Diagnosing Vehicles with Automotive Batteries

Liang He
University of Colorado Denver

Linghe Kong
Shanghai Jiaotong University

Ziyang Liu
Shanghai Jiaotong University

Yuanchao Shu
Microsoft Research

Cong Liu
University of Texas at Dallas

ABSTRACT

The automotive industry is increasingly employing software-based solutions to provide value-added features on vehicles, especially with the coming era of electric vehicles and autonomous driving. The ever-increasing cyber components of vehicles (i.e., computation, communication, and control), however, incur new risks of anomalies, as demonstrated by the millions of vehicles recalled by different manufactures. To mitigate these risks, we design `B-Diag`, a battery-based diagnostics system that guards vehicles against anomalies with a cyber-physical approach, and implement `B-Diag` as an add-on module of commodity vehicles attached to automotive batteries, thus providing vehicles an additional layer of protection. `B-Diag` is inspired by the fact that the automotive battery operates in strong dependency with many physical components of the vehicle, which is observable as correlations between battery voltage and the vehicle's corresponding operational parameters, e.g., a faster revolutions-per-minute (RPM) of the engine, in general, leads to a higher battery voltage. `B-Diag` exploits such physically-induced correlations to diagnose vehicles by cross-validating the vehicle information with battery voltage, based on a set of data-driven norm models constructed online. Such a design of `B-Diag` is steered by a dataset collected with a prototype system when driving a 2018 Subaru Crosstrek in real-life over 3 months, covering a total mileage of about 1, 400 miles. Besides the Crosstrek, we have also evaluated `B-Diag` with driving traces of a 2008 Honda Fit, a 2018 Volvo XC60, and a 2017 Volkswagen Passat, showing `B-Diag` detects vehicle anomalies with >86% (up to 99%) averaged detection rate.

CCS CONCEPTS

• **Computer systems organization → Sensors and actuators**.

MobiCom '19, October 21–25, 2019, Los Cabos, Mexico

ACM ISBN 978-1-4503-6169-9/19/10…$15.00
https://doi.org/10.1145/3300061.3300126

KEYWORDS

vehicle diagnostics; batteries-as-sensors; CPSes

ACM Reference Format:
Liang He, Linghe Kong, Ziyang Liu, Yuanchao Shu, and Cong Liu. 2019. Diagnosing Vehicles with Automotive Batteries. In *The 25th Annual International Conference on Mobile Computing and Networking (MobiCom '19), October 21–25, 2019, Los Cabos, Mexico.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3300061.3300126

1 INTRODUCTION

• **Background.** The automotive industry is increasingly employing software-based solutions to provide value-added features on vehicles, such as automatic crash response and remote diagnostics, especially with the coming era of (hybrid) electric vehicles and autonomous driving. As a result, modern vehicles are commonly installed with software systems consisting of hundreds of millions of lines of codes distributed across over 80 Electronic Control Units (ECUs) [1, 2], rendering vehicles prototypical cyber-physical systems (CPSes). The ever-increasing cyber components of vehicles, however, prove to be a double-edged sword and incur new risks to vehicles' reliability/safety [3–5].

First, software system becomes error-prone with the ever growing data volume in the in-vehicle network [6–8]. Taking the automatic gear shifting in Fig. 1 as an example:

(a) the vehicle's engine control module first gathers readings of the crankshaft position sensor to calculate the RPM[1],
(b) it then actuates based on the thus-calculated RPM to control the activation frequency of spark plug,
(c) the engine control module also broadcasts the RPM to other ECUs via the in-vehicle network, e.g., in form of the controller area network (CAN) [9],
(d) the transmission control module receives and then processes the broadcasted RPM, and changes gears accordingly.

As can be seen, any software defects in the computation/communication/control of the above process could compromise the gear shifting. Software flaws, unfortunately, have been frequently identified in vehicles: (i) a bug causing unintended

[1]Revolutions per minute (RPM) quantifies the engine speed.

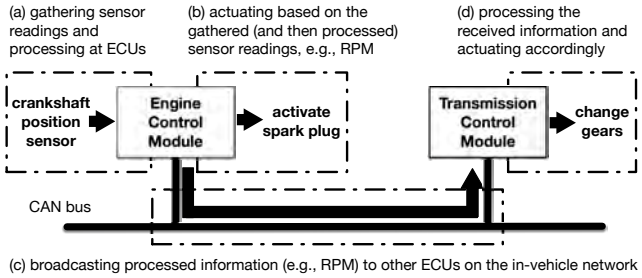


Fig. 1: Vehicle's cyber operations: gathering, processing, transmitting information and actuating accordingly.

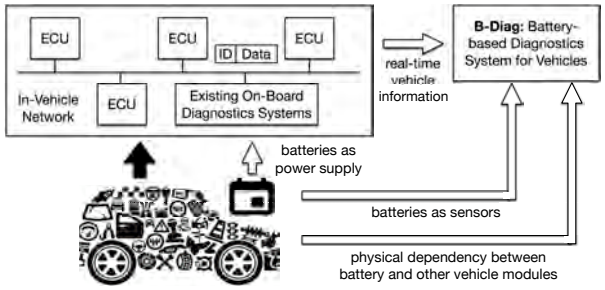


Fig. 2: `B-Diag` diagnoses vehicles with a cyber-physical approach by exploiting automotive batteries as sensors.

acceleration forced Toyota to recall 7.5 million vehicles between 2009–2011 [10], (ii) a glitch unlocking the door without notifying drivers caused Jaguar to recall 65,000 Range Rover in 2015 [11], (iii) defects in the cruise control software caused Chrysler to recall 4.8 million vehicles in 2018 [12], to name a few.

Second, the proliferation of in-vehicle sensing and communication modules eases the inter-connection between cars and third-party devices, thus exposing new vulnerabilities to cyber attacks [13–19]. For example, many work on the injection and modification of data packets in the in-vehicle network through WiFi, Bluetooth, or other cyber interfaces have been reported [20–24]. People have even successfully stopped a Jeep Cherokee on a highway by masquerading its in-vehicle data packets [25], triggering a recall of 1.4 million vehicles by Jeep in 2015 [26].

These risks, albeit of different causes, lead to the same consequence of *unintended information in the in-vehicle network*, referred to as *cyber anomalies*, disrupting the automotive industry and degrading vehicles' reliability/safety.

• **State-of-the-Art.** Vehicle anomalies are traditionally diagnosed with the On-Board Diagnostics System (OBD-II) [27], which however, is ineffective in detecting cyber-induced anomalies, as demonstrated by the fact that many of the above cyber flaws/attacks do not trigger any diagnostic trouble code of OBD-II. To fill this need of anomaly diagnostics, researchers have designed various solutions such as message authentication [28–32] and intrusion detection [33–35]. These solutions, however, still suffer from the following three deficiencies. First, these solutions are defective in systematically exploiting a vehicle's CPS nature [36] — i.e., a system of sub-systems interacted constantly in the cyber and physical spaces — missing a reliable opportunity in vehicle diagnostics, as we will see in this work. Second, these solutions are commonly implemented at vehicles' ECUs as part of the in-vehicle network, and thus also suffer from the risks of anomalies thereof, i.e., the diagnostics systems themselves could be abnormal [31, 37, 38]. Last but not the least, many existing solutions are grounded on an offline knowledge of known vehicle anomalies, thus being defective in adapting to unexpected but inevitable vehicle dynamics [39–43].

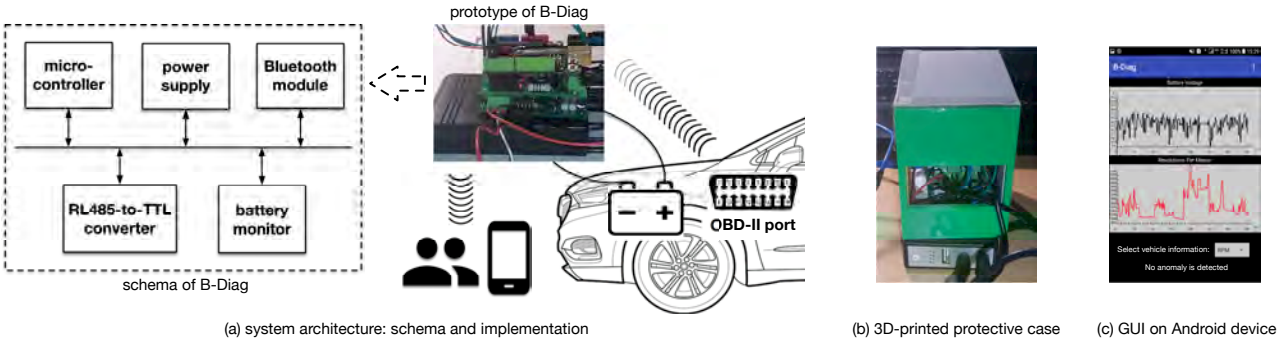
Table 1: A (nonexclusive) list of vehicle information that are corroborated to be diagnosable by `B-Diag`.

Vehicle Information	
1) Absolute Throttle Position B	12) Intake Manifold Pressure
2) Accelerator PedalPosition D	13) Mass Air Flow Rate
3) Accelerator PedalPosition E	14) O2 Sensor1 Equivalence Ratio
4) Air Fuel Ratio (Commanded)	15) O2 Sensor1 Equivalence Ratio (alternate)
5) Air Fuel Ratio (Measured)	16) O2 Sensor1 Wide-Range Voltage
6) Commanded Equivalence Ratio	17) Throttle Position (Manifold)
7) Engine Coolant Temperature	18) Transmission Temperature (Method 1)
8) Engine Load	19) Transmission Temperature (Method 3)
9) Engine Load (Absolute)	20) Voltage (Control Module)
10) Engine RPM	21) Voltage (OBD Adapter)
11) Fuel Level (From Engine ECU)	22) Volumetric Efficiency (Calculated)

• **Battery-based Diagnostics of Vehicles.** To mitigate these deficiencies, we design a battery-based diagnostic system for vehicles, called `B-Diag`, and implement `B-Diag` as an add-on module of commodity vehicles attached to automotive batteries, thus providing vehicles an additional protection on top of the traditional OBD-II (see Fig. 2). `B-Diag` has the following salient properties.

(1) Diagnosing with a Cyber-Physical Approach. The foundation of `B-Diag` is the fact that many physically inter-connected modules of the vehicle operate in close dependency — e.g., a faster engine RPM increases the alternator's output current and then the automotive battery's voltage — which is observable as correlations among the vehicle's operational parameters in the cyber space. `B-Diag` exploits such correlations to diagnose vehicles with a cyber-physical approach by: (i) capturing the physically-induced correlations in the cyber space with data-driven norm models constructed online, and (ii) detecting (and then verify) vehicle anomalies by cross-validating, in real-time, the vehicle information. These online constructed norm models also make `B-Diag` adaptive to the inevitable changes in vehicles.

