Detecting Vehicle Anomaly in the Edge via Sensor Consistency And Frequency Characteristic

Fei Guo, Zichang Wang, Suguo Du, Huaxin Li, Haojin Zhu, *Senior Member, IEEE*, Qingqi Pei, *Senior Member, IEEE*, Zhenfu Cao, *Senior Member, IEEE*, Jianhong Zhao

***Abstract*—Autonomous vehicles are expected to significantly enhance the human mobility. However, recently researchers have discovered and demonstrated some attacks on vehicles, which have caused a panic among the public. Furthermore, these attacks have demonstrated that the security issue is still one of the major challenges of vehicles. In this paper, we propose a novel edge computing based anomaly detection, coined EVAD, which exploits edge based sensor data fusion to identify the anomaly events. The time domain property, i.e., correlation between different intra-vehicle sensors, and the frequency domain property of sensor data are utilized to judge whether an anomaly has occurred within the vehicle. Especially, to reduce the computation overhead and improve the performance, multiple sensors will be organized as ring architecture, which is a tradeoff of detection accuracy and complexity. In addition, the major components (e.g., anomaly detection module) of EVAD are embedded in edge computing devices, which make the anomaly detection be more efficient and privacy-preserving. Meanwhile, a more appropriate model is generated on the cloud server, of which computation overhead maybe heavy for edge computing devices. This paper evaluates the performance of EVAD under different scenarios, and the experimental results demonstrate its feasibility and efficiency. The average true positive rate achieves 99.5% with 1% false positive rate.**

***Index Terms*—Edge computing, vehicle anomaly detection, consistency, sensor correlation, frequency domain.**

I. Introduction

Modern vehicles have been an indispensable way for human mobility. The large-scale adoption of sensors and Electronic Control Units (ECUs) brings intelligence to modern vehicles and convenience to our daily life. However, attacks targeting modern vehicles have been demonstrated, drawing increasing attention to vehicle security from the academic and the industry. These attacks are mainly through some loopholes on the ECUs, attaching to the inter Controller Area Network (CAN) bus and accessing it through wireless channels and injecting/spoofing instruction messages inside a vehicle. By this way, an attacker can take over the control of the vehicle and deviate its system from a safe operational regime. For instance, Charlie et al. [2] proposed an attack which could control the multi-media, the power system and the braking system of vehicles without any physical access, which caused the recall of millions of vehicles. To thwart attacks on vehicles, many approaches are proposed. For example, the cryptology-based CAN bus protocols are the most intuitive solutions [3]. However, due to the resource-constrained property of CAN bus, the cryptology-based CAN bus no longer meets the high demand of real-time response [4]. Therefore, the practicability of cryptology-based solutions might be limited in the real scenario.

Recently, designing practical and efficient anomaly detection solutions for intra-vehicle systems is becoming an important research topic, because of their advantages of identifying the attacks at an early stage and the ease of being compatible with existing vehicle systems. Machine learning based mechanisms [5], [6] have been proposed to achieve the anomaly detection. In the existing solutions, some behavior patterns of a vehicle are extracted to train a model in non-attack scenarios. Then the model is deployed to discover abnormal patterns and protect the vehicle against the various attacks or invalid ECUs. Considering the fact that, today there are in excess of 100 sensors onboard, which generate massive autonomous vehicle sensor data. Advances in more powerful sensors (camera, lidar) and in-vehicle networking (e.g., Automotive Ethernet) will produce richer data, so a more scalable and time/bandwidth efficient anomaly detection scheme is greatly desired.

In this study, we propose a scalable and efficient vehicular anomaly detection system named EVAD (Edge Computing Based Vehicle Anomaly Detection). EVAD exploits both time domain and the frequency domain property of sensor data as the criterion to detect anomalies. On the one hand, we have observed that some sensors' readings are mutually correlated due to the existence of certain physical phenomena of a vehicle. So abrupt changes of correlations in the time domain can indicate an occurrence of anomalies. On the other hand, when an anomaly occurs, the reading of the abnormal sensor would deviate from its previous readings abruptly, which can be detected in the frequency domain after Fourier transforming. These two properties of vehicular sensor data are utilized to detect vehicle anomalies in this paper. The synthetically

Fei Guo, Zichang Wang, Huaxin Li and Haojin Zhu are with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Minhang, Shanghai, 200240, China(e-mail: zhu-hj@sjtu.edu.cn).

Suguo Du is with the Antai College of Economics and Management, Shanghai Jiao Tong University, Shanghai 200240, China.

Qingqi Pei is with the School of Telecommunications Engineering, Xidian University, Xian, Shaanxi 710071, China.

Zhenfu Cao is with the School of Computer Science and Software Engineering, East China Normal University, Shanghai, China.

Jianhong Zhao is with Yanfeng Visteon, Xuhui, Shanghai, 200223, China.

Fei Guo and Zichang Wang are the co-first authors. Haojin Zhu is the corresponding author.

The preliminary version of this paper titled "Detecting Vehicle Anomaly by Sensor Consistency: An Edge Computing Based Mechanism" was published in the Proceeding of IEEE Global Communications Conference, 2018[1].

Manuscript received XXX, XX, 2015; revised XXX, XX, 2015.

utilized properties of sensor data itself and with others can make the performance of EVAD better.

Furthermore, the correlations of sensors can be organized as a ring architecture that can bring significant advantages to our work. On the one hand, the ring architecture takes multiple in-vehicle sensors into consideration simultaneously, which makes the ring be longer and increases the robustness of the detection mechanism. On the other hand, the ring architecture incurs a lower computation overhead since it avoids some redundant pairwise computation, i.e., a sensor is only compared with its adjacent nodes in the ring.

In addition, EVAD leverages edge computing paradigm to offload the computing task to the nearest edge node, which is expected to further speed up the data aggregation from the multiple on-board vehicle sensors and achieve the real-time anomaly detection. Since the data are processed by edge nodes and won't be uploaded to the cloud server, which requires a long time delay[7], it is expected to prevent sensitive user data, like location privacy, which is a long-standing topic[8], [9], [10], from leaking to un-trusted Internet.

The main contributions of this paper are summarized as follows:

- We present a novel edge computing based vehicle anomaly detection architecture, which is expected to achieve high efficiency, bandwidth resource saving, and privacy preservation, based on emerging edge computing paradigm.
- We present EVAD, a real-time vehicle anomaly detection system, associating with analyzing the multiple correlations between different in-vehicle sensors and the Power Spectral Density (PSD) of sensor data in frequency domain, which is obtained by Fourier transforming.
- We propose some novel and less computation complexity algorithms to generate the anomaly detection model, calculating the correlations, identifying the correlation ring, deciding the thresholds for time and frequency domain analysis to detect anomalies. We utilize the ring architecture to organize the sensor data for speeding up the detection.
- We implement and evaluate the anomaly detection performance of EVAD in different attack scenarios on a real-world vehicular data set, large to 223 GB. Our experimental results quantitatively show that EVAD achieves overall 99.5% true positive rate with 1% false positive rate, and demonstrate the effectiveness and robustness of EVAD.

The remainder of this paper is organized as follows. We introduce some preliminaries in Section II, and Section III describes the framework of the anomaly detection system, EVAD. In Section IV, we illustrate the evaluation and performance of the EVAD, and Section V brings the discussion and future work. Finally, Section VI provides some related work and Section VII concludes the whole paper.

