IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

Secure Many-To-Many Authentication and Key Agreement Scheme for Vehicular Networks

Mr. Nagaraja G[1], Nama Manasa[2], Poorvika Nagesh B N[3], Preethi G R[4], Priyanka A[5]
Associate Professor, Department of Information Science and Engineering[1]
Student, Department of Information Science and Engineering[2,3,4,5]
S J C Institute of Technology, Chikkaballapur, Karnataka, India

Abstract: *Increase in demand for web and communication technology, vehicles will analyze and choose their all-time knowledge collected by varied cloud service suppliers (CSPs) in a conveyance network. However, in an exceedingly conveyance network atmosphere, period knowledge area units transmitted through wireless channels might result in security and privacy problems. To avoid access for third parties, vehicle authentication, and key agreement mechanism have been considered collectively the promising security measures in conveyance network environments. Besides, most of the solutions concentrate on authentication between one vehicle and one CSP. In such methods, the implementation of economical authentication for several vehicles and CSPs at the same time is typically difficult. Further, they're conjointly subjected to performance limitations because of the overhead incurred. to unravel these problems, we have a tendency to propose a many-to-many authentication and key agreement theme for secure authentication between multiple vehicles and CSPs. The projected theme will forestall unauthorized access and supply SK- security (strong key). To improve the service, the CSP solely has to broadcast associate degree anonymous messages sporadically rather than having to get a singular anonymous message for every vehicle. Similarly, once a vehicle needs to request the services of m CSPs, it solely has to send one request message rather than n. Therefore, the proposed theme not solely implements many-to-many communication however conjointly considerably reduces the computation and communication overhead.*

Keywords: Base station, Registration authority, Cloud service provider, Diffie-hellman key exchange

REFERENCES

[1]. Y. Yu et al., "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 767–778, Apr. 2017.
[2]. L. Zhang, "OTIBAAGKA: A new security tool for cryptographic mixzone establishment in vehicular ad hoc networks," IEEE Trans. Inf. Forensics Security, vol. 12, no. 12, pp. 2998–3010, Dec. 2017.
[3]. Q. Jiang, J. Ni, J. Ma, L. Yang, and X. Shen, "Integrated authentication and key agreement framework for vehicular cloud computing," IEEE Netw., vol. 32, no. 3, pp. 28–35, May 2018.
[4]. J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Edge computing in VANETs—An efficient and privacy-preserving cooperative downloading scheme," IEEE J. Sel. Areas Commun., vol. 38, no. 6, pp. 1191–1204, Jun. 2020.
[5]. R. Yu et al., "Cooperative resource management in cloud-enabled vehicular networks," IEEE Trans. Ind. Electron., vol. 62, no. 12, pp. 7938–7951, Dec. 2015.
[6]. S. Azodolmolky, P. Wieder, and R. Yahyapour, "Cloud computing networking: Challenges and opportunities for innovations," IEEE Commun. Mag., vol. 51, no. 7, pp. 54–62, Jul. 2013.
[7]. J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment," IEEE Trans. Inf. Forensics Security, vol. 15, pp. 1654–1667, 2020.
[8]. J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," IEEE Trans. Dependable Secure Comput., early access, Mar. 11, 2019, doi: 10.1109/TDSC.2019.2904274.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

[9]. V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," IEEE Trans. Inf. Forensics Security, vol. 10, no. 9, pp. 1953–1966, Sep. 2015.

[10]. J. Zhang, H. Zhong, J. Cui, Y. Xu, and L. Liu, "An extensible and effective anonymous batch authentication scheme for smart vehicular networks," IEEE Internet Things J., vol. 7, no. 4, pp. 3462–3473, Apr. 2020.

[11]. J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibanez, "Internet of Vehicles: Architecture, protocols, and security," IEEE Internet Things J., vol. 5, no. 5, pp. 3701–3709, Oct. 2018.

[12]. Z. Ning et al., "A cooperative quality-aware service access system for social Internet of Vehicles," IEEE Internet Things J., vol. 5, no. 4, pp. 2506–2517, Aug. 2018.

[13]. Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm," IEEE Trans. Intell. Transp. Syst., vol. 18, no. 10, pp. 2740–2749, Oct. 2017.

[14]. M. Ma, D. He, H. Wang, N. Kumar, and K.-K.-R. Choo, "An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks," IEEE Internet Things J., vol. 6, no. 5, pp. 8065–8075, Oct. 2019.

[15]. A. I. Croce, G. Musolino, C. Rindone, and A. Vitetta, "Sustainable mobility and energy resources: A quantitative assessment of transport services with electrical vehicles," Renew. Sustain. Energy Rev., vol. 113, Oct. 2019, Art. no. 109236.