Improvement of False Positives in Misbehavior Detection

Shuntaro Azuma, Manabu Tsukada, Kenya Sato

Improvement of False Positives in Misbehavior Detection

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*—By faking vehicle information on cloud servers, an adversary may deliberately cause traffic congestion and/or accidents. Misbehavior means sending masqueraded data to cloud servers in this paper. In our previous research, we proposed "A Method of Detecting Camouflage Data with Mutual Position Monitoring". Cloud servers can detect masqueraded position data from malicious vehicles by increasing the threshold value of our detecting method. However, there are some problems. In this paper, we clarify what kind of malicious behavior is targeted, and we propose two new measures to address the false positives problem. First, we weight for public vehicles such as police cars, and cloud servers can trust vehicles even if they below the threshold value. Second, we dynamically determine the threshold value with consideration of vehicle density. Next, we evaluate the two methods. We find that the method of weighting for each vehicle was very effective, and the method of dynamic determination also showed good results. There is not much difference between our previous method and weighting for each vehicle at low threshold value, but this new one helps considerably suppress false positives at high threshold. The advantage of the dynamic determination model is that false positives do not depend on each base station, because the threshold is dynamically determined. This works more effectively in lower vehicle densities. Our results indicated that these two countermeasures was practical against false positives.**

Keywords–vehicle security; V2X communication; misbehavior detection.

I. INTRODUCTION

In recent years, research on autonomous driving and vehicle-to-vehicle (V2V) communication have been conducted in the Intelligent Transport Systems (ITS) field. In addition, vehicles have vehicle-to-cloud (V2C) communication with cloud servers using mobile lines. When vehicles are connected to various targets, malicious acts have enormous impact. This paper represents further work on our previous publication "A Method of Detecting Camouflage Data with Mutual Position Monitoring" [1]. In our previous research, we proposed how to detect malicious vehicles which sent masqueraded data of their positions. We evaluated the detection rates and received good results. We found that we could detect completely malicious vehicles by increasing the threshold value of our detecting method. However, we have some problems. We especially considered the false positives problem in our previous research. We thought that vehicle densities affect false positives, so we calculated them in high vehicle densities. We cloud find high vehicle densities help suppress false positives, but this countermeasure is effective in only this situation. We should address the false positives problem in low vehicle densities. In this paper, we will reveal our research's target at first. Next, we will describe the operation of proposed method. Then, we will describe improvements of previous research, which are methods of weighting for each vehicle and dynamic determination, and then we will describe the evaluation of these methods.

II. THREAT ANALYSIS OF TRANSMISSION DATA

There exits previous works researching the detection of malicious vehicles in V2X communication [2] [3], as a matter of fact, the definition of a malicious vehicle is ambiguous. In this section, we analyze attacks on vehicle communication and clarify what kind of malicious vehicles are

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.

