# Towards a Secure Resource Sharing Architecture in Connected Vehicles

Saeid Sabamoniri[†], Harrison Kurunathan[*], Pedro M. Santos[‡], Munkenyi Mukhandi[¶], Fernando Alves[¶]
[*] *CISTER/ISEP*, [†] *CISTER/FEUP*, [‡] *CISTER/U. Aveiro* , [¶] *VORTEX-CoLab*
{ssmon, jhk}@isep.ipp.pt, pss@ua.pt, {munkenyi.mukhandi, fernando.alves}@vortex-colab.com

***Abstract*—Modern vehicular applications have increased computational demands, which in turn have spurred an interest in leveraging vehicles as distributed resources. We propose a novel framework for vehicles to dynamically share their physical resources, such as GPUs and memory, which enables cooperative computation. These physical resource sharing can enhance the overall system efficiency and prevent a single node being overburdened. To ensure secure resource sharing, we employ efficient physical-layer-based key generation to mitigate threats like eavesdropping. We also propose a sharing-participant selection scheme to select the optimal one through evaluation of several factors such as resource availability, and reliability. This approach balances computational efficiency and security among the vehicles participating in sharing resources. Our simulation results showcase the effectiveness of this framework in enhancing computational resource utilization while providing a secure and reliable operation in urban vehicular networks.**

***Index Terms*—Resource sharing, PHY-layer key generation, score-based selection scheme.**

## I. Introduction

The modern automotive industry is transitioning towards increasingly intelligent and connected vehicles. With the domain of Intelligent Transportation Systems (ITS) booming, new applications are on the horizon that demand heavy computational resources, like autonomous driving, real-time traffic management, and infotainment systems [1]. Though modern vehicles are equipped with powerful onboard processors, sensors, and communication modules, vehicles can face constraints in terms of processing power, energy efficiency, and storage capacity when running critical (*e.g.*, autonomous driving) and non-critical applications (*e.g.*, infotainment apps) simultaneously. Therefore, vehicles could improve their quality of service towards passengers by offloading non-critical but latency-sensitive computation (*e.g.*, gesture identification) to other vehicles or roadside edge infrastructure. Through these methods vehicles can offload intensive tasks, share data for cooperative perception, and even share resources for cooperative computation. Furthermore, with the current trend towards electric vehicles, vehicular energy management becomes a novel concern, which can be alleviated by offloading expensive non-critical computation.

This work was supported by the CISTER Research Unit (UIDP/UIDB/04234/2020), financed by National Funds through FCT/MCTES (Portuguese Foundation for Science and Technology); by project Route 25 (ref. TRB/2022/00061 - C645463824-00000063), funded by the EU/Next Generation, within call n.º 02/C05-i01/2022 of the Recovery and Resilience Plan (RRP) and HAL4SDV funding within the Chips Joint Undertaking (Chips JU) - the Public-Private Partnership for research, development and innovation under Horizon Europe – and National Authorities under grant agreement n° 101139789. The work of Saeid Sabamoniri is supported by a Ph.D. Scholarship from FCT, grant nr. 2023.00896.BD.

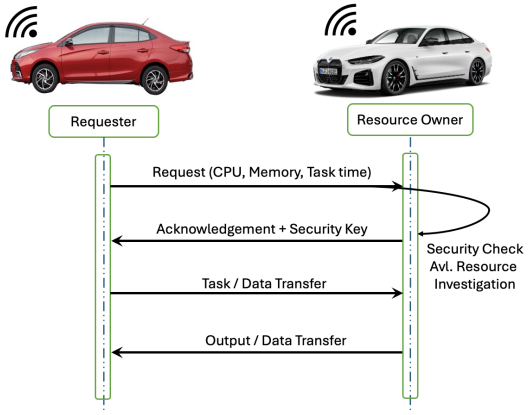


Fig. 1. Communication flow for resource sharing with a physical layer security scheme between connected vehicles

Traditionally, computational demands have been addressed through cloud-based designs [2], [3]. Cloud-based approaches are susceptible to deteriorating performance metrics like high latency, and increased vulnerability to security breaches. Moreover, the methods to do so are well-known and outside the scope of this paper. Modern vehicle components such as GPUs, storage units, and sensors need no longer be tied to single functionality. They can be virtualised and dynamically allocated across multiple applications and even multiple vehicles. For example, a high-performance processor that is dedicated to a critical functionality like advanced driver-assistance systems (ADAS) can be used to support real-time diagnostics or facilitate over the air update (OTA) of another vehicle when the ADAS is idle. This is a service-oriented architecture, where the physical resources are abstracted and shared amongst vehicles to improve modularity .

