63rd FITCE International Congress
26 - 28 September 2024, Kraków, Poland

k-anonymity in Resource Allocation for V2X

Andres Vejar[1]; Faysal Marzuk[2]; Piotr Chołda[3]

Institute of Telecommunications, AGH University of Krakow, Kraków, Poland

[1]avejar@agh.edu.pl, [2]marzuk@agh.edu.pl, [3]piotr.cholda@agh.edu.pl

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 paper, we study centralized vs. k-anonymity based resource allocation in 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. In this work, we analyze the centralized allocation vs. k-anonymous allocation models. To show a potential deterioration introduced by anonymity, we quantify the gap in the optimal goal (based on resource allocation and with aim at energy reduction) in both cases.

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 [4]. The vehicle-to-everything (V2X) system, which is an application of ITS, enables the exchange of information between vehicles and their surroundings [1]. Vehicles can communicate through vehicle-to-vehicle (V2V) and vehicle-to-roadside unit (V2RSU) communications. 6G V2X communication systems can easily be targeted by different security attacks due to their high mobility, highly dynamic topology, and variety of communications [1]. The deployment of AI techniques in the design of vehicular edge computing (VEC) networks has limitations due to robust security mechanisms and considerations of privacy and ethics, as well as new security developments [4]. 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 reidentification and unauthorized monitoring [4]. k-anonymity and its trade-off with differential privacy and computationally intensive blockchain transactional registration used to address privacy and efficiency requirements in vehicular networks [3]. A framework for sharing private data within vehicular ad hoc networks (VANET) using federated learning (FL) and local differential privacy was introduced in [2]. This approach guarantees protection against inference and gradient leakage attacks while providing higher efficiency than conventional FL-based methods. A local differential privacy technique was used to provide a privacy preservation solution for VANET by excluding the need for a third party to anonymize critical information [5]. The disclosure of sensitive data, such as vehicle positions in location services, is considered a potential threat to the privacy of users [7]. k-anonymity method used to maintain location privacy in edge computing (EC) [9], and to preserve location privacy on the Internet of Vehicles (IoV) [8]. To tackle the challenge of designing a secure 6G V2X communication system with EC services, anonymization techniques can be used to protect the identity of the system's users by reducing specific vehicles' information. If the resource allocation system is compromised by malicious agents, the identification of each vehicle is available to the attacker, and this information can be used to escalate the attacks to other elements of the system. It is important to reduce the surface of attack in the infrastructure. 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.

System Description

We consider a 6G V2X communication system that includes sets of vehicles and RSUs as shown in Figure 1. 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. As a case study, we investigate an allocation scenario consisting of 4 RSUs and 32 vehicles.

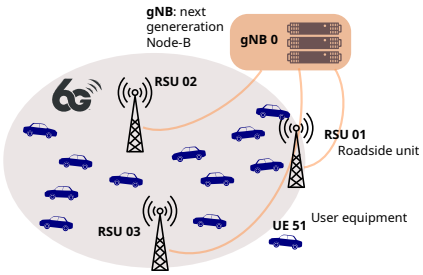

Figure 1: An example of a V2X communication system.

Each vehicle, if assigned to an RSU, will upload its computational tasks to be processed. Vehicle information includes: 1) communication demand, indicated by D_v, in the range 10 – 60 kbits; 2) computation demand, indicated by Φ_v, in the range 100 – 150 cycles/bit; and 3) transmission power, indicated by P_v, in the range 23 – 33 dBm. This information (D_v, Φ_v, P_v) is used to calculate the communication delay, the computation delay, and the energy consumption for centralized allocation [6]. 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 reidentification. 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_v, Φ_v, P_v) is then distributed in the vehicle proximity cluster, and the aggregate measurement is pooled into its average value. Each vehicle, by V2RSU communication, transmits the aggregated triplet values, denoted by $< D_v, \Phi_v, P_v >$ to the RSUs. Similarly, the 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 sharing the same value of $< D_v, \Phi_v, P_v >$. The k-private allocation system receives only the aggregated data from vehicles $< D_v, \Phi_v, P_v >$ and the aggregated SINR from gNB, $<$ SINR $>$.

