MULTIMEDIA COMMUNICATIONS TECHNICAL COMMITTEE
http://www.comsoc.org/~mmc

MMTC Communications - Frontiers

Vol. 16, No. 6, November 2021

CONTENTS

SPECIAL ISSUE ON Data Sharing and Communication between Connected and Autonomous Vehicles

Guest Editor: Dapeng Wu
Chongqing University of Posts and Telecommunications, China
wudp@cqupt.edu.cn

This special issue of Frontiers focuses on data sharing and communication between connected and autonomous vehicles. The research topics of the papers in this special issue include how to a comprehensive analysis of TEASER and NDT for autonomous vehicular applications, a tutorial of cooperative perception on connected and automated vehicles, a design of resilient and intelligent Internet of vehicles, and how to conduct task scheduling in a vehicular edge computing system.

The first paper studies the performance difference between TEASER and NDT when they are applied to align two pieces of LiDAR data generated by autonomous vehicles. As the first step in cooperative perceptions, data alignment is critical to ensure LiDAR data can be accurately positioned and fused. In this paper, the authors detail the difference between the above-mentioned two methods and give an experimental comparison.

The second paper provides an overview of the enabling techniques for implement cooperative perception among autonomous vehicles. It starts from the discuss of different level of autonomous driving vehicles, followed by a detailed discussion on various technologies available for cooperative perception, including object detection, data fusion, wireless communications, security, etc. This paper can serve as a tutorial on how cooperative perception can be implemented on autonomous vehicles.

The third paper discusses joint AI and blockchain for security, privacy and trust-related risks in the Internet of Vehicles (IoV). This paper also presents problems, challenges, requirements, and solutions using ML and blockchain to address aforementioned issues in IoV.

The fourth paper discusses a vehicular edge computing scheduling pipeline for connected and autonomous vehicles exploring scheduling optimization, pipeline design and vehicle to edge interactions. Through the proposed pipeline, the data, generated by on-board sensors, is used towards various edge serviceable tasks. The proposed pipeline facilitates data transfer and fusion for cooperative object detection of multiple vehicles. Through real-world experiments, w performance and robustness of our pipeline are evaluated on different device architectures and under different scenarios. It is demonstrated that the proposed pipeline achieves a real time deadline capable edge to vehicle interaction via vehicle-edge data transfer and on-edge computation

Dapeng Wu is currently a professor at the Chongqing University of Posts and Telecommunications, Chongqing, China. He authored more than 100 publications and two books. His research interests are in social computing, wireless networks, and big data. Prof. Wu serves as TPC Chair of 10th Mobimedia and program committee member for numerous international conferences and workshops. He served or is serving as an Editor or/and Guest Editor for several technical journals, such as IEEE IoT, Elsevier Digital Communications and Networks, ACM/Springer Mobile Network and Applications. He is a senior member of the IEEE.

Comprehensive Analysis of TEASER and NDT for Autonomous Vehicle Applications

Dominic Carrillo, Deyuan Qu, and Qing Yang
Univerisity of North Texas, USA
DominicCarrillo, DeyuanQu @my.unt.edu, Qing.Yang@unt.edu

1. Introduction

We propose a verification of the Truncated least squares Estimation And Semidefinite Relaxation (TEASER) by experimentation evaluation, and algorithm analysis. From the TEASER paper, the authors indicate that TEASER has improved the optimization robustness of the estimation between outliers from two sets of 3D point cloud datasets along with being bounded sub-optimality. Their goal was to use Truncated Least Squares to reduce the time complexity of the estimation. This has vastly outperformed the Iterative Closest Point (ICP) algorithm and Normal Distribution Transform (NDT) algorithm, which has deployed on our Connect Autonomous Vehicle (CAV), AutonomouStuff Polaris GEM.

3D maps enable self-driving cars to locate themselves in the environment. To use the map and LiDAR data for localization, it is necessary to find a point cloud correlation between the sensor's measurement and the provided map [1]. This approach is called scan matching. Our current approach utilizes NDT scan matching to solve the localization problems, this approach is faster in computation, more consistent and robust than the common ICP approach [2].

However, TEASER is robust as well, it can also solve problems without correspondences (e.g., hypothesizing all-to-all correspondences) where it outperforms ICP, and it is more accurate than Go-ICP while being magnitude faster [3]. This is the main motivation of this project that we want to compare the performance between both TEASER and NDT since both claim to be faster than ICP. However, there is no conducted comparison research of the two approaches. Our project goal is to have an implementation of TEASER in our CAV to compare it with NDT.

2. Related Work

In this section, we discuss the related works for the algorithms and their computation process.

2.1 TEASER Algorithm

TEASER is an algorithm that computes estimation between outliers from two-point cloud images. Within the two images there are multiple key points that will give us knowledge of where the two images align with each other, correspondents. The correspondents will have an average slope with other points becoming inliers. If they do not fall under the inlier's aspect of the slope, then they are outliers. Having knowledge of the corresponding inliers or outliers then matching between the two-point cloud images can take place. The TEASER algorithms are seen as follows [3]:

Algorithm 1: *Truncated least squares Estimation And SEmidefinite Relaxation (TEASER)*

Data: points (a_i, b_i) and bounds $\beta_i (i = 1, ..., N)$, threshold c^2 (default: $c^2 = 1$), graph $G(V, \mathcal{E})$ (default: G describes the complete graph);
Result: $\hat{s}, \hat{R}, \hat{t}$;

% Compute TIM and TRIM;
$b_{ij} = b_j - b_i, a_{ij} = a_j - a_i, \delta_{ij} = \beta_i + \beta_j, \forall (i,j) \in \mathcal{E}$;
$s_{ij} = \frac{\|b_{ij}\|}{\|a_{ij}\|}, \alpha_{ij} = \frac{\delta_{ij}}{\|a_{ij}\|}, \forall (i,j) \in \mathcal{E}$;
% Decoupled estimation of s, R, t;
$\hat{s} = \texttt{estimate}\ s(\{s_{ij}, \alpha_{ij} : \forall (i,j) \in \mathcal{E}\}, c^2)$;
$G'(V', \mathcal{E}'') = \texttt{maxClique}(G(V, \mathcal{E}'))$ *% prune outliers*;
$\hat{R} = \texttt{estimate}\ R(\{a_{ij}, b_{ij}, \delta_{ij} : \forall (i,j) \in \mathcal{E}''\}, c^2, \hat{s})$;
$\hat{t} = \texttt{estimate}\ t(\{a_{ij}, b_{ij}, \beta_i : i \in V'\}, c^2, \hat{s}, \hat{R})$;
return $\hat{s}, \hat{R}, \hat{t}$;

1. For each point in source point cloud, A, and in reference point cloud, B, find the correspondents between A and B.
2. Calculate the scale (TIMs).
3. Calculate the translation and rotation (TRIM).
4. Return transformation estimation.

TEASER calculates the transformation estimation using outliers between the two-point cloud images.

2.2 NDT Algorithm

In the NDT algorithms estimation is similar to the classic ICP algorithm. The estimation of the rotation, and translation are being calculated by using the Gaussian distribution, which is different than ICP's Euclidean distance, between points. The algorithms steps are as follows [4]:

1. For each point in reference point cloud, Y, insert into a voxel bi in set B voxels.
2. For each voxel in B, calculate the mean and covariance.
3. Till registration converges, for each point in source point cloud, X, calculate the Gaussian distribution of each voxel and the score of transformation.

NDT will be able to find what it believes is the best transformation between the 2-point cloud images.

Algorithm 2: NDT Registration

Data: Two point clouds: X, and Y;
Result: An aligned $\bar{p}$ being the point cloud;
% Initialisation:
% Allocate cell structure B
forall *points* $\bar{y}_k \in Y$ **do**
  find the cell $b_i \in B$ that contains $\bar{y}_k$
  store $\bar{y}_k$ in b_i
end
forall *cells* $b_i \in B$ **do**
  $Y' = \{\bar{y}_1, \cdots, \bar{y}_m\} \leftarrow$ all points in b_i
  $\bar{\mu}_i \leftarrow \frac{1}{n}\sum_{k-1}^{m} \bar{y}_k$
  $\sum_i \leftarrow \frac{1}{m-1}\sum_{k-1}^{m}(\bar{y}_k - \bar{\mu})(\bar{y}_k - \bar{\mu})^T$
end
% Registration:
while *not converged* **do**
  $score \leftarrow 0$
  $\bar{g} \leftarrow 0$
  $\mathbf{H} \leftarrow 0$
  forall *points* $\bar{x}_k \in X$ **do**
    find the cell b_i that contains $T(\bar{p}, \bar{x}_k)$
    $score \leftarrow score + \bar{p}(T(\bar{p}, \bar{x}_k))$
    update $\bar{g}$
    update $\mathbf{H}$
  end
  solve $\mathbf{H}\Delta\bar{p} = -\bar{g}$
  $\bar{p} \leftarrow \bar{p} + \Delta\bar{p}$
end

Figure 1 Connected Autonomous vehicle System.

3. System and Tools

In this section, we will introduce our system design and tools implementation used to conduct our experiment.

Our project and all experiments will be based on the GEM vehicle platform as shown in Figure 1. This car is equipped with sensors such as Velodyne-LiDAR, camera, and a high-performance computer [5]. The purpose of this project is to first use Velodyne-LiDAR to collect raw data, then use TEASER and NDT algorithms to do 3D point cloud registration, and finally utilize the transform output to align point clouds to merge them together thus creating a new point cloud.

3.1 ROS and Autoware

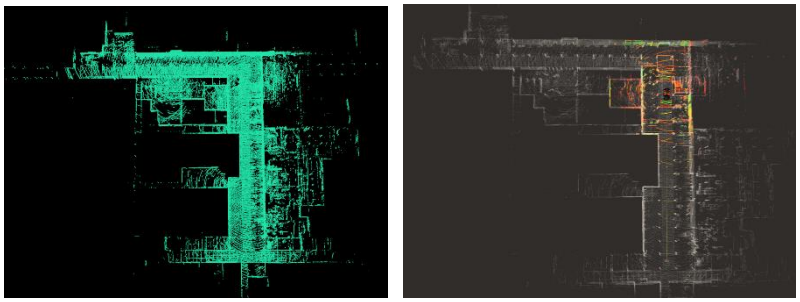
ROS and Autoware are our software platforms which have been installed on the high-performance computer. Robot Operating System (ROS) is a set of computer operating system architecture designed for robot software development. It is an open-source meta-level operating system (post-operating system) that provides operating system services, including hardware abstract description, step-by-step driver management, execution of shared functions, message transfer between programs, and program release package management [6]. Autoware is an open-source platform or software for autonomous driving technology, which based on ROS and provides algorithms and alternatives for perception, location mapping, detection and planning required for autonomous driving navigation, as well as an easy-to-use graphical user interface (GUI) - Runtime Manger [7].

3.2 Autoware Runtime Manager

Runtime Manager is the GUI of Autoware which makes it easy for simulation and operation of autonomous driving vehicle. We can launch ROS nodes using runtime manager. For the LiDAR data collection, the specific operation is to first launch the Velodyne-LiDAR sensor, and then run the ROSBAG Record node in the runtime manager. Then select the topic(/point_raw) related to the LiDAR sensor to start recording. The recorded LiDAR data will be saved in ROSBAG format, which includes all the raw 3D point clouds, data size, topic, time, and other information. We have recorded several sets of point cloud data in different scenarios, which will be used in our experiment.

3.3 LiDAR Dataset Collection

We have collected several sets of 3D point cloud data using the above method. All the data were collected inside the UNT Discover Park building. We used the raw LiDAR data to generate a visual map through the NDT mapping algorithm, shown in Figure 2, you can see that our experiment starts from the downstairs in our CSE department, and the terminal point is at the entrance of the Discover Park cafeteria.



(a) (b)

Figure 2 (a) 3D Point Cloud Map; (b) Simulate 3D Point Cloud Map using RVIZ tool.

4. Implementation

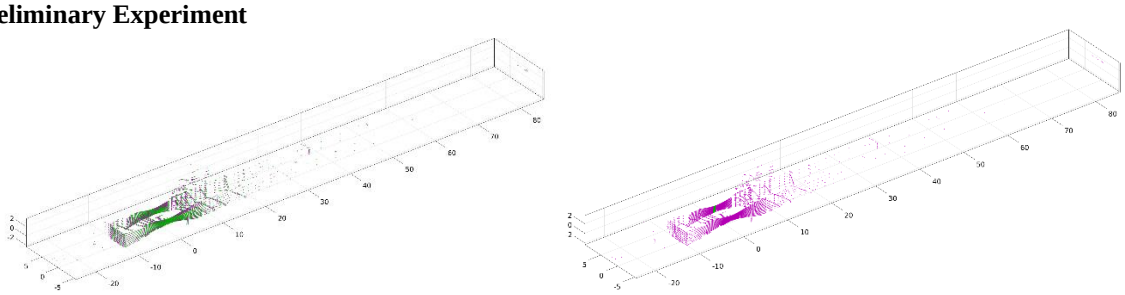
In this section, we discuss the implementation of the experiment. We will incorporate data manipulation and not two different LiDAR data files as our first steps of preliminary evaluation. Our plan is to start from a data manipulation to verify the algorithms are working. From there we will add additional steps till our work showcases that we can generate a map from point clouds. However, as mentioned before we want to verify the performance of the algorithms efficiency and any other metrics systems that allow us to find comparisons between the algorithms.

In the algorithm's code, we have integrated time duration of start and stop around the solving of the registration between point clouds. This will allow us to view the time it takes to calculate the registration between the two-point clouds.

5. Performance Evaluation

In this section, we present our preliminary real-world experiment evaluation utilizing the two registration algorithms.

5.1 Preliminary Experiment



(a) (b)

Figure 3 (a) Preliminary Result run of NDT; (b) Preliminary Result run of TEASER.

Our experiment is to be conducted with repeatable verification evaluations on TEASER and NDT; this will allow us to verify their runtime claims. We will take measurements of the runtime and efficiency performance of TEASER and NDT to find comparisons between the two-algorithms. As we conducted are preliminary experiment, we took 5 different point cloud files and ran an average of 5 run to get the algorithm's runtime. Figure 3(a) and 3(b) is a point cloud representation of one of these runs.

