IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 23, 2019, accepted October 25, 2019, date of publication October 31, 2019,
date of current version November 13, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2950805

Hybrid and Multifaceted Context-Aware Misbehavior Detection Model for Vehicular Ad Hoc Network

FUAD A. GHALEB[1,2], MOHD AIZAINI MAAROF[1], ANAZIDA ZAINAL[1], BANDER ALI SALEH AL-RIMY[1], FAISAL SAEED[3], AND TAWFIK AL-HADHRAMI[4]

[1]Cyber Security X Lab, School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, Johor 81310, Malaysia
[2]Department of Computer and Electronic Engineering, Sana'a Community College, Sana'a 5695, Yemen
[3]College of Computer Science and Engineering, University of Taibah, Medina, Saudi Arabia
[4]School of Science and Technology, Nottingham Trent University, Nottingham NG11 8NS, U.K.

Corresponding authors: Fuad A. Ghaleb (fuadeng@gmail.com), Mohd Aizaini Maarof (aizaini@utm.my), and Tawfik Al-Hadhrami (tawfik.al-hadhrami@ntu.ac.uk)

This work was supported by the Ministry of Higher Education (MOHE) and the Research Management Centre (RMC) at the Universiti Teknologi Malaysia (UTM) under Postdoctoral Fellowship Scheme (VOT Q.J130000.21A2.04E00) jointly with Nottingham Trent University, Nottingham, U.K.

ABSTRACT Vehicular Ad Hoc Networks (VANETs) have emerged mainly to improve road safety and traffic efficiency and provide user comfort. The performance of such networks' applications relies on the availability of accurate and recent mobility-information shared among vehicles. This means that misbehaving vehicles that share false mobility information can lead to catastrophic losses of life and property. However, the current solutions proposed to detect misbehaving vehicles are not able to cope with the dynamic vehicular context and the diverse cyber-threats, leading to a decrease in detection accuracy and an increase in false alarms. This paper addresses these issues by proposing a Hybrid and Multifaceted Context-aware Misbehavior Detection model (HCA-MDS), which consists of four phases: data-collection, context-representation, context-reference construction, and misbehavior detection. Data-centric and behavioral-detection-based features are derived to represent the vehicular context. An online and timely updated context-reference model is built using unsupervised nonparametric statistical methods, namely Kalman and Hampel filters, through analyzing the temporal and spatial correlation of the consistency between mobility information to adapt to the highly dynamic vehicular context. Vehicles' behaviors are evaluated locally and autonomously according to the consistency, plausibility, and reliability of their mobility information. The results from extensive simulations show that HCA-MDS outperforms existing solutions in increasing the detection rate by 38% and decreasing the false positive rate by 7%. These results demonstrate the effectiveness and robustness of the proposed HCA-MDS model to strengthen the security of VANET applications and protocols.

INDEX TERMS Hybrid, context-aware, misbehavior detection, vehicular ad hoc network (VANET), false information attacks, Kalman Filter, Hampel Filter.

I. INTRODUCTION

With the advancement in embedded systems and artificial intelligence, vehicle automation has become a reality. Vehicles (which could be cars, airplanes, drones, or any mobile objects) coordinate their movements and perceive the surrounding environment using line-of-sight based sensors such as cameras, acoustic sensors, RFID, GPS, and infrared. Currently, the automotive industry has extended this concept by equipping the vehicles with Wireless Access for Vehicular Environment (WAVE) devices [1], which provide the vehicles with a second source of information. These devices allow vehicles to cooperatively exchange information with each other to expand their perception beyond the line-of-sight-based sensors. Thus, vehicles can be aware of the vehicles and smart objects in their vicinity, reaching to a visibility range of 1km, this has led to the emergence of new networks, so-called Vehicular Ad hoc Networks (VANETs). With VANETs, vehicles can communicate with each other using many forms of communication, such

The associate editor coordinating the review of this manuscript and approving it for publication was Omer Chughtai.

as Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I), (i.e., vehicle to roadside units (RSUs) or vice versa). Accordingly, many innovative applications have been suggested to improve road safety, traffic efficiency, movement coordination of mobile robots, and network agility. An extensive review of such applications can be found in [2], [3]. With VANETs, vehicles have the ability to navigate safely under hazardous driving conditions, such as accident situations, slippery roads, and fog.

The performance of any VANET applications relies on the availability of accurate and reliable context-information shared by neighboring vehicles [4]–[6]. Context-information messages contain information related to vehicles' position, speed, acceleration, orientation, and driving status, among many other features. Vehicles broadcast their context information to warn other vehicles about their existence on the road. Accordingly, the applications use such information to improve road safety, traffic flow efficiency, and network performance. Because context-information messages contain the mobility status of vehicles, the terms context-information, and mobility information are used interchangeably in this paper. The context information is referred to as basic safety messages part 1 (BSM.1 in the IEEE standard [7]) and cooperative awareness messages (CAM in ETSI standard [8]). Both standards assume that vehicles broadcast their information to all vehicles in their vicinity in single-hop communication mode at a high rate. It has also been standardized that a vehicle should broadcast its context information with up to 10 messages per second within a communication range up to 1km. Most VANET applications rely on the integrity of this information; thus, VANET applications present a host of new security challenges.

VANETs are vulnerable to many types of cyber-attacks, which can disrupt any envisioned application and, consequently, may lead to catastrophic losses in lives and assets. Due to the cooperative nature of VANET applications, the integrity of the information shared among vehicles is an important security requirement. Sharing the false information by attackers can lead to catastrophic results. For instance, malware can be used to infect the vehicle's operating system and put the vehicle under the attacker's control. Accordingly, the attacker can exploit the compromised vehicle to manipulate and share false context information with other vehicles. Such attacks (which are referred to as context-related attacks) can create an illusion to trigger vehicles to respond to a non-existing event. Once a vehicle becomes under the attacker's control, it can be used for terrorist acts, assassinations, kidnapping, or redirecting the traffic to cause accidents and congestion. The attacker, for example, can make vehicles deliberately run over a crowd of people. Attackers can also create a ghost (hidden) vehicle that imitates a hard brake. Such misbehavior may force vehicles behind to either brake or change their lanes and, consequently, expose them to a critical situation. The attacker may also redirect the traffic by spreading false congestion messages. The studies that have investigated the influence of misbehavior in VANETs [9]–[11] revealed that the misbehavior could significantly degrade the traffic flow, the performance of the routing protocol, and channel utilization. Many potential attacks and security challenges in VANETs have been discussed in detail in [5], [12], [13]. The false information-related attacks (context-derived attacks) pose high threats, and their detection is challenging and still an open research problem in VANETs [7], [8], [14]. Accordingly, this paper focuses on detecting misbehaving vehicles that share false context information.

Several solutions have been proposed to protect the integrity of the information in VANETs using cryptographic techniques [12], [15], [16]. However, most of these solutions are not able to prevent misbehaving vehicles from manipulating their own context information and spreading it to the network. That is, when a vehicle comes under the attacker's control, the attacker can easily manipulate the context information in the vehicle before applying the cryptography techniques. Consequently, cryptography-based protection becomes ineffective. To overcome such a challenge, it is necessary to locally and autonomously detect the misbehaving vehicles that falsify their own information. Although many solutions have been proposed in the literature to address the misbehavior detection problem of VANETs, most of these solutions are not able to effectively detect false information attacks, rendering VANET applications vulnerable to many kinds of attacks.

Misbehavior detection solutions can be categorized into three approaches: entity-centric, data-centric, and a hybrid approach. In the entity-centric approach, vehicles are evaluated based on their identities or behaviors against predefined rules or protocols in [17], [18]. The entity-centric approach is expensive, designed for long-term detection, and can address only specific types of obvious attacks, such as uncooperative behavior, masquerading, and replay attack [5], [15]. Such solutions are either not suitable or ineffective to locally and autonomously detect misbehaving vehicles that share false context information. Moreover, due to their highly unreliable contexts, vehicles may not be able to behave as expected. Thus, such solutions end up with high false alarm rates. The data-centric approach, on the other hand, focuses on evaluating the vehicles' behavior, based on the consistency and plausibility of their generated information [15], [19]. Although data-centric techniques are promising in effectively determining the correctness of the messages, existing techniques rely on predefined and static context thresholds, which are not suitable for the dynamic and uncertain vehicular context [15], [19]. The use of predefined static context thresholds in dynamic and harsh vehicular environments adversely affects the detection performance in terms of high false alarms and a low detection rate. Furthermore, most of the existing solutions have been evaluated based on simple attack scenarios. More advanced attackers that are aware of the predefined context thresholds can bypass these thresholds and perform successful attacks. Consequently, such solutions are vulnerable to more sophisticated attacks, which

are aware of such shortcomings. In the hybrid approach, vehicles are evaluated based on their behavior, identities, and the consistency and plausibility of their generated information. Because neither a data nor entity-centric approach alone can effectively address the problem of misbehavior in VANETs, combinations of data- and entity-centric techniques have been suggested by many researchers in the literature [6], [15], [19], [20]. However, most of these solutions [6], [15], [19], [20] are only suggested in an abstract form; and no implementation has been conducted. In their study, [6] developed MDS that directly integrates the data-centric, behavioral, and trust techniques to improve the detection accuracy. However, the main drawbacks of this solution lie in overlooking the context dynamicity and the dynamic data uncertainty of the information, as well as lack of proper integration. The integration of none-context aware techniques has led to poor detection performance in VANETs. In addition, the aim of the integration was to cover different types of attacks. However, the study overlooked the sophisticated attacks that share false context information, which is more detrimental than those ordinary, easy-to-detect attacks.

To sum up, existing solutions have been designed based on unrealistic assumptions about vehicular contexts, such as stationary noise and an ideal communication environment, which do not hold for highly dynamic vehicular contexts and a dynamic and heterogeneous noise environment [4], [21]. That is, the accuracy of context information changes based on time and space [22], which in turn, decreases the detection accuracy and increases the rate of false alarms of the misbehavior detection model [23]. The extant misbehavior detection solutions are not able to adapt to the dynamic and harsh environment of VANETs due to the use of static context thresholds in a highly dynamic context. These solutions are vulnerable to sophisticated attacks in which the attackers are aware of the context and the used thresholds. These challenges adversely affect the detection performance of the existing solutions.

To this end, this study aims at addressing these issues by proposing a hybrid context-aware misbehavior detection model (HCA-MDS) to improve the detection accuracy of misbehavior detection. The predefined static consistency, plausibility, and behavioral thresholds were replaced by dynamic context references that are constructed online and updated in a timely fashion. The proposed model utilizes the Kalman filter [4], [21], Box and Whisker plot [24], and Generalized Hampel filter [25] to construct the context references that adapt to the dynamic context. First, the Kalman filter is used in each vehicle to track the consistency of the data received from the vehicles in its vicinity. The Kalman filter algorithm can accurately predict and estimate the correct information, even under a dynamically uncertain and unreliable environment [21]. Representative multifaceted context features were derived from the consistency and plausibility of the context information as well as the behavioral activities of the vehicles. The Box and Whisker Plot method is used to summarize the innovation error of the Kalman filter to reduce the variance resulted from the highly dynamic context. Hampel filter-based algorithms were then proposed to construct multifaceted spatiotemporal context references. To detect the attack progression in its initial stages, the context references are built and updated online in a timely fashion. To cope with attack diversity and improve the detection of sophisticated attacks, multifaceted data-centric and behavioral-based classifiers were then developed using an unsupervised Hampel filter-based outlier-detection method. Each vehicle is classified as misbehaving or benign based on the consistency and plausibility of its information as well as its behavioral activities. Vehicles that deviated significantly from the dynamic context references were considered misbehaving ones. With the proposed HCA-MDS, each vehicle evaluates the vehicles in its communication range in real-time. Thus, misbehaving vehicles can be identified before the attack takes place.

The contribution of this paper is five-fold as follows.

- A context-aware detection model that able to cope with the highly dynamic vehicular context and effectively and autonomously detects the misbehaving vehicles has been developed, as opposed to the existing non-context aware solutions that use predefined static context thresholds.
- A dynamic context references have been constructed online and updated in a timely fashion using Kalman filter, Hampel filter, and Box and Whisker Plot by utilizing the temporal and spatial correlations of the context information, which improves the robustness and reduces the rate of false alarms.
- Representative multifaceted context features were derived from the consistency and plausibility of the context information as well as the behavioral activities of the vehicles.
- A hybrid detection model has been proposed, in which multiple context-aware behavioral and data-centric classifiers were developed utilizing the proposed dynamic context reference and a Hampel-based z-score algorithm to improve the detection accuracy of sophisticated attacks in addition to cover a wide range of attacks.
- An unsupervised outlier-robust, Hampel-filter-based classifiers were developed to evaluate the vehicles based on the consistency and plausibility of their generated data as well as their behavior to avoid the impact of the attackers' data during online context references construction.

The rest of this paper is organized as follows. The related works are reviewed in Section II. The proposed model is elaborated in Section III. Section IV presents the performance evaluation and the experimental setup. Section V illustrates and discusses the results. Section VI discusses the implications of the proposed model. Recommendations for future work and conclusions are presented in Section VII.

II. RELATED WORK

VANET applications rely on the context-information messages that are periodically shared among

vehicles [4]–[6]. As such, the safety, traffic efficiency, and network agility are affected by the correctness of the contents of these messages [5], [12]. As life-saving decisions are made based on the information generated and shared by the communicating vehicles, protecting the integrity of such information is the ultimate goal of any VANET security solutions [9]–[11]. However, a misbehaving vehicle that manipulates its own information and shares it with neighboring vehicles can disrupt any potential application in VANETs [5], [12], [13]. An attacker (context-derived attacker) can sneak into the vehicle's systems and force the vehicle to share false information with a valid cryptographic certificate. Therefore, detecting such misbehaving vehicles, locally and autonomously, is crucial for VANET security. Many solutions have been proposed for detecting false information attacks (context-related attacks) and identifying misbehaving vehicles [26]–[32]. As mentioned above, these solutions can be categorized into three approaches, namely, entity-centric [18], [33]–[35], data-centric [5], [6], [26]–[31], [36]–[50], and hybrid [6], [51], [52].

A. ENTITY-CENTRIC APPROACH

The entity-centric approach evaluates the vehicles either based on trust, which is related to their identities, or their behavioral activities [12], [15]. Thus, this approach can be further categorized into two sub-approaches, the behavioral-based approach, and the trust-based approach. In the behavioral-based approach [18], [33]–[35], vehicles are evaluated based on their behavior against VANET protocols, while, in the trust-based approach [32], [53], [54], vehicles are evaluated according to a predefined trust value assigned to each vehicle by an authority, for example, police and emergency vehicles can have higher trust value than others vehicles.

