

Figure 8: Graph showing comparison of Packet Delivery Ratio between existing and proposed system.

• **Control Overhead**

Sending a payload of data (reliably) over a communications network requires sending more than just the desired payload data, itself. It also involves sending various controls and signaling data (TCP) required achieving the reliable transmission of the desired data in question. The control signaling is overhead.

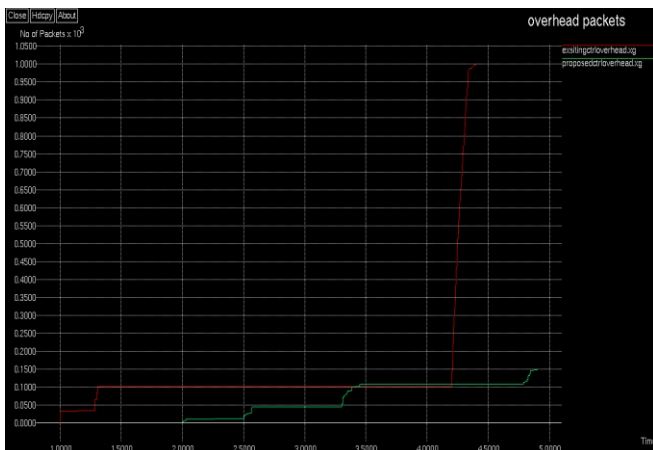


Figure 9: Graph showing comparison of control overhead between existing and proposed system.

6. Conclusion

The data collected from sensor network are correlated, so the direct transmission of data from the sensor node to sink wastes too much energy. So to reduce the number and amount of data transmission, use the data aggregation techniques. Here in This scheme tree based approach is used and also in this scheme slicing and mixing operation is used so security is increased by encrypting the sliced data. And it also provides privacy, confidentiality, authentication, data freshness and accuracy at low communication and computation overhead during data aggregation. Thus it overcomes the energy burden imposed by the hop by hop based privacy preservation protocol on an aggregation node by allowing aggregation on encrypted data.

Besides, future works will also consider the heterogeneous wireless sensor network and also planning to include the integrity checking mechanism into our system. For verifying the correctness of the final aggregated result without

introducing a significant overhead.

References

- [1] Vaibhav Pandey, Amarjeet, Narottam Chand, “A review on data aggregation techniques in wireless sensor network”, Journal of Electronics & Electrical Engineering, ISSN: 0976-8106 & E-ISSN: 0976-8114, Vol.1, Issue 2, 2010, pp-01-08.
- [2] Nadini.S.Patil, Prof. P.R.Patil, “Data Aggregation in wireless sensor network”, IEEE International Conference on Computational Intelligence and Computing Research, 2010, ISBN 97881 8371 3627.
- [3] K. Akkaya and I. Ari. “In-network Data Aggregation in Wireless Sensor Networks”, Handbook of Computer Networks, Ed. H. Bidgoli, John Wiley & Sons, Vol. 2, pp. 1131-1146, 2008.
- [4] Hongjuan Li, Kai Lin, Kequi Li, “Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks”, Computer Communication, 34 (2011); 591-597.
- [5] Kargupta, H.; Datta, Q.W.S.; Sivakumar, K, “On the privacy preserving properties of random data perturbation techniques”, In Proceedings of the IEEE International Conference on Data Mining, Melbourne, FL, USA, November 19–22, 2003; pp. 99–106.
- [6] S. Peter, D. Westhoff, and C. Castelluccia, “A Survey on the Encryption of Convergecast-Traffic with In-Network Processing”, IEEE Transactions on Dependable and Secure Computing, vol. 7, no.1.
- [7] Hassan Cam, Suat Ozdemir, Prashant Nair, Devasenapathy Muthuvinashiappan, H.Ozgun Sanli, “Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks”.
- [8] J.Girao, D.Westhoff, M.Schneider “CDA: Concealed Data Aggregation for reverse multicast traffic in Wireless Sensor Networks”, In proc.40th International Conference on Communications, IEEE ICC, May 2005.
- [9] Domingo-Ferrer J. A provably secure additive and multiplicative privacy homomorphism. In Proceedings of the 5th International Conference on Information Security, Sao Paulo, Brazil, September 30–October 2, 2002; pp. 471–483.
- [10] Castelluccia, C.; Mykletun, E.; Tsudik, G. Efficient aggregation of encrypted data in wireless sensor networks. In Proceedings of the 2nd Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, MobiQuitous, San Diego, CA, USA, July 17–21, 2005; pp. 109–117.
- [11] Chien -Ming Chen, Yue-Hsun Lin, Ya-Ching Lin, Hung-Min Sun, “RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks”. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL 23, NO 4, APRIL 2012.
- [12] Taban, G.; Gligor, V.D. Privacy-preserving integrity-assured data aggregation in sensor networks. In Proceeding of International Symposium on Secure Computing, SecureCom, Vancouver, Canada, August 29–31, 2009; pp. 168–175.

- [13] Agrawal, R.; Kiernan, J.; Srikant, R.; Xu, Y. Order preserving encryption for numeric data. In Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data, Paris, France, June 13–18, 2004, pp. 563–574.
- [14] Chan, H.; Perrig, A.; Song, D. Secure hierarchical in-network aggregation in sensor networks. In Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, October 30–November 3, 2006; pp. 278–287.
- [15] He W, Liu X, Nguyen H, Nahrstedt K, Abdelzaher T, "PDA: Privacy preserving data aggregation in wireless sensor networks". Proceedings of 26th IEEE International Conference on Computer Communications (Infocom 2007), Anchorage, Alaska, USA, May 2007:2045-2053.