5.2 Preliminary Evaluation

From our experiment we had gathered results seen here in this table:

PCD Files	NDT Avg (ms)	TEASER Avg (ms)	# Of Points
1637535760.587973000	693.4	304.8	28504
1637535750.501887000	1476.6	305.4	28531
1637535634.411389000	786.4	311.4	28531
1637535733.960749000	2699.8	318.2	28611
1637535759.680210000	1204.8	304.8	28530

Table 1 Runtime averages of the NDT and TEASER algorithm with corresponding PCD file.

From the table we can see that TEASER has a quicker runtime with a consistent average between all 5-point cloud files. We can deduce the reason why TEASER, in the implementation TEASER would use correspondents between the two-point clouds. Therefore, TEASER does not go through all the points in the point cloud file. Whereas, in the NDT implementation it would down-sample the point cloud thus be inconsistent and would go through all the points in the down-sample point cloud.

7. Conclusion

This analysis is a work in progress as we are continuing to complete a more in-depth analysis between NDT and TEASER. We will address issues within the implementation of the algorithm along with gathering log data from the results once the computation is completed such as correspondence, and transformation error. We have prospecting applications that are desired by the autonomous vehicles research community as for mentioned to generate high-definition maps then these maps can be used for localization or object detection inferencing.

References

[1] Robotics Knowledgebase, "NDT matching with Autoware," 11-May-2020. [Online]. Available: https://roboticsknowledgebase.com/wiki/

simulation/NDT-Matching-with-Autoware/.
[2] Autoware, "NDT Literature Review." [Online]. Available: https://autowarefoundation.gitlab.io/autoware.auto/AutowareAuto/ndt-literature-review.html.
[3] H. Yang, J. Shi, and L. Carlone, TEASER: Fast and Certifiable Point Cloud Registration. arXiv, 2001.07715, 2020.
[4] Merten, Heinz. "The three-dimensional normal-distributions transform." threshold 10 (2008): 3.
[5] Dhakal, Sudip, Deyuan Qu, Dominic Carrillo, Qing Yang, and Song Fu. "OASD: An Open Approach to Self-Driving Vehicle." In 2021 Fourth International Conference on Connected and Autonomous Driving (MetroCAD), pp. 54-61. IEEE, 2021.
[6] Robot Operating System. [Online]. Available: https://en.wikipedia.org/wiki/Robot_Operating_System.
[7] Autoware.AI. [Online]. Available: https://www.autoware.org/autoware-ai.
[8] H. Yang, J. Shi, and L. Carlone, “Mit-spark/teaser-plusplus: A fast and robust point cloud registration library,” GitHub. [Online]. Available: https://github.com/MIT-SPARK/TEASER-plusplus.

An Overview of Cooperative Perception in Autonomous Vehicles

Kaitlynn Whitney
Department of Computer Science and Engineering
University of North Texas, USA
kaitlynnwhitney@my.unt.edu

1. Introduction

The Society of Automotive Engineers (SAE) have published guidelines for six autonomous driving levels (0-5) [14]. The goal of autonomous vehicles is to achieve a level 5 autonomous vehicle. Dynamic Driving Task (DDT) refers to all the real-time operational and tactical functions that are required to operate a vehicle in on-road traffic (motion control (steering, acceleration and deceleration), monitoring driving environment (object and event detection and response - OEDR), maneuver planning, etc.), it does not include strategic functions, selection of destinations or trip scheduling [14].The Operational Design Domain (ODD) will refer to the operating conditions specifically designed for that feature to function (the essential presence or absence of traffic, roadway characteristics, or environmental, geographical, and time-of-day restrictions) some of these conditions change periodically during on-road operations [14].

The classification of the six autonomous levels listed in this section can be summed up by the logic flow diagram (figure 1) provided by [14]. Level 0 is the standard on-road vehicle with no DDT assistance from the vehicle and can be referred to as the N o Driving Assistance system. The vehicle can have active safety systems, such as a vehicle-to-vehicle (V2V) warning system. Level 1, the driver assistance system, has some driving automation but is still reliant on the human driver for the remaining DDT functions. The key thing about a driving assistance automation system is that the system can perform either the lateral (speeding up or slowing down) or the longitudinal (acceleration or deceleration) vehicle motion, but not in unison. For level 2, or partial driving automation system, the automation takes care of both the lateral and longitudinal vehicle motion simultaneously. The human driver supervises the drive and completes the OEDR of the ODD as the DDT is taken care of by the automated system. The human driver must not fully rely on the autonomous vehicle and be ready to intervene at any given point.

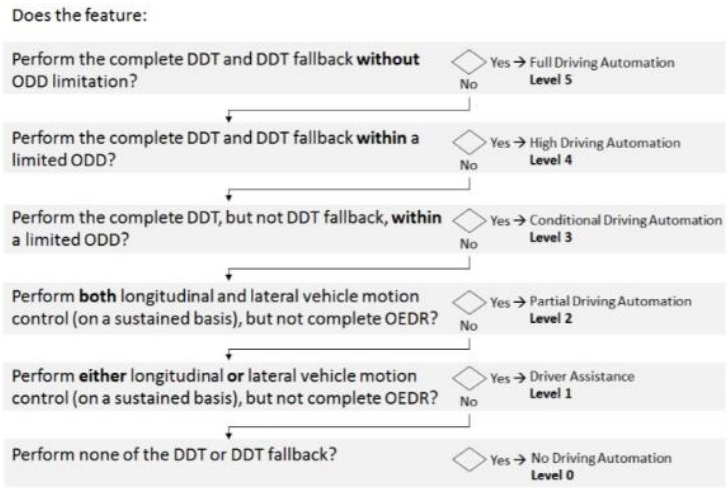


Figure 1: Simplified logic flow diagram for assigning driving automation level to a feature

A level 3 autonomous driving system, or conditional driving automation, still relies on human intervention though at the request of the automated driving system (DDT fallback) in order to achieve a minimal risk condition under certain circumstances. For example, a level 3 automation driving system is able to fully operate DDT features in a low-speed environment such as stop-and-go traffic [14].

Level 4, or high driving automation, does not require a human driver to intervene, the vehicle can take control of all DDT (including curb-to-door services) and achieve a DDT fallback system if a human driver does not intervene. If the autonomous vehicle reaches its ODD limit (during certain weather conditions, geographical restriction, or time-of-day) it will issue an alert to the passenger that they need to take over in order to complete their trip.

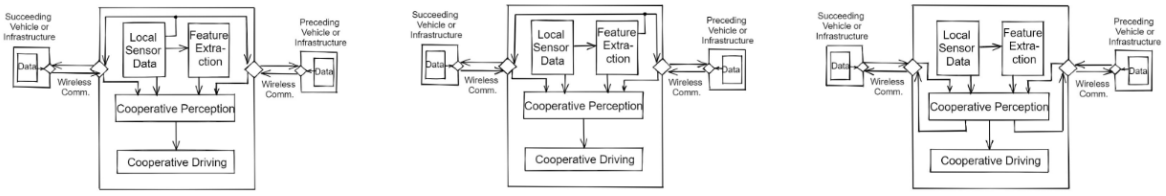
For level 5 (f ull driving automation), the autonomous vehicle has complete control of DDT and DDT fallback and does not require any human supervision. A full driving autonomous vehicle can operate under all road conditions in which can be reasonably operated initially by a human driver. There are no restrictions for the vehicle to operate during

certain weather conditions, geographical restriction, or time-of-day. There could be conditions in which the driver will not be able to manage a driven environment (blizzard, flooded roads, glare ice, etc.) [14].

The remaining sections of this paper are organized as follows. Section 2 breaks down the different fusion levels of an autonomous vehicles system architecture. Section 3 covers cooperative perception and the multiple challenges involved. Future experiments are discussed section 4. And finally, the conclusion of the paper is in section 5.

2. System Architecture

The system architecture relies on the three subsystems shown in figure 2: feature extraction, cooperative perception, and cooperative driving. Raw data is processed at the feature extraction and cooperative perception locations which is used by cooperative driving to warn the driver when to be cautious. The type of data received for cooperative perception from connected vehicles, via wireless communication, is determined by the fusion level.



(a) $Low-level\ Fusion$ (b) $Feature-level\ Fusion$ (c) $High-level\ Fusion$

Figure 2: System Architecture at Three Fusion Levels

There are three fusion levels [7]: low-level (figure 2a), feature-level (figure 2b), and high-level (figure 2c. The level of fusion determines what and when local data is transmitted to connected vehicles. A low-level fusion (figure 2a) transfers raw data directly from the sensors to connected vehicles. Low-level fusion allows for more accuracy when processing data from distinct manufacturers [8], though requires large bandwidth since the raw data files are the largest. The issue is that the communication delay increases in uncertainty with the increase of the data size [4]. Feature-level fusion (figure 2b) is when local data is passed after the features are extracted from raw data but prior to cooperative perception calculations. High-level fusion (figure 2c), sends local data after the cooperative perception calculations and is the most common approach as the complexity is less than the other two fusion levels. High-level fusion allows for the smallest data transfer size of the three levels. High-level fusion requires a reference object to be shared between vehicles and is best when communicating with vehicles whose components are from the same manufacturer [8].

The sensors on a vehicle consist of three different types: motion, range, and vision. Motion sensors collect speed and direction; range sensors consists of light detection and ranging (LiDAR) and radio wave (radar) sensors; vision sensors are cameras that collect images or video of the vehicle's surroundings. Feature extraction is where some initial calculations for cooperative perception occur and utilizes the data from motion and range sensors. The data from motion sensors is used in the calculation of the vehicle's change in position over time. Range sensor data is utilized to calculate the location and tracking information of an object. The feature extraction results are used by the cooperative perception block for further calculations.

The cooperative perception box is where local (raw sensor and feature extraction) and remote data are utilized to assist with various calculations pertinent to safe functionality of autonomous vehicles. Cooperative perception allows the vehicles to become aware of its surrounding environment. The local data for detection and tracking of objects is combined with remote data to assist with any hidden objects that the local vehicle's sensors were not able to detect allowing the vehicle to make movement predictions (slow down, stop, lane changing, etc.). A more in-depth discussion about cooperative perception can be found in section 3.

The job of the cooperative driving section is to notify the driver as soon as they should be cautious, based on the position of surrounding objects. Cooperative driving relies on the calculations provided by the cooperative perception box to determine when notifications are necessary and when to move (achieved through driver warning and lane changing algorithms). More on cooperative driving can be found in [4] and [3].

Wireless communication between connected vehicles is how local data is shared remotely and will be referred to as messages in accordance with [4]. There is a trade-off between communication performance and information quantity so the message size and transmission period should be carefully considered [11]. A more in-depth look into the wireless communications can be found in section 3.

3. Cooperative Perception

Cooperative Perception, or Cooper [8], is the process of using shared remote data from connected vehicles in order to increase the overall accuracy of the local data. The data shared between the vehicles can help identify hidden objects that local sensors of a vehicle may not have sensed. The vehicle achieves an understanding of its surroundings through object detection and map merging and uses wireless communication to receive and transfer data between connected vehicles.

Object Detection

In order for a vehicle to navigate the roads safely, it must interpret sensor data to recognize obstacles on the road (traffic signs, road markings, pedestrians, etc.). Data from connected vehicles can help improve the accuracy of object detection as well as assist the vehicle in identifying hidden objects that were not sensed by local sensors. 2D object detection relies on data received from image sensors such as cameras or video and 3D object detection relies on LiDAR sensors for object detection in the vehicle's surroundings.

Deep Many-Tasks (Deep MANTA) [6] introduces a convolutional network that detects vehicles simultaneously, localize vehicle parts (even when the parts are not visible), produces a visible characterization, and determines a 3D dimension estimation of the vehicle with the use of 2D imaging. Deep MANTA relies on is a new coarse-to-fine architecture which boosts vehicle detection.

LiDAR point clouds have an advantage of spatial dimension over 2D images though re-constructed data from different LiDAR devices could have different point densities. The higher in density the LiDAR is, the higher its resolution (resulting in higher accuracy) but the more expensive it is. An industry standard 64-beam LiDAR, provides the highest density while a 16-beam LiDAR provides sparser data though is much more affordable. Researchers at [8] propose a detection method that works on both high-density and low-density data. The approach involves the use of Sparse Point-cloud Object Detection (SPOD) since it can modify low density point clouds. Researchers at [8] suggest the use of cooperative sensing methods to improve the overall detection accuracy of the LiDAR.

Due to the price in LiDAR hardware, image data can help to improve the accuracy of lower-tier LiDAR equipment. [10] propose a novel Camera-LiDAR Object Candidates (CLOCs) fusion networks significantly improves the performance of single-modality detectors through a low-complexity multi-modal fusion framework. [5] apply a new approach to extract low-level visual features based on spatial pooling to achieve high object detection performance with a focus on pedestrian detection and tracking.

Map Merging

Map merging assists the vehicle in understanding its surrounding on the roads. With the use of range sensor technology, scan matching has been essential for map building, map merging, and pose estimation [4]. The Cooperative Perception, or Cooper [8], is the process of using shared remote data from connected vehicles in order to increase the overall accuracy of the local data. The data shared between the vehicles can help identify idea behind scan matching is to find a transformation that correlates between the scanned local data and the range sensor data. One of the goals of researchers at [4] is to establish a spatial map that is sufficient for driving control assistance with the use of scan matching exploring both closed-form solution (ICP) and correlative scan matching (CSM).

ICP finds the closest point as the correspondence and uses a formula to find where the solution converges [4]. There is no guarantee that the closest point is the correct corresponding point leading to many cases where the maps are partially overlapped or scan points do not match up exactly. Scan points are limited by the hardware of a sensor resulting with differences in sensing range or resolution. [4] suggests that the closest point should be limited by some threshold distance.

CSM relies on a probabilistic scan matching method [4]. Through the current observations of the data, CSM finds a pose that is most probable by comparing previous observations of the observation model of a map, pose of an observer, and the sensor readings. CSM is able to provide a strong solution by finding the global maximum value [1].

