Malicious attack detection based on traffic-flow information fusion

Ye Chen
Beijing University of Technology,China
chenye202558@sina.com

Yingxu Lai
Beijing University of Technology,China
laiyingxu@bjut.edu.cn

Zhaoyi Zhang
Beijing University of Technology,China
1426134439@qq.com

Hanmei Li
Beijing University of Technology,China
1403901750@qq.com

Yuhang Wang
Beijing University of Technology,China
w18738778778@163.com

***Abstract*—While vehicle-to-everything communication technology enables information sharing and cooperative control for vehicles, it also poses a significant threat to the vehicles' driving security owing to cyber-attacks. In particular, Sybil malicious attacks hidden in the vehicle broadcast information flow are challenging to detect, thereby becoming an urgent issue requiring attention. Several researchers have considered this problem and proposed different detection schemes. However, the detection performance of existing schemes based on plausibility checks and neighboring observers is affected by the traffic and attacker densities. In this study, we propose a malicious attack detection scheme based on traffic-flow information fusion, which enables the detection of Sybil attacks without neighboring observer nodes. Our solution is based on the basic safety message, which is broadcast by vehicles periodically. It first constructs the basic features of traffic flow to reflect the traffic state, subsequently fuses it with the road detector information to add the road fusion features, and then classifies them using machine learning algorithms to identify malicious attacks. The experimental results demonstrate that our scheme achieves the detection of Sybil attacks with an accuracy greater than 90% at different traffic and attacker densities. Our solutions provide security for achieving a usable vehicle communication network.**

***Index Terms*—Vehicular networks, Attack detection, Sybil attacks, Traffic flow characterization, Information fusion**

I. Introduction

With the development of cooperative vehicle infrastructure technology, vehicle-to-everything (V2X) in vehicle networking plays a significant role in improving road safety, traffic efficiency, and in-vehicle infotainment systems [1]. The V2X communication technology relies on the basic safety message (BSM) sent periodically by vehicles to transmit information, such as their location and speed [2]. Such traffic information is essential for map navigation, which provides drivers with optimal path selections. An attacker can interrupt the path selection of normal vehicles by maliciously modifying or falsifying the information in the specified fields of the BSM. As the scope of the attack expands, it can also affect the global traffic status in the attack area and even threaten the safety of normal vehicles. Therefore, it is crucial to detect malicious attacks on BSMs.

While employing the BSM technology to improve the efficiency of traffic operations, it is essential to meet the security requirements of vehicle privacy protection and message unlinkability [3], as normal traveling vehicles broadcast their BSMs by using legitimate, untraceable pseudonyms to protect their private information [4]. Unfortunately, when attackers exploit such pseudonym schemes, their malicious attacks remain hidden in legitimate BSMs for propagation, which not only affects the driving status of normal vehicles but also hides the real identity of the attacker and complicates the attack identification using malicious attack detection systems. This behavior is generally referred to as Sybil attacks in vehicular networking [5]. Therefore, detecting complex malicious behaviors, including Sybil attacks, is an important issue that needs to be addressed urgently.

Researchers have been studying and designing attack detection models for BSMs. Kamel [6], proposed a misbehavior detection scheme based on local plausibility checks in vehicles, plausibility and consistency checks of vehicle driving states in broadcast messages, reports of suspected vehicle misbehavior uploaded by local observer vehicles, and the cloud management center discriminates the behavior of suspect vehicles. The proposed scheme demonstrated a good detection ability in case of a single attack. However, the detection ability deteriorated in a complex attack scenario, which includes Sybil attacks, and relied on an honest majority of neighboring observer vehicles. Malith [7] proposed a method of anomalous vehicle detection based on traffic physical quantities, obtained by analyzing the microscopic parameters (i.e., speed and space-headway) derived from the traffic flow theory and by comparing the consistency of these parameters under different traffic scenarios; he proposed to employ the traffic flow theory for anomalous data detection of BSMs in vehicular networks. The scheme introducing the traffic flow theory is inspiring; it incorporates data from loop coil vehicle detectors for comparison and does not rely on internal consistency checks of messages; instead, it

This work was supported by the National Key R&D Program of China (Key Technologies and Applications of Security and Trusted Industrial Control System, No. 2020YFB2009500); Natural Science Foundation of Beijing Municipality (No. 19L2020).

ISBN 978-3-903176-48-5

only proposes two features: headway time distance and speed. The experiment in our study was conducted only on straight roads, without traffic circles, intersections, highways, traffic lights, and other complex road conditions.

Many of the current relevant detection schemes employ plausibility and consistency checks, while others are based on the verification of real physical metrics. Existing schemes demonstrate promising results in some single attack category scenarios. However, their ability to detect attackers is compromised when attackers tamper with message contents or falsify physical quantities. Unlike schemes based on plausibility checks, which utilize joint learning, neighbor observers, and trust reputation, the effectiveness of the neighbor observers-based scheme relies on an honest majority in the traffic scenario. When attack density increases, most attacking nodes degrade the detection effectiveness. To solve the aforementioned problem, it is necessary to analyze the essential characteristics of the attack behavior and construct critical features based on the differences between normal and attack behaviors.