In the context of connected autonomous vehicles (CAV), secure resource sharing is essential to maintain the integrity of the vehicular network. Through resource sharing, vehicles rely on interconnected systems for sharing the computational workload, storage memory, or even functions leading to distributed decision-making. A simple functionality like remote software update can become susceptible to malicious exploitation such as data leakage, denial-of-service or unauthorized access to

critical vehicle operations [4]. Traditional security mechanisms are not efficient to combat against these dynamic attacks [5]. Hence, there is a need for a lightweight security strategy to be integrated into the resource-sharing framework [6]. In this line, we propose PHY-layer based key generation technique to secure and authenticate the exchange. Unlike traditional heavy cryptographic computations like RSA or ECC, PHY layer based key generation uses properties of the wireless channel available at the transeiver making it lightweight and efficient [3]. Also the keys are generated dynamically making it suitable for resource-constrained or mobile devices.

Figure 1 presents the communication flow of the proposed model for resource sharing with a physical layer security scheme between connected vehicles. In this work, we propose a novel framework for physical resource sharing so that the overburdening of any single node's computational utilization in vehicular networks can be prevented. We develop a score-based metric to maintain the balance of resource fairness and reliability. Furthermore, to ensure secure resource sharing, we employ a physical-layer-based (PHY) key generation mechanism [7], [8] that develops keys based on the unique channel parameters between the vehicles to mitigate malicious actions like eavesdropping or data altering.

The contributions of this work are as follows:

- we propose a novel physical resource sharing framework for vehicular networks using a weighted score metric.
- we integrate a PHY-based key generation mechanism that leverages unique channel characteristics to establish cryptographic keys between resource-sharing vehicle.
- Through simulation and the standard tools of NIST, we study the selection of the resource-sharing vehicle and the robustness of the underlying security protocol

The rest of the paper is structured as follows: Section II presents the related works in line with resource sharing in vehicles and their security schemes. In Section III, we introduce our resource sharing architecture and our key generation scheme. In Section IV, we present the results in the fronts of resource sharing and randomness of keys generated and finally we present some future scopes in Section V.

## II. Related work

Resource-sharing mechanisms help in alleviating the computational workload by obtaining the necessary resources from other connected actors. The purpose of resource sharing is to achieve better computational efficiency, while concomitantly maintaining fairness. Such mechanisms are used in grid/cloud computing [9]–[12] and in the most recent versions of mobile edge computing platforms [13]. In our work, we extend it to CAV as the demands for resources and the applications they supports are constantly increasing. Computational offloading and resource allocation in vehicular networks have been enabled using techniques like nonorthogonal multiple access (NOMA) within a mobile edge computing (MEC) framework in [14]. This work formulates a latency minimization problem, decomposed into convex optimization, accounting for vehicle sojourn time. Their method improves task completion latency. In our work, we aim at reducing the computational workload by sharing abundant resources at a specific node.

The research in [15] proposes a relay hopping and differentiated task prioritization (RHATP) for reducing processing delay in vehicular networks by offloading tasks from high-load roadside units (RSUs) to low-load ones using idle vehicles as relays. They formulates a weighted average system delay minimization problem to allocate heterogeneous tasks based on delay sensitivity. In our work, we use a weighted scoring functionality to choose the vehicles that could share their resources for joint-computation.

