]	1.0 [s]
Radio spread model	ITU-R P.1411	LTE-Macro
Base station ground clearance	1.5 [m]	

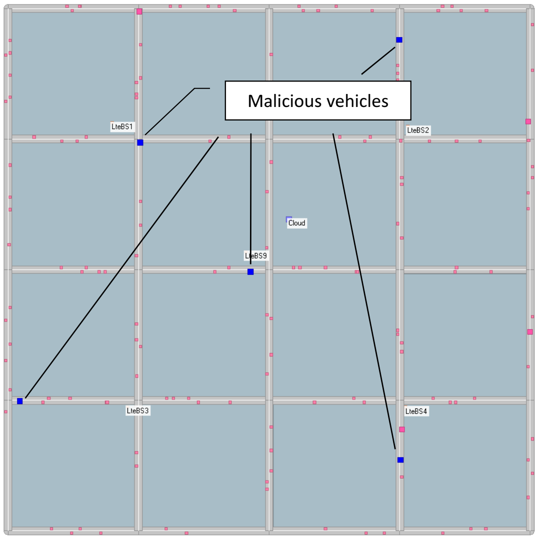


Figure 9. One scene when the simulator is running

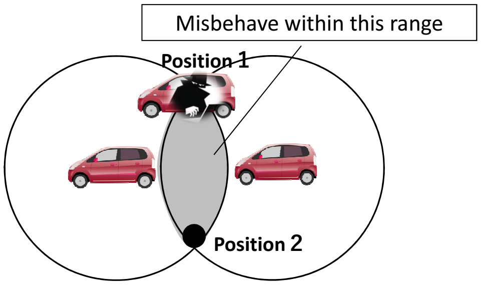


Figure 11. Misbehavior in V2V communication coverage with peripheral vehicles

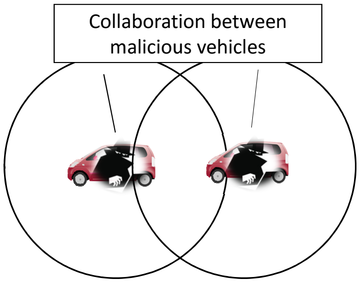


Figure 12. Collusion between malicious vehicles

C. *Evaluation of Misbehavior Detection*

Figure 10 shows per-threshold detection rates of masqueraded data from data aggregated in a cloud server. Masqueraded data transmitted to a cloud could be detected at 100% by increasing the proposed method's threshold. However, when the threshold was low, we could not completely detect all of masqueraded data. The reason is shown in Figure 11 and 12. Figure 11 shows an example of misbehavior in V2V communication coverage with peripheral vehicles. A malicious vehicle masquerades its own position (position 1) to position 2 in V2V communication coverage. In this case, since peripheral vehicles guarantee masqueraded information from a malicious vehicle, a misbehavior becomes possible. Figure 12 shows a collusion between malicious vehicles. Since they mutually guarantee masqueraded position information, cloud server trusts these information. However, these problems can be addressed by increasing the prescribed number of times (threshold values) in Figure 8. By increasing the threshold values, we can create the situation shown in Figure 13, and it is possible to limit masquerading by malicious vehicles.

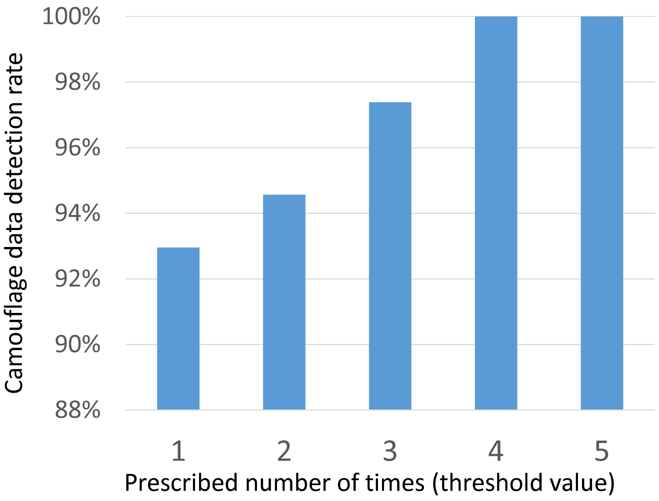


Figure 10. Misbehavior detection rates in a cloud received data

D. *Evaluation of Misdetection Rate*

Figure 14 shows false detection rates (false positives) of our proposed method, which is based on the average vehicle density in Japan. The method's threshold is the number of PVIDs which is necessary for cloud servers to trust. In the previous section, we found that an increase in the threshold improves the detection rates of masqueraded data. Here, we will calculate the false positive detection rates (false positive), regarding whether cloud servers trust information on vehicles that are not misbehaving.