1) BEHAVIORAL-BASED TECHNIQUES

The behavioral-based approach has been investigated in intrusion detection and misbehavior detection in MANET and WSN networks and many solutions have been proposed, such as Watchdog and Pathrater [55], CORE [56], and CONFIDANT [57]. Several models have been suggested to encourage cooperation among vehicles in VANETs. The watchdog mechanism was adopted to detect forwarding misbehavior [18], [33]–[35]. However, these solutions are insufficient to detect misbehaving vehicles that share false information Ghosh *et al.* [58] proposed a misbehavior detection approach based on analyzing vehicles' mobility behavior after sending the safety messages, to detect any potential misbehavior. Although this solution is suitable for detecting specific types of false event messages such as false crash-notification messages or false braking notification messages, it cannot detect non-event type messages, such as false context information messages. In general, the behavioral approach alone is not suitable for detecting misbehaving vehicles that send false information because it focuses on monitoring the behavior of the nodes against a known protocol or service. Nevertheless, vehicles may follow the protocol rules but send a false message payload. In addition, due to traffic density and vehicles' mobility, vehicles may not behave as expected, and the behavior can be wrongly classified. Given that existing behavioural techniques are unaware of the context, high false alarm and low detection rates are common for context-related attacks.

2) TRUST-BASED TECHNIQUES

The trust-based approach [32], [53], [54] evaluates the vehicles either based on their previous interaction, i.e., vehicles that have misbehaved in the past are likely to misbehave in the future, or based on predefined trust values linked to their identities, such as police vehicles. Unfortunately, trust values describe only the previous behavior but not the current trust state. In addition, trust establishment needs a long time to form or update the vehicle's trust values. Moreover, the trust approach is vulnerable to the zero-day attacks that take place when a trusted vehicle turns to become a misbehaving one due to malware infection. Furthermore, trust-based solutions in ad hoc and dynamic networks such as VANETs are complex, expensive, and ineffective for short term detection such as local detection [5], [31], [32].

B. DATA-CENTRIC APPROACH

The data-centric approach focuses on detecting misbehaving vehicles by analyzing the plausibility and the consistency of their generated data [6], [26], [27], [31], [37], [39], [40], [42]–[48], [59]. The data-centric approach is suitable for locally and autonomously detecting misbehaving vehicles that share false information [5], [6],[50]. This approach can be further categorized into two subcategories: the event-based approach and the context-based approach.

1) EVENT-BASED APPROACH

The event-based approach [27], [29], [31], [36], [58] focuses on detecting misbehaving vehicles that send false event messages such as false crash notification, false road hazard notifications, or false congestion warnings. Many event-based misbehavior detection solutions have been proposed. However, event-based detection solutions are too application-specific [36]. That is, a misbehavior detection system for each application must be designed. In addition, attackers that manipulate the context can send plausible and consistent messages that will deceive any potential applications. Given that many applications have not yet matured enough, designing an event-based detection system is still in its early stages. Event-based approaches can detect the attack once it develops into a time-critical event.

2) CONTEXT-BASED APPROACH

A more general approach for locally and autonomously detecting misbehaving vehicles is to analyze the context of information messages [6], [37]–[49]. Such an approach can detect the attackers in their early stages, i.e., before the attack develops to advanced stages and inflicts damage.

Two main techniques have been used for the evaluation stage: the message plausibility check and the message consistency check. The message plausibility check technique uses the known implausible facts for detecting false mobility messages. Mobility data plausibility check techniques have been employed by many researchers [6], [37], [39], [41]–[49] to build plausibility-based detection systems that can detect implausible information in a particular known data model of the real world [6], [15]. Examples of implausible contents include a speed of 700km/h, two vehicles occupying one position at the same time, a vehicle that exists in multiple positions at the same time, and transferring information beyond the communication capabilities. Such content is an obvious indication of incorrect messages. Message plausibility validation needs a set of pre-defined rules or protocol specifications that describe the physically impossible content. The plausibility model can vary from narrowly defined rules, such as violating laws of physics (e.g., violating maximum distance movement), up to rules that allow a high range of variation, such as those affected by the accuracy of context information. Some plausibility rules include determining the minimum and maximum boundaries of messages' delay tolerance, velocity, positioning error, and broadcasting frequency. For example, a context-information message becomes obsolete 100ms after creation. As they are broadcasted within 100ms in a single-hop communication mode, these messages cannot tolerate delays longer than this time period. Accordingly, receiving a message with a delay longer than 100ms is a sign of misbehavior, as it should be dropped by the source before broadcasting. Similarly, receiving a message with a speed of 700km per hour is implausible using existing vehicles' technologies. A major advantage of plausibility-based detection is that the message plausibility verification is simple, which makes it efficient for real-time applications. Although plausibility-based detection is robust against colluding attacks as it does not rely on assumptions such as honest majority, it relies on unrealistic assumptions about the availability of accurate mobility information all the time. That is, due to dynamic and heterogeneous noise in the vehicular environment, the uncertainty of the mobility information is high and dynamic. Therefore, the predefined static plausibility thresholds increase false alarms and decrease the detection rate of misbehavior detection solutions.

The consistency checks of the context information have been used in several studies [27], [41], [45], [49], [44], [60]–[63]. Data consistency techniques study the relationship between messages received from independent sources to detect any inconsistencies [27], [49]. Unlike message plausibility, data consistency correlates messages that have originated from different sources, been sent at different time epochs, or been received from different senders. Consistency-based detection does not require a pre-defined data-model or known rule to perform detection. Most of these approaches do not consider the dynamic uncertainty of the mobility information and the unreliability of the information. Furthermore, these approaches assume that mobility information is accurate, and the communication channel is ideal. However, in VANETs, mobility information is acquired from a harsh and dynamic heterogeneous noise environment and broadcasted in an unreliable communication channel. In such environments, mobility information has dynamic uncertainty and incompleteness, and overlooking such issues leads to low detection rates and high false alarms when identifying the misbehaving vehicles. A consistency reference model which is built using unsupervised methods can help to overcome these challenges. There are several unsupervised approaches that can be used to construct the consistency reference model, including mathematical [6], probabilistic [45], [64], machine learning [65], and statistical approach [26], [31].

Several consistency models have used Kalman filter-based algorithms to construct the consistency model. The Kalman filter infers the parameters of interest from indirect, inaccurate, uncertain, and independent sources. The innovation errors of the Kalman filter are used as an inconsistency indicator. The vehicle that fails to be consistent with its previous mobility information is considered as a misbehaving vehicle [41], [45], [44], [63]. However, the main limitation of existing solutions that rely on Kalman filters is the use of a predefined static noise covariance matrix to represent the heterogeneous and dynamic noises surrounding the vehicular sensors such as GPS sensors [4], [45]. In such a case, the Kalman filter produces inaccurate estimations. Consequently, these solutions fail to differentiate between false and true information. Adaptive Kalman filter algorithms can be used to acquire, share, and track the mobility information of neighboring vehicles. A detailed description of such algorithms can be found in [4], [21]. To the extent of differentiating between false and true information, a temporal summary of innovation errors of each neighboring vehicle is constructed and compared with a spatial summary built from the innovation errors of all the neighboring vehicles together. If a vehicle deviates much from the spatial summary, it is considered as a misbehaving vehicle.

C. HYBRID APPROACHES

Many researchers suggest integrating the data-centric and entity-centric features to address a wide range of misbehaviors. Bissmeyer *et al.* [6] proposed a context-based trust model that integrates the consistency and plausibility features with some behavioral features. Vehicles with higher trust values are considered genuine, while vehicles with low trust values are considered misbehaving ones. The main advantage of such a solution is that the trust value can be constructed online so that the misbehaving vehicle can be identified locally and autonomously. However, there are two main limitations of such a solution, as follows. This solution overlooks the vehicular dynamic and noisy vehicular context, which renders finding a suitable trust threshold that can adapt to the dynamic vehicular context difficult. In addition, this solution is vulnerable to illusion attacks and context-derived attacks, in which attackers can create false traffic and mobility patterns that have high similarity with the real traffic patterns

Grover *et al.* [52] trained a misbehavior detection model using the random forest algorithm. Raw data-centric and behavioral attributes were used to train the model. The main disadvantage of this model is that it is too scenario specific. That is, if the road, vehicle density, and driver behavior change, the performance of the model will degrade. In our previous work [51], data-centric, behavioral features, and context-based features were used to train a detection model using an artificial neural network algorithm. Although the model can effectively predict many types of attack, the model is ineffective to detect a novel attack.

To sum up, misbehaving in terms of manipulating mobility information can adversely affect both traffic efficiency and road safety, leading to catastrophic loss of lives and/or assets. Detecting the misbehaving vehicles locally and autonomously is challenging in VANETs, due to the harsh environment and the unreliable dynamic context. A vehicle may unintentionally send inaccurate information due to the heterogeneous noise environment or faulty sensors. In addition, due to the high levels of congestion and high mobility of vehicles, a considerable amount of context messages are lost, causing incomplete information. As mentioned earlier, several researchers have proposed detection models based on either entity-centric [18], [33]–[35], data-centric approaches [6], [15], [37]–[48] or hybrid approaches [6], [51], [52] to detect false information and identify misbehaving vehicles. However, the entity-centric approach is insufficient to locally and instantaneously detect misbehaving vehicles that spread false mobility information. On the other hand, some data-centric approaches are event-based [27], [29], [31], [36], [58] which are application- and attack-specific, and cannot detect the misbehavior in its initial stage; hence, they are ineffective for VANET critical applications and protocols such as safety, traffic applications and routing protocols. Although the context-based approach is more effective than the event-based approach, overlooking the dynamic context together with the presence of heterogeneous noises, and the unreliable communication renders such an approach ineffective. The hybrid approach proposed by Bissmeyer *et al.* [6] combines the capabilities of the entity-centric and data-centric approaches into one model. However, this solution overlooks the vehicular dynamic and noisy context, which makes it difficult to determine a suitable trust threshold that adapts to the vehicular context. This solution is also vulnerable to illusion attacks and context-derived attacks, in which an attacker can share false traffic and mobility patterns. As a result, such a solution suffers from low detection accuracy and/or a high rate of false alarms. The hybrid approach is more promising to effectively detect many types of illusion and context derived attacks because it combines many detection concepts in a single model. However, the extant hybrid solutions suffer in many ways. The use of predefined and static security thresholds in both the data-centric and entity-centric techniques is the major drawback of those solutions. The highly dynamic context has been vastly neglected. To this end, in this study, a hybrid model that combines multiple context-aware classifiers has been designed and developed to identify the misbehaving vehicle locally and autonomously by analyzing the mobility information and vehicle behavior. As opposed to the predefined static thresholds used by Bissmeyer *et al.* [6], the proposed solution in this study uses a multifaceted and adaptive context-reference model that is built online and updated in a timely fashion by analyzing the spatial and temporal correlation of the mobility information to reduce the false alarms and increase the detection rate. Table 1 shows the shortcomings of and the challenges faced by the extant solutions, as well as the proposed solution to address such issues. Table 1 shows the shortcomings and challenges of the existing solutions and how the proposed solution has addressed such problems.

III. THE PROPOSED MISBEHVIOUR DETECTION MODEL

The proposed misbehavior detection model is host-based; i.e., it is deployed for each vehicle to detect local misbehavior early in its initial stages before it develops into a sophisticated attack. Due to the absence of labeled attack data, the proposed solution uses an unsupervised statistical method to detect unknown attacks. This method is based on the mobility information, which is the main building block of many critical VANET applications. In addition, such mobility information is the target for many types of difficult-to-detect attacks that can easily disrupt VANET applications and services. The proposed model is composed of a set of multifaceted base classifiers to consolidate the diversity of the ensemble, which in turn, improves the capability of the model to detect many types of misbehaviors that can tamper with VANET data. Furthermore, the model is context-aware, in which the context-based features are used to train the base classifiers. Therefore, the model is able to adapt to any changes in the context.

Toward building the detection classifiers, adaptive context reference was firstly constructed using Kalman Filter, Box-Plot, and Hampel Filter so that the deviation from these boundaries is considered misbehaving. As shown in Fig. 1, the proposed misbehavior detection model consists of four main phases: Mobility Data Collection Phase, Context Representation Phase, Context Reference Construction Phase, and Misbehavior Detection Phase.

A. DATA COLLECTION PHASE

As shown in Fig. 1, this phase consists of three sub-phases: Mobility Data Acquisition, Mobility Data Broadcasting, and Mobility Data Preparation. Each vehicle is responsible for acquiring and sharing its own mobility information with the neighboring vehicles. The vehicle is also responsible for predicting the missing mobility information of the vehicles in its vicinity.

1) MOBILITY DATA ACQUISITION

Each vehicle acquires the mobility information from different sensors, such as the positioning sensor, speedometer sensor, accelerometer sensor, and gyro sensor. Because the

TABLE 1. Comparison between the misbehavior detection solutions and the proposed solution.

