k-anonymity in Resource Allocation for Vehicle-to-Everything (V2X) Systems

Andres Vejar, Faysal Marzuk, and Piotr Chołda

AGH University of Kraków, Kraków, Poland

https://doi.org/10.26636/jtit.2025.FITCE2024.1998

Abstract — Sixth generation (6G) vehicle-to-everything (V2X) systems face numerous security threats, including Sybil and denial-of-service (DoS) cyber-attacks. To provide a secure exchange of data and protect users' identities in 6G V2X communication systems, anonymization techniques – such as k-anonymity – can be used. In this work, we study centralized vs. k-anonymity based resource allocation methods in a vehicular edge computing (VEC) network. Allocation decisions for vehicular networks are classically posed as a centralized optimization task. Therefore, an information flow is transmitted from the vehicles to the communication premises. In addition to a resource allocation decision, vehicle information is not required. We analyze the centralized allocation versus k-anonymous allocation models. To show a potential deterioration introduced by anonymity, we quantify the gap in the optimal goal in two cases: based on resource allocation and with aim at energy reduction. Our numerical results indicate that energy consumption rises by 1% in smaller scenarios and 23% in medium scenarios, whereas it decreases by 14% in larger scenarios.

Keywords — k-anonymity, privacy-enhancing technologies, resource allocation in 6G, vehicle-to-everything (V2X) systems

1. Introduction

Sixth generation (6G) networks are expected to facilitate and enhance the services of intelligent transportation systems (ITS) by integrating artificial intelligence (AI) techniques with machine learning (ML) algorithms [1]. The vehicle-to-everything (V2X) system, which is an application of ITS, enables the exchange of information between vehicles and their surroundings [2]. Vehicles can communicate through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, such as the roadside unit (RSU), as shown in Fig. 1. The newly proposed 6G V2X communication systems can easily be targeted by different security attacks due to their high mobility, highly dynamic topology, and variety of communications [3].

The deployment of AI techniques in the design of vehicular edge computing (VEC) networks has limitations due to robust security mechanisms, considerations of privacy and ethics, as well as new security developments [1]. The collection and processing of data in VEC systems require the protection of user privacy with privacy-enhancing technologies (PET), including differential privacy and data anonymization methods, to reduce the risk of re-identification and unauthorized monitoring [1].

Several applications of PETs involve k-anonymity [4] and its variations [5], [6]. The privacy and efficiency requirements in vehicular networks can be addressed using k-anonymity. To achieve these requirements, k-anonymity with differential privacy can be combined with transactional blockchain registration [7].

A framework for the sharing of private data within ad hoc vehicular networks (VANET) is introduced using federated learning (FL) and local differential privacy [8]. This approach guarantees protection against inference and gradient leakage attacks while providing higher efficiency than conventional FL-based methods. A local differential privacy technique is used to provide a privacy preservation solution for VANET by excluding the need for a third party to anonymize critical information [9]. The disclosure of sensitive data, such as vehicle positions in location services, is considered a potential threat to the privacy of users [10]. The k-anonymity method is used to maintain location privacy in edge computing (EC) [11], and to preserve location privacy on the Internet of Vehicles (IoV) [12].

Zero-trust architectures that provide privacy by design need to be privileged to provide essential data security and privacy preservation requirements for the 6G V2X allocation process. Due to the various V2X applications, such as V2P and V2V communications, the design of a secure and private management system is a critical concern [13].

Ensuring secure data exchanges requires trusted management in the allocation process. To address the challenge of designing a secure 6G V2X communication system with VEC services, anonymization techniques can be used to protect the identity of users by reducing specific vehicle information. That leads to a reduction of the surface of attack in the V2X infrastructure.

If the resource allocation system is compromised by malicious agents, the identification of each vehicle is available to the

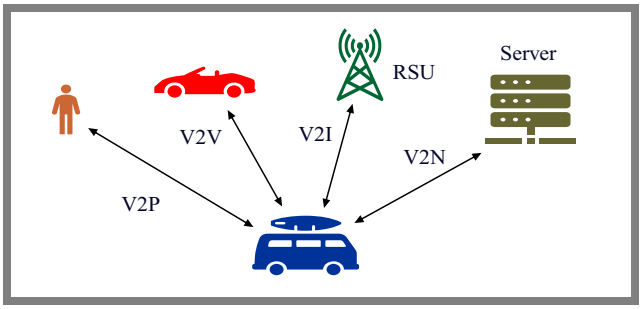

Fig. 1. Types of V2X communications.

attacker. This information can be used to escalate the attacks to other elements of the 6G V2X system, notably V2V and V2P. In this work, we study the effect of incorporating k-anonymity into the 6G V2X allocation system.

