A false density information attack detection scheme using overlap of communication range in VANET

Masashi Yoshida\(^{a)}\), 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
\(^{a)}\) yoshida@sasase.ics.keio.ac.jp

Abstract: In Vehicular Ad Hoc Network (VANET), it is important to detect false information. The previously published scheme detects the false information by utilizing vehicle density to verify validity of the information. However, this scheme cannot verify validity of the density. We propose a false density information attack detection scheme using overlap of communication range of vehicles. Since a vehicle can calculate the number of vehicles in neighbor’s communication range using a received density, the density can be detected as false if there are too much vehicles outside of the overlapped range. Simulation results show that the proposed scheme improves the true positive rate of false information detection.

Keywords: vehicular ad hoc network (VANET), security, false information, false density

Classification: Fundamental Theories for Communications

References


[5] K. Zaidi, M. B. Milojicic, V. Rakocevic, A. Nallanathan, and M. Rajarajan,
1 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). One of the challenging task in VANET is to detect false information [1]. Although many RSU-based false information detection schemes have been proposed [2, 3], deploying many RSUs causes high construction cost. Thus, we focus on detection schemes without RSUs [4, 5]. The critical issue to realize the detection without RSU is that a vehicle cannot detect false information sent from the outside of its communication range such as a false emergency alert. Zaidi et al. solved this problem by leveraging Traffic Flow (TF) exchanged among neighbor vehicles to notify the traffic accident instead of an emergency alert [5]. Since TF can be calculated from vehicle density and speed of vehicles within the communication range, the false traffic information can be detected without RSU. However, this scheme uses vehicles density observed by neighbor vehicles to detect the false information despite that this scheme cannot verify the validity of density. Thus, an attacker can make the false TF look legitimate.

In order to address this problem, in this paper, we propose a false density information attack detection scheme using overlap of communication range of vehicles. Since an attacker has to illegally change its own density to avoid the detection, the number of vehicles calculated from the attacker’s density might significantly differ from the number of vehicles calculated from density of legitimate vehicles. Based on this notion, we argue that a vehicle can detect the false density by calculating the number of vehicles in a communication range of each neighbor vehicle from a received density and the number of vehicles in the overlap of communication range of vehicles.

2 Conventional schemes

Zaidi et al. propose to replace an emergency alert with an average TF among neighbor vehicles for the ease of false information detection. In order to detect the false TF and false speed without RSUs, this scheme leverages following two characteristics of TF. Firstly, since TFs observed by multiple vehicles in the same area tend to be similar, TF that differs from an average TF among neighbor vehicles is detected. Secondly, since a theoretical value of speed and TF can be expressed as a function of density around a vehicle, speed and TF that differ from the theoretical value are detected.
2.1 Verification of validity of speed and TF

A vehicle periodically sends information of its density (vehicles/km), speed (km/hour), TF (vehicles/hour), position and unique ID to neighbor vehicles in its own communication range. Here, a vehicle calculates its own density by dividing the number of unique IDs of neighbor vehicles in its own communication range by a diameter of the communication range. Upon receiving these values, vehicle \( i \) calculates the theoretical value of TF \( f_{th} \) and speed \( v_{th} \) from the function of the received density \( k \) as follows;

\[
v_{th} = V_{const} - \frac{k}{V_{const}} K_{const}
\]

\[
f_{th} = V_{const} \cdot k - \frac{k^2}{V_{const}} K_{const}
\]

where \( V_{const} \) and \( K_{const} \) denote a constant value related to speed and a constant value related to density, respectively. The values of \( V_{const} \) and \( K_{const} \) are determined through the least squares method by collecting pairs of speed and density of neighbor vehicles. Then, the vehicle gets differences between both the received values and the theoretical values, and the received TF and the average of TF. If these two differences are below thresholds, vehicle \( i \) calculates its own TF with the verified speed and density around itself.

2.2 Shortcoming of the conventional scheme

Since this scheme cannot verify the validity of density, an attacker can avoid the detection by sending false density so that the false speed and false TF match the theoretical values. Although an average TF restricts the falsification, an attacker can degrade the TF of the area enough to stage a false accident by repeatedly sending false TF which does not significantly differ from the average. Therefore, it is critical to devise the scheme to more restrict the falsification than the average of TF among neighbors.

3 Proposed scheme

Here, we propose a false density information attack detection scheme using overlap of communication range of vehicles. The main idea of the proposed scheme is that since attacker has to illegally raise its own density so that theoretical values match the false values, the number of vehicles calculated from attacker’s density is large compared to the legitimate one. In order to compare the number of vehicles, we leverage the fact that a vehicle can count the number of vehicles in the overlapped range of the communication range between itself and neighbor vehicles. Since the number of vehicles in the overlapped range is true, the number of vehicles in the outside of the overlapped range, i.e., the difference between the number of vehicles calculated from neighbor’s density and the number of vehicles in the overlapped range, becomes large if the neighbor vehicle is an attacker.

3.1 Attacker model

We assume that attackers send false TF or false speed to stage a traffic accident. In addition, the attackers try to avoid detection by sending an illegally raised
density to make legitimate vehicles mistakenly judge the false speed and TF as legitimate.

