A False Information Attack Detection Scheme using Density of Vehicles and Overlap of Communication Range in VANET

Masashi Yoshida, Hiromu Asahina, Shuichiro Haruta, and Iwao Sasase
Dept. of Information and Computer Science, Keio University
3-14-1 Hiyoshi, Kohoku, Yokohama, Kanagawa 223-8522, Japan,
Email: yoshida@sasase.ics.keio.ac.jp

***Abstract*—In Vehicular Ad Hoc Network (VANET), it is important to detect a false information attack, by which attackers try to stage traffic accidents. The state of the art of the false information detection scheme detects the attacker by leveraging that the attacker sends traffic flow differs from both the average traffic flow of the neighbor vehicles in the same area and the theoretical traffic flow calculated from the mathematical relation among the density, speed and the traffic flow. However, this scheme cannot detect an attacker who tries to gradually manipulate the legitimate traffic flows by repeatedly sending a false speed, density or traffic flow that does not differ from the theoretical traffic flow and the average traffic flow. In this paper, we propose a false information attack detection scheme using density of vehicles and the overlap of vehicles' communication range. Since the vehicle density is calculated through the number of neighbor vehicles and diameter of the communication range, the validity of the density can easily be verified through the number of vehicles in the overlap of vehicles' communication range. By using this verified density and the mathematical relation mentioned above, the false traffic flow can be easily detected. Simulation results show that the proposed scheme improves the true positive rate of the false speed by 50% at most and of the false traffic flow by 87.5% at most.**

I. Introduction

Recently, Vehicular Ad Hoc Network (VANET) is getting much attention to provide road safety to vehicles by sharing information with neighboring vehicles or road side units (RSUs) through wireless communication. One of the challenging task in VANET is to detect the false information attacks that an attacker sends the false information, such as the false emergency alert, false speed, false brake, to stage the traffic accident [1]. Especially, the false emergency alert may cause serious damage to road safety. Since the emergency alert is rapidly broadcast over a wide range to notify the occurrence of traffic accident, an attacker can easily manipulate the traffic condition through the false emergency alert. Thus, there are many of false information attack detection schemes focusing on the false emergency alert, such as the long term trust-based scheme [2], the position-based misbehavior detecting scheme [3] as well as the relation of position and time based misbehavior detecting scheme [4]. These schemes mainly focus on the detection of the false emergency alert that does not match the road condition collected through RSUs. Although the detection accuracy of these schemes increases as the number of RSUs increases, deploying many of RSUs causes high construction cost. This motivates the need for the false emergency alert detection schemes without RSUs.

There are some false information detection schemes without RSUs [5] [6]. However, since a vehicle cannot know the road condition outside of the communication range without RSUs, these schemes cannot detect the false information sent from the outside of the communication range of a vehicle. In order to overcome this, Zaidi et al. propose to make the emergency alert unnecessary by leveraging the decrease in the traffic flow around a vehicle as the sign of the occurrence of a traffic accident instead of sending emergency alerts [7]. Since the traffic flow can be calculated from the speed and density received from the vehicles in the communication range, it is not necessary to verify the information sent from the outside of the communication range. We pay attention to [7] because only this scheme overcomes the limitation that a vehicle cannot verify the occurrence of traffic accident outside of communication range without RSUs. In addition, false traffic flow can be easily detected based on the following two characteristics of the traffic flow (i) the traffic flow matches mathematical relation among a speed, density and traffic flow described in [8], (ii) the traffic flows observed by multiple cars in the same area tend to be similar. Thus, a legitimate vehicle can easily find an attacker by detecting a traffic flow that does not match the mathematical relation or differs from an average of traffic flows received from neighbor vehicles. However, this scheme cannot detect an attacker who sends a false speed, density or traffic flow that matches the mathematical relation and does not significantly differ from the average traffic flows. Since the traffic flow is calculated from the density, speed and traffic flow that are received from neighbor vehicles, the traffic flow gradually decreases every time the legitimate vehicle accepts the false speed or false density or false traffic flow. As a consequence, the legitimate vehicle detects a traffic accident by mistake. Thus, it is critical to verify the validity of the traffic flow, speed and density through another way other than the mathematical relation and the average of the traffic flows.

