Vehicular Communications 27 (2021) 100304

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

Detection of anomalous vehicles using physics of traffic

Malith Ranaweera [a,*], A. Seneviratne [b], David Rey [a], Meead Saberi [a], Vinayak V. Dixit [a,*]

[a] School of Civil and Environmental Engineering, University of New South Wales, Sydney, NSW 2052, Australia
[b] School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia

ARTICLE INFO

Article history:
Received 9 June 2020
Received in revised form 18 August 2020
Accepted 17 September 2020
Available online 24 September 2020

Keywords:
Anomalous nodes
Traffic flow theory
VANET security

ABSTRACT

The world is embracing the presence of connected autonomous vehicles which are expected to play a major role in the future of intelligent transport systems. Given such connectivity, vehicles in the networks are vulnerable to making incorrect decisions due to anomalous data. No sophisticated attacks are required; just a vehicle reporting anomalous speeds would be enough to disrupt the entire traffic flow. Detection of such anomalies is vital to ensure the security of a vehicular network. We propose the use of traffic flow theory for anomalous data detection in vehicular networks, by evaluating the consistency of microscopic parameters which are derived by traffic flow theory (i.e. speed and space-headway) with macroscopic views of traffic under different traffic conditions. Though a little attention has been given to using traffic flow properties to determine anomalous basic safety message (BSM) data, the fundamental nature of traffic flow properties makes it a robust assessment tool. Usually, traffic flow data are determined through roadside units (RSUs) such as cameras and loop detectors; they are financially impractical to roll out on an entire network. Therefore, the method proposed in this study establishes traffic flow data that are used as "ground truth" through RSUs if available, or by the vehicles' own sensor systems. The numerical results indicate that the proposed method provides extremely reliable and consistent predictions of anomalous BSM data. The more the road segment is congested, the higher the accuracy of the anomalous space-headway detection. The anomalous speed detection performs robustly well across all the traffic conditions. The study also finds that both global and local ground truths provide consistent results.

1. Introduction

The emergence of wireless V2X communication is expected to facilitate ubiquitous communication between vehicles, transport infrastructure and the cloud. The integrity of the data that are sent through these networks is crucial for the success of Intelligent Transport Systems (ITS). The default nature of these vehicular networks currently is content-oriented, which means that their primary objective is to deliver content and rely on traditional methods for guaranteeing the provenance of the data that are transmitted [6]. Modern vehicles, which connect to these vehicular networks, are computational units with significant capabilities, thus create security vulnerabilities that are present in all modern networked systems. Moreover, threat vectors and the possibilities of malfunctioning of these vehicular endpoints are significantly greater [2]. However, due to the nature of vehicular networks, the current cryptographic digital signatures and other authentication mechanisms which provide methods of determining the authenticity of the messages are not adequate to secure vehicular networks and guarantee the provenance of the data that are exchanged [11]. For instance, vehicles following proper encryption with valid signatures could still send invalid or false information [21]. This becomes even more challenging because of the ephemeral nature of the vehicular nodes that connect to these networks as they can connect and leave the network within a very short period of time.

There have been numerous proposals for ensuring the provenance of data in ephemeral sensing networks. They leverage the availability of anchor nodes, which are trustworthy [27] [29]. We argue that these anchor nodes are naturally present in ITS and provide the ground truth. Thus, the macro level information of the local phenomena of physical traffic that is provided by these anchor points can be combined with traffic theory to guarantee the provenance of the data in vehicular networks. For example, if there is an accident on the road at a particular location, it is reflected in the dynamics of the traffic flow, and its spatiotemporal evolution is a fundamental phenomenon as exemplified by the traffic congestion indications of maps such as Google maps [31].

* Corresponding authors.
E-mail addresses: malith.ranaweera@unsw.edu.au (M. Ranaweera), a.seneviratne@unsw.edu.au (A. Seneviratne), d.rey@unsw.edu.au (D. Rey), meead.saberi@unsw.edu.au (M. Saberi), v.dixit@unsw.edu.au (V.V. Dixit).

https://doi.org/10.1016/j.vehcom.2020.100304
2214-2096/

Essentially, observed traffic data that are transmitted by a cohort of vehicles from a specified region at a given time should be consistent with the fundamental properties described by traffic flow theory, namely the fundamental relationship between flow, density and speed. The trusted anchor nodes, that act as external data sources, such as loop detectors and other RSUs measure traffic density, flow and speed at relatively short time intervals. RSUs can be considered to be trusted anchor nodes as they will be installed and maintained by organisations that are responsible for the maintenance of the road networks. The information obtained from these trusted anchor nodes thus can be used together with traffic flow theory to determine the validity of the data that are being provided by each vehicle. The estimates of microscopic data provided by a vehicle once verified can be then combined with data from the trusted anchor nodes from specified small regions to form macro level views of regions, which can be used to further increase the provenance of the data of the vehicular network.

In this work, we demonstrate the viability of combining the information obtained from secure anchor nodes with traffic flow theory, for the detection of anomalous data in a vehicular network. We do recognise that loop-detectors or camera-based systems might not be available throughout the network to provide ground truth. In this case, we also propose a localised method, in which a vehicle uses its own sensor data to identify the local traffic conditions to assess abnormality in vehicular information being transmitted via BSMs. In addition, the evaluation of the BSM data is done in a decentralised manner by the vehicle receiving the data, which also makes it computationally efficient. Therefore, our method is robust as it infers ground-truth data either through RSUs or through the sensor system of the vehicle assessing the abnormality itself.

We derive the average generalised traffic flow quantities from an RSU, namely loop detectors. Then use the traffic flow parameters, namely the mean space-headway and speed calculated, and the fact that they are bounded by the physics of traffic flow under steady-state conditions, to identify vehicles that are generating anomalous data. The simulations of the proposed system show that by using only the data from only one type of RSU: loop detectors, it is possible to detect anomalies reliably, across different traffic states in different traffic scenarios and thus make the following contributions:

- We propose a new method to detect microscopic anomalous data using a ground truth based on macroscopic views of a system and traffic flow theory.
- The method detects anomalies irrespective of the intent of the sources which does not rely on an honest majority, and
- We show that the detection method provides similar results using a localised ground truth when a global ground truth cannot be established.

The rest of the paper has been organised as follows. Section 2 reviews the background in the literature, and the methodology used is described in Section 3. Section 4 elaborates the numerical experiments. Section 5 discusses the results and evaluates the applications of the proposed methodology, while Section 6 concludes the work.

2. Background

In vehicular networks, either defective nodes (due to sensor and communication errors) or malicious nodes can transmit anomalous data. The objective of this work is to implement a mechanism to detect anomalous data independent of the intent of its source. Therefore, we use the term anomalous data broadly.

In VANETs security, the existing literature for anomalous nodes detection can be divided into two major categories, namely node centric and data centric detection [19]. Node centric approaches examine data sources by observing their behaviour, attributes (e.g. packet frequency and message format etc.) and security mechanisms they utilise such as authentication. Data centric approaches evaluate the consistency and plausibility of the content of the message received to determine their validity. The consistency-based methods rely on comparing data obtained from different data sources (e.g. other nodes in the neighbourhood and self-sensors etc.), whereas the plausibility-based methods use models of data (e.g. kinematic models, the relation between time, distance, signal speed and rules of physics etc.) [8].

The early study by Golle et al. [7] looked at detecting and correcting malicious data. They assessed and scored the data being received according to a consistency-based model. The proposed scheme relies mainly on the distinguishability of individual nodes and the connectivity with other vehicular nodes to detect malicious data in a distributed manner. However, they have not evaluated the performance of their methodology.