(2) Exploiting Batteries as Sensors. `B-Diag`'s cross-validation of vehicle information requires a trustworthy ground, to which no information from the in-vehicle network satisfies due to the risks of cyber-induced anomalies. As a mitigation, `B-Diag` novelly grounds its cross-validation on the voltage of automotive batteries by exploiting batteries as sensors: (i) battery voltage can be reliably (and easily)



(a) system architecture: schema and implementation (b) 3D-printed protective case (c) GUI on Android device

Fig. 3: We have prototyped B-Diag as an add-on module of commodity vehicles attached to automotive batteries.

(a) 2018 Subaru Crosstrek (b) attach the prototype to battery (c) OBD-II adapters (d) OBD-II port in vehicle (e) summary of traces

Fig. 4: Using B-Diag's prototype to collect the real-life driving data of a 2018 Subaru Crosstrek.

collected from the physical batteries without going through the in-vehicle network, thus serving as the *hardware-based root of trust* [44] and making the cross-validation *reliable*; (ii) battery operates in strong dependency with many vehicle modules, and thus battery voltage correlates with many vehicle parameters, making the cross-validation *effective*. This way, B-Diag's anomaly detection will be robust and effective even when the in-vehicle network is compromised. Such a battery-based diagnostics of B-Diag also magnifies its practicality because no re-designing of existing in-vehicle network is needed, which is crucial for the cost-conscious automotive industry with only 4–9% profit margin [45]. Table 1 summarizes the vehicle information that has been corroborated to be diagnosable by B-Diag.[2]

The design of B-Diag is steered by a dataset collected with a prototype system when driving a 2018 Subaru Crosstrek in real-life over 3 months, covering a total mileage of about 1,400 miles. Besides the Crosstrek, we have also evaluated B-Diag using driving traces collected from a 2008 Honda Fit, a 2018 Volvo XC60, and a 2017 Volkswagen Passat, showing B-Diag detects anomalies in vehicle information with >86% (up to 99%) detection rate on average. In this paper, we use B-Diag's diagnosis of engine RPM as a complete walk-through example, and then validate B-Diag's ability of individually diagnosing the vehicle information listed in Table 1. An integrated approach to diagnose all vehicle information in real-time, however, is still missing in this work.

2 SYSTEM PROTOTYPING

We have prototyped B-Diag as an add-on module of commodity vehicles attached to their automotive batteries, as shown in Fig. 3(a), including: (i) an Arduino-based micro-controller attached to the automotive battery in the vehicle's engine cabin, (ii) a battery monitor collecting the voltage of the automotive battery in real-time, (iii) a RS485-to-TTL converter transforming the voltage signal and sending it to the micro-controller, (iv) a Bluetooth module collecting the vehicle information from the in-vehicle network — e.g., via the OBD-II port with off-the-shelf OBD-II adapters — and reporting the results to the smartphone of the vehicle's driver/owner, and (v) a power supply supporting the above components. This prototype is installed in a 3D-printed protective case, as shown in Fig. 3(b). Fig. 3(c) shows an example of the prototype's GUI on an Android phone. Note the Bluetooth-based collection of vehicle information from the OBD-II port is only for the ease of implementation. Wired OBD-II adapters are readily available in the literature and could be adopted to further improve the reliability. The total hardware cost of this prototype is below US$50, which could be further reduced, e.g., by using the automotive battery to power the prototype and thus removing the power supply.

We have used this prototype of B-Diag to collect the real-life driving traces of a 2018 Subaru Crosstrek, as shown in Figs. 4(a) and (b). We used four commodity Bluetooth OBD-II adapters (Fig. 4(c)) to collect the vehicle information via the OBD-II port at 10Hz (Fig. 4(d)) and upload the information to B-Diag's prototype. These data are collected over 3 months, on both highway and urban roads, and also when driving during rush hour traffic jams and in snowing/raining weather, as summarized in Fig. 4(e). These data cover most of activities during driving such as turning, breaking, cruise control, operating the vehicle's e-systems such as air con and radio, etc. No abnormal behavior of the vehicle is observed during the collection of these traces, which is also confirmed

[2]Please see [46] for the details of these vehicle information.

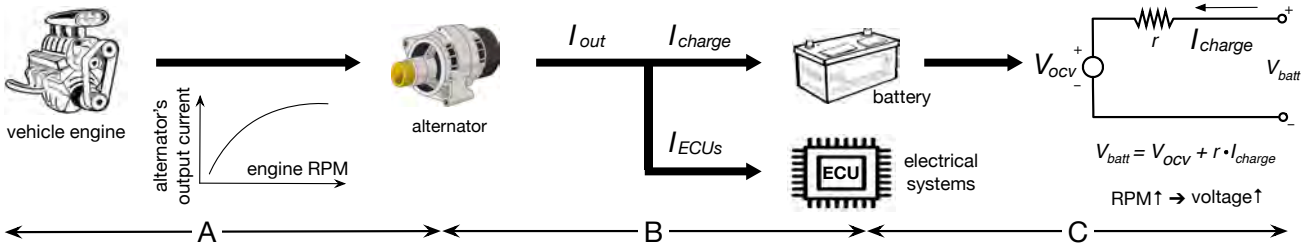


Fig. 5: Other things being equal, a faster engine RPM leads to a higher battery voltage.

when performing its regular maintenance at the auto dealer. This way, we treat these collected traces as normal. We have also identified another Bluetooth OBD-II adapter (not among the four adapters in Fig. 4(c)) that is not reliable in collecting the driving traces. We will use the "abnormal" vehicle information collected with this faulty adapter to evaluate `B-Diag`, as we explain in Sec. 5.1.

Note that such an installment of `B-Diag` is general for all vehicles because (i) all automotive batteries have positive/negative terminals exposed to the environment, via which `B-Diag` can be connected and thus the battery voltage collected; (ii) OBD-II port — under the dash in virtually all modern vehicles — has been mandatory for all vehicles sold in the US since 1996 and Europe since 2001, via which the well-defined vehicle information can be collected in real-time without knowing the vehicle architecture or the format of the in-vehicle messages.

Knowing the hardware components of `B-Diag`, we explain `B-Diag`'s diagnostic algorithms in the next two sections, steered by the above empirically collected driving traces.

3 CASE-STUDY: DIAGNOSING ENGINE RPM WITH BATTERY

We first use `B-Diag`'s detection of anomalies in engine RPM as an example to walk through its diagnostics of vehicles. The related algorithms are also applicable to the detection of anomalies in other vehicle information listed in Table 1, as we elaborate in Sec. 4.

3.1 Automotive Battery and Engine

We first explain the physically-induced correlations between the automotive battery and vehicle's engine.

• **Automotive Battery.** Automotive battery — normally a rechargeable lead-acid battery with 12/24V nominal voltage depending on vehicle type — supplies the necessary current to the starter motor and the ignition system while cranking to start the engine. The battery will be charged by the vehicle's alternator once the engine is running. It is crucial to note that even (hybrid) electric vehicles such as Chevrolet Volt and Bolt — which use high-voltage (e.g., up to 400V) battery packs to supply the driving power — have such low-voltage batteries, ensuring their compatibility to standard 12/24V automotive accessories.

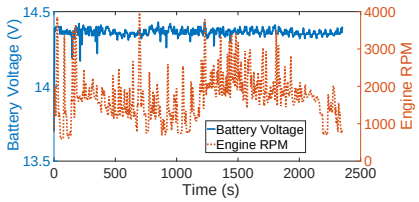
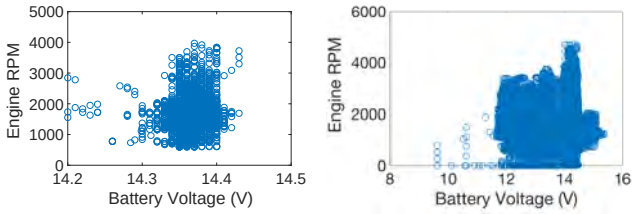


Fig. 6: Exemplary traces of battery voltage and engine RPM.

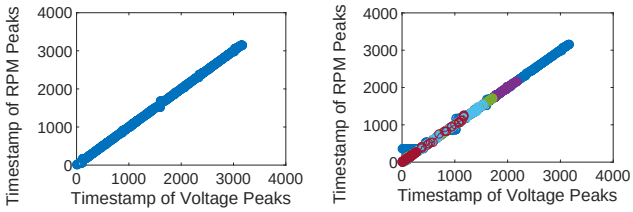
• **Engine RPM.** Revolutions per minute (RPM) is the metric quantifying the engine speed, defined as the number of rotations per minute made by engine's crankshaft and monitored by the crankshaft position sensor in real-time. RPM is crucial to engine's timing functions for ignition, fuel injection, spark events, and valve timing. For example, RPM is needed to determine the activation frequency of spark plugs, normally every 10–17ms [36], to control the fuel injection to each cylinder in real-time. As a result, inaccurate RPMs cause a variety of problems such as misfiring, motor vibration, backfires, hesitant acceleration, abnormal shaking, or, the car may simply do not start [47, 48]. Koscher et al. has experimentally demonstrated the feasibility of fabricating engine RPM via cyber attacks [22], rendering the abnormal RPM a real-life risk. For example, fabricating a large RPM to a low level could falsely convince the Power Steering Control Module (PSCM) that the vehicle is driving slowly, thus tricking PSCM to start a diagnostic session even when driving on a highway, causing critical safety risk [24].

• **Physical Dependency betw. Battery and Engine.** The automotive battery and engine operate in close dependency, as summarized in Fig. 5. First, the engine's rotation triggers that of the alternator at a speed about 1–3 times of engine RPM [49]. The alternator's rotation, in turn, generates an electric power that is monotonic to its rotation speed (up to a certain safe level). This way, a faster RPM leads to a larger output current I_{out} of the alternator (see part-A of Fig. 5) [50]. Second, part of the alternator's I_{out} is used to power the vehicle's electrical systems, and the remaining current charges the battery. Other things being equal, a larger I_{out} increases the battery's charging current (see part-B of Fig. 5). Third, a larger charging current increases the battery voltage. This can be explained by the battery's circuit model shown in Part-C of Fig. 5: the battery will have a voltage of $V_{\text{batt}} = V_{\text{ocv}} + r \cdot I_{\text{charge}}$ when charging with current I_{charge} [51], where r is the internal resistance of the battery.



(a) with the trace in Fig. 6 (b) with all traces in Fig. 4(e)

Fig. 7: Weakly correlated battery voltage and RPM.



(a) with the trace in Fig. 6 (b) with all traces in Fig. 4(e)

Fig. 8: Strongly correlated peaks of battery voltage and RPM.