In this paper, we propose a false information attack detection scheme using density of vehicles and the overlap of vehicles' communication range. The main idea of our scheme is that since an attacker has to illegally raise its own density so that the falsified speed or traffic flow matches the

mathematical relation, the number of vehicles calculated from the attacker's density might be too much compared with the number of vehicles calculated from the legitimate vehicle's density. Based on this notion, we argue that a vehicle can detect the attacker by calculating the number of vehicles in the communication range of each neighbor vehicle from the received density. In order to realize this, we employ the fact that a vehicle can count the number of vehicles in the range where its own communication range overlapping with neighbors' communication range. Since the number of vehicles in the overlapped range is true, the difference between the number of vehicles calculated from the false density and the number of vehicles in the overlapped range becomes too much compared to the other neighbors. In other words, a vehicle can detect the neighbor vehicle who sends the density that indicates the existence of too many number of vehicles outside of the overlapped communication range as an attacker. Although an attacker can manipulate the density to avoid being detected by the proposed scheme, this manipulation changes a speed or traffic flow to the abnormal value that does not match the mathematical relation.

The contributions of the paper can be summarized as follows

1) We propose a novel false information detection which enables to detect the false density, speed and traffic flow more certainly by leveraging the overlap of communication range and the mathematical relation among a speed, density and traffic flow.
2) The proposed scheme improves the true positive rate of the false speed detection and the false traffic flow detection by 50% or more and 87.5% or more, respectively.

The rest of this paper is constructed as follows: The conventional scheme is described in Section II. The proposed scheme is described in Section III. Simulation results are shown in Section IV. The conclusion of the paper can be found in Section V.

II. Conventional schemes

Zaidi et al. propose a false information detection scheme without RSUs by employing the decrease in the traffic flow as the sign of the occurrence of an accident instead of sending emergency alerts. A characteristic of the traffic flow, which a traffic flow around a vehicle decreases as the vehicle approaches to the scene of the accident, makes it possible to notify an occurrence of an accident without emergency alerts. Therefore, it is not necessary to verify a reliability of a received emergency alert by collecting a traffic condition through RSUs. In addition, the traffic flow has two remarkable characteristics to detect a false information easily that fitting Greenshield's traffic model and the traffic flows observed by multiple cars in the same area tend to be similar [8]. Thus, a false information attack can be easily detected by detecting a traffic flow that differs from the traffic model or differs from an average of multiple sample traffic flows which are received from neighbor vehicles.

A. System model

This scheme assumes the situation where many of vehicles moves on the highway and thus there are no intersections or no traffic lights. There is no RSU, or the distance between RSUs is too long. All vehicles are equipped with wireless access devices which enable vehicles to exchange the message which consists of speed, density, sample traffic flow and position along with the periodically exchanged beacon message. The radius of the communication range is much longer than the width of road and the vehicles are densely connected with each other. Vehicles can identify each vehicle with a unique ID.

B. Algorithm

The algorithm of the conventional scheme consists of the calculation of a traffic flow around a vehicle and the detection of an arbitrary manipulated traffic flow. In order to calculate a traffic flow of an area where a vehicle exits, each vehicle periodically exchanges a sample traffic flow with neighbor vehicles. The sample traffic flow of vehicle j $Flow_j$ is given as

$$Flow_j = \frac{1}{n} \sum_{i \in N(j)} Speed_i \times Density_j, \tag{1}$$

where $N(j)$, $Speed_i$ and $Density_j$ denote the neighbor vehicles of vehicle j, a speed of vehicle i and density of vehicles around vehicle j, respectively. In order to detect the false density, speed and sample traffic flow, this scheme utilizes the Greenshield's traffic model, which is a mathematical relationship between a density and speed and between a density and traffic flow. Figure 1 shows the Greenshield's traffic model. Assuming that there is no attacker at the beginning of the algorithm. V_f and K_j in Fig.1 are determined based on the traffic condition at that time. These values are determined through the least square method by gathering a speed and density from neighbor vehicles. In order to detect an arbitrary manipulation of a sample traffic flow, a vehicle periodically exchanges the speed and density with the neighbor vehicles along with a sample traffic flow. In addition, a vehicle periodically calculates the average of received sample traffic flows as a baseline for detecting an arbitrary manipulated sample traffic flow. If a received density or speed or sample traffic flow satisfies following three conditions, the received traffic flow is regarded as being manipulated.