A method for cooperative detection of malicious nodes was proposed in [14] to detect attackers on the roadside via position verification. This research presumes that longer the time a vehicle is found to be trustworthy, the higher the likelihood of the vehicle is not exhibiting an abnormality in its data. They determined a minimum threshold distance (d_{min}) a vehicle should travel in a plausible manner to be accepted as being reliable. The recommended minimum value for d_{min} was twice the expected communication range of a node. Even though a higher d_{min} provides better reliability, it increases the amount of time needed to assess the trustworthiness of vehicles, and thus large values of d_{min} was discouraged. They then enforce a mechanism (described as transitive trust) for broadcasting the determined trustworthiness of a vehicle to its neighbours to make the trust establishment more efficient. Consequently, a vehicle outside a vehicle's communication range knows the trustworthiness of the vehicle without having to assess it by itself and thus makes the inference faster. However, this method works only when a majority of vehicular nodes are trustworthy and at least there is a vehicle in front and behind of a considered vehicle.

Leinmüller et al. [13] [16] [15], developed a method to enhance VANET security via vehicle position verification using geographic ad-hoc routing information. They used several *sensors* both autonomously and cooperatively to assess the consistency and plausibility of the data received. For *autonomous detection*, they used a set of techniques including maximum density threshold, overhearing, acceptance range threshold, mobility grade threshold and map-based verification. *Maximum density threshold* is based on the idea that its physical dimensions restrict the number of vehicles in a given location. By looking at the packets sent by the same vehicle to the other nodes in the neighbourhood, vehicles determine the possibility of a vehicle faking its position in *over hearing*. *Acceptance range threshold* is based on the rule that nodes can send packets only within a specified communication range, whereas *mobility grade threshold* sets a pre-defined a maximum speed for vehicles and verifies whether a vehicle exceeds it or not. *Map-based verification* filters unrealistic off-street coordinates using maps. They further improved their detection using *cooperative techniques* involving proactive and reactive cross checking with the neighbour vehicles. The vehicles share information about their local neighbourhood to verify the consistency of the information.

Schmidt et al. [23] argued that since vehicles respond to their local conditions, each vehicle should be able to assess their traffic environment independently. Therefore anomalous node detection should be performed in a distributed manner. They use beacon data to classify vehicular nodes as honest, malicious and neutral.

That information is then communicated to the other vehicles. To determine the trustworthiness of a vehicle, they used the minimum threshold distance mechanism from their previous studies [14]. They also used vehicle movement information, sensor readings, acceptable ranges of beacons, and realistic positions (e.g. vehicle coordinates must be on the road). Their approach involved individual modules for each feature, which as a collective provided a reputation index for the vehicles. Using consistency and plausibility-based models [8], this work provides a complete system covering both node centric and data centric detection criteria.

Ruj et al. [22] take advantage of the fact that even though a malicious sender can manipulate timestamps and provide faulty locations to a vehicle, the receiving vehicle requires the relationship between the timestamp of the message, their position and the time of arrival of the message to adhere to the laws of physics. Their assumption is that since a malicious node cannot know the exact position of a targeted vehicle, the parameter manipulations are erroneous, and therefore it is easy to detect. This might not be a valid assumption since vehicles broadcast their positions periodically via CAMs (Cooperate Awareness Messages).

Bißmeyer et al. [3] proposed a method for identifying intrusions into a vehicle network with a focus on denial of service for existing traffic and creating illusionary traffic, through the verification of vehicle movement data. Together with the implausibility detectors implemented in [16] [15] they apply a verification mechanism based on the prediction of vehicle movement adopted from [28] which uses a Kalman filter to track vehicles. They further enhanced the detection by taking GPS positional errors into consideration.

Bißmeyer et al. [2] expanded on their work by performing consistency and plausibility checks via verifying vehicles' identities and positions at the application layers of both the sender and the receiver. They adopt the detection methods used in [15] [3] [28]. The work was evaluated using a test attack scenario with real-world vehicles that misuse emergency electronic brake lights.

Sedjelmaci et al. [24] have proposed an efficient light-weighted intrusion detection mechanism, namely ELDV, to secure vehicular networks. Similar to the watchdog model proposed by Wahab et al. [29], they also rely on guard vehicles to protect the network. First, they determine how many guard vehicles should be utilised within a given region and then use a set of specific rules to detect Blackhole, Sybil and False alarm attacks. Further, they develop a vehicle behaviour evaluation method (VBE) by integrating these modules to determine the trustworthiness of the vehicles. Though the method provides a high detection rate and low false-positive rate, its applicability might be limited to the specific scenarios for the rules were defined.

Similar to [5] Lai et al. [12] proposed another vehicular cluster based approach for secure communication in VANET. The proposed system is a software defined network architecture for 5G VANET. Their architecture consists of two components, namely forming a localised vehicular cluster for group communication and facilitating communication to the formed groups to connect to the internet. The first component ensures the integrity of the content shared among the vehicles, while the second component handles the authentication. Although they claim that their method outperforms the other methods, their work lacks an in depth comparison.

Recently a number of machine learning-based approaches have been proposed to detect anomalies. Singh et al. [25] used SVM (Support Vector Machine) and Logistic Regression to detect BSMs that contain falsified locations. The authors trained and tested their models using the VeReMi dataset [9]. They modelled five different types of position faking behaviours and used different combinations of position, relative position and speed as the feature vector. They claim that the detection performance of the SVM classifier is relatively better and that removing the speed parameter from the features yield better training times. So et al. [26] combined a number of data-centric plausibility metrics such as position and movement plausibility as the feature vectors to two machine-learning models, KNN (K-Nearest Neighbors) and SVM to detect fake positions. They also used the VeReMi dataset to train the models and the same types of position faking behaviours to evaluate their models. They claim significant improvements in the detection precision and further deliver a dataset specifically for ML-based methods. Although these findings are interesting, the experiments themselves are specific and dependent on an accurately labelled dataset, making these methods sensitive to the training data sets.

Liang et al. [18] also proposed another machine-learning method which utilises traffic flow dynamics and data from a vehicle's neighbourhood to detect anomalies reliably. They have implemented a feature extraction algorithm and a classifier based on self-organising maps. The feature extraction algorithm first calculates a vehicle flow value and estimates the sender's position upon receiving of messages, then uses the trained self-organising map to classify the received message. They also rely on the notion that traffic flow is similar for vehicles in the same neighbourhood. Though their method demonstrated improvements in the detection accuracy, their proposed method as all other machine-learning techniques is sensitive to the training data and requires a pre-selected trustworthy training dataset.

Although most of these works use plausibility and consistency techniques to detect malicious nodes, they are often limited by their reliance on an honest majority, as well as bandwidth constraints and hardcoded thresholds. Furthermore, they have all relied on the fundamental laws of motion and communication.

However, there is a rich set of literature which describes the fundamental physical laws of traffic that can add immense value to detect anomalous data which have not been considered in any of these studies.

Our detection method is unique because it is based on a universal theory of traffic flow physics, and it is not attack or scenario specific. Therefore, it has a wide range of applications as far as traffic theory goes. To the best of our knowledge, this has not been done before.

Unlike the other methods described above based on kinematics laws of motion and vehicular physics, we do not rely on a sequence of past data from a vehicle or relationships between parameters in the same message. Instead, we use macroscopic views derived from a single RSU type, loop detector data, to analyse the parameters separately.

The method we propose does not rely on a trustworthy pre-labelled data set and does not require computationally extensive training like other machine learning-based methods that have been proposed. It is not financially or computationally expensive because it does not require sophisticated sensors that monitor a traffic network with a high resolution. Moreover, providing a ground truth to vehicles to detect anomalies at a vehicle level reduces processing overhead at RSUs and avoid the potential single point of failures.

Further, our method is robust to failures and unavailability of external data sources. It detects anomalies using a vehicle's own sensor data, by establishing ground truth locally even when the external sources fail to provide information.

Our method does not rely on any specific model but uses the fundamental relationships and assumptions of traffic flow theory which makes it more generic. We analyse speed and density parameters separately. Therefore, instances reporting accurate flow conditions with faulty speed and space-headway [32] values can be detected.