Based on analyses, we concluded that the attack behavior in V2X essentially focuses on affecting the traffic flow constituted by normal vehicles, such as causing false congestion by increasing the Sybil nodes to increase the traffic density, affecting the path planning choice of other vehicles, using the sudden appearance of vehicles to cause normal vehicles to stop sharply, or even causing serious traffic accidents. Therefore, based on the content of vehicle BSMs, we further constructed traffic flow-related derived features by combining attack behavior characteristics, which can improve the detection ability for Sybil attacks. By contrast, in a situation of low attacker density and traffic flow, the impact of their behavior on the global traffic flow is reduced, and it becomes difficult to identify the attack behavior using regular methods. To solve this problem, we analyzed BSMs during this time period and fused the road information within the scene to construct the traffic flow information fusion feature data for the specified road section and reinforced the impact generated by the attack behavior to achieve a better detection effect. The contributions of this study are as follows:

- Different from the current Sybil attack detection schemes in the VANET, we propose a new idea of attack detection on road traffic flow for the first time, focused on the impact of the attack behavior on the traffic flow rather than the attacker itself, making it demonstrated a good generalization ability.
- We proposed a construction method for 19 traffic flow fusion features, including location speed, message frequency, and number of blocking points. Achieved an attack detection model based on the fusion of multi-source traffic flow information, making it have a composite Sybil attack detection ability independent of traffic density and attack density, and it can deal with complex traffic scenarios with compound attacks.
- Our experiments based on the publicly available dataset VeReMi Extension demonstrated that the proposed traffic flow fusion detection method is very effective in detecting Sybil attacks in complex scenarios, and the accuracy rates are higher than 90%.

II. Related Studies

In a traffic scenario using the V2X technology for communication, vehicles exchange information with each other to improve the efficiency of road operations and guarantee safety while driving. BSM content is the most basic physical quantity of vehicle kinematic characteristics containing information such as the current position, speed, acceleration, and head direction of the vehicle. These messages form the basis for constructing the characteristics of road traffic flow, and the correct message content is the key to securing the safety and improving the efficiency of traffic scenarios. When attackers use BSMs to implement their malicious attacks through forgery and tampering, serious damages are caused to various applications in VANETs, causing network paralysis, significant reduction in traffic efficiency, and even serious traffic accidents. Therefore, detection of attacks on BSMs is crucial in securing V2X communication and is a prerequisite to terminate any future attacks.

A. Attacker Model

Attackers employ different strategies to fake Sybil vehicles and include compound attack scenarios in which these vehicles affect the original path and direction of other vehicles to a certain extent for the purpose of the attack. The characteristic of Sybil attacks is that Sybil nodes are almost close to the positions of real vehicles obtained via BSM analysis. Therefore, analyzing the specific features of the attack behavior and further constructing derived features based on the original traffic flow features, such as the frequency of sending messages, path changes, and the number of road congestion points, further improves the detection method's ability to detect the attack behavior. Kamel's team proposed a Sybil attack specifically to provide a composite Sybil attack model based on the misbehavior-based management organization architecture [6]. In this study, four composite attack models containing Sybil attacks were selected and are described below.

The GridSybil attack is illustrated in Fig. 1. The attacker employs a legitimate pseudonym to fake the appearance of multiple Sybil nodes (ghost cars) gathered on the road, thus creating false traffic congestions to achieve interference with normal vehicle path selection.

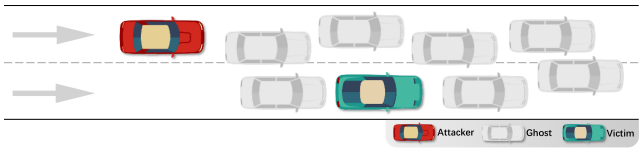

Fig. 1. GridSybil Attack.

In the DoSRandomSybil attack illustrated in Fig. 2, the attacker sends messages at a higher frequency than the frequency specified in the protocol, thus taking up more channel resources. The attacker also fills the message fields in the BSM with random values, which heavily occupies local detection resources and paralyzes traffic services in the region.

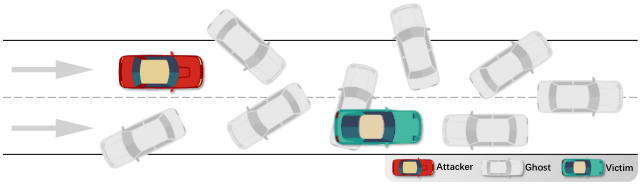

Fig. 2. DoSRandomSybil Attack.

The DoSDisruptiveSybil attack is depicted in Fig. 3. Based on the DoS attack, the attacker continuously broadcasts falsified V2X messages containing data that are derived based on messages from neighboring vehicles. These attack messages are derived from real vehicle data to cheat the message internal plausibility checks and evade detection.

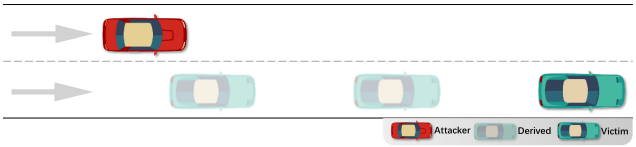

Fig. 3. DoSDisruptiveSybil Attack.

The DataReplaySybil attack is illustrated in Fig. 4. The attacker replays the message of the neighboring vehicle and tampers with some of its content, thereby tricking the detection system into not identifying the real victim vehicle.

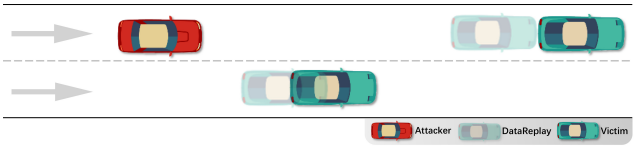

Fig. 4. DataReplaySybil Attack.

For all types of vehicle misbehaviors containing the aforementioned attack categories, existing detection schemes can be divided into data consistency-based methods and node-cooperation-based methods and can be further combined with blockchain technology, reputation, and trust-based detection methods.

B. Data Consistency-Based Methods

The data-centric detection approach can be divided into two types based on the data source. The first type analyzes the physics variables of the communication between vehicle nodes and compares whether the real metrics and the metrics declared in the BSM content are the same. Based on this, it identifies messages with BSM content different from the real physical communication metrics as suspicious attacks.