Solutions	Techniques	Shortcomings	Challenges	Proposed Solution
Entity-Centric [18, 33-35]	Behavioral-based [18, 33-35]	• Low detection rate because behavioral features are ineffective to identify false information related attacks • High false alarms because in the extant behavioral techniques are too sensitive to the communication status	• Vehicles' high mobility and traffic density make communication channels unreliable. Thus, it is difficult to pre-define any expected behavior.	• A dynamic behavioral-based reference for the expected behavior was constructed from the spatial and temporal correlation of vehicles' behaviors in the vicinity using the Hampel filter-based method. • The behavioral reference is constructed online and updated in a timely fashion using unsupervised learning approach • Thus a context-aware behavioral classifier has been developed in the proposed model.
	Trust-based [32, 53, 54]	• Vulnerable to novel attacks • Expensive for distributed and sparse networks	• It is difficult to establish long-term trust system in ad hoc networks as well as define suitable trust value short-term in a highly dynamic environment is challenging	• Trust-based techniques have not been included in the proposed model.
Data-Centric (Event-Based) [27, 29, 31, 36, 58]	Consistency and plausibility [27, 29, 31, 36, 58]	• Application- or attack-specific • Detection is triggered in the last stages of attacks	• Most of VANET applications not yet fully standardized. Thus, any proposed solution will be subject to revision after the standardization or after each new emerging application.	• The study has focused on the context-related attacks because these are a pre-stage of any event-based attacks. Furthermore, it is common to believe that manipulating context-information is the initial step of any type of attack in VANETs.
Data-Centric(Context-Based) [6, 37-49]	Consistency -based [6, 37-49]	• High false alarms rate or/and low detection rate in the extant consistency-based techniques, due to the use of predefined and static consistency thresholds • Vulnerable to context-aware attackers	• Heterogeneous and dynamic noises, dynamic communication status and deriver behavior makes context information has dynamic uncertainty	• A dynamic data-centric context-reference that represents data-consistency has been constructed using Kalman Filter, Box-Plot, and Hampel filter utilizing the spatial and temporal correlation among context-information received from neighboring vehicles. Three context factors were considered: drivers' behavior, environmental noises, and communication unreliability. • The consistency-based classifier was developed using Hampel based filter utilizing the consistency reference
	Plausibility based [6, 37-49]	• Low detection rate or/and high false alarms rate due to the use of predefined and static plausibility thresholds. • Vulnerable to context-aware attackers	• Dynamic uncertainty due to the harsh and unreliable dynamic context.	• A dynamic data-centric context-reference that represents data-plausibility has been constructed using the Hampel filter, utilizing the spatiotemporal correlation among three context factors that were considered drivers' behavior, environmental noises, and communication unreliability. • Several plausibility-based classifiers were developed using a Hampel-based filter utilizing the constructed consistency reference and the plausibility reference.
Hybrid [6, 51, 52]	Data-Centric + Entity-Centric [6, 51, 52]	• Low detection rate or/and high-false alarms rate due to the use of predefined and static consistency and plausibility thresholds.	• Vehicles' high mobility and traffic density make communication channel unreliable. Thus, it is difficult to pre-define any expected behavior • Heterogeneous and dynamic noises, dynamic communication status and deriver behavior gives context information dynamic uncertainty	• A new context-aware hybrid model was designed and developed by combining the proposed context-aware behavioral and data-centric classifiers to improve the detection of performance under dynamic vehicular context. • A dynamic, multifaceted hybrid context reference model is used to evaluate the vehicles so as to improve both accuracy and adaptability to VANET dynamic context.

positioning sensor is susceptible to a dynamic and heterogeneous noise environment, the positioning information, which is an important element in the mobility messages, has dynamic uncertainty. Therefore, an improved adaptive Kalman Filter algorithm, which was proposed in [4] (also called the Enhanced Innovation Adaptive estimation Kalman Filter EIAEKF), has been used to acquire the mobility information and estimate the measurements of noise covariance and instantaneously update the Kalman filter algorithm. The main advantage of EIAEKF is its robustness to the dynamic and heterogeneous noise environment and its ability to effectively estimate the uncertainty of the mobility information.

2) MOBILITY DATA BROADCASTING

Due to the high mobility of vehicles, mobility data becomes outdated quickly [66]. Thus, vehicles need to broadcast their mobility information at high rates (10 messages per second, according to the VANET standards) [67]. The high

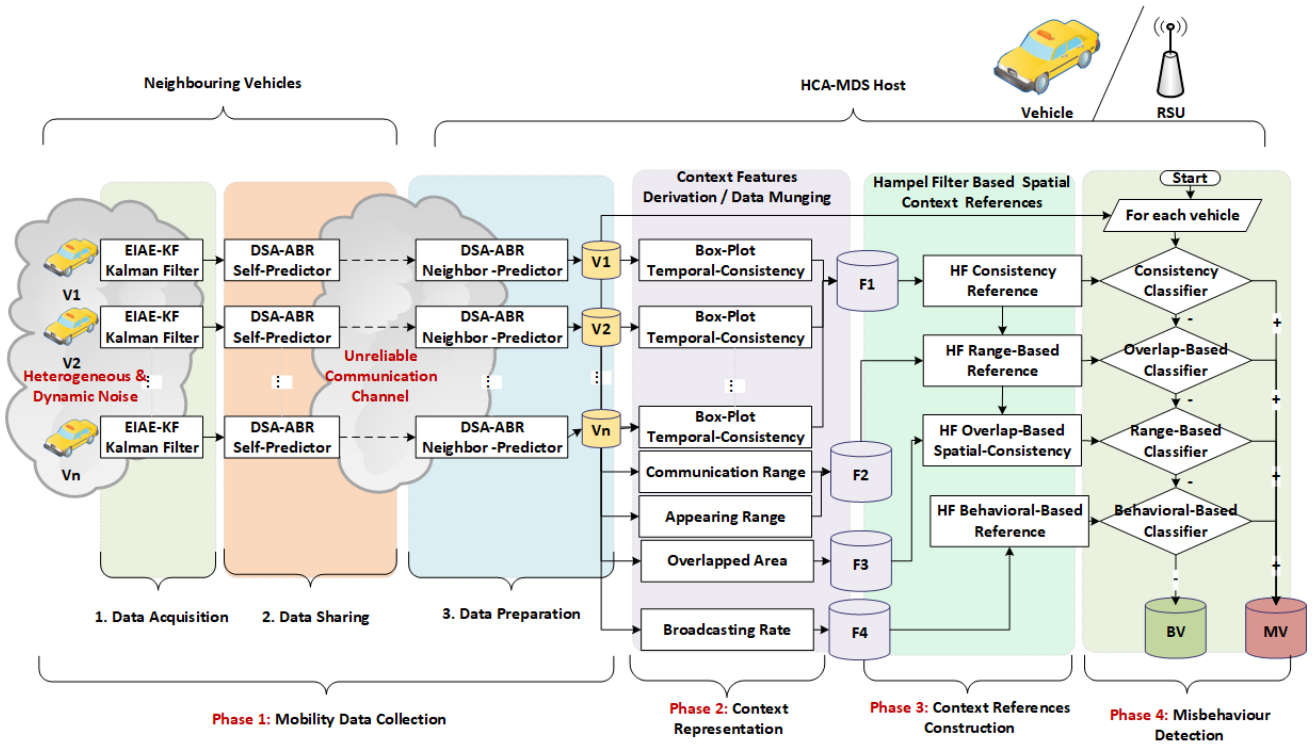

FIGURE 1. The proposed misbehavior detection model (HCA-MDS).

broadcasting rates, in addition to the vehicles' density and the harsh environment, render the communication channel unreliable and thus lead to the loss of a considerable amount of mobility information. In the direction of addressing this issue, many broadcasting schemes have been suggested for VANETs to adjust the broadcasting rate according to vehicle density [68], traffic flow [69], channel characteristics [70], and/or driving status [21]. The adaptation based on driving status is more reliable, as the number of vehicles that need to access the communication channel is low [67]. Therefore, the vehicles that are in a critical situation can broadcast their mobility information and predict the omitted (un-broadcasted) messages, assuming a linear mobility process. For the purpose of this research, the driving-situation aware adaptive broadcasting scheme (DSA-ABR) proposed in [21], is adopted to broadcast the mobility information. DSA-ABR has two main components: the self-predictor algorithm and neighbor predictor algorithm. The self-predictor algorithm is responsible for adapting the broadcasting rate according to the driver situation. As the self-predictor algorithm takes the uncertainty of the information into consideration when broadcasting the message, the broadcasting rate is reduced significantly. Moreover, the self-predictor allows vehicles to share the parameters of their mobility models as well as the uncertainty of the information, which enhances the prediction accuracy of the lost and/or omitted information in the neighboring vehicles. The neighbor predictor algorithm, on the other hand, is used to collect mobility messages broadcast by the neighboring vehicles.

3) MOBILITY DATA PREPARATION

The neighbor predictor algorithm of the DSA-ABR is responsible for collecting the mobility messages broadcast by neighboring vehicles, as well as predicting the lost and/or the omitted mobility messages. It uses a modified version of the Kalman Filter, in which the parameters of the self-predictor algorithm of the neighboring vehicles are shared along with the mobility information to improve the prediction accuracy [21]. The output of this phase is a dataset for each neighboring vehicle. Each dataset contains a history of vehicles' mobility information at each 100ms.

B. CONTEXT REPRESENTATION PHASE

In this phase, the features that represent the context are derived. Three context factors were considered for the construction of the context references: the driver's behavior, environmental noises, and communication status. These three factors have a direct impact on the data-consistency, plausibility, and vehicles' behavior, raising the need for context-aware systems. Due to drivers' maneuvering behavior, vehicles may drive in and out of communication ranges of each other, causing intermittent communication and loss of context information. Similarly, due to high vehicle mobility and variable traffic density, communication channels become congested, causing intermittent communication and loss of context information and thus an incomplete context. This issue has been partially addressed during the data collection stage, where the lost messages are predicted using our previously

published Kalman filter-based algorithm, i.e., DSA-ABR [21]. The impact of communication loss will appear as prediction errors due to the uncertainty of the prediction model. This uncertainty may be increased due to the environmental noises surrounding the vehicles' sensors. The unreliable communication, driver maneuvering behavior, and environmental noises cause contradictions between the output of the mobility model (Kalman prediction phase) and the measurement errors. This contradiction appears in the form of a Kalman innovation error. Therefore, the innovation errors of the Kalman filter were used as the main context features that represent the dynamic vehicular context.

As shown in Fig. 1, there are four main derived features that represent the context and which are used to evaluate the vehicles based on their data-consistency, data-plausibility, and behavior against network protocols. They are then used to construct the context references of the neighboring vehicles using spatial and temporal analysis of the consistency among neighboring vehicles' context information. The first set of features determines the Consistency Score (CS) of each vehicle, which is used to evaluate the vehicles' data-consistency using the Kalman filter-based algorithm (see Algorithm 1, Lines 4-7), and is referred to as F1 in this paper. The second set of features determines the Range-based plausibility Score (RS), which is used to evaluate the plausibility of the vehicles' data in terms of the reported communication range and is referred to as F2. The third set of features determines the Overlapping-based plausibility Score (OS), which is used to evaluate vehicles' data- plausibility in terms of reported overlapped occupation area and is referred to as F3. The fourth feature determines the Behavioral Score (BS), which is used to evaluate the vehicles' broadcasting behavior and is referred to as F4.

Algorithm 1 shows the pseudocode for extracting context features (F1-F4) utilizing the Kalman filter for consistency features derivation and Box-Plot for generating the temporal summary. Table 2 explains the symbols used, followed by a detailed description of each set. The detailed description of this algorithm is presented in the following subsections.

TABLE 2. Description of symbols.

Symbol	Description
$y_k^{NV(i)}$	Received mobility data at time epoch k from vehicle $NV(i)$
F	Kalman Filter Transition Matrix refer to [21] for calculation
$\check{y}_{k\|k-\tau(i)}^{NP(i)}$	Predicted mobility data at time epoch k from vehicle $NV(i)$
$e_k^{NV(i)}$	Innovation error of neighboring vehicle $NV(i)$ at time epoch (k)
$K_k^{NV(i)}$	Kalman-Gain refer to [21] for calculation
$\check{y}_k^{NP(i)}$	Estimated mobility data at time epoch k from vehicle NV(i)
$\tau(i)$	The time epoch of last received mobility data
$UL_{k(i)}$	Box-Plot Upper limit
$p(x,y)$	Position of the host
$p_i(x_i,y_i)$	Position of neighboring vehicles ($NV(i)$)
$ol_k^{NV(i,j)}$	The overlapping status between the vehicle (i) and vehicle (j) at time epoch (k)
$TW_k^{NV(i)}$	Time window calculated separately for each vehicle $NV(i)$
$os_k^{NV(i)}$	Overlapping status of the vehicle (i) at time epoch (k)

Algorithm 1 Data Preparation and Features Derivation Algorithm

1: *FOR* each time epoch k ***DO***
2: *FOR* each message $y_k^{NV(i)}$ received from neighboring vehicles $NV(i)$***DO***
3: *IF* the message $y_k^{NV(i)}$ belongs to exisiting vehicle ***THEN***
4: *Predict* *the state* $\check{y}_{k|k-\tau(i)}^{NP(i)} = F * y_{k-\tau(i)}^{NV(i)}$
5: *Calculate* *the Kalman filter innovation error* $e_k^{NV(i)}$

$$e_k^{NV(i)} = \begin{cases} y_k^{NV(i)} - \check{y}_{k|k-\tau(i)}^{NP(i)} & \text{if a message is recieved} \\ e_{k-\tau(i)}^{NV(i)} * (k - \tau\,(i)) & \text{Otherwise} \end{cases}$$

6: *Calculate* *Kalman-Gain* $K_k^{NV(i)}$
7: *Estimate* *the actual state* $\check{y}_k^{NP(i)} = \check{y}_{k|k-\tau(i)}^{NP(i)} + K_k^{NV(i)} * e_k^{NV(i)}$
8: *Use* Box-Plot to summarize the $e_k^{NV(i)}$
9: *Derive* the consistency features ($F1$)

$$F1 = CS \rightarrow cs_k^{NV(i)} = \max(UL_{k(i)}, e_k^{NV(i)})$$

10: *ELSE* (the message $y_k^{NV(i)}$ belongs to new vehicle)
11: *Store* the new vehicle's information in a tracking table
12: *Set* the consistency features ($F1$) to zero
13: *ENDIF* and continue
14: *Derive* *the communication range based plusablity feature(F2)*

$$F2 = RS \rightarrow rs_{k=0}^{NV(i)} = \|p(x,y) - p_i\,(x_i, y_i)\|$$

15: *Derive* the overlap based plausibility features ($F3$)

$$F3 = OS \rightarrow os_k^{NV(i)} = \sum_{k=0}^{TW} ol_k^{NV(i,j)}, \forall j \in NV(i, TW)$$

16: *Drive* the behavioral features *(F4)*

$$F4 = BS \rightarrow bs_k^{NV(i)} = \frac{Total\ ReceivedMessages\ from\ Vehicle\ (i)}{Connection\ Time}$$

17: END FOR LOOP
18: END FOR LOOP

1) F1: CONSISTENCY SCORE (CS)

Each vehicle collects the mobility information from neighboring vehicles to evaluate data consistency and represents the context reference in terms of context data consistency. Due to the intermittent communications and harsh VANET environment, mobility data is inaccurate and unreliable. To this end, the Kalman filter-based broadcasting scheme, namely the DSA-ABR scheme [21], was used to broadcast the context data, infer more accurate data, predict the missing data, and track the consistency of the mobility data received from neighboring vehicles. As shown in Algorithm 1, Lines 4-7, the Kalman filter is used to predict and then estimate the mobility information received from neighboring vehicles. Because the innovation sequence of

the Kalman Filter can describe the discrepancy between the expected (the predicted mobility information) and reported (the actual) mobility information by the vehicles, it has been used to represent the consistency of the information. That is, the Kalman filter innovation sequence of each vehicle has been used to represent the temporal consistency of the mobility information of each vehicle. Because vehicular context is highly dynamic, the variances of the innovation sequences of the vehicles are high. Therefore, the innovation sequence of each vehicle is summarized using the Box and Whisker Plot method to reduce the variance among the innovation sequences of the neighboring vehicles. Hence, there are two main steps to derive the Consistency Score (CS) feature. The innovation sequence is firstly represented by a series of innovation error vectors recorded in each time epoch for each neighboring vehicle $(i)E^{NV(i)} = \{\ldots e_{k-1}^{NV(i)}, e_k^{NV(i)}, e_{k+1}^{NV(i)}, \ldots\}$. As shown in Algorithm 1, Line 5, the innovation error of a neighboring vehicle $NV(i)$ at specific time epoch k is then calculated according to the following equation.

$$e_k^{NV(i)} = \begin{cases} y_k^{NV(i)} - \check{y}_{k|k-\tau(i)}^{NP(i)} & \textit{if a message is recieved} \\ e_{k-\tau(i)}^{NV(i)} * (k - \tau\,(i)) & \textit{Otherwise} \end{cases} \tag{1}$$

where $e_k^{NV(i)}$ is the vector of the innovation error of the neighboring vehicle $NV(i)$ at the time epoch k, $y_k^{NV(i)}$ is the mobility information vector as received from the neighboring vehicle $NV(i)$ at the time epoch k, $\check{y}_{k|k-\tau(i)}^{NV(i)}$ is the predicted mobility information vector using the last received messages (at the time epoch $\tau(i)$) and Kalman Filter prediction, and $\tau(i)$ is the time epoch when the last message was received. More details about the computation of Kalman filter innovation error is described in [21].

