A Method of Detecting Camouflage Data with Mutual Vehicle Position Monitoring

Shuntaro Azuma, Manabu Tsukada, Teruaki Nomura, Kenya Sato

A Method of Detecting Camouflage Data with Mutual Vehicle Position Monitoring

Shuntaro Azuma
Graduate School of Science
and Engineering Information 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

Teruaki Nomura and Kenya Sato
Graduate School of Science
and Engineering Information Engineering
Doshisha University
Kyoto, Japan

***Abstract*—Due to the development of V2V communication, such safe driving support as collision prevention and adaptive cruise control has been achieved. Furthermore, in recent years, in addition to infrastructure-to-vehicle communication (V2I communication) and communication with a cloud server using mobile lines is also possible (V2C communication), and such communication is generally called V2X communication. Through V2X communication, vehicle's peripheral information can be shared with other vehicles on a cloud server. However, the influence of inappropriate information on the cloud must be addressed. By faking vehicle information, a system using a cloud server, perhaps deliberately causing congestion and/or accidents. In this research, we propose a method that detects camouflage data from all of that aggregated data on a cloud server using V2X communication and utilizing the surrounding vehicle information. We also analyze possible threats and the requirements for the data that are sent to a cloud, clarify security, and evaluate the proposed method's implementation. We detected 93% of the camouflage data, and improved the detection rate 100% by increasing the threshold value of the proposed method and, enhancing the effect of guaranteeing the data's reliability. Furthermore, we showed the false positives of the proposed method and its execution processing time and examined feasibility.**

Keywords–vehicle security; V2X communication; detecting camouflage data.

I. INTRODUCTION

In recent years, research on automatic driving and V2V communication is 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 V2I communication with roadside aircraft and V2P communication with tablets owned by pedestrians. Vehicles can also do V2C communication with a cloud server using mobile lines, and the kinds of communication we mention here are generally referred to as V2X communication. While vehicles perform V2X communication, a cloud server can collect various kinds of information, and we can create a Local Dynamic Map (LDM) [1] for cooperative driving from the collective management of road and vehicle information. This type of communication sometimes is referred as probe information systems [2] or floating car data (FCD) [3]. In addition, various systems and services can be provided, such as the simplification of such management tasks 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, camouflage data transfer to a cloud influences a system. Attacks against safe driving support services using a cloud also pose a threat because the intentional transfer of camouflage data to a cloud camouflage acts are on the rise. Attackers can block roads or cause traffic congestion by sending to a cloud a camouflage information that pretends to be involved in an accident. As a type of vehicle disguising acts, various camouflage acts have been identified, such as camouflaging both driving and position information as well as the vehicle's condition. In this research, we focus on camouflage position information among all of the data received by a cloud from vehicles and detect them by mutually monitoring the position information of vehicles using V2X communication.

II. ANALYSIS THREAT OF TRANSMISSION DATA

There are things researching the detection of malicious vehicles in V2X communication [4] [5], but in reality malicious vehicles are ambiguous. In this section, we analyze attacks on vehicle communication and show what kind of malicious vehicles to be solved in this research.

A. Threats, Requirements, and Resolution example

Table I shows analysis of the transmission data to a cloud server. The threats include eavesdropping attacks, falsifications, and spoofing. Spoofing attacks are divided into vehicle pretense and data camouflage. Vehicle pretense means that attackers pretend to be other vehicles. For example, even though one vehicle doesn't have any trouble, an attacker pretends to be the vehicle and then calls the police with a lie that it had an accident. An example of data camouflage is when a vehicle's own position information or status is masked.

