A Survey on Conventional and Secure Routing Protocols in Wireless Sensor Networks

A. L. Sreenivasulu and P. Chenna Reddy

Abstract Wireless sensor networks are one of the emerging fields. This has been supported by advanced technologies and smart sensor nodes that are cost-effective and easily deployable. Our survey is concentrated on conventional routing techniques and security routing protocols in WSNs. The review provides the knowledge about different routing protocols in terms of energy efficiency, location awareness, and security. This paper aims to help the researchers entering into the field of wireless sensor networks by providing the complete understanding of the recent developments.

Keywords Sensor nodes · Energy · Security · Wireless sensor networks Routing

1 Introduction

Wireless sensor networks (WSNs) play a crucial role in the communication technology. WSNs contain sensor nodes that are distributed geographically. The utilization of WSNs is extended to the field of resource monitoring [1, 2], structural monitoring [3, 4], environmental monitoring [5–7], health monitoring [8, 9], and animal tracking [10, 11]. The sensor nodes collect the data from the environment and forwards to the base stations. The sensor nodes work with the battery power. Therefore, they work for a limited time. Figure 1 shows the composition of WSNs.

WSNs are composed of major challenges such as to minimize the energy consumption and to increase the node lifetime. The efficient routing mechanisms are

A. L. Sreenivasulu (✉) · P. Chenna Reddy
Department of Computer Science and Engineering, JNTUA,
Anantapuramu, Andhra Pradesh, India
e-mail: intellseenu@gmail.com

P. Chenna Reddy
e-mail: pcreddy1@rediffmail.com

H. S. Saini et al. (eds.), *Innovations in Electronics and Communication Engineering*,
Lecture Notes in Networks and Systems 33,
https://doi.org/10.1007/978-981-10-8204-7_47

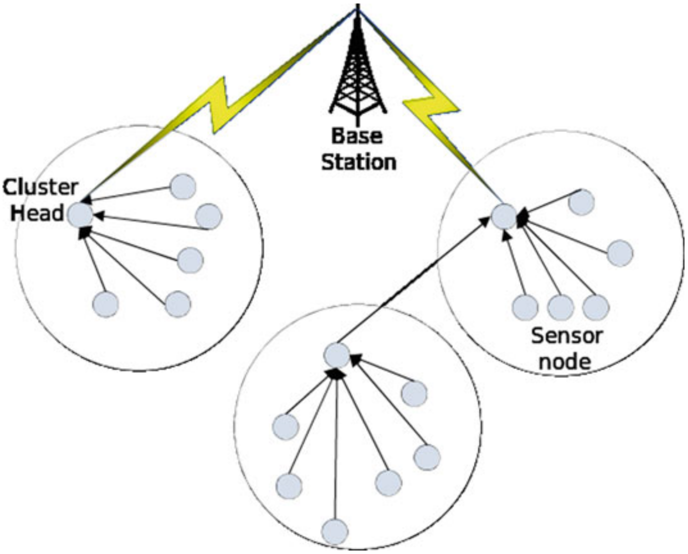

Fig. 1 Organization of wireless sensor network

needed to increase the data accuracy, to decrease the cost, to increase the throughput, and to provide the security in sensor networks.

2 Characteristics of WSNs

At the time of routing, the node properties decide the characteristics of networks which are given below. In [12], the network cost is defined as the organized cost of the path from source to destination. In [13], the clustering coefficient is measured by using the localized connection of the nearer nodes. In [14], the authors define the degree of the node by calculating the direct connections of the source node.

2.1 Energy Efficient Protocols in WSNs

In WSNs, energy management of the nodes is treated as an important issue. In [15], authors proposed the dynamic power management routing protocol to handle the energy management in sensor networks. This protocol automatically turns off the nodes that are in idle state to preserve the battery power. In [16], Jing-hui Zhong made an attempt to increase the lifetime of the network by preserving the energy using the Local Wake-up Scheduling (LWS). A bioinspired approach called as ant colony optimization is used to achieve the energy optimization. In the LWS, the network is divided into two groups. One group is in active mode and another group is in sleep mode. If the nodes in the active group drain their energy, then the nodes automatically go to the sleep state, and the nodes in the other group come alive.

In [17], sleep scheduling algorithm is proposed for multiple target tracking in sensor networks (SSMTT). For every node, the scheduling time is in the dynamic nature, i.e., based on the network condition. If the nodes are in the active state, the sleep time is scheduled, and if the nodes are in the sleep state, the wake-up time is initiated. SSMTT is more useful in conserving the energy of the sensor nodes.

In [18], the authors made a contribution by proposing the medium reservation preamble-based MAC protocol (MRPM). The nodes in the network are contended for the channel allocation within the duration period. When the nodes are in the active state, they contend for the channel; otherwise, they simply ignore the period of contention. The authors also made some modifications by shortening the contention period using the combination of both SYNC and RTS packets.