Secondly, each vehicle generates a temporal summary $TS_k^{NV(i)}$ for each vehicle in its vicinity using the Box and Whisker Plot method (see the pseudocode in Algorithm 3, Line 4). The Box and Whisker Plot method has been used to reduce the false alarms that may arise due to the usage of the innovation error sequence of Kalman filter. This sequence is a random variable with highly dynamic statistical parameters due to the harsh and heterogeneous dynamic noise environment in VANETs. Thus, the consistency score (CS) has been used to represent vehicles' data consistency. Accordingly, the consistency score of a vehicle (i) at time epoch (k) can be calculated as follows.

$$F1 = CS \rightarrow cs_k^{NV(i)} = \max(UL_{k(i)}, e_k^{NV(i)}) \tag{2}$$

where $UL_{k(i)}$ denotes the upper limits of Box and Whisker Plot and $e_k^{NV(i)}$ denotes the innovation error of Kalman filter (see the pseudocode in Algorithm 1, Lines 5 and 9, and Algorithm 2, Lines 4 and 8).

2) F2: RANGE-BASED PLAUSUIBILITY SCORE (RS)

This feature is derived based on the fact that vehicles can communicate only within their communication range. Due to the uncertainty of the mobility information, the communication range can vary according to the context (see Fig. 2). Therefore, the communication range at which new vehicles communicate is selected as a range-based plausibility feature (RS). Thus, the range-based score of a vehicle (i) at time epoch (k) can be calculated as follows.

$$F2 = RS \rightarrow rs_{k=0}^{NV(i)} = \|p(x, y) - p_i\,(x_i, y_i)\| \tag{3}$$

where $p(x, y)$, $p_i\,(x_i, y_i)$ are the position vectors of a subject vehicle and its neighboring vehicle (i), respectively, and $rs_{k=0}^{NV(i)}$ is the Euclidian distance between those two vehicles (see the pseudocode in Algorithm 1, Line 14).

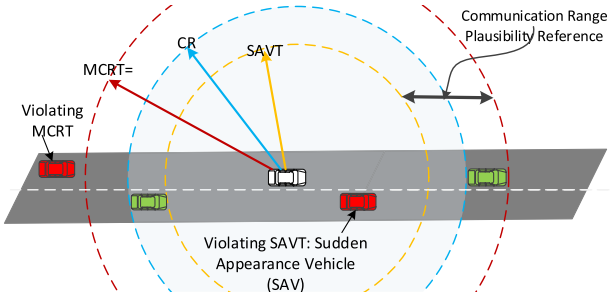

FIGURE 2. Communication range-based context reference.

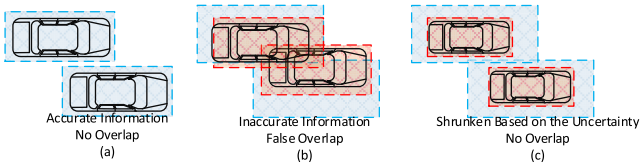

FIGURE 3. Overlap-based context-reference.

3) F3: OVERLAP-BASED PLAUSIBILITY SCORE (OS)

This feature is derived based on the fact that two vehicles cannot occupy the same area at the same time. Because the context is highly dynamic, vehicles may appear to overlap due to the dynamic uncertainty of the mobility information (see Fig. 3 (a) and (b)). Thus, the overlap score $os_k^{NV(i)}$ of a vehicle (i) is the count of how often the vehicle (i) overlapped with any neighboring vehicle NV (j) in its vicinity within a time window (TW), starting after vehicles change their pseudonym identifications. The overlapping-based plausibility score is calculated as follows.

$$F3 = OS \rightarrow os_k^{NV(i)} = \sum_{k=0}^{TW} ol_k^{NV(i,j)}, \quad \forall j \in NV(i, TW) \tag{4}$$

where $ol_k^{NV(i,j)}$ is a binary variable whose value depends on the presence or absence of overlapping between the vehicles (i) and (j) at each time epoch (k) (see the pseudocode in Algorithm 1, Line 15).

4) F4: BROADCASTING-BASED BEHAVIOURAL SCORE (BS)

Because neighboring vehicles are exposed to similar traffic conditions, environmental noises, and communication status,

their broadcasting behaviors are quite similar. Thus, spatial correlation among the broadcasting behavior of neighboring vehicles' drivers can be utilized to construct a behavioral reference such that vehicles that deviate much from this reference are considered misbehaving vehicles. Accordingly, F4 can be calculated as follows.

$$F4 = BS \rightarrow bs_k^{NV(i)} = \frac{Total\ Received\ Messages\ from\ Vehicle\ (i)}{Connection\ Time} \quad (5)$$

where $bs_k^{NV(i)}$ is the behavioral score of the neighboring vehicle (i) at time epoch (k) (see Algorithm 1, Line 16)

C. CONTEXT REFERENCES CONSTRUCTION PHASE

Four context references have been constructed (see Fig. 1). These references can be grouped into two types: data-centric and behavioral-based references (multifaceted context reference). The data-centric based references represent the consistency and plausibility of the mobility information, which includes Consistency-Based Reference, Communication Range-Based Plausibility Reference, and Overlapping-Based Plausibility Reference. On the other hand, the Behavioral-Based Reference represents the broadcasting behavior or cooperativeness of the vehicle. These references are used to represent the context from a different perspective (multi-faceted). The spatial correlation among neighboring vehicles has been utilized to construct their context references. The Hampel Filter Algorithm has been applied for each reference as follows. Let x be a feature under consideration, e.g., the Vehicle Data-Consistency feature, which is denoted by $F1$ in Fig. 1 and Algorithm 1. The Hampel filter-based context reference CR_k at time epoch (k) can be computed as follows.

$$CR_k = \begin{cases} \emptyset_k = median\,(x) \\ \delta_k = 1.4826 \times median\,\{|x - \emptyset_k|\} \\ HUB_k = \emptyset_k + \beta \times \delta_k \\ HLB_k = \emptyset_k - \beta \times \delta_k \end{cases} \quad (6)$$

where $\emptyset_k\emptyset_k$ is the median,$\delta_k\delta_k$ is the median absolute deviation, HUB_kHUB_k is the Hampel filter upper bound, HLB_kHLB_k is the Hampel filter lower bound, and β is a threshold whose values are selected heuristically in a way that maximizes the accuracy. Because the vehicular context is highly dynamic due to vehicles' high mobility, critical VANET applications require a high rate of context-awareness messages. Thus, it worth noting that the context references are built and updated every 100ms so as to capture the highly dynamic temporal change of the context data.

D. MISBEHAVIOR DETECTION PHASE

As can be seen from Fig. 1, the model is composed of four different classifiers, each of which corresponds to one of the features derived in Section B. These classifiers are used to identify the potential misbehaving vehicles. Three of the classifiers are data-centric-based, and one is behavioral-based. The first data-centric-based classifier is the Consistency-Based Classifier, and the other two are Plausibility-Based Classifiers; one of them is a Communication Range-Based Classifier, and the other is an Overlap-Based Classifier. The fourth classifier is the behavioral-based classifier. All the classifiers utilize the constructed context references to differentiate between benign and misbehaving vehicles. The basic operation concept of these classifiers can be summarized as follows.

The context reference model parameters' are used to evaluate the consistency of the messages based on their deviation from the context reference. The evaluation is calculated using a Hampel Filter-based z-score outlier detection ($z = (x - \mu)/\sigma$), where μ is the arithmetic mean and σ is the standard deviation. The Hampel filter replaces the arithmetic mean μ, and standard deviation σ by the median $\emptyset_k$ and median absolute deviation (MAD) δ_k, respectively. Thus, the Hampel based z-score can be rewritten as follows.

$$z_k^{NV(i)} = \frac{x_k^{NV(i)} - \emptyset_k}{\delta_k} \quad (7)$$

where $z_k^{NV(i)}$ is the score of the neighboring vehicle $(NV(i))$ with respect to the feature $x_k^{NV(i)}$ at time epoch (k), $\emptyset_k$ is the Hampel filter median, and δ_k is the median absolute deviation. Thus, the classification rule in Equation (8) is then used to decide whether the consistency score does not deviate much from the spatial consistency reference model CR_k as follows.

$$c_k^{NV(i)} = \begin{cases} 0 & benign\ vehicle\ if\ HLB_k < z_k^{NV(i)} < HUB_k \\ 1 & misbehaving\ vehicle\ if\ Otherwise \end{cases} \quad (8)$$

A similar procedure was followed to construct the other proposed classifiers, namely the Communication Range-Based classifier, Overlap-Based classifier, behavioral-based Classifier. Equation (7) is used to calculate the score of each vehicle with respect to each feature, and then Equation (8) is used to check whether the neighboring vehicle $NV(i)$ is a misbehaving vehicle or not. Thus, the final decision was taken by aggregating the output of those classifiers using the logical ''OR'' operation. That is, if the output of one of the classifiers is positive, then the vehicle is considered a misbehaving vehicle (MV) (see phase 4 in Fig. 1). The following subsections provide detailed descriptions and further explanations of each classifier.

1) CONSISTENCY-BASED CLASSIFIER

Algorithm 2 illustrates the pseudocode of the consistency-based classifier. Table 3 explains the symbols used. As shown in the pseudocode, each vehicle acquires its mobility data using the EIAE-KF algorithm and broadcasts them to the vehicles in its vicinity using the Kalman filter-based self-predictor algorithm in the DSA-ABR scheme. Each vehicle then collects the mobility data of the vehicles in its communication range using the neighbor-predictor algorithm in the DSA-ABR scheme. Next, each vehicle uses Box and

Algorithm 2 Consistency Based Classifier (CRM_k)

Input: Kalman filter innovation Sequences of all neighbouring vehicles (E), time window w

Output: CRM_k is the context reference model at the time epoch k

1: FOR each time epoch k**DO**

2: ***Obtain*** the innovation sequence E_i for each vehicle i in its vicinity //Derived Features

3:

$$\forall e_{k(i)} \in E : e_k^{NV(i)} = \begin{matrix} y_k^{NV(i)} - \check{y}_{k|k-\tau(i)}^{NP(i)} & \textit{if a message is recieved} \\ e_{k-\tau(i)}^{NV(i)} * (k - \tau\,(i)) & \textit{Otherwise} \end{matrix}$$

4: ***Apply***- Box-Plot to generate the temporal summary $TS_k^{NV(i)} = \{\mu_k, IQR, LB_k\ UB_k\}$.

$$TS_k^{NV(i)} = \begin{cases} \mu_{k(i)} = (Q_1 + Q_3)/2 \\ IQR_{k(i)} = (Q_3 - Q_1) \\ UL_{k(i)} = Q_3 + 1.5IQR \\ LL_{k(i)} = Q_3 - 1.5IQR \end{cases}$$

5: ***Apply***- **Hampel-Filter** to generate the context reference from the spatial summary $S_k = \{\emptyset_k, \delta_k, CUB_k CLB_k\}$.

6: ***Compute***

$$CRM_k = \begin{cases} \emptyset_k = median\left(TS_{k(n\times w)}\right) \\ \delta_k = 1.4826 \times median\left\{\left|TS_{k(n\times w)} - \emptyset_k\right|\right\} \\ CUB_k = HUB_k = \emptyset_k + \beta \times \delta_k \\ CLB_k = HLB_k = \emptyset_k - \beta \times \delta_k \end{cases}$$

CRM_k is the consistency based context reference model at the time epoch k.

7: ***Compute*** the consistency score $ts_k^{NV(i)}$

$$ts_k^{NV(i)} = \max\left(UL_{k(i)}, e_k^{NV(i)}\right) \rightarrow cs_k^{NV(i)} = \frac{ts_k^{NV(i)} - \emptyset_k}{\delta_k}$$

8: ***Detect*** Misbehaving Nodes $c_k^{NV(i)}$

$$c_k^{NV(i)} = \begin{cases} 0 & \textit{benign vehicle if } CUB_k < cs_k^{NV(i)} < HUB_k \\ 1 & \textit{misbehaving vehicle Otherwise} \end{cases}$$

9: END FOR LOOP

the Whisker Plot method to generate a temporal summary $TS_k^{NV(i)}$ from the innovation error of the Kalman filter of each vehicle in its vicinity (see Algorithm 1, line 4). After that, each vehicle uses the temporal summaries of the neighboring vehicles to construct a spatial consistency context reference model CRM_k using a Hampel filter-based algorithm (see Algorithm 1, line 6). A temporal consistency score is then calculated for each neighboring vehicle, based on its deviation from the context reference CRM_k. The score $cs_k^{NV(i)}$ is calculated using a Hampel Filter-based z-score ($z = \frac{x_t - \mu}{\sigma}$) (see Algorithm 2, line 8). The Hampel filter replaces the arithmetic mean , μ, and the standard deviation , σ, by the median, $\emptyset_k$, and the median absolute deviation $(MAD)\delta_k$,

TABLE 3. Description of symbols.

