Reminding Drivers of the Stalking Vehicles on the Road

Wei Sun
The Ohio State University
sun.1868@osu.edu

Kannan Srinivasan
The Ohio State University
kannan@cse.ohio-state.edu

Abstract—**Being followed by other vehicles during driving is scary and causes privacy leakage (e.g., location), which can make our blood run cold and even make run moves. Moreover, deliberately following the other vehicles may cause significant traffic accidents. The following vehicle needs to maintain an appropriate separation from the following vehicle without getting lost and uncovered. To put the driver's privacy and safety first, it is essential to discriminate between stalking vehicles (i.e., following abnormal vehicles) and normal following vehicles. However, there are no infrastructure-free and ubiquitous in-vehicle systems that can achieve abnormal following vehicle detection while driving.**

To this end, we propose P2D2, a Privacy-Preserving Defensive Driving system that can detect the abnormal following vehicles through the sensor fusion. Specifically, we will use the camera to extract each following vehicle's following time, and use the IMU sensors (e.g., Gyroscope) to extract our vehicle's critical driving behavior (e.g., making a left or right turn). We harness the space diversity of IMU sensing data to remove the artifacts of road surface conditions (e.g., bumps on the road surface) on critical driving behavior (CDB) detection. Then, we leverage the machine learning-based anomaly detection algorithm to detect the abnormal following vehicles based on the following vehicle's following time and our vehicle's critical driving behavior within the following time. Our experimental results show the F-1 score of 97.45% for the abnormal following vehicle detection in different driving scenarios during our daily traffic commute.

I. Introduction

A. Background and Motivation

1) Background: Are you worried about being followed by other vehicles during driving? Do you want to have a smart in-vehicle system that can uncover or detect the abnormal following vehicles for you during driving? These two questions drive us to further explore privacy-preserving defensive driving. As development of modern vehicles, especially connected and automated vehicles (CAV) have proliferated our daily lives. Recent study [1] shows that Americans drive about 25 miles and spend about one hour behind the wheel every day. As we can see, driving a vehicle on the road becomes an important part of our daily life, which can make our lives more convenient. At the same time, it is essential to achieve privacy-preserving defensive driving on the road.

2) Privacy-Preserving Driving: It is very common to see celebrities getting stalked either on foot or by the car during driving. Normal people also get stalked in their daily lives due to different kinds of reasons. For example, the driver hops up on road rage, creepy admirers, and an ex who's not ready to move on. Approximately, 58% of females and 49% of males have experienced being stalked before age of 25 according to Centers for Disease Control and Prevention (CDC) [2]. It can be a very frightening situation to endure and cause privacy leakage (e.g., location privacy, driving behavior, and daily living habit), when we are abnormally followed by other vehicles during driving.

3) Defensive Driving: Moreover, it is risky to follow the other vehicles during driving without maintaining an adequate separation consistently or intermittently, which would be endangering the followed vehicles and others [3], [4], [5], [6], [7], [8]. Since the drivers of the following vehicles have the pressure to follow our vehicle without getting lost and being uncovered, abnormally following the other vehicles in purpose may cause significant car accidents. Let alone tailgating, which is the second most irritating thing drivers do [9].

Therefore, to achieve privacy-preserving defensive driving, it is essential to detect the abnormal following vehicles during driving. However, to the best of our knowledge, there are no in-vehicle smart systems that can uncover or detect the abnormal following vehicles during driving.

B. Prior Art and Challenges on Vehicle Detection

We have seen some prior works that are related to our vehicle detection and sensing. For example, FarSight [4] is a smartphone-based ranging system for safe car following. Allergie [10] uses commodity passive RFID tags to predict the relative vehicle location for safe driving. Auto++ [11] can detect the approaching vehicles for smartphone users through passive acoustic monitoring. CycleGuard [12] is an acoustic-based collision detection system for cyclists with smartphones. However, these smartphone-based vehicle sensing works do not target the problem of the abnormal following vehicle detection. Moreover, they only leverage single sensor data (i.e., either acoustic or camera sensing data) for the sensing purpose, thereby failing to characterize the object of interest reliably.

The straightforward idea for the abnormal following vehicle detection is to leverage the large-scale camera monitoring system on the road to compare the driving trajectory of the following vehicles and our vehicles. However, this infrastructure-based sensing system will introduce high costs and heavy

Symposium on Vehicles Security and Privacy (VehicleSec) 2023
27 February 2023, San Diego, CA, USA
ISBN 1-891562-88-6
https://dx.doi.org/10.14722/vehiclesec.2023.23025
www.ndss-symposium.org

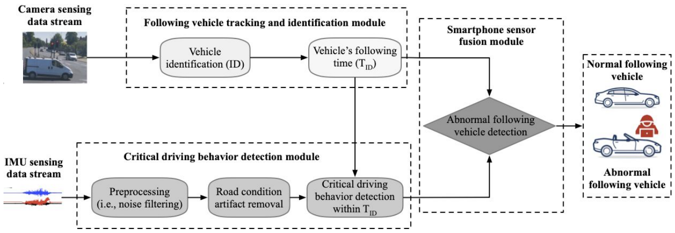
Camera sensing data stream
Following vehicle tracking and identification module
Vehicle identification (ID)
Vehicle's following time (T_{ID})
Smartphone sensor fusion module
Abnormal following vehicle detection
Normal following vehicle
Abnormal following vehicle
IMU sensing data stream
Critical driving behavior detection module
Preprocessing (i.e., noise filtering)
Road condition artifact removal
Critical driving behavior detection within T_{ID}

Fig. 1: The workflow of P2D2 for the abnormal following vehicle detection with the sensor fusion based on the following vehicle's following time and our vehicle's critical driving behavior within the following time.

workloads due to the large-scale deployment. Therefore, we aim to design an infrastructure-free system that can detect the abnormal following vehicles during driving. To uncover or detect the abnormal following vehicles during driving, simply comparing the driving trajectory of the following vehicles and our vehicle will introduce high false positive and false negative detection. This is because the abnormal following vehicle may not have the same driving trajectory as us. The abnormal following vehicles can simply follow us, no matter where and how we drive. Furthermore, the normal following vehicles may simply have the same driving trajectory as us due to the single-track road or same driving destination.