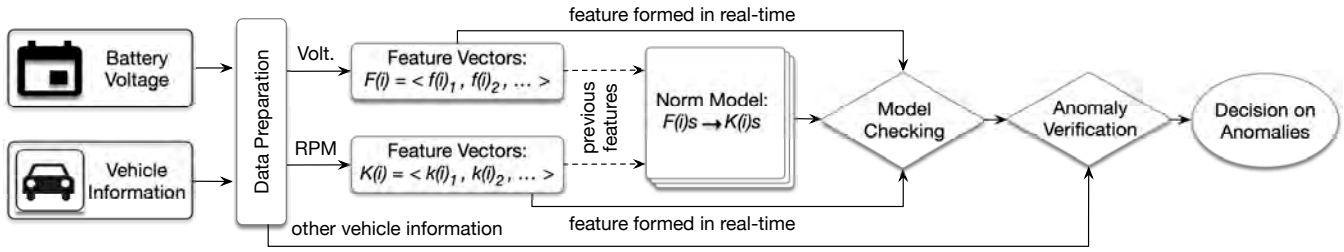


Fig. 9: B-Diag detects (and verifies) the anomalies in engine RPM based on battery voltage with an online data-driven model.

Combining these three facts uncovers a dependency between the automotive battery and engine induced by their physical design/connection — *the battery will has a higher voltage with a faster engine speed.*

• **Correlation betw. Battery Voltage and RPM.** We next examine if such a dependency between battery and engine could be observed as a correlation between the vehicle's corresponding operational parameters.

Observation-I: Weakly Correlated Raw Readings. Fig. 6 plots the traces of battery voltage and engine RPM during a 39-minute driving trip, and Fig. 7(a) shows the corresponding scatter plot, confirming their dependency that a larger RPM, in general, leads to a higher voltage. Significant variance, however, is observed: the battery voltage varies in a wide range of [14.2,14.4]V when the RPM is about 2,000, rendering such a correlation weak. Also, the two traces have only a small Pearson correlation coefficient of 0.06. Fig. 7(b) plots all the voltages and RPMs of the 64 traces summarized in Fig. 4(e), confirming again such *weakly correlated raw readings of battery voltage and engine RPM.* A potential explanation for such a weak correlation is that the battery voltage is affected by, besides the engine RPM, a variety of other factors, such as the power requirements of the vehicle's electrical systems (i.e., I_{ECUs} in Fig. 5), and thus rendering the battery voltage highly dynamic [52].

Observation-II: Strongly Correlated Peaks. We further identify the local maximums of the RPM/voltage readings in Fig. 6, referred to as *peaks*, and then use *dynamic time warping* [53] to align these peaks' time-stamps, as shown in Fig. 8(a). The close-to-diagonal warp path indicates we can find a voltage peak at a similar time whenever an RPM peak is observed, i.e., the peaks of battery voltage and engine RPM are synchronized (and hence correlated). Fig. 8(b) plots the warp paths obtained by aligning the RPM/voltage peaks of all the 64 Crosstrek traces in Fig. 4(e), validating again such *strongly correlated RPM/voltage peaks.* Note that here the correlation between RPM/voltage peaks is in a general sense and not necessarily in terms of the Pearson correlation.

B-Diag exploits the above two correlations between the battery voltage and engine RPM to detect the potential anomalies in RPM readings, as we explain next.

3.2 Detecting RPM Anomalies with Battery

Fig. 9 shows an overview of B-Diag's detection of potential anomalies in engine RPM: taking as input (i) the real-time battery voltage collected from the battery directly and (ii) the engine RPM from the in-vehicle network, B-Diag outputs an online decision value indicating if anomalies are detected in RPM readings. B-Diag conducts such an anomaly detection with three steps: data preparation, norm model construction, and anomaly detection. In what follows, we elaborate on the design of B-Diag using the trace shown in Fig. 6.

• **Data Preparation.** B-Diag applies a set of operations to prepare the collected battery voltage and engine RPM before constructing the norm model.

Data Alignment. B-Diag collects battery information from the battery and vehicle information from the in-vehicle network. Such different approaches of data collection make the collected battery voltage and engine RPM (likely) not aligned in the time domain. B-Diag aligns the data by exploiting the engine's cranking time as the anchor, which can be reliably identified based on the fact that both the battery voltage and engine RPM (i) keep stable before cranking and then (ii) change abruptly and significantly while cranking,

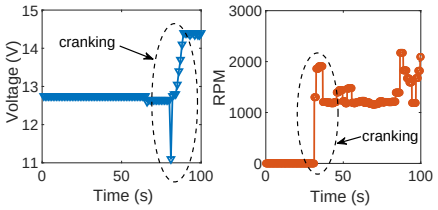


Fig. 10: `B-Diag` **aligns the battery voltage and the engine RPM based on engine's cranking time.**

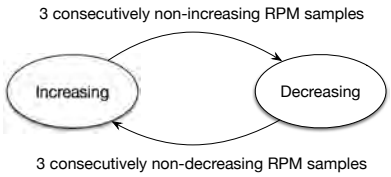


Fig. 11: `B-Diag` **confirms a transition in the trend of RPMs only when observing such a transition with three consecutive RPM samples.**

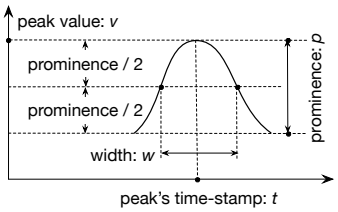


Fig. 12: `B-Diag` **describes a peak with its peak** v**, time-stamp** t**, width** w**, and prominence** p**.**

as shown in Fig. 10. `B-Diag` detects the cranking time by identifying the local min/maximums of voltage/RPM with significant magnitudes and are proceeded by stable readings.

Real-Time Peak Detection. `B-Diag`, besides collecting and recording the battery voltage and engine RPM, also checks the RPM to determine, in real-time, if a new RPM peak is observed, and triggers its diagnostics of potential anomalies if yes. Specifically, `B-Diag` identifies and maintains the current *trend* of RPMs as *increasing* or *decreasing* — a peak is detected if the *trend* changes from *increasing* to *decreasing*. `B-Diag` confirms such a change in *trend* only when it has been observed with three consecutive RPM samples, as illustrated in Fig. 11, reducing the variance in the peak detection caused due to signal dynamics.

Time Window Construction. `B-Diag` maintains the time at which the previous RPM peak is observed, denoted as t_{pre}. Once detecting a new RPM peak, `B-Diag` constructs a time window of $[t_{\text{pre}}-T_w, t_{\text{pre}}]$, where T_w is the window size. The window terminates at t_{pre}, instead of the current time t_{now}, because not all properties of the newly detected RPM peak can be determined at t_{now}, as we explain later.

Peak Identification in Time Window. `B-Diag` fetches the two time-series of battery voltage and engine RPM within the above-constructed time window, and then identifies the peaks therein. `B-Diag` describes each peak by its peak value v, width w, prominence p, and time-stamp t, as illustrated in Fig. 12, i.e., peak $= \{v, w, p, t\}$. `B-Diag` stores the peaks in the current time window to facilitate identification of peaks in the next window, exploiting their (likely) overlapping. Also, `B-Diag` discards the 10% of peaks (in both voltage and RPM) with the least prominence in the window, further improving its tolerance to the inherent dynamics of voltage and RPM readings. Note that neither the width or the prominence of a peak can be determined upon its detection. This is why the time window ends at the time of previous peak.

• **Norm Model Construction.** `B-Diag` constructs an online norm model capturing the relationship between the battery voltage and engine RPM, based on the two correlations observed in Sec. 3.1. Instead of manually constructing rules that map the battery voltage to RPM, we opted to use a machine learning-based classifier to increase the accuracy of `B-Diag`'s mapping. Specifically, `B-Diag` abstracts each of the two sub-traces of battery voltage and RPM in the time window to a 10-parameter feature vector, i.e.,

$$F = \{f_1, f_2, \cdots f_{10}\} \text{ for battery voltage,}$$
$$G = \{g_i, g_2, \cdots g_{10}\} \text{ for engine RPM,}$$

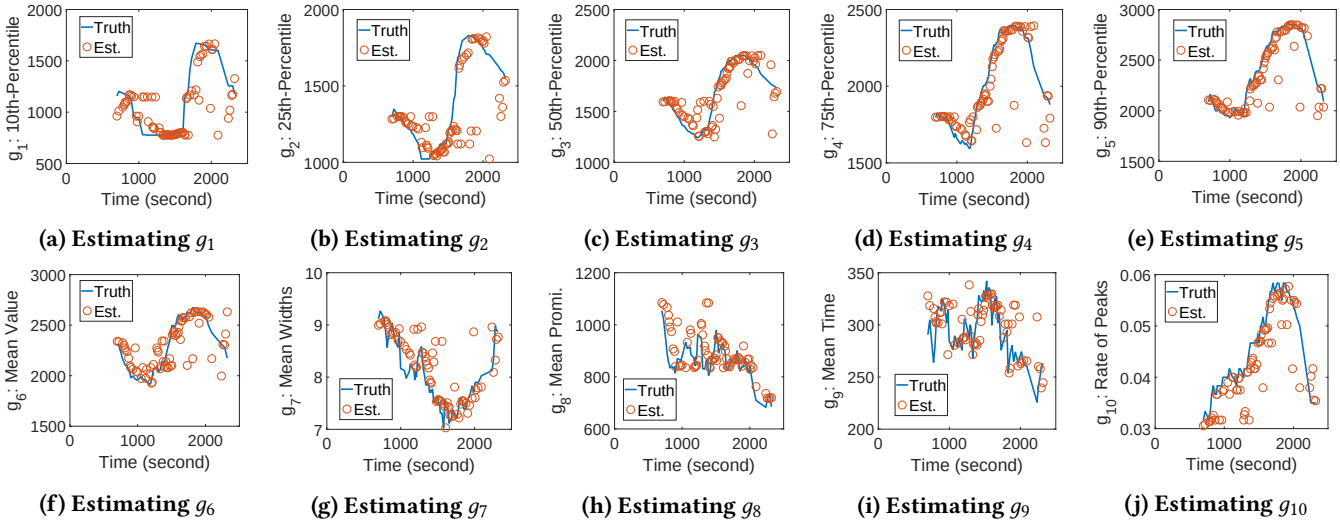
and constructs a norm model that estimates Gs based on Fs.

