













Model as opposed to single sensitive location. The results proves that applying mix zone graph model at multiple sensitive locations as compared to single sensitive location increases the privacy level of the participator. Hence the proposed system provides better results as compared to the existing techniques in terms of increased privacy level and reduced storage space as well as time. In future, mix zone graph model can be applied on multiple sensitive locations of semantic trajectories.

## References

- [1] T. Campbell, S. B. Eisenman, N. D. Lane, E. Miluzzo, and R. A. Peterson, "People-centric urban sensing," in *Proc. 2nd Ann. Int. Workshop on Wireless Internet*, 2006, p. 18, ACM.
- [2] Sheng Gao, Jianfeng Ma, Weisong Shi, Senior Member, IEEE, Guoxing Zhan, and Cong Sun, "TrPF: A Trajectory Privacy-Preserving Framework for Participatory Sensing" *IEEE transactions on Information Forensics and security*, vol. 8, no. 6, June 2013.
- [3] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, "Traffic-aware multiple mix zone placement for protecting location privacy," in *Proc. IEEE INFOCOM*, 2012, pp. 972-980.
- [4] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in *Proc. 3rd Int. Conf. Pervasive Computing (PERVASIVE'05)*, 2005, pp. 152-170.
- [5] H. Lu, C. S. Jensen, and M. L. Yiu, "Pad: Privacy-area aware, dummy based location privacy in mobile services," in *Proc. 7th ACM Int. Workshop on Data Engineering for Wireless and Mobile Access*, 2008, pp. 16-23, ACM.
- [6] M. E. Nergiz, M. Atzori, and Y. Saygin, "Towards trajectory anonymization: A generalization-based approach," in *Proc. ACM SIGSPATIAL ACM GIS 2008 Int. Workshop on Security and Privacy in GIS and LBS*, 2008, pp. 52-61.
- [7] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *Proc. Int. Conf. Pervasive Services*, 2005, pp. 88-97.
- [8] L. Sweeney, "k-anonymity: A model for protecting privacy," *Int. J. Uncertainty Fuzziness and Knowledge Based Syst.*, vol. 10, no. 5, pp. 557-570, 2002.
- [9] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in *Proc. 3rd Int. Conf. Pervasive Computing (PERVASIVE'05)*, 2005, pp. 152-170.
- [10] J. Freudiger, M. H. Manshaei, J. Y. Le Boudec, and J. P. Hubaux, "On the age of pseudonyms in mobile ad hoc networks," in *Proc. IEEE INFOCOM*, 2010, pp. 1-9.
- [11] J. Freudiger, M. Raya, M. Fleglyhzi, P. Papadimitratos, and J. P. Hubaux, "Mix-zones for location privacy in vehicular networks," in *Proc. 1st Int. Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS 07)*, Vancouver, BC, Canada, 2007.
- [12] A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz, "AnonymSense: Opportunistic and privacy-preserving context collection," *Pervasive Comput.*, vol. 5013, pp. 280-297, 2008.
- [13] T. H. You, W. C. Peng, and W. C. Lee, "Protecting moving trajectories with dummies," in *Proc. IEEE Int. Conf. Mobile Data Management*, 2007, pp. 278-282.
- [14] M. Terrovitis and N. Mamoulis, "Privacy preservation in the publication of trajectories," in *Proc. IEEE 9th Int. Conf. Mobile Data Management (MDM'08)*, 2008, pp. 65-72.
- [15] M. E. Nergiz, M. Atzori, and Y. Saygin, "Towards trajectory anonymization: A generalization-based approach," in *Proc. ACM SIGSPATIAL ACM GIS 2008 Int. Workshop on Security and Privacy in GIS and LBS*, 2008, pp. 52-61.
- [16] A. T. Palma, V. Bogorny, B. Kuijpers, and L. O. Alvares, "A clustering-based approach for discovering interesting places in trajectories," in *Proc. 2008 ACM Symp. Applied Computing 2008*, pp. 863-868, ACM.