When merging map data from multiple vehicles, the sensor configuration can vary between vehicles giving a level of complexity when trying to identify the relative positions as the maps for each vehicle will have varying scan points. Areas that do overlap may not be sufficient enough to be useful due to the longer safety gaps for collision avoidance [4]. Non-vehicle objects (trees, moving pedestrians, etc.) add more complexity to the situation.

Wireless Communication

Wireless communication is essential for cooperative perception as it allows connected vehicles to share data. One of the many considerations when using wireless communication is the amount of data that will be transmitted between vehicles, which can be determined by the fusion level as discussed in section 2. The size should be carefully considered as communication delay becomes more uncertain as the size of data increases [4].

Researchers at [3] tested the movement of data utilizing four different wireless connections, IEEE 802.11g, IEEE802.11n, 3G HSDPA, and 4G LTE. Performance in the average communication delay was better for IEEE 802.11g and IEEE 802.11n wireless communications than 3G HSDPA and 4G LTE. Though, the performance of IEEE 802.11g and IEEE 802.11n both decrease as the distance between vehicles is increased while 3G HSDPA and 4G LTE were not affected by the distance between the vehicles [3]. Research conducted by [11] aims to improve the reliability of vehicle-to-everything (V2X) communication utilizing the common ns-3 network simulator. The connections tested use the IRS-G5 V2X standard, which is based on the IEEE 802.11p Wi-Fi, and transmit with the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. The reliability of the V2X communication depends on the channel load [11].

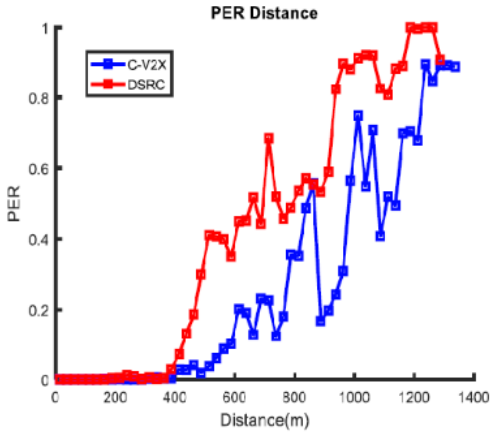


Figure 3: PER Comparison of IEEE 802.11p (red) and LTE-V2X (blue) by [9]

Cellular V2X (C-V2X) is being researched by [9] to leverage and enhance current cellular network features and elements to enable low-latency and high-reliability communications among various nodes in vehicular networks. IEEE 802.11p is considered to be a dedicated short-range communications (DSRC) which is considered a V2X technology by the Institute of Electrical and Electronics Engineers (IEEE) organization. For C-V2X, the connection relies on cellular radio instead of WLAN for the connection. Figure 3, from [9], shows the comparison of the packet error rate (PER), which is used to test the performance of an access terminal's receiver of IEEE 802.11p (red) and C-V2X (blue). The C-V2X connection is able to establish a better wireless communication for a distance of approximately 600m.

4. Future Experiments

Security is a huge concern with having connected vehicles share information. Two notable papers pertaining to autonomous vehicle security are [2] and [12]. Researchers from [2] bring up the importance of security and address many challenges pertaining to unmanned autonomous vehicles. The researchers suggest a new way to view various unmanned autonomous vehicles with spatially secure communication. Researchers from [12] work to improve security through a multi-layer defense framework in order to achieve a secure flow for information from external communication to the physical autonomous vehicle.

Researchers from [9] have a few suggestions in further development of the C-V2X communication technology. Multi-access Edge Computing (MEC) is a potential upcoming technology of 5G networks. To integrate C-V2X with MEC include various challenges in order to achieve efficient convergence of the communication-computing-storage resources [9].

Other ways to assist with the advancement of cooperative perception is through the use of edge devices, which is an infrastructure in which the autonomous vehicle can receive information about detected objects in the area. Researchers at [13] developed a Vehicular Edge Computing Scheduling Pipeline for connected and autonomous vehicles. The edge computation assists the autonomous vehicles with data transfer and fusion for cooperative object detection of multiple vehicles to assist with the autonomous vehicle's perception of a large area. Object detection is one of the foundations that must be further developed for safe self driving autonomous vehicles. Works such as [5] have combined research to utilize both image and LiDAR detection. While others [8] focus

on advancing specifically detection through LiDAR. With an increase in accuracy for detected and tracked objects, autonomous vehicles will become safer drivers.

5. Conclusions

Through wireless communication, vehicles are connected in order to share local data. Cooperative perception in autonomous vehicles is the idea of using the shared data in order to obtain higher accuracy in object detection and map merging to procure a safer self driving potential. Data from motion, range, and vision sensors are used from both the local and remote vehicles to perform calculations for cooperative perception. Cooperative perception calculations are used in cooperative driving to assist the driver in maintaining safety while driving and performing safe lane changes. Wireless communication reliability is a hurdle to overcome in order to achieve full automation. The size of the data being sent is indirectly proportional to the communication certainty of the wireless network. There is still much to accomplish in security, wireless communication, infrastructure connection, and cooperative perception in order to achieve a safe and fully autonomous self driving vehicle.

References

[1] Edwin B. Olson. “Real-time correlative scan matching”. In: 2009 IEEE International Conference on Robotics and Automation. 2009, pp. 4387–4393. doi: 10.1109/ROBOT.2009.5152375.
[2] Seong-Woo Kim and Seung-Woo Seo. “Cooperative Unmanned Autonomous Vehicle Control for Spatially Secure Group Communications”. In: IEEE Journal on Selected Areas in Communications 30.5 (2012), pp. 870–882. doi: 10.1109/JSAC.2012.120604.
[3] Seong-Woo Kim, Wei Liu, Marchelo H. Ang Jr., Emilio Frazzoli, and Daniela Rus. The Impact of Cooperative Perception on Decision Making and Planning of Autonomous Vehicles. July 2015. doi: 10.1109/MITS.2015.2409883.
[4] Seong-Woo Kim, Baoxing Qin, Zhuang Ji Chong, Xiaotong Shen, Wei Liu, Marcelo H. Ang Jr., Emilio Frazzoli, and Daniela Rus. Multivehicle Cooperative Driving Using Cooperative Perception: Design and Experimental Validation. Apr. 2015.
[5] Sakrapee Paisitkriangkrai, Chunhua Shen, and Anton van den Hengel. “Pedestrian Detection with Spatially Pooled Features and Structured Ensemble Learning”. In: IEEE Transactions on Pattern Analysis and Machine Intelligence 38.6 (2016), pp. 1243–1257. doi: 10.1109/TPAMI.2015.2474388.
[6] Florian Chabot, Mohamed Chaouch, Jaonary Rabarisoa, Celine Teuliere, and Thierry Chateau. “Deep MANTA: A Coarse-To-Fine Many-Task Network for Joint 2D and 3D Vehicle Analysis From Monocular Image”. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). July 2017.
[7] Juwang Shi, Wenxiu Wang, Xiao Wang, Hongbin Sun, Xuguang Lan, Jingmin Xin, and Nanning Zheng. “Leveraging Spatio-Temporal Evidence and Independent Vision Channel to Improve Multi-Sensor Fusion for Vehicle Environmental Perception”. In: 2018 IEEE Intelligent Vehicles Symposium (IV). 2018, pp. 591–596. doi: 10.1109/IVS.2018.8500665.
[8] Qi Chen, Sihai Tang, Qing Yang, and Song Fu. Cooper: Cooperative Perception for Connected Autonomous Vehicles based on 3D Point Clouds. May 2019.
[9] Shanzhi Chen, Jinling Hu, Yan Shi, Li Zhao, and Wen Li. “A Vision of C-V2X: Technologies, Field Testing, and Challenges With Chinese Development”. In: IEEE Internet of Things Journal 7.5 (2020), pp. 3872–3881. doi: 10.1109/JIOT.2020.2974823.
[10] Su Pang, Daniel Morris, and Hayder Radha. “CLOCs: Camera-LiDAR Object Candidates Fusion for 3D Object Detection”. In: 2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). 2020, pp. 10386–10393. doi: 10.1109/IROS45743.2020.9341791.
[11] Gokulnath Thandavarayan, Miguel Sepulcre, and Javier Gozalvez. Generation of Cooperative Perception Messages for Connected and Automated Vehicles. Dec. 2020. doi: 10.1109/TVT.2020.3036165.
[12] Cong Gao, Geng Wang, Weisong Shi, Zhongmin Wang, and Yanping Chen. “Autonomous Driving Security: State of the Art and Challenges”. In: IEEE Internet of Things Journal (2021), pp. 1–1. doi:10.1109/JIOT.2021.3130054.
[13] Sihai Tang, Zhaochen Gu, Song Fu, and Qing Yang. “Vehicular Edge Computing for Multi-Vehicle Perception”. In: 2021 Fourth International Conference on Connected and Autonomous Driving (Metro-CAD). 2021, pp. 9–16. doi: 10.1109/MetroCAD51599.2021.00011.
[14] Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. Apr. 2021.

Blockchain Meets AI for Resilient and Intelligent Internet of Vehicles

Pranav K. Singh, Central Institute of Technology at Kokrajhar, India
Sukumar Nandi, Indian Institute of Technology Guwahati, India
Sunit K. Nandi, Indian Institute of Technology Guwahati, India
Uttam Ghosh, Vanderbilt University, Nashville, TN, USA
Danda B. Rawat, Howard University, Washington, DC, USA

INTERNET OF VEHICLES (IOV) SYSTEMS OVERVIEW

A. Overview

In the new era of the Internet of Everything (IoE), the traditional VANETs enabled by vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication have evolved to the Internetof Vehicles (IoV). IoV is the concept that connects smart and intelligent vehicles to any other entities around them, such as vehicles, infrastructure, pedestrians, networks, grids, UAVs, etc., through vehicle-to-everything (V2X) or cellular V2X (C-V2X) technologies [1]. The generic view of IoV is shown in Fig. 1.

B. Applications

IoV is expected to solve the major challenges of our transportation by improving road safety, minimizing road congestion, reducing fuel consumption and CO2 emissions, solving parking issues, and minimizing expenses and space by enabling cab sharing, etc. The remarkable advancements in on-board capabilities of vehicles (sensing, computation, storage, communication), radio access technologies (RAT), network architectures, protocol stacks have enabled automated driving and platooning. These advancements brought IoV to the center of Industry 4.0. andled to promising areas of intelligent transportation, vehicle manufacturing, payment services, predictive maintenance, usage-based insurance, intelligent parking, automation, infotainment, software, energy, secure data sharing, data trading, vehicle life cycle, etc. [2].

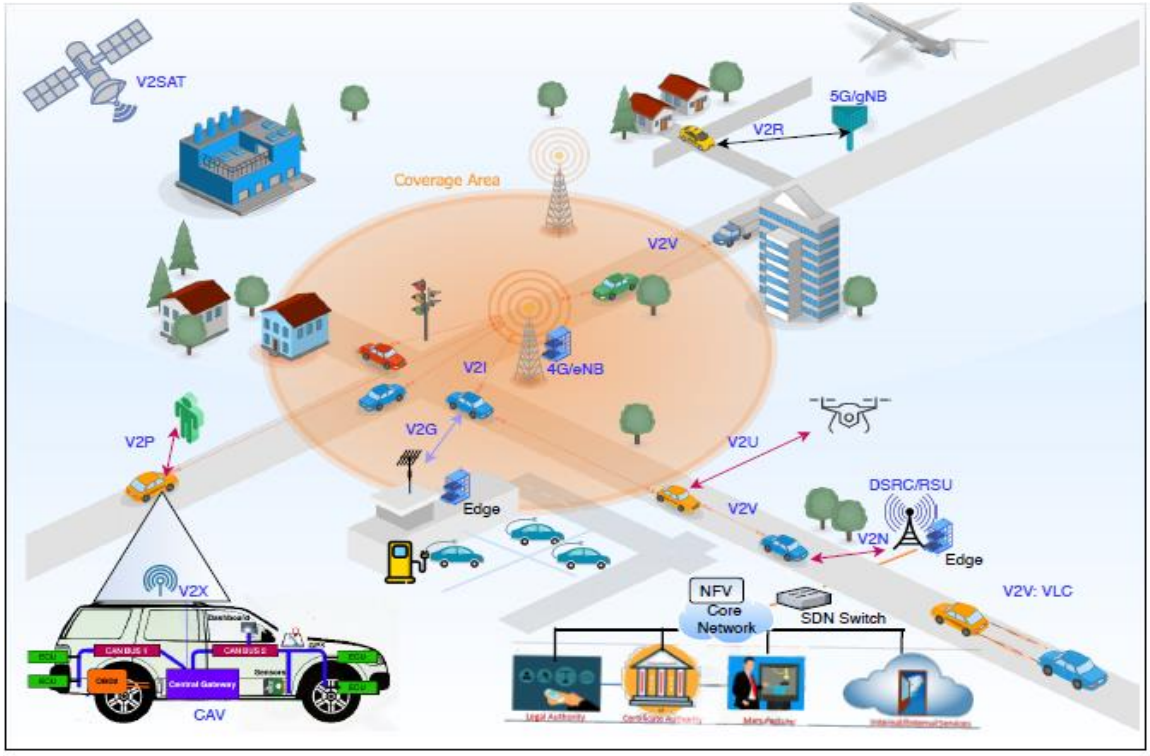


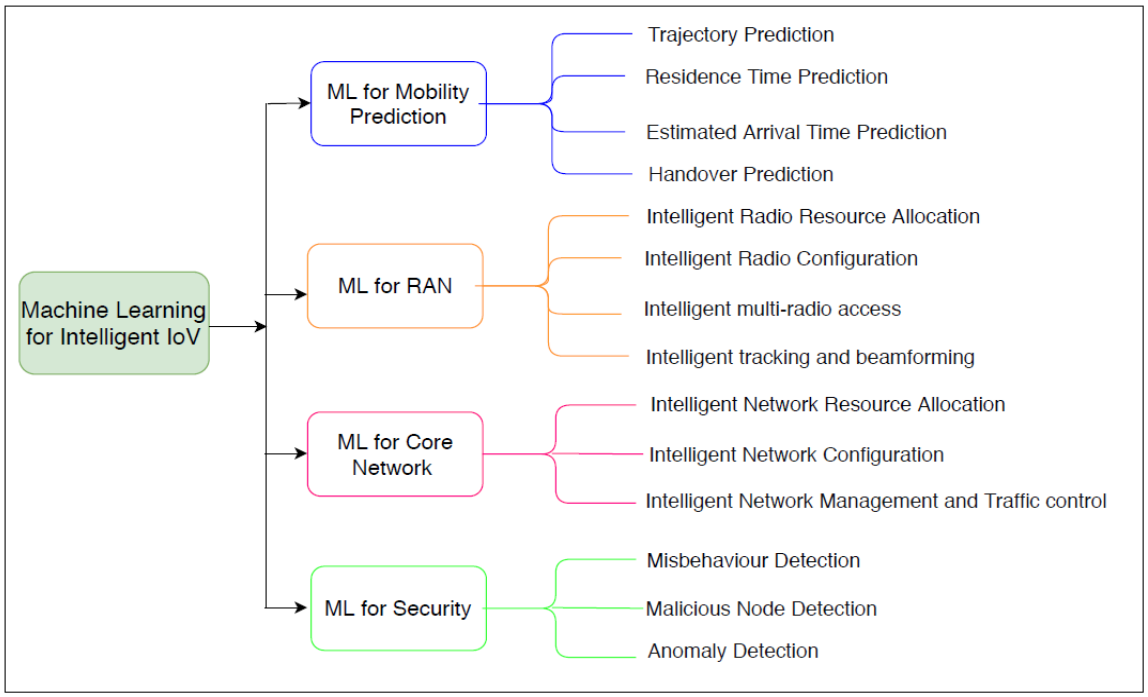
Fig. 1: An Overview of Internet-of-Vehicles