Further, we show that the detections based on microscopic and macroscopic views of traffic are consistent with each other and

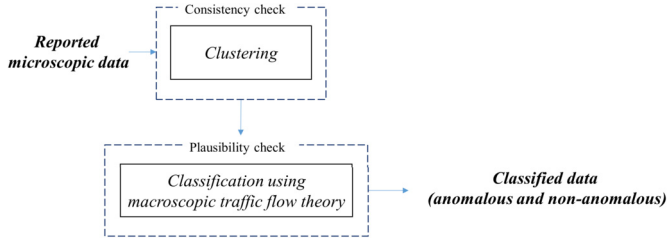


Fig. 1. Schematic illustration of the proposed framework.

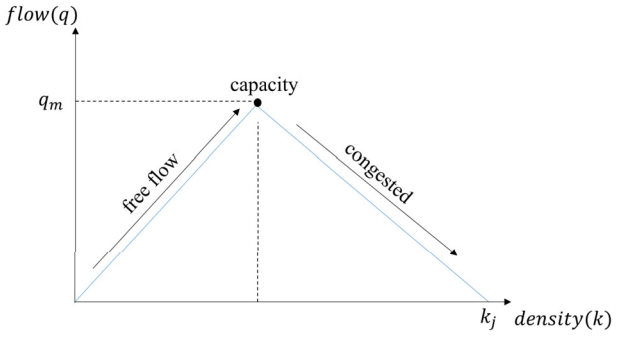


Fig. 2. Flow-density diagram.

microscopic ground truth can be used when a macroscopic ground truth cannot be established.

In our work, we make use of traffic flow theory to develop a method which discerns anomalous data reported by vehicular nodes. The method exploits the consistency of the reported data to cluster them and uses deviations from ground truth to classify the clusters. We do not rely on any prior knowledge of the environment and do not assume an honest majority. The establishment of ground truth and all the classifications are based on the data and fundamental physical laws dictated by traffic flow theory that can be collected in real time.

Fig. 1 summarizes the contribution of this work.

3. Model for detection of anomalous data

VANETs consist of two types of communication channels, namely control channel (CCH) and service channel (SCH) [10]. CCH facilitates the transmission of safety critical information including vehicular speed, position, space-headway, acceleration and timestamps etc., by broadcasting Basic Safety Messages (BSMs) aka. Beacons. SCH broadcasts Decentralised Environmental Notification Messages (DENMs) to share specific event-related information such as accidents, weather conditions etc. In this work, we propose a methodology for identifying vehicles that transmit invalid BSMs using only space-headways and speeds, without loss of generality. The purpose of the study is to evaluate the applicability of traffic flow theory [4] [17] to identify anomalous BSM data. The relationships are further described below.

Traffic flow theory describes the physics of vehicular traffic. It describes the spatio-temporal evolution of traffic flow. Therefore, any information contained in the VANET messages can be substantiated by traffic flow theory as it must comply with this physics. The theory describes vehicular traffic flow using three fundamental parameters, namely speed (v), density (k) and flow (q).

When a vehicle travels on an uncongested lane, it can move at ***free-flow*** speeds. As the number of vehicles on a lane increases, density increases and reaches a state of maximum flow (q_m), known as its ***capacity*** (see Fig. 2). After this point, the lane starts getting ***congested*** and speed drops as density increases. When density reaches its maximum, called the jam density (k_j), flow and speed become zero.

We define ***anomalous data*** as deviations from the actual value. For instance, if a vehicle claims that its speed is 60 kmh^{-1} though its actual speed is 80 kmh^{-1}, it is regarded as anomalous. Therefore, any vehicle claiming a false space-headway or a speed is anomalous as per our definition. We are not concerned with the intent of the vehicle producing anomalous data.

The ***detection criteria*** utilise space-headway *(s)* and speed *(v)* parameters in the BSM message for a given time period. Space-headway is defined as the distance between the front of the following vehicle and the front of its leader. Measures of density and speed collected by RSUs (e.g. Loop detectors) are used to evaluate the validity of this data retrieved from BSMs. When such external traffic flow information sources cannot infer a global ground truth, a vehicle can establish a localised ground truth using its own sensor data about density and speed. In this work, both global ground truth and local ground are considered.

Steady-state conditions are useful assumptions used in traffic flow theory to analyse and understand real-world traffic phenomena. Under steady-state conditions the average space-headway ($\bar{s}$) between vehicles should be equal to the inverse of the density *(k)* [17], and the vehicle speeds should be equal to the speeds observed by the roadside units. We argue that anomalous data can be detected for a given evaluation period using the deviation of the localised space-headways and speeds from the density *(k)* and the average speed ($\bar{v}$) acquired from roadside units or vehicular sensors.

Therefore, we define a ground truth during a given time window as, ***Ground Truth*** $= (\frac{1}{\bar{k}}, \bar{v})$; where, $\frac{1}{k}$: is the space-headway estimated from the density ($\bar{k}$) and $\bar{v}$: is the average speed either estimated from the road side units or collected from the sensors of a vehicle.

The detection methodology can be formulated as follows. Let N be a set of vehicular nodes on a given lane communicating over time window $T = [t_1, t_2]$. n_i is the i^{th} node, where $i \leq k_j.L$. k_j is jam density and L is lane length.

Each vehicle broadcasts its space-headway periodically, with a period of times (t) to its neighbours. Averaging the values during the time window T, each node maintains a history for each of its neighbours which can be represented by a vector $H_i(t)$ as

$$H_i(t) = \begin{bmatrix} \frac{\sum_t^{t+T} s_1(t)}{T} \\ \frac{\sum_t^{t+T} s_2(t)}{T} \\ \vdots \\ \frac{\sum_t^{t+T} s_{i-1}(t)}{T} \\ \frac{\sum_t^{t+T} s_{i+1}(t)}{T} \\ \vdots \\ \frac{\sum_t^{t+T} s_N(t)}{T} \end{bmatrix} \quad (1)$$

$\exists(\bar{k}, \bar{v}) \in P$ where P is the set of traffic states across traffic flow fundamental diagram and $n_r \in N$ *s.t.* either $n_r \in A$ or $n_r \notin A$, where A is the set of anomalous nodes.

Assuming a set of observers collecting traffic flow information and producing generalised traffic flow quantities, for example, density ($\bar{k}$) and speed ($\bar{v}$) for a lane of length L over the time window T are

$$\bar{k} = \frac{\sum_{n_i \in N} t_i}{LT} \quad (2)$$

$$\bar{v} = \frac{\sum_{n_i \in N} d_i}{\sum_{n_i \in N} t_i} \quad (3)$$

Algorithm 1: Anomalous space-headway detection.

Input : N Set of vehicular nodes, $\bar{s}_n \forall n \in N$ Average claimed vehicular headways and $1/\bar{k}$ Ground Truth headway derived from traffic flow theory
Output: Anomalous space-headways

```
KMNS ← kmeans(s̄_n, 2) ;
(c_1, c_2) ← centroids ∈ KMNS;
(L_1, L_2) ← labels ∈ KMNS;
if |c_1 − 1/k̄| < |c_2 − 1/k̄| then
    return CorrespondingHeadways(∀s̄_n, L_1);
else
    return CorrespondingHeadways(∀s̄_n, L_2);
end
/*CorrespondingHeadways returns the relevant average space-headways given the label inputs*/
```

where t is the time a vehicle spends on the lane and where d is the distance it travels on the lane.
Otherwise using localised definitions,

$$\bar{k} = \frac{1}{\bar{s}_i} \tag{4}$$

$$\bar{v} = \bar{v}_i \tag{5}$$

where $\bar{s}_i$ is the average space-headway of the vehicle and where $\bar{v}_i$ is the average speed of the vehicle.