C. Our Design

In this paper, we present P2D2, a Privacy-Preserving Defensive Driving system that can uncover or detect the stalking vehicles (i.e, abnormal following vehicles) during driving with sensor fusion. The abnormal following vehicle will follow our vehicle, no matter how and where we drive our vehicle. In other words, the abnormal following vehicles will still follow us, when we make a left or right turn and detour. So, we can extract the following time of all the following vehicles with a camera and sense our vehicle's critical driving behavior (CDB) with IMU sensors (e.g., Gyroscope) for abnormal following vehicle detection. Since the gyroscope readings are the result of forces introduced by the driver's control as well as the road's horizontal and vertical geometry (e.g., bumpy road), we need to remove the artifacts of road surface conditions on gyroscope data readings. Therefore, we propose a road condition artifact removal approach for accurate critical driving behavior detection by harnessing IMU sensing data across the x, y, and z-axis.

After we have extracted the following vehicle's following time and our vehicle's critical driving behavior within the following vehicles' following time, we propose a machine learning-based anomaly detection algorithm to detect the abnormal following vehicles with sensor fusion. Specifically, we leverage Local Outlier Factor (LOF) for anomaly detection, which can measure the local deviation of the density of a given sample in comparison to its neighbors and has demonstrated its superiority over the other anomaly detection algorithms (e.g., OC-SVM and Isolation forest algorithms).

Contributions We summarize the contribution of our work as follows:

- To the best of our knowledge, this is the first privacy-preserving defensive driving system that can detect the abnormal following vehicles during driving with the sensor fusion.
- We propose a road condition artifact removal approach by harnessing the IMU sensing data across the x, y, and z axis for accurate critical driving behavior detection.
- Our experimental results demonstrate the efficiency of our system in detecting the abnormal following vehicles for privacy-preserving driving.

II. P2D2's Design

A. Following Vehicle's Following Time Estimation

1) Our Design: To track the following vehicles, we use the camera to monitor the following vehicles at the rear view of our vehicle. We aim to identify and track each following vehicle and further estimate each following vehicle's following time, which will be an important feature for abnormal following vehicle detection.

2) Following Vehicle Tracking and Identification: To track and identify the following vehicles, we use the You Only Look Once (YOLO) algorithm [13], which can provide real-time object detection and identification in videos, images, and live feeds with high speed and accuracy. It has been demonstrated its superiority in various real-world applications such as autonomous driving [14], wildlife monitoring and detection [15], human identification with camera systems [16]. Specifically, YOLO algorithm mainly uses a deep convolutional neural network to provide real-time object detection and recognition [13], which mainly consists of residual boxes, bounding box regression, and intersection over union for real-time object detection and recognition. The residual boxes are used to detect the object in the gridded cells of the image, which is experimentally proven to have a good performance on object recognition. The bounding box regression is used to highlight the outline of the detected object in the image. To have the perfect surrounding outline for each object, the intersection over the union is used.

3) Following Time Estimation: The YOLO model for vehicle identification is trained on COCO dataset [17], which is a large-scale object detection, segmentation, and captioning dataset that has been widely used in computer vision for object detection. We will use the pre-trained YOLO model [18] to track and identify the following vehicles. As a result, each following vehicle's following time is estimated, which is defined as the time duration the following vehicle appears in the rear view of our vehicle. Specifically, we can calculate each following vehicle's following time as follows:

$$T_{ID} = \frac{N_L - N_F}{f_r} \tag{1}$$

where f_r denotes the frame rate, N_L denotes the index of the frame the following vehicle has disappeared in the rear view of our vehicle and N_F denotes the index of the frame the following vehicle has first appeared in the rear view of our vehicle.

After we obtain each following vehicle's following time, we can suspect that the vehicles that are following us for a long period of time are stalking us. However, if we only use following time to detect the abnormal following vehicles, it will have high false positive detection. This is because the normal following vehicle may simply have the same driving path as us due to the same driving destination. To further enhance our detection, we need to consider our vehicle's driving behavior. Intuitively, if we make a left/right turn and the following vehicles still follow us, we can be pretty sure that the following vehicles are stalking us. So, in the next section, we discuss how to detect the driver's driving behavior with the IMU sensors.

B. *Our Vehicle's Critical Driving Behavior Detection*

1) Motivation: One fact about the abnormal following vehicles is that they will follow us no matter where and how we drive. Within the following vehicle's following time, if our vehicle makes more left/right turns, we can highly suspect this following vehicle is abnormally following us. So, it is important to characterize our vehicle's driving behavior within the following time for the abnormal following vehicle detection. To this end, we define the critical driving behavior (i.e., making left/right turns) of our vehicle, which will be used to detect abnormal following vehicles together with the following time.