C. Key Enablers

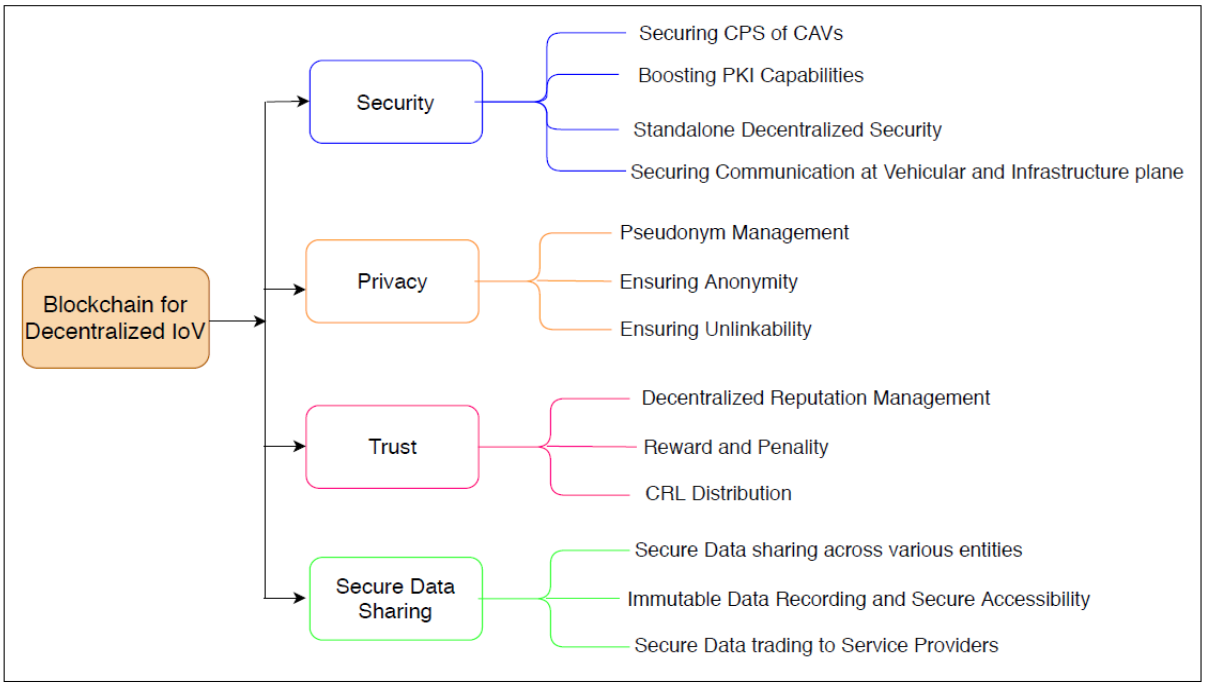
To support a wide variety of IoV applications and services, some of the best-known RATs are DSRC / IEEE 802.11p, Wi-Fi, 4G, new 5G (NR) radio, 6G (envisioned) [3], white space TV, millimeter wave (mmWave) and visible light communications (VLC). Three well-known regional protocol stacks developed over DSRC for vehicular communications are Connected Vehicle (WAVE), the Cooperative-ITS (C-ITS), and the ARIB STD-T109 in the USA, Europe, and Japan,respectively [4]. However, it is soon realized that a single RAT (DSRC) and traditional solutions at core may not support diverse QoS requirements of emerging applications. For instance, these regional protocol stacks over DSRC may not be sufficient to provide the end-to-end latency and throughput requirements of Autonomous Vehicles (AVs). Thus, various technologies are being developed and tested to handle the highly dynamic (variable

density, high mobility, diversified QoS) and complex IoV. The ultimate goal is to provide secure, seamless, ultrareliable low latencyconnectivity and support high throughput and high capacity.

Artificial Intelligence (AI) s a promising approach for making IoV intelligent. AI is imple- mented using machine learning (supervised, unsupervised, reinforcement) models. AI integrationinto IoV can help improve resource allocation and management, decision making, and detect misbehaviors, anomalies, and intrusions. Blockchain is the next revolutionizing technology [5], which can be integrated as a decentralized security framework in the IoV. Leveraging Blockchaininto IoV can improve security, privacy, and trust. It can secure the cyber-physical system (CPS) ofconnected and autonomous vehicles (CAVs), boost PKI capabilities, and enhance the scalability and availability of the IoV security framework. The inherent characteristics of Blockchain can also be capitalized to enable a wide variety of services in IoV, such as secure data sharing and trading among two or more entities.



(a) AI/Machine Learning for Intelligent IoV



(b) Blockchain for Decentralized IoV

Fig. 2: AI and Blockchain for IoV

I. AI AND BLOCKCHAIN FOR IOV

In this section, we discuss major IoV challenges that AI and blockchain can solve.

A. AI for IoV

Fig. 2a lists major IoV challenges such as mobility management, radio, and network resource management, and security [3], where AI/ML can play a vital role.

Finding the vehicle's future position in IoV is challenging because of its highly dynamic nature. Mobility prediction can play a crucial role in various applications and services for IoV.AI and ML can help in an accurate mobility prediction, facilitating better handover and radio resource management and avoiding degradation of the expected QoE and QoS.

The conventional techniques in the radio access network (RAN) may not satisfy the high throughput and ultralow-delay requirement of IoV. Thus, AI/ML techniques are being explored to address the challenges associated with conventional radio resource allocation, radio configuration,multi-radio access, tracking, and beamforming.

The HetNet scenario results in new challenges at the core network of IoV in terms of network resource allocation, configuration, management, and traffic control. The AI/ML techniques are being widely used in IoV for network radio resource allocation, transmission power control, beamforming, load balancing, scheduling, traffic offloading, admission control, dynamic routing,etc.

The cyber-physical systems of smart and connected vehicles and V2X communication are susceptible to various hacks and attacks. Major attacks are denial-of-service (DoS), Replay, Sybil, man-in-middle, bogus and fake information propagation, wormhole, blackhole attacks,etc. The malicious behaviors of IoV users are another big challenge. Although various solutions (PKI, group signature) have been proposed, the detection of malicious behavior, anomaly, and intrusions, and prevention from the mentioned attacks remains the biggest challenge to beaddressed. Various deep learning models are being explored to detect misbehavior and attacks and help the trusted authority take preventive measures.

B. Blockchain for IoV

IoV ecosystem (in-vehicle (sensors), communication (V2X), control, applications, and ser- vices) faces several challenges in terms of security, privacy, trust management, data, and resourcesharing and trading. Fig. 2b lists IoV challenges related to security, privacy, trust, and securedata sharing where blockchain can help.

1) Blockchain to solve the challenges of IoV: The list of IoV challenges that blockchain can solve are as follows:

a) Security, Privacy, and Trust: Integration of sensors and vehicle-to-everything connectivity expands attack vectors for malicious entities. Extensive data sharing and open wireless broadcast attract adversaries to exploit privacy. IoV users with malicious intents exploit existing security flaws to gain over others. The blockchain integration into IoV with smart contracts and an advanced cryptographic approach can address these challenges, improve security, preserve privacy, and build trust.

b) Availability and Fault Tolerance: In a state-of-the-art centralized IoV system, tackling the single point of failure and ensuring data and service availability are among the most significant challenges. The distributed and decentralized nature of blockchain eliminates the reliance on central servers or clouds and allows replication of records among other peers. Thus, blockchain adoption can make IoV fault-tolerant, and resilient [6].

c) Data Sharing: The CAVs generate massive data, which must be shared securely among peers and service providers for safety, traffic, and other services. However, the state-of-the-art data sharing mechanism lacks security, user privacy, reliability, trust, and efficiency. Blockchain has proven its strength to build trust and reliability in similar topologies and is capable of resolving other limitations of secure and private data sharing of IoV.

d) Data and Resource Trading: IoV provides excellent business opportunities for vehicle owners and service providers by enabling the trade of data and resources. However, the existing system does not facilitate such a platform for data and resource trade, which is fair, secure, transparent, and preserves the user's privacy. Blockchain has the potentials to provide a secure, trusted, fair, and decentralized platform for data and resource trading among various IoV entities.

e) Traffic Monitoring and Control: The traffic monitoring (traffic condition, rule violation), automated traffic control & management rely on data generated by vehicles uploaded to RSUs and edges for storage. However, they are vulnerable to attacks related to data availability,data integrity, and user privacy. The immutable nature of blockchain makes it difficult for the adversaries to alter those data. The distributed storage features can enhance accessibility and ensured security against DoS attacks.

f) ITS and Payment Services: With a massive number of vehicles on the road, it is very challenging to implement ITS and other payment services like E-tolls, intelligent parking, usages based insurance, over-the-air update, etc. Blockchain with the smart contract can securely and efficiently implement these services.

C. Joint AI and Blockchain for IoV

In this paper, we propose to leverage the salient and best features of both blockchain andAI for security, privacy and trust-related risks to make IoV resilient and intelligent for better performance. We also present open problems, challenges and requirements and potential solutionsusing ML and blockchain to address aforementioned issues in IoV.

II. The need for Secure and Resilient Vehicular PKI

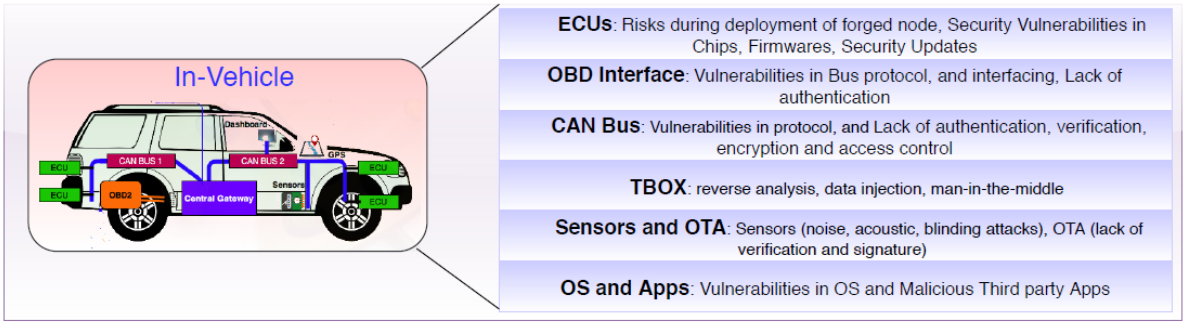


Fig. 3: Security Risks at In-Vehicle System

Over the years, IoV has witnessed security attacks and hacks (DefCon, GeekPwn) [4]. The attack surface is increasing day by day because of feature integrations in the form of intelligence (sensors, ECUs, CAN), applications, services, and HetNet connectivity (V2X). Researchers havealso raised concerns over open V2V communication, which can be exploited by adversaries to breach privacy by linking pseudonyms and tracking the movement [7]. This section highlights security privacy and trust issues and key requirements to these ends.

A. Security and Privacy Risks

Security risks of IoV are on the following aspects In-vehicle (Connected and Intelligent devicesand applications), V2X communication, Service platforms (Edge, Fog, and Cloud), and Data.Fig 3 illustrates how the in-vehicle system of CAV itself is vulnerable to various types of attacks.V2X communications have several security risks associated with them. Mainly due to flaws in the communication protocol stacks, lack of proper security management and detection mech-anisms, and vulnerabilities in RATs interface and mode of communications. Some of the well-known attacks are DoS, DDoS, man-in-the-middle (MiM), Sybil, Greyhole, Blackhole, and Wormhole.

The centralized service platforms on clouds face several security challenges due to the lack of strong access control policies, certificate management, authentication mechanism, audit, intrusiondetection mechanisms, etc. They are also vulnerable to DoS and DDoS attacks.

The security of data generated and exchanged by various entities of IoV is paramount. For example, data related to location, speed, heading, brake, acceleration, tire pressure, fuel consumption, vehicle profile, driving behavior, etc. These data enable safety applications, traffic management, and other services. If these data are falsified or tampered with, it will be a severe threat to drivers and occupants' safety. Traffic management, services, and associated business applications will also be affected.