Nguyen's team [8] achieved a method to detect location faking attacks by getting information from the physical signals received by the vehicle from a multi-array antenna to verify the authenticity of the GPS location in V2X messages. This type of scheme detects attacks with the help of the amount of truth in the physical information [9] [10] [11] [12]and has a short response time to attacks, which can provide the vehicle with enough time to react. Although physical signal-based detection schemes have a significant advantage in terms of response speed, in real traffic scenarios, the RSSI values declared in the messages can not only be tampered with by attackers but also receive the influence of building occlusion, which is not completely reliable and requires further analysis and judgment supported by other methods.

The second one is to determine whether a node has committed an attack by analyzing the consistency and plausibility of the content of multiple consecutive BSMs of a vehicle node. To solve the problem that existing detection systems cannot adapt to the dynamic changes of VANET scenarios, Sultana [13] proposed a framework for misbehavior detection in VANET based on software-defined networks. Ghaleb [14]analyzed the spatio-temporal relationships during vehicle movement to establish a contextual reference model for online updates. There have been several approaches to construct feature vectors [15] [16] based on the plausibility check values and use machine learning [17] [18] [19] to classify and detect attacks. Reasonable consistency checks are the most widely used case in vehicle misbehavior detection and the closest scheme to the current reality of vehicle node computational resources, but scenarios involving Sybil attacks in which ghost vehicles faked by kinematic simulation are often able to fool the reasonableness detection system.

C. Node-Cooperation-Based Methods

In a scenario, the vehicle nodes and roadside unit nodes involved in the network communication also act as observers to collect and detect information about other vehicle nodes within the communication range. Once the observer detects an abnormal message, it reports the BSM sent by the suspicious node and the related sensor data to the upper-level MDS for further detection. The scheme proposed by Gyawali [20] demonstrates that the it is possible to direct neighbor observers, and such cooperative-based machine learning schemes [21] [22] can detect false alarm attacks and location forgery attacks. Each vehicle could collect broadcast from its neighbors for detection results and aggregate them to detect misbehaving vehicles. The local traffic density-based VANET behavior detection approach [23] measures local traffic density from two independent sensors. It uses it as evidence of specific traffic conditions to detect attacks.

D. Reputation and Trust-Based Detection Methods

Reputation schemes are biased in judging the behavior of vehicles through collective opinions; the schemes represent the behavioral characteristics of vehicles over time and can predict the behavior of vehicles in future periods based on enough relevant information. Some schemes consider the establishment of trust management mechanisms in the upper layers of vehicle nodes [24] [25] [26], simultaneously, the protection of vehicle privacy has also received much attention from researchers; approaches to detect attacking vehicles while protecting the privacy of normal vehicles and not revealing their driving paths or driving habits [27] [28] has become a hot research topic: privacy protection is vital in attack detection. In the designed solution, we try to protect the privacy of vehicles by hiding their individual driving characteristics as much as possible, integrating the vehicle nodes into the road traffic flow for analysis and not detecting them for individual vehicles.

III. Traffic Flow Information Fusion Solution

Our detection model focuses on solving the honest majority problem, reducing the impact of traffic density variations on detection effectiveness and detecting compound Sybil attacks in complex traffic road scenarios. Detection methods that rely on observer vehicles require a honest majority, and an increase in attacker density when traffic density is low can affect the effectiveness of detection. To solve these problems, we analyze the original purpose of the attack behavior, investigate the impact of the attack behavior on the traffic flow, and use it as a basis to identify the characteristics of the attack behavior occurring on the road. We add real data fed back by road detectors to construct multi-dimensional traffic flow fusion features, eliminate the uncertainty of observer vehicles, and avoid the honest majority problem. Meanwhile, the scheme with vehicle nodes as detection objects generally relies on the plausibility verification method, but in real traffic scenarios, complex traffic scenes and sensor errors can affect the effectiveness of plausibility verification, and the BSM content of vehicle broadcasts can be tampered with, affecting the detection effect. Unlike existing detection schemes, the detection object of this method is not a single vehicle node, but it is to detect whether there is an attack on a particular road within a specified time window, remove the limitations of the plausibility verification method, and make the detection model have better generalization capability to compound attacks and complex traffic scenarios.

Finally, we propose a method to construct features to detect attacks based on BSM content and fuse traffic flow information and road data. The method has the advantage of not requiring a vehicle node as an observer to provide others' behavioral information while being independent of traffic flow density and attacker density and being able to detect attacks in complex scenarios. The overall model structure is shown in Fig. 5.

The variables used for the subsequent feature construction descriptions in this scheme and their definitions are provided in Table I.

TABLE I
Detection Results Traffic Densities

Variables	Definition
$RoadID_i$	Unique identification of road ID
$T_k\,(T_0 \sim T_1)$	Time window
S	Collection of BSM data
M_j	Number jth BSM
$M_{j.roadid}$	The road ID attributed to the jth BSM
$M_{j.sendTime}$	Send time of the jth BSM
$M_{j.senderPseudo}$	Sender pseudonym for jth BSM
$M_{j.speed}$	Travel speed of the jth BSM
N_{bi}	Number of vehicles on road i
$N_{Deviate}$	Number of vehicles not on the road for BSM
ρ_i	Road traffic density
n_{bs}	Vehicles per second
M_{jp}	Pseudonym in message
$\bar{V}_{Speedi}$	Average speed
S^2_{Speedi}	Variance of speed
R_{Speedi}	Extreme difference of speed
σ_{Speedi}	Standard deviation of velocity
$S^2_{s-Numberi}$	Variance of the number of vehicles per second sequence in the time window
$S^2_{s-Speedi}$	The variance of the sequence of the sum of vehicle speeds per second in the time window
$SUM_{Congestion}$	Total number of congestion points on the road during the time window
$f_{s-Messagei}$	Frequency of roadside specified road messages per second

A. Traffic Flow Characteristics from BSM

Our scheme uses a roadside node RSU as an entity that collects BSM message contents within a specified scenario, as a road facility within a specific scenario area has more computing and storage resources than a vehicle node and can receive BSM contents sent by all vehicles traveling on the road within its communication domain. The RSU collects the BSMs sent by all the vehicles in the communication area within a time window and constructs the traffic flow characteristics of each road in the scenario based on the traffic flow status and the preset zone road information.