We assume that the whole vehicular group consists of two distinct clusters (i.e. anomalous and non-anomalous). As the non-anomalous cluster is one homogeneous cluster which cannot be clustered further meaningfully, there cannot be multiple honest clusters. Therefore applying univariate kmeans [30] clustering algorithm where $K = 2$ to minimize the sum-of-squares criterion,

$$minimize \sum_{k=1}^{K} \sum_{j \in c_k} ||\bar{s}_j - m_k||^2 \tag{6}$$

where m_k is the centroid of c_k, divides $H_i(t)$ into two clusters with centroids m_1 and m_2 with corresponding sets of vehicular nodes N_1 and N_2. $N = N_1 \cup N_2$ and $N_1 \cap N_2 = \emptyset$.

n_r is predicted to be anomalous (i.e. $n_r \in \tilde{A}$ where $\tilde{A}$ is the set of predicted anomalous nodes) if it belongs to a cluster whose centroid deviates the most from the ground truth value. This is represented as,

$$n_r \in \begin{cases} \tilde{A}, & \text{if}((|m_1 - 1/\bar{k}| > |m_2 - 1/\bar{k}|) \wedge n_r \in N_1) \quad \vee \\ & ((|m_1 - 1/\bar{k}| < |m_2 - 1/\bar{k}|) \wedge n_r \in N_2); \quad \bar{k} \in P \\ \bar{\tilde{A}}, & \text{otherwise} \end{cases} \tag{7}$$

Applying the same methodology, a vehicle disseminating anomalous speeds can be detected as

$$n_r \in \begin{cases} \tilde{A}, & \text{if}((|m_1 - \bar{v}| > |m_2 - \bar{v}|) \wedge n_r \in N_1) \quad \vee \\ & ((|m_1 - \bar{v}| < |m_2 - \bar{v}|) \wedge n_r \in N_2); \quad \bar{v} \in P \\ \bar{\tilde{A}}, & \text{otherwise} \end{cases} \tag{8}$$

As described in Algorithm 1, anomalous space-headways broadcasted by vehicles can be detected.

In simple terms, we cluster the averaged values of space-headways, and recognise the cluster with the centroid closest to the ground truth as non-anomalous to label the corresponding nodes as honest. Note that, to classify data, we use the distance from ground truth to the centroid of each cluster. The ground truth is not determined by what other vehicles report but by the data reported by RSUs and data obtained via a vehicle's own sensors.

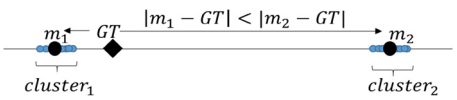


Fig. 3. Distinguishing clusters (m_1 and m_2 are centroids of the clusters and GT is the ground truth).

Table 1
Notation definitions.

Notation	Definition
s	space headway
v	speed
k	density
q	flow
k_j	jam density
T	considered time interval
GT	ground truth

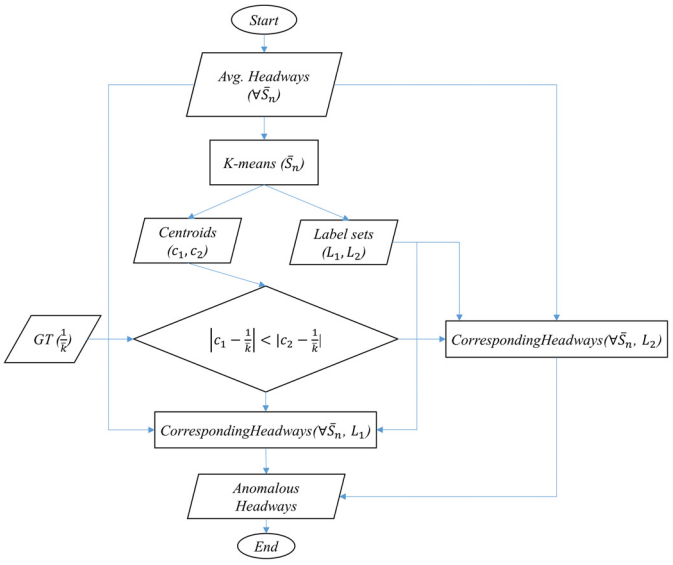


Fig. 4. The detection flow chart.

Therefore, the system does not rely on an honest majority. For example, as in Fig. 3, as the distance between GT and m_1 is less than the distance between GT and m_2, the cluster with centroid m_1 is recognised as non-anomalous. Thus, space-headways are categorised as anomalous and non-anomalous. This detection method is used to identify anomalous speed information as well (see Table 1 for the notations and the definitions).

We assume that information collected by RSUs (e.g. loop detectors) is disseminated to other vehicles and entities in short time intervals. On receiving this information, centralised entities such as Certification Authorities can use it for global verification, whereas vehicular nodes can use it for local verification at an individual vehicle level.

The proposed method analyses systematic deviations between the BSM parameters broadcasted by a vehicle and the ground truth to identify anomalies. The larger the deviation, the higher the likelihood that the source is anomalous. In this way, anomalies can be detected independently.

The entire procedure for the anomalies detection can be summarised as in Fig. 4.

4. Numerical experiments

The design of the experiments and data are elaborated in this section.

(a) Schematic network segment

(b) M4 motorway segment: Vehicular flows originating from the nodes 0 and 1 depart at 3 and 4

Fig. 5. The networks studied: The left hand driving is enforced as per Australian driving rules.

4.1. Experimental design

We describe the simulation networks, the vehicular demand and the traffic states studied here.

4.1.1. Simulation networks

The performance of the proposed method was evaluated by simulating realistic traffic environments using Simulation of Urban Mobility (SUMO) [1]. We test the method using two different simulation networks, namely a schematic two-lane test network with a bottleneck (see Fig. 5a) [20] and a network comprising motorway, the M4 in Sydney (see Fig. 5b), under real-world traffic flow conditions.

4.1.2. Vehicle demand

A demand of 3750 of vehicles was simulated on the schematic test network over 235 minutes. We increased the flow rate over time. Similarly, a total demand of 2000 vehicles over a period of 60 minutes and 5000 vehicles over a period of 200 minutes were simulated to generate the range of traffic states in the Sydney M4 network to analyse free flow and congested conditions. The data we collected was shown to represent realistic operational conditions (see Fig. 6 and Fig. 7). The networks simulated and their output are provided in Appendix.

4.1.3. Studied traffic conditions

The simulations were designed to assess the performance of the proposed method across free-flow and congested conditions. As shown in Fig. 6, the average speed and density of the traffic system change over time. The speed and density values are averaged over 10 second (T=10 s) periods. During some time periods, these traffic flow parameters are fairly constant, indicated as steady state in Fig. 6 representing free flow conditions and congested states. For example, in the schematic two lane network, traffic flow parameters are relatively constant between 20-90T, 110-180T, and 200-270T (see Fig. 6a and 6b) which correspond to the free flow state, whereas 400-470T corresponds to the congested state.

The fundamental relationship between traffic flow and density is shown in Fig. 7. These plots highlight the traffic states at which the model was evaluated. For instance, in Fig. 7a, 20-90T and 110-180T represent free flow states, 200-270T represents a capacity state and 400-470T represents a congested state. The time periods during which the states shown in Fig. 7a were simulated are shown in Fig. 6a.

4.2. Anomalous data

To emulate anomalous data, a percentage of the total number of vehicles in the simulation are categorised as producing erroneous data. These vehicles generate data that deviate from their true value as described below.

In every simulated scenario, the anomalous vehicles may claim a space-headway with an error that is uniformly distributed between [-0.9, 0.9] at increments of 0.1, and a speed (v_c) with in the range of $v_c = v_a \pm r v_a; r \in [0.1, 0.9]$, where v_a is its actual speed.

5. Results

We compare the predicted and actual anomalous vehicles to interpret the results of the anomalous space-headway and speed detection. We calculate precision, recall, f-measure and false positive rates for different scenarios and traffic states under different percentages of anomalous vehicles.