II. Preliminaries

In this section, we take a look at the fundamental of the EVAD to efficiently detect the vehicle anomalies.

A. Controller Area Network

Controller Area Network (CAN), the *de facto* standard in-vehicle network protocol, prompts the modern automobile an integrated system that achieves real-time interactions with roads, vehicles, and people [11]. As the central bus connecting all the ECUs together, CAN contains information of each sensor as long as the related ECU is transmitting messages to the CAN bus. Thus, we can collect information from different ECUs for anomaly detection through CAN bus. On the one hand, the property of broadcast is more suitable for the high demand of real-time communication. On the other hand, any ECUs connected to CAN bus could get or send any messages broadcast on the bus, which could be utilized by the attacker to control the vehicle. Furthermore, the bandwidth of CAN bus is just 1Mb/s. The constriction of communication resources would have limitations on the expansion of ECUs and make the cryptology-based CAN bus protocols are futile, adopted in the vehicle. Moreover, the restriction also proposes a requirement on anomaly detection system not interfering the communication of CAN bus. In this paper, with the employment of the Global Positioning System (GPS) sensor, the Inertial Measurement Unit (IMU) sensor and the external system, the robustness of the anomaly detection system is further improved since these systems are independent from the vehicles. And it is much more difficult for attackers to invade both the ECUs and the external system simultaneously, which make the anomaly detection more practical.

B. Correlation of In-vehicle Sensors.

The correlation between two variables describes how close these two have a relationship with each other. Since vehicles are cyber-physical systems, the correlation between different vehicle sensors reflects how similar they react to the same physical phenomenon, which forms one of the criteria for anomaly detection. For instance, most of vehicles have multiple speed measurements from different sources, such as rotational speed from sensors on wheels, GPS speed measured by location changes, and the speed that is calculated with the assistance of gearbox principal axis. These speed readings should be highly correlated in normal state, otherwise the vehicle is under the anomaly circumstance. Therefore, the correlation of in-vehicle sensors can be used to detect in-vehicle anomaly [12]. In this paper, we propose a novel method that leverages the correlations to detect the anomaly in the early stage. For example, if the tire speed is suddenly and nearly 0 miles/hour while the GPS speed is high (e.g., 40 miles/hour), we would conclude that some anomalies, have occurred since these two values violate the natural correlation between the tire speed and the GPS speed. These correlations bring a natural redundancy for anomaly detection, and the EVAD needn't any other redundant sensor for detection, which would not take any communication burden to CAN bus and also not occupy communication resources of the CAN bus.

C. Frequency Domain Analysis

In electronics, control systems engineering, and statistics, the frequency domain refers to the analysis of mathematical

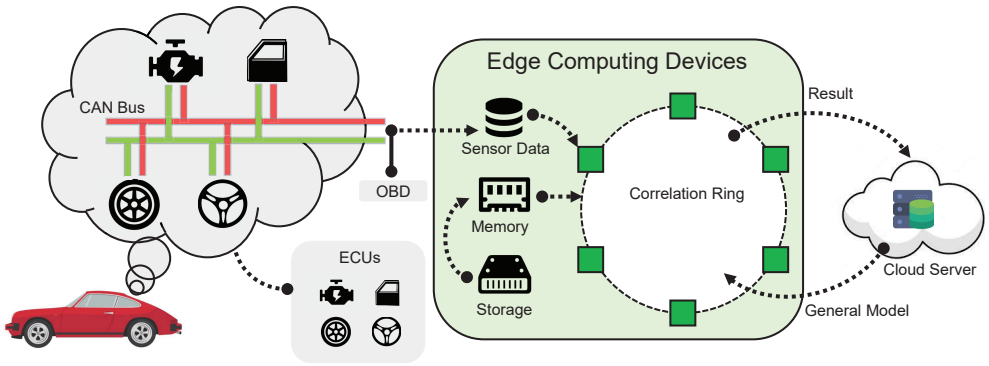


Fig. 1. The system overview.

functions or signals with respect to frequency, rather than time[13]. Put simply, a time-domain graph shows how a signal changes over time, whereas a frequency-domain graph shows how much of the signal lies within each given frequency band over a range of frequencies [14]. Fourier Transform[15], as the following equation, could be used to transform the data in the time domain to frequency distribution in the frequency domain.

$$F(\omega) = \mathcal{F}[f(t)] = \int_{-\infty}^{\infty} f(t)e^{-j\omega t}dt, \quad (1)$$

where $\mathcal{F}[\cdot]$ indicates Fourier transform. ω is the corresponding frequency with the usual meaning of (2π) and j is the unit imaginary number.

The sudden change of sensor data, resulting from anomalies, would interfere with the normal PSD in the frequency domain. The sudden change can be represented by impulse function($\delta(t)$), the Fourier transform of which would be a constant number, as follow.

$$F(\omega) = \mathcal{F}[\delta(t)] = \int_{-\infty}^{\infty} \delta(t)e^{-j\omega t}dt = a(constant). \quad (2)$$

The uniform distribution of impulse function in frequency domain makes the power spectrum distribution of abnormal data in the high-frequency band higher than normal data. Because the distribution of normal data in frequency domain concentrate mainly in the low-frequency band, that in the high-frequency band is nearly zero.

And the additivity of Fourier transforming makes the difference of PSD between anomaly and normal be the PSD of sudden change. So the PSD would be higher in the high-frequency band under the anomaly circumstance.

And the frequency domain property, PSD, is another feature utilized to detect anomalies. The association analysis of time domain and frequency domain could concretely depict the characteristic of sensor data, which could lead to a more efficient anomaly detection.

D. Edge Computing

Edge computing refers to the technology that moves the computations to the edge devices of the network, where the downstream and upstream data are on behalf of the cloud services and Internet of Things (IoT) services respectively [16]. By doing this, only the computing results are required to be transmitted to the cloud server[17]. In this study, we adopt edge computing for efficient anomaly detection due to the following merits. Firstly, computing at the edge of the network saves the bandwidth resources[18], since it saves the efforts of transmitting a huge number of intermediately computational data to the cloud server. Secondly, edge computing achieves shorter response time thanking to a closer distance to data sources and a smaller number of data needed to be transmitted. Thus, it can detect and respond to anomalies more quickly to avoid more severe damage to the vehicles. Thirdly, the edge computing prevents most of the privacy sensitive data from being leaked through a potentially untrusted Internet, because edge computing devices can complete most of the services so that the corresponding sensitive data won't be exposed to Internet. And more, in this paper, the edge computing devices are designed to get the model for anomaly detection from cloud servers in advance. The cloud server undertakes the task for model generation, of which the computation overhead may be heavy for edge computing devices.