Security requirements about threats includes 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

TABLE I. ANALYSIS THREATS ABOUT TRANSMISSION DATA

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

 ISBN: 978-1-61208-573-9

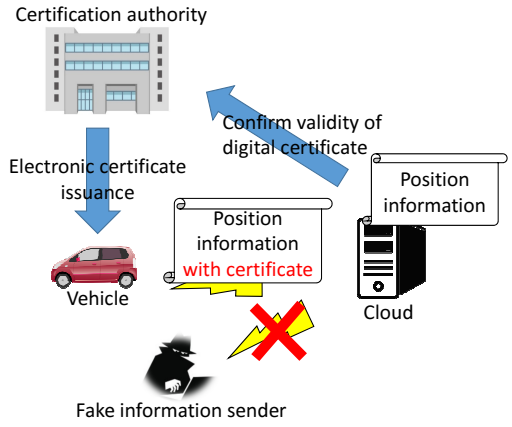

Figure 1. PKI to adapt to vehicles

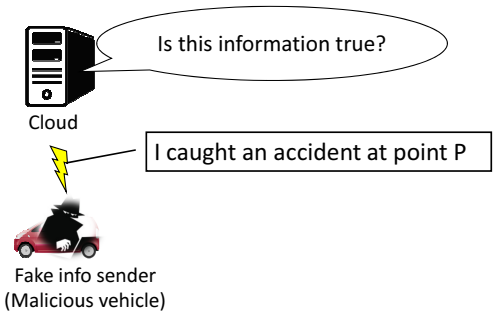

Figure 2. Problem of settling by this research

because the certificate guarantees vehicles. Data reliability prevents attackers from camouflaging data. It doesn't involve resolution at all.

B. Difference Between Node and Data Reliability

Node reliability means that a cloud server trusts a particular vehicle and believes that it isn't pretending to be a different vehicle. The previous section showed that, PKI measures adapts to the vehicles to resolve the problem. A cloud might be able to verify the electronic certification and confirm the transmitter information by the mechanism shown in Figure 1.

This research focuses on such data camouflages, as described in Figure 2 in spoofing acts. Since the data encryption and PKI don't confirm whether the received data are camouflage, the problem, which is resolved by these methods, is different from the one we focus on in this research. We propose a method that can handle such examples as when the given matter, which guarantees the reliability of the data in an act, camouflages vehicle data.

III. PROPOSAL

In this section, we propose a method to detect camouflage data from among data sent to the cloud.

A. Outline

Vehicles use V2X communication. When they send their position information to a cloud server, they also send other information than just their position. In this research, the cloud detects camouflage data from the received data using the relay base station information in V2C communication and peripheral vehicles in V2V communication. We explain them separately to simplify the movement outline of proposed technique.

B. Presuppositions

1) A safe channel has been secured by a preliminary relationship of mutual trust among all vehicles and the cloud server
2) Vehicles and the cloud have been mutually certified beforehand.
3) Relationships of mutual trust have been built by a base station with a cloud server.

C. Definition of Terminology in Proposed Method

- Vehicle ID

The ID used by a vehicle during V2V communication; a public ID that is different for every vehicle.

- V2C Vehicle ID

The ID used for peculiar questions during V2C communication. This secret ID is not available to others. V2C Vehicle and Vehicle IDs are uniquely related.

- Via Base Station (BS) ID

This unique ID in a relay base station for V2C communication. It adopts bidirectional one time ID signaling, and establishes its life-time.

- Peripheral Vehicle (PV) ID

The ID received by a vehicle from other vehicles by V2V communication.

D. Use of Base Station Information in V2C Communication

When sending position information using V2C communication, a vehicle attaches the V2CVehicleID to its position information and sends it to the cloud. The relay base station on the V2C communication, is encapsulated and make a header from the ViaBSID in the position that was sent from a vehicle. The V2CVehicleID for all of the vehicles preserve the registration beforehand in the cloud, which knows a request that can confirm vehicle's identify by checking the V2CVehicleID. The possible communication range covered by a base station's area and the ViaBSIDs are also registered with cloud.

Figure 3 indicates an example of base station information in V2C communication. The vehicles possess V2CVehicleID; the base stations possess ViaBSIDs. The V2CVehicleIDs are regarded as either V2C_A or V2C_B, and ViaBSID, where the base stations are unique, is made by BS1 or BS2 as simple explanations. When a vehicle performs V2C communication, it obtains the information that the cloud will a relay base station as well as its position information: ViaBSID and V2CVehicleID.