5.1. Evaluation

Evaluation metrics for these experiments are defined as follows. As defined in the section 3, A is the set of anomalous nodes and $\tilde{A}$ is the predicted set of anomalous nodes. Therefore, precision is the proportion of the predicted anomalous nodes that are actually anomalous = $n(\tilde{A} \cap A)/n(\tilde{A})$ and recall is the proportion of the total relevant anomalous nodes correctly predicted = $n(\tilde{A} \cap A)/n(A)$. False positive rate is the proportion of incorrectly predicted anomalous nodes = $n(\tilde{A} \cap \bar{A})/n(\bar{A})$ and f-measure is the harmonic mean of precision and recall.

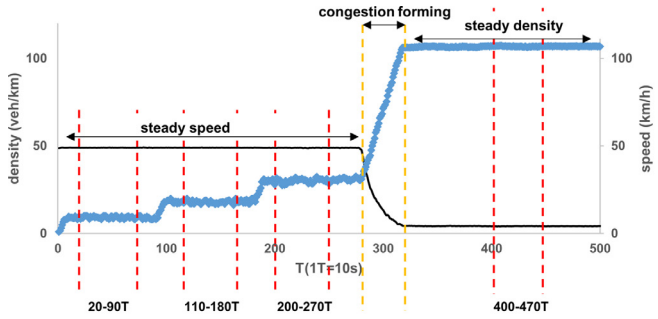
We further perform a sensitivity analysis with 10%, 20% and 40% of the total number of vehicles being anomalous to evaluate the performance of our method.

The results (generated using the global ground truth) for the networks when 40% of the total vehicles are anomalous are shown in Fig. 8 (For the complete set of results see the Appendix). The figure contains the detection results for different traffic conditions (i.e. free-flow, at capacity and congested) per considered BSM parameter (i.e. space-headway and speed). Each plot shows, how precision, recall, f-measure and false positive rate vary over the considered range of anomalous factor (r).

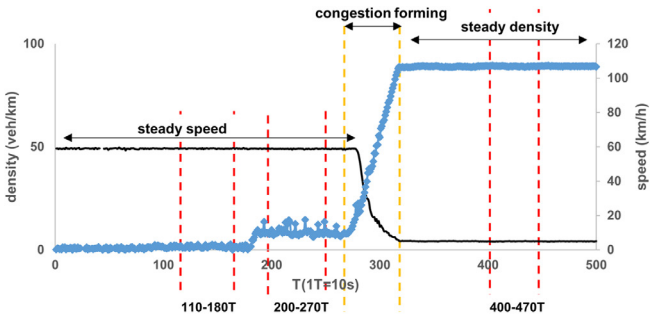
5.2. Schematic network

Lane changes were found to have an adverse impact on the performance of detection of anomalous space-headway data (see Fig. 8a). Because of the left lane merges into the right lane, there is a considerable amount of vehicles moving out of the left lane during free flow and congested conditions. This makes anomalous space-headway detection difficult in the left lane as lane changes cause large variances in the left lane space-headways.

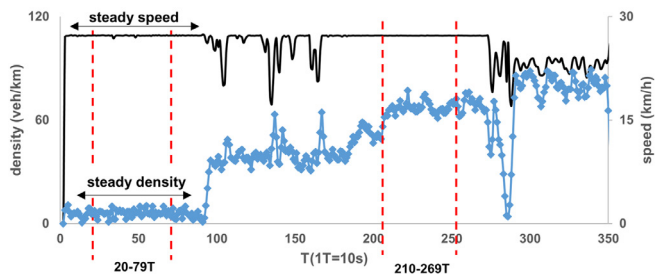
Although lane changes do not pose a problem in the detection on the right lane during free-flow conditions, the efficiency of the space-headway detection deteriorates at capacity due to lane changes. This can be observed in Fig. 8a, where precision, recall



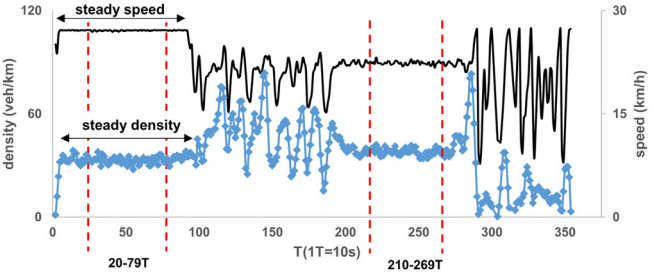
(a) Schematic network right side lane



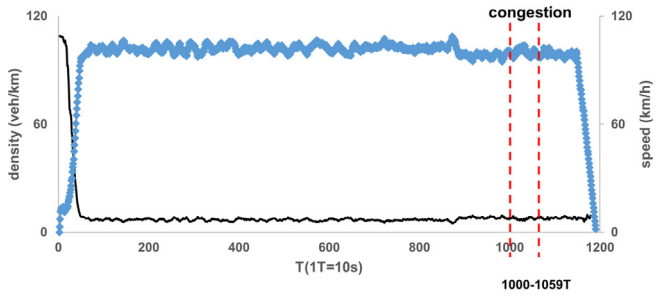
(b) Schematic network left side lane



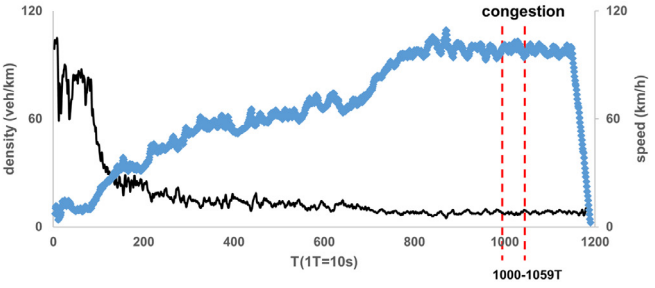
(c) Sydney M4 network right side lane



(d) Sydney M4 network left side lane



(e) Sydney M4 network right side lane (a congested situation)



(f) Sydney M4 network left side lane (a congested situation)

Fig. 6. Density (♦ y-axis left) and speed (— y-axis right) overtime.

and f-measure are relatively low for the space-headway detection during capacity conditions. However, in congested conditions, the performance of detecting anomalous space-headway data on both lanes is good. The impact of lane changes is minimal hence does not pose a problem.

In contrast, for the anomalous speed detection precision, recall, f-score are greater than 0.7, 0.9, 0.8 respectively and false positive ratio is less than 0.04 across all traffic states. The efficiency of anomalous speed detection in congested conditions is slightly degraded due to stop-start events (see Fig. 8a).

5.3. Motorway: Sydney M4 network

Results were similar to those found in the schematic network. The performance of the anomalous space-headway detection has a precision above 0.86, recall above 0.99, f-score above 0.92 and false positive ratio below 0.01 for the anomalies outside the range of [+0.4,-0.4] during congested conditions (see the Appendix). The anomalous speed detection worked reasonably well providing a minimum of 0.89 for precision, 0.89 for recall, 0.94 for f-score and 0.01 for false positive ratio for the anomalies outside the range of [+0.6,-0.6] across traffic states. A similar pattern can be observed in the experiment results done with localised ground truth (see the Appendix).

In the weaving sections (see Fig. 5b) the anomalous space-headway and speed detection deteriorated due to lane changes.

As observed in Fig. 8a and b, the false positive rates are reasonably low across different traffic conditions in both speed and space-headway detections.