1) The density, speed and traffic flow are different from Greenshield's traffic model over a threshold.
2) The traffic flow is lower than the baseline of traffic flows and the difference between them is over a threshold.
3) There is a significant difference in the result of t-test between the received sample traffic flows and the baseline of traffic flows.

If the arbitrary manipulation is detected, the sender of the traffic flow is reported to neighbor vehicles as a malicious vehicle.

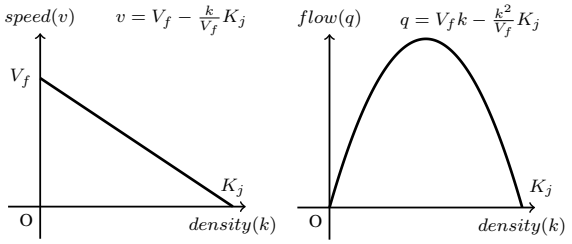


Fig. 1. Greenshield's traffic model

C. Shortcomings of the conventional scheme

Since the threshold and traffic model are shared over a network, an attacker can make the legitimate vehicles to falsely detect the occurrence of an accident by manipulating the traffic flow of the legitimate vehicles through the following two ways, (i) sending an arbitrarily decreased sample traffic flow, which is not over the threshold, over a plurality of times, (ii) sending an arbitrarily decreased speed which fits the traffic model.

1) sending an arbitrarily decreased traffic flow: An attacker can manipulate a traffic flow of a legitimate vehicle by repeatedly sending an multiple arbitrarily decreased sample traffic flows which are not over the threshold. Since a traffic flow of a vehicle is an average of the sample traffic flow received from neighbor vehicles, the traffic flow of a vehicle gradually decreases every time the vehicle accepts the arbitrarily decreased flow. As a consequence, a traffic of the vehicle falls below the boundary value of the accident.

2) sending an arbitrarily decreased speed: An attacker can manipulate a traffic flow of a legitimate vehicle by sending multiple arbitrarily decreased speeds which fit to the traffic model. Since a sample traffic flow which a vehicle sends is a product of its own density and an average of speeds received from neighbor vehicles, a sample traffic flow which a vehicle sends gradually decreases every time the vehicle accepts the arbitrarily decreased speeds. As a consequence, traffic flows of the vehicles which receives the sample traffic flows gradually decreases. In other words, the baseline to detect an arbitrarily decreased traffic flow decreases, and thus an attacker can more easily send arbitrarily decreased traffic flows.

In order to overcome the above two shortcomings, it is critical to guarantee the reliability of the received information, i.e., the sample traffic flow, speed and density, through another aspect in addition to the Greenshield's traffic model and the similarity of the traffic flow.

III. Proposed Scheme

Here, we propose a false information attack detection scheme using density of vehicles and the overlap of vehicles' communication range. The main idea of our scheme is that since an attacker has to illegally raise its own density so that the falsified speed or sample traffic flow fits the Greenshield's traffic model, the number of vehicles calculated from the attacker's density might be too much compared with the number of vehicles calculated from the legitimate vehicle's density. Based on this notion, we argue that a vehicle can detect the attacker by calculating the number of vehicles in the communication range of each neighbor vehicle from the received density. In order to realize this, we employ the fact that a vehicle can count the number of vehicles in the range where its own communication range overlapping with neighbors' communication range. Since the number of vehicles in the overlapped range between a vehicle and attacker is true, the number of vehicles in the outside of the overlapped range, which is calculated from the false density and the number of vehicles in the overlapped range, becomes too much compared to the other neighbor vehicles. Therefore, a vehicle detects the neighbor vehicle who sends the density that indicates the existence of too many number of vehicles outside of the overlapped communication range as an attacker. Although an attacker can manipulate the density to avoid being detected by the proposed scheme, this manipulation changes a speed or traffic flow to the abnormal value that does not match mathematical relation.