III. System Design

In this section, we propose an edge computing based mechanism named EVAD to detect the vehicle anomaly. The architecture of EVAD is shown in Fig. 1, and the EVAD is mostly embedded in the edge computing device to gain the benefits of the edge computing. The edge computing device is an intermediary device between the vehicle and the cloud server. And the edge device is independent to them, so it could protect itself from intrusion. EVAD consists of four modules. In *Data Collection Module*, EVAD connects to the CAN bus through the On-board Diagnostic Interface, monitoring and buffering the messages. In *Model Generation Module*, which is supported by cloud server different from other three modules, EVAD selects appropriate sensor pairs based on the pre-collected data to build a general model for the target vehicle, which consists of a correlation ring, in concrete the sensor selected and their orders, the specific frequency range of PSD and preliminary thresholds for determining whether there is an anomaly. And then cloud server sends the general model to edge computing devices. In *Anomaly Detection Module*, EVAD analyzes sensor data in time domain and frequency

```
main():
  if the vehicle stops:
    waiting;
  load the general model from cloud server;
  start two threads: Detection() and Fetch();
  when the threads exit:
    \\the intermediate data are the average and the
    \\standard deviation of the samples
    save the intermediate data to the storage;
Fetch():
  while(true):
    fetch the messages from the CAN bus;
    extract the data for the correlation analysis;
    if the engine stop:
       exit;
Detection():
  while(true):
    if the data of a period are not collected totally:
      waiting;
    if the detection is the first one:
      load the data from the storage;
    for i in the number of the correlation ring:
      calculate the new PCC Pi_new;
      if  Pi_new<Pi_old & |Pi_new-Pi_old|/(1-Pi_old)>ϵ:
        send out an alarm;
      else:
        calculate the new intermediate data;
      transform the data to frequency domain;
      calculate the power spectral density PSDi(j);
      \\j is the frequency band.
      if the sum of PSDi(j) in specific range > δ
        send out an alarm.
    every 10 times of the period:
      transmit the statement to the transmit terminal;
    if the engine stop:
       exit;
```

Fig. 2. The algorithm of the EVAD.

domain. EVAD calculates the multiple correlations of the variables on each node of the correlation ring using real-time collected data. At the same time, EVAD transforms the sensor data to the frequency domain and calculates the PSD. Associating with the above results, EVAD determines whether an anomaly occurs in the vehicle. Once an anomaly is detected, *Result Submitting Module* enables the edge computing device to alert the driver and transmit the result to the cloud server. The architecture of EVAD is lightweight since there are only two memory blocks: one for buffering the new sensor data and the other for storing *intermediate data*. The whole algorithm of EVAD is shown in Fig. 2 , and we elaborate the details of each module as follows.

A. Data Collection Module

As shown in Fig. 1, the major components of EVAD can be deployed at an edge computing device. And On-Board Diagnostic (OBD) Interface could collect all the vehicle messages[19]. EVAD is designed to passively read CAN messages through the OBD Interface and performs analysis and detection inside the edge computing device that is independent to the vehicle. The sensor data is transformed and decoded from the 0/1 bit stream on CAN bus. Without interfering the normal running of the CAN bus, EVAD is expected to be resilient to the intrusion attacks towards the vehicles. Before launching the anomaly detection, EVAD pre-collects some sensor data, and sends them to *Model Generation Module* which is supported by the cloud server, to generate the general model. Then, in the driving scenario, the real-time collected data are sent to *Anomaly Detection Module* to detect anomalies.

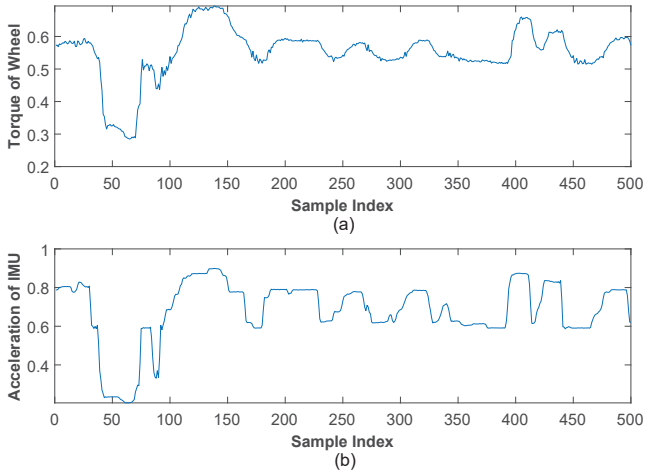


Fig. 3. The top figure shows the torque of wheel and the bottom is the acceleration of IMU, which both are linear normalized. And the PCC of these two sensor data is 0.8733.

B. Model Generation Module

This module is supported by cloud server, and it contains three steps: *correlations computing*, *correlation ring building* and *frequency domain analysis*

1) Correlations Computing: Since correlation between different sensors (e.g., speed of wheel VS GPS speed) is one of the features for EVAD to detect anomalies, it is crucial to choose an appropriate criterion to evaluate the correlations. In this paper, the Pearson Correlation Coefficient (PCC)[20] is chosen to calculate the correlation between different sensors, which is formulated as:

$$Corr = \frac{\sum_{i=1}^{n}(X_i - \overline{X})(Y_i - \overline{Y})}{(n-1)\delta_X \delta_Y}, \tag{3}$$

where n is the length of re-sampled sequences X and Y, and δ_X, δ_Y are the sample standard deviations of X and Y, respectively. Generally, the closer the absolute value of $Corr$ is to 1 (or -1), the more positively (or negatively) linear relevant the two variables are assumed to be. For instance, as shown in Fig. 3, the data from the torque of wheel and the acceleration of IMU are relevant with PCC value of 0.8733. And if $Corr = 0$, it is supposed that there is no correlation between these two variables.

However, directly calculating the PCCs of all sensor pairs suffers from the following limitations. Firstly, since not all pairs of sensors have strong correlations, the pairs of sensors that are tightly correlated should be paid more attention than those irrelevant pairs in our anomaly detection mechanism. Secondly, some correlations might not be directly reflected on sensor readings based on our knowledge. For instance, the PCC between the wheel speed and acceleration is small. However, the PCC between the differential of wheel speed and acceleration or the integral of acceleration and wheel

TABLE I
CORRELATION PAIRS

ID	Variable 1	Variable 2	*Corr*
1	time	GPS time	1.0000
2	speed of left front wheel	speed of left rear wheel	1.0000
3	speed of left front wheel	speed	0.9999
4	speed of left front wheel	speed of right front wheel	0.9998
5	speed	GPS speed	0.9996
6	position of steer	wheel angle	0.9951
7	fuel	integration of GPS speed	-0.9651
8	differential of speed	acceleration	0.9437
9	acceleration of IMU in x-axes	angular velocity of IMU in z-axes	0.9306
10	torque of wheel	acceleration	0.9138
11	acceleration	acceleration of IMU in y-axes	0.9066
12	differential of speed of right front wheel	acceleration	0.8713
13	torque of brake	brake pedal	0.8673
14	wheel angle	angular velocity of IMU in z-axes	0.6558
15	acceleration	throttle pedal - brake pedal	0.6377
16	position of steer	acceleration of IMU in x-axes	0.5331

speed is larger (i.e., 0.8713 in our dataset), which means more correlated. Lastly, some correlations associate with more than two sensors. For example, the acceleration is correlated with the difference between throttle and brake pedal readings, of which PCC is 0.6377, indicating the pair is relevant to some extent.

Therefore, to capture the correlation between sensors via a more efficient way, EVAD firstly identifies the sensor pairs that are related to the same physical phenomenon. In addition, the sensor data in some pairs have been processed empirically such as calculating differential or integral of some sensor data. Then EVAD calculates the PCCs of these selected sensor pairs' data. Table I illustrates some PCCs of sensor pairs from our dataset. And we can find that the correlations between the variables that measure the same physical quantity is close to 1. In other words, they are highly correlated. However, the correlation involving three or more variables is weakly correlated. Note that, the correlation between the left and the right wheel speed is not always 1, since making a turn requires different motions of two side wheels.