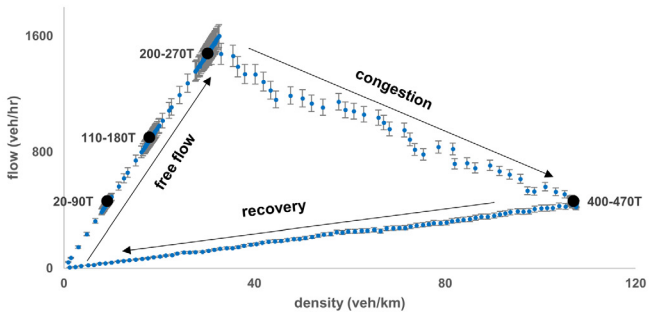
Further, in both networks, the detections get better when the percentage of anomalous nodes increases as it raises cluster densities.

As anticipated, the detection accuracy is improved as the deviation of the anomalous data from the real values increases. The proposed method for anomalous speed detection worked reasonably well under all the different traffic conditions (freeflow, at capacity and congested as shown in the Appendix).

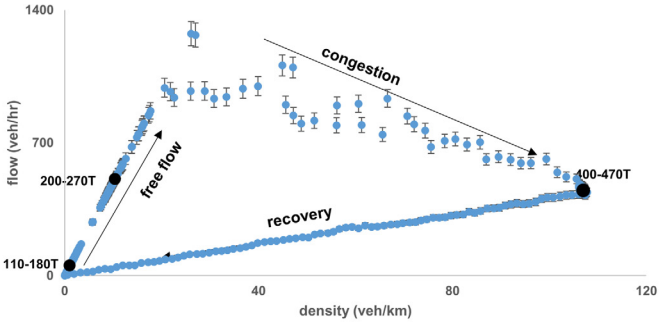
The anomalous space-headways detection performed well only during congested conditions (see the Appendix). Lane-changing was the main reason for the poor performance during free-flow and capacity conditions. In a steady state, when a vehicle changes its lane, its follower on the previous lane experiences an abrupt increase in the space-headway, whereas the new follower's space-headway drops instantly.

Overall, the results can be summarised as in the following Table 2.

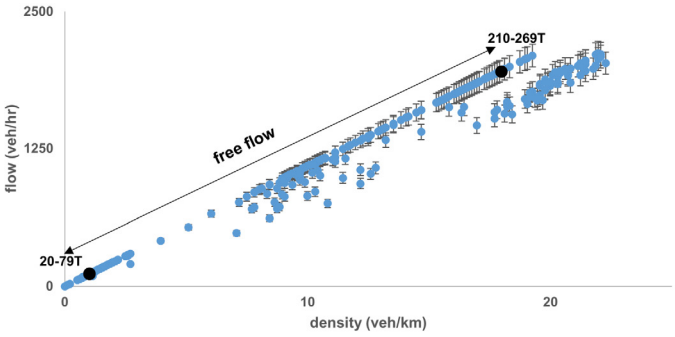
The models discussed in the literature to date are fundamentally different from that proposed in this study. Essentially, most



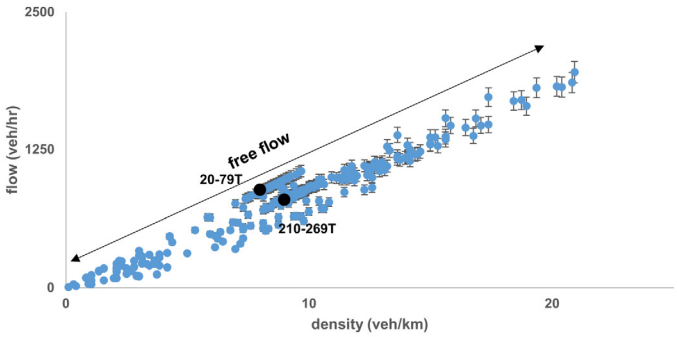
(a) Schematic network right side lane



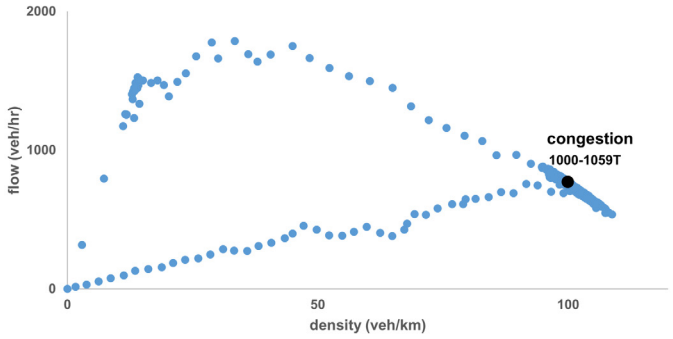
(b) Schematic network left side lane



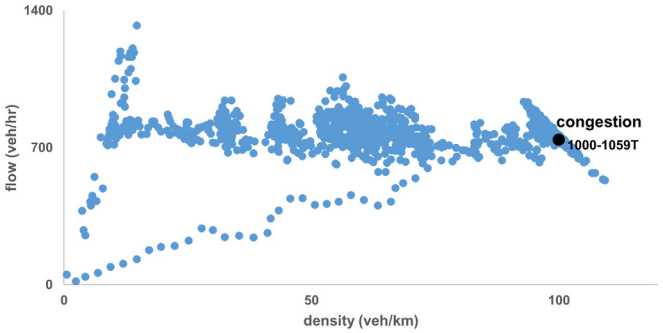
(c) Sydney M4 network right side lane



(d) Sydney M4 network left side lane



(e) Sydney M4 network right side lane (a congested situation)



(f) Sydney M4 network left side lane (a congested situation)

Fig. 7. Fundamental traffic flow diagrams for each lane (• indicates the states studied).

methods rely on finding inconsistencies in the data sent in the BSM message, for instance, using kinematic theory. However, a smart malicious vehicle can intelligently bias the data to ensure that the BSM message is wrong while adhering to the consistency check of the kinematic data (see [22][28]). Similarly, reputational methods only work if a large number of vehicles are not anomalous. Finally, machine learning methods are sensitive to the training data and are not easily generalizable to new situations and datasets.

The method proposed in this study uses "traffic flow theory" on the data collected from its own sensors as a litmus to evaluate the BSM data. The fact that they are two separate sources of data, but are required by the physics of traffic to be consistent, is what is used to evaluate the integrity of the data. This method is not susceptible to the weaknesses of the kinematic theory, as it uses to separate data sources. It also does not have the failings of the reputation-based methods that require a large number of vehicles to be good. Finally, due to the reliance on fundamental principles of traffic flow theory, it is more generalizable and transferable than machine learning methods. Table 3 summarises how our method stands out.