Figure 4 shows a countermeasure example of a position data camouflage act. We can detect the position information that is being camouflaged at another base department using the relay base station information in V2C communication.

E. Using Peripheral Vehicle Information in V2V Communication

Vehicles exchange VehicleIDs with nearby vehicles using V2V communication. A vehicle views the other vehicles other vehicles in the potential V2V communication area as peripheral vehicles. A VehicleID that is received from a peripheral

 ISBN: 978-1-61208-573-9

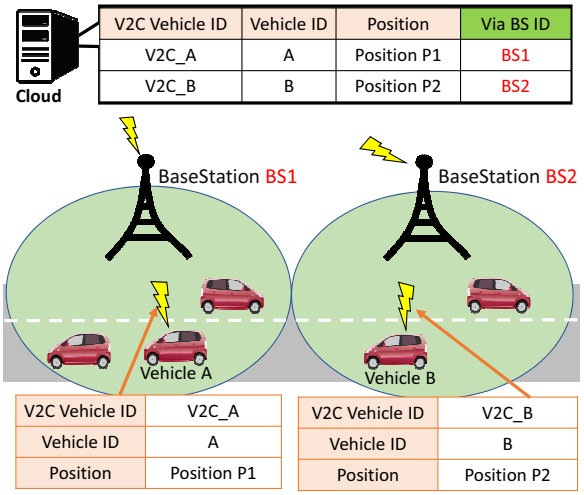

Figure 3. Use example of base station information in V2C communication

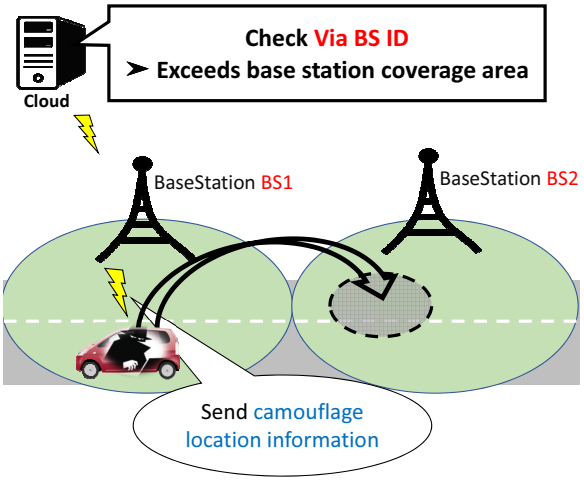

Figure 4. Advantage of using base station information

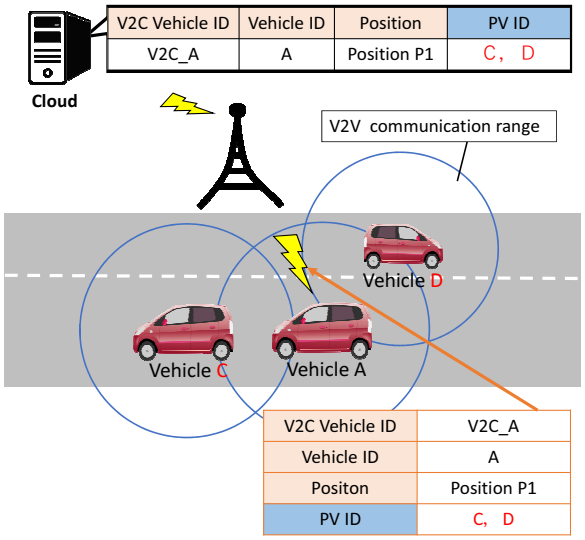

Figure 5. Use example of peripheral vehicle information in V2V communication

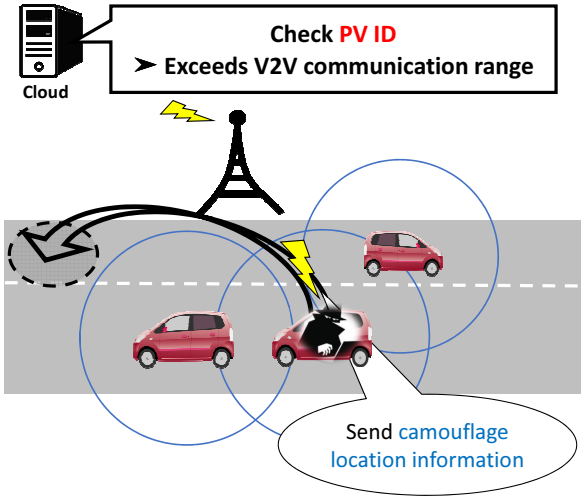

Figure 6. Advantage of using peripheral vehicle information

vehicle is regarded as peripheral vehicle information (PVID). In our proposed technique, only VehicleID information is exchanged by V2V communication.

When a vehicle sends its position information to a cloud, the V2CVehicleID, its VehicleID, and the PVID are attached by V2V communication. The PVID shows a guarantee that nearby vehicles are in the V2V communication possible area. Figure 5 shows an example of peripheral vehicle information by V2V communication. Vehicle A communicates with the others vehicles in the area where V2V communication is possible and acquires VehicleIDs from Vehicles C and D. Vehicle A handles the acquired VehicleIDs as PVIDs and verifies their nearby position with peripheral Vehicles C and D.

Figure 6 shows a countermeasure example of a position data camouflage act. We assume that a malicious vehicle camouflaged its position information. The cloud confirms the PVID sent with the position information from a vehicle, and compares a vehicle's position information that is relevant to the PVID with the information of the vehicle that transmitted. When comparing the position information that is outside the possible V2V communication area, the cloud determined that the received position information has been camouflaged. However when the position information does not exceed the area, the cloud trusts the received position information. Vehicles acquire peripheral vehicle information using V2V communication and mutually monitor it. This helps the cloud detect camouflage data.

F. Detection Method of Camouflage Data With V2X Communication

Our proposed technique is a combination of the two described above by using V2X communication (Figure 7). The cloud receives not only the position and the VehicleID information data but also the data attached to the peripheral vehicles and the relay base station information monitored mutually by V2X communication. Camouflage data can be detected through these data, as described in Figure 8.

The V2CVehicleID is used in the first step on Figure 8. Next, we verified whether the data received by the cloud were sent from a vehicle. Second, we compared the ViaBSID with the position information of a transmission vehicle to confirm whether it exists in the area covered by the relay base station. When the position information of the transmission vehicle