As shown in Fig. 4, location tracking by dumping V2V safety messages (BSMs and CAMs) and performing syntactic and semantic linkage attacks are among the main location privacyrisks. Since these safety messages are delay-sensitive and disseminated in V2V mode as plaintext(encryption not recommended due to delay), an adversary can easily eavesdrop and extract usefulsensitive Spatio-temporal information. The adversary can use powerful tracking algorithms to reveal the location of the driver and occupants. Data shared with service providers and uploaded to cloud platforms via secure V2I also poses a privacy risk. For example, vehicle data are shared with manufacturers, insurance firms, service centers, map providers, and others for better servicesbut can also be exploited to breach privacy.

B. Misbehaviour and Malicious Activities

Vehicles, roadside sensors (traffic detecting units), RSUs, network elements, and other IoV entities register with trusted authorities and receive certificates (long-term and short-term) and cryptographic materials (key pairs). These materials and certificates are used in communication toensure confidentiality (V2I/I2V, I2I), integrity, authenticity through the signing and verification process. On the other hand, these certifications and materials do not safeguard the IoV from internal threats posed by compromised, malevolent, or misbehaving entities. For example, a vehicle in the network can broadcast misleading and false information about its kinematics, creating chaos and jeopardizing road safety. Similarly, a compromised or faulty traffic detection unit (TDU) can push wrong traffic info (congestion at that road even when no traffic) to the traffic authority (TA). When this incorrect info is propagated to commuters by TA, it may disruptthe entire traffic in that zone. Such types of actions are known as misbehavior in IoV. Malicious entities can transmit misleading information on purpose, while malfunctioning or compromised entities can unintentionally convey wrong info. These attackers are considered insiders and activeattackers since they have the necessary certificates and cryptographic materials to communicate in an IoV. By getting access to their vehicle's CAN bus (since the protocol is vulnerable),these attackers can change the payload of outgoing safety and awareness messages. It's also conceivable for attackers to use a MiM and replay attack to change sensor data. [8].

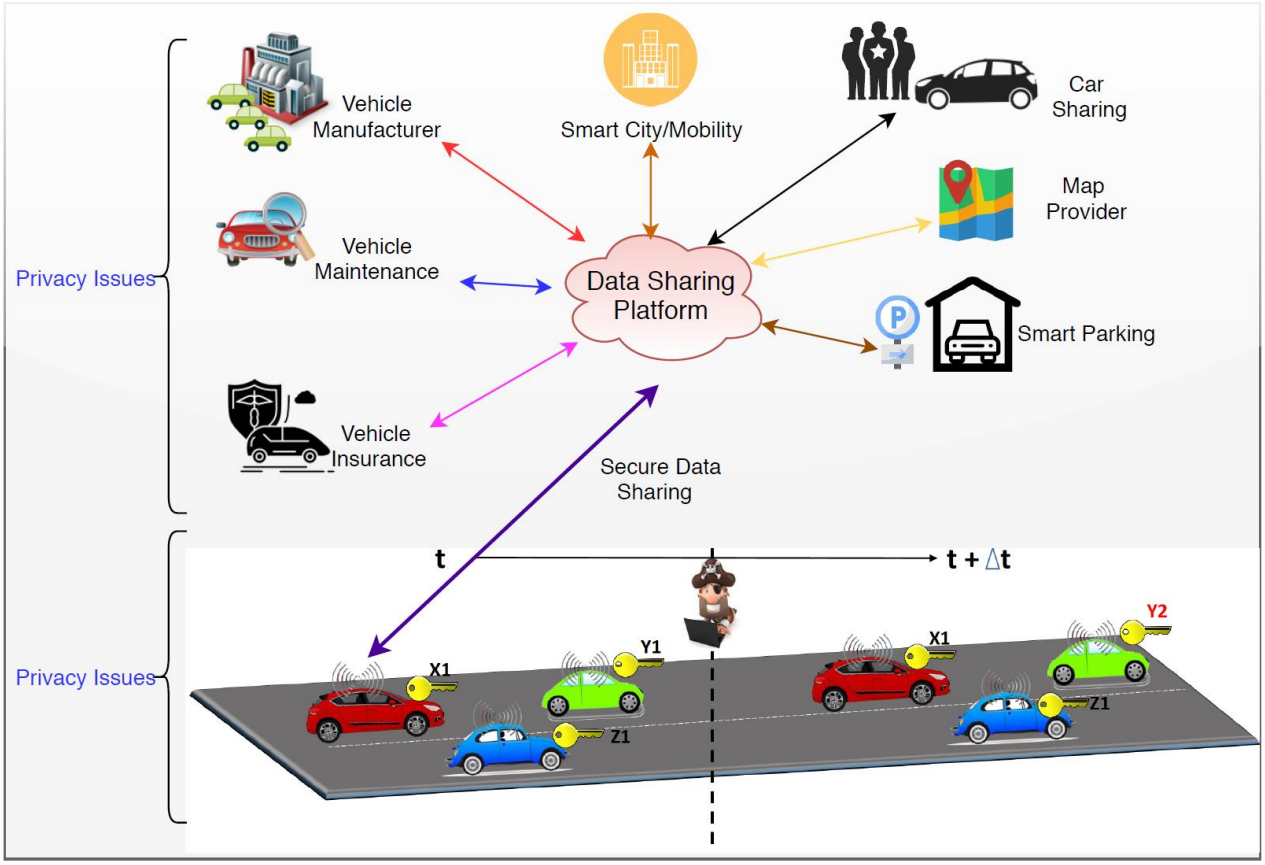


Fig. 4: Privacy Risks in IoV

Fig. 5 depicts an example of one such type of misbehavior known as position falsification attack. The vehicle misbehaves by changing the payload of the safety message to produce bogus positions and broadcasting them through V2V. As depicted in Fig. 5, When the misbehavingnode is close to the position of the intersection, it is overwhelming false location informationand creating confusion for other vehicles [9]. Such types of misbehavior can have disastrous consequences, which may pose a risk to other nodes nearby. Because the message is generatedby an insider (authorized peer), it gets verified and accepted for processing by other receiving vehicles that are part of the same authentication system. As a result, a wide range of safety-relatedapplications that rely on actual position data may be adversely affected.

C. Security, Privacy and Trust Requirements

Avoiding those IoV security and privacy risks and misbehavior may lead to severe conse- quences. Thus, guaranteeing security and privacy and dealing with misbehavior (trust manage- ment) are vital requirements of the IoV for its acceptability. Some of those key requirementsare summarized below.

1) Security Requirements: There is a need for strong security solutions and mechanisms at different levels of IoV.

In-vehicle Security: The in-vehicle system demands advanced hardware security solutions and modules to secure OBD2, ECUs, T-BOX, event recorder, storage, onboard units, sensors (LiDAR, RADAR, GPS, Cameras, TMPS, Gyroscope), etc. There is a need for secure designand development of software (OS and Apps) and firmware of the

vehicles. Over-the-Air update of software and firmware needs to be secure and immutable. The in-vehicle

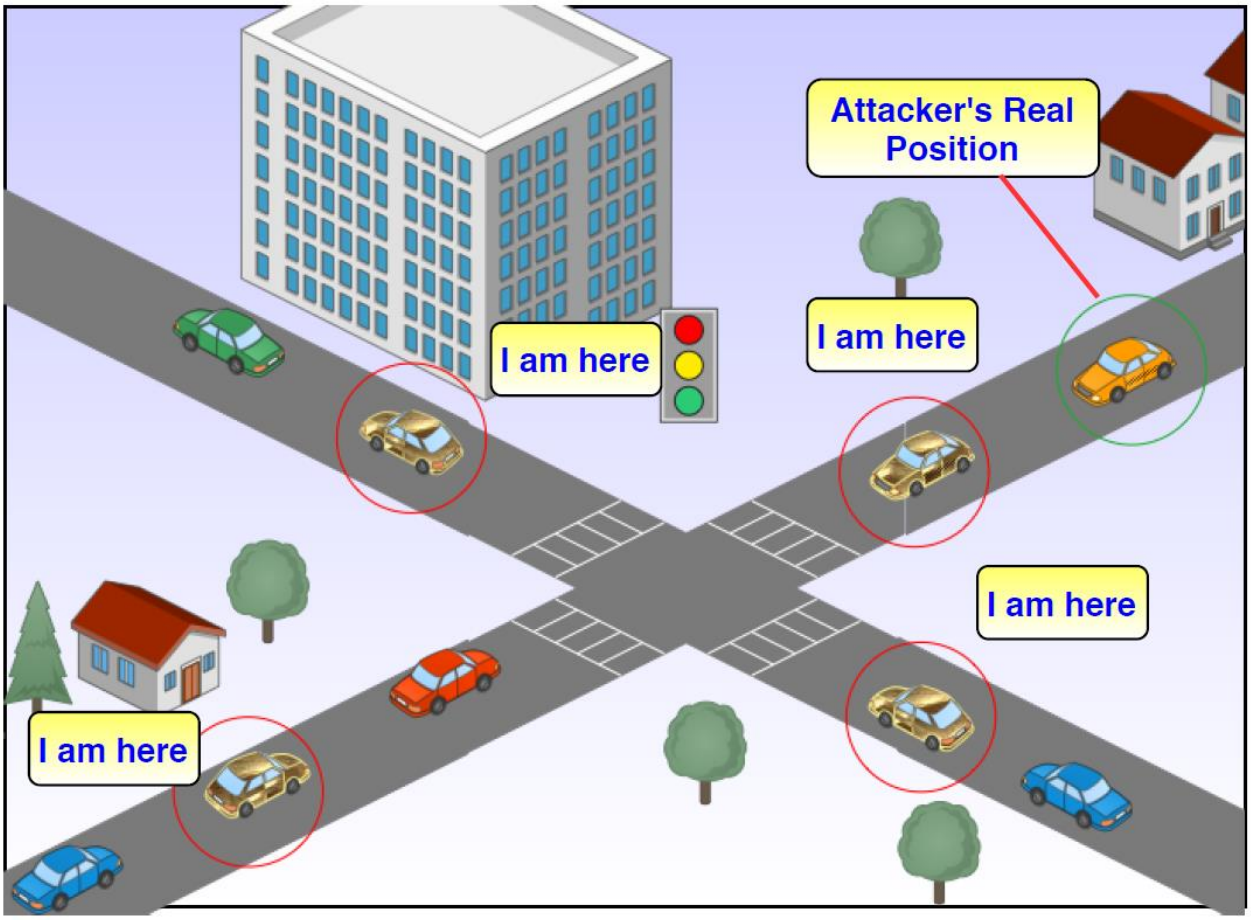


Fig. 5: Misbehavior (Position Falsification Attack) in IoV.

communication modules such as CAN, FlexRay, LIN, Ethernet, Bluetooth, etc., need to be secured. The core security functions such as encryption, access control, authentication, integrity check, signing,and verification need to be utilized. Besides, we need to have a strong firewall and anomaly detection mechanisms for the in-vehicle system.

V2X Security: Securing the HetNet V2X communications (DSRC, cellular, VLC, Wi-Fi, etc.)will be challenging. However, all forms of V2X communication need to fulfill the following security requirements. (1) Advanced cryptographic approaches must be used to fulfill security requirements such as availability, access control, authentication, confidentiality, non-repudiation,integrity, and data verification at different planes of IoV. These should be used in such a way thatdata from an authenticated entity can be transmitted to other entities(s) of the system securely without any alteration or tampering. (2) The consistency and rationality of the communication data need to be protected. (3) The security of data stored at the cloud, fog, and edge and their secure exchange (offloading, uploading) with infrastructure and vehicles must be guaranteed.

Service Platforms: Deployed security capabilities for cloud platforms need to be strengthenedfor IoV services. Essential security requirements are as follows. (1) The data access control mechanisms need to be enhanced and highly secured. (2) Need to ensure secure cross-cloud (OEMs, government agencies, service providers) or fog interactions. (3) There is a need to establish trust among service providers to determine the level of data sharing and exchange. (4) Strong authentication mechanisms, security policies, and firewalls must be in place to secureuser and vehicle data stored in the cloud from malicious users and hackers.

Privacy Requirements:: A strong privacy protection mechanism is required to prevent attackers from exploiting private data about the vehicle, the driver, and the occupants. In IoV, thereare three distinct kinds of privacy protection mechanisms: (1) Vehicle's actual identity should not be revealed. (2) Vehicle's location should not be tracked, and (3) All data exchanged in IoV are protected against privacy. The following are the IoV's most important privacy requirements: [10]:

Minimum disclosure: The information about the user that is absolutely necessary for IoV functionalities should be revealed, and it should be kept minimal.

Anonymity: The usage of pseudonyms provides anonymity, which is one of the most commonways to preserve privacy. For example, the messages delivered by a vehicle should be anonymouswithin a set of subjects, such as potential vehicles, and should not reveal the vehicle's real identity.**Unlinkability:** The use of a pseudonym aids authentication while keeping the true identity hidden. However, if a pseudonym is used in the same context for a long time, it will becomelinkable. Therefore, to achieve the unlinkability of pseudonyms, a set of pseudonyms is used.

To avoid linkability in the given context, these pseudonyms must be changed over time.

Trust Management: In the IoV, trust management is a crucial concept for identifyingand revoking malicious and misbehaving nodes. The adoption of proper trust models helps in determining the trustworthiness of the message and its sender. The following are the major requirements for trust management in IoV: **Misbehavior Detection:** One of the most important aspects of trust management is detecting malicious and misbehaving nodes. Its goal is to keep an eye on the system in order to spot any potentially misbehaving nodes and keep the IoV from straying from its normal course. The technique for detecting misbehavior works in four stages [8]: Local detection of the misbehaving entity, reporting of the misbehavior to the central authority or Misbehavior Authority (MA), assessment by the MA to establish whether the entity is truly misbehaving or simply faulty, and lastly reaction by the registration authority (RA) to protect the system.

Accountability and Traceability: To establish accountability, the specified action should be unambiguously assigned to an individual entity via a fair methodology or protocol. Traceability can help with this in the IoV. Only authorized and highly trusted authorities should be able to trace a pseudonym and link it to the user's true identity. Under some specific instances, such authorities must attempt to trace or map a pseudonym to a real identity. Only MA, for example, should be permitted to do tracing in order to identify the real misbehaving entity.

