Journal of Advances in Science and Technology
Vol. 16, Issue No. 1, March-2019, ISSN 2230-9659

A Review on Privacy and Energy-Efficiency Perspective of Wireless Sensor Network's Data Aggregation Techniques

Phakade Shirish Vitthalrao[1]* Dr. C. Ram Singla[2], Dr. Omprakash Rajankar[3]

[1] Ph.D. Student, Sunrise University, Alwar. Rajasthan

[2] Professor, Ph.D. Guide, Sunrise University, Alwar. Rajasthan

[3] Associate Professor, SET's NBN Sinhgad School of Engineering, Pune

Abstract – For sensing and data processing Wireless Sensor Network (WSN) consist of spatially spread minute sensor nodes. They are equipped with limited energy and low memory. During sensing, processing, transmission and reception of sensed data considerable amount of energy is consumed. Resulting in malfunctioning of these sensor nodes. Various data aggregation techniques can be adapted so as to overcome such restrictions and to expand network lifespan. With data gathering, collection and aggregation of significant information is done in an energy efficient way at sink node. Network lifespan can be improved as well as multiple data of same type can also be avoided. In this research, a review with regards to wireless sensor network's energy efficient dependent data aggregation techniques is talked about. Energy-efficiency and privacy perspective of different data aggregation techniques in a wireless sensor networks (WSN) are discussed in depth.

Key Words – Data Aggregation, WSN, Review, Energy Efficiency and Privacy.

- x -

1. INTRODUCTION

To monitor actual environment or current status of equipment, Wireless sensor network which is an ad-hoc network consisting of a huge amount of sensor nodes are used. WSN is deployed increasingly in military, industrial and civilian applications. Sensor nodes organize themselves into a tree topology post deployment with base station as root of operations. Along path of tree topology Sensor nodes gathers different types of information within a fixed time interval sends them to base station (BS) for further processing. Consumption of energy during transmission will effects lifetime of sensor nodes in a network. Therefore, as an influential technique to minimise amount of data transfer methodology of data aggregation has been extensively applied in WSN. To decrease communication overflow and to extend lifetime of network TAG [1] arranges every node into an aggregation tree. But, there is lack of data security with respect to privacy in TAG as malicious node can easily decrypt and access important information of other nodes. Slice-Mix-AggRegaTe (SMART) algorithm [2] was put forth for addressing and resolving this problems. So as to conceal raw information of nodes every node in SMART slices its data into a predefined fixed number of packets and transmits data packets to its neighbor nodes in a network. Moreover, large amount of energy is consumed with slicing technique that leads to a huge number of exchanged messages. PECDA [3] and ESMART [4] were proposed to decrease consumption of energy consumption, with data slicing performed only on leaf nodes, thereby minimizing energy consumption and communication overhead . There is always a presence of many exchanged messages during data slicing process in a large network. With regards to aim of securing and assuring data privacy, further reduction in amount of nodes exchanging their data pieces can thereby decreases energy consumption of a network.

2. LITERATURE REVIEW

The Wireless Sensor Network (WSN) has got much importance these days. With the tracking and monitoring activities become essential, the deployment of sensor networks through wireless medium have also increased. Although sensors are unavoidable in many fields, they got many issues pertaining to energy, routing, security, coverage, delay, architecture etc. The primary responsibility of these tiny nodes is continuously monitor the area of interest according to the protocol design and forwards the gathered data to the sink. The batteries of the sensor nodes are limited one and it is difficult

www.ignited.in

to replace or recharge. During the while a sensor node runs out of its power, the network may get partitioned and the coverage of application area is lost. The nodes in the application environment are capable of self-configuring together and processing the information data [5].