Feature Extraction. `B-Diag` forms its feature vectors of Fs and Gs based on the two correlations observed in Sec. 3.1: (i) defining f_1–f_5 and g_1–g_5 based on the weakly correlated raw readings of voltage and RPM, thus facilitating the detection of RPMs' unusual values; (ii) defining f_6–f_{10} and g_6–g_{10} based on the strongly correlated peaks of voltage and RPM, thus facilitating the detection of RPMs' unusual dynamics. The weakly correlated raw readings of battery voltage and RPM indicates the feasibility to infer RPMs based on battery voltage, but the accuracy of such an estimation may be limited. As a mitigation, `B-Diag` uses the statistics, instead of the raw values, of voltage/RPM readings to form the first part of its feature vectors. Specifically, for each time window, `B-Diag` uses the $[10, 25, 50, 75, 90]$% percentiles of the voltage and RPM readings as f_1–f_5 for F and g_1–g_5 for G, respectively. `B-Diag` forms the second part of its feature vectors based on the strongly correlated peaks of voltage and RPM. Specifically, for each time window, `B-Diag` uses the mean of the voltage/RPM peaks' value as f_6/g_6, width as f_7/g_7, prominence as f_8/g_8, relative time-stamp as f_9/g_9, and the ratio of their counts over the window size as f_{10}/g_{10}. The relative time-stamp of a peak is defined as its relative position in the current time window, i.e., $t_{\text{r}} = t - (t_{\text{pre}} - T_w)$ where t is the peak's time-stamp. Also, `B-Diag` defines f_{10} and g_{10} as the normalized peak counts to the window size — i.e., the rate at which peaks are observed — to reduce its dependency to the particular setting of window size.

This way, by constructing two feature vectors for each time window, `B-Diag` transforms the two time-series of battery voltage and engine RPM into another two time-series of their corresponding feature vectors, i.e.,

$$\mathbb{F} = \{F^1, F^2, \cdots\} \text{ for battery voltage,}$$
$$\mathbb{G} = \{G^1, G^2, \cdots\} \text{ for engine RPM.}$$

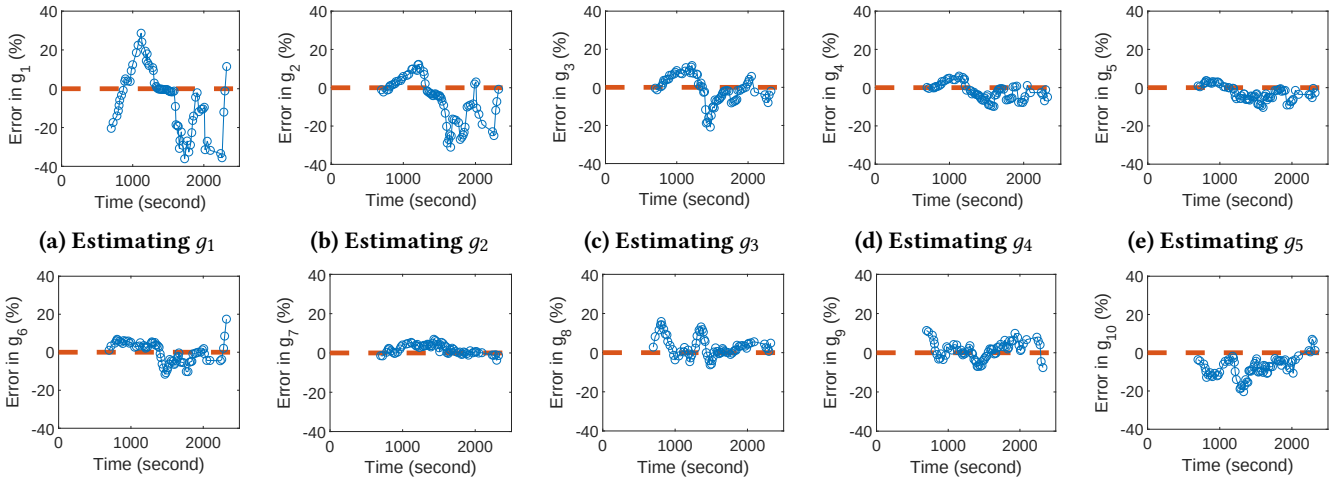
Classifier. `B-Diag` uses machine learning-based classifiers to construct a norm model that maps from $\mathbb{F}$ to $\mathbb{G}$. We opted



(a) Estimating g_1 (b) Estimating g_2 (c) Estimating g_3 (d) Estimating g_4 (e) Estimating g_5

(f) Estimating g_6 (g) Estimating g_7 (h) Estimating g_8 (i) Estimating g_9 (j) Estimating g_{10}

Fig. 13: Estimating the features of engine RPM based on those of battery voltage, with the traces in Fig. 6 as an example.



(a) Estimating g_1 (b) Estimating g_2 (c) Estimating g_3 (d) Estimating g_4 (e) Estimating g_5

(f) Estimating g_6 (g) Estimating g_7 (h) Estimating g_8 (i) Estimating g_9 (j) Estimating g_{10}

Fig. 14: An averaged error of 0.8–11% is achieved when estimating the features of RPM based on battery voltage, but with significant variance.

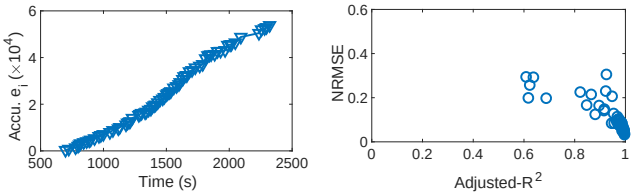
to use *decision tree* as the classifier because of its simplicity and high interpretability.[3] Again, taking the traces in Fig. 6 as an example and with a 10-minute time window, Fig. 13 plots the results when estimating $\mathbb{G}$, or more specifically the g_is in each of the feature vector $G \in \mathbb{G}$, based on $\mathbb{F}$. Fig. 14 summarizes the estimation errors normalized to the corresponding true values (i.e., the error ratios): (i) the errors are clustered around 0 and thus accurate, e.g., the mean errors when estimating g_1–g_{10} are within $[0.8, 11]$%; (ii) variance, however, is observed in both the estimation errors of individual g_is and across different g_is, thus requiring further mitigation when grounding `B-Diag`'s anomaly detection on these errors.

[3]We have tried other classifiers such as KNN and SVM, and observed no clear advantages over the decision tree.

• **Anomaly Detection.** For the i-th time window (and the corresponding feature vectors F^i and G^i), `B-Diag` trains a tree-based model based on the previous feature vectors (i.e., F^1 to F^{i-1} and G^1 to G^{i-1}), and then uses the trained model to estimate G^i based on F^i — an anomaly in RPM is detected if the empirically collected $G^i = \{g^i_j\}$ deviates significantly from the model estimated $\hat{G}^i = \{\hat{g}^i_j\}$ ($j = 1, 2, \cdots, 10$). Specifically, `B-Diag` defines the error of estimating G^i as

$$e_i = ||G^i - \hat{G}^i|| = \sum_{j=1}^{10} \sqrt{(\hat{g}^i_j - g^i_j)^2}/g^i_j \times 100\%. \quad (1)$$

Such a summation of individual estimation errors of g_js suppresses their relatively large variance observed in Fig. 14. To



(a) Accumulated e_is obtained with the traces in Fig. 6, showing clear linearity

(b) Fitting accumulated e_is linearly with all traces in Fig. 4(e)

Fig. 15: The accumulated e_is (see Eq. (1)) increase linearly.

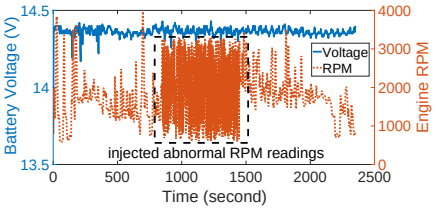


Fig. 17: Adding anomalies to genuine RPM readings in Fig. 6.

collaborate this, Fig. 15(a) plots the accumulated e_is obtained with the traces shown in Fig. 6, which increases steadily and linearly. Fig. 15(b) plots the goodness-of-fit when fitting the accumulated e_is linearly for each of the 64 traces summarized in Fig. 4(e). The fact that all the fitting results are clustered at the right-bottom corner of the figure — i.e., with close-to-1 Adjusted-R^2 and close-to-0 NRMSE — validates the high fitting goodness and thus the linearity of accumulated e_is.

This linearity of accumulated e_is allows `B-Diag` to describe it as a linear regression model. A linear parameter identification problem is thus formulated as

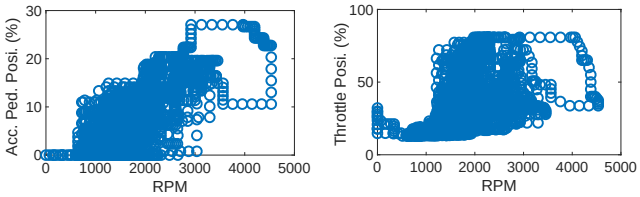
$$E_{\text{acc}}[i] = S[i] \cdot t[i] + \delta[i], \tag{2}$$

where for the i-th time window ending at time $t[i]$, $E_{\text{acc}}[i]$ is the accumulated e_is, $S[i]$ is the regression parameter, and $\delta[i]$ is the identification error. The regression parameter S represents the slope of the linear model and thus the averaged e_i over time. The identification error δ represents the residual which is not explained by the model. `B-Diag` uses the Recursive Least Squares (RLS) algorithm to solve such a linear regression. Also, the reliable linear model of accumulated e_is indicates the corresponding identification error δs should be small and stable in the normal cases, motivating `B-Diag` to make its decision on anomaly detection based on δs. Specifically, `B-Diag` defines

$$\tau_i = |\delta_i - \mu(\delta_1 : \delta_{i-1})| / \sigma(\delta_1 : \delta_{i-1}), \tag{3}$$

i.e., τ_i is the deviation of δ_i from the mean of $\{\delta_1, \cdots, \delta_{i-1}\}$ in terms of their standard deviation, and concludes an anomaly in RPM is detected if $\tau_i > \theta$. We set θ=5 by default [35, 54].

• **Anomaly Verification.** `B-Diag` further verifies the detected anomalies by exploiting the fact that engine RPM, besides correlates strongly with the battery voltage, also correlates with other vehicle parameters. For example, we have



(a) RPM v.s. acc. pedal

(b) RPM v.s. throttle position

Fig. 16: `B-Diag` verifies the detected RPM anomalies based on the correlations between RPM and other vehicle information, e.g., accelerator pedal position and throttle position.