Results

We compare the k-anonymous V2X allocation model presented in Fig. 1 with the centralized allocation model [6]. The scenarios consider an initial density of 126 RSUs/km^2, and a density of vehicles of 1000 vehicles/km^2. Note that for 190 vehicles not all the original constraints are satisfied, which allows for a reduced energy consumption in the k-anonymous version than in the centralized version.

Allocation	selected/available RSUs	# 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

Conclusions

The current implementation shows how variations in optimal allocations are affected when PET is applied to the V2X system. More advanced techniques, considering the incorporation of online allocation by AI models, will be analyzed in further work.

Acknowledgments

This research was 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 modern research infrastructure of the science sector 2014–2020 financed by the European Regional Development Fund.

References

[1] Mishri AlMarshoud, Mehmet Sabir Kiraz, and Ali H. Al-Bayatti. "Security, Privacy, and Decentralized Trust Management in VANETs: A Review of Current Research and Future Directions". In: *ACM Comput. Surv.* 56.10 (June 2024). ISSN: 0360-0300. DOI: 10.1145/3656166. URL: https://doi.org/10.1145/3656166.

[2] Hajira Batool, Adeel Anjum, Abid Khan, Stefano Izzo, Carlo Mazzocca, and Gwanggil Jeon. "A secure and privacy preserved infrastructure for VANETs based on federated learning with local differential privacy". In: *Information Sciences* 652 (2024), p. 119717. ISSN: 0020-0255. DOI: https://doi.org/10.1016/j.ins.2023.119717. URL: https://www.sciencedirect.com/science/article/pii/S0020025523013026.

[3] Chen Gu, Xuande Cui, Meng Li, and Donghui Hu. "An Efficient and Privacy-Preserving Information Reporting Framework for Traffic Monitoring in Vehicular Networks". In: *IEEE Transactions on Vehicular Technology* 72.6 (2023), pp. 7900–7913. DOI: 10.1109/TVT.2023.3241656.

[4] Mamoona Humayun, Noshina Tariq, Majed Alfayad, Muhammad Zakwan, Ghadah Alwakid, and Mohammed Assiri. "Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey". In: *IEEE Access* 12 (2024), pp. 25469–25490. DOI: 10.1109/ACCESS.2024.3365634.

[5] Zainab Iftikhar, Adeel Anjum, Abid Khan, Munam Ali Shah, and Gwanggil Jeon. "Privacy preservation in the internet of vehicles using local differential privacy and IOTA ledger". In: *Cluster Computing* 26.6 (May 2023), pp. 3361–3377. ISSN: 1573-7543. DOI: 10.1007/s10586-023-04002-0. URL: http://dx.doi.org/10.1007/s10586-023-04002-0.

[6] Faysal Marzuk, Andres Vejar, and Piotr Chołda. "Optimal Resource Allocation for 6G V2X Communication Systems". In: *Przegląd Telekomunikacyjny+ Wiadomości Telekomunikacyjne* (2024).

[7] Zhenle Qi and Wen Chen. "Location Privacy Protection of IoV based on Blockchain and K-anonymity Technology". In: *2023 6th International Conference on Electronics Technology (ICET)*. 2023, pp. 15–21. DOI: 10.1109/ICET58434.2023.10211967.

[8] Bo Wang, Jing Liu, and Laixin Dai. "K-Anonymity-Based Privacy-Preserving and Efficient Location-Based Services for Internet of Vehicles Withstand Viterbi Attack". In: *Proceedings of International Conference on Image, Vision and Intelligent Systems 2022 (ICIVIS 2022)*. Ed. by Peng You, Heng Li, and Zhenxiang Chen. Singapore: Springer Nature Singapore, 2023, pp. 1016–1028. ISBN: 978-981-99-0923-0. DOI: 10.1007/978-981-99-0923-0_101. URL: http://dx.doi.org/10.1007/978-981-99-0923-0_101.

[9] Shiwen Zhang, Biao Hu, Wei Liang, Kuan-Ching Li, and Brij B. Gupta. "A Caching-Based Dual K-Anonymous Location Privacy-Preserving Scheme for Edge Computing". In: *IEEE Internet of Things Journal* 10.11 (2023), pp. 9768–9781. DOI: 10.1109/JIOT.2023.3235707.