Given the non-deterministic nature of resource sharing, it is mainly used in non-critical applications. For instance, [16] presents a video streaming service model by obtaining data from vehicles. They formulate the problem as mixed-integer nonlinear programming for calculating the payment for the video service. A consortium blockchain-based resource-sharing proposed in [17] encapsulated interactions as transactions by the RSUs. They use a proof-of-reputation mechanism to reduce computational power consumption and motivate vehicles involved in resource sharing. Resource sharing and consensus increased the reputation value of every vehicle. A digital twin-based fair trading platform built upon a consortium blockchain for vehicular resource sharing in the cloud is used in [18]. The consortium blockchain enforces smart contracts through a Proof-of-Stake (PoS) consensus algorithm. While these existing works emphasize resource sharing, they often lack robust security mechanisms to protect shared resources. In this work, we propose a weighted scoring framework that facilitates resource sharing based on availability, coupled with a PHY-layer-based scheme to ensure secure resource sharing.

Researchers in [19] present a security-aware dynamic device-to-device (D2D) spectrum resource-sharing mechanism to enhance the security of vehicular networks. Their method models the joint D2D spectrum resource-sharing process as a weighted bipartite graph matching problem whose weights are obtained from closed-form solutions of power control. This security-aware and power allocation mechanism is compatible with existing cellular networks and of small cell base station applications. The security of our proposed method is facilitated through physical layer-based key generation, which could be beneficial as we are dealing with vehicles doing resource sharing within the vicinity.

Multi-Agent Deep Reinforcement Learning has been used in designing optimal caching strategies for the Internet of Vehicles [20]. Their proposed framework incentivizes sharing caching resources while minimizing errors in estimating content needs through machine learning. Extensive simulation results with different system parameters demonstrate the efficiency of the proposed solution. As caching lowers acquisition delays of the content like video streaming, this method through prediction of needed resources can help in meeting the needs of the vehicular network.

In this paper, we consider CAVs as distributed systems and target the resource allocation process among the CAVs in special environment scenarios. One of the challenges in

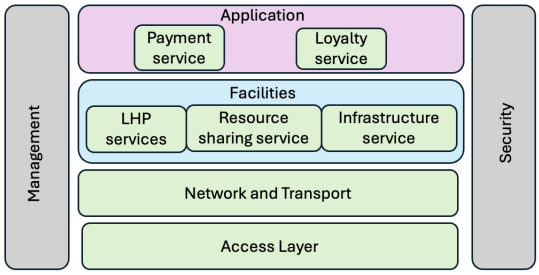


Fig. 2. Physical Resource sharing architecture using LHP protocol

this field of study is wide range of data services with various QoS requirements [21]. The resources could be software or hardware entities. For example, in the vehicle routing process, the routing protocol can share the routing information as a software resource with neighboring CAVs, such as the work done in [22] and [23]. Furthermore, we target the computational hardware resources like CPU, GPU, and memory to be shared through sharing services. The motivation of this work is to enable smart ITS through sharing of resources as the the data processing and computational requirements for providing a wide variety of services are constantly increasing [24].

## III. Secure Resource Sharing Architecture

To make computational resource sharing available in CAVs, we propose a new resource-sharing architecture (Fig. 2) that facilitates communication and security while being compliant to ETSI C-ITS standards. Resources are computational facilities in each vehicle, such as CPU, GPU, and memory. A vehicle can request neighbouring vehicles to share their resources to help in improving task efficiency for the requester, such as fetching a critical update over-the-air for the requester because at a given moment it has from insufficient memory. The Long Heterogeneous Platooning (LHP) formation protocol has been proposed in [25] to make it possible to form a very long platoon with different types of vehicles on the roads. Figure 1 shows the communication flow among vehicles in the resource sharing scenario. The proposed communication model fits easily into the LHP protocol by using its *Platoon Management Message (PMM)* message containers to support the available resources in each vehicle (more details in subsection III-A).

In the facilities layer of the architecture, *resource sharing* and *LHP services* modules are considered. The former one deals with the participant selection and cost evaluation of the resource-sharing process (Sec. III-B), and the latter one provides information on the available resources at each CAV. The resource sharing module uses the LHP services module while performing its resource discovery phase. Identity information, the necessary amount of computational resources, and the time period of use make up a request message. All potential participants who have been requested information on their available resources use a PMM message to declare the information. Next, a multi-feature evaluation method selects the vehicle with the highest score and sends it a sharing request. In the case of accepting the request, a physical layer key generation method is leveraged to encrypt the communicated data among the requester and resource owner in the sharing process.