2) Correlation Ring Building: After calculating the correlations between sensor pairs, we can detect the vehicle anomaly based on these correlations in some extents. EVAD selects multiple correlations and organizes them in a ring architecture, which has the following advantages. First of all, only the correlations related to the sensors in the correlation ring need to be calculated, thus the computation overhead can be reduced. Then, since the computation complexity of the correlation ring is low, it can perform the detection process involving as many correlations as possible within the limited time and resources. Finally, using the ring architecture ensures every node has been examined twice, improving the accuracy of EVAD.

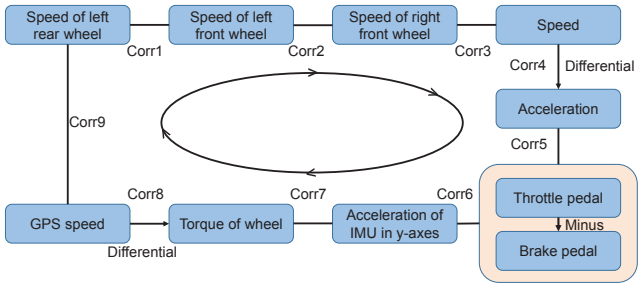


Fig. 4. The correlation ring of EVAD. The correlation ring is comprised of 10 variables and 9 nodes. And the arrow represents that the differential or the integral of the variable at the tail is correlated with that at the head.

The simplest correlation ring contains only three nodes, such as acceleration of IMU in x-axis, angular velocity of IMU in y-axis as well as position of steer in z-axis. To build a more complex correlation ring, an intuitive method is to construct a map structure for all sensor pairs, and find the one with enough correlations. Fig. 4 illustrates one of the correlation rings for our vehicle data, which consists of 10 variables and 9 nodes. In this ring, the difference between the throttle pedal and brake pedal is combined as a node. And the arrow represents that the differential or the integral of the variable at the tail is correlated with that at the head.

3) Frequency Domain Analysis: After building correlation ring, the frequency domain analysis could be utilized as a make up of correlation analysis. This step is just analyzing the data of each sensor itself. At first, we could apply the Fourier transforming to transfer the sensor data in the time domain to frequency domain. Then, we obtain the Power Spectral Density (PSD) of sensor data. PSD is calculated by follow equation[21]:

$$PSD(i, j\omega) = \mathcal{F}[f^2(t)] = \int_{-\infty}^{+\infty} f^2(t) e^{-j\omega t} dt \qquad (4)$$

where i is windows index, and $\mathcal{F}[\cdot]$ indicates Fouier transforming. ω is the corresponding frequency with the usual meaning of (2π) and j is the unit imaginary number.

In order to display the feature intuitively and clearly, the middle and the bottom figures of Fig. 5 show the PSD in logarithm form. As shown in Fig. 5, the PSD of GPS speed is mainly distributed in low frequency band. And to display the PSD difference of GPS speed in anomaly and normal state, the anomaly occurred at the 13041^{st} sample index. The anomaly is generated because of the inaccuracy of sensor perception, which is represented by multiplying some continuous samples by a parameter(e.g. 1.2 in Fig. 5). And we can find that the color of the anomaly in high-frequency band is brighter than which in a normal state. And it demonstrated that the PSD of the anomaly in high-frequency band would be higher than that in a normal state. This is the reason why the feature of PSD is utilized to detect the anomaly. In this paper, we calculated the sum of the PSD in the specific range of high-frequency band as another criterion to detect anomalies.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2907692, IEEE Transactions on Vehicular Technology

C. Anomaly Detection Module

In this module, EVAD analyzes the correlation between different sensors in time domain and the sum of PSD in the specific frequency band in frequency domain simultaneously. After obtaining general model from cloud server, EVAD would totally analyze n variables, where n refers to the number of the nodes in the correlation ring, and generate the detection result, which indicates whether there is an anomaly. Frequency domain analysis would also utilize the variables in the correlation ring.

Whatever a threshold exceeding happens in time domain or frequency domain, it would be judged as an anomaly occurs. To eliminate the impact of noises on the PCC and ensure the sensitiveness of the detection, we employ the sliding window method in the detection. In each time window, totally 1000 samples, which is represented by n_1, are used for calculating every PCC value in time domain and PSD in frequency domain, and the sliding window step contains 100 samples, which is represented by n_2.

In practice, the detection in this module should be time-efficient enough to guarantee that no data from the CAN bus would be piled up. Otherwise, the memory would be exploded due to the accumulation effect of data transmission in a long term. Our evaluation in Section IV will show that the ring architecture is able to meet the requirement of the time efficiency.

1) Correlation Analysis: In this part, EVAD fetches the *intermediate data* from the memory device, which is saved at the end of the last normal driving trip and used in the next detection window. The *intermediate data* includes $Corr_{n_1}$, the average $\overline{X_{n_1}}$ and the standard deviation δ_{n_1} of the former n_1 samples. Then, EVAD calculates the PCCs of the sample set in the new detection window and compares it with the former one for every correlation pairs to adaptively determine whether an anomaly occurs. We introduce the method calculating the PCCs in new detection window as follows.

When the *intermediate data* are fetched, we generate the $Corr$ of all the n_1+n_2 samples with the numerical value of the last n_2 samples. After calculating the average $\overline{X}$ of the n_1+n_2 samples, the standard deviation δ is :

$$\delta = [\frac{1}{n_1+n_2}\sum_{i=1}^{n_1+n_2}(X_i-\overline{X})^2]^{\frac{1}{2}}, \tag{5}$$

Then we have:

$$\begin{aligned}(n_1+n_2)\delta^2 =& \sum_{i=1}^{n_1}[(X_i-\overline{X_{n_1}})^2+2(X_i-\overline{X_{n_1}})(\overline{X_{n_1}}-\overline{X}) \\ &+(\overline{X_{n_1}}-\overline{X})^2]+\sum_{i=n_1+1}^{(n_1+n_2)}(X_i-\overline{X})^2,\end{aligned} \tag{6}$$

where

$$\sum_{i=1}^{n_1}(X_i-\overline{X_{n_1}})^2 = n_1\delta_{n_1}^2, \tag{7}$$

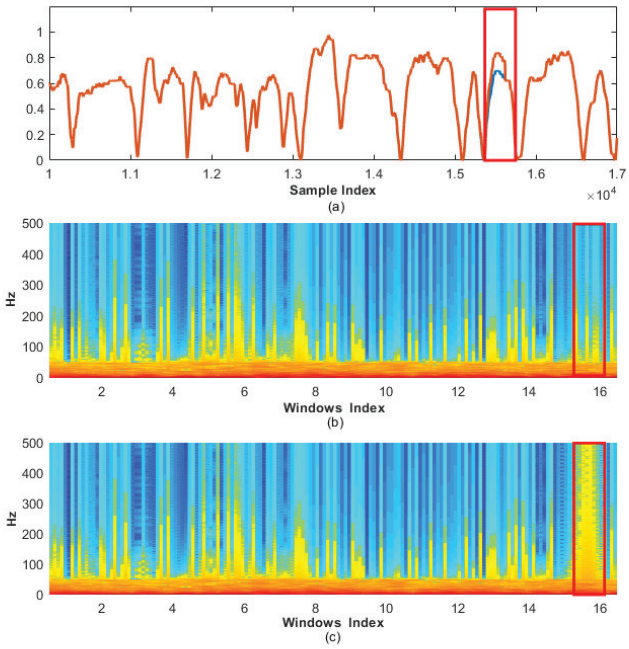


Fig. 5. The top figure shows the data of the GPS speed in normal(blue) and anomaly (orange) state. The anomaly occurs at the 13041^{st} sample index, which is highlighted by a red rectangle. The middle figure shows the PSD of GPS speed in normal state. And the bottom figure shows the PSD of GPS speed in anomaly state, which is highlighted by a red rectangle.

$$\sum_{i=1}^{n_1}[2(X_i-\overline{X_{n_1}})(\overline{X_{n_1}}-\overline{X})] = 0. \tag{8}$$

Since $(\overline{X_{n_1}}-\overline{X})^2$ and $\sum_{i=n_1+1}^{n_1+n_2}(X_i-\overline{X})^2$ are easy to calculate, the standard deviation of all the samples δ can be calculated. Using the same method, $\sum_{i=1}^{n}(X_i-\overline{X})(Y_i-\overline{Y})$ in Eq. (3) can also be calculated. Thus we could obtain the $Corr$ in new detection time window based on the current samples and the *intermediate data* of the former window, which can reduce the computation complexity and overhead of anomaly detection.