2) Challenges: We will use IMU sensors (i.e., Gyroscope) to sense our vehicle's critical driving behavior. The gyroscope sensor can indicate the driver's left/right turn. Note that using IMU sensors for driving behavior detection has already been exploited (e.g., V-Sens [19]). However, we cannot directly apply them to solve our problem for two reasons. First of all, we do not need to differentiate the different driving behaviors for anomaly detection, which is computationally complex due to the time-series data comparison. We will estimate the number of our vehicle's critical driving behaviors within the following vehicle's following time. Furthermore, the prior work on driving behavior detection is not practical, since it does not consider the impact of road surface conditions on driving behavior detection. The bumps or potholes on the road surface will pollute the gyroscope readings, which will cause the wrong detection.

3) Our Design: To this end, we can remove the artifacts of road surface conditions on our vehicle's critical driving behavior detection by analyzing the gyroscope readings across different dimensions. Specifically, when we drive the vehicle on a bumpy road, it will mainly affect the gyroscope readings over the x-axis. However, when the driver makes left/right turns, it will mainly affect the gyroscope readings over the y and z axis. Therefore, we can eliminate the effect of the road surface condition by leveraging the gyroscope readings across the different axis. This is feasible since we just detect the critical driving behaviors without discriminating against them.

To demonstrate this, we drive the vehicle on a smooth road and make turns during driving. Instead of plotting the raw gyroscope readings over time, we will first filter out the random noise to eliminate the effect of the vehicle's vibration and the drift of gyroscope readings. We use Savitzky-Golay filter with a window size of 101 and polynomial order of 3 for the noise filtering, as it can achieve good performance empirically [20]. Fig. 2 shows the gyroscope readings over time without noise filtering, when we drive the vehicle and make a left turn. After applying the Savitzky-Golay filter, we can see the gyroscope readings are smooth over time, when we drive the vehicle and make a left turn as shown in Fig. 3. This noise-filtering step will make our critical driving behavior detection more robust. Next, we will illustrate how to eliminate the impact of road surface conditions on gyroscope readings for critical driving behavior detection.

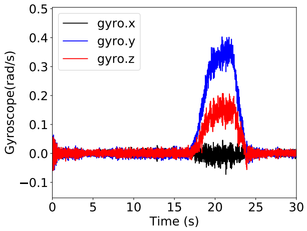

Fig. 2: Raw gyroscope readings over time, when we drive our vehicle and make a left turn.

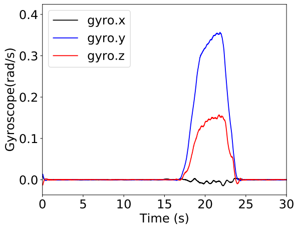

Fig. 3: Gyroscope readings over time after filtering out the noise, when we drive our vehicle and make a left turn.

As shown in Fig. 4, we can see the significant variation of gyroscope readings across the y and z axis, when we make turns. However, the gyroscope readings across the x-axis are stable due to the smooth road surface. Comparably, we also drive the vehicle over two bumps on the road surface without making any turns. As shown in Fig. 5, we can see that gyroscope reading over the x-axis vary significantly, when the vehicle is driven through the bumps. However, the gyroscope readings over the y and z-axis are quite stable. So, we can just analyze the variation of gyroscope readings over the y or z-axis to detect the critical driving behaviors. Since we do not need to discriminate each specific driving behavior, we propose to measure the variation of the gyroscope readings over the y or z-axis for critical driving behavior detection. To do so, we empirically set a variation threshold to construct a hypothesis test for this sake. Fig. 6 shows the CDF of the maximum gyroscope reading when we make turns. As we can see, the maximum gyroscope readings take the value from the range of $[0.2, 0.7]$, which depends on the significance of turns. In our experiments, we will set the threshold to 0.16 for critical driving behavior detection.

So far, we have discussed how to extract the following time of each following vehicle and the critical driving behavior of our vehicle within the following time, which can be leveraged to detect the abnormal following vehicles through smartphone sensing data fusion. Next, we will illustrate the details of our anomaly detection algorithm for abnormal following vehicle detection.

C. *Sensor Fusion-based Anomaly Detection*

1) Overview: After we obtain the following vehicle's following time and our vehicle's critical driving behavior within the following time, we adopt Local Outlier Factor (LOF) as our anomaly detection algorithm to detect the abnormal following vehicles, which has demonstrated good performance on anomaly detection. To do so, we first need to align the

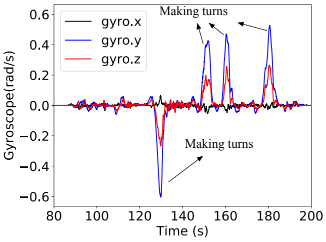

Fig. 4: Gyroscope readings over time, when the driver makes turns during driving on the smooth road.

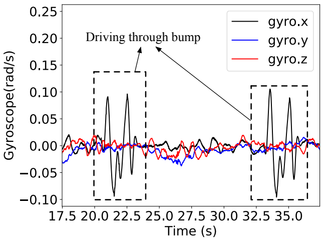

Fig. 5: Gyroscope readings over time, when the driver drives through two bumps in a straight line.

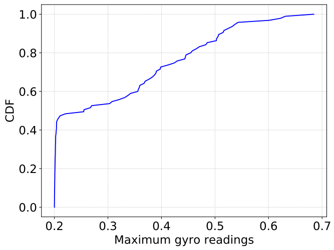

Fig. 6: CDF of the maximum gyroscope readings at the detected left/right turning action.

following vehicle's following time to our vehicle's critical driving behavior (CDB) for accurate CDB extraction within each following vehicle's following time. Then, we use LOF algorithm to derive the anomaly score of the following vehicle, which will be used to detect the abnormal following vehicles.