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**

 ISBN: 978-1-61208-643-9

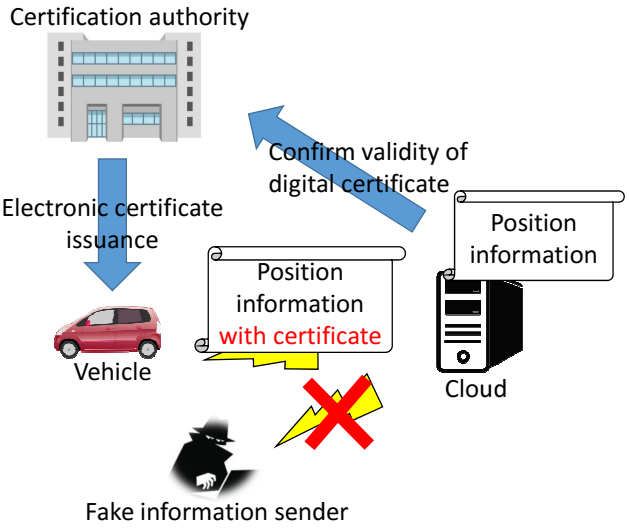


Figure 1. PKI to adapt to vehicles

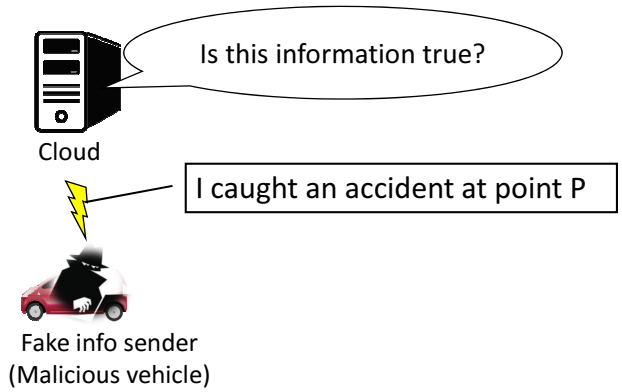


Figure 2. Problem of settling by this research

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 this problem. A cloud may be able to verify the electronic certification and confirm the transmitter's information by the mechanism shown in Figure 1.

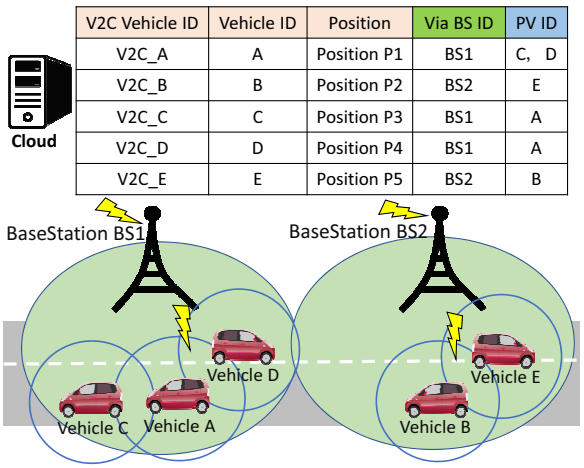
However, this research focuses on data masquerade, as described in Figure 2. Since data encryption and PKI do not confirm whether the received data are masqueraded, data masquerade is inherently different from node reliability which can be resolved by these methods. We will propose a method that can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

III. OUR PREVIOUS RESEARCH

In this section, we will explain our previous research again. We use vehicle-to-everything (V2X) communication and detect masqueraded data of vehicle's position.

A. Pre-suppositions

1) A safe channel has been secured by relationships of mutual trust among all vehicles and cloud servers.



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 3. Use example of peripheral vehicle information in V2X communication

2) Vehicles and cloud servers have been mutually certified beforehand.
3) Relationships between cloud servers and base stations have been built.

B. 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 (Via 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.

C. 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 vehicle-to-cloud (V2C) communication and peripheral vehicles in vehicle-to-vehicle (V2V) communication.

Figure 3 shows the picture of misbehavior detection in our previous research, and Figure 4 shows how to detect masqueraded data in a cloud. A cloud receives not only position information or VehicleID but also peripheral vehicle's and relay base station's information.