2. System Description

Table 1 summarizes the mathematical notation used to describe the system under study.

We consider a 6G V2X communication system that includes sets of vehicles and RSUs, as shown in Fig. 2. RSUs extend the computation and communication capabilities to vehicles by being deployed closer to end users. In our infrastructure of the system under study, vehicles need to send their data to RSUs for processing (offloading option).

We investigate a scenario consisting of a set of RSUs ($i = 1, 2, \ldots, I$) and a set of vehicles ($j = 1, 2, \ldots, J$). Each RSU i has several available resource blocks (RBs) per time interval, denoted by M_i. Each vehicle j, if it is associated with RSU i, will require several RBs to upload its data, indicated by $R_{i,j}$. The required number of RBs depends on the signal-to interference, noise ratio (SINR) values, and the uplink data rates. We need to determine the optimal assignments between RSUs and vehicles in order to decide whether to turn on or off the RSU. Our objective is to reduce the energy consumption and the number of active RSUs depending on the number of RBs required by each vehicle and subject to uplink bandwidth and uplink time constraints illustrated by SINR and inter-cell interference (ICI). We calculate SINR values for the uplink of

Tab. 1. Mathematical notations used throughout the paper.

Symbol	Meaning
I	Set of RSUs
J	Set of vehicles
P_j	Transmission power of vehicle j
D_j	Communication demand of vehicle j
Φ_j	Computation demand of vehicle j
M_i	Available uplink RBs per time slot for RSU i
F_i	Maximum available computation capacity of RSU i
$\mathcal{L}_j$	Maximum allowed latency for vehicle j
$\mathrm{R_{i,j}}$	Required RBs per time slot to send data
$\gamma_{i,j}$	SINR value for vehicle j and RSU i
$\mathrm{H}_{i,j}$	Threshold value for $\gamma_{i,j}$
$\mathrm{U}_{i,j}$	Required uplink data rate of vehicle j
$\mathcal{U}_{i,j}$	Link capacity between vehicle j and RSU i
ψ_i^J	Energy coefficient of RSU server's chip architecture
x_i	Decision variable to turn on/off the RSU i
$y_{i,j}$	Decision variable indicating whether vehicle j is associated with RSU i or not

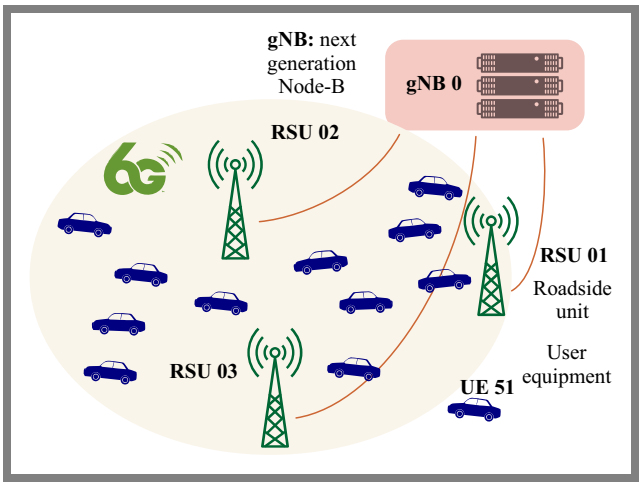

Fig. 2. An example of a V2X communication system.

data from the ICI aggregate uplink, the coverage of the RSU, and the distance between the vehicle and the interference RSU [14].

After calculating the SINR values for each vehicle, we determine the RB's data rates depending on different modulation orders, SINR ranges, and efficiencies from the mapping table given in [15]. This mapping is used to determine the number of required RBs where an RB per time interval of 0.25 ms consists of 12 sub-carriers of 60 kHz spacing and each sub-carrier consists of 14 OFDM symbols. The number of RBs $R_{i,j}$ required by each vehicle to process its data is calculated as $R_{i,j} = U_{n,v} \times (12 \times 14 \times \text{efficiency})^{-1}$.