Revocation and CRL Distribution: When misbehavior is detected, trust management in the IoV should have a fair revocation process that can act effectively. Some reputation-building processes with a reward and penalty system should also be implemented. If the misbehavioris deliberate, the corresponding vehicle should be penalized, and its reputation score should be deducted. Such misbehaving entities should be issued a warning. After crossing the specified threshold, an active revocation (revocation of current certificates) or passive revocation (not able to request more certificates) should be invoked.

Scalability: Since IoV is very dynamic (varying density), it can experience high traffic during peak hours. Thus, the system deployed for trust management must be scalable to deal with alarge number of nodes.

Decentralization: Centralized trust management systems for IoV face several challenges in terms of performance, scalability, robustness, fault-tolerance, privacy, and security [11]. Thus, there is a need for fully decentralized trust management for highly dynamic and distributed IoV.

D. Standardization Efforts

The security standard IEEE 1609.2 specifies security, privacy protection, and trust managementin the connected vehicle protocol stack of the USA. The security standards ETSI TS 102 940V 1.2.1 and ETSI TS 102 941 specify the security, privacy, and trust in the Cooperative-ITS protocol stack of Europe. Various other efforts are underway by SAE (J3061), ITU (FG and SG17), ISO/TC22, CEN, and 3GPP (C-V2X). The IEEE and ETSI standards recommend

using pseudonyms for privacy. However, determining when and how to change pseudonyms is still a work in progress. Misbehavior detection and trust management are still in the initial phases of development under those standards.

AI AND BLOCKCHAIN BASED FRAMEWORK

The integration of AI and Blockchain in IoV can help to a great extent for its security privacy and trust management. In this section, the AI and Blockchain driven solution for the same is discussed through a generic illustration (Fig. 6).

A. ML for Intrusion and Misbehavior Detection

Machine Learning (ML) paradigm facilitates building models that can anticipate the expected behavior by learning from experience. The data-driven approaches enable the machine to learn the relationship, which are hidden, and models for misbehavior detection can leverage this to finddeviations. The deep learning models are found suitable in approximating such relationships.

Over the years, various ML-based solutions have been proposed for intrusion, anomaly, and misbehavior detection in VANETs. As shown in Fig. 6, the ML can help to detect intrusions in in-vehicle network and misbehavior in vehicular as well as infrastructure plane of IoV.

For an in-vehicle network, the intrusion is detected by comparing the current action against theexpected actions. The deep learning models can extract the features from the behavior patterns ofthe nodes and look for the existing feature map to predict the malicious activities of node(s). The training of deep learning models through probability-based feature vectors will also be helpfulin detecting intrusions.

For misbehavior detection, the power of ML can be utilized to cope up with insider attacks. First, data-centric mechanisms (basic plausibility checks) can be used to check message consis- tency in the vehicular plane. For example, to check if two consecutive safety messages coming from the same node have plausible separating distance or not. Based on the results, the node- centric approach powered by deep learning models at the infrastructure plane can be invoked to detect the misbehaving or faulty entity.

B. Blockchain for Security, Privacy and Trust

In IoV, a blockchain can be deployed at different planes such as in-vehicle, the RSU oredge plane, and at service plane (standalone or hierarchical way). The planes that can support resources required for the transaction processing and procedure for forming new blocks can be considered. The private blockchain is found to be more suitable for such contexts.

Security: To secure complex cyber-physical system against hacks and attacks (mentioned above) of in-vehicle, there can be a separate private blockchain. The powerful nodes, such as gateways and switches, can be considered as blockchain nodes. The consensus protocols cankeep nodes synchronized with each other. All communications across ECUs can be consideredas transactions. The smart contracts can be used, which can invoke ML for anomaly or intrusion detection, and if detected, those transactions can be dropped (depending on the defined danger level) and should not be considered in blocks. Similarly, to secure vehicular plane, blockchain deployed at the edge can be helpful. Participating vehicles generate a series of transactions for various events happening on the road, such as applying the harsh brake, detecting slippery roads, etc. Transactions generated by vehicles on the road are sent to the associated RSU.

The suspicious transaction can be dropped at the edge level (smart contract can be used with local detection events). An RSU stores the transaction in its memory pool and simultaneously propagates the transaction among the peer RSUs. The block formation task is entrusted to the RSUs (edge nodes). RSUs pick a random set of transactions from their pool of received transactions and perform a mathematical operation on the selected transactions in order to form a block. Oncea block is formed, an RSU propagates the formed block to its network of RSUs. Each RSU inthe network verify the received block and accept it if it is a valid one.

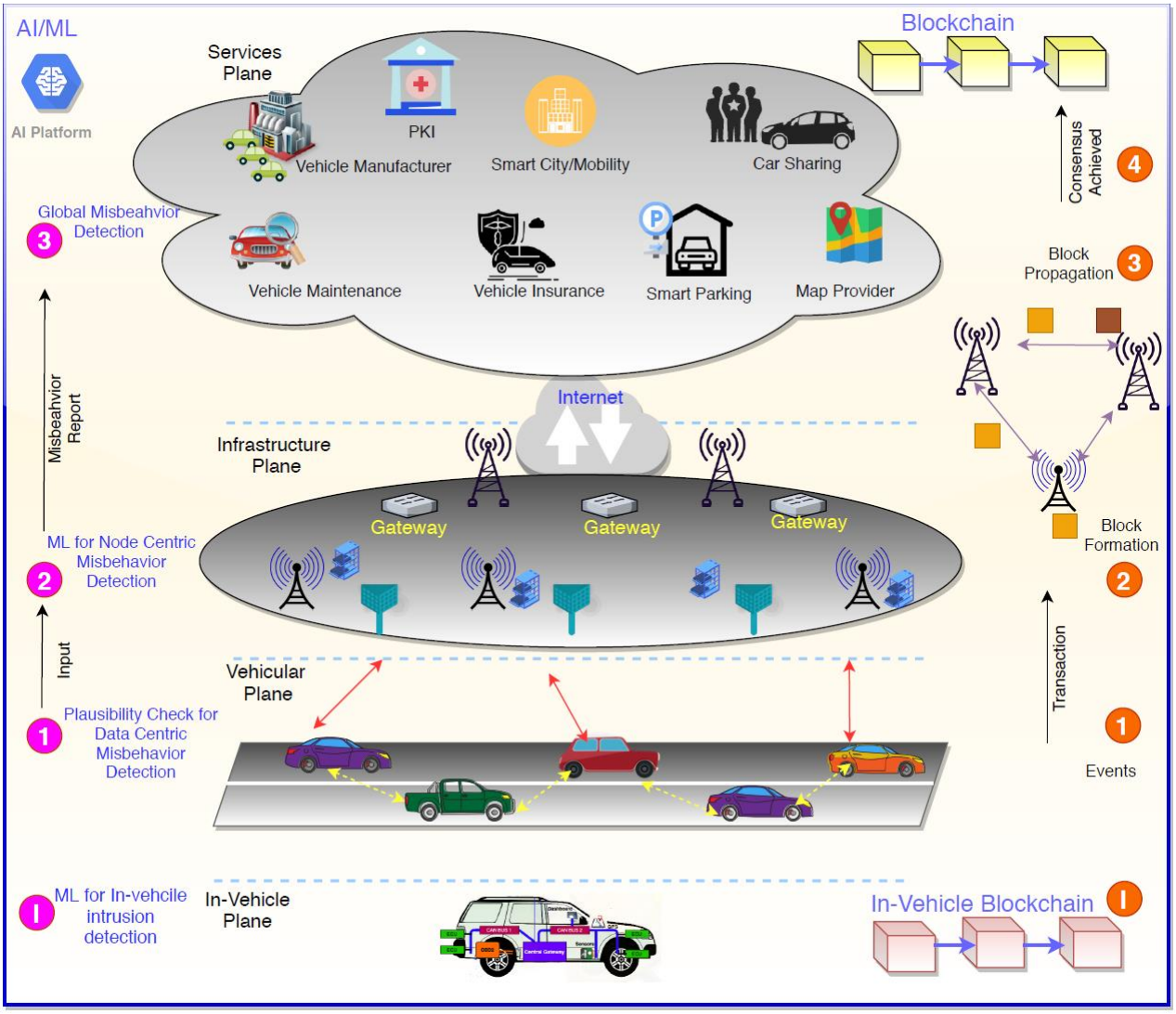


Fig. 6: AI and Blockchain for Security Privacy and Trust in IoV (a Generic View)

Privacy and Trust Management: The Public Key Infrastructure (PKI)-based pseudonym authentication mechanism can be used in the deployed blockchain at the cloud with a certain decentralization for better certificate and pseudonym management and their efficient distribution.The location privacy can be preserved with masquerading concepts over the existing pseudonym change mechanism, which need to be backed up by proof-of-claim and casual dependency to ensure traceability (by trusted authority) and non-repudiation [7]. To preserve the privacy indata sharing, smart contracts can be used to sign agreements between the vehicle (owner) and service providers. The blockchain can be invoked to ensure that signed smart contacts do not

get tampered with. It also enforces proper access control to implement secure and authentic data accessibility and services. The reputation management can also be implemented using smart contracts to penalize the misbehaving vehicles and revoke the certificate or rewarding them (better trust value) based on the report received from the infrastructure plane. The power of AI can be utilized to ensure accountability in the system.

OPEN CHALLENGES AND RESEARCH PERSPECTIVES

This section of the article discusses challenges and research opportunities in AI and Blockchainenabled IoV.

A. Performance: Latency, Throughput, Energy and Scalability

Blockchain and AI adoption to IoV may require handling massive data and transaction pro- cessing in a highly dynamic environment. Thus maintaining performance to the allowable la- tency threshold, throughput, and energy are major concerns [12]. The acceptable latency for safety and non-safety applications is in the range of 100ms to 1 second. For delay-sensitive safety applications, maintaining latency in milliseconds for the entire process of communication, transaction processing, consensus, and block formation will be the biggest challenge. Similarly, maintaining throughput, minimizing energy consumption (mainly electric vehicles), and dealing with a large number of nodes in peak hours of IoV are the biggest challenges of AI andBlockchain integration.

B. Security, Privacy, Transparency

AI and Blockchain integration into IoV may result in a tradeoff between Security and Privacy and Privacy and Transparency. Dealing with such a scenario will be very challenging. Security flaws have also been reported to Blockchain technology structure, peer-to-peer system, and application in the past. The poisoning attack in AI/ML algorithms may mislead the decision making. Ensuring anonymity of users' identity and providing unlinkability of transactions aretwo major concerns from a privacy perspective. AI powers can be misused to link the pseudonym identity and transactions. Thus security, privacy, and transparency need to be widely explored prior to AI and Blockchain integration.

C. Heterogeneity, Deployment Strategies and Standardization

IoV is heterogeneous at access networks, core network technologies, data formats, etc. Thus, dealing with HetNet and different data formats and semantics are very challenging. AI and Blockchain deployment strategy used in one scenario of IoV may not be suitable for other scenarios. For example, Proof-of-Work (PoW) may be ideal for delay-tolerant non-safety applications where security is a major concern but not suitable for delay-sensitive safety applications. Similarly, if the complex AI models (deep learning) used with PoW may lead to high computation, overhead, and delay. Thus, the selection of a proper combination of AI and Blockchainis challenging. The interoperability and standardization of the AI and Blockchain deployment strategy for IoV remain the most significant concerns to be addressed.

There are enormous research opportunities to tackle the challenges mentioned above. HowAI and Blockchain can complement each other in IoV is not yet explored much. More efforts need to be put in to fulfill the QoS, security, privacy, and trust requirement of IoV. Making the Blockchain solution for IoV quantum secure using advanced cryptography such as lattice-based and multivariate mechanisms is one of the hot topics. How private blockchain can be used to secure the complex in-vehicle CPS is another area of research. Designing and developing the adversarial machine learning models for IoV is another open research area. The HetNet scenario of IoV itself opens enormous research opportunities to develop a common, interoperable, and standard security framework.

CONCLUSION

For public acceptance and successful implementation of IoV, security, privacy protection, and trust management are critical aspects. The Blockchain and AI-based solutions can be integrated with the widely used security infrastructure, namely PKI for IoV, such as Security certificate management System (SCMS) in the USA and ETSI TS 102 940 and 941 in Europe to achievethe desired level of protection against security and privacy threats. The trust management processcan also be enhanced by ML-based misbehavior detection and inheriting the blockchain-based incentivization approach for revocation (reward and penalty). The AI can help detect anoma-lies and intrusions at different planes of IoV when invoked through the smart contract logic. Blockchain as a decentralized solution can prevent malicious activities and resolve fault-toleranceand scalability issues. This article discussed the role of AI and Blockchain in IoV separately. Thenhighlighted the security, privacy, and trust issues in the IoV. How AI and Blockchain can help in dealing with security, privacy and trust issues was discussed through a framework. Furthermore, this article has discussed several open challenges and possible future research directions to tacklethem.

REFERENCES

[1] H. Abou-Zeid, F. Pervez, A. Adinoyi, M. Aljlayl, and H. Yanikomeroglu, "Cellular v2x transmission for connected and autonomous vehicles standardization, applications, and enabling technologies," *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 91–98, 2019.

[2] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: architecture, protocols, and security," *IEEE internet of things Journal*, vol. 5, no. 5, pp. 3701–3709, 2017.

[3] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6g: Machine-learning approaches," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 292–307, 2019.

[4] P. K. Singh, S. K. Nandi, and S. Nandi, "A tutorial survey on vehicular communication state of the art, and future research directions," *Vehicular Communications*, vol. 18, p. 100164, 2019.

[5] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, 2018.

[6] G. Tripathi, M. A. Ahad, and M. Sathiyanarayanan, "The role of blockchain in internet of vehicles (iov): Issues, challenges and opportunities," in *2019 International Conference on contemporary Computing and Informatics (IC3I)*. IEEE, 2019, pp. 26–31.

[7] P. Singh, A. Agarwal, G. Nakum, D. Rawat, and S. Nandi, "Mpfslp: Masqueraded probabilistic flooding for source-location privacy in vanets," *IEEE Transactions on Vehicular Technology*, pp. 1–1, 2020.

