ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

A Survey on Data Aggregation in Wireless Sensor Network

M.Lalithambigai[1], S. K.Salini [2]

Assistant Professor, Dept. of BCA., Kongunadu Arts & Science College, Coimbatore, India[1]

M.Phil Research Scholar, Kongunadu Arts and Science College, Coimbatore, India[2]

ABSTRACT: A wireless sensor network is a collection of large number of sensor nodes at least one base station. The sensor node is an autonomous small device that consists of mainly four units that are sensing, processing, communication and power supply. These sensors are used to collect the information from the environment and pass it on to base station. The collected data is processed, analyzed and presented to useful application. In wireless sensor network the most challenging task is a life time with help of data aggregation we can enhance the lifetime of the network. In some application such as: wireless sensor network, data mining, cloud computing data aggregation is widely used. In many sensor applications, the data has been collected from the individual nodes and it is aggregated at a base station or host computer. To reduce the energy consumption, many systems also can perform in-network aggregation of sensor data at the intermediate nodes and route to the base station. A challenge to data aggregation is how to secure aggregated data from disclosing during aggregating process as well as obtain accurate aggregated results.

KEYWORDS: Wireless Sensor Network; Data Aggregation; Network life time; Security

I. Introduction

The wireless sensor network is ad-hoc network deployed in physical or environmental condition, and it measured physical parameters such as sound, pressure, temperature, and humidity. It is formed by large number of sensor nodes. Sensor nodes may be homogeneous or heterogeneous. These networks are highly distributed and consist of many number of less cost, less power, less memory and self-organizing sensor nodes. Data Aggregation is an important technique to achieve power efficiency in the sensor network. Data aggregation attempts to collect the most critical data from the sensors and make it available to the sink in an energy efficient manner with minimum data latency. Data aggregation protocols aim to combine and summarize data packets of several sensor nodes so that amount of data transmission is reduced. When the base station queries the network, instead of sending each sensor node's data to base station, one of the sensor nodes called data aggregator, collects the information from its neighboring nodes, aggregates them and sends the aggregated data to the base station improving the bandwidth and energy utilization in the network.

II. LITERATURE SURVEY

Vivaksha Jariwal and Devesh Jinwala [19] they, propose a novel approach for secure data aggregation in wireless sensor networks. In this approach uses homomorphic encryption EC-OU algorithm to attain data confidentiality while allowing in-network aggregation. And also used an additively digital signature algorithm based on Elliptic Curve Digital Signature Algorithm (ECDSA) to achieve integrity of the aggregate. To combining the greatest feature of EC-OU and ECDSA to attain confidentiality and integrity

M. Sardaraz, M. Tahir, and Ataul Aziz Ikram [14] they say that, a secure data aggregation framework (SDAF) for (WSNs). The goal of the framework is to ensure data integrity and data confidentiality. SDAF uses two types of keys. Base station shares a unique key with each sensor node that is used for integrity and the aggregator shares a unique key with each sensor node (within that cluster) that is used for data confidentiality. Sensor nodes calculate a message authentication code (MAC) of the sensed data using shared key with base station, which verifies the MAC for message integrity. Sensor nodes encrypt the sensed data using shared key with aggregator, which ensures data confidentiality. This framework has low communication overhead as the redundant packets are dropped at the aggregators.

Anita A.Gosavi and Sonali U.Nimbhorkar [2] explain that, aggregation using simple averaging method is highly vulnerable to node compromising attacks and through the compromised sensor nodes the attacker can send false data to the aggregator to change the aggregate values. An iterative filtering algorithm is the most effective solution for such purpose. These algorithms simultaneously aggregate data from multiple sources and provide trust estimation of these sources, usually in a form of corresponding weight factors assigned to data provided by each source.