 ISBN: 978-1-61208-573-9

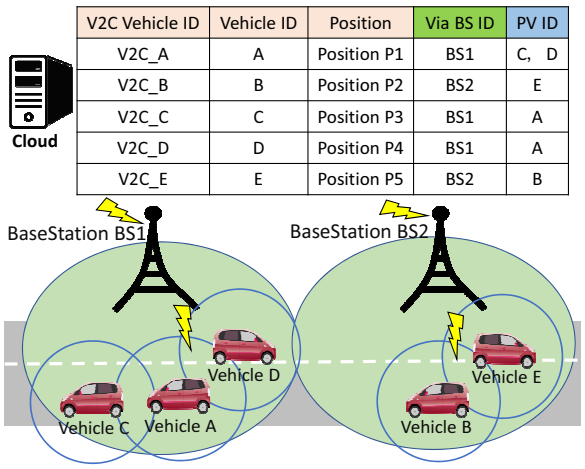

Figure 7. Use example of peripheral vehicle information in V2X communication

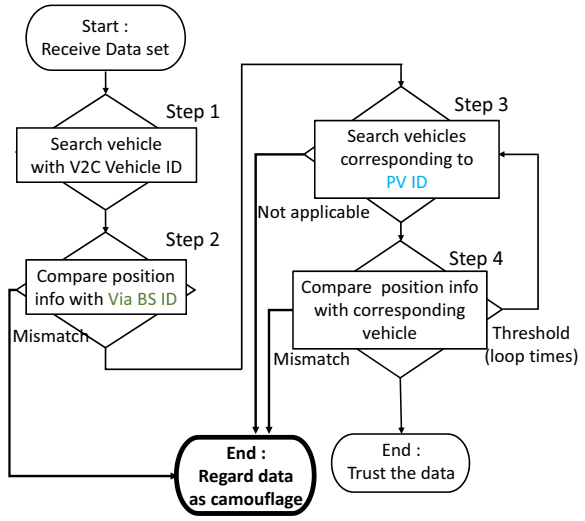

Figure 8. Camouflage data detection procedure to a vehicle send data

exceeds the area covered by the relay base station, we assume that consistency can't be maintained, and that the position information was authorized by camouflage data. A camouflage act in another base department is stopped by this step. In the third or fourth stage, camouflage data are detected based on vehicle information near the transmission vehicle using a PVID. The third step's adjustment-lessness occurs when a vehicle, which doesn't exist around the transmitter, is regarded as a peripheral vehicle. It isn't possible to camouflage another nearby vehicle because a mutual VehicleID exchanged for peripheral vehicles by the V2V communication. The position information of the data, which didn't reach the prescriptive number of times, or peripheral vehicles and the data which couldn't maintain consistency, are identified as camouflage at the fourth stage. We can treat a location's camouflage beyond the possible V2V communication area and make the data more credible by setting up specified execution count. The data, which didn't meet the condition, violates authorization and cant't be trusted in the second, third, or fourth stages.

IV. EVALUATION AND CONSIDERATION

To evaluate the usefulness of our proposed camouflage data detection method, we calculate the evaluation. And then we consider the practicality of our proposal from the evaluation obtained.

TABLE II. SIMULATION PARAMETER

Simulator	Scenargie2.0	
Vehicle number	158 [cars] (five of the send camouflage 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]	

A. Simulator

In this paper, we used Scenargie [6] as a simulator to evaluate the performance of our evaluation of the proposed method. Scenargie is a network simulator developed by Space-Time Engineering (STE). By combining expansion modules, like LTE, V2V communication and, multi-agent simulation can be constructed. In addition, since communication systems and evaluation scenarios are becoming more complicated, this ingenious simulation has greatly reduced the effort required to create scenarios. Examples include GUI scenario creation, map data, the graphical information display of a communication system, and a radio wave propagation analysis function.

B. Evaluation Model

For the evaluation environment, we used a 1 square kilometer square Manhattan model and the 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 across Japan is 158 [cars/km^2]. The 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 our model with a two-ray model using direct waves and reflected waves from the ground. This model closely resembles reality.

C. Evaluation of Camouflage Data Detection

Figure 9 shows the per-threshold detection rate of the camouflaged data from data aggregated in a cloud server. A camouflage data transmitted to a cloud could be detected at 100% by increasing the proposed method's threshold. However, when the threshold was low, completely detecting all of the incorrect data was impossible. The reason is shown in Figs. 10 and 11. The former shows an example where location information can be disguised in a possible range within a range in which peripheral vehicles and the V2V communication range are possible. In this case, since peripheral vehicles guarantee camouflage information from a malicious vehicle, camouflaging the position information becomes possible. Figure 11 show a collusion between malicious vehicles. Since they guarantee mutual position camouflage information, there are trying to fool the cloud into trusting the camouflage data. In other words, this is an inadequate PVID to help with data spoofing. These problems can be addressed by increasing the prescribed number of times (threshold values) shown in Figure 8. By increasing the threshold values, we can create the situation shown in Figure 12 and it is possible to limit deception by malicious vehicles.