After getting the correlations in the i-th time window, EVAD determines whether there is an anomaly detected between the sensor pair according to whether the following two inequalities are both satisfied:

$$Corr_i \le Corr_{i-1} < 1, \tag{9}$$

$$\frac{|Corr_i - Corr_{i-1}|}{1-Corr_{i-1}} \ge \epsilon, \tag{10}$$

where $Corr_i$ and $Corr_{i-1}$ are the correlations in the i-th and $\{i-1\}$-th time window for a certain sensor pair, and ϵ is the threshold to control detection accuracy and false positives. To get the better performance, the threshold could be adjusted according to the environment and the type of the vehicle.

2) Frequency Domain Analysis: In this part, EVAD would firstly transform the sensor data in time domain to frequency distribution in frequency domain and then calculate the PSD of the corresponding n variables. However the density would vary from the physical feature. In other words, the considered range of frequency band would be different to detect anomalies. In this paper, for some variables, we choose the PSD between 101Hz to 500Hz or 401Hz to 500Hz within the scope of consideration. And the sum of PSD in the considered range of frequency band, accumulation diversity, could be more notable for detecting anomalies.

After getting the PSD of the i-th time window, EVAD determines whether there is an anomaly occurring for the corresponding variable, according to whether the following inequality are satisfied:

$$\sum_{j=R_{min}}^{R_{max}} PSD(i, j\omega) > \eta, \tag{11}$$

where R_{min} and R_{max} are the boundaries of the selected specific frequency range, and η is the threshold for frequency domain analysis of the corresponding variable in the general model obtain from the cloud server.

D. Result Submission Module

In this module, EVAD gets the result from *Anomaly Detection Module*. If the vehicle is in a normal state, EVAD would transmit the result to the cloud server in a fixed period without any other operation. Otherwise, EVAD would trigger an alert and the edge computing device would instantly transmit the status to the cloud server. In this module, EVAD can save much bandwidth and energy by transmitting only the essential data. And most of the privacy sensitivity data would not be transported to the cloud server. Therefore EVAD can protect the privacy-sensitive data of users during anomaly detection period. In the meantime, EVAD also validates the connection of the edge computing device and the cloud server through the periodic acknowledgment (ACK) message from the cloud server.

IV. Evaluation

In this section, we evaluate the performance of our proposed EVAD. We first introduce our dataset and demonstrate the feasibility of exploiting PCC and frequency domain analysis to detect vehicle anomaly. Moreover, we evaluate the effectiveness of the anomaly detection of EVAD under different scenarios, and measure the system overhead.

A. Dataset

The dataset is from the Open Sourcing 223GB of Driving Data [22], collected in Mountain View, CA by Lincoln MKZ. The ECU messages in this dataset were collected under different weathers and were recorded by the Robot Operate System (ROS) automatically. We first extract the ECU data from the ROS messages, and then filter the non-significant data, such as the pictures taken by cameras on the vehicle.

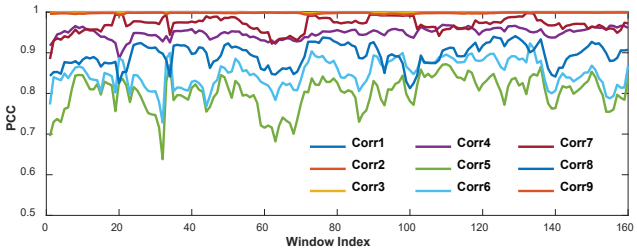
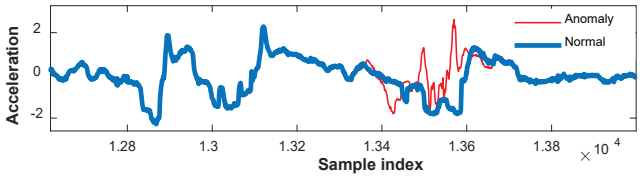
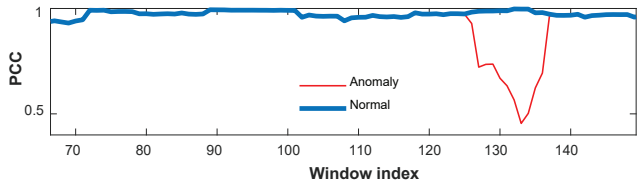


Fig. 6. The PCCs of correlation ring.



(a) Anomaly/normal acceleration of IMU in y-axes



(b) Anomaly/normal PCC

Fig. 7. The acceleration data and the PCC in normal/anomaly scenario.

The processed dataset contains 165 variables and more than 30 million data items. Note that, since the original sample rates of the data are different, we re-sample all the data to 10Hz for analyzing them more efficiently. Furthermore, we utilize linear normalization to eliminate the effect of measurement levels for anomaly detection. Since the original dataset is collected in normal driving scenarios, we generate the anomaly data by modifying the normal data to simulate the anomaly scenarios, which will be introduced in details in the following subsections.

B. Analysis of Effectiveness

In this section, we demonstrate the feasibility of EVAD on detecting vehicle anomalies. The correlation ring extracted from our dataset is shown in Fig. 4.

1) Correlation Analysis: Fig. 6 illustrates the PCC variations in the correlation ring during the normal driving scenarios. It is observed that all PCCs are higher than 0.6, which reveals the strong correlations among all sensors. Therefore, EVAD could regard the vehicle status as normal according to PCCs.

We perform a case study to show the anomaly detection process. In Fig. 7(a), the blue line represents the normal data collected from the IMU in the y-axes while the abnormal data is described in the red line. And the normal PCC between the acceleration of IMU in y-axes and wheel torque (i.e., *Corr7* in Fig. 4) is shown as the blue line in Fig. 7(b).