A. Attacker model

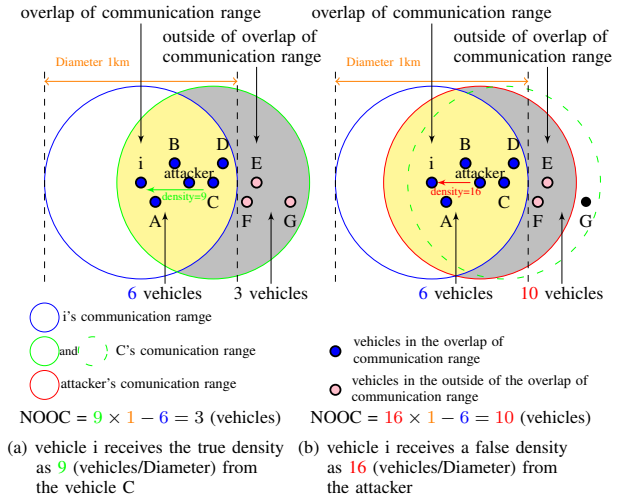
We assume that attackers know the threshold of traffic flow and the Greenshield's traffic model as well as legitimate vehicles know. Attackers try to stage a traffic accident by sending false information such as a low speed or low traffic flow with raised density so that these values fit the traffic model.

B. Overview

We assume our system model is the same as the conventional scheme. For ease of understanding, we use a toy example of the proposed scheme shown in Fig. 2. Specifically, Fig. 2(a) shows the situation where C sends a true density, and Fig. 2(b) shows the situation where an attacker sends a false density. In order to verify the reliability of the received density from a sender, i estimates the Number of vehicles in the Outside of the Overlap of Communication range between i and a sender (NOOC), and NOOC is given as

$$NOOC = Density \times Radius - NOC. \tag{2}$$

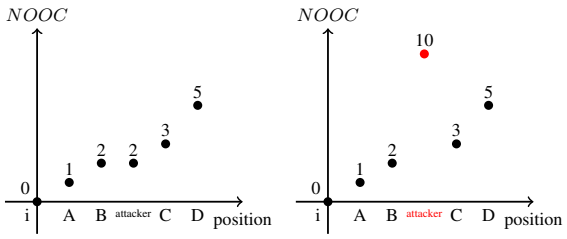
NOC denotes the Number of vehicles in the Overlap of the Communication ranges of i and a sender. In Fig.2(a), NOOC equals to the number of vehicles in the grey range. On the other hand, in Fig.2(b), NOOC does not equal to the number of vehicles in the grey range. Thus, i can determine that the density received from the attacker is false. Specifically, i uses the fact that, NOOC between i and attacker should be less than or equal to NOOC between i and C since the outside of the overlapped communication range between i and attacker is included in the outside of the overlapped communication range between i and C. Since the size of the outside of overlap of communication range linearly increases as the distance between vehicles increases, there should be a linear relation between NOOC and the distance between vehicles. Fig.3 shows the distance between vehicle i and vehicle i's neighbor vehicles versus NOOC of the neighbor vehicles. Fig.3(a) and Fig.3(b) show the situations where the attacker sends a true density and the attacker sends a false density, respectively As shown in Fig.3(a), NOOC of the attacker should be the value



(a) vehicle i receives the true density as 9 (vehicles/Diameter) from the vehicle C

(b) vehicle i receives a false density as 16 (vehicles/Diameter) from the attacker

Fig. 2. an overview of the proposed scheme.



(a) the attacker would send true density

(b) the attacker sends false density

Fig. 3. the relation between the position of the neighbor vehicle and the neighbor vehicles' NOOC

in between the neighbor vehicle B's NOOC i.e., 2 and the neighbor vehicle C's NOOC i.e., 3. Despite that, calculated attacker's NOOC is 10 as shown in Fig3(b) and is not the values between the B's NOOC i.e., 2 and the C's NOOC i.e., 3. Thus, the receiver i can easily detect the false density.

C. Algorithm

The proposed algorithm consists of three steps which are the verification of density, the verification of speed and the verification of traffic flow. The proposed verifications replace the verifications of the conventional scheme. Figure 4 shows the flowchart of the proposed scheme. Information which passes all the verifications is accepted and will be used in the next verification. On the other hand, if the received message is judged as unacceptable, the received message is rejected and the sender is reported as malicious. However, only if the received density does not satisfy the magnitude correlation but the difference is within the threshold, the density is rejected but judging if the sender is malicious or not is deferred. This is because a vehicle may move before the verification of the density is done and the legitimate density may include an error.