 ISBN: 978-1-61208-643-9

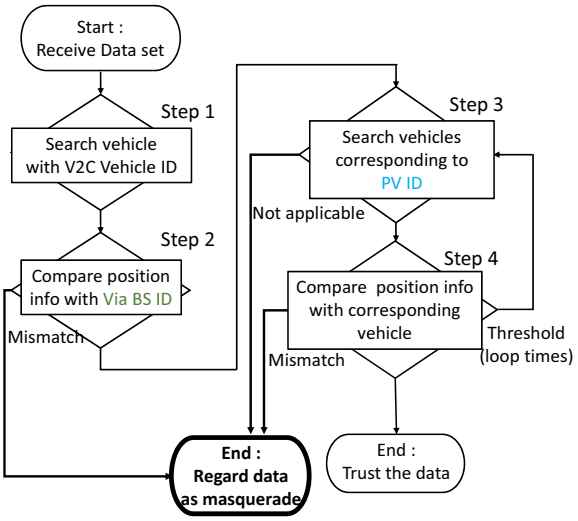


Figure 4. Misbehavior data detection procedure

D. How to Detect Misbehavior data

V2CVehicleID is used in the first step on Figure 4. Cloud servers confirm whether received data is sent from vehicles or not. Second, cloud servers compare Via Base Station ID (ViaBSID) with received position information to confirm whether a sending vehicle exists in relay base station's coverage area. When the received 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 and fourth step, cloud servers detect masqueraded data by using peripheral vehicle IDs (PVIDs). Third, cloud servers search vehicles corresponding to sending vehicle's PVID. Firth, cloud servers compare the received position 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 the 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 this threshold, we can assure more reliable data.

E. Advantage of This Proposal

Figure 5 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. In addition, 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 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.

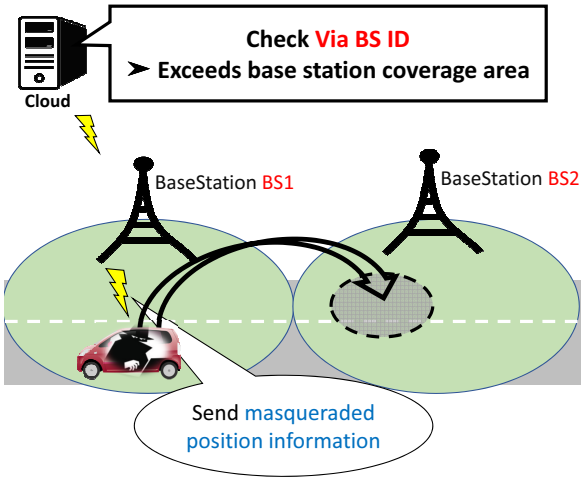


Figure 5. Advantage of using base station information

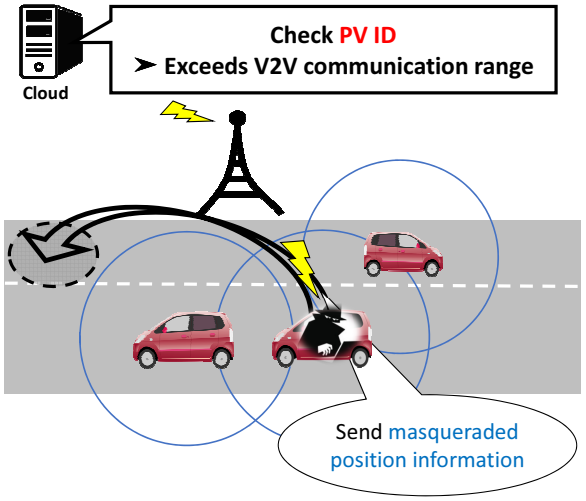


Figure 6. Advantage of using peripheral vehicle information

IV. DEVELOPMENT OF OUR PROPOSED METHOD

We have some problems, especially false positives. Therefore, we propose here two new points to solve them.

1) We weight the public vehicles and trust cloud servers more even for vehicles below the threshold.
2) We dynamically determine the threshold value with consideration of vehicle density.

A. False Positives

We know that increasing the threshold in our method can help detect masqueraded data. However, when we increased

TABLE II. PREVIOUS 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]	

 ISBN: 978-1-61208-643-9

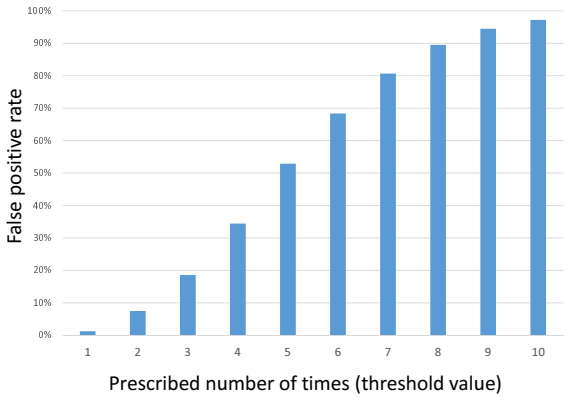


Figure 7. False positives by threshold value under Japanese average vehicle density (158[cars/km^2]) environment