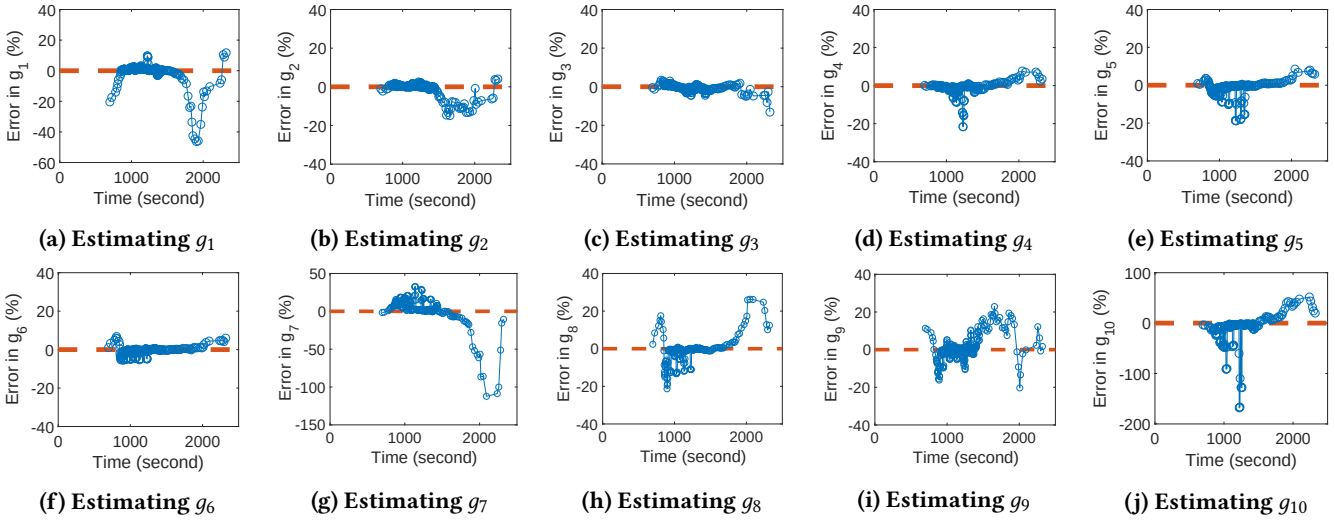
identified the physically-induced correlations between RPM and the accelerator pedal position and throttle position, as shown in Fig. 16. `B-Diag` further exploits these non-battery correlations with RPM to verify the above-detected RPM anomalies, based on the hypothesis that RPM anomalies, besides causing abnormal behavior with regard to the battery voltage, will also cause its abnormal behaviors with regard to other correlated vehicle information. `B-Diag` conducts such an anomaly verification, again, via norm model construction and then checking, with similar approaches explained above. `B-Diag` will confirm the detected RPM anomalies if abnormal behaviors between RPM and any of these correlated vehicle information is detected.

• **Walk-Through Example.** Next we use a walk-through example to show how `B-Diag` detects and then verifies anomalies in engine RPM based on the battery voltage. Specifically, we emulate RPM anomalies by injecting randomly fabricated RPM readings into the traces in Fig. 6, and test if `B-Diag` can detect such anomalies. Fig. 17 plots the altered RPM trace after injecting anomalies during the time period of [849, 1449]s. Applying `B-Diag` to the thus-altered trace with a window size of 600s, Fig. 18 plots the errors when estimating RPM's feature parameters based on those of the battery voltage, showing much degraded accuracy at $\{g_5, g_7, g_8, g_9, g_{10}\}$ when compared to Fig. 14.[4] Fig. 19 plots the accumulated estimation errors — i.e., e_is as defined in Eq. (1) — showing the injected anomalies change the slope of the accumulated e_is, and thus being detectable. Note that no anomaly is detected when applying `B-Diag` to the raw traces in Fig. 6, and thus no false detection is caused. We further verify the detected RPM anomalies by cross-validating with the accelerator pedal position and throttle position, which are confirmed with the changed slopes of accumulated e_is (see Fig. 20).

4 DIAGNOSING VEHICLE BEYOND RPM

We have used the detection of RPM anomalies with battery voltage to walk through `B-Diag`'s cyber-physical approach of vehicle diagnostics. Besides the engine, physical dependencies with the automotive battery also exists at other vehicle

[4]The specific feature parameters with degraded estimation accuracy will depend on the particular anomalies.



(a) Estimating g_1 (b) Estimating g_2 (c) Estimating g_3 (d) Estimating g_4 (e) Estimating g_5

(f) Estimating g_6 (g) Estimating g_7 (h) Estimating g_8 (i) Estimating g_9 (j) Estimating g_{10}

Fig. 18: The abnormal RPMs in Fig. 17 magnify the errors when estimating $\{g_5, g_7, g_8, g_9, g_{10}\}$, when compared to Fig. 14.

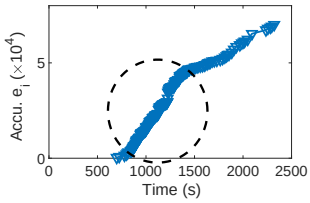


Fig. 19: Abnormal RPMs change the slope of the accumulated e_is with regard to battery voltage, and thus being detectable.

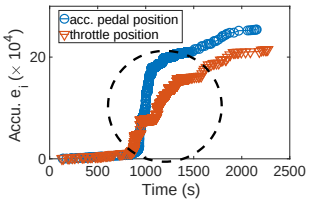


Fig. 20: Abnormal RPMs change the slopes of the accumulated e_is regarding to acc. pedal position and throttle position.

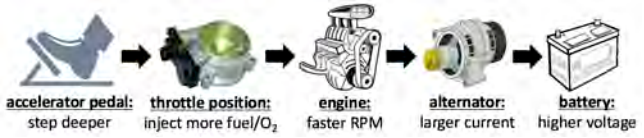


Fig. 21: Physically-induced correlations among a vehicle's accelerator pedal, throttle, engine, alternator, and battery.

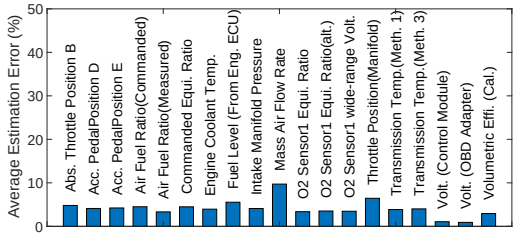


Fig. 22: Errors in estimating feature vectors of vehicle information listed in Table 1 (besides those relate to engine RPM).

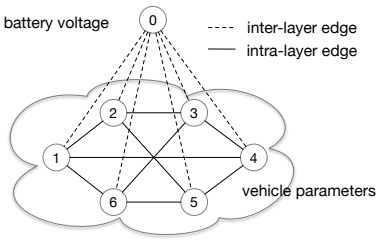


Fig. 23: B-Diag uses a correlation graph to abstract the vehicle and the correlations thereof.

modules, thus offering opportunities to generalize B-Diag's anomaly detection to other vehicle information. Specifically, examining the physical inter-connection among vehicle's sub-systems, Fig. 21 shows a dependency diagram among vehicle's accelerator pedal, throttle, engine, alternator, and battery. Steered by this dependency diagram, we further checked the related vehicle information collected when driving the Crosstrek, and confirmed the correlations with the battery voltage at the information listed in Table 1. As an example, Fig. 22 plots the averaged error when estimating the vehicle information listed in Table 1 (besides those relate to engine RPM), or more specifically their feature vectors, based on the traces collected during the same trip as with Fig. 6 , showing averaged errors within [0.9, 9.7]%. Note that Fig. 21 may not be thorough in capturing the physical dependency among vehicle's sub-systems, and thus Table 1 may not be exclusive. These multi-modal correlations between battery voltage and other vehicle information enable B-Diag to act as a comprehensive diagnostic system for vehicles.

To facilitate the systematic exploitation of these physically-induced correlations for vehicle diagnostics, B-Diag abstracts the vehicle with a 2-layer correlation graph $\mathbb{G}_{\text{corr}} = \{V, E\}$, in which: (i) the vertex set V represents the operational parameters of the vehicle with the battery voltage at the upper layer and other vehicle parameters at the lower layer; (ii) the edge set E captures the correlations among vehicle parameters, i.e., an edge $e_{i,j}$ connecting vertex v_i and v_j exists in E if v_i and v_j are correlated. Fig. 23 shows an exemplary correlation graph.

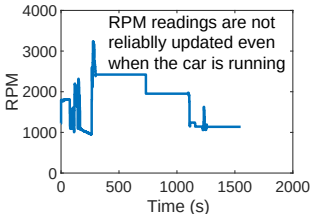


Fig. 24: RPM collected with an unreliable adapter.

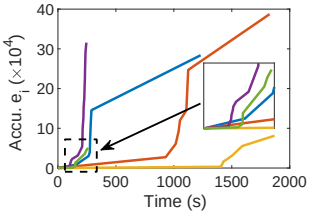


Fig. 25: Accu. e_is of engine RPM with abnormal traces.

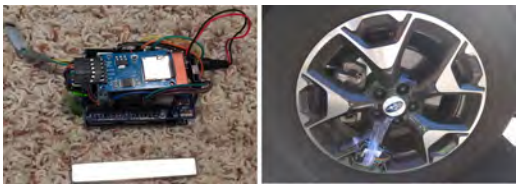
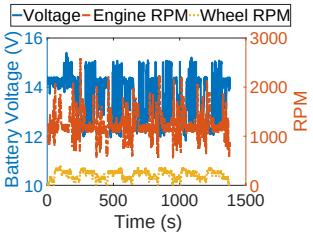
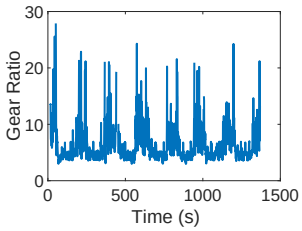


Fig. 26: Attach a Hall-based RPM sensor to the wheel.



(a) Raw traces



(b) Gear ratio

Fig. 27: Emulating abnormal engine RPM with wheel's RPM.

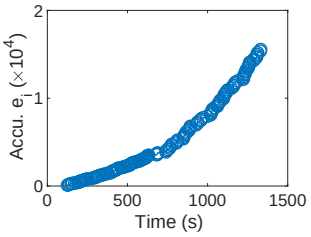


Fig. 28: Accumulated e_is of emulated anomalies.

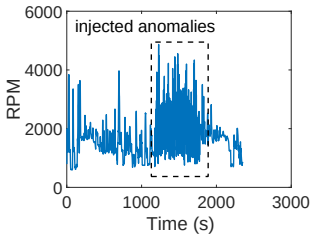


Fig. 29: Example on injected abnormal RPM with AM-2.

This 2-layer correlation graph facilitates exploiting the uniqueness of automotive batteries to diagnose vehicles: (i) battery voltage can be directly (and easily) collected from the battery without going through the in-vehicle network, thus being tolerable to the risks of cyber-induced anomalies thereof and serving as a trustworthy ground for B-Diag's diagnostics of vehicles; (ii) battery draws power from the alternator and supplies power to the vehicle's electrical systems, implying strong correlations between battery voltage and many vehicle parameters. As a result, the correlation graph consists of two types of edges: the *inter-layer edges* representing the correlations between battery voltage and other vehicle parameters, and the *intra-layer edges* capturing the pairwise correlations between vehicle parameters besides battery voltage. Note the correlation graph also defines B-Diag's ability/limit of diagnosing vehicles, i.e., which vehicle modules/parameters B-Diag can guard.