1) verification of Density: Upon receiving a density, a vehicle verifies the density by checking if the linear relation is satisfied or not. The algorithm of the verification of density is shown in Algorithm 1. The algorithm consists of four steps. Assuming that the vehicle i receives the density. Firstly,

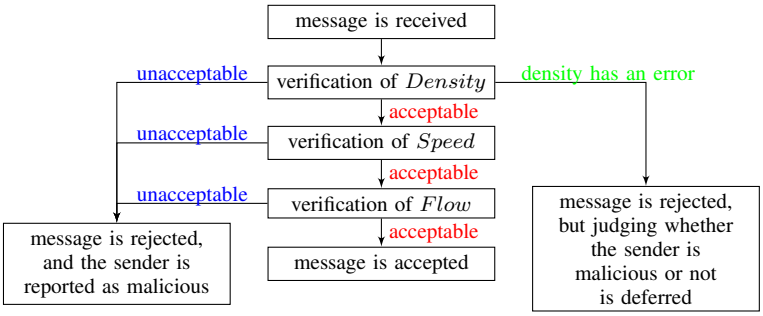


Fig. 4. Flowchart of the proposed scheme

TABLE I
NOTATION TABLE

Notation	Meaning
$OC_{(j,i)}$	Overlap of Communication ranges between j and i
$NOOC_{(j,i)}$	the Number of vehicles in the Outside of $OC_{(j,i)}$
$NOC_{(j,i)}$	the Number of vehicles in $OC_{(j,i)}$
$Diameter$	a diameter of communication range
TS	Theoretical Speed
$DOOC_{(j,i)}$	Density in the Outside of $OC_{(j,i)}$
$ASOOC_{(j,i)}$	an Average of Speeds in the Outside of $OC_{(j,i)}$
$SSOC_{(j,i)}$	Sum of Speeds in $OC_{(j,i)}$
$TSOOC_{(j,i)}$	Theoretical Speed in the Outside of $OC_{(j,i)}$
$TH_{density}$	Threshold for a verification of density
TH_{speed}	A Threshold for a verification of speed
$THOOC_{speed}$	Threshold for a verification of speed in the Outside of the Overlap of Communication range

i creates the list of neighbor vehicle's ID sorted by the distance from i. Secondly, NOC between the receiver i and neighbor vehicles is counted. Thirdly, NOOC between i and neighbor vehicles is calculated. Here, NOOC between the receiver i and j-th neighbor vehicle in the sorted list is denoted as $NOOC_{(j,i)}$. Fourthly, it is checked whether $NOOC_{(j,i)}$ satisfies the following inequality

$$NOOC_{(j-1,i)} \leqq NOOC_{(j,i)} \leqq NOOC_{(j+1,i)}. \quad (3)$$

The $NOOC_{(j,i)}$ satisfying (3) is judged as acceptable. If $NOOC(j,i)$ does not satisfy (3), there are two possible cases whether the difference between $NOOC(j,i)$ and $NOOC(j-1,i)$ or $NOOC(j+1,i)$ is over the threshold or not. In the former case, i rejects the received density and reports the sender as an attacker.

2) verification of Speed: If the density is acceptable, a received speed is verified. The algorithm of the verification of speed is shown in Algorithm 2. In order to check whether the received speed fits the traffic model or not, the Theoretical Speed (TS) is calculated through the Greenshield's traffic model. If the difference between the TS and a received speed is within a threshold, this received speed is judged as acceptable, otherwise this speed is judged as unacceptable.