Symbol	Description
$e_k^{NV(i)}$	Innovation error of neighboring vehicle $NV(i)$ at time epoch (k)
$y_k^{NV(i)}$	Received mobility data
$\check{y}_{k\|k-\tau(i)}^{NP(i)}$	Predicted mobility data
$\tau(i)$	The time epoch of last received mobility data
$TS_k^{NV(i)}$	Temporal Consistency Summary
$\mu_{k(i)}$	The mean at epoch (k) of a vehicle (i)
$IQR_{k(i)}$	Interquartile Range
$UL_{k(i)}$	Box-Plot Upper limit
$LL_{k(i)}$	Box-Plot Lower limit
$\emptyset_k$	Median of the vehicles' temporal summaries
δ_k	The median absolute deviation of vehicles' temporal summaries
HUB_k	Hampel Upper Bound, also called CUB_k consistency upper bound
HLB_k	Hampel Lower Bound, also called CLB_k consistency lower bound
CRM_k	The consistency-based context reference model
$ts_k^{NV(i)}$	Temporal consistency score for the neighboring vehicle (i)
$cs_k^{NV(i)}$	Spatial consistency score for the neighboring vehicle (i)
$c_k^{NV(i)}$	Misbehaving status of the vehicle (i)

respectively. Hampel filter has two main tuning parameters: the length of the sliding time window w, and the number of accepted median absolute deviations β (See Algorithm 3, line 6). A length of two seconds sliding window was selected to reduce the false positive rate produced when the vehicular context becomes highly dynamic. This value was obtained from the used broadcasting scheme [21], which supports an average of 2 seconds broadcasting interval without sacrificing the accuracy of the mobility information. β equals to 1.8 was found the best value that minimizes the false positive rate in the absence of the attacker's data. Finally, hypothesis testing is conducted to evaluate whether the consistency score of a vehicle does deviate much from the spatial consistency reference model or not (see Algorithm 2, line 8). Table 2 presents a description of the pseudocode symbols used in Algorithm 2.

2) COMMUNICATION RANGE-BASED CLASSIFIER

The communication range-based classifier is used to detect the implausible messages in which the distance between the communicating vehicles exceeds the maximum communication range (see Fig. 2). The accepted communication range for the first appearance of any vehicle (newly appeared vehicles) should fall between the Hampel filter upper bound ($MCRT$) and lower bound ($SAVT$) thresholds (see Fig. 2). Algorithm 3 shows the pseudocode of the proposed communication-range based classifier. Table 4 explains the symbols used. The accepted communication range of the vehicles in the vicinity of the vehicle that runs the misbehavior detection should be less than the $MCRT$ value or higher than the $SAVT$ value when it appears for the first time. A vehicle is considered to be misbehaving if it has violated these rules (see Algorithm 3, line 4).

3) OVERLAP-BASED CLASSIFIER

In a normal situation, two vehicles cannot occupy the same space at the same time. However, due to misbehavior activities by misbehaving vehicles, vehicles may overlap with each other. The overlap-based classifier considers the presence of

Algorithm 3 Communication Range Based Classifier ($CRPRM_k$)

Input: M_k the set of all received messages in the time epoch k
FAD_w the set of the first appearance distances of the active neigboring vehicles
CRM_k the current context refernce
Output: RS_k the range based decision vector
1: $\forall$ *vehicle* $i \in M_k$ *caluclate the distance* $d_k^{NV(i)}$ *between this vehicle and vehicle* i:

Calculate $d_k^{NV(i)} = \|p(x,y) - p_i(x_i,y_i)\| \quad \forall vehiclei \in FAD_w$

2: $\forall$ *vehiclei* $\in FAD_w$

Compute $CRPR_k$

$$= \begin{cases} \emptyset_k = median\,(FAD_w) \\ \delta_k = 1.4826 \times median\left\{\left|CRFO_{k(n\times w)} - \emptyset_k\right|\right\} \\ MCRT_k = \emptyset_k + \beta \times \delta_k + CUB_k \\ SAVT_k = \emptyset_k - \beta \times \delta_k - CUB_k \end{cases}$$

3: ***Compute*** the range-based score $rs_k^{NV(i)} = \frac{d_k^{NV(i)} - \emptyset_k}{\delta_k}$
4: $\forall$*vehicle i add* $\in M \cup FAD_w$

$$\textbf{\textit{Set}}\, r_k^{NV(i)} = \begin{cases} 0 & benign\ if\ first\ apearing \\ & SAVT_k < d_k^{NV(i)} < MCRT_k \\ 0 & benign\ if\ not\ first\ appearing \\ & d_k^{NV(i)} < MCRT_k \\ 1 & misbehaving\ Otherwise \end{cases}$$

5: ***Append*** $r_k^{NV(i)}$ to CR_k and **Return** RS_k

TABLE 4. Description of symbols.

Symbol	Description
$d_k^{NV(i)}$	The distance between the host vehicle and the neighboring vehicles ($NV(i)$) during the first contact at time epoch (k)
$p(x,y)$	Position of the host
$p_i(x_i,y_i)$	Position of neighboring vehicles ($NV(i)$)
FAD_w	Set of neighboring vehicles that have an active connection
$CRPR_k$	Communication Range-Based Plausibility Reference
$rs_k^{NV(i)}$	The range-based score for the neighboring vehicle (i) at time epoch (k)
$\emptyset_k$	The median of the temporal summaries of all vehicles
δ_k	The median absolute deviation
CUB_k	Data Consistency Upper Bound at time epoch (k) obtained from consistency reference CRM_k
$SAVT_k$	Sudden Appearance Vehicle Threshold
$MCRT_k$	Maximum Allowed Communication Range at time epoch (k) for a vehicle
$r_k^{NV(i)}$	Range Status of the neighboring vehicle (i) at time epoch (k)

an overlapping area as a potential attack. Due to the highly dynamic context, harsh, and heterogeneous noise environment in VANETs, the overlap among vehicles can occur out of malicious activities due to inaccurate mobility information. Existing overlapping-based solutions are unaware of this issue. The uncertainty of the information has not been considered, which leads to a high rate of false alarms. Unlike the existing algorithm proposed in [6], [46], the model proposed

Algorithm 4 Overlap-based Plausibility Classifier ($OLRM_k$)

Input: M_k the set of all received messages at the time epoch k CRM_k the current context reference at the time epoch k
Output: OL_k the decision vector at the time epoch k

1: FOR each message $i \in M_k$
2: Set $os_k^{NV(i)} = 0$ // *Score Initialization*
3: FOR each message $j \in M_k$ but not i
4: $$d_{(i,j)} = \left\|p_i\,(x_i,y_i) - p_j\,(x_j,y_j)\right\|$$
5: $$d_{min(i,j)} = \min\left(\left(\frac{w_i + w_j}{2}\right), \left(\frac{l_i + l_j}{2}\right)\right)$$
6: IF $\left|d_{(i,j)} + CUB_k\right| < d_{min(i,j)}$ **THEN**
// the CUB_k is obtained from the CRM_k
7: Set $os_k^{NV(i)} = ol_k^{NV(i)} + 1$ and **SET** $os_k^{NV(j)} = ol_k^{NV(j)} + 1$
8: END IF
9: END FOR LOOP
10: END FOR LOOP
11: Set $OLR_k = \begin{cases} \emptyset_k = median\,(OS_k) \\ \delta_k = 1.4826 \times median\,\{|OL_k - \emptyset_k|\} \\ OUB_k = \emptyset_k + \beta \times \delta_k \\ OLB_k = \emptyset_k - \beta \times \delta_k \end{cases}$
12: Compute the range-based score $rs_k^{NV(i)} = \frac{d_k^{NV(i)} - \emptyset_k}{\delta_k}$
13: $o_k^{NV(i)} = \begin{cases} 0 & benign\ vehicle\ if\ OUB_k > os_k^{NV(i)} > OLB_k \\ 1 & misbehaving\ vehicle\ Otherwise \end{cases}$
14: Append $os_k^{NV(i)}$ and **Return** OS_k

TABLE 5. Description of symbols.

Symbol	Description
$os_k^{NV(i)}$	The overlapping score of a vehicle (i) at time epoch (k)
w_i, l_i	Width and length of the vehicle (i)
OS_k	A vector contains the overlapping scores of neighboring vehicles at time epoch (k)
OLR_k	Overlap-based Plausibility Reference
OUB_k	Maximum Overlap Score at time epoch (k)
$\emptyset_k$	The median of the temporal summaries of all vehicles
δ_k	The median absolute deviation
OUB_k	Maximum Overlap Score at time epoch (k)
OLB_k	Minimum Overlap Score at time epoch (k)
$o_k^{NV(i)}$	Overlapping status of the vehicle (i) at time epoch (k)

by this study is context-aware, as it takes the uncertainty of the mobility information into account.

Algorithm 4 shows the pseudocode of the proposed overlap-based classifier, and Table 5 explains the symbols used. The area that each vehicle occupies is represented by a rectangle. The width and length of the vehicles are assumed to be known and used to represent the occupation area. Then, the rectangles that represent the occupation areas are shrunk based on the uncertainty of the mobility information. The uncertainty of mobility information is obtained from the context reference namely the consistency upper bound CUB_k (see Algorithm 2, Line 6). As overlapped vehicles involve both benign and misbehaving vehicles, they cannot be considered to be misbehaving. As such, the false positive rate increases

Algorithm 5 Behavioral Based Classifier (BRM_k)

Input: M_k the set of all received messages at the time epoch k

Output: B_k the decision vector at the time epoch k

1: $\forall vehiclei \in M_k$ **Compute** the Updating Rate

$$BUR_{k(i)} = \frac{TotalReceived\ Messages}{ConnectionLength}$$

2: Calculate $BR_k = \begin{cases} \emptyset_k = median\,(BUR_k) \\ \delta_k = 1.4826 \times median\,\{|BUR_k - \emptyset_k|\} \\ BUB_k = \emptyset_k + \beta \times \delta_k \\ BLB_k = \emptyset_k - \beta \times \delta_k \end{cases}$

3: Obtain $b_k^{NV(i)} = \begin{cases} 0 \quad benign\ vehicle\ if \\ \quad BUB_k > bs_k^{NV(i)} > BLB_k \\ 1 \quad misbehaving\ vehicle\ Otherwise \end{cases}$

4: Append $b_k^{NV(i)}$ to B_k and **Return** B_k

TABLE 6. Description of symbols.

Symbol	Description
$d_k^{NV(i)}$	Innovation error of neighboring vehicle NV (i) at time epoch (k)
$bs_k^{NV(i)}$	The behavioral score for the neighboring vehicle (i) at time epoch (k)
BR_k	Behavioral-based Context Reference
$b_k^{NV(i)}$	Behavioral status of the neighboring vehicle (i) at time epoch (k)
$bs_k^{NV(i)}$	The behavioral score for the neighboring vehicle (i) at time epoch (k)
$\emptyset_k$	The median of the temporal summaries of all vehicles
δ_k	The median absolute deviation
BUB_k BLB_{k_k}	Hampel Filter Upper Bounds at time epoch (k) Hampel Filter Lower Bounds at time epoch (k)

dramatically. In order to address this issue, a Hampel filter-based classifier is constructed. The classifier uses the Hampel filter parameters as an overlap-based plausibility reference for the decision.

4) BEHAVIORAL-BASED CLASSIFIER

The data-centric based classifiers constructed in the previous section are not able to detect the sophisticated context-aware attacks. A sophisticated attack can spread false mobility information that can bypass the consistency and plausible-based classifiers. For example, malware can manipulate the mobility information and makes it similar to the normal movement patterns of benign vehicles. Such attacks can flood the communication channel by unnecessary broadcasts, disrupt the cooperation concept of VANET, and conduct a successful, false information-based attack. Thus, it is imperative to design a behavioral-based classifier to detect such sophisticated attacks. Algorithm 5 shows the pseudocode of the proposed behavioral-based classifier, and Table 5 describes the symbols used.

IV. PERFORMANCE EVALUATION

The experimental setup and performance metrics are discussed in the following subsections.

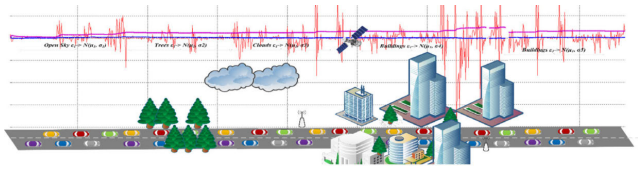

FIGURE 4. Mixed noise scenario.

A. EXPERIMENTAL SETUP

Extensive simulation has been conducted to evaluate the performance of the proposed model. Many common procedures for evaluating misbehavior detection solutions were carried out, including dataset selection and preprocessing, environmental noise injection, communication simulation, and misbehavior simulation, as performed in [6], [45]. For the sake of the simulation, the Matlab tool was used to simulate the environmental noises, communication channels, and misbehaving vehicles [6], [17], [18], [23], [45].

1) DATASETS AND PREPROCESSING

Next Generation Simulation (NGSIM), a real-world traffic dataset, which contains vehicles' trajectories recorded each 100ms was used in this study. This dataset was generated by the United States Department of Transportation (US DOT) Federal Highway Administration (FHWA) [71]. It represents the ground truth information of neighboring vehicles' trajectories [71], [72]. In order to ensure that the evaluation has considered all types of driver behaviors, the dataset was divided based on driver behavior into four different clusters. For each vehicle, three features were selected to represent driver behavior, namely: time headway, space headway, and lane changing ratio. The selected features were aggregated by finding their means and variance that were then used as input for the K-Means clustering algorithm [73]. These clusters describe four types of driving regime: free-flowing, random flowing, car flowing, and lane changing behavior. The purpose of such categorization is to ensure that the vehicle behavior has no influence on the performance of the proposed scheme.

B. SIMULATING THE ENVIRONMENTAL NOISES

Various types of environmental noise were injected into vehicles' trajectories in the NGSIM dataset to represent VANET' harsh environment. In this study, a combination of stationary white noises with zero mean, non-stationary white noise with time-varying variance, and correlated noises that have been reported by several studies in VANET context acquisition [48] were employed to simulate the dynamic and heterogeneous environmental noise (see Fig. 4). Noise injection is a common procedure to simulate the measurement of noises in a VANET environment [4], [74]. The detailed description of the noise types, noise scenarios, and the simulation used in this study can be found in our previous publication [4]. The acquisition algorithm presented in [4] was also used to acquire the context information in each vehicle.

1) SIMULATING THE MESSAGES LOSSES

Due to the impact of communication reliability on the attackers and the detection model, nine communication scenarios were simulated. In each scenario, the message arrival rate was modeled as a Poisson distribution with 9 different message arrival properties ranging from 1 to 0.3 within each 100ms from each neighboring vehicle. Thus, nine message loss ratios ranging from 0% to 40% were used. These nine scenarios represent different communication statuses in VANETs. Each vehicle uses the broadcasting scheme presented by [21] to efficiently share their own information and effectively collect the context information of the neighboring vehicles.

2) SIMULATING THE MISBEHAVING VEHICLES

Due to the absence of a ground truth labeled dataset for evaluating misbehavior detection systems in the vehicular network, simulating the misbehavior is a common evaluation procedure. Two types of misbehaviors were simulated, faulty vehicles and attackers. Three types of faults were injected in the datasets, namely, spikes, noises, and constant type attacks. The first two types of faults were detected and corrected before misbehavior detection was started through the EIAE-KF algorithm, as they were considered as inconsistent context information during the acquisition phase. Meanwhile, the constant faults were detected by the proposed CA-DC-MDS. The second type of misbehavior is attacker actions, which can be grouped into two types, basic attacks, and sophisticated attacks. Positioning noises, position jumping, message suppression attack, cheating with context information attack, sudden position jumping, and random jumping are examples of these basic attacks [75], [76]. In addition, in the sophisticated attacks, attackers are aware of the context and, consequently, can perform incremental jumps to carry out attacks such as an illusion attack [77].

