Abstract

The Wireless Sensor Networks (WSNs) are composed of sensor nodes that are deployed in remote and hostile environments to sense, process and communicate vital information to the base station. Due to the stringent constraints on the resources in the sensor nodes, it is essential to optimally devise the WSN operational paradigms, to minimize the resource overhead. Since, communications costs always are significantly higher than that for processing the sensed data the WSNs typically, employ in-network processing, so as to minimize effectively, the total number of packets eventually transmitted to the base station. Such in-network processing is largely based on data aggregation operations that aggregate the data into a compact representation viz. a data aggregate for further transmission. However, due to the ubiquitous and pervasive deployment of the sensor nodes, the security concerns in WSNs are anyway critical. Therefore, it is necessary to ensure the security of the data aggregator nodes that depend on various other nodes for the eventual output using carefully designed approaches. In this paper, we investigate various approaches for data aggregation with a view to critically analyze the same and propose a new approach for secure data aggregation.
References

1. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci. 2002. Wireless sensor networks: a survey. Computer Networks, 38(4):393 – 422, 2002. ISSN 1389-1286. doi: DOI:10.1016/S1389-1286(01)00302-4.
2. Crossbow, mica, wireless measurement system , datasheet. http://www.xbow.com/products/product_pdf_files/wireless_pdf/mica2_data.pdf
3. Ramesh Rajagopalan and Pramod K. Varshney. 2006. Data aggregation techniques in sensor networks: A survey. Comm. Surveys Tutorials, IEEE, 8:48–63.
4. E. Fasolo, M. Rossi, J. Widmer, and M. Zorzi. 2007. In-network aggregation techniques for wireless sensor networks: a survey. IEEE Wireless Communication, 14(2):70–87.
5. Alzaid Hani, Foo Ernest and Nieto Juan Gonzalez. 2008. Secure data aggregation in wireless sensor network: a survey. In: Proceedings of the sixth Australasian conference on Information security (AISC ’08), pages 93–105. Australian Computer Society, Inc., ISBN 978-1-920682-62-0.
6. Einar Mykletun, Joao Girao, and Dirk Westhoff. 2006. Public key based crypto schemes for data concealment in wireless sensor networks. In IEEE International Conference on Communications.
7. S. Peter, D. Westhoff, and C. Castelluccia. 2010. A survey on the encryption of convergecast traffic with in-network processing. IEEE Transactions on Dependable and Secure Computing, 7(1).
8. Kshitija Nandgaonkar, Swarupa Kamble. 2016. A survey on privacy-preserving data aggregation without secure channel. International Research Journal of Engineering and Technology (IRJET), 3(1).
9. D. Westhoff, J. Girao, and M. Acharya. 2006. Concealed data aggregation for reverse multicast traffic in sensor networks: encryption key distribution and routing adaptation. IEEE Trans. Mobile Comput., 5(10):1417–1431.
10. Josep Ferrer and Domingo. 1996. A new privacy homomorphism and applications. Inf. Process. Lett., 60(5):277–282, ISSN 0020-0190.
11. Domingo-Ferrer and Joseph. 2002. A provably secure additive and multiplicative privacy homomorphism. In ISC ’02: Proceedings of the 5th International Conference on Information Security, pages 471–483, London, UK, Springer-Verlag. ISBN 3-540-44270-7.
12. Hongjuan Li, Kai Lin, and Keqiu Li. 2010. Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks. Computer Communications, In Press, Corrected Proof, 2010. ISSN 0140-3664.
13. J. Girao, D. Westhoff, and M. Schneider. 2005. Cda: Concealed data aggregation for reverse multicast traffic in wireless sensor networks. In IEEE Intl Conf. Comm.
14. Claude Castelluccia. 2005. Efficient aggregation of encrypted data in wireless sensor networks. In In MobiQuitous, pages 109–117. IEEE Computer Society.
15. M. Oenen and R. Molva. 2007. Secure data aggregation with multiple encryption. In Proceedings of Fourth European Conference on Wireless Sensor Networks.
16. Xinyang Huang, Ming Yang, and Yong Tong. 2007. An efficient and secure aggregation of encrypted data for wireless sensor network based on dynamic cluster. In SpringSim ’07: Proceedings of the 2007 spring simulation multiconference, pages 51–57, SanDiego, CA, USA, 2007. Society for Computer Simulation International. ISBN 1-56555-312-8.
17. S. Peter, P. Langendo, and K. Piotrowski. 2007. On concealed data aggregation for
wireless sensor networks. In Fourth IEEE Consumer Comm. and Networking Conf. (CCNC).
18. Tatsuaki Okamoto and Shigenori Uchiyama. 1998. A new public-key cryptosystem as secure as factoring. In Eurocrypt ’98, LNCS 1403, pages 308–318. Springer-Verlag.
19. Josh Benaloh Clarkson. 1994. Dense probabilistic encryption. In Proceedings of the Workshop on Selected Areas of Cryptography, 120–128.
20. David Naccache and Jacques Stern. 1998. A new public key cryptosystem based on higher residues. In CCS ’98: Proceedings of the 5th ACM conference on Computer and communications security, pages 59–66, New York, NY, USA. ACM. ISBN 1-58113-007-4. doi: http://doi.acm.org/10.1145/288090.288106.
21. Suat Ozdemir and Yang Xiao. 2009. Hierarchical concealed data aggregation for wireless sensor networks. In Proc. of Embedded Systems and Communications Security Workshop in conjunction with IEEE SRDS 2009.
22. Julia Albath and Sanjay Madria. 2009. Secure hierarchical data aggregation in wireless sensor networks. In Proceedings of the 2009 IEEE conference on Wireless Communications and Networking.
23. Don Johnson, Alfred Menezes and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa).
24. P. Levis, N. Lee, M.Welsh, and D. Culler. 2003. Tossim: accurate and scalable simulation of entire tinynos applications. In SenSys ’03: Proceedings of the 1st international conference on Embedded networked sensor systems. New York, NY, USA: ACM Press, 126–137.

Index Terms

Computer Science Wireless

Keywords

Confidentiality, Integrity, Privacy Homomorphism, Data Aggregation, Secure Data Aggregation.