In the simulation environment shown in Table V, Figure 14 shows that the false positives when all 158 cars are not misbehaving. By increasing the threshold value, false positive rates improved. Increasing the threshold value under Japanese average vehicle density, cloud servers erroneously detects normal communication as abnormal.

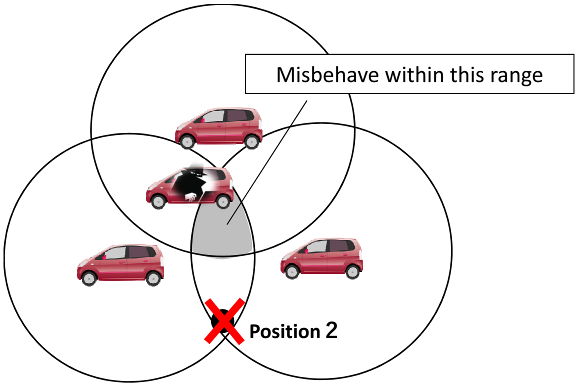


Figure 13. Restriction on misbehavior accompanying an increase in information on peripheral vehicles

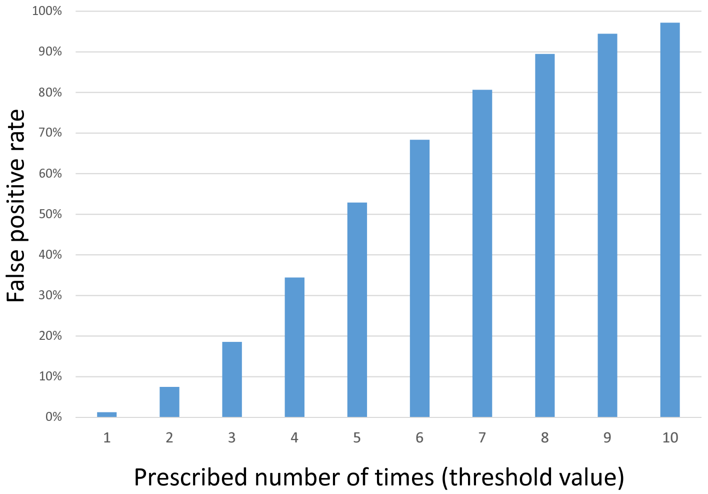


Figure 14. False positives by threshold values under Japanese average vehicle density (158[cars/km^2]) environment

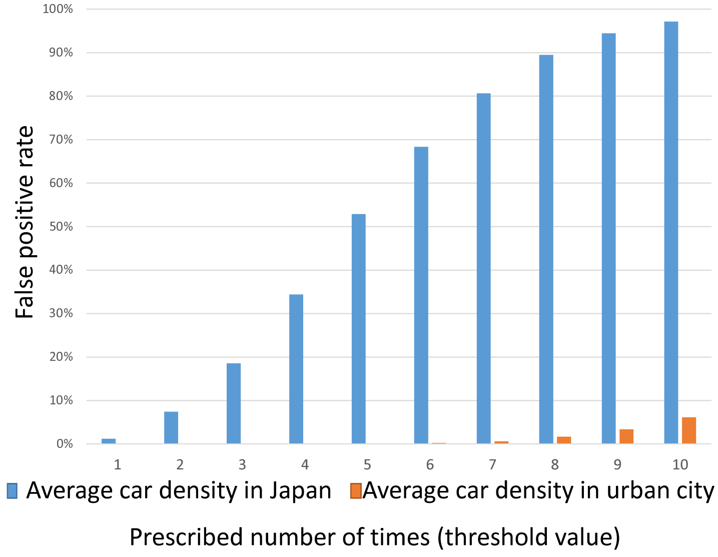


Figure 15. False positive comparison with urban area's average vehicle density (1128 [cars/km^2]) environment