In this paper, we use the proposed model in a parking-lot scenario where the CAVs are sharing resources with the others in their vicinity. Assuming that all CAVs in the resource-sharing application have already passed the requirements determined by the enrollment authority (EA) of the ITS system according to the corresponding standards like [26], we propose a security key generation method to be used in the physical layer of the resource sharing architecture.

### A. LHP protocol

The LHP protocol enables the formation of long platoons with different vehicle types, utilizing sub-platoon and virtual leader concepts for intra-platoon communication and platoon-level operations. Coordination in LHP platoons is achieved through ETSI ITS-compliant messages, including an extended CAM message and PMM message to support decision-making in the long platoon application. Each participating vehicle's facilities are considered in the formation of the LHP platoons. Sub-platoon leaders are selected from vehicles with superior facilities to provide better support (for followers) and communication with the front leader. The facilities' information considered in PMM includes but is not limited to communication technology (e.g. standard and antenna), sensors (e.g. lidar, radar, and camera), and computational resources. Our proposed architecture extends LHP capabilities toward resource sharing in platoons.

### B. Score metric for the selection of resource sharing vehicle

To select the optimal vehicle for resource sharing, we evaluate each vehicle based on multiple characteristics: available memory, GPU capacity, reliability, speed, and determinism. Each characteristic is assigned a specific weight reflecting its contribution to the overall utility. The vehicle with the highest calculated score is chosen for resource sharing. The weights can be assigned to reflect the need for the operation. For instance, for an application needing just GPU the user can define a larger weight to $w_g$ compared to the other qualities.

Let $N$ represent the number of vehicles in the system. For each vehicle $i$, where $i \in 1, 2, \ldots, N$, $M_i$, the available memory (in GB), $G_i$, the available GPU (in TFLOPS), $R_i$, the Reliability and the $S_i$:, Speed (in Gbps) are considered.

For each vehicle, the normalized attributes are computed by dividing the respective attribute by its maximum value across all vehicles. The score $S$ for vehicle $i$ is calculated using a weighted sum of the normalized values:

$$S = w_m \left( \frac{M_i}{\max(M)} \right) + w_g \left( \frac{G_i}{\max(G)} \right) + w_r R_i + w_s \left( \frac{S_i}{\max(S)} \right) \tag{1}$$

The vehicle with the highest score is selected as the optimal vehicle for resource sharing:

$$\text{Selected Vehicle} = \arg\max_i(S_i). \tag{2}$$

The scoring system ensures that vehicles with better computational capacity, higher reliability, and better network speed are prioritized. This enhances the efficiency and performance of resource sharing.

### C. Path loss model

Let us take a scenario where 30 vehicles are in a parking lot. In such a case, modeling the wireless communication between them requires consideration of a suitable path loss model. Given the unique environment of a parking lot characterized by line-of-sight (LOS) and nonline-of-sight(NLOS) conditions due to other vehicles and structural obstructions, we consider the log-normal model.

$$L(d) = L_0 + 10n\log_{10}\left(\frac{d}{d_0}\right) + X_\sigma \tag{3}$$

Where:

- $L(d)$ is the path loss at distance $d$ (in dB),
- $L_0$ is the reference path loss at a reference distance $d_0$ (usually 1 meter),
- $n$ is the path loss exponent, which characterizes how quickly the signal decays with distance (typically between 2 and 6 depending on the environment),
- $d$ is the distance between the transmitter and receiver,
- $d_0$ is the reference distance,
- $X_\sigma$ is a random variable representing shadow fading, which accounts for environmental factors like obstacles. It follows a normal distribution with mean zero and standard deviation $\sigma$ (typically 6-12 dB).

For a parking lot, both LOS and NLOS conditions need to be considered. In LOS conditions, the path loss exponent $n$ is typically smaller, usually around 2, while in NLOS conditions, $n$ tends to be larger, typically between 3 and 4 [27].