We can know that the normal PCC in Fig. 7(b) is always higher than 0.9. And then, we simulate abnormal acceleration by replacing the samples around $Sample_{13400}$ with samples

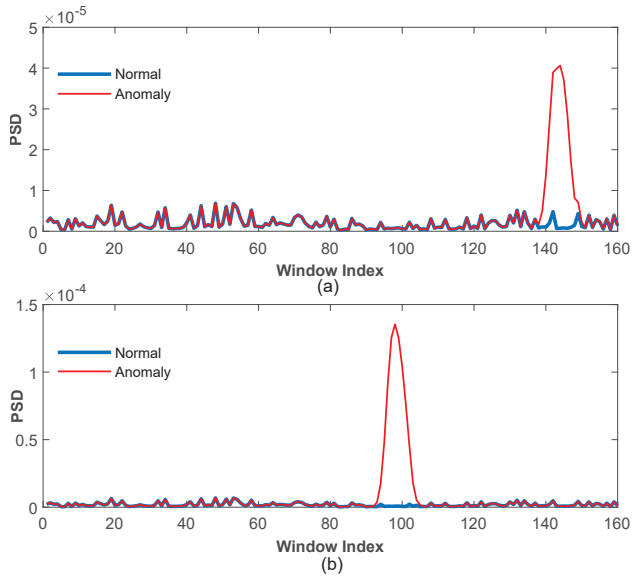


Fig. 8. The sum of the PSD in the specific frequency range of 101Hz to 500Hz. The top figure is in the case, where the anomaly is generated by multiplying 300 samples by 1.2 beginning at a random start. And the bottle figure is in the same case, but the multiplier parameter is 0.5.

collected from another trip, the corresponding PCC being shown as the red line in Fig. 7(b). It is observed that when EVAD calculates the PCC of *Corr7* for the abnormal data, the PCC drops to 0.45 drastically. Therefore, EVAD would judge that there is an anomaly occurring if a dropping cusp of PCC has appeared.

2) Frequency Analysis: To verify the feasibility of utilizing PSD for anomaly detection, in this part, we also analyze the case, where sensor perception is not precise, with the consideration that this case is more difficult to detect than others. Fig. 8 exhibits the sum of PSD in specific frequency range change along with the sliding window moving forward. In Fig. 8, the blue line represents the sum of PSD in the normal state of the speed measured by the left rear wheel. Correspondingly, the red line represents the sum of PSD in the anomaly state. And the multiplier parameters are 1.2 for Fig. 8(a) and 0.5 for Fig. 8(b). For analyzing speed to detect anomaly, we select 101-500Hz as the specific frequency range to add together. From Fig. 8, we can find that no matter the parameter is bigger or smaller than 1, the sum of PSD of the anomaly speed in a specific frequency range would be much bigger than in the normal state clearly. So if we utilize the sum of PSD in specific frequency range to detect anomaly, we only need to compare the sum of PSD with the threshold η. Moreover, we can find that the sum of PSD with the parameter 0.5 is bigger than 1.2. The reason is that the sudden change of 0.5 is greater than 1.2.

C. Overall Performance Evaluation

In this subsection, we evaluate the overall performance of EVAD under different anomaly scenarios. We simulate the abnormal data by modifying the normal data in the following three attack strategies. The first is replacing the continuous samples with the normal data of a different trip. An attack scenario (Scenario A in Fig. 7) related to this strategy is that a sensor is hijacked by the attack and reports the false message. The second strategy is multiplying some continuous samples by a parameter δ (e.g., 1.2 in our experiment). This strategy simulates the scenario (Scenario B) that the sensor is no longer accurate. The final strategy is choosing samples in normal scenarios randomly and intermittently, and replacing them with samples from other trips. This strategy simulates the scenario (Scenario C) that a sensor is suffering from the wireless message injection attack. Some injected messages broadcast on the CAN bus randomly, which is the easiest way in these three strategies.

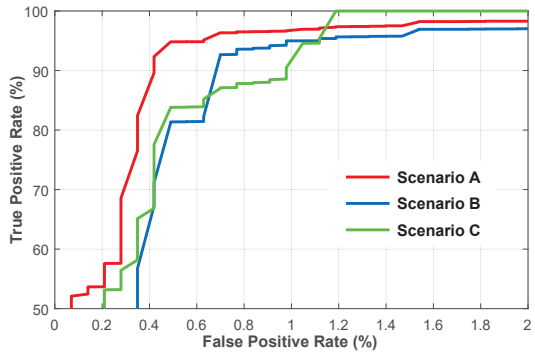


Fig. 9. The ROC curves of the EVAD performance without frequency analysis. Scenario A, B, C are correspondingly replacing continuous samples, multiplying samples, randomly replacing samples respectively.

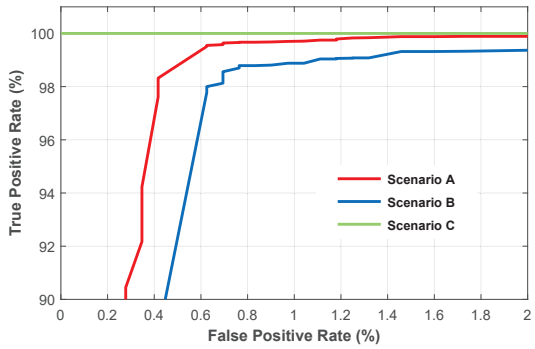


Fig. 10. The ROC curves of the EVAD performance with frequency analysis. Scenario A, B, C are correspondingly replacing continuous samples, multiplying samples, randomly replacing samples respectively.

We test 10000 attacks for each scenario and adjust the parameter ϵ for time domain analysis and η for frequency domain analysis to get the receiver operating characteristic curves (ROC). In each attack of any scenario, we randomly choose a target node (sensor) from the correlation ring, and modify 300 message samples of this node using one of the above three strategies. The performance of anomaly detection without frequency analysis is shown in Fig. 9. Correspondingly, the performance of anomaly detection with frequency analysis is shown in Fig. 10. As shown in Fig. 10, EVAD can achieve the average 99.5% true positive rate with 1% false positive rate (FPR). Even in the worst case (Scenario B), EVAD can still achieve 98.8% true positive rate with 1% FPR. It means that EVAD is promising to accurately detect

anomalies under different scenarios. Different from the method that only utilizing the correlation consistency to detect the anomalies (as shown in Fig. 9), the complementary frequency analysis method could make the detection for scenario C almost achieve 100% accuracy (as shown in Fig. 10). Under the circumstance of that, the 300 injected messages would make 300 sharp spikes in the sensor data. So the violent change in the sensor data would make the PSD in the high-frequency band higher, and thus it was able to be detected with high accuracy, nearly 100%. And in the other two scenarios, the performance with frequency analysis is also higher than without frequency analysis.

Besides, the average time required for performing an anomaly detection is only 31.7ms for the correlation ring with 10 variables in a sliding window. Compared to the anomaly detection time without frequency analysis, which is 3.2ms[1], the time with frequency analysis is also practical. And more, to save the sensor data and the intermediate data of the former moving window, EVAD only needs some Mega Byte memory for the correlation ring with 10 variables. In summary, our experimental results prove the effectiveness and the efficiency of EVAD on detecting vehicle anomalies.

V. Discussion and Future Work

The EVAD combines the merits of pair-wise correlation, ring structure, frequency domain analysis, and edge computing. From the Sec. IV, we can get the conclusion that the EVAD is practical and has a good performance in operating time and detection results. But in this paper, there are some limitations on the EVAD. First, the effect of frequency domain analysis is less useful for the anomaly detection to the nodes, which consist of more than one sensors. The reason is that the addition or the subtraction between sensors maybe eliminate or disturb the frequency distribution feature. Moreover, how to decide the specific range of frequency to detect also need to be studied.

In future, we would consider implement EVAD in the real-world scenario, including communication protocol, computing ability of edge device and so on. In particular, at first, to detect anomalies in edge computing devices, we need to provide computing capability for edge devices and code some program for corresponding services. Moreover, to implement EVAD, we also need to design a protocol for vehicle-edge-cloud communication, including naming, data abstraction, service management and so on. And then, we need to transform and decode the signal on the CAN bus to get the sensor data for anomaly detection. Well leave it to our future work.