3) verification of Flow: If the speed is acceptable, a received sample traffic flow is verified through the verification of an average of speeds and a density in the outside of the overlap of communication range. The algorithm of the verification of traffic flow is shown in Algorithm 3. The algorithm consists of five steps. Firstly, i creates the list of neighbor vehicle's ID sorted by the distance from i. Secondly, Sum of Speeds in the Overlap of Communication range between j and i ($SSOC_{(j,i)}$) is calculated. Thirdly, an Average of Speeds in

Algorithm 1 verification of density

Premize: reciever is a vehicles i, sender is a vehicles j
Output: acceptable or deferred or unacceptable
1: SortedVehicles ← vehicles' ID in order of position;
2: **for** ($k = 0$; $k < SortedVehicles.size()$; k++) **do**
3: $NOC_{(k,i)} = 0$;
4: **for** ($l = 0$; $l < SortedVehicles.size()$; l++) **do**
5: if ($Position_l$ is in $OC_{(k,i)}$) {
6: $NOC_{(k,i)}$ = $NOC_{(k,i)} + 1$;}
7: **end for**
8: $NOOC_{(k,i)} = Density_k \times Diameter - NOC_{(k,i)}$;
9: **end for**
10: if ($NOOC_{(j,i)}$ satisfies (3)) { return accepted; }
11: else if ($NOOC_{(j,i)}$ + $TH_{density}$ or
$NOOC_{(j,i)}$ - $TH_{density}$ satisfies (3)) {
12: return deffered; }
13: else { return unaccepted; }

Algorithm 2 verification of speed

Premize: reciever is a vehicles i, sender is a vehicles j
Output: acceptable or unacceptable
1: $TS = V_f - \frac{Dentisy_j}{V_f} K_j$;
2: if ($\mid TS - Speed_j \mid \leqq TH_{speed}$) { return accepted; }
3: else { return unaccepted; }

the Outside of the Overlap of Communication range between j and i ($ASOOC_{(j,i)}$) is calculated. Fourthly, a Density in the Outside of the Overlap of Communication range between j and i ($DOOC_{(j,i)}$) is calculated. Fifthly, if theoretical speed based on the traffic model and average speed have difference or not is checked. In order to check this, the $DOOC_{(j,i)}$ is converted to the Theoretical Speed in the Outside of the Overlap of Communication range between j and i ($TSOOC_{(j,i)}$) through the Greenshield's traffic model. If the difference between the $TSOOC_{(j,i)}$ and $ASOOC_{(j,i)}$ is within a threshold, the received sample traffic flow is judged as acceptable, otherwise the received sample traffic flow which is used to calculate $ASOOC_{(j,i)}$ is judged as unacceptable.

IV. Evaluation

A. Simulation Setup

In order to compare the performance of the proposed scheme with the conventional scheme, a computer simulation was done using Ns3 with Simulation of urban mobility (SUMO) [9]. Ns3 is a modular C++ library and framework that is used for network simulations. SUMO is a software tool that is used to generate vehicular traffic by specifying speed, types, behavior, and number of vehicles. The simulation parameters are shown in TABLE II. The ratio of the attackers is 20% to the total number of vehicles. The behavior of attackers and legitimate vehicles are as follows. The attackers decrease the values of a speed, density and sample traffic flow and manipulate the other two values to match the traffic model. On the other hand, the legitimate vehicles send their actual speed, density and sample traffic flow. In order to show the effectiveness of our scheme, we evaluate the detection accuracy calculated as:

$$TPR = \frac{TP}{TP + FN} \qquad FPR = \frac{FP}{FP + TN},$$

Algorithm 3 verification of traffic flow

Premize: reciever is a vehicles i, sender is a vehicles j
Output: acceptable or unacceptable
1: SortedVehicles ← vehicles' ID in order of position;
2: $SSOC_{(j,i)} = 0$;
3: **for** ($l = 0$; $l < SortedVehicles.size()$; $l++$) **do**
4: if ($Position_l$ is in a $OC_{(k,i)}$) {
5: $SSOC_{(j,i)} = SSOC_{(j,i)} + Speed_l$;}
6: **end for**
7: $NOOC_{(j,i)}$ is calculaed in the same way as the Algorithm 1;
8: $ASOOC_{(j,i)} = \frac{Flow_j \times Diameter - SSOC_{(j,i)}}{NOOC_{(j,i)}}$;
9: $DOOC_{(j,i)} = \frac{NOOC_{(j,i)}}{\mid Position_j - Position_i \mid}$;
10: $TSOOC_{(j,i)} = V_f - \frac{DOOC_{(j,i)}}{V_f} K_j$;
11: if ($\mid TSOOC_{(j,i)} - ASOOC_{(j,i)} \mid \leqq THOOC_{speed}$) {
12: return accepted; }
13: else { return unaccepted; }

where TPR, FPR, TP, TN, FP, and FN denote True Positive Rate, False Positive Rate, the number of True Positive, True Negative, False Positive, and False Negative, respectively.