With such an abstracted correlation graph $\mathbb{G}_{\text{corr}}$, B-Diag's detection/verification of anomalies at each vehicle information is transformed to the construction (and then checking) of the data-driven norm model(s) defined by the corresponding inter/intra-layer edges. This way, B-Diag can take a round-robin approach to check the individual inter-layer edges of $\mathbb{G}_{\text{corr}}$ for anomaly detection: substituting the engine RPM in Sec. 3 with the target vehicle information and detecting/verifying the anomalies thereof with similar approaches.[5]

5 EVALUATIONS

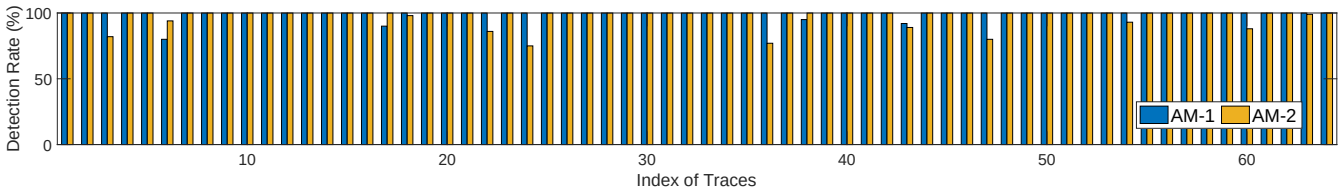
We have evaluated B-Diag with four vehicles: a 2018 Subaru Crosstrek, a 2008 Honda Fit, a 2018 Volvo XC60, and a 2017 Volkswagen Passat. The major challenge in B-Diag's evaluation is the short of real-life cases on vehicle anomalies, gathering of which incurs safety risks. We mitigate this by evaluating B-Diag with (i) anomalies caused by an unreliable OBD-II adapter, (ii) emulated anomalies based on wheel's RPM, and (iii) simulated anomalies by injecting fabricated values to normal vehicle traces.

5.1 B-Diag against "True" Anomalies

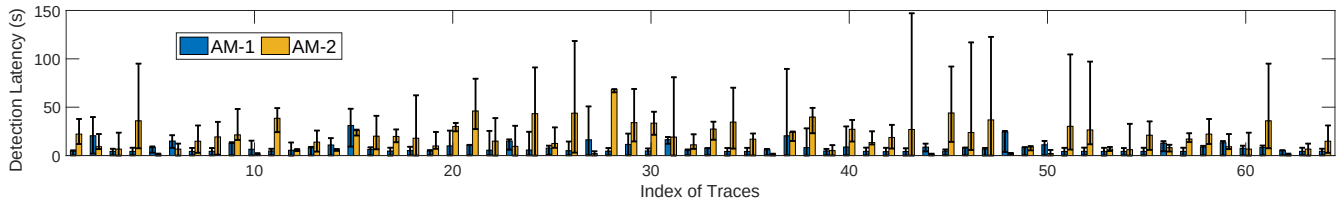
• **Methodology.** We have identified one faulty Bluetooth OBD-II adapter that is unreliable in collecting the vehicle information, as plotted in Fig. 24 with the engine RPM as an example: the RPM keeps constant for up to over 10 minutes when driving the Crosstrek in urban road with frequent acceleration and braking. We have further verified the unreliability of this adapter with different vehicles. The abnormal vehicle information collected with this faulty adapter serves as a promising candidate to evaluate B-Diag's ability in detecting the anomalies thereof, even though these anomalies are caused due to the faults of the OBD-II adapter and not the vehicle. For example, the deficient updates of engine RPM in Fig. 24 could map to faulty (or hacked [22]) tachometer of the vehicle.

• **Evaluation Results.** We have collected 5 abnormal vehicle traces with the Subaru Crosstrek using this "faulty" adapter, each lasting about {25, 41, 33, 6, 6} minutes. We then apply B-Diag with a moving window of 60s to these traces, to detect the anomalies in the vehicle information listed in Table 1. B-Diag successfully detects the anomalies in *all* these vehicle information of *all* the 5 traces. As an example, Fig. 25 plots the accumulated e_is of the engine RPM of these abnormal traces: the abrupt changes in slopes validate the detectability of anomalies thereof by B-Diag.

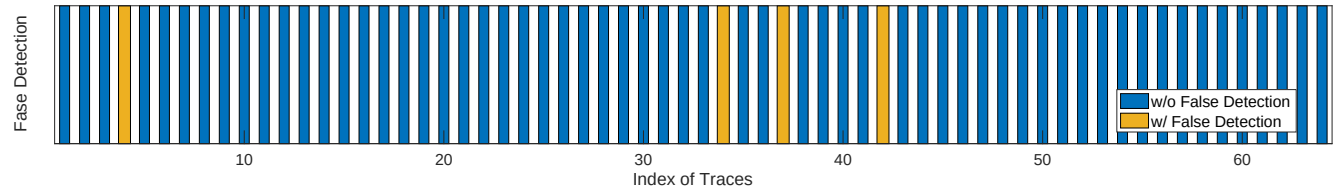
[5]It is possible to design advanced scheduling methods to check the edges based on factors such as the criticality of vehicle information [55].



(a) `B-Diag` **achieves >75% detection rate against RPM anomalies for each of these traces, with an averaged detection rate of** 99% **(with AM-1) and** 97% **(with AM-2) across all traces**



(b) `B-Diag` **achieves <68s average latency in detecting the RPM anomalies for each of these traces, with an averaged detection latency of** 8**s (with AM-1) and** 19**s (with AM-2) across all traces**



(c) `B-Diag` **falsely detects RPM anomalies in 4 out of the 64 traces**

Fig. 30: `B-Diag`**'s detection rate, latency, and false detection against RPM anomalies, with the 64 Crosstrek traces in Fig. 4(e).**

• **Adapter Faults or Vehicle Faults?** The above evaluation of `B-Diag` leads to an interesting and important question: can `B-Diag` differentiate the anomalies caused due to the faults of its own data collection and those by the actual vehicle failures? The answer is confirmative because the faults of data collection will cause anomalies in all the collected vehicle information, while the actual vehicle failures will, unless in a rare case where most of the vehicle modules fail, cause anomalies only in the vehicle information related to the faulty vehicle modules. Also note the risk of these adapter-caused anomalies can be reduced by employing reliable OBD-II adapters, e.g., using the wired OBD-II adapters to collect the vehicle information instead of those based on Bluetooth.

5.2 B-Diag against Emulated Anomalies

Next we evaluate `B-Diag` by emulating anomalies of engine RPM based on the wheel's RPM empirically collected during the same driving trip. Wheel RPM quantifies the rotation speed of the vehicle's wheels. Mechanically,

$$RPM_{\text{wheel}} = \alpha_i(t) \cdot RPM_{\text{engine}}, \tag{4}$$

where $\alpha(t)$ is the gear ratio at time t, determined by the real-time driving behavior. The empirically collected wheel's RPMs are a promising candidates to emulate the anomalies of engine RPMs during the same driving trip, because: (i) wheel's RPMs fall in the legal range of engine RPM (i.e., with $\alpha_i(t)$=1), making the thus-emulated anomalies possible to occur in practice and not diagnosable by existing range-based diagnostics systems [2, 36], (ii) the wheel RPM is strongly correlated to, but different from, the engine RPM, and such a correlation is dynamic over time.

Inspired by this, we build an Arduino-based RPM sensor with a hall sensor and a magnetic, and attach it to the front-right wheel of the Subaru Crosstrek (see Fig. 26). Fig. 27(a) plots the collected wheel RPM, engine RPM, and battery voltage during a 23-minute drive of the vehicle. The corresponding gear ratio during this driving is plotted in Fig. 27(b). We then emulate the abnormal engine RPMs by concatenating the first 10-minute trace of engine RPM and the last 13-minute trace of wheel RPM, and examine if `B-Diag` is able to detect such emulated anomalies. Fig. 28 plots the accumulated e_is obtained with such an emulation, whose change in slope at about the 10.5th minute — i.e., about 0.5 minute after the emulated anomalies begin — validates `B-Diag`'s ability of detecting such anomalies.

5.3 B-Diag against Simulated Anomalies

We also evaluated `B-Diag` against simulated anomalies in the vehicle information.

• **Anomaly Model.** We emulate vehicle anomalies by injecting fabricated vehicle information to the collected normal

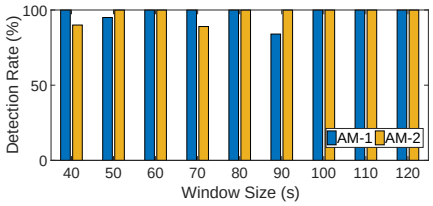


Fig. 31: Detection rate v.s. window size.

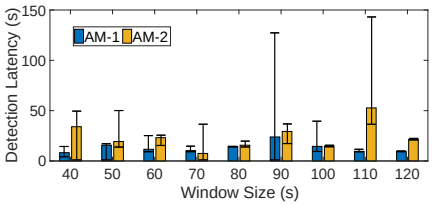


Fig. 32: Detection delay v.s. window size.

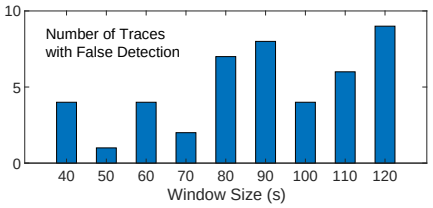


Fig. 33: False detection v.s. window size.

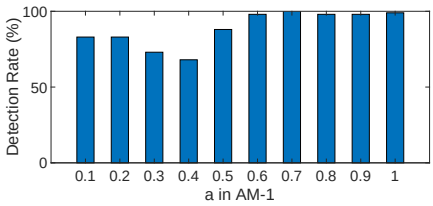


Fig. 34: Detection rate v.s. AM-1's model parameter a in Eq. (5).

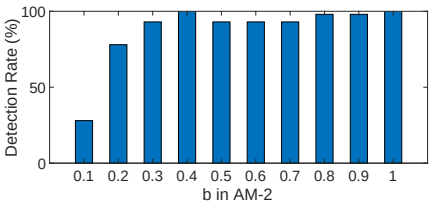


Fig. 35: Detection rate v.s. AM-2's model parameter b in Eq. (6).

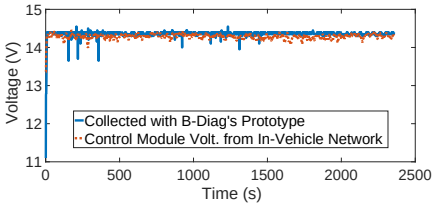


Fig. 36: `Control Module Voltage` is a close approximation to battery voltage.

traces. Specially, denoting the genuine time series of the targeting vehicle information (e.g., engine RPM) as $v(t)$, we inject anomalies to $v(t)$ with the following two anomaly models, emulating the fabrication and masquerade attacks in practice [35].