VI. Related Work

Vehicle attack. With the prevalence of ECUs in modern vehicles, security issues have been studied by recent researches. Rouf et al. [23] utilized vulnerabilities of Tire Pressure Monitoring Systems (TPMS) to inject spoofed messages illegally turn on the low tire pressure warning lights on a vehicle. The reason behinds this attack is that the TPMS did not employ any countermeasures for intrusion attacks. At the SyScan360 International Forward-Looking Information Security Conference in 2015, hackers demonstrated how to crack Jeep Free Light, Tesla MODEL S and BYD Qin models, respectively, as a challenge to vehicle cyber security[24]. The Keen Lab[25] demonstrated attacks to Tesla motors remotely, which can control arbitrary CAN bus and ECUs without any physical access. More seriously, the Keen Lab demonstrated attacks to Tesla motors remotely again, after Tesla implemented a new security mechanism code signing to do signature integrity check of system firmware that will be FOTAed to Tesla motors in Sept 2016[26]. Recently, Bayerische Motoren Werke AG (BMW) vehicles are suffering from the research of Keen Lab, by whom 14 vulnerabilities with local and remote access vectors in BMW connected cars were found[27].

Defense Mechanisms for vehicles. To enhance the security of modern vehicles against the above attacks, several defense mechanisms have been proposed. Most of them [28], [29] utilized message authentication protocols to protect the messages broadcast on the CAN bus. However, they would make the real-time vehicle systems suffer from heavy communication delays. Furthermore, Lu et al. [30] proposed the method for filtering injected false data in wireless sensor networks. They utilized the random graph metrics of sensor node deployment and the cooperative bit-compressed authentication technique to filtering the injected data which may be applied to intra-vehicle sensor network.

Anomaly detections. Anomaly detection is the first line to protect the cyber-physical systems[31], [12], [32], [33], [34]. Narayanan et al. [35] utilized the Hidden Markov Model to complete the anomaly detection task. Cho et al. utilize the period of CAN frames as the fingerprint to authenticate the validity of ECUs[31] and resist the invalid ECU to send messages on the CAN bus. Moreover, they propose another fingerprint to detect anomalies which identify the attacker ECU by measuring and utilizing voltages on the in-vehicle network [32], and Kenib et al. also utilize the feature to detect anomaly[36]. Ganesan et al. [12] used the cluster analysis and the pair-wise correlation to determine the context and detect the vehicle anomaly. Different from them, in this paper, we utilize the correlation ring and the edge computing technology to build a more efficient and robust anomaly detection mechanism.

VII. Conclusion

In this paper, we propose EVAD, a novel anomaly detection mechanism to enhance vehicle security. EVAD utilizes multiple correlations between different intra-vehicle sensors and the sum of PSD in a specific high-frequency band as the criterion to detect the vehicle anomaly. To reduce the computation overhead and improve the privacy of vehicle information, the correlations are organized in the ring architecture and the edge computing technology is employed. In EVAD, the edge device and the cloud server perform their own functions. Cloud server is responsible for generating general model and edge node for detecting the anomaly in real time according to the model. We perform comprehensive experiments to evaluate the performance of EVAD, and the results show that EVAD can

achieve average 99.5% true positive rate with 1% false positive rate.

ACKNOWLEDGMENT

This work is supported by the National Science Foundation of China under Grant (No. U1636209), the Shanghai Committee of Science and Technology, China (No. 18511111502) and the Xi'an Key Laboratory of Mobile Edge Computing and Security (201805052-ZD3CG36).

REFERENCES

[1] Z. Wang, F. Guo, Y. Meng, H. Li, H. Zhu, and Z. Cao, "Detecting vehicle anomaly by sensor consistency: An edge computing based mechanism," in *Global Communications Communications*. IEEE, 2018.

[2] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, 2015.

[3] A. V. Herrewege, D. Singele, and I. Verbauwhede, "Canauth - a simple, backward compatible broadcast authentication protocol for can bus," in *Ecrypt Workshop on Lightweight Cryptography*, 2011, p. 7.

[4] P. S. Murvay and B. Groza, "Source identification using signal characteristics in controller area networks," *IEEE Signal Processing Letters*, vol. 21, no. 4, pp. 395–399, 2014.

[5] A. Bezemskij, G. Loukas, R. J. Anthony, and D. Gan, "Behaviour-based anomaly detection of cyber-physical attacks on a robotic vehicle," in *International Conference on Ubiquitous Computing and Communications and 2016 International Symposium on Cyberspace and Security*, 2017, pp. 61–68.

[6] H. Li, L. Zhao, M. Juliato, S. Ahmed, M. R. Sastry, and L. L. Yang, "Poster: Intrusion detection system for in-vehicle networks using sensor correlation and integration," in *ACM Sigsac Conference*, 2017, pp. 2531–2533.

[7] H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service-oriented vehicular networks," *IEEE Wireless Communications*, vol. 16, no. 4, pp. 16–22, 2009.

[8] H. Li, H. Zhu, S. Du, X. Liang, and X. . Shen, "Privacy leakage of location sharing in mobile social networks: Attacks and defense," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 646–660, 2018.

[9] H. Li, Q. Chen, H. Zhu, D. Ma, H. Wen, and X. S. Shen, "Privacy leakage via de-anonymization and aggregation in heterogeneous social networks," *IEEE Transactions on Dependable and Secure Computing*, 2017.

[10] H. Li, H. Zhu, and D. Ma, "Demographic information inference through meta-data analysis of wi-fi traffic," *IEEE Transactions on Mobile Computing*, vol. 17, no. 5, pp. 1033–1047, 2018.

[11] J. Zhong, S. Du, L. Zhou, H. Zhu, F. Cheng, C. Chen, and Q. Xue, "Security modeling and analysis on intra vehicular network," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, Sept 2017, pp. 1–5.

[12] A. Ganesan, J. Rao, and K. Shin, "Exploiting consistency among heterogeneous sensors for vehicle anomaly detection," SAE Technical Paper, Tech. Rep., 2017.

[13] S. A. Broughton and K. Bryan, *Discrete Fourier analysis and wavelets: applications to signal and image processing*. John Wiley & Sons, 2018.

[14] Frequency domain. [Online]. Available: https://en.wikipedia.org/wiki/Frequency_domain

[15] R. N. Bracewell and R. N. Bracewell, *The Fourier transform and its applications*. McGraw-Hill New York, 1986, vol. 31999.

[16] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[17] L. Ma, X. Liu, Q. Pei, and Y. Xiang, "Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing," *IEEE Transactions on Services Computing*, 2018.

[18] L. Zhou, L. Yu, S. Du, H. Zhu, and C. Chen, "Achieving differentially private location privacy in edge-assistant connected vehicles," *IEEE Internet of Things Journal*, 2018.

[19] L. Zhou, S. Du, H. Zhu, C. Chen, K. Ota, and M. Dong, "Location privacy in usage-based automotive insurance: Attacks and countermeasures," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 196–211, 2019.

[20] L. I.-K. Lin, "A concordance correlation coefficient to evaluate reproducibility," *Biometrics*, vol. 45, no. 1, pp. 255–268, 1989. [Online]. Available: http://www.jstor.org/stable/2532051

[21] R. G. Brown, P. Y. Hwang *et al.*, *Introduction to random signals and applied Kalman filtering*. Wiley New York, 1992, vol. 3.