In general the nodes in the network are act as source, sink and router for communicating the information. The information transfers in WSNs are accomplished by means of single hop or multi-hop communication. If the distance between the source and destination is minimum then single hop communication is preferred and vice versa. The different applications of WSNs are includes border surveillance to smart home monitoring. Overhearing, collision and idle listening forms a major part of energy wastage on a network. To address consumption of energy because of idle listening, adaptive/non adaptive duty cycling schemes are introduced. Various transmission power adjustment and collision free protocols are addressed the above said issues. Data collected by nodes in an area of interest was converted to an aggregated [6] form according to application request, for example averaging the temperature and humidity. Procedure of data aggregation involves combination in observed information from different nodes at intermediate level and conveys aggregated information to sink. Since the nodes in the observation field generates certain amount of redundant data in order for ensure the accuracy. To reduce the redundant data transmissions the generated data from different sources can be aggregated and it is done by suitable data aggregation techniques. The cluster head/central coordinator or any intermediate node is allocated to collect the information from other nodes and do the aggregation operation [7], [8].

Large amount of energy consumption is wasted in overhearing, collision and idle listening. concerning energy consumption in regards is because of idle listening, adaptive/non adaptive duty cycling schemes are introduced. Various transmission power adjustment and collision free protocols are addressed the above said issues [9]. Data thus collected by nodes in region of interest was converted to an aggregated form according to application request, for example averaging humidity and temperature. The process of data aggregation involves the combination of observed data from different nodes at intermediate level and conveys the aggregated information to the sink. Since the nodes in the observation field generates certain amount of redundant data in order for ensure the accuracy. To reduce the redundant data transmissions the generated data from different sources can be aggregated and it is done by suitable data aggregation techniques. The cluster head/central coordinator or any intermediate node is allocated to collect the information from other nodes and do the aggregation operation.

In WSNs the in network processing i.e. data aggregation plays a vital role for reducing the unnecessary transmissions. It leads redundancy minimization; reduced collision and enhancing the life time of WSNs. Authors [10] of this paper details the report of Elliptic Curve homomorphic encryption techniquesand clearly noted that performance when the mapping function during the process of decryption. In this paper authors suggested the homomorphic encryption as per Okamoto-Uchiyama technique for caring all entities at an end point information privacy. Further efficiency and practicability of this approach validated using Tmote Sky and iMote 2 network platforms. They proven that the proposed one utilizes lesser energy with better performance compared to the previous schemes. Authors of the paper [11] put forwarded data gathering approach in WSNs using prediction models. It devoid the superfluous information transmissions and minimizes the datatransmission cost. Due to that, the energy required by the nodes is greatly reduced. In order for enhancing the energy efficiency the cluster head nodes in the given area rotated timely. Authors [12] of the paper much concentrated on data aggregation in wireless senor networks. This paper analyses the false data insertion by the nodes along with dissimilar kinds of attacks. In this approach authors suggested the end to end privacy, which detects the attacks earlier by verifying in each and every hop. It reduces the loading effect of sink node. The same implemented on MicaZ and TelosB mote and the outcomes are validated experimentally and simulation. Authors [13] of the paper mainly concerned about the energy consumption in the wireless sensor networks. They developed a cluster based routing protocol intra-balanced LEACH (IBLEACH), which is a extended version of LEACH protocol. In this work they effectively balance the energy utilization of the nodes in the cluster by implementing IBLEACH. The outcomes of this approach evaluated by means of lifetime and energy consumption and the same compared with the existing schemes.

The authors of [14] presented a distinct Power Scheduling (PS) algorithm of distributed nature for continuous monitoring of WSNs. The technique takes benefit of the time scale discrepancy among sensor network re-configuration stages and data transmitting stages. In [15] the authors proposed an EECBSS scheme, which is a cluster based scheduling technique that balances the energy efficiency and network lifetime. It has three phases: Cluster topologies is determined in first phase and CH was selected based on residual levels of energy. In second phase, scheduling algorithm is presented which allocated a TDMA schedule to avoid collision. Third phase, involves model of energy consumption was introduced to highest residual levels of energy internetwork systems. Authors of [16] have proposed an Energy efficient sleep scheduling for cluster based aggregation, which support high rate

www.ignited.in

of data transmission and reduces energy consumption.