[8] J. Kamel, M. R. Ansari, J. Petit, A. Kaiser, I. B. Jemaa, and P. Urien, "Simulation framework for misbehavior detection in vehicular networks," *IEEE Transactions on Vehicular Technology*, 2020.

[9] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[10] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 770–790, 2017.

[11] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, "Blockchain-based adaptive trust management in internet of vehicles using smart contract," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–15, 2020.

[12] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K.-Y. Lam, and L. H. Koh, "Blockchain for the internet of vehicles towards intelligent transportation systems: A survey," *IEEE Internet of Things Journal*, 2020.

vPranav Kumar Singh (Member, IEEE) received the Ph.D., B.Tech. and M.Tech. in ComputerScience and Engineering. He is working as an Assistant Professor with the Department of Computer Science and Engineering, Central Institute of Technology at Kokrajhar, India. He has more than 13 years of teaching experience. He has also served as a Nodal Officer NKN and IPv6Road Map of CITK, an initiative by the Government of India. He served as a Technical Program Committee (TPC) member for several international conferences. He is an active reviewer of many top Journals. He has published around 34 journal articles/conference papers. His research interestsinclude vehicular communications, security and privacy, software-defined vehicular networking, QoS and QoE in wireless communication, intelligent transportation systems, blockchain, and the IoT. Contact him at snghpranav@gmail.com

Sukumar Nandi is a Professor in the Department of Computer Science and Engineeringand Head, Centre for Linguistic Science and Technology at the Indian Institute of TechnologyGuwahati. He is Fellow of Indian National Academy of Engineering, Senior Member ACM,Senior Member IEEE, Fellow of the Institution of Engineers (India) and Fellow of the Institutionof Electronics and Telecommunication Engineers (India). He completed his Ph.D. in ComputerScience and Engineering from Indian Institute of Technology Kharagpur. He has more than100 journal publications and several international conference publications. His areas of researchinterests include Networks (Specifically: QoS, Wireless Networks), Computer and Network Security, Data Mining, VLSI and Computational Linguistic. . Contact him at sukumar@iitg.ac.in

Sunit Kumar Nandi (Student Member, IEEE) is currently pursuing the Ph.D. degree in computer science and engineering with the IIT Guwahati. He is the Leading Officer with TechnoFAQ Digital Media, an e-magazine focusing on science, engineering, business, and education. Hehas spent two years in the telecom industry, and seven years in developing open-source softwareas a volunteer with the team at the SuperX Operating System Project. He also mentors startupsin developer operations, IT infrastructure, and financial services. He published 20 articles ininternational journals and conferences. His research interests include operating systems, computer networking, and cognitive data mining. Contact him at sunitnandi834@gmail.com

Uttam Ghosh is working as an Assistant Professor of Practice in EECS, Vanderbilt University,Nashville, Tennessee, USA. Contact him at ghosh.uttam@ieee.org

Danda B. Rawat (IEEE Senior Member, 2013) is a Professor in the Department of Electrical Engineering & Computer Science (EECS), Director of DoD Center of Excellence in AI/ML (CoE-AIML), Director of the Howard University Data Science and Cybersecurity Center, Direc- tor of Cyber-security and Wireless Networking Innovations (CWiNs) Research Lab, Graduate Program Director of Graduate CS Programs and Graduate Cybersecurity Certificate Programat Howard University, Washington, DC, USA. Dr. Rawat is engaged in research and teachingin the areas of cybersecurity, machine learning, big data analytics and wireless networking for emerging networked systems including cyber-physical systems, Internet-of-Things, multi domainoperations, smart cities, software defined systems and vehicular networks. He has secured over $16 million in research funding from the US National Science Foundation (NSF), US Departmentof Homeland Security (DHS), US National Security Agency (NSA), US Department of Energy, National Nuclear Security Administration (NNSA), DoD and DoD Research Labs, Industry (Microsoft, Intel, etc.) and private Foundations. Dr. Rawat is the recipient of NSF CAREER Award in 2016, Department of Homeland Security (DHS) Scientific Leadership Award in 2017, Researcher Exemplar Award 2019 and Graduate Faculty Exemplar Award 2019 from Howard University, the US Air Force Research Laboratory (AFRL) Summer Faculty Visiting Fellowship in 2017, Outstanding Research Faculty Award (Award for Excellence in Scholarly Activity) at GSU in 2015 and the Best Paper Awards (IEEE CCNC, IEEE ICII, BWCA) among others. He has delivered over 30 Keynotes and invited speeches at international conferences and workshops.Dr. Rawat has published over 200 scientific/technical articles and 10 books. He has been serving as an Editor/Guest Editor for over 50 international journals including the Associate Editor of IEEE Transactions of Service Computing, Editor of IEEE Internet of Things Journal, Associate Editor of IEEE Transactions of Network Science and Engineering and Technical Editors of IEEENetwork. He has been in Organizing Committees for several IEEE flagship conferences suchas IEEE INFOCOM, IEEE CNS, IEEE ICC, IEEE GLOBECOM and so on. He served as a technical program committee (TPC) member for several international conferences. He served asa Vice Chair of the Executive Committee of the IEEE Savannah Section from 2013 to 2017. Dr. Rawat is a Senior Member of IEEE and ACM, a member of ASEE and AAAS, and a Fellowof the Institution of Engineering and Technology (IET). He is an ACM Distinguished Speaker. Contact him at db.rawat@ieee.org

Vehicle Edge Interaction From an Edge Scheduling Perspective

Sihai Tang and Fu Song
Department of Computer Science and Engineering
University of North Texas, USA
SihaiTang@my.unt.edu, Song.Fu@unt.edu

1. Introduction

Autonomous vehicles are becoming more and more relevant today. There is no denying the benefits of an autonomous vehicle in terms of driver and pedestrian safety. By delegating the driving decision to on-board computing units, the driver-related issues such as driving under the influence and other human operating errors are significantly reduced. In addition to the safety benefits, we are also witnessing a blossom of various other uses [22], [29], [34], with amber alert detection and collision avoidance being the most prominent [35]. To facilitate the self-driving process, various sensors need to relay their sensing data of the surrounding environment to the on-board computing unit. This is usually handled by an array of sensors such as the LiDAR, cameras, radar, GPS, IMU, and more. Due to the vast array of sensors, it is estimated that an autonomous vehicle will generate 4 terabytes of data
or more in two hours [2]. To enhance driving, connected and autonomous vehicle (CAV) technology enables raw-data level and feature-map level data sharing among vehicles [5], [7], [8], which utilizes extraneous data from other vehicles to drastically improve the detection capabilities of a single vehicle.

Currently, most car manufacturers focus on uploading their data to the cloud. However, the expensive data transmission, exacerbated network congestion and prolonged latency between vehicles and the cloud make real-time object detection inaccurate if not infeasible.

With these limitations, autonomous vehicle manufacturers opt to use cellular connectivity to facilitate data between vehicles and computing platforms [1]. With 5G infrastructure yet to reach maturity, the information type, size, and variety are often restricted due to the availability and location [3]. We typically see the use of dedicated software and hardware such as dedicated short-range communication (DSRC) as the channel of data dissemination between different vehicles, but this too is limited to the information type and size. While DSRC can broadcast the GPS, IMU and speed information for other vehicles to stay aware, large sensor data from HD cameras and LiDAR requires higher bandwidth which DSRC cannot provide. Those 2D images and 3D point clouds are useful for improving the perception range and accuracy of vehicles leveraging edge computing [7].

Extensive research on how to improve the safety for all parties involved in a autonomous car points to CAV as the solution [30], [31]. Stemming from this, with communication between vehicles, we open the possibility of cooperative perception, which eliminates many faults of a single vehicle operating on its own sensors. However, as is with all things, we face challenges in the area of cooperative perception as well. Works such as [4], [7], [8], [15] present the limitations as well as the advantages of sharing sensor data between vehicles.

While these works greatly improve the outlook of autonomous vehicles, they still rely on the use of traditional platforms of data sharing such as cellular or DSRC. With the emerging edge computing paradigm, we find that although works such as [7] is suitable for edge, there are no end-to-end edge systems that can address the challenges of using the edge as well as the ability to fully facilitate the process of cooperative perception on the edge. In this paper, we design and evaluate our scheduling pipeline design for the transfer and fusion of different types of data between vehicles and edge nodes to achieve cooperative perception. We propose the use of edge nodes as a targeted and purposed system to facilitate the exchange of large sensor data towards safer driving.

2. Related Work

In this section, we investigate the existing literature on vehicular edge computing for scheduling and pipeline design in the connected autonomous vehicle (CAV).

Edge for vehicles. [22] provided us a comprehensive review of development and challenges of autonomous vehicle in edge environment. [14] proposed a vehicle-to-vehicle communication enhancement scheme by introduced the hierarchical edge-based preemptive route creation, two-stage learning and context-aware edge selection approach to improve the packet forwarding performance. As edge computing becomes a mainstream solution to process data remotely for autonomous, [25] investigated the service migration and

resource management from intra- and inter-tier communication in edge and fog computing. In addition, many existing works mentioned about edge for vehicles but focused on MEC (Mobile-Edge-Computing). [12] an [16] solved the offloading and caching computing in vehicle networks for mobile-based edge separately.

Resource allocation and offloading. Resource allocation plays an important role in CAV system optimization problem. [24] studied the tradeoff between execution time and energy consumption for the problem of computation offloading. They also designed a game theory model to minimize the combination of energy overhead and delay. Similarly, Zhang [33] designed a system to reduce the weighted cost of time latency and energy consumption using mobile devices as the edge ends. [20] also proposed a computation offloading technique in terms of energy-efficiency in edge cloud computing. [11] proposed a distributed offloading scheme by helping multiple users learn their long-term offloading strategies and proved a Nash equilibrium can be achieved. [19] propose a method
to allocate resources in uncertain conditions improve the reliability of Vehicle-to-infrastructure system.

Scheduling. Scheduling on edge side and between edge to vehicle is a prevalent topic in recent years. Most of the paper focused on communication and scheduling strategy on mobile based edge ends. [23] proposed a framework to formulate the communication and resource computation jointly and promote an optimal strategy on data scheduling using deep reinforcement learning approach. [9] optimized the task scheduling by designed a dynamic scheduling scheme regarding queue-based and time-based approach to allocate tasks in hybrid mobile environments. [21] designed a time-driven workflow scheduling mechanism to efficiently improve the completion time of reasoning tasks in edge environments by applying the Markov decision process and Q-learning algorithm in their simulated annealing. In addition, [32] also applied Markov decision process in their method but combine with other
optimization algorithm in deep reinforcement learning. He also implemented a representative features extraction by merging parameter-shared network architecture together with convolutional neural network.

3. System Design and Formulation

We plan to design an optimization algorithm centered around the Edge side scheduling, with the primary focus being on the profiling and establishing the baseline performance of the native pipeline from F-Cooper. In Fig. 1, we detail the overall schematic of the system. Through this, we hope to make the first step towards eliminating the challenges of safe collaborative driving through the use of Edge, with the focus on edge design and scheduling.

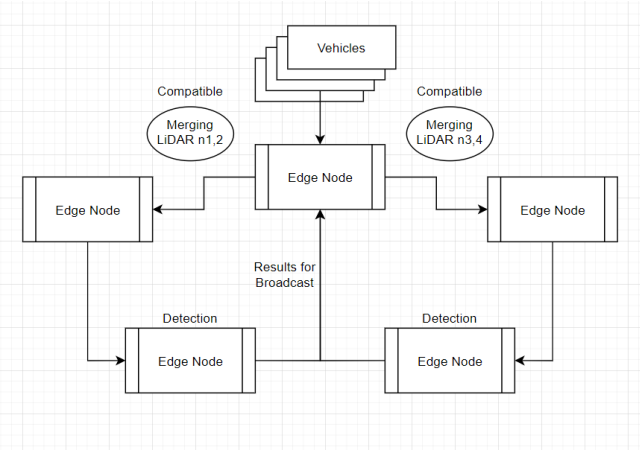


Fig. 1. The Vehicles designate cars with the capability of requesting service from the edge node network. As the requests are received, the edge node handling the message transactions will cluster the requests into potential groups for further processing. Through this pipeline, a wide array of models can then be deployed to the correct vehicle cluster for faster and more accurate processing.

The Potential Problem Formulation is as follows. At any given timeslot, the data of each vehicle can be: (1) Processed locally: select features to send to edge. (2) In queue to be uploaded to the Edge: time restricted based on speed (Certain time frame before the location data is irrelevant.) (3) On the Edge awaiting processing or awaiting either deletion or storage.

At any given time, the Edge node will consider the following:

(1). Resources available (Possible consideration of Down sampling) (2). Deadline assignment and tracking for each vehicle (3). Tasks awaiting execution (Estimated execution time) (4). Tasks in execution (Estimated completion time)

4. Experiment and Analysis

We conducted an experiment emulating the run-time process of F-Cooper using the open-source code cited in [7]. Through this, the vehicles will be able to request for an extension of F-Cooper to be performed. We then profile F-Cooper through analysis of the current pipeline implemented to identify potential points of optimization.

	Temperature	Power	Memory	Utilization
GTX 1060 6GB	39C	27W/120W	301MB	1%

Table I: The Status of the GPU when not under a workload. Here the Idle temperature of having F-Cooper loaded in the background is around 39 Celsius with a power draw of around 27 watts. The total memory usage is also very low at only 300 MB.

As F-Cooper is inherently a lightweight process capable of running on an edge device, it has several components that we analyze through our experiment. Since F-Cooper supports the use of the GPU, we prioritize the utilization of the GPU over the CPU in our experiment. In our experiment, we will profile the following elements of the process in order to establish a good baseline for future work on the optimization and scheduling: (1). GPU usage (2). GPU energy consumption (3). Total Run-time for a complete processing run of one frame of data (4). Algorithmic break down of the components as well as their formulations

In our proposed pipeline architecture, the data preprocessing for F-Cooper is not necessary as the handshaking assumes that the data is pre-compatible. Also, the model training step will also be excluded as the Edge is assumed to have access to the latest models available for servicing the compatible vehicles. With these two big limiting factors removed from the F-Cooper process, we now look specifically at the following steps of voxel generation and forwarding as well as the inference speed.