B. Detection accuracy

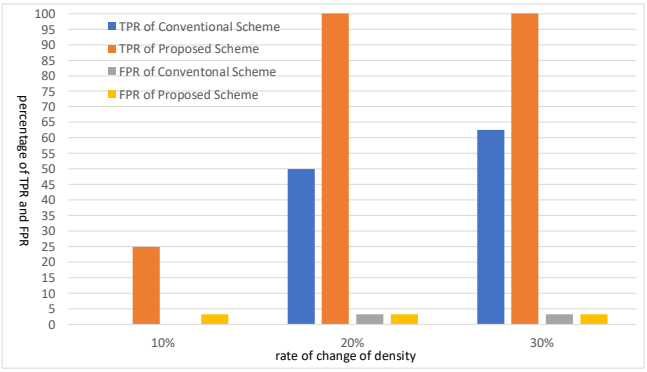
Figure 5(a) shows the rate of change of density by an attacker versus TPR and FPR. As shown in Fig.5(a), TPR increases as the change rate of density increases in both conventional and proposed scheme, and TPR of the proposed scheme is higher than of the conventional scheme. Especially, when the attackers decrease the value of density by 10%, the TPR of the conventional scheme is 0% while the TPR of the proposed scheme is 25%. This is because the proposed scheme verifies the received density not only by utilizing the Greenshield's traffic modelbut also by checking whether the received density is too much or not compared with the legitimate vehicle's density through the inequality of NOOC.

Figure 5(b) shows the rate of change of speed by an attacker versus TPR and FPR. As shown in Fig.5(b), TPR increases as the change rate of speed increases in both conventional and proposed scheme. It is also observed that TPR of the proposed scheme is higher than of the conventional scheme. This is because the proposed scheme utilizes not only the Greenshield's traffic modelto guarantee the reliability of received speed and density but also the theoretical value of speed, which is compared with the received speed, by using the verified density. In addition, when the attackers decrease the value of a speed by 3%, the FPR of the conventional scheme is 6.25% and the FPR of the proposed scheme is 3.15%. This is because the conventional scheme mistakenly judges a false speed as correct, and thus some legitimate vehicles judged as malicious due to the decreased sample traffic flow calculated from the false speed.

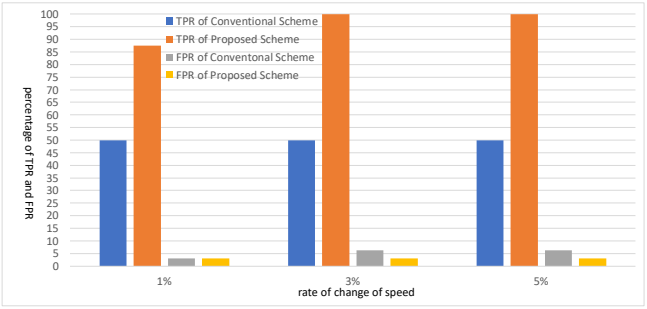
Figure 5(c) shows the rate of change of traffic flow by an attacker versus FPR and FPR. As shown in Fig.5(c), TPR increases as the change rate of traffic flow increases in both conventional and proposed scheme, and TPR of the proposed scheme is higher than of the conventional scheme. This is because the proposed scheme relies the reliability of the sample traffic flow on not the similarity of neighbor vehicles' traffic flows but the theoretical values calculated from the verified density. In addition, when the attackers decrease the value of a sample traffic flow by 30%, the TPR of the