In a parking lot, vehicles can obstruct the LOS path between two vehicles, leading to NLOS conditions. The presence of such obstructions can cause multipath fading, which is reflected in the random variable $X_\sigma$, representing the shadow fading. The shadow fading can vary based on the layout of the parking lot, including factors such as the density of parked vehicles, the height of the vehicles, and the physical structures (e.g., walls or barriers) surrounding the lot. This can be modeled as:

$$X_\sigma \sim \mathcal{N}(0, \sigma^2) \tag{4}$$

Where $\mathcal{N}(0, \sigma^2)$ represents a normal distribution with zero mean and variance $\sigma^2$, where $\sigma$ typically ranges from 6 dB to 12 dB, depending on the level of obstruction.

### D. Secret Key Generation

Manufacturers can remotely deliver software packages like patches, performance enhancers, or security updates without physically accessing the vehicle. This is a fundamental pillar of SDVs as it facilitates continuous improvement and adaptation of vehicle systems. Enabling an application like OTA through shared physical resources introduces significant challenges in security and system integrity. A compromised update can affect multiple vehicle functions and lead to catastrophic damage if resources are not properly sandboxed. This shows a mandatory need for security protocols in line with the shared hardware to ensure safe and reliable operation in the SDV ecosystem. Classical encoding techniques assign a unique binary code to each quantization bin within a defined range. These binary codes are then used to generate secret bits, which help in encrypting and secure data transmission in a vehicular network. By mapping a binary code to each bin, a public-key cryptosystem can extract and utilize these secret bits for encryption.

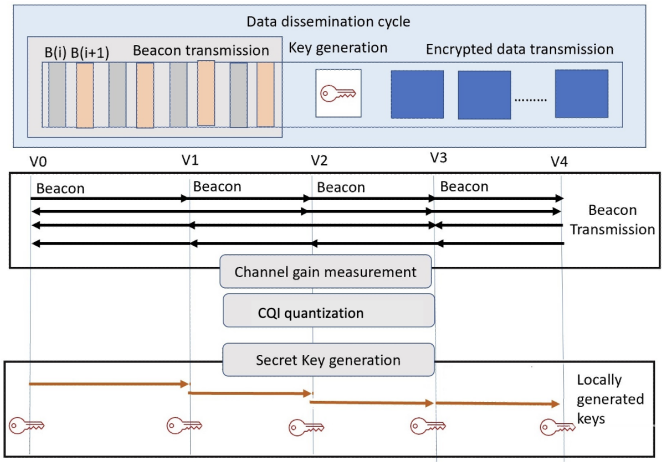


Fig. 3. PHY-layer key generation for the LHP protocol

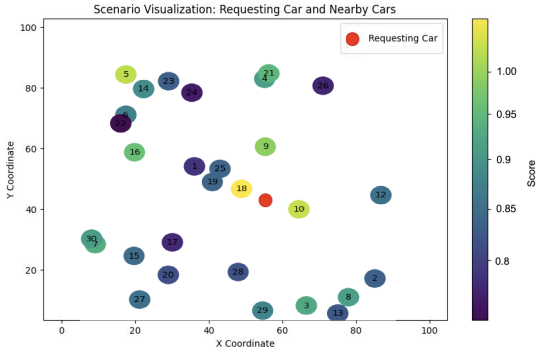


Fig. 4. Simulation of the parking lot scenario where the requesting vehicle seeks to gain resources from the nearby vehicles based on scores.

An encoding method assigns a binary code to each bin, ensuring that a secret key is generated. We utilize gray coding as an encoding method where neighboring codewords differ by only one bit. This ensures efficient encoding with minimal errors. The secret key for each vehicle is determined by a specific rule, where certain values are assigned based on a modular function. A predefined sequence of Gray codewords