	Temperature	Power	Memory	Utilization
GTX 1060 6GB	40C	27W/120W	1927MB	32%

Table II: The status of the GPU when under a single F-Cooper workload. Here the temperature is up by 1 degree Celsius over the idle temperature and the total memory usage is up to around 2 GB as compared to the 300MB of when it was idle.

However, as the main portion of training the model for accuracy is calculation of the loss function, to gouge the
difference between the prediction to the ground true, we briefly examine the process to estimate the impact of running such on an Edge device.

The relationship between the input data and the amount of processing time required to run such calculations indicate that as more objects enter the area of service, the more processing power is needed should we require model updates during downtime.

GPU Usage. F-Cooper considers both the CPU and the GPU as a potential source of computational power, however, to focus on more realistic profiling, we opted to use the Nvidia GeForce GTX 1060 GPU. This GPU has a maximum power draw of 120 watts and a total of 6 gigabytes of memory.

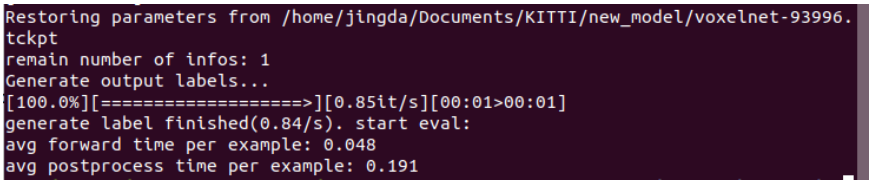


Fig 2. The average time for a single F-Cooper run is broken down. With Label generation and evaluation as the two main components of interest.

In our first task, we loaded all the process threads into the edge system and profiled the overall GPU status. As we see in Table I, the status of the GPU when not under a workload. Here the Idle temperature of having F-Cooper loaded in the background is around 39 Celsius with a power draw of around 27 watts. The total memory usage is also very low at only 300 MB. With this data as our baseline, we move on to the full profiling of the GPU with F-Cooper running one frame of data inference.

The status of the GPU when under a single F-Cooper workload is shown in Table II. Here the temperature is up by 1 degree Celsius over the idle temperature and the total memory
usage is up to around 2 GB as compared to the 300MB of when it was idle. This increase in both temperature and
memory usage is a big increase when taking into consideration that we are just running inference for one frame of data. As a continuous stream of data is fed through the F-Cooper's native pipeline, the amount of processes being loaded comes to around 1.7 GB, which is very large to run an inference process. In addition to the memory increase, we also saw the increase in temperature. As one frame is very small, a realistic workload will ramp up the temperature and thus force the GPU to draw more power to both cool and process the workload more efficiently. We this that this is a key factor to optimizing the performance of the pipeline.

Run Time Average. Just the physical hardware usage is not enough for a good pipeline design, so we also conducted a profiling for the overall speed of F-Cooper broken down into the following parts:
(1) Label Generation (2) Total Run-time for a complete processing run of one frame of data (3) Algorithmic break down of the components as well as their formulations

As seen in Fig. 2, the average time for a single F-Cooper run is broken down. With Label generation and evaluation as the two main components of interest. We observe the rapid generation of the labels at around 0.85 iterations of tasks per second. Following the label generation, the evaluation step comes next. First, the Voxels are forwarded from the neural network at a rate of 0.048 seconds per example. This is the time that it takes for the native pipeline to extract and initiate the process of sending the voxels to the target. After the extraction and forwarding of the voxels per example, the native pipeline then continues with the local inference portion, to generate a prediction for the example at hand. As we see in the figure, the average post process inference time per example is around 0.191 seconds, which is long when compared to the voxel extraction and forwarding step.
However, as we only focus on profiling the native pipeline of F-Cooper, the relative time it takes to receive and also
inference the example timing is not tested.

5. Discussions
The profiling of the F-Cooper native pipeline has shown possibilities for the use of an algorithm-based scheduling
optimization. For example, the workload of the native pipe gives credence to the heavy weight nature of the entire process.

In our proposed approach, the background resource usage can be optimized for much less usage towards the task at hand. For example, in our profiling, the native F-Cooper pipe shows around 30 percent GPU usage for just the inference of a single frame. This is most likely using the GPU for tasks that can be routed to the CPU, such as pre-loading the model weights and other similar tasks. Further observations made based on the profiling results
indicate that while F-Cooper achieves real time speeds, it is still linear in nature for the job execution order. As the voxels forwarding is not a crucial step that is depended on by the evaluation and prediction tasks later on, it can be separated for variable scheduling instead of a static sequential order of execution.

6. CONCLUSIONS
In this project, we have identified that the existing literature does not focus on the approach of integrating edge with autonomous vehicles specifically. While efforts have been made towards this end, we do not see the scalability for the existing works.

We believe that through optimization, a pipeline can be designed and formalized for current and future efforts, thus allowing for the easy transition for works such as F-Cooper to fully migrate to various edge platforms without loss of performance.

In our experiment, we profiled F-Cooper based on the publicly available code published by the authors. Based on
our experimental analysis, we find that there exist many opportunities to apply our proposed algorithm to optimize the existing native pipeline of F-Cooper. We believe that in a future work, we can formulate a formal method that allows for such a process to be widely adopted for future research in this field.

References

[1] Connectivity — tesla. https://www.tesla.com/support/connectivity.
[2] For self-driving cars, there's big meaning behind one big number: 4 terabytes. https://newsroom.intel.com/editorials/self-driving-cars-
bigmeaning- behind-one-number-4-terabytes/.
[3] Verizon vs at&t vs t-mobile vs sprint: Choose the best 5g carrier- cnet. https://www.cnet.com/how-to/verizon-vs-at-t-vs-t-mobile-vssprint-
choose-the-best-5g-carrier/.
[4] O. Altintas and T. Higuchi. Multi-level hybrid vehicle-to-anything communications for cooperative perception, Oct. 24 2019. US Patent
App. 15/958,969.
[5] E. Arnold, M. Dianati, and R. de Temple. Cooperative perception for 3d object detection in driving scenarios using infrastructure sensors,
2019.
[6] D. Camps-Mur, A. Garcia-Saavedra, and P. Serrano. Device-to-device communications with wi-fi direct: overview and experimentation. IEEE
wireless communications, 20(3):96–104, 2013.
[7] Q. Chen, X. Ma, S. Tang, J. Guo, Q. Yang, and S. Fu. F-cooper: feature based cooperative perception for autonomous vehicle edge
Computing system using 3d point clouds. In ACM/IEEE Symposium on Edge Computing (SEC), 2019.
[8] Q. Chen, S. Tang, Q. Yang, and S. Fu. Cooper: Cooperative perception for connected autonomous vehicles based on 3d point clouds. In IEEE
Intl Conference on Distributed Computing Systems (ICDCS), 2019.
[9] X. Chen, N. Thomas, T. Zhan, and J. Ding. A hybrid task scheduling scheme for heterogeneous vehicular edge systems. IEEE Access,
7:117088–117099, 2019.
[10] L. Ding, Y. Wang, P. Wu, L. Li, and J. Zhang. Kinematic information aided user-centric 5g vehicular networks in support of cooperative
perception for automated driving. IEEE Access, 7:40195–40209, 2019.
[11] T. Q. Dinh, Q. D. La, T. Q. Quek, and H. Shin. Learning for computation offloading in mobile edge computing. IEEE Transactions
on Communications, 66(12):6353–6367, 2018.
[12] J. Du, F. R. Yu, X. Chu, J. Feng, and G. Lu. Computation offloading and resource allocation in vehicular networks based on dual-side cost
minimization. IEEE Transactions on Vehicular Technology, 68(2):1079–1092, 2018.
[13] R. Girshick. Fast r-cnn. In Proceedings of the IEEE international conference on computer vision, pages 1440–1448, 2015.
[14] S. Guleng, C.Wu, Z. Liu, and X. Chen. Edge-based v2x communications with big data intelligence. IEEE Access, 8:8603–8613, 2020.
[15] T. Higuchi, M. Giordani, A. Zanella, M. Zorzi, and O. Altintas. Value anticipating v2v communications for cooperative perception. In IEEE
Intelligent Vehicles Symposium, 2019.
[16] R. Q. Hu et al. Mobility-aware edge caching and computing in vehicle networks: A deep reinforcement learning. IEEE Transactions
on Vehicular Technology, 67(11):10190–10203, 2018.
[17] J. B. Kenney. Dedicated short-range communications (dsrc) standards in the united states. Proceedings of the IEEE, 99(7):1162–1182, 2011.
[18] S. Kim and W. Liu. Cooperative autonomous driving: A mirror neuron inspired intention awareness and cooperative perception approach.
IEEE Intelligent Transportation Systems Magazine, 8(3):23–32, 2016.
[19] A. Kovalenko, R. F. Hussain, O. Semiari, and M. A. Salehi. Robust resource allocation using edge computing for vehicle to infrastructure
(v2i) networks. In 2019 IEEE 3rd International Conference on Fog and Edge Computing (ICFEC), pages 1–6. IEEE, 2019.
[20] X. Li, Y. Dang, M. Aazam, X. Peng, T. Chen, and C. Chen. Energy efficient computation offloading in vehicular edge cloud computing.
IEEE Access, 8:37632–37644, 2020.
[21] K. Lin, B. Lin, X. Chen, Y. Lu, Z. Huang, and Y. Mo. A time-driven workflow scheduling strategy for reasoning tasks of autonomous driving
in edge environment. In 2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing,
Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), pages 124–131. IEEE,
2019.
[22] S. Liu, L. Liu, J. Tang, B. Yu, Y. Wang, and W. Shi. Edge computing for autonomous driving: Opportunities and challenges. Proceedings of
the IEEE, 107(8):1697–1716, 2019.
[23] Q. Luo, C. Li, T. H. Luan, and W. Shi. Collaborative data scheduling for vehicular edge computing via deep reinforcement learning. IEEE
Internet of Things Journal, 2020.
[24] M.-A. Messous, H. Sedjelmaci, N. Houari, and S.-M. Senouci. Computation offloading game for an uav network in mobile edge computing.
In 2017 IEEE International Conference on Communications (ICC), pages 1–6. IEEE, 2017.
[25] L. Pacheco, H. Oliveira, D. Ros´ario, E. Cerqueira, L. Villas, and T. Braun. Service migration for connected autonomous vehicles. In 2020
IEEE Symposium on Computers and Communications (ISCC), pages 1–6. IEEE, 2020.
[26] S. Ren, K. He, R. Girshick, and J. Sun. Faster r-cnn: Towards real-time object detection with region proposal networks. In Advances in neural
information processing systems, pages 91–99, 2015.

[27] M. Satyanarayanan. The emergence of edge computing. Computer, 50(1):30–39, 2017.
[28] H. G. Seif and X. Hu. Autonomous driving in the icity—hd maps as a key challenge of the automotive industry. Engineering, 2(2):159–162,
2016.
[29] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu. Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5):637–646, 2016.
[30] A. Talebian and S. Mishra. Predicting the adoption of connected autonomous vehicles: A new approach based on the theory of diffusion
of innovations. Transportation Research Part C: Emerging Technologies, 95:363–380, 2018.
[31] C. Wang, S. Gong, A. Zhou, T. Li, and S. Peeta. Cooperative adaptive cruise control for connected autonomous vehicles by factoring
communication-related constraints. Transportation Research Part C: Emerging Technologies, 2019.
[32] W. Zhan, C. Luo, J. Wang, C. Wang, G. Min, H. Duan, and Q. Zhu. Deep reinforcement learning-based offloading scheduling for vehicular
edge computing. IEEE Internet of Things Journal, 2020.
[33] K. Zhang, X. Gui, D. Ren, and D. Li. Energy-latency tradeoff for computation offloading in uav-assisted multi-access edge computing
system. IEEE Internet of Things Journal, 2020.
[34] Q. Zhang, Y. Wang, X. Zhang, L. Liu, X. Wu, W. Shi, and H. Zhong. Openvdap: An open vehicular data analytics platform for cavs. In
Distributed Computing Systems (ICDCS), 2017 IEEE 38th International Conference on. IEEE, 2018.
[35] Q. Zhang, Q. Zhang, W. Shi, and H. Zhong. Distributed collaborative execution on the edges and its application to amber alerts. IEEE Internetof Things Journal, 5(5):3580–3593, 2018.

MMTC OFFICERS (Term 2020 — 2022)

CHAIR

Jun Wu
Fudan University
China

STEERING COMMITTEE CHAIR

Joel J. P. C. Rodrigues
Federal University of Piauí (UFPI)
Brazil

VICE CHAIRS

Shaoen Wu (North America)
Illinois State University
USA

Liang Zhou (Asia)
Nanjing University of Post and Telecommunications
China

Abderrahim Benslimane (Europe)
University of Avignon
France

Qing Yang (Letters & Member Communications)
University of North Texas
USA

SECRETARY

Han Hu
Beijing Institute of Technology
China

STANDARDS LIAISON

Weiyi Zhang
AT&T Research
USA

MMTC Communication-Frontier BOARD MEMBERS (Term 2016—2018)

Danda Rawat	Director	Howard University	USA
Sudip Misra	Co-Director	IIT Kharagpur	India
Guanyu Gao	Co-Director	Nanjing University of Science and Technology	China
Rui Wang	Co-Director	Tongji University	China
Lei Chen	Editor	Georgia Southern University	USA
Tasos Dagiuklas	Editor	London South Bank University	UK
ShuaiShuai Guo	Editor	King Abdullah University of Science and Technology	Saudi Arabia
Kejie Lu	Editor	University of Puerto Rico at Mayagüez	Puerto Rico
Nathalie Mitton	Editor	Inria Lille-Nord Europe	France
Zheng Chang	Editor	University of Jyväskylä	Finland
Dapeng Wu	Editor	Chongqing University of Posts & Telecommunications	China
Luca Foschini	Editor	University of Bologna	Italy
Mohamed Faten Zhani	Editor	University of Quebec	Canada
Armir Bujari	Editor	University of Padua	Italy
Kuan Zhang	Editor	University of Nebraska-Lincoln	USA
Bin Tan	Editor	Jinggangshan University	China