 ISBN: 978-1-61208-573-9

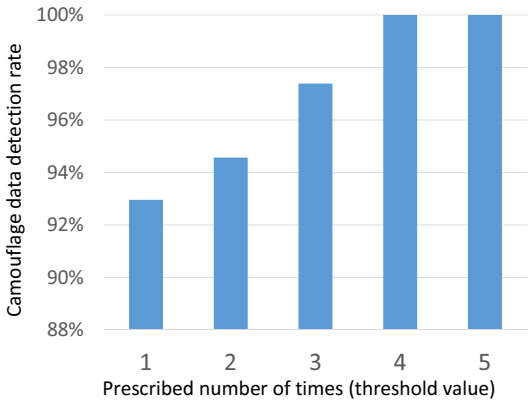

Figure 9. Detect rate of the camouflage data in cloud concentration data

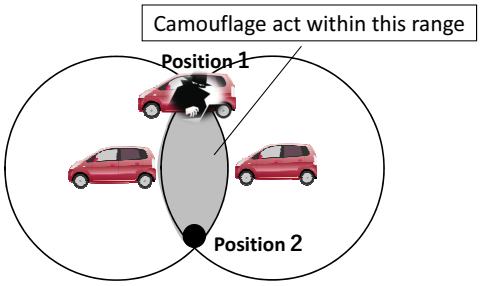

Figure 10. Camouflage acts in V2V communication coverage with peripheral vehicles

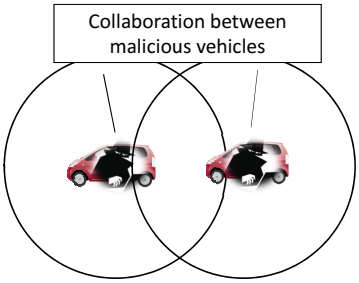

Figure 11. Collusion between malicious vehicles

D. *Evaluation of Misdetection Rate*

Figure 13 shows the false detection rate (false positives) of the proposed method based on the average car density in Japan. The method's threshold is the amount of information data of the peripheral vehicles that is necessary for a cloud to trust the information. In the previous section, we found that an increase in the threshold improves the detection rate of the camouflage data. Here, we consider the false positive detection rate, (false positive), regarding whether a cloud trusts information on vehicles that are not conducting camouflage activities. In the simulation environment shown in Table II, Figure 13 shows that not all 158 cars are doing camouflage acts and the false positives were measured. By increasing the threshold value, the false detection rate improved. Increasing the threshold value in the average Japanese vehicle density erroneously detects normal communication as abnormal.

Therefore, the false positives under the average vehicle density environment in Osaka, which has the highest average car density in Japan, are indicated by Figure 14. In a high vehicle density zone, since much peripheral vehicle information can be acquired by V2V communication, even if the threshold is increased, an increase in the false detection rate can be suppressed. Therefore, we found that the proposed method is more effective in areas with high vehicle density. Actually, the influence of camouflage acts of vehicle information is great in areas with high vehicle density. The proposed method, can guarantee that the information transmitted by vehicle to a cloud is better in areas where more peripheral vehicles exist than in areas with fewer peripheral vehicles. Our proposed method is

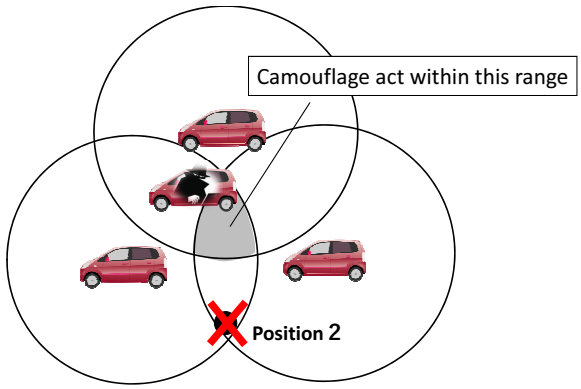

Figure 12. Restriction on camouflage acts accompanying increase in information on peripheral vehicles

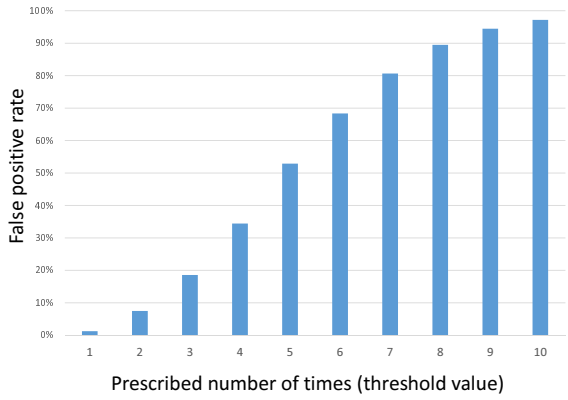

Figure 13. False positives by threshold value under Japanese average vehicle density (158[cars/km^2]) environment