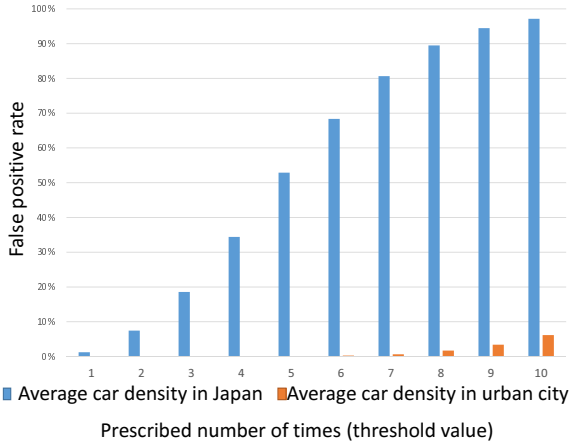


Figure 8. False positives comparison with urban area average vehicle density (1128 [cars/km^2]) environment

threshold values, false positive rates dramatically increased. Therefore, we considered the false positives problem in our previous research. Figure 7 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 simulation environment shown in Table II, Figure 7 shows the false positives when all 158 cars are not misbehaving. By increasing the threshold value, false positive rates increased. By increasing the threshold value under Japanese average vehicle density, cloud servers erroneously detect normal communication as abnormal.

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 8. 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. Tables III and IV show precision, recall, and F-measure in our proposed method. Even looking at these tables, we can make the same statement as 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	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.97	0.94
F-measure	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.97

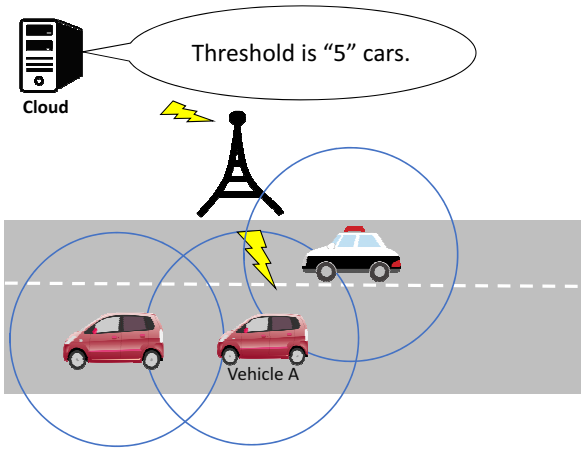


Figure 9. Examples when using a method of weighting for each vehicle

B. *Weighting for Each Vehicle*

This good result (Figure 8) only applies in the urban area. We need to take another measure under the environment of Japanese average car density. In addition, we must consider the lesser number of cars in the streets at nighttime and the lower density environment. Figure 10 shows our new countermeasure to the false positives. We give more 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