C. DATASETS SAMPLES

Table 5 shows the dataset samples used to evaluate and validate the proposed CAMDS scheme. The dataset samples were collected by 15 vehicles that were randomly selected from different driving regimes, in addition to one dataset that was collected by one simulated RSU. Each dataset was replayed under the nine communication scenarios mentioned above, in a heterogeneous and dynamic noise environment.

D. PERFORMANCE METRICS

Five performance metrics were used to evaluate the proposed HCA-MDS model, namely: detection accuracy, false positive rate (*FPR*), detection rate (*DR*), precision, and F-measure. *FPR* and *DR* are common evaluation metrics for validating the effectiveness of misbehavior detection models in VANETs [45]. As fixed thresholds can lead to either a reduce false-positive or increase detection rate, these two evaluation metrics must be studied together in order to evaluate the effectiveness of the proposed detection scheme. The precision determines how precise the model is out of those predicted positive, i.e., how many of them are actually positive. It is a good measure to determine when the costs of False Positive are high. Moreover, as the amount of data for attacks is less than that for normal data, $F-Measure$ is a suitable evaluation metric, as it does not take the true negative into account. It is more informative than the other metrics when evaluating binary classifiers on imbalanced datasets [78]. These evaluation metrics are calculated according to the following

TABLE 7. NGSIM Dataset selected samples.

Dataset	Vehicle Id	Speed (km/h)	Neighbors	Duration (s)
DS1	13	60.5	177	94.8
DS2	252	83.9	255	55.8
DS3	455	77.8	260	60.3
DS4	2280	86.4	270	54.1
DS5	5	80.6	119	70.2
DS6	1133	114.1	214	39.3
DS7	1687	80.6	314	76.5
DS8	1	64.8	134	88.4
DS9	268	94.3	255	58.5
DS10	1066	118.8	225	47.5
DS11	1964	77.4	317	72.9
DS12	7	81.0	127	71.1
DS13	1593	76.0	294	74.2
DS14	2885	59.4	200	94.5
DS15	1899	71.6	331	78.8
DS16	RSU	100.8	284	57.3

$$\begin{aligned} &Detection\ Accuracy \\ &= 100\% \times \frac{Total\ Number\ of\ Correct\ Classified\ Vehicles}{Total\ number\ of\ Vehicles} \end{aligned} \tag{9}$$

$$\begin{aligned} &False\ Positive\ Rate\ (FPR) \\ &= 100\% \times \frac{Total\ Number\ of\ Misclassified\ Genuine\ Vehicles}{Total\ number\ of\ Genuine\ Vehicles} \end{aligned} \tag{10}$$

$$\begin{aligned} &Detection\ Rate\ (DR) \\ &= Recall \\ &= 100\% \times \frac{Total\ Number\ of\ Correctely\ Classified\ Attackers}{Total\ number\ of\ Actual\ Attackers} \end{aligned} \tag{11}$$

$$\begin{aligned} &Precision \\ &= 100\% \times \frac{Total\ Number\ of\ Correctely\ Classified\ Attackers}{Total\ number\ of\ Vehicles\ Classfied\ as\ Attackers} \end{aligned} \tag{12}$$

$$\begin{aligned} &F\text{-}Measure \\ &= 100\% \times \frac{2 \times Recall \times Precision}{Precision + Recall} \end{aligned} \tag{13}$$

V. RESULTS AND DISCUSSION

Here, the performance of the proposed hybrid context-aware misbehavior detection model (HCA-MDS) on the network and its effectiveness and robustness under dynamic are discussed and compared with previously proposed approaches.

A. PERFORMANCE COMPARISON

To demonstrate the improvement gained, the overall detection accuracy, false-positive rate, detection rate (recall),

TABLE 8. The effectiveness of the proposed model.

Scheme	Accuracy (%)	FPR (%)	DR /Recall (%)	Precision (%)	F-Measure (%)
HCA –MDS (Proposed)	93.51	4.45	86.11	85.00	84.44
DCA –MDS (Proposed)	90.98	2.33	66.18	89.19	75.05
Bissmeyers' ECT-MDS [6]	74.79	2.98	30.65	83.50	44.49
Stübing's et al MDS [40]	87.37	4.79	62.55	86.91	71.60
HMDS (MDS [40] + ECT-MDS [6])	83.84	11.20	73.36	69.58	70.66

precision, and F-measure of the proposed Hybrid and Context-Aware Models (namely DCA-MDS, and HCA-MDS) are compared with those of the ECT-MDS [6], MDS [40] and HMDS (MDS [40] and ECT-MDS [6]) models. DCA-MDS is short for the data-centric context-aware MDS because it uses the data-centric classifiers of the proposed HCA-MDS. It has been separated to demonstrate the advantage of the proposed hybrid approach compared to the data-centric approach. The ECT-MDS model [6] combines data-centric detection techniques proposed by Stübing's MDS [40] with behavioral techniques as well as trust-based techniques. The MDS [40] has been used as a baseline for misbehavior detection by many previous researchers [6], [45]. The HMDS has been implemented by the authors of this paper to compare the hybrid and context-unaware model with the proposed hybrid context-aware model (HCA-MDS). It combines the behavioral-based features, as suggested by Bissmeyer *et al.* [6], with data-centric based features. as proposed in Stübing et al.'s MDS [40]. It is worth noting that ECT-MDS, MDS, and HDMS are unaware of the context. That is, static security thresholds are used to classify the vehicles as either benign or misbehaving. However, the proposed models, HCA-MDS and DCA-MDS, are context-aware, where the predefined static context thresholds have been replaced by a dynamic context reference that is constructed online to adapt to the current context.

B. EFFECTIVENESS EVALUATION

Table 8 lists the average of the experimental results of the proposed Hybrid and Context-Aware MDS model (HCA-MDS) using the evaluation metrics listed above. It can be seen that the proposed HCA-MDS has achieved the highest accuracy (93.51%) compared to the non-hybrid and non-context aware based approaches, namely the MDS model [40] (see Fig. 5 (a)). Moreover, the results in Table 8 show that 93.51% of the vehicles were correctly classified by the HCA-MDS, while the DCA-MDS correctly classified 90.98% of the tested vehicles. In contrast, only 74.79% of the vehicles are correctly classified by the ECT-MDS and 87.37% by the baseline model. ECT-MDS has the lowest accuracy (74.79%) compared to other studied models. This is due to the difficulties in choosing a proper trust threshold suitable for the different vehicular contexts. Furthermore, the context-aware model (DCA-MDS) achieves the lowest false positive rate (2.33%) compared to non-context aware and hybrid models (see Fig. 5 (b)). The HMDS produces the highest false-positive rate with all scenarios. This is because behavioral classifier is highly sensitive to the dynamic vehicular context. On average, the detection rate of the proposed hybrid model is 86.11% compared to 66.18%, 30.65%, 62.55, 73.36 for the non-hybrid, and non-context-aware (MDS), and hybrid and non-context aware MDS (ETC-MDS and HMDS) models, respectively (see Fig. 5 (c)). In terms of false-positive rate (FPR), DCA-MDS achieved the lowest false alarm rate (2.33%), followed by the ECT- baseline MDS (2.98%). Both the proposed model, HCA-MDS, and the MDS baseline produced higher false alarm rates than DCA-MDS and ECT-MDS. HMDS achieved the worst false alarm rate of 11.20%, due to the fact that the behavioral features are highly context-dependent. Although the false-positive rate of the proposed HCA-MDS model is slightly higher than that of DCA-MDS and ECT-MDS, it achieves the lowest detection rate compared to the other studied models (see Fig. 5 (c)).

The precision results in Table 6 show the proportion of the misbehaving vehicles reported by the model that were correctly classified. It evaluates the accuracy of the model when the cost of false alarms is high. Thus, by comparing the false positive rate in Table 8 with the precision, it can be noticed that the precision and false positive rate have an indirect relationship, i.e., if the false positive rate increases, the precision will decrease. The proposed DCA-MDS achieves the best precision among the studied models (89.19%) compared to 86.91% for MDS, 85.0% for HCA-MDS, and 83.5% for ECT-MDS, while the lowest precision was achieved by HMDS (69.58%). However, the detection rate of DCA-MDS is relatively lower than that of HCA-MDS.

As the number of misbehaving vehicles (10%) is lower than the number of benign vehicles (90%), the accuracy measure cannot be considered as a good performance measure. Moreover, it is easy to optimize either the detection rate or false positive rate, but it is challenging to make a trade-off between those two measures together. Therefore, the harmonic mean of precision and recall, namely the F-Measure, has been used to evaluate the overall performance of the proposed model in the unbalanced datasets. The results in terms of F-measure show that the proposed model HCA-MDS achieved the best trade-off between precision and recall (84.44%) compared to the related models, while ECT-MDS achieved the worst performance (44.49%) (see Fig. 5 (d)). The overall performance achieved by the HCA-MDS is 84.44% compared to 75.05 for the proposed context-aware data-centric model DCA-MDS, 44.49% for

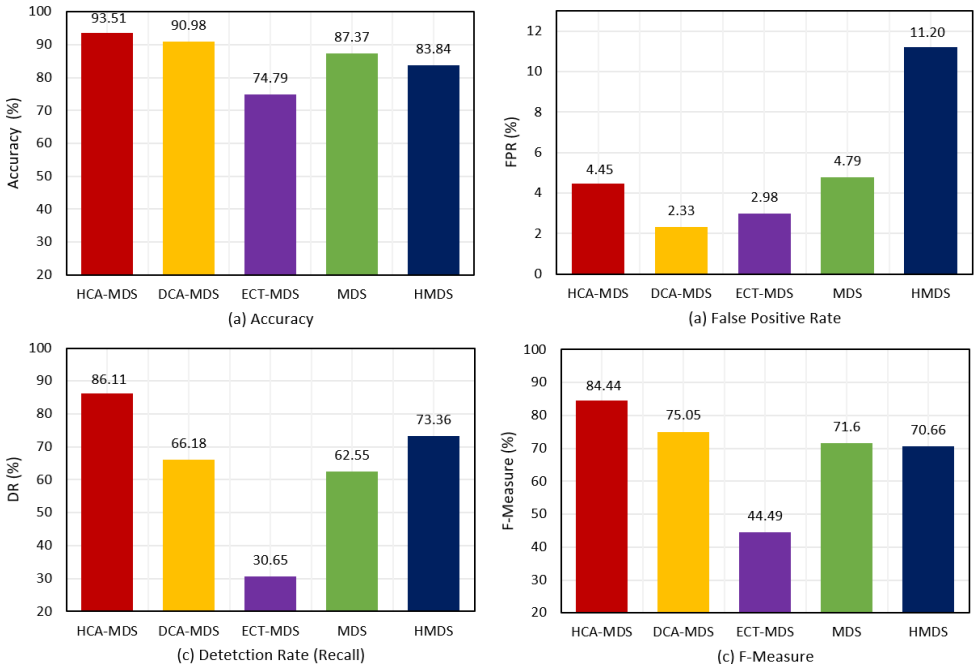

FIGURE 5. Comparison of the effectiveness results among the proposed and the existing models.

the trust-based data-centric model ECT-MDS [6], 71.60% for the data-centric model MDS [40], and 70.66% for the hybrid and context-unaware model HDMS. These results show the advantage of context-aware based models (HCA-MDS and DCA-MDS) over the non-context aware models (MDS, HMDS, and ECT-MDS) in terms of the effectiveness of the VANET context. It also shows the advantage of the hybrid context-aware model (HCA-MDS) compared to the non-hybrid context-aware model (DCA-MDS).

C. ROBUSTNESS EVALUATION

Fig. 6 (a), (b), (c), and (d) show the effect of the dynamic context on the performance of the studied models. They also provide a detailed comparison of the results achieved by the proposed Hybrid, and Context-Aware Models (namely HCA-MDS and DCA-MDS) and non-context-aware models (ECT-MDS model [6], MDS model [40], and HDMS) in terms of the robustness and the adaptability to the dynamic context. In Fig. 6 (a), (b), (c), and (d), the X-axis of each subfigure represents nine communication scenarios, ranging from an ideal communication channel to the worst communication channel. In the ideal communication scenario (scenario number 1 in Fig. 6), all broadcasted messages from neighboring vehicles were received by the vehicles hosting the misbehavior detection model. In the worst scenario (scenario number 9 in Fig. 6), only 20% of the transmitted messages were received by the MDS model, due to the communication loss problem. In the other studied scenarios (from the second scenario to the last studied scenario), the messages received ratio degraded from 90% to 30%. The Y-axis of Fig. 6 (a), (b), (c), and (d) represent the average accuracy, false alarm rate (FPR), detection rate (DR), and F-measure, respectively of the 16 datasets used in the experiments (as shown in TABLE 7).

It can be observed from Fig. 6 (a), that the accuracies of the proposed models (HCA-MDS and DCA-MDS) are stable compared to the non-context aware models. The accuracy of HCA-MDS is stable, at above 90%, in all the studied scenarios. Similarly, the accuracy of the DCA-MDS is stable at around 90% accuracy but lower than that of HCA-MDS. It is obvious that both the HCA-MDS and DCA-MDS models can adapt to the dynamic vehicular context. The reason why HCA-MDS has higher accuracy than the DCA-MDS is the inclusion of the behavioral classifiers to improve accuracy. The accuracy of the MDS baseline was stable under highly reliable scenarios, i.e. when the rate of the arrived message was high. However, it drops gradually to 71% under the low reliable scenarios (Scenarios #5, 6, 7, and 8 in Fig. 6 (a)). Although the accuracy of the HMDS under ideal and high reliable scenarios is high, the accuracy rapidly drops to below 65%. The drop in the accuracy of the hybrid model, HDMS, is due to the fact that the behavioral features are more sensitive to the vehicular context. This suggests why the MDS baseline has better accuracy than the other non-context aware and hybrid model, HDMS. ECT-MDS has low detection accuracy compared to the other studied scenario. Furthermore, the accuracy of the ECT-MDS slightly decreases when the message loss increases. The drop in the accuracy of the ECT-MDS is due to difficulties in establishing a suitable trust threshold that can fit all studied scenarios.