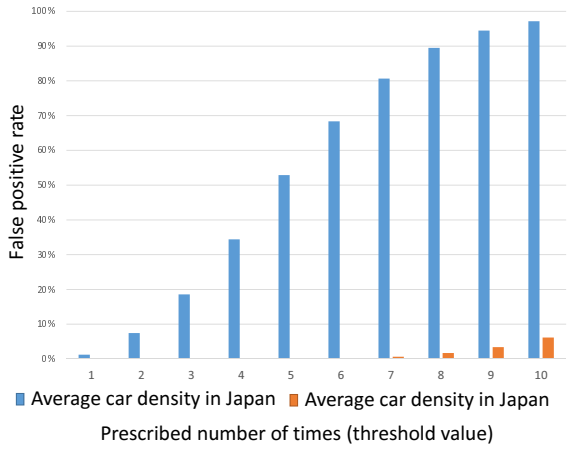

Figure 14. False positive comparison with Osaka average vehicle density (1128 [cars/km^2]) environment

TABLE III. ENVIRONMENT IN THE PROCESSING TIME MEASUREMENT

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

TABLE IV. PROCESSING TIME OF UNJUST MEASURE TO A VEHICLE OF SEND DATA

Threshold	Detected in step2	Detected in Figure 8's step4	Usual end
1	0.1[ms]	0.31[ms]	0.31[ms]
2	0.1	[0.31,0.53]	0.53
3	0.1	[0.31,0.76]	0.76
4	0.1	[0.31,0.96]	0.96
5	0.1	[0.31,1.2]	1.2
6	0.1	[0.31,1.4]	1.4
7	0.1	[0.31,1.6]	1.6
8	0.1	[0.31,1.8]	1.8
9	0.1	[0.31,2.0]	2.0
10	0.1	[0.31,2.2]	2.2

useful in traffic congestion zones where self-vehicle spoofing acts have a huge impact.

E. Measurement of Processing Time

In the evaluation environment shown in Table III, the processing time necessary for the detection of camouflage data is evaluated by Table IV, based on the detection method of camouflage data in Figure 8. The processing time of one vehicle is shown. By using BSIDs, camouflage data can be detected at the beginning of the processing by the proposed method, and 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 camouflage data by PVID is repeated. Even during the repetition, since the processing time changes depending on whether the 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 camouflage 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 the proposed method increases, the processing time required for normal termination increases. 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.

V. CONCLUSION

In the Intelligent Transport Systems (ITS), using a cloud server is inevitable. For providing a safe driving support service using a cloud, camouflaging vehicle information and spoofing a vehicle are threatening. In this research, we used V2X communication, obtained information from various objects, and described measures against vehicle spoofing. We proposed a method that detects camouflage data from the information transmitted by vehicles to a cloud. By using the information of a relay base station in V2C communication and the peripheral vehicle information using V2V communication, measures are taken against camouflaging vehicle information. By increasing the proposed method's threshold, the detection rate of camouflage data was improved and vehicle information was made more reliable. Our proposed method can be adapted to depopulated regions by changing the amount of the data of peripheral vehicle information required as the detection rate improves based on car density. In overcrowded vehicle ares, we confirmed that our proposed method is the most effective.

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] Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM), September 2014. ETSI EN 302 895 V1.1.1 (2014-09).

[2] International Standardization Organization. (2009). Vehicle probe data for wide area communications (ISO 22837:2009).

[3] Schafer, R. P., Thiessenhusen, K. U., Brockfeld, E., and Wagner, P. (2002). A traffic information system by means of real-time floating-car data.

[4] 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, (2017).

[5] Gongjun Yan, Stephan Olariu, and Michele C. Weigle, Providing VANET security through active position detection, Computer Communications, (2008).

[6] " SPACE-TIME Engineering ", URL：https://www.spacetime-eng.com/en/ [accessed：2017-07-07].

 ISBN: 978-1-61208-573-9