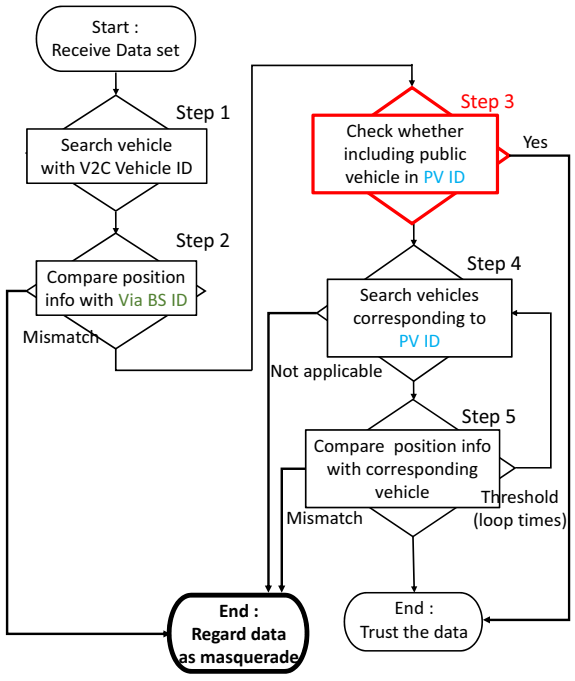


Figure 10. New flowchart of weighting for each vehicle

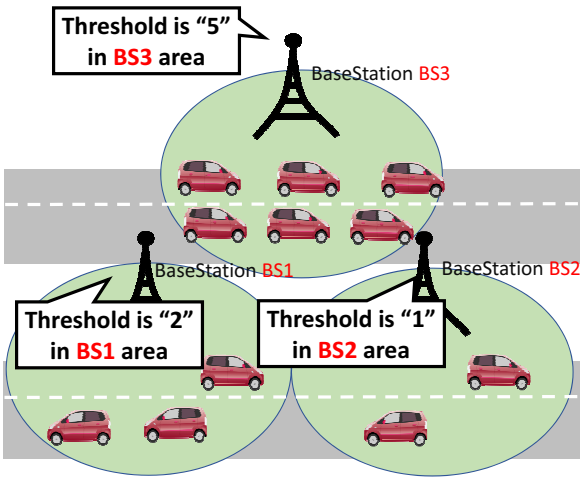


Figure 11. Examples when using dynamically threshold determination

information) does not exceed the threshold value, this one is trusted by a cloud. We consider the environment shown in Figure 9. This case is that 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 positives if public vehicles are running even in low vehicle density areas.

C. Dynamic Determination of Threshold

Based on the results (shown in Figures 7 and 8), we calculate vehicle density for each base station and change the threshold value for each base station. Figure 11 shows the overall picture. We set a prescribed percentage as the threshold value. When vehicle densities in base stations change, the threshold also changes for each base station. We think that this method is effective in solving the false positives problem because we can adjust the threshold dynamically in areas where a vehicle density is low, or during times when there are few vehicles.

V. EVALUATION AND CONSIDERATION

We will calculate false positive rates to evaluate our new points. Next, we will consider the practicality of our new points from the evaluation obtained.

A. Simulator

In this paper, we use Scenargie [4] 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 an evaluation environment, we use one square kilometer Manhattan model and use simulation parameters shown in Table V. 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. 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.

TABLE V. SIMULATION PARAMETER

Simulator	Scenargie2.0	
Vehicle number	158 [cars] (including two police cars.)	
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]	

C. Evaluation of Weighting for Each Vehicle

Figure 12 shows false positive rates when using a method of weighting for each vehicle, and Table VI shows precision, recall, and F-measure. Comparing to Figure 7, we can find that false positives are considerably suppressed at high threshold values. When the threshold is low, we do not find much difference. Therefore, we say that public vehicles have little influence on false positives at low threshold values. However, when a vehicle communicates with a public vehicle in this method, cloud servers can trust this one even if its own PVID has not reached the threshold value. Even if there are no peripheral vehicles around vehicles which send their position data to cloud server, but public vehicles driving around them,

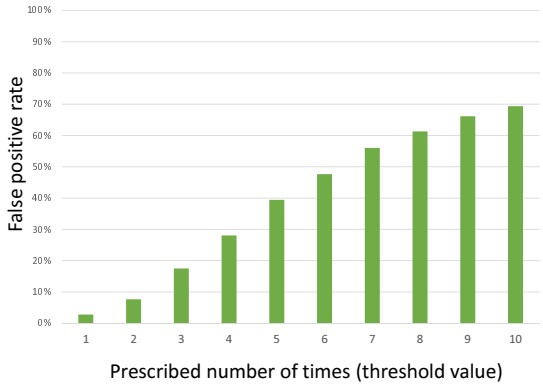


Figure 12. False positives by threshold value when using a method of weighting for each vehicle