To reflect the traffic flow condition of a road within a time window from multiple perspectives, the three most essential elements of traffic flow need to be considered: traffic density, travel speed, and traffic flow. By combining each element, as well as the sender pseudonym, position, and current speed provided in the BSM content, a total of seven traffic flow-related features are constructed through a simple sequence calculation, and the construction method of this scheme is given below through a feature construction example for one of the roads.

Message collection: We set the unique identification information of the road as $RoadID_i$ and collect all the BSM messages attributed to the road $RoadID_i$ in a total time period $T_k\,(T_0 \sim T_1)$ of 60s.

$$S = \{M_j \mid M_{j.roadid} = RoadID_i, T_0 \le M_{j.sendTime} < T_1\} \tag{1}$$

Feature 1: From the above set S, the list of sender pseudonyms in all the BSM messages L are extracted. After counting, we can obtain the critical judgment feature: the number of vehicle nodes N_{bi} in the current road counted by the BSM message source.

$$L = \{M_{jp} \mid M_{j.senderPseudo} \in S\} \tag{2}$$

Feature 2: By combining the geographic location coordinates in each message received by RSU with road information, it can be determine whether the declared position of the vehicle is on the road. If the distance from the road exceeds the specified threshold, then it is judged as not being driven on the road, and the number $N_{Deviate}$ is counted as a feature.

Features 3,4,5,6: $M_{j.speed}$ is the speed information in the BSM content, which is also given by a pair of coordinate values. In the 60 s time window, the driving speed of each vehicle is recorded, and then the mean, variance, extreme deviation, and standard deviation of the message speed sequence on the road are calculated separately to reveal different traffic flow characteristics $\bar{V}_{Speedi}$, S^2_{Speedi}, R_{Speedi}, σ_{Speedi}.

Feature 7: Traffic flow density information ρ_i is calculated based on the road length and the number of vehicles as the base feature.

The traffic flow base features are derived from the content of BSM, which does not involve complex statistical calculations

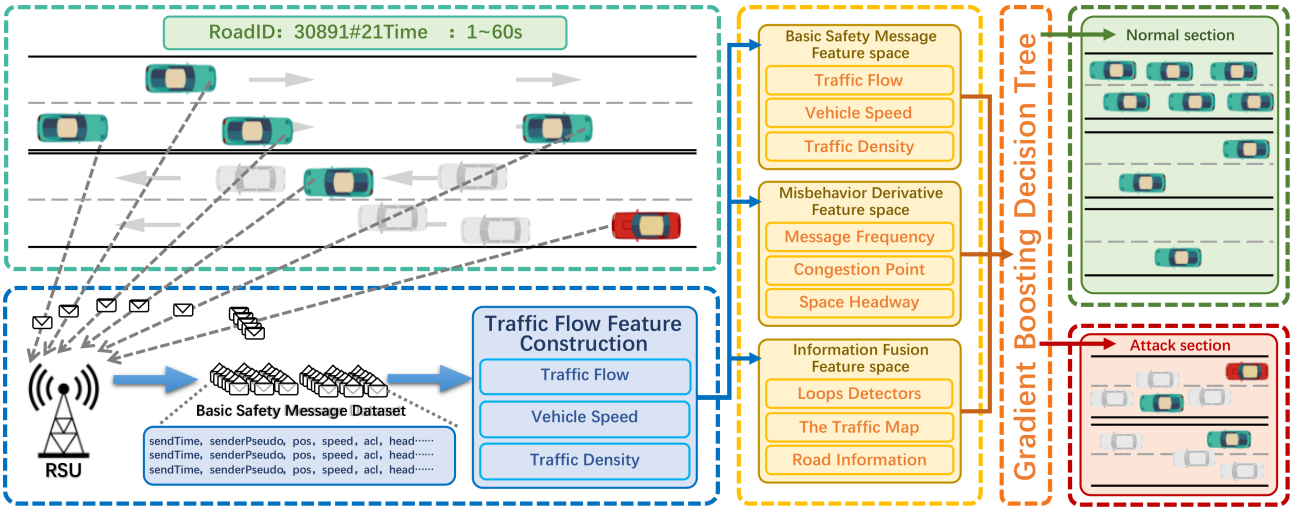

Fig. 5. Overview of the Traffic Flow Information Fusion Detection Model.

volume and attack behavior characteristics, and a single traffic flow feature is reflected from the content of BSM to restore the actual traffic scene parameters.

B. Derived Features Based on Attack Behavior

Traffic flow features constructed using BSM content have detected some common attack categories, such as random position attacks, but the detection capability for Sybil attacks needs to be improved.

Therefore, this method uses the content provided in BSM to consider the vehicles on the road as a complete set as per the characteristics of the attack behavior and constructs traffic features derived for a section of the road to express and study the impact of the attack behavior on the traffic flow. Each feature corresponds to specific features of different attack categories, and following the example given above, the feature construction method is as follows.

Feature 8: In the set S, the 60s time window is sliced second by second, and the number of vehicle nodes on the road in each second of the change sequence is counted n_{bs}. Ghost cars always appear suddenly; therefore, the number of vehicle nodes will suddenly increase during a Sybil attack, producing a large increase in the number once, and calculating the variance of the sequence of the number of vehicle nodes $S^2_{s-Numberi}$ can reflect to some extent the degree of fluctuation of the number of vehicle nodes on the road increase or decrease.

$$S^2_{s-Numberi} = \frac{\sum_{i=1}^{k} (n_{bs} - \bar{n})^2}{k-1} \tag{3}$$

Feature 9:$M_{j.speed}$ is the speed information in the BSM content, given by a pair of coordinate values. Different from the overall analysis in terms of the construction of the derived features, we also use a 60s time window that slices second by the second to obtain the total speed of all the vehicle on the road in each second to form a sequence and calculate the variance $S^2_{s-Speedi}$. The sudden appearance of multiple ghost vehicle nodes will cause the total vehicle speed to fluctuate once, which is the information that needs to be captured by this feature.