Then, the false positive rates under the average vehicle density environment in urban city (Osaka), which has the highest average car density in Japan, are shown in Figure 15. In a high vehicle density area, since vehicles can acquire a lot of peripheral vehicle information in V2V communication, even if the threshold is increased, an increase of the false detection rate can be suppressed. Therefore, we found that our proposed method is more effective in areas with high vehicle density than lower density. Actually the influence of masquerading vehicle information is great in areas with high vehicle density. Malicious act such as faking driving and position information may cause the large accident in higher density than lower. Our proposed method can guarantee transmitted information from vehicle to cloud servers, and it works better in areas with a larger number of peripheral vehicles than in areas with fewer peripheral vehicles. Our proposed method is useful in traffic congestion zones where data masquerade has a huge impact. Table III and IV show precision, recall, and F-measure in our proposed method. Even looking at this table, we can say the same above.

TABLE III. F-MEASURE UNDER 158[cars/km^2] ENVIRONMENT

Threshold	1	2	3	4	5	6	7	8	9	10
Precision	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
Recall	0.99	0.93	0.81	0.66	0.47	0.32	0.19	0.11	0.056	0.029
F-measure	0.99	0.96	0.90	0.79	0.64	0.48	0.32	0.19	0.11	0.056

TABLE IV. F-MEASURE UNDER 1128[cars/km^2] ENVIRONMENT

Threshold	1	2	3	4	5	6	7	8	9	10
Precision	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
Recall	1.0	1.0	1.0	1.0	1.0	1.0	0.99	0.98	0.97	0.94
F-measure	1.0	1.0	1.0	1.0	1.0	1.0	1.0	0.99	0.98	0.97

E. *Comparison of ARIB STD-T109 and IEEE 802.11P*

ARIB STD-T109 is a V2V communication's standard used in Japan. In a previous evaluation we used this standard based on V2V communication in the simulator. IEEE802.11p is a Dedicated Short Range Communication (DSRC) standard for wireless vehicular networks in the United States and Europe [8] [9]. IEEE802.11p, which is the standard for transports and the network layers, is standardized as the part of IEEE 1609 [10] family and defines the architecture and security physical layer access etc. for DSRC. The main differences between ARIB STD-T109 and WAVE are the frequency band and the number of channels. We will confirm that what kind of difference using ARIB STD-T109 will make with IEEE802.11p in our proposed method. The simulation environment using IEEE802.11p is shown in Table V.

F. *Differences Among Misbehavior Detection Rates*

Figure 16 shows the per-threshold detection rates of masqueraded data from data aggregated on a cloud server. Unlike Figure 10, it is the result of using IEEE802.11p. Compared to using T109, the detection rates improve with IEEE802.11p. When the threshold value is 3, the detection rate is 100%. To determine this difference, our proposed method must determine how much vehicles communicate with peripheral vehicles. If there are many communication targets around a vehicle, cloud servers can trust vehicles and exclude malicious vehicles. T109 has a lower frequency than IEEE802.11p. However since IEEE802.11p has strong propagation strength, vehicles can be communicated to more peripheral vehicles, leading to better results.

G. *Differences Among Misdetection Rates*

Figure 17 shows the false detection rates (false positives) of the proposed method based on the average car density in Japan when we used IEEE802.11p. It shows considerably better results than Figure 14. As stated above, this is related

TABLE V. SIMULATION PARAMETER

Simulator	Scenargie2.0	
Vehicle number	158 [cars] (five of the send masquerade positions.)	
Area	1000 [m] × 1000 [m]	
Communication mode	IEEE802.11p	LTE
Use frequency band	5.9 [Ghz]	2.5 [GHz]
Communication interval	100 [ms]	1.0 [s]
Radio spread model	ITU-R P.1411	LTE-Macro
Base station ground clearance	1.5 [m]	