The authors of [17] have suggested and implemented an algorithm of High Energy First (HEF) which addresses problems related to predictable outcomes. It had enhanced to be an optimal CH selection algorithm thus prolonging network lifetime. The authors of [18] have introduced a Power Aware (PA) technique to improve network lifetime. The idea was that the every sensor area should be supervised should be monitored relatively by one SN and other SN such that the network is monitored at all-time within their functioning range. The authors of [19] have presented a LSW which is a local wake-up scheduling method and is built on ant colony based scheduling scheme to enhance sensor network lifetime. The algorithm works in two phases: First phase involves finding a set of SNs which provides entire coverage and in second phase finds replacements in SNs exhaust remaining amount of energy in a network.

"The authors of [20] have presented a resilient steady clustering technique (RSCT) which will maintain durability and steadiness to the sensor network by reducing the unnecessary and avoidable cluster head (CH) changes and minimizing clustering and networking overheads. The authors have introduced a new SN that acts as a standby node (SBN) in the cluster. This SBN performs the tasks of CH, whenever the actual CH moves (or dies) from the cluster. Later the CH re-elect the new SBN. This process keeps the network available and serviceable without any interruption" To address the various scheduling issues, the authors of [21] have proposed energy efficient MATSS algorithm which is multi-attribute time-slot scheduling (MATSS). Algorithm of MATSS focus to prolong SN lifetime with prior available time-slot and neighboring condition as per multi-part dynamic routing (MPDR) neighbour conditions. Based on these parameters the SN scheduled as sleep and wakeup mode in every available frame of time. Choosing of SN is done depending on state of neighbor SNs and parameter of energy by distribution data amongst them.

Cluster-based algorithms and Tree-based algorithms are two major topologies utilised by existing data aggregation algorithms.

2.1. Tree-Based Algorithms

Term of "slicing-mixing" and SMART algorithm was primarily put forth by He et al. [22]. Every node is sliced its raw information into some parts and transfer them to nodes without leaf. Each node mix accepted information with self-data and transmit recent aggregated output to its pre-existing node after distribution of data pieces. Lastly every aggregation results is received at base station in a network. But, it becomes compulsory in providing retention of privacy of information that was transferred by nodes with non-leaf types. Because of nodes that are labelled as non-leaf aggregates information of its child nodes to produce combined outcomes. Previous data of non-leaf nodes is avoided in leaking it to remaining nodes. Hence PECDA scheme and ESMART scheme have given respectively by Li et al. [24] and Wang et al. [23]. To resist malicious threats together they had merely done leaf node's data slicing and sent these pieces of information to their nodes in neighbour along pathways securely. Depending on polynomial functions Ozdemir et al. [25] suggested a data aggregation protocol PRDA, Nodes of sensor uses polynomial functions in representing those information and to hide real information it transfers of polynomial function's coefficients to non-leaf nodes. Based on homomorphic encryption in [26] PDKP protocol was suggested by Zhou et al. So as to secure confidentiality of information and for sensing integrity of data it uses symmetric in terms of coding and decoding cryptography-dependent secured privacy MAC's homomorphism and holomorphic. For dynamically selecting amount of data pieces and its sizes that enhances behaviour in slicing of data Hua et al. provided an idea of ASSDA protocol in [27].

2.2. Cluster-Based Algorithm

To decrease energy consumption CPDA scheme in [22] uses protocols of clustering and algebraic characteristics of polynomials. In an algorithm provided by Ozdemir et al. [28] IPHCDA protocol, "an elliptic curve cryptography dependent homomorphic encryption is implimented in achieving hierarchical aggregation of data. Because of end-to-end data aggregation information integrity is guaranteed and by key encryption confidentiality of data is assured. LPDA was suggested in [29]. Cluster head delivers a base value to other nodes before data aggregation, then such nodes primarily takes out base value from their own information, and later adds a random number that is produced by themselves. An aggregation algorithm, which assigns specific encryption keys for every individual node to ensure security of data is handed over by Elhoseny et al. [30]. BinaryString which is produced by elliptical curve encryption algorithm, ID number of these nodes, distance between this node to cluster head and index of transmission is contained by encryption key of a node." Based on cluster privacy-preserving, in [31], Fang et al. had given a model about data aggregation scheme CSDA. It implies slice-assemble technology to get better data privacy and flexibility. As scale of network changes number of pieces will vary too. Various emerging aggregation techniques are provided last few years time. But, to ensure sensory data security existing aggregation techniques exhaust huge energy.