John Major. J, Shajin Prince and Akuluri Rakesh [9] explains, several data aggregation schemes based on privacy homomorphism encryption have been designed and reviewed on wireless sensor networks. Cluster heads can exactly aggregate the cipher texts without decryption; thus, transmission overhead is reduced. Though, the base station only fetches the aggregated result, which origin two problems. First, the usage of aggregation function is obliged. Second, the base station cannot confirm the data integrity and authenticity. In this paper go to overcome the above two drawbacks. In the design, the base station can recover all the sensing data even the data has been aggregated. Besides, the design has been concluded and adopted on both homogeneous and heterogeneous wireless sensor networks.

Mousam Dagar and Shilpa Mahajan [15] describe security requirements in data aggregation that is confidentiality and integrity, ought to be consummated. Specifically, the fundamental security issue is data confidentiality that protects the sensitive transmitted data from passive attacks, such as eavesdropping. Data confidentiality is especially very important in a hostile environment, where the wireless channel is at risk of eavesdropping. Though there are many methods provided by cryptography, the difficult encryption and decryption operations, like modular multiplications of large numbers in public key primarily based cryptosystems, will assign the sensor's power quickly. The other security issue is data integrity that prevents the compromised source nodes or aggregator nodes from considerably altering the final aggregation value. Sensor nodes are easy to be compromised because they lack expensive tampering-resistant hardware, and even that tampering-resistant hardware may not continually be reliable. A compromised node will modify, forge or discard messages.

Ramesh Rajagopalan and Pramod K. Varshney [17] says that ,data aggregation attempts to collect the most critical data from the sensors and make it available to the sink in an energy efficient manner with minimum data latency .Data latency is important in many applications such as environment monitoring where the freshness of data is also an important factor. It is critical to develop energy efficient data aggregation algorithms so that network life time is enhanced. There are several factors which determine the energy efficiency of a sensor network such as network architecture the data aggregation mechanism and the underlying routing protocol.

Suat Ozdemir and Yang Xiao [18] explain that, as the majority of wireless sensor network applications require a certain level of security, it is not possible to sacrifice security for data aggregation. In addition, there is a strong conflict between security and data aggregation protocols. Security protocols require sensor nodes to encrypt and authenticate any sensed data prior to its transmission and prefer data to be decrypted by the base station. On the other hand, data aggregation protocols prefer plain data to implement data aggregation at every intermediate node so that energy efficiency is maximized. Moreover, a data aggregation result in alterations in sensor data and therefore it is a challenging task to provide source and data authentication along with data aggregation. Due to these conflicting goals, data aggregation and security protocols must be designed together so that data aggregation can be performed without sacrificing security.

In many sensor applications, the data has been collected from the individual nodes and it is aggregated at a base station or host computer. To reduce the energy consumption, many systems also can perform in-network aggregation of sensor data at the intermediate nodes enroute to the base station. The most existing aggregation algorithms and systems do not include any provisions for providing security, and consequently these systems are vulnerable to a large variety of attacks. In particular, the compromised nodes can be used to inject the false data that leads to incorrect the aggregates being computed at the base station. Miriyala Markandeyulu, Guttikonda Prashanti [14] discussing the security vulnerabilities of data aggregation for systems, and present a survey of robust and secure aggregation protocols that are resilient to false data injection attacks.

III. CONCLUSION

The wireless sensor networks are usually composed for hundreds or thousands of less expensive, low-powered sensing devices with limited memory, communication resources and computational. These networks offer potentially low-cost solutions for an array of problems in both civilian applications and military including battlefield target tracking, environmental and health care monitoring, wildfire detection, and traffic regulation. Due to the low deployment cost requirement of wireless sensor networks, sensor nodes have simple hardware and severe resource constraints. Hence, it is a challenging task to provide efficient solutions to data gathering problem. Among these constraints ,in designing wireless sensor network protocols ‘‘battery power” is the most limiting factor To reduce the power consumption of wireless sensor networks, several mechanisms are proposed like control packet elimination, radio scheduling, topology control ,and most important one is data aggregation. It helps in minimization of energy consumption, communication overheads and tries to reduce the problem of localized congestion. It allows collecting useful data from the sensor nodes and then transmitting useful data to the end nodes or sink node.