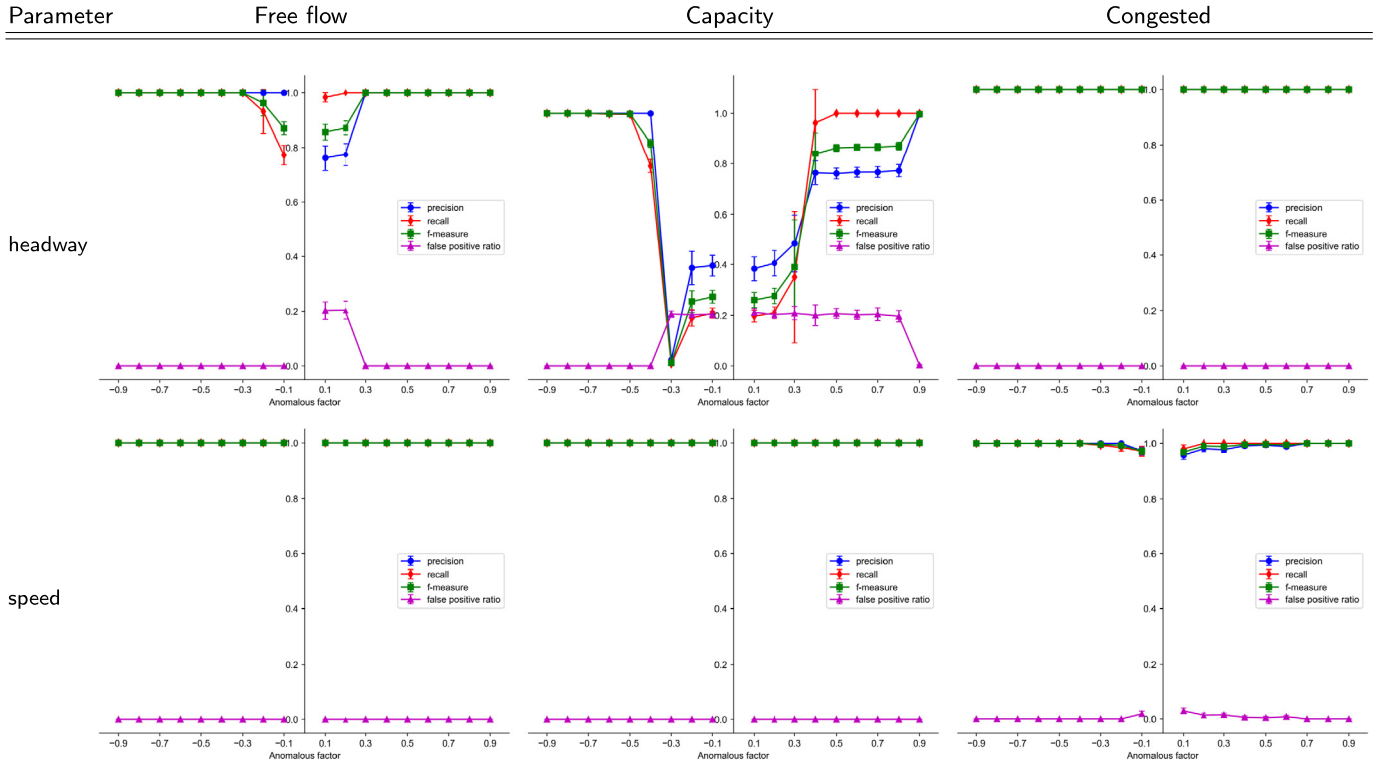
Table 2
Results summary.

	Free flow	Capacity	Congested
space-headway	✗	✗	✓
speed	✓	✓	✓

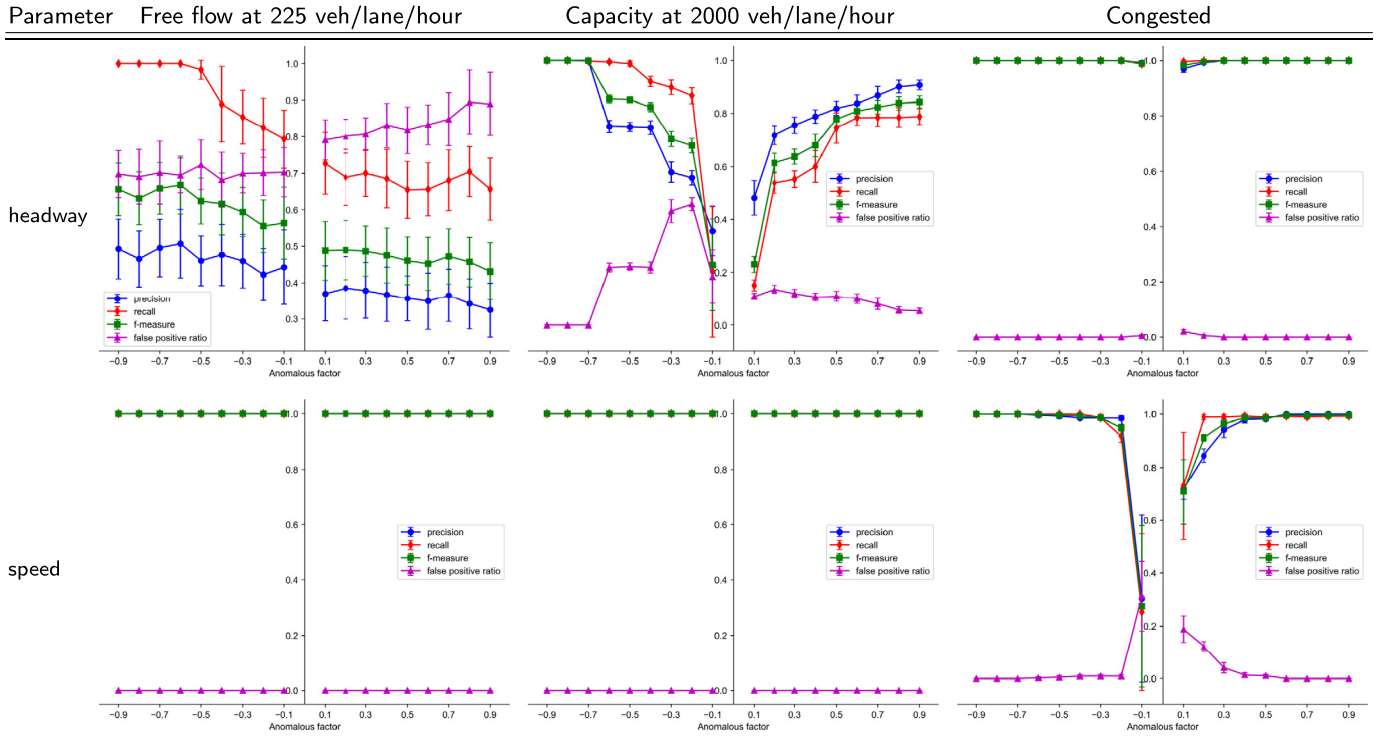
The performance of the detection during free flow and capacity is affected by lane changes and varying safety distances kept by drivers, and the performance during the congested states is affected by brakes. ✓ and ✗ represent the reliability and unreliability of the detection method.

6. Conclusion

This work evaluates the applicability of traffic flow fundamentals to detect anomalous nodes in vehicular networks. Unlike the previous studies focused on kinematic models, reputation systems and machine learning approaches, we recognise that anomalous vehicles are a traffic problem. Our method evaluates the trust-



(a) Precision, recall, f-measure and false positive ratio behaviour when 40% of the vehicles are anomalous on the right lane of the schematic system



(b) Precision, recall, f-measure and false positive ratio behaviour when 40% of the vehicles are anomalous on the right lane of Sydney M4

Fig. 8. Precision, recall, f-measure and false positive ratio behaviour when 40% of the vehicles are anomalous. The complete set of results is in the Appendix available at https://github.com/malithrana/dav-using-tp.

Table 3
Results comparison.

	Rely on internal consistency of messages	Rely on an honest majority	Sensitive to training data sets
Kinematic models	✓	✗	✗
Reputation-based models	✗	✓	✗
Machine Learning models	✗	✗	✓
Traffic flow theory models	✗	✗	✗

worthiness of space-headway and speed parameters of beacons independently using traffic flow theory.

However, establishing a global ground truth is challenging when the required infrastructure is not present. Although we assume the accessibility to the ground truth, there can be occasions where this information is not available. In such circumstances, vehicles can establish a localised ground truth using the data received via their own sensor systems. According to the experiments, the results are similar for the detections performed using both local and global ground truths (see the Appendix).

In our work, we propose the use of a parsimonious traffic flow model based on steady state conditions. Though lane changing is an integral part of traffic dynamics, the steady state traffic flow relationships and phenomena have been shown to be fundamentally enduring with lane changing. In the micro-simulation experiments that were performed, lane changes did exist and were observed. We demonstrate that the steady-state traffic flow theory does predict anomalies reasonably well. In fact, speed detection was found to perform robustly well with lane changes. However, lane changes do have a significant detrimental impact on space-headway detection in free-flow conditions; it however performs robustly well where it matters, in congested conditions. Therefore, we can rely more on the speed detection model to discern anomalies in free flow conditions, where the headway detection might not perform well.