3. CONCLUSION

A comprehensive review on privacy and energy efficiency based data aggregation in a WSN is presented in this paer. As much of energy is exhausted in course of transmitting, processing, and accepting sensed information, data aggregation has resulted significantly. In collecting and aggregating sensed information and eliminating redundancy, data aggregation has played an important role. It helps in decreasing traffic on network and consumption of power, thereby improving network lifespan and its efficiency. In a tree-based aggregation Power Consumption is low throughout data transmission as compared to grid based or cluster aggregation.

REFERENCES

1. S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong (2002), "Tag: A 505 tiny aggregation service for ad-hoc sensor networks," ACM SIGOPS 506 Operating Systems Review, vol. 36, no. SI, pp. 131–146.

2. W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher (2002), "Pda: 508 Privacy-preserving data aggregation in wireless sensor networks," in 509 IEEE INFOCOM 2007-26th IEEE International Conference on Com- 510 puter Communications. IEEE, pp. 2045–2053.

3. T. Wang, X. Qin, Y. Ding, L. Liu, and Y. Luo (2018), "Privacy-preserving 512 and energy-efficient continuous data aggregation algorithm in wireless 513 sensor networks," Wireless Personal Communications, vol. 98, no. 1, pp. 514 665–684.

4. C. Li and Y. Liu (2013), "Esmart: energy-efficient slice-mix-aggregate for 516 wireless sensor network," International Journal of Distributed Sensor 517 Networks, vol. 9, no. 12, p. 134509.

5. Zhu, N., and Vasilakos, A. V.: "A generic framework for energy evaluation on wireless sensor networks", Wireless Networks, vol. 22, no. 4, pp. 1199 – 1220.

6. Esmaeil Rezaei and Safieh Ghasemi (2018), "Energy-Aware Data Aggregation in Wireless Sensor Networks Using Particle Swarm Optimization Algorithm", American Journal of Information Science and Computer Engineering, vol. 4, no. 1, pp. 1 - 6, 2018.

7. Martin Haenggi (2005), "On Distances in Uniformly Random Networks", IEEE Transactions on Information Theory, Vol. 51, No. 10, pp. 3584-3586.

8. IllsooSohn, Jong-Ho Lee, and Sang Hyun Lee (2016), "Low- Energy Adaptive Clustering Hierarchy Using Affinity Propagation for Wireless Sensor Networks", IEEE Communications Letters, vol. 20, no. 3, March 2016, pp. 1-5.

9. Venkataramanan C and Giriraj Kumar SM (2014), "Markov Fuzzy based Mac Protocol for life time maximization of Wireless Sensor Network", International Journal of Computers and Applications, Vol. 36, No.4, pp. 1-7

10. Jie Cui, Lili Shao, Hong Zhong, Yan Xu and Lu Liu (2017), "Data aggregation with end-to-end confidentiality and integrity for large-scale wireless sensor networks," Peer-to-peer Networking and Applications, Springer, pp. 1-16.

11. Adwitiya Sinha and D. K. Lobiyal (2015), "Prediction Models for Energy Efficient Data Aggregation in Wireless Sensor Network," Wireless Personal Communications, Sprin vbger, pp. 1 - 19.

12. Omar Rafik Merad Boudia, Sidi Mohammed Senouci and Mohammed Feham, "Secure and efficient verification for data aggregation in wireless sensor networks," International Journal of Network Management, Aug 2017, pp. 1-17.

13. Ahmed Salim, WalidOsamy and Ahmed M. Khedr (2014), "IBLEACH: intra-balanced LEACH protocol for wireless sensor Networks," Wireless Networks, Springer, pp. 1515 - 1525.

14. C. Jandaeng, W. Suntiamontut, and N. Elz (2011), "PSA: the packet scheduling algorithm for wireless sensor networks," International Journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks, Vol. 3, No. 3, pp. 1–12.