Considering I RSUs with a number of available uplink RBs (M_i) and J vehicles with a number of required RBs per time slot for uploading the data from vehicle j to the i RSU $R_{i,j}$, we need to determine $y_{i,j}$ which denotes whether the vehicle j is associated with RSU i or not; and x_i which indicates whether to turn the RSU i on or off. We formulate an optimization problem to minimize the energy consumption and the number of active RSUs as:

$$\min\ \omega_1 \sum_{i\in \mathrm{I}} x_i + \omega_2 \sum_{i\in \mathrm{I}} \sum_{j\in \mathrm{J}} \left(\frac{P_j \mathrm{D}_j}{\mathcal{U}_{i,j}} + \frac{\psi_i^J \mathrm{D}_j \Phi_j}{\mathrm{f}_{i,j}^{-2}} \right) y_{i,j}\,, \quad (1)$$

$$\text{s.t.} \quad \sum_{j\in \mathrm{J}} \mathrm{R}_{i,j}\, y_{i,j} \leqslant \mathrm{M}_i, \quad \forall\, i \in \mathrm{I}\,, \quad (2)$$

$$\sum_{j\in \mathrm{J}} \gamma_{i,j}\, y_{i,j} \geqslant \mathrm{H_{i,j}}, \quad \forall\, i \in \mathrm{I}\,, \quad (3)$$

$$\sum_{j\in \mathrm{J}} \mathrm{f}_{i,j}\, y_{i,j} \leqslant \mathrm{F}_i, \quad \forall\, i \in \mathrm{I}\,, \quad (4)$$

$$\sum_{i\in \mathrm{I}} \mathrm{L}_{i,j}\, y_{i,j} \leqslant \mathcal{L}_j, \quad \forall\, j \in \mathrm{J}\,, \quad (5)$$

$$\sum_{i\in \mathrm{I}} y_{i,j} = 1, \quad \forall\, j \in \mathrm{J}\,, \quad (6)$$

$$x_i \geqslant y_{i,j}, \quad \forall\, i \in \mathrm{I}, \quad \forall\, j \in \mathrm{J}\,, \quad (7)$$

$$x_i,\ y_{i,j} \in \{0, 1\}, \quad \forall\, i \in \mathrm{I}, \quad \forall\, j \in \mathrm{J}\,. \quad (8)$$

3. Results

As a case study, we first investigate an allocation scenario consisting of 4 RSUs and 32 vehicles. Table 2 lists the parameter values that are used in the calculations and evaluations, where the values are assumed according to the service requirements for 6G V2X services and to guarantee the QoS requirements of the communications system [16].

Each vehicle, if assigned to an RSU, will upload its computational tasks to be processed. Vehicle information includes:

1) communication demand, indicated by D_j, in the range $10 - 60$ kbits,
2) computation demand, indicated by Φ_j, in the range $100 - 150$ cycles/bit,
3) transmission power, indicated by P_j, in the range $23 - 33$ dBm.

This information D_j, Φ_j, P_j is used to calculate the communication delay, the computation delay, and the energy consumption for centralized allocation [17]. If the allocation system is breached, these details can be exploited to uncover, monitor, and further compromise the privacy of UEs.

Designing systems with enhanced privacy techniques such as k-anonymity or differential privacy can reduce the probability of unwanted or unauthorized tracking and re-identification.

In this work, we use V2V communication to achieve k-anonymity through proximity clusters. We assume that V2V communication is secured in its radius of operation. The triplet D_j, Φ_j, P_j is then distributed in the vehicle proximity cluster, and the aggregate measurement is pooled into its average value.

Each vehicle, by V2I communication, transmits the aggregated triplet values, denoted by $< D_j, \Phi_j, P_j >$ to the RSUs. Similarly, the next generation Node-B (gNB) estimates the SINR values of each vehicle with respect to each RSU. To minimize user information leakage, the SINR values are also aggregated for each proximity cluster and are denoted by $<$ SINR $>$.