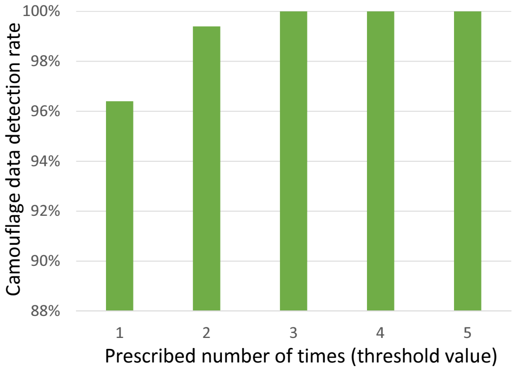


Figure 16. Misbehavior detection rates in a cloud received data when using IEEE802.11p

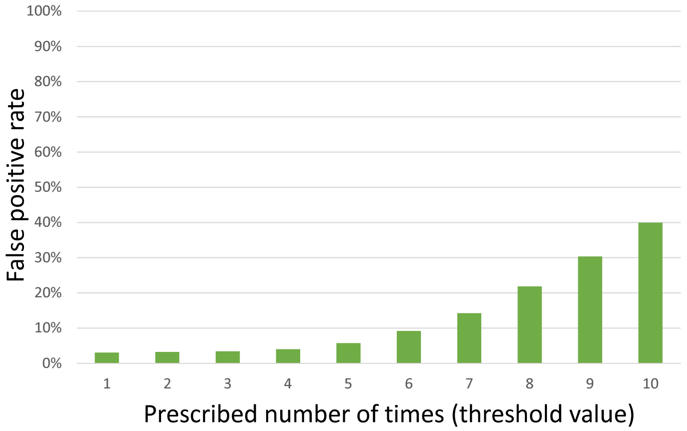


Figure 17. False positives by threshold value under Japanese average vehicle density (158[cars/km^2]) environment when using IEEE802.11p

to the fact that vehicles using IEEE802.11p can communicate with peripheral vehicles, and our proposed method works well.

Figure 18 indicates the false positives under an average vehicle density environment in an urban city (Osaka), which has the highest average car density in Japan. The graph shows almost the same result as Figure 17. When T109 was used, the results were significantly different depending on the car density because the number of peripheral vehicles (that can communicate) increased due to the greater vehicle density. However, since there is only slight difference when IEEE802.11p is used, we believe that it was probably communicating with vehicles that can already communicate under an average Japanese car density environment. This means that the results did not change even under an average Japanese vehicle density environment. When using T109, a suitable threshold must be set for various vehicle densities, but since there is no change in the decreasing positives when using IEEE802.11p, a certain threshold may be satisfied under any vehicle density environment.

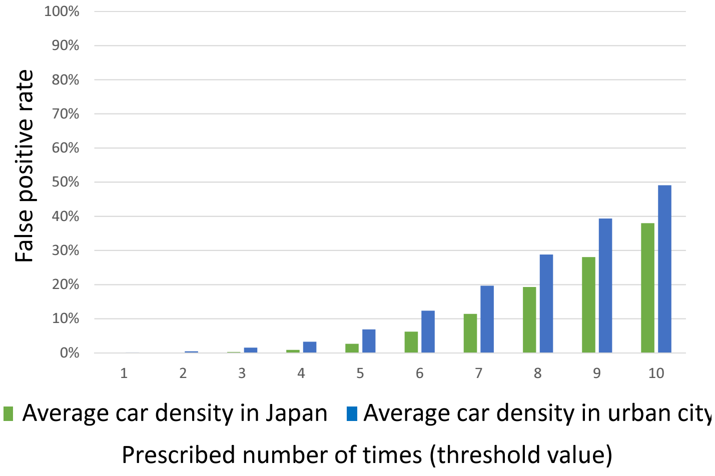


Figure 18. False positive comparison with urban area's average vehicle density (1128 [cars/km^2]) environment when using IEEE802.11p

H. *Evaluation When Increasing Malicious Vehicles*

We believe that we can improve our proposed system by increasing the number of malicious vehicles and setting the threshold value to 5. When the number of malicious vehicles is increased, the false positives are shown in Figure 19, and 20. In both T109 and IEEE802.11p, the amount of the false positives did not change even when the malicious vehicles are increased because five regular vehicles were included in the communication targets (peripheral vehicles). Therefore, even ian increase in the number of malicious vehicles increases did not affect the false positives of regular vehicles. Unfortunately, this result is not good.