15. E. Srie Vidhya Janani and P. Ganesh Kumar (2015), "Energy Efficient Cluster Based Scheduling Scheme for Wireless Sensor Networks," The Scientific World Journal, Vol. Article ID 185198, 9 pages, https:// doi.org /10.1155 /2015 /185198.

16. S. Jothi and M. Chandrasekaran (2016). "Energy Efficient Sleep-Scheduling for Cluster Based Aggregation in Wireless Sensor Network," Asian Journal of Information Technology, 15: pp. 3718-3724.

17. B.-C.Cheng, H. H. Yeh, and P.H. Hsu (2011), "Schedulability analysis for hard network lifetime wireless sensor networks with high-energy first clustering," IEEE Transactions on Reliability, vol. 60, no. 3, pp. 675 – 688.

www.ignited.in

18. M. Cardei and D. Z. Du (2005), "Improving wireless sensor network lifetime through power aware organization," Wireless Networks, vol. 11, no. 3, pp. 333–340.

19. M. K. Watfa and F. A. Shahla (2009), "Energy efficient scheduling in WMSNs," INFOCOMP Journal of Computer Science, vol. 8, No. 1, pp. 45 – 54.

20. Jain K, Kumar A, Vyas V. (2018), "A resilient steady clustering technique for Sensor Networks," Special Issue Submission: Applications of Evolutionary Computing in Computer Science IJAEC: Volume 11, Issue 2.

21. Palaniappan S, Periasamy P (2017), "Proposed Energy Efficient Multi Attribute Time Slot Scheduling Algorithm for Quality of Service in Wireless Sensor Network," Wireless Pers Commun doi.org/ 10.1007/ 11277- 017-4821

22. W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher (2007), "Pda: Privacy-preserving data aggregation in wireless sensor networks," in IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications. IEEE, 2007, pp. 2045 – 2053.

23. T. Wang, X. Qin, Y. Ding, L. Liu, and Y. Luo (2018), "Privacy-preserving and energy-efficient continuous data aggregation algorithm in wireless sensor networks," Wireless Personal Communications, vol. 98, no. 1, pp. 665 – 684.

24. C. Li and Y. Liu (2013), "Esmart: energy-efficient slice-mix-aggregate for wireless sensor network," International Journal of Distributed Sensor Networks, vol. 9, no. 12, pp. 134-139.

25. S. Ozdemir, M. Peng, and Y. Xiao (2015), "Prda: polynomial regression- based privacy-preserving data aggregation for wireless sensor networks," Wireless communications and mobile computing, vol. 15, no. 4, pp. 615–628.

26. Q. Zhou, G. Yang, and L. He (2014), "An efficient secure data aggregation based on homomorphic primitives in wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 10, no. 1, p. 962925.

27. P. Hua, X. Liu, J. Yu, N. Dang, and X. Zhang (2018), "Energy-efficient adaptive slice-based secure data aggregation scheme in wsn," Procedia Computer Science, vol. 129, pp. 188–193.

28. S. Ozdemir and Y. Xiao (2011), "Integrity protecting hierarchical concealed data aggregation for wireless sensor networks," Computer Networks, vol. 55, no. 8, pp. 1735–1746.

29. K. Zhang, H. Huang, Y. Wang, and R. Wang (2017), "Link-based privacy- preserving data aggregation scheme in wireless sensor networks," in International Conference on Industrial IoT Technologies and Applications. Springer, pp. 119–129.

30. M. Elhoseny, X. Yuan, H. K. El-Minir, and A. M. Riad (2016), "An energy efficient encryption method for secure dynamic wsn," Security and Communication Networks, vol. 9, no. 13, pp. 2024–2031.

31. W. Fang, X. Wen, J. Xu, and J. Zhu (2017), "Csda: a novel cluster-based secure data aggregation scheme for wsns," Cluster Computing, pp. 1–12.

Corresponding Author

Phakade Shirish Vitthalrao*

Ph.D. Student, Sunrise University, Alwar. Rajasthan