[22] Open sourcing 223gb of driving data. [Online]. Available: https://medium.com/udacity/open-sourcing-223gb-of-mountain-view-driving-data-f6b5593fbfa5

[23] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *Usenix Security Symposium, Washington, Dc, Usa, August 11-13, 2010, Proceedings*, 2010, pp. 323–338.

[24] B. Zou, M. Gao, and X. Cui, "Research on information security framework of intelligent connected vehicle," in *Proceedings of the 2017 International Conference on Cryptography, Security and Privacy*. ACM, 2017, pp. 91–95.

[25] Keen security lab of tencent. car hacking research: Remote attack tesla motors. [Online]. Available: https://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/

[26] Keen security lab of tencent. new car hacking research: 2017, remote attack tesla motors again. [Online]. Available: https://keenlab.tencent.com/en/2017/07/27/New-Car-Hacking-Research-2017-Remote-Attack-Tesla-Motors-Again/5

[27] Keen security lab of tencent. new vehicle security research by keenlab: Experimental security assessment of bmw cars. [Online]. Available: https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/

[28] B. Groza, S. Murvay, A. V. Herrewege, and I. Verbauwhede, "Libracan: A lightweight broadcast authentication protocol for controller area networks," *Acm Transactions on Embedded Computing Systems*, vol. 16, no. 3, p. 90, 2017.

[29] O. Hartkopp and R. M. SCHILLING, "Message authenticated can," in *Escar Conference, Berlin, Germany*, 2012.

[30] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen, "Becan: A bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 1, pp. 32–43, Jan 2012.

[31] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection." in *USENIX Security Symposium*, 2016, pp. 911–927.

[32] ——, "Viden: Attacker identification on in-vehicle networks," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 1109–1123.

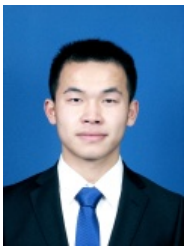
[33] Y. Meng, Z. Wang, W. Zhang, P. Wu, H. Zhu, X. Liang, and Y. Liu, "Wivo: Enhancing the security of voice control system via wireless signal in iot environment," in *Proceedings of the Eighteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ser. Mobihoc '18. ACM, 2018, pp. 81–90.

[34] W. Zhang, Y. Meng, Y. Liu, X. Zhang, Y. Zhang, and H. Zhu, "Homonit: Monitoring smart home apps from encrypted traffic," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. ACM, 2018, pp. 1074–1088.

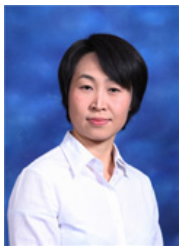
[35] S. N. Narayanan, S. Mittal, and A. Joshi, "Obdsecurealert: An anomaly detection system for vehicles," in *IEEE International Conference on Smart Computing*, 2016, pp. 1–6.

[36] M. Kneib and C. Huth, "Scission: Signal characteristic-based sender identification and intrusion detection in automotive networks," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2018, pp. 787–800.

Fei Guo is currently pursuing the Ph.D. degree in Computer Science and Technology at Shanghai Jiao Tong University, China. He received his master's degree in Computer Science and Technology from Shanghai Jiao Tong University, China,in 2012, and bachelor's degree in Computer Science and Technology from East China Normal University, China in 2010. His research interests include security of Internet of Things and edge computing.



Zichang Wang, is currently a master candidate in department of computer science and engineering, Shanghai Jiao Tong University and he completed his bachelor's degree in computer science from SJTU in 2018. He is now interested in security of vehicle network, edge computing and Internet of Things.



Suguo Du received the Ph.D. degree from the School of Mathematical and Information Sciences, Coventry University, U.K., in 2002. She is currently an Associate Professor with the Department of Management Science, Shanghai Jiao Tong University, China. Her current research interests include risk and reliability assessment, vehicular networks security and privacy protection, and social networks security management. Her research has been supported by the National Science Foundation of China.

Huaxin Li received his two M.Sc. degrees in Department of Computer Science and Engineering, Shanghai Jiao Tong University and Computer and Information Science, University of Michigan, respectively. He received the B.Sc. degree in Department of Computer Science and Engineering, Shanghai Jiao Tong University, China, in 2015. His research interests include vehicular security, social networks privacy, smartphone security, and applied machine learning.

Haojin Zhu (M09SM16) received the B.Sc. degree in computer science from Wuhan University, China, in 2002, the M.Sc. degree in computer science from Shanghai Jiao Tong University, China, in 2005, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Canada, in 2009. Since 2017, he has been a Full Professor with the Computer Science Department, Shanghai Jiao Tong University. His current research interests include network security and privacy enhancing technologies. He published over 40 international journal papers, including JSAC, TDSC, TPDS, TMC, TWC, TVT, and 60 international conference papers, including the ACM CCS, ACM MOBICOM, ACM MOBIHOC, the IEEE INFOCOM, and the IEEE ICDCS. He received a number of awards, including the IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award in 2014, Top 100 Most Cited Chinese Papers Published in International Journals in 2014, the Supervisor of Shanghai Excellent Master Thesis Award in 2014, a Distinguished Member of the IEEE INFOCOM Technical Program Committee in 2015, the Outstanding Youth Post Expert Award for Shanghai Jiao Tong University in 2014, and the SMC Young Research Award of Shanghai Jiao Tong University in 2011. He was a co-recipient of Best Paper Award at the IEEE ICC in 2007 and Chinacom in 2008 the IEEE GLOBECOM Best Paper Nomination in 2014, and the WASA Best Paper Runner-up Award in 2017. He received the Young Scholar Award of Changjiang Scholar Program from the Ministry of Education of P. R. China in 2016.

Qingqi Pei received his B.S., M.S. and Ph.D. degrees in Computer Science and Cryptography from Xidian University, in 1998, 2005 and 2008, respectively. He is now a Professor and member of the State Key Laboratory of Integrated Services Networks, also a Professional Member of ACM and Senior Member of IEEE, Senior Member of Chinese Institute of Electronics and China Computer Federation. His research interests focus on digital contents protection and wireless networks and security.

Zhenfu Cao received the B.Sc. degree in computer science and technology and the Ph.D. degree in mathematics from Harbin Institute of Technology, Harbin, China, in 1983 and 1999, respectively. His research interests mainly include Number Theory, Cryptography and Information Security. Up to now (since 1981), more than 400 academic papers have been published in Journals or conferences.

He was exceptionally promoted to Associate Professor in 1987, became a Professor in 1991 and is currently a Distinguished Professor in East China Normal University, China. He also serves as a member of the expert panel of the National Nature Science Fund of China. He has received a number of awards, including the Youth Research Fund Award of the Chinese Academy of Science in 1986, the Ying-Tung Fok Young Teacher Award in 1989, the National Outstanding Youth Fund of China in 2002, the Special Allowance by the State Council in 2005, and a corecipient of the 2007 IEEE International Conference on Communications-Computer and Communications Security Symposium Best Paper Award in 2007. Prof. Cao is also the leaders of Asia 3 Foresight Program (61161140320) and the key project (61033014) of National Natural Science Foundation of China. He is a senior member of the IEEE.

Jianhong Zhao received his master's degree in automotive electronic from Jilin University in 2005. As a researcher in Tongji University for electric vehicle, then as a lead engineer in SAIC for electric vehicle and intelligent vehicle. Now he is working in Yanfeng Visteon and focused on cockpit electronic and automated driving.