





























## 6. CONCLUSION

The Sybil assault is covered in full in this article, and a Hybrid method is typically recommended. When using this strategy, the SDRSU and Unique Tag Algorithms are merged; as the velocity increases, the Unique tag algorithm may be used to come across the Sybil attack, and as the velocity decreases, the SDRSU may be used to detect the Sybil assault. Observations show that the detection fee is much advanced when the hybrid strategy is used, as demonstrated by the results. The proposed method has a significant challenge in that the velocity threshold has not yet been determined, necessitating further inquiry into the characteristics of the streets as a result. A problem is also presented by the algorithm code. Packages made available through VANET can be divided into three categories: security, comfort, and enterprise programs, among others. The adoption of VANET, on the other hand, is a major problem due to its high mobility, ubiquitous hyperlink interruption topology, and a proliferation of security vulnerabilities.

Future studies in VANET should concentrate on more effective and less expensive protection mechanisms in order to keep the network at peace and robust in the future.

## REFERENCES

- [1] H. Hamed, A. Keshavarz-Haddad and S. G. Haghghi, "Sybil Attack Detection in Urban VANETs Based on RSU Support," Iranian Conference on Electrical Engineering (ICEE), Mashhad, 2018, pp.602-606.
- [2] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP — Sybil Attacks Detection in Vehicular Ad Hoc Networks," in IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 582-594, March 2011.
- [3] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, pp. 1103-1114, June 2012.
- [4] Salam Hamdan, Amjad Hudaib & Arafat Awajan (2019): Detecting Sybil attacks in vehicular ad hoc networks, International Journal of Parallel, Emergent and Distributed Systems.
- [5] H. Hamed, A. Keshavarz-Haddad and S. G. Haghghi, "Sybil Attack Detection in Urban VANETs Based on RSU Support," Iranian Conference on Electrical Engineering (ICEE), Mashhad, IEEE, 2018, pp. 602-606.
- [6] F. A. I. W. on Vehicular Ad Hoc Networks (VANET), "Fleetnet: Communication platform for vehicular ad hoc networks," in Zukunftsforum Mobiles Internet 2010, October 2004.
- [7] T. Kosch and M. Strassberger, "The role of new wireless technologies in automotive telematics and active safety," in 8th Symposium Mobile Communications in Transportation, 2004.
- [8] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," in In European Wireless (Euro Wireless), 2002.
- [9] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "Caravan: Providing location privacy for vanet," in Embedded Security in Cars (ESCAR) Workshop, 2005.
- [10] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, 2005.
- [11] G. Calandriello, P. Papadimitratos, A. Liyo, and J.-P. Hubaux, "Efficient and robust pseudonymous authentication in vanet," in ACM International Workshop on Vehicular Inter-Networking (VANET), 2007.
- [12] S. Rass, S. Fuchs, M. Schaffer, and K. Kyamakya, "How to protect privacy in floating car data systems," in ACM International Workshop on Vehicular Inter-Networking (VANET), 2008.
- [13] B. Parno and A. Perrig, "Challenges in securing vehicular networks," Fourth Workshop on Hot Topics in Networks (HotNets-IV), 2005.
- [14] A. Studer, E. Shi, F. Bai, and A. Perrig, "Tacking together efficient authentication, revocation, and privacy in VANETS" in Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2009.
- [15] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in Vanets," in ACM International Workshop on Vehicular Inter-networking (VANET), October 2004.
- [16] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in SASN, Nov 2005.
- [17] Y. Yao et al., "Voiceprint: A Novel Sybil Attack Detection Method Based on RSSI for VANETs," 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), IEEE, Denver, CO, 2017, pp. 591-602.

## Authors Profile



**Mrs Sireesha Kakulla** received her B.Tech from Acharya Nagarjuna University, Andhra Pradesh and M.Tech from JNTUH. She is pursuing her Ph.D from Koneru Lakshmaiah University, Guntur. Her research interests include computer systems and networking, wireless communications, Network security, Data Mining, Software Engineering. She is currently working as Assistant Professor in the CSE Department, Andhra Loyola Institute of Engineering and Technology, Vijayawada.



**Dr. Srinivas Malladi** completed his Ph.D from Koneru Lakshmaiah University in Computer science and Engineering. He has more than 20 years of teaching experience and Published more than 35 Scopus and 5 Web of Science research papers. He also published Book chapters in Springer. Under his guidance 2 were awarded and 7 scholars were pursuing Ph.D. His areas of interests include Software Engineering; Object Oriented Programming Computer Systems and Networking, Wireless Communications, Network security, and Data Mining. He attended and organised more than 50 National and International Conferences in his Research Area. He is currently working as Professor in Koneru Lakshmaiah University, Guntur dist.