The method developed in this research only deals with being able to identify whether data received through the CCH channel are anomalous or not. To assess this, we only rely on macroscopic traffic flow information such as average flow, density and speed in the local area of the vehicle assessing a BSM message. This data can be received either through RSUs (such as loop detectors, cameras etc.) or the vehicle's own sensor systems that infer these traffic flow parameters. The method proposed then evaluated the consistency of the BSM message with these macroscopic traffic flow parameters. We do not assume that 100% of vehicles are connected, or that we are receiving data regularly and reliably; we are only evaluating the correctness of the data when they are received. To provide additional realism, we have used a test schematic network and an actual network of Sydney. We will test the current work with data from different networks in future work.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Simulation results, networks and data

The complete set of results is available at:
https://github.com/malithrana/dav-using-tp

The studied traffic networks and simulated dataset are available at:
https://github.com/malithrana/dav-using-tp/tree/master/data

References

[1] M. Behrisch, L. Bieker, J. Erdmann, D. Krajzewicz, Sumo–simulation of urban mobility: an overview, in: Proceedings of SIMUL 2011, The Third International Conference on Advances in System Simulation, ThinkMind, 2011.

[2] N. Bißmeyer, K.H. Schröder, J. Petit, S. Mauthofer, K.M. Bayarou, Short paper: experimental analysis of misbehavior detection and prevention in vanets, in: 2013 IEEE Vehicular Networking Conference, IEEE, 2013, pp. 198–201.

[3] N. Bißmeyer, C. Stresing, K.M. Bayarou, Intrusion detection in vanets through verification of vehicle movement data, in: 2010 IEEE Vehicular Networking Conference, IEEE, 2010, pp. 166–173.

[4] C. Daganzo, C. Daganzo, Fundamentals of Transportation and Traffic Operations, vol. 30, Pergamon, Oxford, 1997.

[5] W. Farooq, M. Ali Khan, S. Rehman, A novel real time framework for cluster based multicast communication in vehicular ad hoc networks, Int. J. Distrib. Sens. Netw. 12 (2016) 8064908.

[6] M. Gerla, E.K. Lee, G. Pau, U. Lee, Internet of vehicles: from intelligent grid to autonomous cars and vehicular clouds, in: 2014 IEEE World Forum on Internet of Things, WF-IoT, IEEE, 2014, pp. 241–246.

[7] P. Golle, D. Greene, J. Staddon, Detecting and correcting malicious data in vanets, in: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, 2004, pp. 29–37.

[8] R.W. van der Heijden, S. Dietzel, T. Leinmüller, F. Kargl, Survey on misbehavior detection in cooperative intelligent transportation systems, IEEE Commun. Surv. Tutor. 21 (2018) 779–811.

[9] R.W. van der Heijden, T. Lukaseder, F. Kargl, Veremi: a dataset for comparable evaluation of misbehavior detection in vanets, in: International Conference on Security and Privacy in Communication Systems, Springer, 2018, pp. 318–337.

[10] D. Jiang, L. Delgrossi, Ieee 802.11 p: towards an international standard for wireless access in vehicular environments, in: VTC Spring 2008-IEEE Vehicular Technology Conference, IEEE, 2008, pp. 2036–2040.

[11] I. Kantzavelou, P.F. Tzikopoulos, S.K. Katsikas, Detecting intrusive activities from insiders in a wireless sensor network using game theory, in: Proceedings of the 6th International Conference on PErvasive Technologies Related to Assistive Environments, 2013, pp. 1–8.

[12] C. Lai, H. Zhou, N. Cheng, X.S. Shen, Secure group communications in vehicular networks: a software-defined network-enabled architecture and solution, IEEE Veh. Technol. Mag. 12 (2017) 40–49.

[13] T. Leinmüller, C. Maihöfer, E. Schoch, F. Kargl, Improved security in geographic ad hoc routing through autonomous position verification, in: Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks, 2006, pp. 57–66.

[14] T. Leinmüller, R.K. Schmidt, A. Held, Cooperative position verification-defending against roadside attackers 2.0, in: Proceedings of 17th ITS World Congress, 2010, pp. 1–8.

[15] T. Leinmuller, E. Schoch, F. Kargl, Position verification approaches for vehicular ad hoc networks, IEEE Wirel. Commun. 13 (2006) 16–21.

[16] T. Leinmüller, E. Schoch, F. Kargl, C. Maihöfer, Decentralized position verification in geographic ad hoc routing, Secur. Commun. Netw. 3 (2010) 289–302.

[17] X. Li, S. Jian, J. Monteil, V. Dixit, A probe vehicle-based technique to estimate fundamental diagrams on freeways and arterials, Technical Report, 2016.

[18] J. Liang, J. Chen, Y. Zhu, R. Yu, A novel intrusion detection system for vehicular ad hoc networks (vanets) based on differences of traffic flow and position, Appl. Soft Comput. 75 (2019) 712–727.

[19] D. Manivannan, S.S. Moni, S. Zeadally, Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (vanets), Veh. Commun. 100247 (2020).

[20] M. Ranaweera, A. Seneviratne, D. Rey, M. Saberi, V.V. Dixit, Anomalous data detection in vehicular networks using traffic flow theory, in: 2019 IEEE 90th Vehicular Technology Conference, VTC2019-Fall, IEEE, 2019, pp. 1–5.

[21] M. Raya, P. Papadimitratos, V.D. Gligor, J.P. Hubaux, On data-centric trust establishment in ephemeral ad hoc networks, in: IEEE INFOCOM 2008-The 27th Conference on Computer Communications, IEEE, 2008, pp. 1238–1246.

[22] S. Ruj, M.A. Cavenaghi, Z. Huang, A. Nayak, I. Stojmenovic, On data-centric misbehavior detection in vanets, in: 2011 IEEE Vehicular Technology Conference, VTC Fall, IEEE, 2011, pp. 1–5.

[23] R.K. Schmidt, T. Leinmüller, E. Schoch, A. Held, G. Schäfer, Vehicle behavior analysis to enhance security in vanets, in: Proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop, V2VCOM2008, Citeseer, 2008.

[24] H. Sedjelmaci, S.M. Senouci, M.A. Abu-Rgheff, An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks, IEEE Int. Things J. 1 (2014) 570–577.
[25] P.K. Singh, S. Gupta, R. Vashistha, S.K. Nandi, S. Nandi, Machine learning based approach to detect position falsification attack in vanets, in: International Conference on Security & Privacy, Springer, 2019, pp. 166–178.
[26] S. So, P. Sharma, J. Petit, Integrating plausibility checks and machine learning for misbehavior detection in vanet, in: 2018 17th IEEE International Conference on Machine Learning and Applications, ICMLA, IEEE, 2018, pp. 564–571.
[27] K.F. Ssu, C.H. Ou, H.C. Jiau, Localization with mobile anchor points in wireless sensor networks, IEEE Trans. Veh. Technol. 54 (2005) 1187–1197.
[28] H. Stubing, A. Jaeger, C. Schmidt, S.A. Huss, Verifying mobility data under privacy considerations in car-to-x communication, in: 17th ITS World CongressITS JapanITS AmericaERTICO, 2010.
[29] O.A. Wahab, H. Otrok, A. Mourad, A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles, Comput. Commun. 41 (2014) 43–54.
[30] H. Wang, M. Song, Ckmeans. 1d. dp: optimal k-means clustering in one dimension by dynamic programming, R J. 3 (2011) 29.
[31] M. Yue, L. Fan, C. Shahabi, Inferring traffic incident start time with loop sensor data, in: Proceedings of the 25th ACM International on Conference on Information and Knowledge Management, 2016, pp. 2481–2484.
[32] K. Zaidi, M.B. Milojevic, V. Rakocevic, A. Nallanathan, M. Rajarajan, Host-based intrusion detection for vanets: a statistical approach to rogue node detection, IEEE Trans. Veh. Technol. 65 (2015) 6703–6714.