TABLE II
SIMULATION PAPAMETER

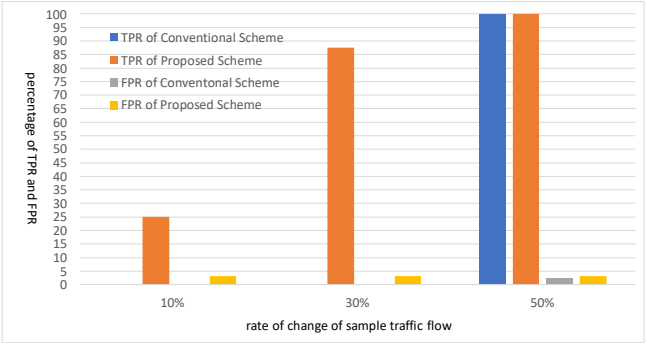
PARAMETER	VALUE
Simulation Time	300sec
Scenario	3 Lane Highway
Max Vehicle Speeds	100km/h
Transmission Rate	Every 0.1s
Wireless Protocol	802.11p
Transmission Range	500m
Ratio of attackers to the number of vehicles	20%
A threshold for a verification of density	6
A threshold for a verification of speed	8km/h
A threshold for a verification of speed in the outside of overlap of communication range	15km/h



(a) the rate of change of density versus TPR and FPR



(b) the rate of change of speed versus TPR and FPR



(c) the rate of change of sample traffic flow versus TPR and FPR

Fig. 5. percentage of TPR and FPR

conventional scheme is 0% and the TPR of the proposed scheme is 87.5%. This is because the conventional scheme can not detect the false sample traffic flow which is within the threshold. On the other hand, the proposed scheme detects it through the verifications of received density and speed which accompany the false sample traffic flow.

On the whole, the FPR of the proposed scheme is constantly 3.15%. This is because, the number of vehicles in the Overlap of communication range may include an error due to the movement of vehicles. As a result, the theoretical values used in the verification of speed and traffic flow also contain an error which incurs FP. Although a legitimate vehicle is removed from the network due to this FP, it can be ignored if the frequency is low because the traffic flow to notify the traffic accident can be calculated correctly until there are certain number of neighbor vehicles.

V. Conclusion

We have proposed a false information attack detection scheme using density of vehicles and the overlap of vehicles' communication range. The proposed scheme successfully improves the traffic model-based conventional scheme by leveraging the fact that attackers should send illegally raised density to make it fit the traffic model. By back-calculating the number of vehicles in the sender's communication range from the number of vehicles in the overlap of communication range, the illegally raised density can be detected. Simulation results shows that the proposed scheme improves the true positive rate of a false speed and the false traffic flow by 50% at most and the true positive rate of a false traffic flow increases 87.5%, respectively.

Acknowledgment

This work is partly supported by the Grant in Aid for Scientific Research (No.26420369) from Ministry of Education, Sport, Science and Technology, Japan.

References

[1] R. Mishra, A. Singh, and R. Kumar, "VANET security: Issues, challenges and solutions," *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 1050–1055, 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7754846/

[2] T. Biswas, A. Sanzgiri, and S. Upadhyaya, "Building long term trust in vehicular networks," *IEEE Vehicular Technology Conference*, vol. 2016-July, pp. 1–5, 2016.

[3] M. Ghosh, A. Varghese, A. Gupta, A. A. Kherani, and S. N. Muthaiah, "Detecting misbehaviors in VANET with integrated root-cause analysis," *Ad Hoc Networks*, vol. 8, no. 7, pp. 778–790, 2010. [Online]. Available: http://dx.doi.org/10.1016/j.adhoc.2010.02.008

[4] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On data-centric misbehavior detection in VANETs," *IEEE Vehicular Technology Conference*, 2011.

[5] R. P. Barnwal and S. K. Ghosh, "Heartbeat message based misbehavior detection scheme for vehicular ad-hoc networks," *Proceedings - 2012 International Conference on Connected Vehicles and Expo, ICCVE 2012*, pp. 29–34, 2012.

[6] F. J. Martinez, C. K. Toh, J. C. Cano, C. T. Calafate, and P. Manzoni, "A Street Broadcast Reduction scheme (SBR) to mitigate the broadcast storm problem in VANETs," *Wireless Personal Communications*, vol. 56, no. 3, pp. 559–572, 2011.

[7] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, "Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6703–6714, 2016.

[8] P. R. D. Kuhne and B. D. Greenshields, "Foundations of Traffic Flow Theory I : Greenshields ' Legacy Highway Traffic," pp. 1–8, 1934.

[9] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO Simulation of Urban Mobility," *Iaria*, no. c, pp. 55–60, 2011.