3.2 Verification of validity of density

We replace detection in the conventional scheme that uses an average of TF with the proposed scheme. For ease of understanding, we use examples shown in Fig. 1. Fig. 1(a) shows the situation where vehicle b sends true density and a group of attackers a, j and c send false density, respectively. Let $\bar{I} \cap J$ denote outside of the overlapped communication range between vehicle i and vehicle j. When vehicle i receives density $k_j$ from vehicle j, vehicle i calculates the number of vehicles in $\bar{I} \cap J$ as follows;

$$|\bar{I} \cap J| = k_j \times 2r - |I \cap J|,$$

where $r$ and $|I \cap J|$ denote radius of the communication range and the number of vehicles in the overlapped communication range between vehicle i and vehicle j, respectively. Here, vehicle i can know $|I \cap J|$ by counting neighbor vehicles whose position is inside of communication range of vehicle j. Vehicle i also can calculate $|\bar{I} \cap J|$ in the same way. In order to determine that density of vehicle j is too much, vehicle i uses the fact that when distance between vehicle i and vehicle j, $\bar{I} \cap B$ contains $\bar{I} \cap J$ and thus $|\bar{I} \cap B|$ is larger than $|\bar{I} \cap J|$. Fig. 1(b) shows distance between vehicle i and neighbor vehicles of vehicle i versus the number of vehicles in the outside of the overlap of communication range between vehicle i and neighbor vehicles. As shown in Fig. 1(b), $|\bar{I} \cap J|$, i.e. 8, is not a value in between $|\bar{I} \cap J|$, i.e. 0, and $|\bar{I} \cap B|$, i.e. 3. Therefore, vehicle i can judge vehicle j as an attacker. Specifically, when $|\bar{I} \cap J|$ exceeds $|\bar{I} \cap B|$ beyond a threshold, vehicle i judges vehicle j as an attacker. Here,
vehicle $i$ can detect attacker $a$. Thus, we argue that the proposed scheme can detect attackers whether they form a group or not.

However, the proposed scheme cannot detect attackers at the farthest place in a communication range of a legitimate vehicle (e.g., attacker $c$). In order to deal with such attackers, the proposed scheme shares vehicle ID of detected attackers among all legitimate vehicles. In addition, an attacker can place nonexistent attackers referred to as sybil vehicles at the farthest place in communication ranges of all legitimate vehicles. Although the proposed scheme cannot deal with this situation, these sybil vehicles can be detected by checking Received Signal Strength Indication [6].

### 4 Evaluation

#### 4.1 Simulation setup

A computer simulation has done using NS3\(^1\) with SUMO\(^2\) which simulates three lane highway. The evaluation metrics are shown in Table I. Vehicles move at a random speed in the same direction. The thresholds for verification of TF, speed and density are 500 (vehicles/h), 8 (km/h) and 6 (vehicles), respectively.

#### 4.2 Detection accuracy

Fig. 2(a) shows the rate of falsification of TF versus TPR and FPR when attackers is 20\% to the total number of vehicles. As shown in Fig. 2(a), when the attackers decrease the value of TF by 30\%, the proposed scheme improves TPR by 87.5\%. This is because threshold of the proposed scheme can be more strict than that of the conventional scheme. In addition, the FPR of the proposed scheme is 3.15\% regardless of the rate of falsification of TF. This is because the number of vehicles in the overlap of communication range may include an error due to the movement of vehicles. However, we argue that such a low FPR does not affect the road safety. Even though some legitimate vehicles are judged as attackers, they can receive neighbor vehicles’ information. Thus, they can know traffic conditions and calculate their TF around them. Fig. 2(b) shows the rate of attackers versus the accuracy when the rate of falsification of TF is 10\%, 30\% or 50\%. As shown in Fig. 2(b), the proposed scheme keeps high accuracy regardless of the ratio of attackers. This is because the proposed scheme can detect attackers whether they form a group or not. On the other hand, the accuracy of the conventional suddenly decreases, i.e. accuracy of the conventional scheme (30\%) at 25\% attackers and accuracy of the conventional scheme (50\%) at 45\% attackers. This is because the conventional

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Explain</th>
</tr>
</thead>
<tbody>
<tr>
<td>TPR</td>
<td>the number of detected attackers per the number of attackers</td>
</tr>
<tr>
<td>FPR</td>
<td>the number of mistakenly detected legitimate vehicles per the number of legitimate vehicles</td>
</tr>
<tr>
<td>accuracy</td>
<td>the number of correctly classified vehicles per the total number of vehicles</td>
</tr>
</tbody>
</table>

---

\(^1\)https://www.nsnam.org/

\(^2\)http://sumo.sourceforge.net/
scheme allows attackers to send false information. Therefore, legitimate vehicles receive more false information as the rate of attackers increases. As a result, legitimate vehicles are mistakenly detected as attackers.

5 Conclusion

We have proposed a false density information attack detection scheme using overlap of communication range of vehicles. The proposed scheme successfully improves the conventional scheme by detecting an attacker who sends too much density compared to the other neighbor vehicles. Simulation results show that the proposed scheme detects more attackers who send false TF than the conventional scheme.

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.