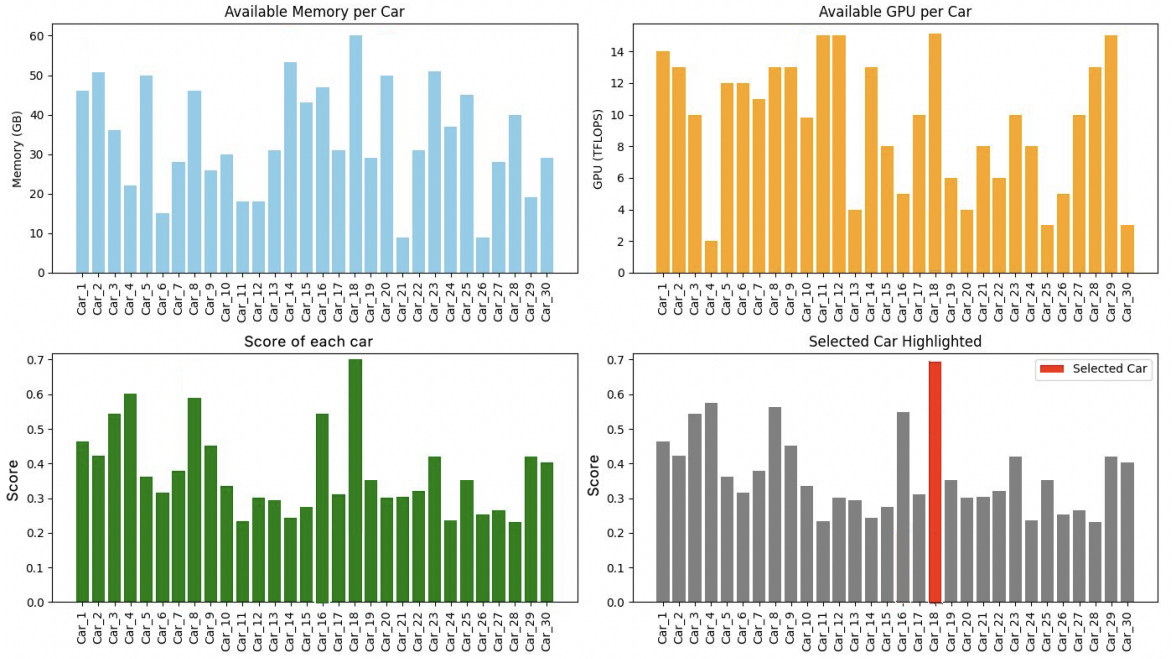


Fig. 5. Performance metrics of vehicles in alliance with the scenario and vehicles selected based on the highest score criteria

allows for structured encryption, ensuring a smooth and secure transition between codewords. These generated keys can be either symmetric or asymmetric, depending on the required security level. Elliptic-Curve Cryptography (ECC) is used in generating keys where the connected vehicles agree on an elliptic curve and a defined base point. Each vehicle generates a private key and its corresponding public key, which will be the base point on the elliptic curve. Channel Quality Indicator (CQI) quantization maps continuous channel quality values into discrete levels. This categorizes the communication channel into predefined states. This process helps in adapting transmission parameters, such as modulation and coding schemes. The strength and reliability of the wireless link is assessed through channel gain measurement. This is done by evaluating signal characteristics such as received power, fading conditions, and interference levels. These measured values are used as entropy sources for key generation, ensuring that cryptographic keys are dynamically derived from real-time wireless conditions. In our PHY-based security model (Figure 3) using variations in channel gain, unique and symmetric keys are independently generated from communicating nodes without direct key exchange, enhancing security against eavesdroppers.

## IV. Results

For the experimental setup, we consider a parking lot-oriented vehicular environment where cars in the vicinity share physical resources such as GPUs and memory to enhance computational efficiency. We present a simulation of this scenario (Figure 4), where a requesting vehicle (red node) seeks to gain resources from the nearby vehicles. All the vehicles in the scenario are differentiated by scores based on the score metric defined in Section III. Better scores denote better reliability and resource availability in line with available memory and GPU. These functional data are shared with the requesting vehicle, and the decision to choose the vehicle is made based on the highest score.

TABLE I
Randomness of the evaluated input sequence is considered to be successful if all P-values exceed 0.01

| NIST Test | P values |
|---|---|
| Frequency Test | 0.8 |
| Block Frequency Test | 0.9 |
| Cumulative Sums (FWD) | 0.6 |
| Cumulative Sums (REV) | 0.8 |
| Runs | 0.7 |
| FFT | 0.4 |
| Approx. Entropy | 0.3 |
| Serial | 0.42, 0.43 |

Figure 5 shows the amount of available memory and GPU at every car in the vicinity. The score is a result of an amalgamation of all the resources. For instance, cars 11, 12 and 18 almost have the same levels of GPU, however cars 11 and 12 almost have 30 % less memory to share when compared with car 18. As a result of this, car 18 has a much higher score when compared to the other cars in the vicinity.