In terms of the False Positive Rate, both the baseline MDS and the HMDS are greatly influenced by the dynamic

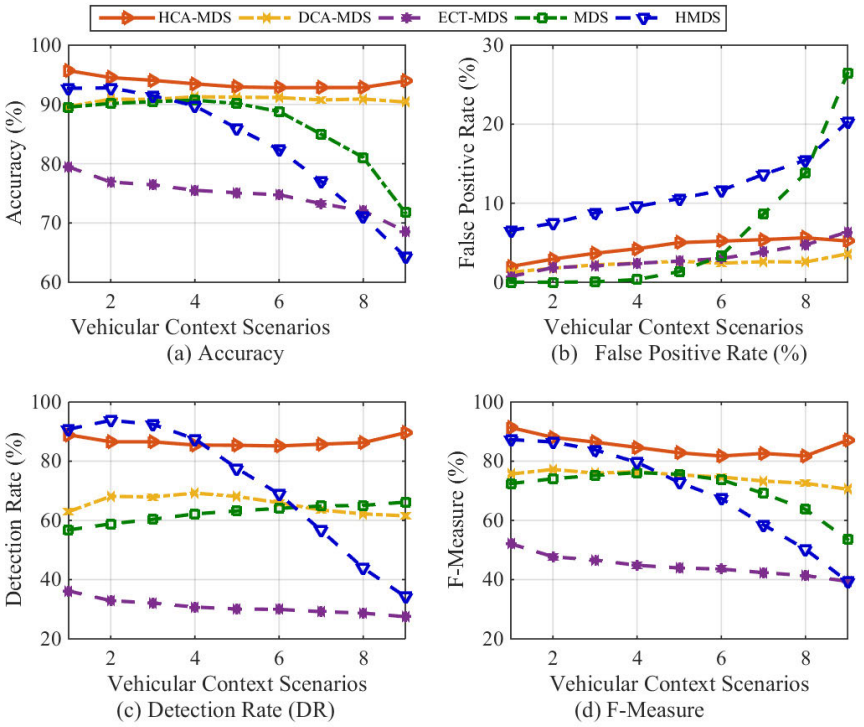

FIGURE 6. Comparison of the robustness results between the proposed and the existing models.

communication status. FPR increases rapidly to more than 26% for MDS and 21% for HMDS, which has a higher false alarm rate under all studied scenarios compared to the other studied models. Although the ECT-MDS model [6] manages to decrease the false positive rate compared to the baseline MDS and HMDS, its detection rate is low (see Fig. 6 (c)). As shown in Fig. 6 (c), the detection rate of ECT-MDS slightly decreases as the communication channel becomes more unreliable. In contrast, the proposed HCA-MDS and DCA-MDS models maintain a higher and stable detection rate with low and stable false alarm rates, even under highly unreliable communication scenarios. Although the DCA-MDS achieved a more stable and lower false positive rate than HCA-MDS (See Fig. 6 (b)), its detection rate was below 80% with all tested scenarios. This is due to the nature of the attackers, which are aware of the context, which renders the data-centric approach unable to differentiate between rogue and misbehaving vehicles. In contrast, the hybrid context-awareness-based model, HCA-MDS, is able to distinguish between rogue and misbehaving vehicles due to the inclusion of the behavioral features, in addition to data-centric features to build both the context reference and perform the detection online. The data rate of the HCA-MDS is higher than 80% with all studied scenarios, while the data-rate of the DCA-MDS is around 70% in most studied scenarios. These results indicate the effectiveness of the proposed hybrid context-aware model HCA-MDS in detecting the context-aware attackers locally and autonomously when the data-centric approach fails. Fig. 6 (d) shows a comparison in terms of the overall performance using F-measure. The proposed HCA-MDS model archived the highest performance in terms of the tradeoff between precision and recall compared with the non-context-aware and non-hybrid model under all scenarios.

The experimental results in Table 8, Fig. 5, and Fig. 6 show that the proposed models, HCA-MDS and DCA-MDS, achieved the highest performance in terms of both their adaptability to the dynamic context and the highest detection accuracy among all the studied models. The HCA-MDS achieved better performance than the DCA-MDS, due to the inclusion of the behavioral features of the vehicles, which represent the context more accurately. On average, HCA-MDS has improved the overall performance by 13%, 14%, 40% compared to the MDS model [40], the hybrid context-unaware MDS model (HMDS), and ECT-MDS [6], respectively. That is, HCA-MDS outperforms the MDS model in increasing the detection rate by 38% and decreasing the false positive rate by 7%. The results confirm that the combination of context-aware design, hybrid detection concepts, and multi-faceted classifiers offer an effective solution to address the misbehavior problem in VANETs.

D. LIMITATIONS OF THE PROPOSED HCA-MDS

Although the proposed HCA-MDS model has significantly improved the detection performance, there is still room for improvement. Because VANET applications related directly to people's safety, detection accuracy should be maximized. In terms of the detection rate, the proposed model could not

detect some attacks due to the high similarity in the behavior and the generated data of both misbehaving and benign vehicles. More representative features that can distinguish misbehavior and normal data are needed. Although the proposed DCA-MDS achieves the lowest false positive rate, the false-positive rate of the proposed hybrid is relatively high. There are two main reasons that account for the higher false-positive rate of HCA-MDS compared to that of DCA-MDS. Firstly, there is a high similarity between normal maneuvering behavior and misbehaving vehicles' behavior. This has caused a portion of benign vehicles during their maneuvering to be classified as attackers. Thus, a mechanism that can distinguish between maneuvering behavior and misbehavior is necessary. Secondly, HCA-MDS takes the decision using the logical ''OR'' function; thus, the false positive is additive. Therefore, studying the uncertainties of the classifier may be useful to improve the decision logic. We are currently working to address these issues. The new findings in this regard will be the subject of our next publication.

VI. IMPLICATIONS

This section explains the implications of the proposed hybrid context-aware misbehavior detection model (HCA-MDS). Because VANET is a type of cyber-physical systems, where information affects the physical world, the integrity of context information is an essential security requirement for any VANET application. As such, the proposed HCA-MDS maintains such integrity by conducting context-aware consistency and plausibility checks on the data sent/received by the neighboring vehicles. In addition, a wide range of applications and protocols such as Cooperative Collision Warning Systems (CCWS) [79], Cooperative Adaptive Cross-Control (CACC) [80], Advanced Driver Assistance Systems (ADAS) [81], Real-time traffic Analysis, and Internet of Vehicles (IoV) can make use of the proposed HCA-MDS for decision making to strengthen their security. For instance, HCA-MDS consolidates the ability of safety and traffic efficiency applications to distinguish between false event patterns and real events. Another example, the routing protocol can avoid considering the misbehaving vehicles in their routing decision so as to increase the network performance. Moreover, HCA-MDS provides consistency, plausibility, and behavioral scores, which can be used to build a reputation for each vehicle for trust establishment in VANETs. The proposed model also can be adopted to detect attacks related to the Internet of Things (IoT) applications, where heterogeneous devices and protocols are used.

The proposed hybrid and context-aware concept can be extended to many applications, even beyond VANET security and transportation safety. It can be used to improve the performance of the Internet of Vehicles (IoV)-based applications, where the context information will be used to improve the routing performance and network agility. It can also be used to provide the integrity of the information that coordinates the movement of swarms of drones or planes.

VII. CONCLUSION AND FUTURE WORK

In this paper, a hybrid multifaceted context-aware misbehavior detection model has been proposed. The experimental results showed the effectiveness of the proposed model in detecting misbehaving vehicles locally during the initial stages, in the dynamic and harsh environment. The proposed model demonstrated its adaptability and robustness, even under highly unreliable communication environments. The model consists of hybrid and multifaceted statistical classifiers that work together to detect sophisticated attacks. The proposed model is context-aware, in which the static security thresholds have been replaced by a context reference. The context reference is constructed and updated online using Kalman and Hampel Filters that utilize the spatial and temporal correlation of the mobility information of the communicating vehicles.

In the future, the limitation of the proposed HCA-MDS model needs to be addressed. The work can be extended by including other techniques, such as artificial intelligence-based classifiers, to examine performance improvement. This can be done through extracting features from the output of the existing unsupervised statistical-based classifiers. These features may be used to distinguish the misbehaving and benign vehicles more accurately. We are currently working on learning the attack pattern from the output of the developed classifiers. The new findings in this regard will be the subject of our next publication.

REFERENCES

[1] *IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture*, IEEE Standard 1609.0-2013, 2013, pp. 1–78.

[2] H. Vahdat-Nejad, A. Ramazani, T. Mohammadi, and W. Mansoor, ''A survey on context-aware vehicular network applications,'' *Veh. Commun.*, vol. 3, pp. 43–57, Jan. 2016.

[3] H. Stübing, ''Car-to-X communication: System architecture and applications,'' in *Multilayered Security and Privacy Protection in Car-to-X Networks*. Wiesbaden, Germany: Springer, 2013, pp. 9–19.

[4] F. A. Ghaleb, A. Zainal, M. A. Rassam, and A. Abraham, ''Improved vehicle positioning algorithm using enhanced innovation-based adaptive Kalman filter,'' *Pervas. Mobile Comput.*, vol. 40, pp. 139–155, Sep. 2017.

[5] R. W. van der Heijden, S. Dietzel, T. Leinmller, and F. Kargl, ''Survey on misbehavior detection in cooperative intelligent transportation systems,'' Oct. 2016, *arXiv:1610.06810*. [Online]. Available: https://arxiv.org/abs/1610.06810

[6] N. Bissmeyer, W. Michael, and K. Frank, ''Misbehavior detection and attacker identification in vehicular ad-hoc networks,'' Tech. Univ. Darmstadt, Darmstadt, Germany, Tech. Rep., 2014.

[7] *IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages*, IEEE Standard 1609.2-2013 and 1609.2-2006, 2013, pp. 1–289.

[8] *European Telecommunications Standards Institute. Intelligent Transport Systems (ITS); OSI Cross-Layer Topics; Part 8: Interface Between Security Entity and Network and Transport Layers*, ETSI, Sophia Antipolis, France, 2013.

[9] T. Leinmuller, E. Schoch, F. Kargl, and C. Maihofer, ''Influence of falsified position data on geographic ad-hoc routing,'' in *Security and Privacy in Ad-Hoc and Sensor Networks*. Berlin, Germany: Springer, 2005, pp. 102–112.

[10] T. Leinmuller and E. Schoch, ''Greedy routing in highway scenarios: The impact of position faking nodes,'' in *Proc. Workshop Intell. Transp. (WIT)*, Mar. 2006, pp. 1–6.

[11] J. Grover, M. S. Gaur, and V. Laxmi, ''Position forging attacks in vehicular ad hoc networks: Implementation, impact and detection,'' in *Proc. 7th Int. Wireless Commun. Mobile Comput. Conf.*, Jul. 2011, pp. 701–706.