Features 10,11,12,13: $M_{j.pos}$ is the location information in the BSM content, which can be used to calculate the distance between vehicle nodes and each other, in addition, to determining the distance relationship between the BSM message source and the road. In a congestion Sybil attack, the attacker virtualizes that Sybil nodes generally appear around the victim vehicle; therefore, detecting the number of neighboring nodes around the vehicle node helps identify Sybil attacks.

According to the road situation, we designate the distance between vehicle nodes less than 5m at a specific moment as the neighbor nodes and measure the variance, extreme deviation, and standard deviation of the sequence of the number of nearest neighbors S^2_{s-Neii}, R_{s-Neii}, and σ_{s-Neii}. Meanwhile, we record the node with more than 5 neighboring nodes as a road congestion point, and the total number of congestion points $SUM_{Congestion}$ of the road in the time window is also recorded as a feature.

Features 14,15: The message frequency of M_j is also a critical feature considered in this scheme to cope with the DoS category of attack behavior, which is calculated based on the BSM message frequency, and the same 60s time window slicing-by-second idea is used to obtain the sequential variance of the number of messages per second $S^2_{s-Messagei}$ and the message frequency per second $f_{s-Messagei}$.

Feature 16: The number of spacing sequence outliers of vehicles traveling in the same direction in the road. Based on the direction information of the road to which M_j belongs, the nodes of vehicles traveling in the same direction on the road are filtered out, the spacing between vehicle nodes is calculated, and the average value $\bar{V}_{Spacedisi}$ is calculated.

C. Traffic Flow Information Integration

Derived traffic flow features constructed by analyzing attack behaviors have been able to detect Sybil attacks and have improved performance in the detection of compound attacks. However, when all traffic scenarios are considered comprehensively, complex traffic scenarios and changing traffic density cannot be handled by context in the BSM alone; therefore,

other data sources on the road need to be added for fusion analysis to improve the detection performance further.

Sybil attacks fake multiple ghost vehicle nodes, but creating false congestion is only one type of attack, and the detection of replay Sybil attacks becomes very difficult when the traffic flow density is low. Using features such as the number of congestion points in traffic flow characteristics, it is impossible to distinguish between Sybil and normal vehicle nodes in replay attacks. Therefore, our detection model chooses to add road loop detector information within the traffic scene as a second data source to accurately discriminate the presence of Sybil nodes in the traffic flow.

The road vehicle loop detector is set at the beginning of each lane, as shown in Fig. 6. It can provide feedback on the actual number of vehicles passing through the detector and the average speed, which can be used as the actual basis for the number of normal vehicles in a particular road section. In current traffic facilities, this detection method is statistically accurate, and the equipment is in a stable operating condition and has an excellent performance under bad weather conditions. Its low cost makes it one of the most widely used traffic detectors globally.

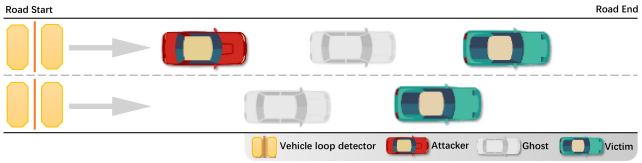

Fig. 6. Vehicle Loop Detector.

For the road attribution of BSM messages, we use the actual distance between the BSM declared geographic location and the road to determine which road the BSM message belongs to and whether the node sending the message belongs to the expected road based on the offset distance $D_{locatei}$ between the BSM node and the road. The message whose offset distance from all road sections exceeds the threshold counted as a message with suspicious behavior, as shown in Equation 4. Based on the above method, we construct fusion features using the vehicle loop detector data as follows.

$$\begin{cases} D_{locatei} \leq 7\text{m} & \text{Message node belongs to the road} \\ D_{locatei} > 7\text{m} & \text{Message node not on the road} \end{cases} \quad (4)$$

Features 17,18,19: The construction data for this part of the feature comes from the return values of the vehicle loop detectors arranged on the road. The data recording frequency of the sensor coil is synchronized with the time window so that the actual number of vehicle nodes passing the road N_{loopi} can be obtained, and the number of vehicle nodes entering the sensor $N_{loop-ini}$ is used to compare with the number of vehicle nodes N_{bi} obtained from the BSM message source. Also, the average vehicle speed V_{loopi} from the coil statistics is used as a fusion feature. The presence of Sybil nodes cannot be accurately determined using BSM messages, while the coil detector can determine the actual number of vehicles passing; therefore, we use the feature that different data sources observe different numbers of vehicle statistics to cope with various traffic road scenarios and low traffic flow. According to the features constructed in the above example, theoretically, N_{loopi} will undercount some of the vehicle nodes that have passed the loop coil and are on the road at the moment of T_0 to correct the sensor data, the following conclusions can be obtained through a logical analysis.

$$\begin{cases} N_{loopi} < N_{bi} & \text{Existence of Sybil nodes} \\ N_{loopi} = N_{bi} & \text{Consistent number of vehicle nodes} \\ N_{loopi} > N_{bi} & \text{Sensor anomalies} \end{cases} \quad (5)$$

By comparing the number of nodes given by the two data sources, it is possible to construct features that can accurately distinguish Sybil attacks and are not affected by traffic density, enabling adaptation to more complex traffic scenarios.

IV. Experimental Results and Analysis

A. Experimental Scenario

Our experiments are based on the open-source misbehavior detection framework [29] (F2MD). F2MD is a branch module of VEINS, which is based on the C++ Objective Modular Network Testbed for network simulation (OMNeT++) and Simulation of Urban Mobility for road traffic simulation (SUMO). It is an open-source framework that has been widely used to run vehicle network simulations and emulations, as well as a simulation platform tool used by the VeReMi Extension dataset.