2) Sensor Data Alignment: After we obtain the camera sensing data and over-time gyroscope readings, we first need to synchronize these two data streams. To do so, before we start the engine of our vehicle, we let the camera and IMU sensors record the sensing data. When the vehicle is moving, the recorded rear view from the camera and IMU sensing readings will change. So, we can synchronize these two data streams by detecting their over-time variations.

3) Unsupervised Anomaly Detection Using Local Outlier Factor: The main idea of LOF algorithm [21] is to compute the anomaly score of the sample that is called LOF. LOF measures the local deviation of the density of the given sample in comparison to its neighbors. The locality is calculated from k-nearest neighbors (we set k to be 20 in our experiments), whose distance is leveraged to estimate the local density. Then, the abnormal objects are identified, whose local density is substantially lower than their neighbors. LOF of a sample s is defined as follows [21]:

$$LOF_m(s) = \frac{\sum_{o\in N_m(s)} \frac{lrd_m(s)}{lrd_m(o)}}{|N_m(s)|} \tag{2}$$

where m is a parameter specifying the minimum number of samples around sample s. $N_m(s)$ is denoted as the m-distance neighborhood of sample s, which is defined as $N_m(s) = \{q \in D \setminus \{s\} \, |d(s,q) \leq m - distance(s)\}$. D denotes the dataset. $d(s,q)$ denotes the distance between s and q. $m-distance(s)$ is denoted as m-distance of sample s, which is defined as the distance between s and $o \in D$ such that (i) $d(s,o') \leq d(s,o)$ for at least m samples $o' \in D \setminus \{s\}$ and (ii) $d(s,o') \leq d(s,o)$ for at most m-1 samples $o' \in D \setminus \{s\}$. $lrd_m(s)$ denotes the local reachability density of sample s, which is defined as follows [21]:

$$lrd_m(s) = 1/(\frac{\sum_{o\in N_m(s)} reach - dist_m(s,o)}{|N_m(s)|}) \tag{3}$$

where $reach - dist_m(s,o) = max\,\{m - distance(o), d(s,o)\}$. As we can see, LOF of sample s is the average ratio of the local reachability density of sample s to the local reachability density of its m-nearest neighbors. The theoretical analysis of LOF's advantages over the other anomaly detection algorithms (e.g., OC-SVM and Isolation forests) can be found in [21]. Then, we can derive the anomaly score of each sample for the abnormal following vehicle detection.

III. Implementation and Evaluation

A. Implementation and Experimental Settings

1) Hardware and System Deployment: We do experiments with the smartphone (i.e., Motorola Moto E) since it has camera and IMU sensors. It will be deployed on the rear deck or rear windshield of our vehicle (i.e., Honda Civic, CRV, Subaru Crosstrek, etc.) to film the rear view of our vehicle for the following time estimation of the following vehicles and read gyroscope data streams for our vehicle's critical driving behavior detection. Note that the smartphone can capture the full rear view of our vehicle (like driving recorder). As we can see from Fig. 8 and Fig. 9, our smartphone's camera can detect all the following vehicles behind us.

2) Software and Implementation: To extract the sensing data from the smartphone, we use two off-the-shelf Android apps for video and IMU sensing data recording respectively. Specifically, we use Background Video Recorder (BVR) [22] for video recording and phyphox [23] for IMU sensing data recording with a sampling rate of 100Hz. After we record the data streams, we will extract the following time and critical driving behavior with Python for signal processing and data analysis. We use a pre-trained deep neural network model proposed in [18] to track and identify the following vehicles. Our LOF-based anomaly detection algorithm is also implemented with Python using sklearn [24] for the abnormal following vehicle detection. We use an OptiPlex 7050 Dell desktop running Ubuntu 16.04 OS on Intel CORE i7 CPU for video data processing with YOLO.

B. System Evaluation

1) Experimental Details.: To evaluate the performance of `P2D2`, we drive the vehicles on the road during our daily traffic commute, which can cover all our daily activities (e.g., grocery shopping, going to work, going to the shopping mall, going out for lunch/dinner, etc.) when we use our vehicle for daily traffic commute. Fig. 7 shows the driving path in the local area during the data collection. We set the value of parameter m in LOF to be 20, and the algorithm used for computing the

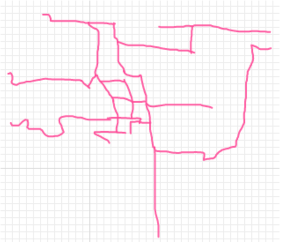

Fig. 7: Driving path in the local area during daily traffic commute.

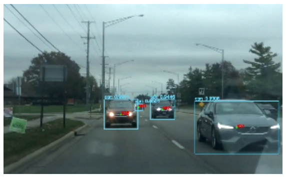

Fig. 8: Tracking and identifying the following vehicles. The identified following vehicles are outlined by the light blue rectangular.

Anomaly detection algorithm	Accuracy	Precision	Recall	F-1 Score
OC-SVM	0.58	1.0	0.52	0.68
Isolation Forest	0.82	1.0	0.79	0.88
LOF	**0.95**	**0.98**	**0.97**	**0.97**

TABLE I: Performance comparison of different machine learning-based anomaly detection algorithms.

nearest neighbors is configured to be automatically decided based on the data set.