[12] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Netw.*, vol. 61, pp. 33–50, Jun. 2017.
[13] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, Apr. 2014.
[14] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A survey of vehicle to everything (V2X) testing," *Sensors*, vol. 19, p. 334, Jan. 2019.
[15] R. W. van der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 779–811, 4th Quart., 2018.
[16] U. Khan, S. Agrawal, and S. Silakari, "A detailed survey on misbehavior node detection techniques in vehicular ad Hoc networks," in *Information Systems Design and Intelligent Applications* (Advances in Intelligent Systems and Computing), vol. 339. New Delhi, India: Springer, 2015, pp. 11–19.
[17] O. A. Wahab, A. Mourad, H. Otrok, and J. Bentahar, "CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks," *Expert Syst. Appl.*, vol. 50, pp. 40–54, May 2016.
[18] O. A. Wahab, H. Otrok, and A. Mourad, "A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles," *Comput. Commun.*, vol. 41, pp. 43–54, Mar. 2014.
[19] F. A. Ghaleb, M. Aizaini Maarof, A. Zainal, M. Rassam, F. Saeed, and M. Alsaedi, "Context-aware data-centric misbehaviour detection scheme for vehicular ad hoc networks using sequential analysis of the temporal and spatial correlation of the consistency between the cooperative awareness messages," *Veh. Commun.*, vol. 20, Dec. 2016, Art. no. 100186.
[20] R. van der Heijden, S. Dietzel, and F. Kargl, "Misbehavior detection in vehicular ad-hoc networks," Univ. Innsbruck, Austria, Tech. Rep., 2013.
[21] F. A. Ghaleb, A. Zainal, A. M. Rassam, and F. Saeed, "Driving-situation-aware adaptive broadcasting rate scheme for vehicular ad hoc network," *J. Intell. Fuzzy Syst.*, vol. 35, pp. 423–438, 2018, Jul. 2018.
[22] N. M. Drawil, H. M. Amar, and O. A. Basir, "GPS localization accuracy classification: A context-based approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 1, pp. 262–273, Mar. 2013.
[23] X. Y. Tian, Y. H. Liu, J. Wang, W. W. Deng, and H. Oh, "Computational security for context-awareness in vehicular ad-hoc networks," *IEEE Access*, vol. 4, pp. 5268–5279, 2016.
[24] B. Iglewicz, "Summarizing data with boxplots," in *International Encyclopedia of Statistical Science*. Berlin, Germany: Springer, 2011, pp. 1572–1575.
[25] R. K. Pearson, Y. Neuvo, J. Astola, and M. Gabbouj, "Generalized hampel filters," *EURASIP J. Adv. Signal Process.*, vol. 2016, p. 87, Jul. 2016.
[26] K. Zaidi, M. Milojevic, V. Rakocevic, and M. Rajarajan, "Data-centric rogue node detection in VANETs," in *Proc. IEEE 13th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Sep. 2014, pp. 398–405.
[27] S. Dietzel, J. Petit, G. Heijenk, and F. Kargl, "Graph-based metrics for insider attack detection in VANET multihop data dissemination protocols," *IEEE Trans. Veh. Technol.*, vol. 62, no. 4, pp. 1505–1518, May 2013.
[28] R. Hussain, S. Kim, and H. Oh, "Privacy-aware VANET security: Putting data-centric misbehavior and sybil attack detection schemes into practice," in *Proc. Int. Workshop Inf. Secur. Appl.* Berlin, Germany: Springer, Aug. 2012, pp. 296–311.
[29] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On data-centric misbehavior detection in VANETs," in *Proc. IEEE Veh. Technol. Conf. (VTC Fall)*, Sep. 2011, pp. 1–5.
[30] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. IEEE INFOCOM 27th Conf. Comput. Commun.*, Apr. 2008, pp. 1238–1246.
[31] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, "Host-based intrusion detection for VANETs: A statistical approach to rogue node detection," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6703–6714, Aug. 2016.
[32] S. A. Soleymani, A. H. Abdullah, W. H. Hassan, M. H. Anisi, S. Goudarzi, and M. A. R. Baee, "Trust management in vehicular ad hoc network: A systematic review," *EURASIP J. Wireless Commun. Netw.*, vol. 1, p. 146, Dec. 2015.
[33] L. Zhengming, C. Chunxiao, and D. Wong, "AWF-NA: A complete solution for tampered packet detection in VANETs," in *Proc. IEEE Global Telecommun. Conf.*, Nov./Dec. 2008, pp. 1–6.
[34] J. Hortelano, J. C. Ruiz, and P. Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs," in *Proc. IEEE Int. Conf. Commun. Workshops*, May 2010, pp. 1–5.
[35] A. Daeinabi and A. G. Rahbar, "Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks," *Multimedia Tools Appl.*, vol. 66, no. 2, pp. 325–338, Sep. 2013.
[36] A. Vulimiri, A. Gupta, P. Roy, S. Muthaiah, and A. Kherani, "Application of secondary information for misbehavior detection in VANETs," in *Proc. Int. Conf. Res. Netw.* Berlin, Germany: Springer, May 2010, pp. 385–396.
[37] R. K. Schmidt, T. Leinmuller, E. Schoch, A. Held, and G. Schafer, "Vehicle behavior analysis to enhance security in vanets," in *Proc. 4th IEEE Vehicle Commun. Workshop (VCOM)*, Jun. 2008. [Online]. Available: https://www.semanticscholar.org/paper/Vehicle-Behavior-Analysis-to-Enhance-Security-in-Schmidt-Leinm%C3%BCller/470b806a3e385be3980f5f1e545d30af51b1359a
[38] T. Leinmuller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 16–21, Oct. 2006.
[39] A. Jaeger, N. Bissmeyer, H. Stubing, and S. Huss, "A novel framework for efficient mobility data verification in vehicular ad-hoc networks," *Int. J. Intell. Transp. Syst. Res.*, vol. 10, pp. 11–21, Jan. 2012.
[40] H. Stübing, A. Jaeger, N. Bissmeyer, C. Schmidt, and S. A. Huss, "Verifying mobility data under privacy considerations in car-to-x communication," in *Proc. 17th ITS World Congr.*, 2010.
[41] H. Stübing, J. Firl, and S. A. Huss, "A two-stage verification process for Car-to-X mobility data based on path prediction and probabilistic maneuver recognition," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Nov. 2011, pp. 17–24.
[42] F. A. Ghaleb, M. A. Razzaque, and I. F. Isnin, "Security and privacy enhancement in VANETs using mobility pattern," in *Proc. 15th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2013, pp. 184–189.
[43] J. Firl, H. Stübing, S. A. Huss, and C. Stiller, "Predictive maneuver evaluation for enhancement of Car-to-X mobility data," in *Proc. Intell. Vehicles Symp. (IV)*, Jun. 2012, pp. 558–564.
[44] F. A. Ghaleb, A. Zainal, and M. A. Rassam, "Mobility information estimation algorithm using Kalman-filter for vehicular ad hoc networks," *Int. J. Inf. Comput. Secur.*, vol. 8, no. 3, pp. 221–240, 2016.
[45] J. Firl, H. Stubing, S. A. Huss, and C. Stiller, "MARV-X: Applying maneuver assessment for reliable verification of car-to-x mobility data," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 3, pp. 1301–1312, Sep. 2013.
[46] N. Biβmeyer, C. Stresing, and K. M. Bayarou, "Intrusion detection in VANETs through verification of vehicle movement data," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2010, pp. 166–173.
[47] H. Stübing, "Facility layer security: Mobility data verification," in *Multi-layered Security and Privacy Protection in Car-to-X Networks*. Wiesbaden, Germany: Springer, 2013, pp. 45–80.
[48] T. Leinmuller, E. Schoch, F. Kargl, and C. Maihofer, "Decentralized position verification in geographic ad hoc routing," *Secur. Commun. Netw.*, vol. 3, no. 4, pp. 289–302, Jul./Aug. 2010.
[49] R. W. van der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," Oct. 2016, *arXiv:1610.06810*. [Online]. Available: https://arxiv.org/abs/1610.06810
[50] F. A. Ghaleb, M. A. Razzaque, and A. Zainal, "Mobility pattern based misbehavior detection in vehicular adhoc networks to enhance safety," in *Proc. Int. Conf. Connected Vehicles Expo (ICCVE)*, Nov. 2015, pp. 894–901.
[51] F. A. Ghaleb, A. Zainal, M. A. Rassam, and F. Mohammed, "An effective misbehavior detection model using artificial neural network for vehicular ad hoc network applications," in *Proc. IEEE Conf. Appl., Inf. Netw. Secur. (AINS)*, Nov. 2017, pp. 13–18.
[52] J. Grover, V. Laxmi, and M. S. Gaur, "Misbehavior detection based on ensemble learning in VANET," in *Advanced Computing, Networking and Security*, P. S. Thilagam, A. R. Pais, K. Chandrasekaran, and N. Balakrishnan, Eds. Berlin, Germany: Springer, 2012, pp. 602–611.
[53] Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-based misbehavior detection in wireless ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 15, no. 8, pp. 1893–1907, Aug. 2016.
[54] X. Li, J. Liu, X. Li, and H. Li, "A reputation-based secure scheme in vehicular ad hoc networks," *Int. J. Grid Utility Comput.*, vol. 6, no. 2, pp. 83–90, 2015.
[55] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, USA, Aug. 2000, pp. 255–265.

[56] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Advanced Communications and Multimedia Security*, B. Jerman-Blažič and T. Klobucar, Eds. Boston, MA, USA: Springer, 2002, pp. 107–121.
[57] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol," in *Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Jun. 2002, pp. 226–236.
[58] M. Ghosh, A. Varghese, A. Gupta, A. A. Kherani, and S. N. Muthaiah, "Detecting misbehaviors in VANET with integrated root-cause analysis," *Ad Hoc Netw.*, vol. 8, no. 7, pp. 778–790, 2010.
[59] K. Lim, K. M. Tuladhar, and H. Kim, "Detecting location spoofing using ADAS sensors in VANETs," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2019, pp. 1–4.
[60] D.-J. Jwo and T.-S. Cho, "A practical note on evaluating Kalman filter performance optimality and degradation," *Appl. Math. Comput.*, vol. 193, pp. 482–505, Nov. 2007.
[61] V. Punzo, M. T. Borzacchiello, and B. Ciuffo, "On the assessment of vehicle trajectory data accuracy and application to the next generation simulation (NGSIM) program data," *Transp. Res. C, Emerg. Technol.*, vol. 19, pp. 1243–1262, Dec. 2011.
[62] H. Huang, D. Zhang, Y. Zhu, M. Li, and M.-Y. Wu, "A metropolitan taxi mobility model from real GPS traces," *J. Universal Comput. Sci.*, vol. 18, pp. 1072–1092, Jan. 2012.
[63] J. Huang and H. S. Tan, "Error analysis and performance evaluation of a future-trajectory-based cooperative collision warning system," *IEEE Trans. Intell. Transp. Syst.*, vol. 10, no. 1, pp. 175–180, Mar. 2009.
[64] S. Dietzel, R. van der Heijden, H. Decke, and F. Kargl, "A flexible, subjective logic-based framework for misbehavior detection in V2V networks," in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw.*, Jun. 2014, pp. 1–6.
[65] J. Grover, N. K. Prajapati, V. Laxmi, and M. S. Gaur, "Machine learning approach for multiple misbehavior detection in VANET," in *Advances in Computing and Communications*, vol. 192. Piscataway, NJ, USA: IEEE, 2011, pp. 644–653.
[66] J. Breu, A. Brakemeier, and M. Menth, "Analysis of cooperative awareness message rates in VANETs," in *Proc. 13th Int. Conf. Telecommun. (ITST)*, Nov. 2013, pp. 8–13.
[67] N. Lyamin, A. Vinel, M. Jonsson, and B. Bellalta, "Cooperative awareness in VANETs: On ETSI EN 302 637-2 performance," *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 17–28, Jan. 2018.
[68] K. Zrar Ghafoor, K. Abu Bakar, M. van Eenennaam, R. H. Khokhar, and A. J. Gonzalez, "A fuzzy logic approach to beaconing for vehicular ad hoc networks," *Telecommun. Syst.*, vol. 52, no. 1, pp. 139–149, Jan. 2013.
[69] D. Lee, S.-W. Chang, and S.-S. Lee, "Velocity based self-configuring time division broadcasting protocol for periodic messages in vehicle-to-vehicle communication," *J. Korean Inst. Commun. Sci. B*, vol. 39, no. 3, pp. 169–179, 2014.
[70] H. J. Qiu, I. W.-H. Ho, K. T. Chi, and Y. Xie, "A methodology for studying 802.11p VANET broadcasting performance with practical vehicle distribution," *IEEE Trans. Veh. Technol.*, vol. 64, no. 10, pp. 4756–4769, Sep. 2015.
[71] FHWA. (2006). *Next Generation Simulation (NGSIM) Vehicle Trajctories Dataset*. [Online]. Available: http://ngsim-community.org/
[72] Y. Hou, P. Edara, and C. Sun, "Modeling mandatory lane changing using Bayes classifier and decision trees," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 2, pp. 647–655, Apr. 2014.
[73] J. A. Hartigan and M. A. Wong, "Algorithm AS 136: A k-means clustering algorithm," *Appl. Statist.*, vol. 28, no. 1, pp. 100–108, 1979.
[74] K. Liu, H. B. Lim, E. Frazzoli, H. Ji, and V. C. S. Lee, "Improving positioning accuracy using GPS pseudorange measurements for cooperative vehicular localization," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2544–2556, Jul. 2014.
[75] N. Bissmeyer, K. Schroder, J. Y. Petit, S. Mauthofer, and K. Bayarou, "Short paper: Experimental analysis of misbehavior detection and prevention in VANETs," *Proc. 5th IEEE Veh. Netw. Conf. (VNC)*, Boston, MA, USA, Dec. 2013, pp. 198–201.
[76] N. Nikaein, S. K. Datta, I. Marecar, and C. Bonnet, "Application distribution model and related security attacks in VANET," *Proc. SPIE*, vol. 8768, Mar. 2013, Art. no. 876808.
[77] N.-W. Lo and H.-C. Tsai, "Illusion attack on VANET applications—A message plausibility problem," in *Proc. IEEE Globecom Workshops*, Nov. 2007, pp. 1–8.
[78] T. Saito and M. Rehmsmeier, "The precision-recall plot is more informative than the ROC plot when evaluating binary classifiers on imbalanced datasets," *PLoS ONE*, vol. 10, Mar. 2015, Art. no. e0118432.
[79] C.-M. Huang and S.-Y. Lin, "Cooperative vehicle collision warning system using the vector-based approach with dedicated short range communication data transmission," *Intell. Transport Syst., IET*, vol. 8, no. 2, pp. 124–134, Mar. 2014.
[80] V. Milanés, S. E. Shladover, J. Spring, C. Nowakowski, H. Kawazoe, and M. Nakamura, "Cooperative adaptive cruise control in real traffic situations," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 1, pp. 296–305, Feb. 2014.
[81] L. Li, D. Wen, N.-N. Zheng, and L.-C. Shen, "Cognitive cars: A new frontier for ADAS research," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 395–407, Mar. 2012.

FUAD A. GHALEB received the B.Sc. degree in computer engineering from the Faculty of Engineering, Sana'a University, Yemen, in 2003, and the M.Sc. and Ph.D. degrees in computer science (information security) from the School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia (UTM), Johor, Malaysia, in 2014 and 2018, respectively. From 2004 to 2012, he was a Lecturer of network and computer engineering with the Sana'a Community College, Yemen. He is involved in different projects with industries related to network and information security. His research interests include vehicular network security, cyber security, intrusion detection, data science, data mining, and artificial intelligence.

Dr. Ghaleb was a recipient of many awards and recognitions, such as the Postdoctoral Fellowship Award from UTM, the Best Postgraduate Student Award from UTM, the Excellence Awards from UTM, and the Best Presenter Award from the School of Computing, Faculty of Engineering, UTM, as well as Best Paper Awards from many international conferences.

MOHD AIZAINI MAAROF received the B.Sc. degree in computer science from Western Michigan University, Kalamazoo, MI, USA, the M.Sc. degree in computer science from Central Michigan University, Mount Pleasant, MI, USA, and the Ph.D. degree in IT security from Aston University, Birmingham, U.K.

He is currently a Professor with the School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia (UTM). He is also the Head of the UTM-CSM Cyber Security X Lab and a member of the Information Assurance and Security Research Group (IASRG), UTM. His research interest includes information system security.

ANAZIDA ZAINAL received the B.Sc. degree in computer science from Rutgers University, NJ, USA, in 1990, and the M.Sc. degree in computer science and the Ph.D. degree in computer science and network security from Universiti Teknologi Malaysia (UTM), Malaysia, in 2000 and 2011, respectively.

She is currently a Senior Lecturer with the School of Computing, Faculty of Engineering, and leading the Information Assurance and Security Research Group (IASRG), UTM. Her research interests include cyber threat intelligence, security analytics, network security, and anomaly detection.

BANDER ALI SALEH AL-RIMY received the B.Sc. degree in computer engineering from the Faculty of Engineering, Sana'a University, Yemen, in 2003, the M.Sc. degree in information technology from OUM, Malaysia, in 2013, and the Ph.D. degree in computer science (information security) from the Faculty of Engineering, Universiti Teknologi Malaysia (UTM), in 2019. His research interests include but not limited to Malware, IDS, network security, and routing technologies.

Dr. Al-Rimy was a recipient of several academic awards and recognitions including but not limited to the UTM Alumni Award, the UTM Best Postgraduate Student Award, the UTM Merit Award, the UTM Excellence Award, the OUM Distinction Award, and the Best Research Paper Award.

FAISAL SAEED received the B.Sc. degree in computer science (information technology) from Cairo University, Egypt, and the M.Sc. degree in information technology management and Ph.D. degree in computer science from Universiti Teknologi Malaysia (UTM), Malaysia. He was a Senior Lecturer with the Department of Information Systems, Faculty of Computing, UTM. He has been an Assistant Professor with the Information Systems Department, Taibah University, Saudi Arabia, since 2017. His research interests include data mining, information retrieval, and machine learning.

TAWFIK AL-HADHRAMI received the M.Sc. degree in IT/applied system engineering from Heriot-Watt University, Edinburgh, U.K., the Ph.D. degree in wireless mesh communication from the University of the West of Scotland, Glasgow, U.K., 2015. He was involved in research at the University of the West of Scotland, Networking Group. He is currently a Senior Lecturer with Nottingham Trent University (NTU), U.K, where he is also a member of the Network Infrastructure and Cyber Security (NICS) Group. His research interests include the Internet of Things (IoT) and applications, network infrastructures and emerging technologies, artificial intelligence, computational intelligence, and 5G wireless communications. He is involved in different projects with industries. He is an Associate Editor of IEEE Access and the IEEE Sensors Journals.