The membership in a cluster is verified by the vehicles that share the same value of $< D_j, \Phi_j, P_j >$. The k-private allocation system receives only the aggregated data from vehicles $< D_j, \Phi_j, P_j >$ and the aggregated SINR from gNB, $<$ SINR $>$.

We compare the k-anonymous V2X allocation model presented in Fig. 2 with the centralized allocation model [17]. The scenarios consider an initial density of 126 RSUs/km^2, and a density of vehicles of 1000 vehicles/km^2.

As can be seen in Tab. 3, our numerical results shows that for small and medium scenarios the energy consumption is increased by 1% and 23% respectively while for the large scenario the energy consumption is reduced by 14%.

We note that for the large scenario of 190 vehicles, not all the original constraints are satisfied, allowing for a reduced energy consumption in the k-anonymous version than in the centralized version.

Tab. 2. Parameter values used in the evaluation.

Parameter	Value	Parameter	Value
RSU coverage	200 m	P_j	23 – 33 dBm
M_i	135 RBs	$H_{i,j}$	–7 dB
F_i	20 GHz	$U_{i,j}$	50 – 100 Mbps
$\mathcal{L}_j$	30 ms	D_j	10 – 60 kbit

Tab. 3. k-anonymous versus centralized allocations.

Allocation	No. of RSUs selected/ available	No. of vehicles	Energy
Centralized	2/4	32	0.002432
k-anonymous	2/4	32	0.002459
Centralized	4/16	127	0.005532
k-anonymous	5/16	127	0.006830
Centralized	7/24	190	0.009790
k-anonymous	7/24	190	0.008454

4. Conclusions

In this study, we investigated the incorporation of PETs into the 6G V2X allocation system. Vehicle information was used to calculate communication delay, computation delay, and energy consumption for centralized allocation. We compared centralized resource allocation versus k-anonymous allocation.

Our implementation indicated how variations in optimal allocations are affected when PET is applied to the V2X system. Noting that the k-anonymous technique implemented can be applied to allocation schemes different from the optimal model studied in this work.

Our numerical results illustrated that energy consumption increased by 1% in smaller scenarios and 23% in medium scenarios, while it decreased by 14% in larger scenarios.

Future research will explore enhanced methods, focusing on integrating online allocation through AI models. We plan to explore enhanced methods, focusing on integrating online allocation through AI models. In addition, we plan to evaluate the proposed algorithms in a real world scenario to demonstrate their effectiveness.

Acknowledgments

This research is supported by the National Research Institute, grant number POIR.04.02.00-00-D008/20-01, on “National Laboratory for Advanced 5G Research” (acronym PL-5G) as part of the Measure 4.2 Development of the modern research infrastructure of the science sector 2014–2020 financed by the European Regional Development Fund.

References

[1] M. Humayun *et al.*, "Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey", *IEEE Access*, vol. 12, pp. 25469–25490, 2024 (https://doi.org/10.1109/ACCESS.2024.3365634).

[2] O. Aouedi *et al.*, "A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions", *IEEE Communications Surveys & Tutorials*, 2024 (https://doi.org/10.1109/COMST.2024.3430368).

[3] M. AlMarshoud, M.S. Kiraz, and A.H. Al-Bayatti, "Security, Privacy, and Decentralized Trust Management in VANETs: A Review of Current Research and Future Directions", *ACM Computing Surveys*, vol. 56, pp. 1–29, 2024 (https://doi.org/10.1145/3656166).

[4] P. Samarati and L. Sweeney, "Generalizing Data to Provide Anonymity when Disclosing Information (Abstract)", *Proc. of the Seventeenth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems. PODS '98*, p. 188, 1998 (https://doi.org/10.1145/275487.275508).

[5] F. Song, T. Ma, Y. Tian, and M. Al-Rodhaan, "A New Method of Privacy Protection: Random k-Anonymous", *IEEE Access*, vol. 7, pp. 75434–75445, 2019 (https://doi.org/10.1109/ACCESS.2019.2919165).

[6] F. Wang, H. Chen, and Y. Zhou. "A Privacy Protection Application of Consumer Personal Information Based on an Improved K-Anonymity Algorithm", *2024 5th International Conference for Emerging Technology (INCET)*, Belgaum, India, 2024 (https://doi.org/10.1109/INCET61516.2024.10593091).