In our proposed method, all communicating vehicles are regarded as peripheral vehicles that can guarantee their own position information. Even if there are malicious vehicles in the position information, no problem occurs as long as a threshold number of regular vehicles exists. For example, we assume that a certain vehicle communicates with 20 peripheral vehicles. When 15 out of 20 units are malicious, should this vehicle be trusted by the cloud? Although the present system is supposed to trusted ism, more than half of the surrounding vehicles are probably malicious. In other words, even though a malicious vehicle may be correctly identified, we can accept a majority of the opinions. This influence increases the number of vehicles that are identified as malicious.

I. *Measurement of Processing Time in Our Proposal*

In the evaluation environment shown in Table VI, the processing time necessary for the detection of masqueraded data is evaluated by Table VII and Table VIII, based on the flowchart of Figure 8. It shows the processing time for one vehicle. By using BSIDs, masqueraded data can be detected at the beginning of processing by the proposed method, and

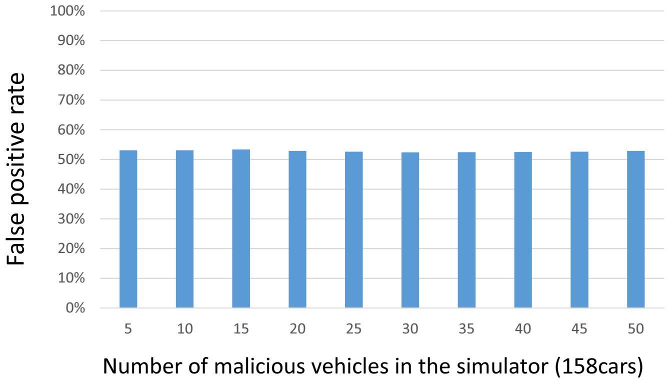


Figure 19. False positives by number of malicious vehicles under Japanese average vehicle density (158[cars/km^2]) environment when using T109

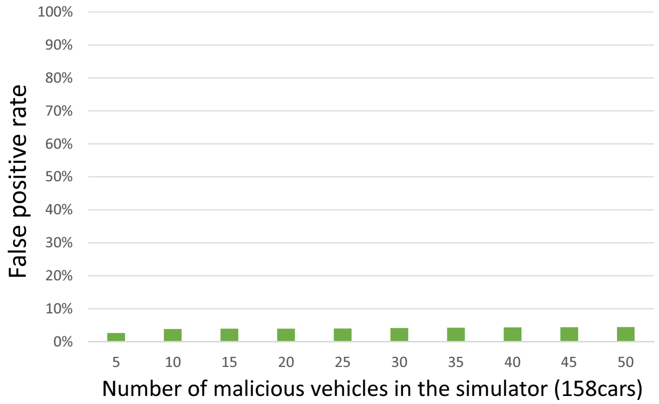


Figure 20. False positives by number of malicious vehicles under Japanese average vehicle density (158[cars/km^2]) environment when using IEEE802.11p

TABLE VI. ENVIRONMENT IN THE PROCESSING TIME MEASUREMENT

OS	macOS Sierra
Processor	1.6GHz Intel corei5
Memory	8GB 1600MHzDDR3
Script	Python
Data base	MySQL, posgreSQL

the processing time becomes relatively fast. In the detection method using PVIDs, the processing time is different for each threshold. By increasing the threshold value, the detection procedure of masqueraded data by PVID is repeated. Even during the repetition, since the processing time changes depending on whether comparative data can be found relatively early or in the final stage, a range was set for the processing time up to Step 4. A case where no masqueraded data is not detected is defined as normal termination, and the upper limit of the processing time at that threshold is indicated. As the threshold of our proposed method increases, the processing time required for normal termination increases. Furthermore, we confirmed that the processing time varies depending on the type of database. As a result of calculating the evaluation under the same condition, we found that MySQL is faster in processing time than posgreSQL.