REFERENCES

1. A. Perrig, R. Szewczyk, D. Tygar, V. Wen, D. Culler, “SPINS: security protocols for sensor networks”, Wireless Networks J. (WINE) 2 (5) (2002) 521–534.
2. Anita A.Gosavi and Sonali U.Nimbhorkar “Analysis of Secure Data Aggregation Mechanisms with the Impact of Collusion Attacks in Wireless Sensor Networks” Volume 6, Issue 2, February-2015.
3. B. Krishnamachari, D. Estrin and S. Wicker, “The impact of data aggregation in wireless sensor networks”, in: Proceedings of the 22nd International Conference on Distributed Computing Systems Workshops, 2002, pp. 575–578.
4. C. Intanagonwiwat, D. Estrin, R. Govindan, J. Heidemann, “Impact of network density on data aggregation in wireless sensor networks”, in: Proceedings of the 22nd International Conference on Distributed Computing Systems, 2002, pp. 457–458.
5. C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, F. Silva, “Directed diffusion for wireless sensor networking”, in: IEEE/ACM Transactions on Networking, Vol. 11, 2003, pp. 2–1
6. I.F. Akyildiz, W. Su and Y. Sankarasubramaniam, E. Cayirci, “A survey on sensor networks”, IEEE Commun. Mag. 40 (8) (2002) 102–114.
7. J. Newsome, E. Shi, D. Song, A. Perrig, The Sybil attack in sensor networks: analysis and defenses, in: Proceedings of the Third IEEE/ ACM Information Processing in Sensor Networks (IPSN’04), 2004, pp. 259–268.
8. J. Yick, B. Mukherjee and D. Ghosal, “Wireless sensor network survey”, Comput. Networks 52 (12) (2008) 2292–2330.
9. John Major. J, Shajin Prince and Akuluri Rakesh “Secure Data Aggregation and Data Recovery in Wireless Sensor Networks” Volume-2, Issue-3, February 2013.
10. Jyoti Rajput , Naveen Garg , “A Survey on Secure Data Aggregation in Wireless Sensor Network”, (2014), pp. 407-412
11. K. Akkaya, M. Demirbas and R.S. Aygun, “The Impact of Data Aggregation on the Performance of Wireless Sensor Networks”, Wiley Wireless Commun. Mobile Comput. (WCMC) J. 8 (2008) 171–193
12. M. Ding, X. Cheng and G. Xue, Aggregation tree construction in sensor networks, in: Proceedings of the 58th IEEE Vehicular Technology Conference, Vol. 4, 2003, pp. 2168–2172.
13. M. Sardaraz, M. Tahir, and Ataul Aziz Ikram SDAF: “A Secure Data Aggregation Framework for Wireless Sensor Networks” Vol. 5, No. 5, October 2013
14. Miriyala Markandeyulu and Guttikonda Prashanti , “Secure Reference Based Data Aggregation Protocol for Wireless Sensor Networks”, Vol . 3, 2013, pp. 978-983.
15. Mousam Dagar and Shilpa Mahajan, “Data Aggregation in Wireless Sensor Network: A Survey” ,Vol 3, no 3 (2013), pp. 167-174
16. R. Rajagopalan and P.K. Varshney, “Data aggregation techniques in sensor networks: a survey”, IEEE Commun. Surveys Tutorials 8 (4) (2006).
17. Ramesh Rajagopalan and Pramod K. Varshney, “Data aggregation techniques in sensor networks: A survey”, 2006
18. Suat Ozdemir and Yang Xiao “Secure data aggregation in wireless sensor networks: A comprehensive overview” Computer Networks 53 (2009) 2022–2037.
19. Vivaksha Jariwala and Devesh Jinwala, “A novel approach for secure data aggregation in wireless sensor networks” September, 2010.
20. W. Zhang, Y. Liu, S.K. Das, P. De, “Secure data aggregation in wireless sensor networks: a watermark based authentication supportive approach”, Elsevier Pervasive Mobile Comput. 4 (2008) 658–680.