2) Evaluation Metrics.: To measure the system performance, we will present the normalized confusion matrix, accuracy, precision, recall, and F-1 score for the abnormal following vehicle detection. Accuracy is defined as the ratio of the correct detection to the total detection. Precision is defined as the ratio of true positive detection to total positive detection. Recall indicates the sensitivity that is defined as the ratio of true positive detection to the total actual positive instances. The f-1 score is the harmonic mean between precision and recall. Moreover, we present the receiver operating characteristic (ROC) curve and precision-recall (PR) curve to characterize the performance of our anomaly detection algorithm in comparison to the random guess. We also compare the LOF-based anomaly detection algorithm with OC-SVM and Isolation forest algorithms.

IV. Experimental Results

A. Microbenchmark

1) Effectiveness of the Following Vehicle Tracking: To demonstrate the performance of YOLO on vehicle identification and tracking, we drive vehicles on the road and use the smartphone mounted in our vehicle to monitor the rear view of our vehicle. Then, we use YOLO [13] to track and identify the following vehicles. As shown in Fig. 8, we find that YOLO can accurately identify each following vehicle and highlight the bounding box of each detected following vehicle. Furthermore, YOLO can continuously detect the following vehicles as shown in Fig. 9, we showcase the following vehicle identification and tracking over the continuous video frames. The following vehicles are detected and highlighted with the bounding box accurately over four-time snapshots. Note that YOLO algorithm can also detect and track other road infrastructures such as traffic lights, passengers, and cyclists.

2) Effectiveness of Following Time Estimation: The following time of each following vehicle is the time duration when this vehicle appears in the field-of-view of the camera. Since we can track each following vehicle, we can obtain each following vehicle's following time as discussed in Sec. II. So, we first show the following time estimation error in Fig. 10. As we can see, the average following time estimation error is around 1.1s, and the maximum following time estimation error is around 2.5s due to the inaccurate following vehicle tracking with YOLO algorithm. Then, we further estimate the following time of each following vehicle, when we drive the vehicle on the road during the daily traffic commute. We show the CDF of the following time of the following vehicles in Fig. 11. We find that 99% of the following time is less than 50 seconds, indicating that the following vehicles are usually not following our vehicle for a long period of time due to the different driving destinations and driving behaviors. However, there are still some cases, in which the following vehicles are following us for about 5 minutes due to the one-lane road, slow traffic, and the same driving path to the same destination (e.g., grocery store).

3) Effectiveness of Number of Critical Driving Behavior Detection: To demonstrate the effectiveness of critical driving behavior detection, we use the approach proposed in Sec. II to detect critical driving behavior such as making left/right turns. Fig. 12 shows the gyroscope readings over time and the detected critical driving behavior indicated by the orange circle. Since these critical driving behaviors (i.e., making left/right turns) will significantly change the gyroscope readings over the y or z-axis, we can see that our detection approach can accurately detect these CDBs. Fig. 13 shows the accuracy of CDB detection, which is defined as the number of correct detection over all the number of CDBs during driving. We can see that the accuracy of CDB detection is around 0.99, which indicates the efficiency of our CDB detection approach. This is because our CDB detection approach mainly harnesses the gyroscope sensing data across different axis to remove road condition artifacts.

Furthermore, we statistically showcase the number of critical driving behaviors within each normal following vehicle's following time. Fig. 14 shows the CDF of the number of critical driving behaviors within the normal following vehicle's following time period. As we can see, the 95th percentile number of critical driving behaviors is three. Empirically, this indicates that the normal following vehicles will not follow us after we make more than three critical driving behaviors (e.g., making left/right turns). However, we can see that some normal following vehicles are still following us after we make four critical driving behaviors. This is because we may share the same driving path with the normal following vehicles.

B. Performance of Abnormal Following Vehicle Detection

1) Performance of LOF-based Anomaly Detection Algorithm: To evaluate the performance of the LOF-based anomaly detection algorithm while varying the threshold (i.e., cut-off probability), we report the receiver operating characteristic (ROC) curve and precision-recall (PR) curve of our anomaly

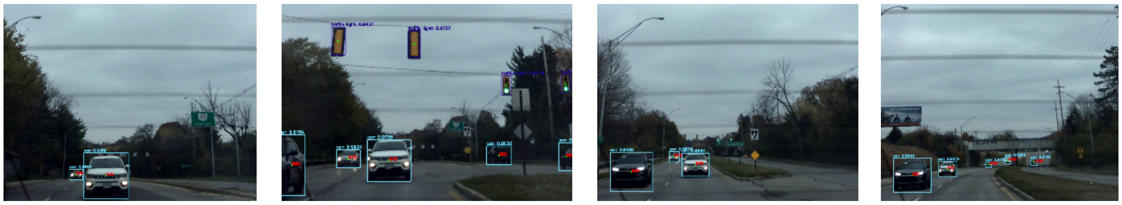

Fig. 9: Tracking the following vehicles over the continuous time frames. Each figure shows the detected following vehicles at the rear view of our vehicle.

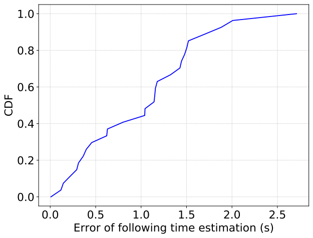

Fig. 10: CDF of the following time estimation error of the following vehicles.