TABLE VII. PROCESSING TIME OF UNJUST MEASURE TO A VEHICLE OF SEND DATA ON MYSQL

Threshold	Detected in step2	Detected in Figure 8's step4	Usual end
1	0.10[ms]	0.31[ms]	0.31[ms]
2	0.10	[0.31,0.53]	0.53
3	0.10	[0.31,0.76]	0.76
4	0.10	[0.31,0.96]	0.96
5	0.10	[0.31,1.2]	1.2
6	0.10	[0.31,1.4]	1.4
7	0.10	[0.31,1.6]	1.6
8	0.10	[0.31,1.8]	1.8
9	0.10	[0.31,2.0]	2.0

TABLE VIII. PROCESSING TIME OF UNJUST MEASURE TO A VEHICLE OF SEND DATA ON POSGRESQL

Threshold	Detected in step2	Detected in Figure 8's step4	Usual end
1	0.15[ms]	0.52[ms]	0.52[ms]
2	0.15	[0.52,0.88]	0.88
3	0.15	[0.52,1.2]	1.2
4	0.15	[0.52,1.6]	1.6
5	0.15	[0.52,2.0]	2.0
6	0.15	[0.52,2.3]	2.3
7	0.15	[0.52,2.7]	2.7
8	0.15	[0.52,3.0]	3.0
9	0.15	[0.52,3.4]	3.4

J. Overall Processing Time

In previous subsection V-I, we showed the processing time in our proposed method, especially the processing time in Figure 8's step 4. If we operate our system in reality, the overall processing time will be as follows.

$$T_{all} = T_1 + T_2 + T_3 \qquad (1)$$

T_{all} : Overall processing time
T_1 : Delay time of V2C communication
T_2 : Database access time
T_3 : Processing time in my proposal

Table VII or VIII which is calculated in the previous subsection corresponds to T_2, T_3. When we consider the total processing time, we need to consider the delay time of V2C communication. We must determine the threshold values based on the V2C communication delay and the allowable range of the delay times of safe driving support systems.

VI. FUTURE WORK

In this section, considering the evaluation result of the previous section we describe what kind of research we will do in the future.

A. Determination of the Appropriate Threshold

The threshold value we set is the number of loops in Figure 8, that is, the number of peripheral vehicles required for a cloud to trust. If we do not decide the appropriate value, our proposed system will not be realistic. Considering the false positive problem, we devise two methods of determining thresholds.

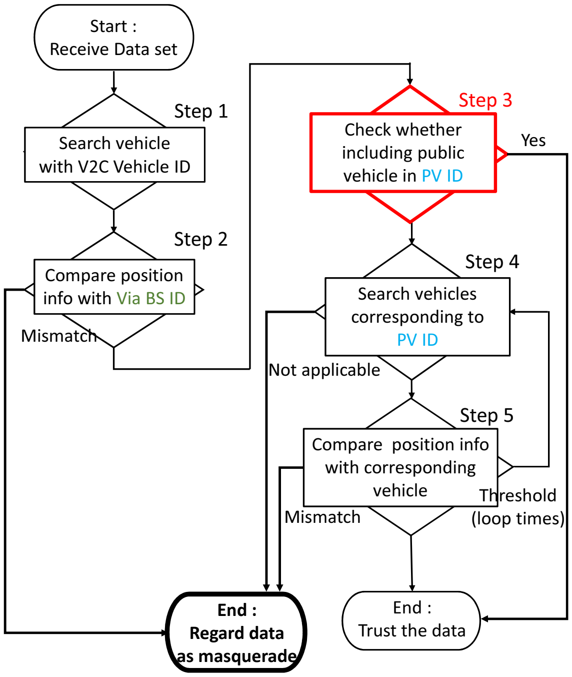


Figure 21. New flowchart introducing vehicle weighting

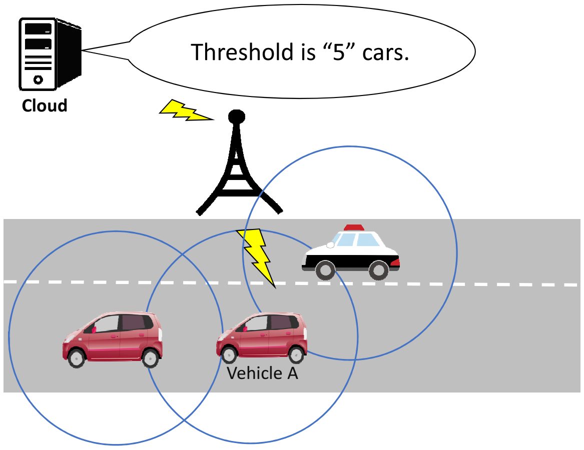


Figure 22. Example when introducing vehicle weighting

1) We weight the public vehicles and trust more on the cloud even for vehicles below the threshold.
2) We dynamicaly determination of threshold value with consideration of vehicle density.