The datasets used in the experiments are all from the Luxembourg SUMO traffic scenario, and the simulation process selects data from different time periods for training and testing respectively. The specific data obtained through the F2MD framework simulation is shown in the Table II.

TABLE II
Number of Vectors of Traffic Flow Characteristics

Time Window	Grid Sybil	DoSDisruptive Sybil	DataReplay Sybil	DoSRandom Sybil
5h-6h	1863	1830	1822	1909
6h-7h	2893	2861	2839	2979
7h-8h	3670	3637	3628	3828

The data were obtained from the F2MD simulation. The overall scenario is shown in Fig. 7A, which includes road categories and facilities such as roads, highways, one-way streets, two-way lanes, roundabouts, intersections, and red lights as shown in Fig. 7B. Using data from three different time periods with different traffic densities, four compound attacks provided in the framework containing Sybil attacks, with multiple different attack densities, are trained and tested separately. Simultaneously, the detection schemes for the three phases proposed were tested and validated separately to compare and analyze the improvement in detection performance of the traffic flow information fusion method.

The simulation used in this dataset was constructed from real traffic data; therefore, it is almost identical to actual road conditions. We used different traffic densities as well as attack category notations for training and testing in various complex road scenarios.

Fig. 7. Realistic Traffic Scenarios with Complex Roads.

B. Evaluation Metrics

The performance of the proposed scheme was evaluated in terms of accuracy, precision, and recall, and these metrics are widely used to compare classification performance. The proposed scheme requires a high detection rate and a low false alarm rate. The confusion matrix in Table III was used to calculate the various parameters.

TABLE III
CONFUSION MATRIX

		Predicted	
		Negative	Positive
Actual	Negative	True Negative (TN)	False Positive (FP)
	Positive	True Negative (TN)	False Positive (FP)

- Accuracy is the ratio of the number of correctly classified attacks or normal behaviors to the overall sample size.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{6}$$

- Precision is the ratio of correctly predicted malicious vehicles to the total number of predicted malicious vehicles.

$$\text{Precision} = \frac{TP}{TP + FP} \tag{7}$$

- Recall is the ratio of malicious vehicles correctly predicted to the total number of actual malicious vehicles.

$$\text{Recall} = \frac{TP}{TP + FN} \tag{8}$$

In this scheme, whether a Sybil node (ghost car) passes on the road within a specified time window is used as the basis for determining whether there is an attack, and malicious vehicle nodes that are yet to launch an attack are not counted as attacking vehicles. The existing dataset was labeled according to this principle and classified by supervised learning to identify the malicious behavior of the four attack models in the traffic scenario.

C. Experimental Result

We tried to use a variety of machine learning algorithms for classification, such as plain Bayes, K-nearest neighbor, logistic regression, random forest, decision tree, support vector machine, and gradient boosting decision tree in advance. Based on the pre-experimental results, the gradient boosting decision tree showed better classification ability in all attack types; therefore, the gradient boosting decision tree was selected for further analysis in this scheme. The comparison results of different machine learning algorithms are shown in Fig. 8 below.

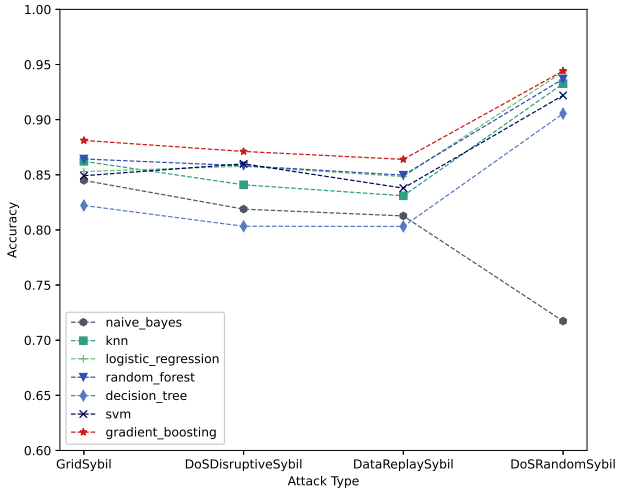

Fig. 8. Experimental Results of Machine Learning Classifier.

First, we validated the improvement in detection capability by information fusion features. Our solution constructs multi-category features from three stages, extracts basic features from BSM, constructs derived features according to the attack behavior, and finally adds road information to construct fusion features; the features constructed in each stage will further improve the features' ability to express traffic flow changes based on the features in the previous stage, and fuses data from other information sources from multiple perspectives; therefore, the GridSybil attack model with an attack density of 10% was used in the experiment. Separation experiments were conducted according to the gradual accumulation of features in three stages, and the results are shown in the following Table IV.

TABLE IV
THREE-STAGE FEATURE ACCUMULATION EXPERIMENTS RESULTS

GridSybil attack prob = 0.1	**BSM**	**BSM +Derivative**	**BSM +Derivative +Integration**
Accuracy	90.02%	92.75%↑	93.68%↑
Precision	67.42%	79.39%↑	83.44%↑
Recall	63.16%	68.95%↑	71.58%↑

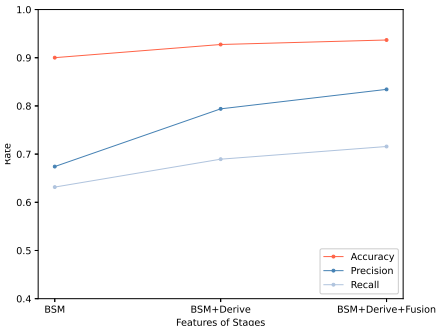

Fig. 9. Results of the Three-Stage Feature Accumulation Experiments.