We used the standard randomness test suite from NIST to verify the randomness of the keys generated between the two vehicles. The NIST provides a set of 16 tests to verify the randomness. Among them, seven are selected to verify the randomness of the keys generated by the vehicles. The P-value in Table I indicates the probability that a highly efficient random number generator could produce a sequence with less

randomness than the input sequence being evaluated. For a successful test, all the recorded P-values must exceed 0.01. Specific tests within this suite required input bit streams that are greater than 106 bits. As shown in Table I, the keys generated between every pair of vehicles have P-values larger than the threshold of 0.01 and they pass the test. This test shows that all the generated secret bit streams are random with a high confidence level of 99%. Higher randomness indicates the complexity of cracking the keys by any malicious eavesdropper.

## V. Conclusion and Future Works

In this paper, we propose a novel physical resource sharing framework for vehicular networks using a weighted score metric. This framework can enable functionalities such as remote OTA and dynamic resource provisioning in cooperative vehicular networks. This method mitigates the overburdening of any single node's computational resources by provisioning resources across the network based on availability and reliability through the score metric. Furthermore, we integrate a physical-layer-based key generation mechanism that leverages unique channel characteristics to establish cryptographic keys between resource-sharing vehicles. Through simulation and the standard tools of NIST, we study the selection of the resource-sharing vehicle and the robustness of the underlying security protocol. We aim at learning the resource-sharing dynamics for realistic vehicular mobility patterns through behavior-driven models like lane changing and congestion-aware rerouting, vehicle mobility, task urgency, and energy constraints. We further aim to explore and compare resource sharing strategies that take into consideration of real-time application requirements, device capabilities, and energy constraints of vehicles. As the applications might want to offload sensitive data, privacy-oriented resource sharing will also be explored in an extended version of this work.

## References


[1] H. Kurunathan *et al.*, "Towards safe cooperative autonomous platoon systems using cots equipment," in *2023 IEEE 24th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE, 2023, pp. 464–469.

[2] J. Pereira, H. Kurunathan, P. M. Santos *et al.*, "Edge-aided v2x collision avoidance with platoons: Towards a hybrid evaluation toolset," in *2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. IEEE, 2023, pp. 68–71.

[3] R. Rafael, H. Kurunathan, and E. Tovar, "An rt-cloud solution towards security in vehicular platooning systems," in *2023 RT-Cloud workshop, 36th Euro Micro Conference on Real-Time Systems*, 2023.

[4] H. I. Ali *et al.*, "Navigating the challenges and opportunities of securing internet of autonomous vehicles with lightweight authentication," *IEEE Access*, 2025.

[5] H. Kurunathan, H. I. Ali, G. Javanmardi, M. Eldefrawy, M. G. Gaitán, R. Robles, P. Yomsi, and E. Tovar, "Adaptive intrusion mitigation in software-defined vehicles using deep reinforcement learning," in *Proceedings of the 4th International Workshop on Real-time and IntelliGent Edge computing*, 2025, pp. 1–6.

[6] W. Tiberti *et al.*, "Tightening up security in low power deterministic networks," in *2020 16th IEEE International Conference on Factory Communication Systems (WFCS)*. IEEE, 2020, pp. 1–7.

[7] H. Kurunathan, K. Li, E. Tovar, A. M. Jorge, W. Ni, and A. Jamalipour, "Drl-keyagree: An intelligent combinatorial deep reinforcement learning-based vehicular platooning secret key generation," *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[8] H. Kurunathan, K. Li, W. Ni, N. Li, E. Tovar, and M. Guizani, "Exploring lstm-assisted a2c for physical layer security in vehicular cyber-physical systems," in *2024 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, 2024, pp. 1177–1182.

[9] X.-H. Sun and M. Wu, "Quality of service of grid computing: Resource sharing," in *Sixth International Conference on Grid and Cooperative Computing (GCC 2007)*, 2007, pp. 395–402.

[10] S. Sabamoniri and A. Souri, "A weighted resource discovery approach in grid computing: Formal verification approach and simulation," *International Journal of Pervasive Computing and Communications*, vol. 15, no. 3/4, pp. 199–223, 2019.