TABLE VI. F-MEASURE WITH A METHOD OF WEIGHTING FOR EACH VEHICLE

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	0.97	0.92	0.83	0.72	0.61	0.52	0.44	0.39	0.34	0.31
F-measure	0.99	0.96	0.90	0.84	0.75	0.69	0.61	0.56	0.51	0.47

 ISBN: 978-1-61208-643-9

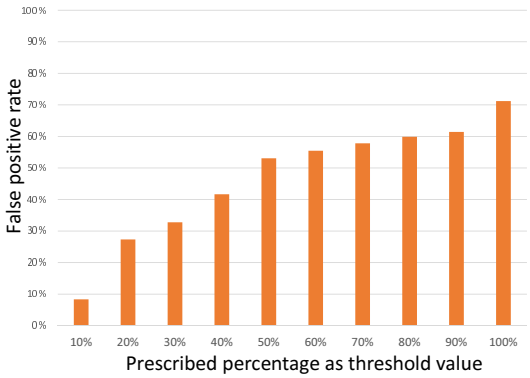


Figure 13. False positives by prescribed percentage when using dynamic threshold determination

TABLE VII. F-MEASURE WITH A METHOD OF DYNAMIC THRESHOLD DETERMINATION

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	0.92	0.73	0.67	0.58	0.47	0.45	0.42	0.40	0.39	0.29
F-measure	0.96	0.84	0.80	0.74	0.64	0.62	0.59	0.57	0.56	0.45

they can be trusted by cloud servers. Our proposed method works more effectively at high threshold. We focused on police cars as public vehicles in this paper, but we guess that we further suppress false positives by weighting buses or taxis running throughout the city.

D. Evaluation of Dynamically Threshold Determination

Cloud servers dynamically determine threshold values at each base station by confirming vehicle densities in base station's coverage area. We calculate false positive rates with this method. Figure 13 shows false positives when using dynamic determination of threshold. This graph's horizontal axis is the ratio of base station's vehicle density as the threshold. It means that cloud servers calculate the number of vehicles traveling in the base station, and we consider the predetermined percentage as the threshold value. Therefore, we do not know the accurate threshold value because there are different vehicle densities for each base station. At low percentage of Figure 13, because the threshold value is lower in each base station, we can suppress false positive rates. For example, when there are 30 vehicles in a base station's coverage area and prescribed percentage is 10%, the threshold value becomes 3. Therefore, cloud servers trust vehicles which have three PVIDs. However, when we set 100% as prescribed percentage in 30 driving vehicles environment, the threshold value becomes 30, so vehicles should communicate with other thirty vehicles for cloud servers trusting them. As the percentage increases, the threshold increases, therefore false positives increase. The advantage of this method is that false positives do not depend on each base station, because the threshold is dynamically determined. If we decide on a single threshold, cloud servers will not respond flexibly.

VI. CONCLUSION

In the Intelligent Transport Systems (ITS), using cloud servers is inevitable. In our previous research, we used V2X communication, obtained information from various objects, and described measures against data masquerade. We cloud completely detect masqueraded data by increasing threshold values. However, we have some problems, which are false positives especially. We proposed two countermeasures against the false positives problem. First, we weight the public vehicles and trust more on cloud servers even for vehicles below the threshold. Second, we dynamically determine the threshold value with consideration of vehicle density. As a result of evaluating these, we succeeded in suppressing false positives. In particular, the method of weighting each vehicle has proven more effective. There is not much difference between previous results and this paper 's results at low threshold values, but at high threshold values, this method help suppress false positive rates. The second measure means that could servers calculate the number of vehicles traveling in the base station, and we consider the predetermined percentage as the threshold value. The advantage of this method is that false positives do not depend on each base station, because the threshold is dynamically determined. In this research, we think that we have improved considerably the false positives problem. In the future, we will propose a method combining both methods or a completely new method, and we would like to conduct a demonstration experiment that also cooperates with Local Dynamic Map (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, ” VEHICULAR 2017, July 2017.

[2] 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.

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

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

 ISBN: 978-1-61208-643-9