1)This good result (Figure 15, 18) only applies in the urban area. We need to take another measure under the environment of Japanese average car density. And also we must consider the lesser nighttime of car streets and the lower density environment. Figure 21 shows our new countermeasure to the false positive. We give weight to public vehicles such as police vehicles and buses than normal vehicles. Even if the vehicle communicating with the public vehicle (that is, the vehicle including the public vehicle in peripheral vehicle information) does not exceed the threshold value, this one is trusted by a cloud. We consider the environment such a Figure 22. In the case the threshold required for the cloud to trust is 5. Vehicle A has only three peripheral vehicles. But because there are a police vehicle in them, a cloud trusts vehicle A. We think that this method will reduce the false positive if public vehicles are running even in low vehicle density areas.

2)Based on the results (Figure 14,15), we calculate vehicle density for each base station and change the threshold value for each base station. Figure 23 shows the overall picture.

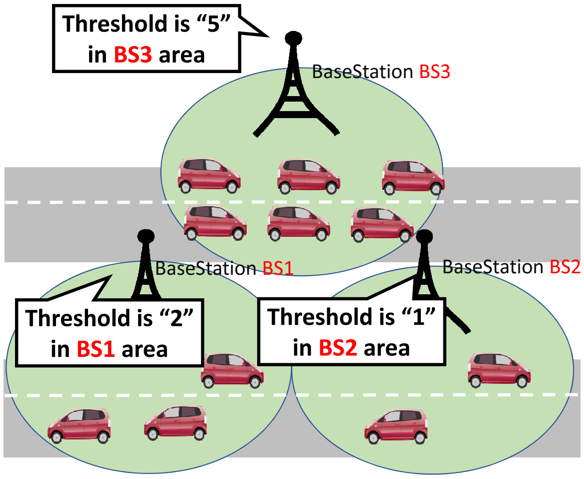
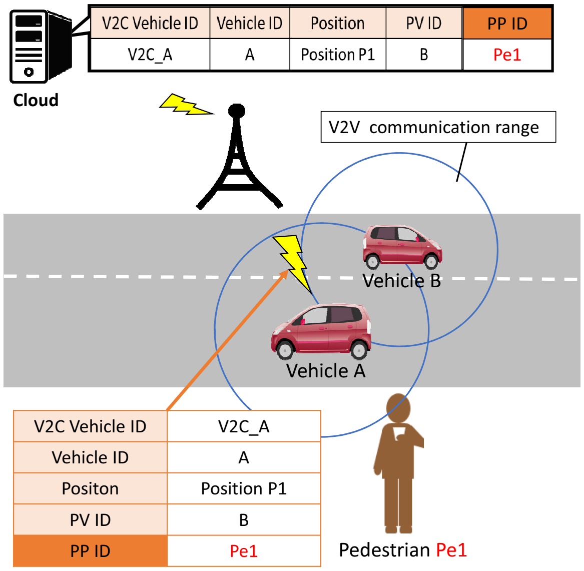

Threshold is “5” in BS3 area
BaseStation BS3
BaseStation BS1
BaseStation BS2
Threshold is “2” in BS1 area
Threshold is “1” in BS2 area

Figure 23. Examples when introducing dynamic threshold determination



V2C Vehicle ID	Vehicle ID	Position	PV ID	PP ID
V2C_A	A	Position P1	B	Pe1

V2C Vehicle ID	V2C_A
Vehicle ID	A
Positon	Position P1
PV ID	B
PP ID	Pe1

Figure 24. Use example of peripheral pedestrian information in V2P communication

Since vehicle information is transmitted to the cloud via a base station, we think that we can calculate the car density inside the base station.