AM-1: Injecting anomalies after a randomly selected time t_{anom} by fabricating $v(t)$ within a legal range:

$$v'(t) = (1 - rand(a)) \cdot v_{\min} + rand(a) \cdot v_{\max} \ (t \geq t_{\text{anom}}), \quad (5)$$

where $v_{\min}$ and $v_{\max}$ are the min/maximum of $v(t)$, $rand(a)$ returns a random value in $[0, a]$, and $a \in [0, 1]$ controls the levels of the fabricated readings (a=0.8 unless specified otherwise). The thus-fabricated vehicle information will still be within the min/maximum of its genuine levels, thus voiding existing range-based diagnostics systems [2, 36]. This is also how we generate the RPM anomalies in Fig. 17.

AM-2: Injecting anomalies after a randomly selected time t_{anom} by shifting $v(t)$s from their true values randomly:

$$v'(t) = (1 - b + 2b \cdot rand(1)) \cdot v(t) \ (t \geq t_{\text{anom}}), \quad (6)$$

where b controls the maximum shift of the fabricated $v(t)$s from their true values (b=0.5 unless specified otherwise). Fig. 29 shows an example of such generated RPM anomalies based on the genuine trace in Fig. 6.

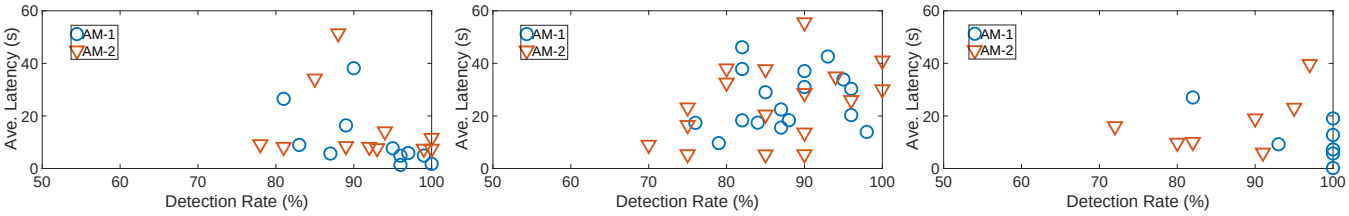
• **Evaluation with Subaru Crosstrek.** We first evaluate `B-Diag` with the 64 driving traces of the Subaru Crosstrek summarized in Fig. 4(e), taking again, the anomalies in engine RPM as an example.

Overall Performance. Fig. 30 summarizes `B-Diag`'s performance in anomaly detection, in terms of the detection rate (Fig. 30(a)), detection latency (Fig. 30(b)), and false detection (Fig. 30(c)), with a 60s moving window. The results in Figs. 30(a) and 30(b) are based on randomly injected RPM anomalies according to AM-1 and AM-2, each with 100 tests. As shown in Fig. 30(a), `B-Diag` achieves an overall averaged detection rate of 99% and 97% against the anomalies injected according to AM-1 and AM-2, respectively, and archives 100% detection rate for many of these 64 traces. The minimum detection rate of these traces with AM-1/2 is 80/75%. Fig. 30(b) shows `B-Diag` detects the anomalies with an averaged latency of less than 31s and 68s, for the two anomaly models respectively. The overall average detection latency across all these 64 traces is 8s for AM-1 and 19s for AM-2. We have also evaluated `B-Diag`'s false detection of anomalies. Specifically, we apply `B-Diag` to the genuine RPM traces without injecting anomalies, and check if any false detection of RPM anomalies is triggered. Fig. 30(c) shows `B-Diag` falsely detects RPM anomalies in only 4 of the 64 traces. Moreover, `B-Diag` only falsely detects the anomalies in $\{1, 1, 2, 2\}$ of the 60s moving windows in the 4 traces with false detection, which last about $\{30, 26, 25, 25\}$ minutes, respectively.

Impact of Window Size. We next evaluate the impact of the size of `B-Diag`'s moving window on its performance in anomaly detection, based on the RPM traces shown in Fig. 6. Figs. 31 and 32 summarize `B-Diag`'s detection rate and latency of injected anomalies with the window size varying from 40–120s, showing an over 84/89% detection rate for all the explored cases and an average latency of 13s and 24s, with AM-1 and AM-2, respectively. No clear dependency between `B-Diag`'s detection rate against anomalies and the window size is observed from Fig. 31. On the other hand, Fig. 32 shows a larger moving window tends to increase the latency of `B-Diag`'s anomaly detection, which is expected as a larger window requires more samples of abnormal RPM readings to conclude the detection of anomalies, thus requiring a longer time. Fig. 33 summarizes the false detection of anomalies when applying `B-Diag` to each of these genuine 64 traces (and thus without anomalies) with varying window size. The

(a) 2008 Honda Fit (b) 2018 Volvo XC60 (c) 2017 Volkswagen Passat

Fig. 37: Further evaluating B-Diag with the driving traces collected with a 2008 Honda Fit, a 2018 Volvo XC60, and a 2017 Volkswagen Passat.



(a) 2008 Honda Fit (b) 2018 Volvo XC60 (c) 2017 Volkswagen Passat

Fig. 38: B-Diag detects the anomalies of Honda Fit, Volvo XC60, and Volkswagen Passat with averaged rate/latency of $\{92\%, 88\%, 96\%\}/\{91\%, 86\%, 87\%\}$ **and** $\{11, 26, 12\}/\{15, 28, 18\}$**s, with the two anomaly models of AM-1 and AM-2, respectively.**

Table 2: Summary of the traces collected with a 2008 Honda Fit, a 2018 Volvo XC60, and a 2017 Volkswagen Passat.

Vehicles	# of Traces	Total Duration	Total Distance
Honda Fit	11	4.7 hour	≈160 miles
Volvo XC60	17	4.1 hour	≈210 miles
Volkswagen Passat	7	29 hour	≈1,840 miles

number of traces in which B-Diag falsely observes anomalies increases as the window becomes larger, varying from 1–9 with window size between 40–120s. Also note that even for traces with falsely observed anomalies, only a limited number of time windows therein detect such anomalies, e.g., with a maximum of 4 windows in all the cases in Fig. 33, and thus accounting for only a limited period when compared to the total driving duration of about 31 hours (as summarized in Fig. 4(e)).

Impacts of Anomaly Models' Parameters. Figs. 34 and 35 summarize B-Diag's detection rates of injected anomalies based on the RPM traces in Fig. 6, with varying a in Eq. (5) and b in Eq. (6) respectively. The results are averaged over 100 tests for each setting. B-Diag detects the anomalies fabricated with AM-1 with over 68% detection rates with $a \in [0.1, 1]$ (see Fig. 34). The relatively low detection rate of 68% with a=0.4 is because in this case, the abnormal RPMs deviate little from their genuine levels. Specifically, with the RPM trace shown in Fig. 6, $a = 0.4$ leads to abnormal RPMs within [573, 2069] according to Eq. (5), which are close to their true values (as observed in Fig. 6). Also note that other things being equal, a smaller deviation of RMP readings from the genuine levels will cause less safety/reliability risks, when compared to those change the RPMs dramatically. Fig. 35 shows B-Diag accurately detects the anomalies when the model parameter b in Eq. (6) is not too small, e.g., with over 93% detection rates when $b \geq 0.3$. The low detection rate with b=0.1 is because, again, a small b in AM-2 causes little deviation of abnormal RPM readings from their true levels.

• **Evaluation with Other Vehicles.** To validate B-Diag's generality with different vehicles, we have further evaluated B-Diag based on the driving traces collected with a 2008 Honda Fit, a 2018 Volvo XC60, and a 2017 Volkswagen Passat (see Fig. 37), each with its respective owner/driver. Table 2 summarizes the details of these traces. Different from the Crosstrek traces where the battery voltage is collected with our prototype and in physical separation of the in-vehicle network, we use the `control module voltage` collected from the in-vehicle network via the OBD-II port as a close approximation of the battery voltage for these three vehicles, for the ease of data collection. The `control module voltage` represents the real-time voltage supplied to the vehicle's ECUs, i.e., the battery voltage minus any voltage drop in the wiring between the battery and ECUs, normally less than a few tenths of a volt. Fig. 36 compares the `control module voltage` with the corresponding battery voltage collected directly from the battery, corroborating their closeness. Fig. 38 plots B-Diag's detection rate and latency against the added anomalies, with a 60s moving window and averaged over 100 runs. For the two anomaly models AM-1 and AM-2, B-Diag detects the anomalies with (i) an averaged detection rate of 92/91% and a latency of 11/15s for Honda Fit, (ii) an averaged detection rate of 88/86% and a latency of 26/28s for Volvo XC60, and (iii) an averaged detection rate of 96/87% and a latency of 12/18s for Volkswagen Passat.

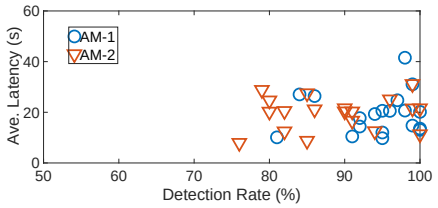


Fig. 39: Using B-Diag to diagnose the information in Fig. 22.

• **Diagnosing beyond Engine RPM.** We also corroborated B-Diag's feasibility as a comprehensive diagnostics system for vehicles. Specifically, we use B-Diag to detect the anomalies at each of these vehicle information in Fig. 22, injected according to the two anomaly models. Fig. 39 summarizes the detection results: all of these anomalies are detected with over 81/76% detection rate and a latency less than 42/31s, with an average of 94/89% and 19/20s, respectively. Note that no false detection is observed when applying B-Diag to the raw traces without injecting anomalies.

Last but not the least, we further verify B-Diag's generality in diagnosing the vehicle information listed in Table 1 — which are originally identified with the Subaru Crosstrek — with the Honda Fit, Volvo XC60, and Volkswagen Passat. The strong correlations of these vehicle information with the battery voltage are observed in all these three vehicles, thus validating B-Diag's generality. This also demonstrates the advantage of B-Diag's cyber-physical approach in vehicle diagnostics: the physical dependencies among a vehicle's individual modules are (likely) general for different vehicles, making the correlations among corresponding vehicle information universal.

6 LIMITATIONS

Below we discuss a few limitations of the current design/evaluation of B-Diag, and their potential mitigations.

• **Norm Model Construction.** B-Diag constructs the norm models with a decision tree defined by 10 features. We will further improve such a model construction by (i) reducing the number of features and (ii) exploiting the (likely) overlapped time windows, thus reducing the complexity and improving the online diagnostics of vehicles. Also, B-Diag assumes the availability of normal traces to construct the norm model. We will further explore B-Diag's ability of vehicle diagnostics when the normal traces are not available.

• **Anomaly Detection and Verification.** B-Diag detects the anomalies based on the τ_is (defined in Eq. (3)) for each time window. An alternative is to conclude the detection of anomalies only when multiple τ_is satisfying Eq. (3) have been observed in several consecutive time windows, trading off between the anomaly detection's false positive and false negative. We will also need to consider the latency of anomaly detection, which is desirable to be as small as possible. We envision the window size should be a promising control knob to reduce the latency. B-Diag verifies the detected anomalies by checking the norm models defining the interplays among vehicle information, and confirms the detected anomalies if any of these checkings fail. We will investigate other methods for anomaly confirmation, e.g., by weighting the checking results of individual norm models.