[7] C. Gu, X. Cui, M. Li, and D. Hu. "An Efficient and Privacy-preserving Information Reporting Framework for Traffic Monitoring in Vehicular Networks", *IEEE Transactions on Vehicular Technology*, vol. 72, pp. 7900–7913, 2023 (https://doi.org/10.1109/TVT.2023.3241656).

[8] H. Batool *et al.*, "A Secure and Privacy Preserved Infrastructure for VANETs Based on Federated Learning with Local Differential Privacy", *Information Sciences*, vol. 652, art. no. 119717, 2024 (https://doi.org/10.1016/j.ins.2023.119717).

[9] Z. Iftikhar *et al.*, "Privacy Preservation in the Internet of Vehicles Using Local Differential Privacy and IOTA Ledger", *Cluster Computing*, vol. 26, pp. 3361–3377, 2023 (https://doi.org/10.1007/s10586-023-04002-0).

[10] Z. Qi and W. Chen, "Location Privacy Protection of IoV Based on Blockchain and K-anonymity Technology", *2023 6th International Conference on Electronics Technology (ICET)*, Chengdu, China, 2023 (https://doi.org/10.1109/ICET58434.2023.10211967).

[11] S. Zhang *et al.*, "A Caching-based Dual K-anonymous Location Privacy-preserving Scheme for Edge Computing", *IEEE Internet of Things Journal*, vol. 10, pp. 9768–9781, 2023 (https://doi.org/10.1109/JIOT.2023.3235707).

[12] B. Wang, J. Liu, and L. Dai, "K-anonymity-based Privacy-preserving and Efficient Location-based Services for Internet of Vehicles Withstand Viterbi Attack", *Proc. of International Conference on Image, Vision and Intelligent Systems 2022 (ICIVIS 2022)*, pp. 1016–1028, 2022 (https://doi.org/10.1007/978-981-99-0923-0_101).

[13] M. Georgiades and M.S. Poullas, "Emerging Technologies for V2X Communication and Vehicular Edge Computing in the 6G Era: Challenges and Opportunities for Sustainable IoV", *2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*, Pafos, Cyprus, 2023 (https://doi.org/10.1109/DCOSS-IoT58021.2023.00108).

[14] R.-H. Hwang, F. Marzuk, M. Sikora, P. Chołda, and Y.-D. Lin, "Resource Management in LADNs Supporting 5G V2X Communications", IEEE Access, vol. 11, pp. 63958–63971, 2020 (https://doi.org/10.1109/ACCESS.2023.3288699).

[15] ETSI, "Evolved Universal Terrestrial Radio Access (E-UTRA). Physical Layer Procedures (Technical Specification)", 3GPP TS 36.213 V17.6.0. Release 17, 2024.

[16] K. Sehla, T.M.T. Nguyen, G. Pujolle, and P.B. Velloso, "Resource Allocation Modes in C-V2X: From LTE-V2X to 5G-V2X", *IEEE Internet of Things Journal*, vol. 9, pp. 8291–8314, 2022 (https://doi.org/10.1109/JIOT.2022.3159591).

[17] F. Marzuk, A. Vejar, and P. Chołda, "Optimal Resource Allocation for 6G V2X Communication Systems". *Przegląd Telekomunikacyjny – Wiadomości Telekomunikacyjne*, vol. 97, pp. 350–353, 2024 (https://doi.org/10.15199/59.2024.4.78).

Andres Vejar, Ph.D.
Institute of Telecommunications
https://orcid.org/0000-0002-2041-0387
E-mail: avejar@agh.edu.pl
AGH University of Kraków, Kraków, Poland
https://www.agh.edu.pl

Faysal Marzuk, M.Sc.
Institute of Telecommunications
https://orcid.org/0000-0002-7576-182X
E-mail: faysal.marzuk@agh.edu.pl
AGH University of Kraków, Kraków, Poland
https://www.agh.edu.pl

Piotr Chołda, D.Sc.
Institute of Telecommunications
https://orcid.org/0000-0003-2018-4057
E-mail: piotr.cholda@agh.edu.pl
AGH University of Kraków, Kraków, Poland
https://www.agh.edu.pl