B. Increase in Communication Target

In this research vehicles only communicated with a cloud and other vehicles. There is vehicle-to-pedestrian (V2P) or vehicle-to-device (V2D) communication in V2X communication. If pedestrians can access a LDM with their smartphones, vehicles can mutually monitor the position information by communicating with the device of the pedestrian. Research that pedestrians can easily access LDM exists [11], so we can realize it by using just information exchanged with V2P communication. Figure 24 indicates the example of peripheral pedestrian information in V2P communication. Vehicle A communicating with pedestrian Pe1, vehicle A gets the peripheral pedestrian ID (PPID). Then vehicle A send these information to a cloud. A cloud can judge whether to trust also from information other than peripheral vehicle information. We think that we can further improve our proposed system.

However there is a problem that the amount of information transmitted by vehicles to a cloud increases, and another problem is how to set a threshold value. People can possess multiple smartphones simultaneously, so the importance of PPID is lower than PVID. We also need to consider those who use malicious behavior with smartphones.

VII. CONCLUSION

In the Intelligent Transport Systems (ITS), using cloud servers is inevitable. For providing a safe driving support service using cloud servers, masquerading vehicle information and spoofing a vehicle are threatening. In this research, we used V2X communication, obtained information from various objects, and described measures against data masquerade. We proposed a method that detects masqueraded data from information transmitted by vehicles to cloud servers. By using information of relay base stations in V2C communication and peripheral vehicle’s information in V2V communication, and our measures are taken against masquerading vehicle information. By increasing our proposed method's threshold, the detection rates of masqueraded data were improved and vehicle information was made more reliable. Our proposed method can be adapted to depopulated regions by changing the amount of data of peripheral vehicle information required as the detection rates improve based on car densities. In overcrowded vehicle areas, we confirmed that our proposed method works most effectively because there were many peripheral vehicles satisfying the threshold. Further we confirmed that the proposed method works well without problems even under different propagation environment schemes (T109 or IEEE802.11p). False positive problems are our future tasks and we are also considering processing time improved. For future research I would like to conduct a demonstration experiment that also cooperated with LDM.

ACKNOWLEDGMENT

A part of this work was supported by KAKENHI (JP 16H02814) and MEXT program for the strategic research foundation at private universities.

REFERENCES

[1] Shuntaro Azuma, Manabu Tsuakda, and Kenya Sato," A Method of Detecting Camouflage Data with Mutual Vehicle Position Monitoring, " VEHICULAR2017, July 2017.

[2] ETSI," Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM), "EN 302 895 V1.1.1, September 2014.

[3] International Standardization Organization," Vehicle probe data for wide area communications, "ISO 22837, 2009

[4] Ralf-Peter Schafer, Kai-Uwe Thiessenhusen, and Peter Wagner," A traffic information system by means of real-time floating-car data, " DLR, January 2002.

[5] Yang, Yuchen Ou, Dongxiu Xue, Lixia Dong, and Decun," Infrastructure-based Detection Scheme of Malicious Vehicles for Urban Vehicular Network, "Transportation Research Board 96th Annual Meeting, January 2017.

[6] Gongjun Yan, Stephan Olariu, and Michele C. Weigle," Providing VANET security through active position detection, "Computer Communications, Vol.31, pp.2883-2897, July 2008.

[7] SPACE-TIME Engineering. Available from: https://www.spacetime-eng.com/en/ 2017.07.07

[8] Daniel Jiang, Luca Delgrossi," IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments, "Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, pp.1550-2252, May 2008.

[9] Stephan Eichler," Performance Evaluation of the IEEE 802.11p WAVE Communication Standard, "Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th, pp.1090-3038, October 2007.

[10] Xinzhou Wu, Sundar Subramanian, and Ratul Guha," Vehicular Communications Using DSRC Challenges, Enhancements, and Evolution, " IEEE Journal on Selected Areas in Communications, Vol.31, No.9, pp.399-408, September 2013.

[11] Ryosuke Sugisaka, Asahi Aono, Ryota Ayaki, and Kenya Sato," Implementation and Evaluation of the Dynamic Map Based on Web, " DICOMO2017, June 2017.