• **Fault Identification.** After detecting/verifying the anomalies, B-Diag will need to identify the corresponding causes, i.e., which modules (or ECUs) of the vehicle fail? Such a fault identification is required to provide a swift repair/forensic, otherwise the vehicle remains unreliable no matter how accurate the anomalies are detected. We will steer B-Diag's fault identification based on the correlation graph defined in Fig. 23, by examining the connectivity among vertexes (i.e., vehicle information) with detected anomalies.

• **Diagnosing beyond Engine RPM.** We have validated B-Diag's ability in individually diagnosing other vehicle information beyond engine RPM in Sec. 4. An integrated solution that guards all vehicle information in real-time, however, is still needed to make B-Diag a comprehensive solution for vehicle diagnosis, especially in view of the possibility of cascaded anomalies in vehicles, i.e., anomalies in one vehicle information may cause anomalies in other information.

• **Evaluation against Real-Life Vehicle Anomalies.** Although we have validated B-Diag with different approaches in Sec. 5, B-Diag's evaluation against real-life vehicle anomalies is still missing. Such an evaluation of B-Diag may cause vehicle malfunction and thus incur safety risks. We will mitigate these challenges with two steps: (i) testing when using jack stands to raise the vehicle from the ground, thus ensuring safety, and then (ii) testing when driving on testing field, such as the Mcity Test Facility at University of Michigan.

7 CONCLUSION

In this paper, we have designed B-Diag, a battery-based diagnostics system that guards vehicles against anomalies in real-time, and implemented B-Diag as an add-on module of commodity vehicles attached to automotive batteries. B-Diag is inspired by the physically-induced correlations between the battery voltage and other operational parameters of the vehicle such as engine RPM. B-Diag exploits these correlations to diagnose vehicles by exploiting automotive batteries as anomaly sensors: cross-validating vehicle information with online constructed norm models with regard to the battery voltage, steered by a dataset collected when driving a 2018 Subaru Crosstrek in real-life for over 3 months. We have evaluated B-Diag based on the driving traces collected with, besides the Crosstrek, a 2008 Honda Fit, a 2018 Volvo XC60, and a 2017 Volkswagen Passat, showing B-Diag detects anomalies in vehicle information with over 86% detection rate on average.

Acknowledgments. We would like to thank the anonymous reviewers and the shepherd, Dr. Marco Gruteser, for constructive suggestions. The work reported in this paper was supported by NSF under Grant CNS-1739577.

REFERENCES

[1] Car Software: 100M Lines of Code and Counting. https://www.linkedin.com/pulse/20140626152045-3625632-car-software-100m-lines-of-code-and-counting.

[2] M. Muter, A. Groll, and F. C. Freiling. A structured approach to anomaly detection for in-vehicle networks. In *IAS'10*, 2010.

[3] Kyong-Tak Cho and Kang G. Shin. Error handling of in-vehicle networks makes them vulnerable. In *CCS'16*, 2016.

[4] Kyong-Tak Cho, Kang G. Shin, and Taejoon Park. CPS approach to checking norm operation of a brake-by-wire system. In *ICCPS'15*, 2015.

[5] J. P. Hubaux, S. Capkun, and Jun Luo. The security and privacy of smart vehicles. *IEEE Security Privacy*, 2(3):49–55, 2004.

[6] BMW cars found to contain more than a dozen flaws. http://www.bbc.com/news/technology-44224794.

[7] Software Glitches in the Auto Industry and What that Means for You. https://www.proservicescorp.com/auto-industry-software-glitches/.

[8] Study: Tesla, Jaguar highest in auto software defects. https://www.usatoday.com/story/money/cars/2016/05/24/jd-power-software-defects-tesla-motors-jaguar-land-rover/84841174/.

[9] CAN Bus. https://www.csselectronics.com/screen/page/simple-intro-to-can-bus/language/en.

[10] Toyota vehicle recalls. https://en.wikipedia.org/wiki/2009%E2%80%9311_Toyota_vehicle_recalls.

[11] Jaguar recall shows how software glitches are the new speed bump. http://fortune.com/2015/07/13/jaguar-recall-software-glitch/.

[12] Fiat Chrysler recalls 4.8 million vehicles that could get stuck in cruise control. http://money.cnn.com/2018/05/25/autos/fca-recall-cruise-control/index.html.

[13] R. R. Brooks, S. Sander, J. Deng, and J. Taiber. Automobile security concerns. *IEEE Vehicular Technology Magazine*, 4(2):52–64, 2009.

[14] D. Nilsson and U. Larson. A roadmap for securing vehicles against cyber attacks. In *NITRD National Workshop on High-Confidence Automotive Cyber-Physical Systems*, 2008.

[15] D. Nilsson and U. Larson. Simulated attacks on CAN buses: vehicle virus. In *AsiaCSN'08*, 2008.

[16] Ishtiaq Rouf, Rob Miller, Hossen Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe, and Ivan Seskar. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In *USENIX Security'10*, 2010.

[17] Tesla responds to Chinese hack with a major security upgrade. https://www.wired.com/2016/09/tesla-responds-chinese-hack-major-security-upgrade/.

[18] Yasser Shoukry, Paul Martin, Paulo Tabuada, and Mani Srivastava. Non-invasive spoofing attacks for anti-lock braking systems. In *CHES'13*, 2013.

[19] A. Palanca. *A stealth, selective, Link-layer Denial-of-Service attack against automotive networks*. PhD thesis, Politecnico Milano, 2016.

[20] Kyong-Tak Cho and Kang G. Shin. Viden: Attacker identification on in-vehicle networks. In *CCS'17*, 2017.

[21] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security'11*, 2011.

[22] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. In *S&P'10*, 2010.

[23] Charlie Miller and Chris Valasek. Adventures in automotive networks and control units. In *DEFCON'11*, 2011.

[24] Charlie Miller and Chris Valasek. CAN Message Injection. http://illmatics.com/can%20message%20injection.pdf.

[25] Hackers remotely kill a Jeep on the Highway — with me in it. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[26] Charlie Miller and Chris Valasek. Remote exploitation of an unaltered passenger vehicle. In *Black Hat USA'15*, 2015.

[27] On-Board Diagnostics. http://www.car-engineer.com/introduction-to-on-board-diagnostic-obd/.

[28] D. K. Nilsson, U. E. Larson, and E. Jonsson. Efficient in-vehicle delayed data authentication based on compound message authentication codes. In *VTC'08*, 2008.

[29] Anthony Van Herrewege, Dave Singelee, and Ingrid Verbauwhede. CANAuth – A Simple, Backward Compatible Broadcast Authentication Protocol for CAN bus. In *LC'11*, 2011.

[30] Chris Szilagyi and Philip Koopman. Low cost multicast authentication via validity voting in time-triggered embedded control networks. In *WESS'10*, 2010.

[31] Kyong Tak Cho. *From Attack to Defense: Toward Secure In-vehicle Networks*. PhD thesis, University of Michigan, 2018.

[32] W. Choi, H. J. Jo, S. Woo, J. Y. Chun, J. Park, and D. H. Lee. Identifying ECUs through inimitable characteristics of signals in controller area networks. *IEEE Transactions on Vehicular Technology*, pages 1–1, 2018.

[33] M. Muter and N. Asaj. Entropy-based anomaly detection for in-vehicle networks. In *IV'11*, 2011.

[34] Tobias Hoppe, Stefan Kiltz, and Jana Dittmann. Security threats to automotive can networks — practical examples and selected short-term countermeasures. In *SAFECOMP'08*, 2008.

[35] Kyong-Tak Cho and Kang G. Shin. Fingerprinting electronic control units for vehicle intrusion detection. In *USENIX Security'16*, 2016.

[36] Armin Wasicek, Mert D. Pese, Andre Weimerskirch, Yelizaveta Burakova, and Karan Singh. Context-aware intrusion detection in automotive control systems. In *ESCAR'17*, 2017.

[37] Charlie Miller and Chris Valasek. A survey of remote automotive attack surfaces. In *Black Hat USA*, 2015.

[38] Patrick E. Lanigan, Soila Kavulya, Priya Narasimhan, Thomas E. Fuhrman, and Mutasim A. Salman. Diagnosis in automotive systems: A survey, 2011.

[39] W. Choi, H. J. Jo, S. Woo, J. Y. Chun, J. Park, and D. H. Lee. Identifying ECUs Using Inimitable Characteristics of Signals in Controller Area Networks. *ArXiv e-prints*, 2016.

[40] P. S. Murvay and B. Groza. Source identification using signal characteristics in controller area networks. *IEEE Signal Processing Letters*, 21(4):395–399, 2014.

[41] David S. Breed. System and method for vehicle diagnostics, 2006.

[42] David S. Breed. Telematics system for vehicle diagnostics, 2004.

[43] Christopher R. Baker, David Ferguson, and John M. Dolan. Robust mission execution for autonomous urban driving. In *IAS'08*, pages 155–163, July 2008.

[44] Galen Hunt, George Letey, and Ed Nightingale. The seven properties of highly secure devices. Technical report, 2017.

[45] Selected worldwide automotive manufacturers' profit margin between January 2016 and June 2016. https://www.statista.com/statistics/697263/automotive-manufacturers-profit-margin-worldwide/.

[46] OBD-II PIDs. https://en.wikipedia.org/wiki/OBD-II_PIDs.

[47] 6 Most Common Crankshaft Position Sensor Symptoms. https://carfromjapan.com/article/car-maintenance/common-crankshaft-position-sensor-symptoms/.

[48] How to Diagnose a Bad or Failing Transmission Speed Sensor? https://www.yourmechanic.com/article/symptoms-of-a-bad-or-failing-transmission-speed-sensor.

[49] Understanding Your Alternator. http://www.hotrod.com/articles/0206sr-understanding-your-alternator/.

[50] Robert Bosch. *Bosch Automotive Electrics and Automotive Electronics*. Springer, 2014.

[51] L. He, G. Meng, Y. Gu, C. Liu, J. Sun, T. Zhu, Y. Liu, and K. G. Shin. Battery-aware mobile data service. *IEEE Transactions on Mobile Computing*, 6(16):1544–1558, 2017.

[52] J. Lepkowski, B. Wolfe, and W. Lepkowski. EMI/ESD solutions for the CAN network. In *NSC'05*, 2005.

[53] Dynamic Time Warping. http://web.science.mq.edu.au/~cassidy/comp449/html/ch11s02.html.

[54] D. Montgomery. *Introduction to statistical quality control*. Wiley, 2000.

[55] Stergios Mavromatis and Alexandra Laiou. Safety assessment of control design parameters through vehicle dynamics model. In *RSS'17*, 2017.