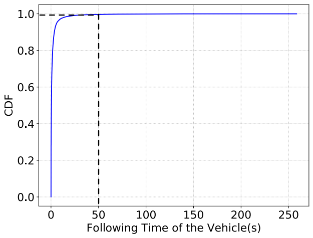

Fig. 11: CDF of the normal following vehicle's following time.

detection algorithm as shown in Fig. 15 and Fig. 16. As we can see, our anomaly detection algorithm is significantly better than the reference line (i.e., random guess). Note, the area under curve (AUC) for ROC and PR curve is 97.88% and 99.69% respectively. Fig. 17 shows the normalized confusion matrix of our anomaly detection algorithm. As we can see, our anomaly detection algorithm has a high true positive rate and true negative rate, which indicates the efficiency of our algorithm in detecting the abnormal following vehicles. However, we see that our algorithm has a false negative rate of 0.03, which indicates that some normal following vehicles will be detected as abnormal following vehicles. We can see that some abnormal following vehicles will be detected as normal following vehicles, as the false positive rate is 0.12. This is because some normal or abnormal following vehicles just simply follow us for a period of time due to the same driving destination, slow traffic flow, single-track road, etc.

2) Comparison with the Other Anomaly Detection Algorithms: We present the performance metrics of LOF, OC-SVM, and Isolation forest algorithms in Table I. As we can see, the accuracy, precision, recall, and F-1 score for the abnormal following vehicle detection using LOF are 0.95, 0.98, 0.97, and 0.97 respectively, which is better than the performance of OC-SVM and Isolation forest algorithm. This is because LOF anomaly detection algorithm measures the local deviation of the density of the given sample to its neighbors, which can characterize the two facts about the abnormal following vehicles that we delineate in Sec. I.

3) Performance across Different Drivers: We measure the performance of the abnormal following vehicle detection across two drivers during their daily traffic commute. Fig. 18 shows the accuracy, precision, recall, and F-1 score of abnormal following vehicle detection across two drivers. As we can see, the performance of the two drivers is close (i.e., the value of evaluation metrics is around 95%), indicating our anomaly detection algorithm is independent of different drivers. This is because the abnormal following vehicles are distinguished from the normal vehicles on the following time and critical driving behaviors, which are independent of the driver's driving pattern.

C. Case Study

We present a case study of the abnormal following vehicle detection. We drive the vehicle for grocery shopping with `P2D2` deployed in our vehicle. We aim to uncover the abnormal following vehicle with our anomaly detection algorithm.

As shown in Fig. 19, the left figure shows the driving path of our vehicle and the abnormal following vehicle in the green line and red line respectively, when we drive our vehicle from home to the grocery store. In the right figure, we show the gyroscope readings along the y-axis over time, which are collected from the smartphone deployed in our vehicle. For the sake of simplicity, we just analyze the detection of the abnormal following vehicles during driving. We find that there is one vehicle following us starting at the 40s. After we have detected four critical driving behaviors (i.e., indicated by the orange circle) of our vehicle, it still follows us. We check if the following vehicle is stalking us using the LOF anomaly detection algorithm based on the following vehicle's following time and our vehicle's critical driving behavior within the following time. As such, we have detected the abnormal following vehicle at 380s. Intuitively, this is because this following vehicle has still followed us after our vehicle has made four turns. Within 380s, we detect this following vehicle as normal following vehicle due to a small number of CDBs within its following time.

V. Related Work

With the development of modern vehicles, especially autonomous vehicles, there are many works focusing on the security and privacy analysis of autonomous vehicles. These works mainly target either the vulnerability of the machine learning models [25], [26], [27], [28] employed by the autonomous vehicles or the LiDAR/Camera sensors' vulnerability [29], [30], [31]. For example, Poltergeist [29] exploits the vulnerability of IMU sensors on acoustic adversarial examples in the modern camera against vision-based autonomous driving. Sun et al. [25] and Cao et al. [26] exploit the vulnerability of LiDAR-based machine learning models employed by autonomous vehicles. Recently, Cao et al. [27] exploits the vulnerability

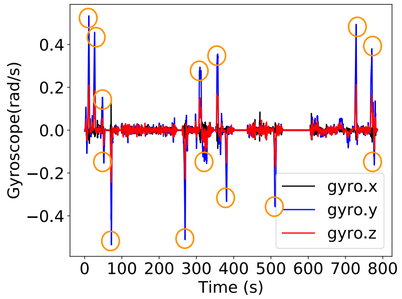

Fig. 12: The orange circle indicates the detected CDB.

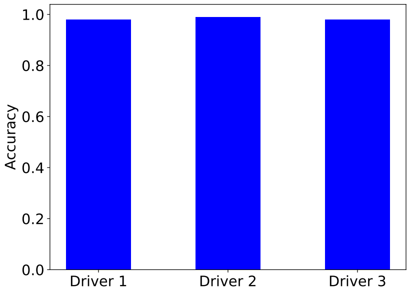

Fig. 13: The accuracy of CDB detection across different drivers.

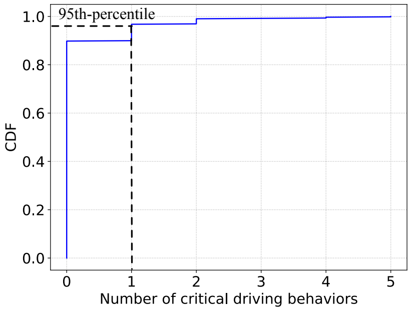

Fig. 14: CDF of the number of CDBs within the normal following time.