[11] A. Belgacem, K. Beghdad-Bey, and H. Nacer, "Dynamic resource allocation method based on symbiotic organism search algorithm in cloud computing," *IEEE Transactions on Cloud Computing*, vol. 10, no. 3, pp. 1714–1725, 2022.

[12] L. Wei, C. H. Foh, B. He, and J. Cai, "Towards efficient resource allocation for heterogeneous workloads in iaas clouds," *IEEE Transactions on Cloud Computing*, vol. 6, no. 1, pp. 264–275, 2018.

[13] R. Cong, Z. Zhao, G. Min, C. Feng, and Y. Jiang, "Edgego: A mobile resource-sharing framework for 6g edge computing in massive iot systems," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14 521–14 529, 2022.

[14] Y. Li, L. Li, and P. Fan, "Mobility-aware computation offloading and resource allocation for noma mec in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 8, pp. 11 934–11 948, 2024.

[15] D. Cao, M. Wu, N. Gu, R. S. Sherratt, U. Ghosh, and P. K. Sharma, "Joint optimization of computation offloading and resource allocation considering task prioritization in isac-assisted vehicular network," *IEEE Internet of Things Journal*, vol. 11, no. 18, pp. 29 523–29 532, 2024.

[16] T. D. Nguyen, T.-D. Nguyen, V. D. Nguyen, X.-Q. Pham, and E.-N. Huh, "Cost-effective resource sharing in an internet of vehicles-employed mobile edge computing environment," *Symmetry*, vol. 10, no. 11, p. 594, 2018.

[17] H. Chai, S. Leng, K. Zhang, and S. Mao, "Proof-of-reputation based-consortium blockchain for trust resource sharing in internet of vehicles," *IEEE Access*, vol. 7, pp. 175 744–175 757, 2019.

[18] C. Tan, X. Li, T. H. Luan, B. Gu, Y. Qu, and L. Gao, "Digital twin based remote resource sharing in internet of vehicles using consortium blockchain," in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, 2021, pp. 1–6.

[19] X. Peng, H. Zhou, B. Qian, K. Yu, F. Lyu, and W. Xu, "Enabling security-aware d2d spectrum resource sharing for connected autonomous vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3799–3811, 2020.

[20] A. Knari, M. Derfouf, M.-A. Koulali, and A. Khoumsi, "Multi-agent deep reinforcement learning for content caching within the internet of vehicles," *Ad Hoc Networks*, vol. 152, p. 103305, 2024.

[21] M. Noor-A-Rahim, Z. Liu, H. Lee, G. G. M. N. Ali, D. Pesch, and P. Xiao, "A survey on resource allocation in vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 701–721, 2022.

[22] A. A. Taleb, "Vanet routing protocols and architectures: An overview," *Journal of Computer Science*, vol. 14, no. 3, pp. 423–434, Mar 2018. [Online]. Available: https://thescipub.com/abstract/jcssp.2018.423.434

[23] M. Sohail, Z. Latif, S. Javed, S. Biswas, S. Ajmal, U. Iqbal, M. Raza, and A. U. Khan, "Routing protocols in vehicular adhoc networks (vanets): A comprehensive survey," *Internet of Things*, vol. 23, p. 100837, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660523001609

[24] A. H. Salem, I. W. Damaj, and H. T. Mouftah, "Vehicle as a computational resource: Optimizing quality of experience for connected vehicles in a smart city," *Vehicular Communications*, vol. 33, p. 100432, 2022.

[25] S. Sabamoniri, P. M. Santos, and L. Almeida, "An ETSI ITS-Compliant formation protocol to support long heterogeneous platoons," in *2023 IEEE Vehicular Networking Conference (VNC)*, 2023, pp. 53–56.

[26] T. I. ETSI, "ETSI TS 102 731 V1.1.1 (2010-09) - Intelligent Transport Systems (ITS); Security; Security Services and Architecture," ETSI, Tech. Rep., Sep. 2010.

[27] J. Park, H.-B. Jeon, J. Cho, and C.-B. Chae, "Measurement-based close-in path loss modeling with diffraction for rural long-distance communications," *IEEE Wireless Communications Letters*, vol. 12, no. 8, pp. 1334–1338, 2023.