According to the cumulative experimental results of the three stages of features shown in Fig. 9, it is evident that the performance indexes of the classification scheme all show a

trend of improvement stage-by-stage. The highest increase in precision was 16%, and the rest of the indexes also improved, which proves that the features constructed in the three stages of this scheme, from simple to deep, gradually use the BSM content and road information to reveal the changes of traffic flow in the time window, better express the changes of road traffic flow after being affected by the attack in the time window, and have good effects for detecting the attack.

Second, we verified that changes in traffic density do not affect the detection effect. Since the simulation provided by the F2MD framework was derived from real traffic flow data, the three-time periods between 5:00 am and 8:00 am in the morning peak represent different traffic flow densities. Therefore, with the selected DoSRandomSybil attack model, features were extracted from the traffic data of different time intervals, and the training and test sets were divided in a 2:1 ratio. The experimental results proved that this scheme is insensitive to the traffic flow density.

TABLE V
DETECTION RESULTS AT DIFFERENT TRAFFIC DENSITIES

DoSRandomSybil attack prob = 0.1	**5h 6h 9 car/min**	**6h 7h 31 car/min**	**7h 8h 63 car/min**
Accuracy	98.31%	95.68%	95.57%
Precision	96.81%	96.12%	93.56%
Recall	90.10%	84.79%	87.07%

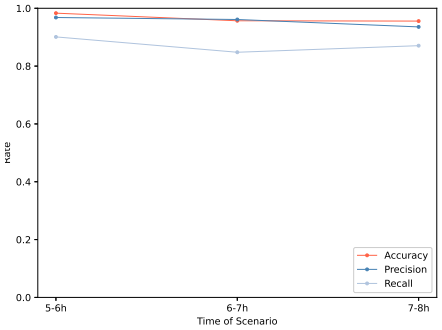

Fig. 10. Detection Results at Different Traffic Densities.

According to the analysis of the results shown in Fig. 10, the classification performance index of this scheme maintains a smooth trend under different traffic flow densities, and the classification accuracy always remains above 95%. The most prominent fluctuation was seen in the recall rate, within 6%, which was mainly because the influence of the derived features on the classification results decreases relatively with the increase in traffic flow density. Simultaneously, because the appearance and departure of vehicles in the scenario are not only from the beginning of the road to enter or the end of the road to leave, there are considerable number of vehicles that appear to be leaving the parking lot into the middle section of the road in the real situation. This actual situation brings data bias to the statistics of the coil data at both ends of the road, which degrades the classification performance; however, the current results are within the acceptable limits.

Finally, we evaluated the impact of the honest majority question on the detection scheme. We aimed to prove that the scheme can effectively face the compound attack containing Sybil and is not affected by the change in attack density and honest majority problem. This experiment was conducted simultaneously for four attack models, and the scenario time period was taken from 7:00-8:00. The attack density was from 5% to 60%, and the experimental results are shown below.

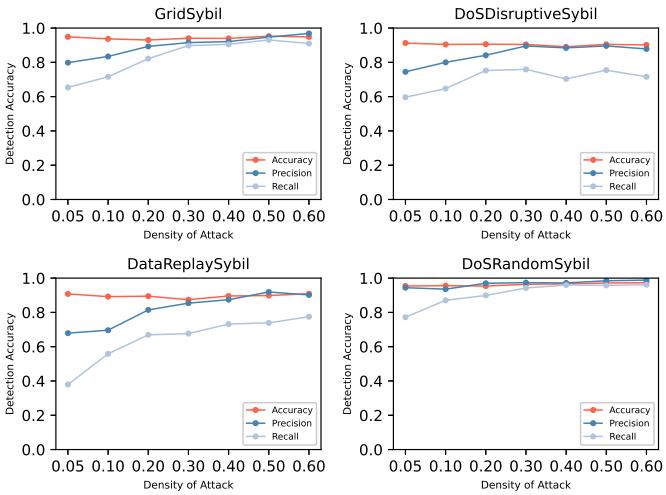

Fig. 11. Experimental Results of Different Attacks.

As shown in Fig. 11, the four attack models were simulated by specifying different attack densities, and based on an analysis of the experimental results, the performance of the classifier improved with the increase in attack density in all four attack types. Based on the lower recall rate in the DataReplaySybil attack model, especially in the case of smaller attack density, the detection effect is not as good as the classification effect of other attack models. This is because the replay attack generally has a clear attack target, and its replay data not only come from the real vehicle nodes that are driving normally, but are also further generated close to realistic driving trajectories through intelligent calculations, which has a very high stealthiness, meanwhile the number of ghost cars generated by DataReplaySybil attack is less than other attack models; therefore, the detection effect is weaker than other three types of attack models.

V. CONCLUSION

Sybil attacks remain a high-risk attack that we will have to face in the future. Due to its highly hidden attack mode, general compliance checks cannot accurately detect its malicious behavior. In this study, based on the original purpose of the attack and the constructed traffic flow characteristics, the attack's impact on a road was reflected so that our detection model can adapt to a variety of compound Sybil attacks with complex traffic scenarios and further add road coil detector data to reduce the impact of traffic density and attacker density on the detection effect by using a multi-source information fusion approach. After summing up we found that in our constructed features, we cannot eliminate the effects of sensor coil errors and vehicles entering midway on the road, which interfere with the feature expression capability, so we will further investigate the methods related to road sensors and introduce multi-source data analysis. According to the future

development of smart transportation, there will be a more significant amount of more credible sensor device data that can be used as the source of multi-source data fusion to further improve the detection performance of Sybil attacks, which will be the next step in our work plan.

REFERENCES

[1] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A Survey," *Computer Networks*, vol. 169, p. 107093, 2020.

[2] A. Dayal, V. K. Shah, B. Choudhury, V. Marojevic, C. Dietrich, and J. H. Reed, "Adaptive Semi-Persistent Scheduling for Enhanced On-road Safety in Decentralized V2X Networks," in *2021 IFIP Networking Conference (IFIP Networking)*, pp. 1–9, 2021.