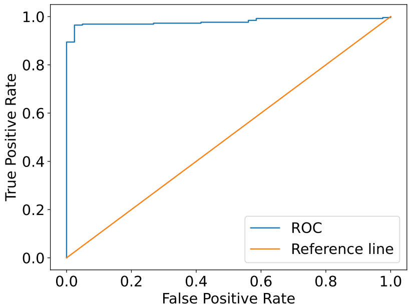

Fig. 15: Receiver Operator Characteristic (ROC) curve of LOF-based anomaly detection algorithm compared with reference line (i.e., random guess).

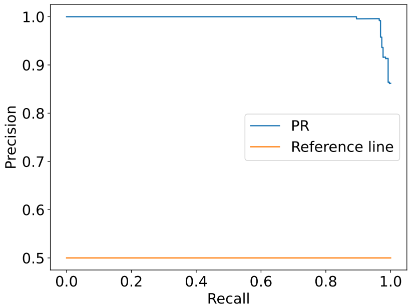

Fig. 16: Precision-Recall (PR) curve of LOF-based anomaly detection algorithm compared with reference line (i.e., random guess).

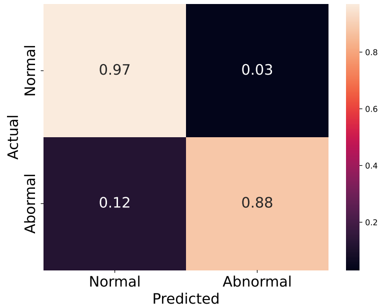

Fig. 17: The normalized confusion matrix of LOF-based anomaly detection algorithm.

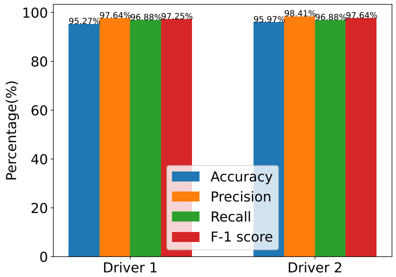

Fig. 18: Performance of the abnormal following vehicles detection across different drivers.

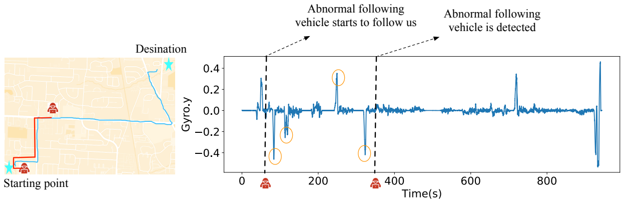

Fig. 19: The left figure shows the driving path of our vehicle and one abnormal following vehicle in the green line and red line respectively. The right figure shows the gyroscope readings on the y-axis over time. An abnormal following vehicle is detected as it follows us within the time period indicated by two dashed lines.

of LiDAR and camera sensor fusion-based machine learning models employed by autonomous vehicles.

Our work is fundamentally different from these prior works. First, these prior works focus on what happened at the front of the vehicle, while we target the privacy issue of what happened in the rear of the vehicle. Second, these prior works mainly analyze the vulnerability of autonomous vehicles instrumented with advanced sensors (e.g., LiDAR and camera) and deep neural networks, while our work discusses an important and common privacy leakage issue in driving scenarios. We also notice that driver authentication [32], [33], [34], [35] has been extensively exploited for privacy-preserving, while our work mainly focuses on the eavesdropping from the other vehicles behind us.

VI. Conclusion

In this paper, we have presented P2D2, the first privacy-preserving defensive driving system that can detect the abnormal following vehicles during driving with sensor fusion. Specifically, we use the camera to estimate the following time of the following vehicles and use the IMU sensors to detect our vehicle's critical driving behavior with the road surface artifacts removal approach. Then, we propose an anomaly detection algorithm to detect the abnormal following vehicles based on the following time and critical driving behavior. Our extensive experiments show the effectiveness of P2D2 on uncovering the abnormal following vehicles for drivers.

Acknowledgment

We are grateful to the anonymous reviewers from VehicleSec 2023 for their insightful feedback. This work was supported by NSF 2007581, NSF 2128567, and NSF 2112471.

References

[1] L. Steele, "How much time do american families spend in their cars?" https://www.fatherly.com/gear/how-much-time-do-american-families-spend-in-their-cars/, 2022.

[2] CDC, "Violence prevention," https://www.cdc.gov/violenceprevention/intimatepartnerviolence/stalking/fastfact.html, 2022.

[3] J. McNabb, M. Kuzel, and R. Gray, "I'll show you the way: Risky driver behavior when "following a friend"," *Frontiers in psychology*, vol. 8, p. 705, 2017.

[4] A. U. Nambi, A. Virmani, and V. N. Padmanabhan, "Farsight: a smartphone-based vehicle ranging system," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 4, pp. 1–22, 2018.

[5] L. A. Pipes, "An operational analysis of traffic dynamics," *Journal of applied physics*, vol. 24, no. 3, pp. 274–281, 1953.

[6] Y. Peng, S. Liu, and Z. Y. Dennis, "An improved car-following model with consideration of multiple preceding and following vehicles in a driver's view," *Physica A: Statistical Mechanics and Its Applications*, vol. 538, p. 122967, 2020.

[7] R. E. Chandler, R. Herman, and E. W. Montroll, "Traffic dynamics: studies in car following," *Operations research*, vol. 6, no. 2, pp. 165–184, 1958.

[8] W. Sun and K. Srinivasan, "On the feasibility of securing vehicle-pavement interaction," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 6, no. 1, pp. 1–24, 2022.

[9] T. Sun, "10 most irritating things drivers do," https://www.thesun.co.uk/motors/3581304/what-grinds-motorists-gears-the-most-irritating-driving-habits-revealed/, 2017.

[10] W. Sun and K. Srinivasan, "Allergie: Relative vehicular localization with commodity rfid system," in *2020 IEEE International Conference on RFID (RFID)*. IEEE, 2020, pp. 1–8.

[11] S. Li, X. Fan, Y. Zhang, W. Trappe, J. Lindqvist, and R. E. Howard, "Auto++ detecting cars using embedded microphones in real-time," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 1, no. 3, pp. 1–20, 2017.

[12] W. Jin, S. Murali, Y. Cho, H. Zhu, T. Li, R. T. Panik, A. Rimu, S. Deb, K. Watkins, X. Yuan *et al.*, "Cycleguard: A smartphone-based assistive tool for cyclist safety using acoustic ranging," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 5, no. 4, pp. 1–30, 2021.

[13] J. Redmon and A. Farhadi, "Yolov3: An incremental improvement," *arXiv preprint arXiv:1804.02767*, 2018.

[14] A. Sarda, S. Dixit, and A. Bhan, "Object detection for autonomous driving using yolo [you only look once] algorithm," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*. IEEE, 2021, pp. 1370–1374.

[15] R.-C. Chen, V. S. Saravanarajan, H.-T. Hung *et al.*, "Monitoring the behaviours of pet cat based on yolo model and raspberry pi," *International Journal of Applied Science and Engineering*, vol. 18, no. 5, pp. 1–12, 2021.

[16] S. S. Sumit, J. Watada, A. Roy, and D. Rambli, "In object detection deep learning methods, yolo shows supremum to mask r-cnn," in *Journal of Physics: Conference Series*, vol. 1529, no. 4. IOP Publishing, 2020, p. 042086.

[17] T.-Y. Lin, M. Maire, S. Belongie, J. Hays, P. Perona, D. Ramanan, P. Dollár, and C. L. Zitnick, "Microsoft coco: Common objects in context," in *European conference on computer vision*. Springer, 2014, pp. 740–755.

[18] "Yolo pretrained model," https://pjreddie.com/darknet/yolo/, 2022.

[19] D. Chen, K.-T. Cho, S. Han, Z. Jin, and K. G. Shin, "Invisible sensing of vehicle steering with smartphones," in *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services*, 2015, pp. 1–13.

[20] R. W. Schafer, "What is a savitzky-golay filter?[lecture notes]," *IEEE Signal processing magazine*, vol. 28, no. 4, pp. 111–117, 2011.

[21] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "Lof: identifying density-based local outliers," in *Proceedings of the 2000 ACM SIGMOD international conference on Management of data*, 2000, pp. 93–104.

[22] G. Play, "Background video recorder (bvr)," https://play.google.com/store/apps/details?id=com.camera.secretvideorecorder&hl=en_US&gl=US, 2022.

[23] ——, "phyphox," https://phyphox.org/, 2022.

[24] sklearn, "Local outlier factor algorithm in sklearn," https://scikit-learn.org/stable/modules/generated/sklearn.neighbors.LocalOutlierFactor.html, 2022.

[25] J. Sun, Y. Cao, Q. A. Chen, and Z. M. Mao, "Towards robust {LiDAR-based} perception in autonomous driving: General black-box adversarial sensor attack and countermeasures," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 877–894.

[26] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao, "Adversarial sensor attack on lidar-based perception in autonomous driving," in *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019, pp. 2267–2281.

[27] Y. Cao, N. Wang, C. Xiao, D. Yang, J. Fang, R. Yang, Q. A. Chen, M. Liu, and B. Li, "Invisible for both camera and lidar: Security of multi-sensor fusion based perception in autonomous driving under physical-world attacks," in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 176–194.

[28] T. Sato, J. Shen, N. Wang, Y. Jia, X. Lin, and Q. A. Chen, "Dirty road can attack: Security of deep learning based automated lane centering under {Physical-World} attack," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 3309–3326.

[29] X. Ji, Y. Cheng, Y. Zhang, K. Wang, C. Yan, W. Xu, and K. Fu, "Poltergeist: Acoustic adversarial machine learning against cameras and computer vision," in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 160–175.

[30] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *Def Con*, vol. 24, no. 8, p. 109, 2016.

[31] J. Shen, J. Y. Won, Z. Chen, and Q. A. Chen, "Drift with devil: Security of {Multi-Sensor} fusion based localization in {High-Level} autonomous driving under {GPS} spoofing," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 931–948.

[32] L. He, Y. Shu, Y. Lee, D. Chen, and K. G. Shin, "Authenticating drivers using automotive batteries," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 4, no. 4, pp. 1–27, 2020.

[33] A. M. Guzman, M. Goryawala, J. Wang, A. Barreto, J. Andrian, N. Rishe, and M. Adjouadi, "Thermal imaging as a biometrics approach to facial signature authentication," *IEEE journal of biomedical and health informatics*, vol. 17, no. 1, pp. 214–222, 2012.

[34] S. Hu, J. Choi, A. L. Chan, and W. R. Schwartz, "Thermal-to-visible face recognition using partial least squares," *JOSA A*, vol. 32, no. 3, pp. 431–442, 2015.

[35] G. Zheng, C.-J. Wang, and T. E. Boult, "Application of projective invariants in hand geometry biometrics," *IEEE transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 758–768, 2007.