[3] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-Preserved Pseudonym Scheme for Fog Computing Supported Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2627–2637, 2018.

[4] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "PRIVANET: An Efficient Pseudonym Changing and Management Framework for Vehicular Ad-Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 8, pp. 3209–3218, 2020.

[5] J. Li, Z. Xue, C. Li, and M. Liu, "RTED-SD: A Real-Time Edge Detection Scheme for Sybil DDoS in the Internet of Vehicles," *IEEE Access*, vol. 9, pp. 11296–11305, 2021.

[6] J. Kamel, I. B. Jemaa, A. Kaiser, L. Cantat, and P. Urien, "Misbehavior Detection in C-ITS: A comparative approach of local detection mechanisms," in *2019 IEEE Vehicular Networking Conference (VNC)*, pp. 1–8, 2019.

[7] M. Ranaweera, A. Seneviratne, D. Rey, M. Saberi, and V. V. Dixit, "Anomalous Data Detection in Vehicular Networks Using Traffic Flow Theory," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, pp. 1–5, 2019.

[8] V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, "Multi-Array Relative Positioning for Verifying the Truthfulness of V2X Messages," *IEEE Communications Letters*, vol. 23, no. 10, pp. 1704–1707, 2019.

[9] V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, "Enhancing Misbehavior Detection in 5G Vehicle-to-Vehicle Communications," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9417–9430, 2020.

[10] S. Ercan, M. Ayaida, and N. Messai, "New Features for Position Falsification Detection in VANETs using Machine Learning," in *ICC 2021 - IEEE International Conference on Communications*, pp. 1–6, 2021.

[11] M. Alzahrani, M. Y. Idris, F. A. Ghaleb, and R. Budiarto, "Robust Misbehavior Detection Scheme for Vehicular Network," in *2021 International Conference on Data Science and Its Applications (ICoDSA)*, pp. 54–60, 2021.

[12] V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, "Physical signal-driven fusion for V2X misbehavior detection," in *2019 IEEE Vehicular Networking Conference (VNC)*, pp. 1–4, 2019.

[13] R. Sultana, J. Grover, and M. Tripathi, "A Novel Framework for Misbehavior Detection in SDN-based VANET," in *2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1–6, 2020.

[14] F. A. Ghaleb, M. Aizaini Maarof, A. Zainal, B. A. S. Al-Rimy, F. Saeed, and T. Al-Hadhrami, "Hybrid and Multifaceted Context-Aware Misbehavior Detection Model for Vehicular Ad Hoc Network," *IEEE Access*, vol. 7, pp. 159119–159140, 2019.

[15] S. So, P. Sharma, and 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)*, pp. 564–571, 2018.

[16] X. Liu, L. Yang, I. Alvarez, K. Sivanesan, A. Merwaday, F. Oboril, C. Buerkle, M. Sastry, and L. G. Baltar, "MISO- V: Misbehavior Detection for Collective Perception Services in Vehicular Communications," in *2021 IEEE Intelligent Vehicles Symposium (IV)*, pp. 369–376, 2021.

[17] A. Le and C. Maple, "Shadows Don't Lie: n-Sequence Trajectory Inspection for Misbehaviour Detection and Classification in VANETs," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, pp. 1–6, 2019.

[18] P. Sharma and H. Liu, "A Machine-Learning-Based Data-Centric Misbehavior Detection Model for Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4991–4999, 2021.

[19] F. Hawlader, A. Boualouache, S. Faye, and T. Engel, "Intelligent Misbehavior Detection System for Detecting False Position Attacks in Vehicular Networks," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, 2021.

[20] S. Gyawali and Y. Qian, "Misbehavior Detection using Machine Learning in Vehicular Communication Networks," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2019.

[21] A. Roy and S. K. Madria, "BLAME: A Blockchain-assisted Misbehavior Detection and Event Validation in VANETs," in *2021 22nd IEEE International Conference on Mobile Data Management (MDM)*, pp. 69–78, 2021.

[22] Y. Li, R. Hou, K.-S. Lui, and H. Li, "An MEC-Based DoS Attack Detection Mechanism for C-V2X Networks," in *2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2018.

[23] J. Zacharias and S. Fröschle, "Misbehavior detection system in VANETs using local traffic density," in *2018 IEEE Vehicular Networking Conference (VNC)*, pp. 1–4, 2018.

[24] J. Müller, T. Meuser, R. Steinmetz, and M. Buchholz, "A Trust Management and Misbehaviour Detection Mechanism for Multi-Agent Systems and its Application to Intelligent Transportation Systems," in *2019 IEEE 15th International Conference on Control and Automation (ICCA)*, pp. 325–331, 2019.

[25] S. Gyawali, Y. Qian, and R. Q. Hu, "Machine Learning and Reputation Based Misbehavior Detection in Vehicular Communication Networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8871–8885, 2020.

[26] K. Sharshembiev, S.-M. Yoo, E. Elmahdi, Y.-K. Kim, and G.-H. Jeong, "Fail-Safe Mechanism Using Entropy Based Misbehavior Classification and Detection in Vehicular Ad Hoc Networks," in *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 123–128, 2019.

[27] S. Gyawali, Y. Qian, and R. Q. Hu, "A Privacy-Preserving Misbehavior Detection System in Vehicular Communication Networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 6147–6158, 2021.

[28] A. Uprety, D. B. Rawat, and J. Li, "Privacy Preserving Misbehavior Detection in IoV Using Federated Machine Learning," in *2021 IEEE 18th Annual Consumer Communications Networking Conference (CCNC)*, pp. 1–6, 2021.

[29] J. Kamel, M. Wolf, R. W. van der Hei, A. Kaiser, P. Urien, and F. Kargl, "VeReMi Extension: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2020.