With the combination of ACO and SSMTT, a better resource allocation protocol is designed by the authors in [19]. This protocol makes the sleep nodes active with less energy consumption. In [20], a low power state routing protocol was designed to schedule the activities to the nodes when they are in active or sleep states. The nodes consume more energy when they need to change the states from sleep to active. It is more than the energy consumed for the packet transfer. Therefore, the nodes having the less energy will be kept in idle state, where they can listen to the packet, but they cannot transfer or receive the packet. The proposed protocol is efficient in covering the sensor region and also the connectivity of the network.

In [21], the TEEM protocol is designed by combining the RTS into a single packet. The TEEM protocol is faster when compared to the S-MAC, and also, it minimizes the energy consumption and maximizes the lifetime of the sensor network. The node listening period is minimized.

In [22], the authors made an attempt to minimize the energy consumption by implementing the ant colony-based AODV (EACAODV) method. The performance of the proposed model is tested with the packet delivery ratio and energy consumption of the network. The results proved that EACAODV is efficient in reducing the network energy.

3 Conventional Routing Protocols in WSNs

The nodes in the sensor network are dedicated to collect the data from the deployed environment and to forward the data to the base station with the help of intermediate nodes. The collected data is forwarded through the access points or gateways to the outer region. The properties of the gateways or access points may be static or dynamic.

The network layer plays a major role in managing the path routing from source to destination. The network layer follows the properties which are as follows:

- Energy management is the threatening issue in the WSNs. Therefore, the energy management protocols are necessary to manage the acquired resources.
- Multi-hop routing is followed by the network layer to establish the connection between source nodes to the base station.
- Data redundancy is another major issue in the WSN, the data duplicates cannot be avoided by the sensor nodes. Therefore, to reduce the data redundancy, suitable protocols need to be designed.

In [23], the authors proposed many protocols by considering the above factors. Among them, some of the protocols are classified as follows:

- Hierarchical routing protocols,
- Data-centric routing protocols, and
- Location-based routing protocols.

3.1 Hierarchical Routing Protocols

These protocols are more popular in preserving the energy of the nodes. It implements the clustering mechanism to organize the group of sensor nodes in the network. The sensor node which is having the more residual energy is selected as the cluster head, and it is responsible for forwarding the data from the source node to the base station.

- Power Efficient Gathering in Sensor Information Systems (PEGSIS) [24]:

The PEGSIS protocol is an energy management protocol where the nearby nodes are used for data exchange and also these nodes will form a chain. The communication establishment between the nodes is done by the traditional algorithms. This PEGSIS has the higher functionality compared to the LEACH. In PEGSIS, there are no policies for selecting the cluster head, energy of the nodes, and location of the nodes. The major drawback for the PEGSIS is data redundancies caused by clustering procedure.

- Power-Aware Clustered TDMA (PACT) [25]:

PACT is one of the efficient hierarchical protocols where the cluster head is selected based on the passive election model. The nodes which have the maximum residual energy are selected as cluster heads. The communication to the base station is established through the source nodes and cluster heads. In AODV routing protocol, the gateways and the cluster head are used to transfer to the data to improve the forwarding efficiency in the MANETs [26].

- Low Energy Adaptive Clustering Hierarchy (LEACH) [27]:

LEACH is one type of adaptive protocol having the highest preference in the hierarchical group. It follows the random selection procedure to elect the cluster head. Later it changes the cluster head over time. The selection of cluster head in the next stages is carried by calculating the distance between the sensor nodes and the cluster head. The major disadvantage of the LEACH is it not suitable for the larger networks and also the network overhead caused by the random selection procedure for cluster head.

- Shortest Hop Routing Tree Protocol [28]:

The shortest path routing protocol works on the principle of collecting only the useful data from the sensor nodes. This will minimize the energy waste in the sensor nodes. The cluster head selection of the proposed routing protocol is based on the highest battery power of the nodes.

- Extending Lifetime of the Cluster Head (ELCH) [29]:

In ELCH protocol, the cluster head selection process is carried by using the voting policy. The cluster head is selected based on the highest polls voted by the sensor nodes. The ELCH Protocol has the self-configurable and hierarchal properties.

- Tree-based Efficient Protocol for Sensor Information [30]:

The tree-based routing protocol adapts the tree structure to transfer the sensed data. In general, there are two methods to construct the tree model. One model is to compute the cost of each path from source node to the base station, and the second one is to find the local algorithm for each sensor node. Here, the local algorithm is implemented using the tree traversal algorithm.

- Threshold Sensitive Energy Efficient (TEEN) [31]:

This protocol has the special properties that can adjust to any unexpected situations in the wireless sensor networks. The major thing in the network is quick response to the critical applications such as environmental disasters. The architecture of the proposed protocol follows the hierarchical routing. The major drawback of the TEEN protocol is it consumes more energy.

3.2 Data-Centric Routing Protocols

Data-centric routing protocols are also referred with query-based routing protocols and it works on the principle of gathering the data by the sensor nodes based on the query processing. The protocols define the set of sensor nodes and process the data aggregation. For connection establishment, data-centric routing protocols follow the on-demand routing.

- Flooding and Gossiping [32]:

Flooding is the mechanism where the sensor nodes gather the data and forward to the nearest nodes until it reaches the sink node. The major drawback of the flooding is it causes collisions, requires more energy, and produces data redundancy. The gossiping is the technique where the sensor nodes gather the data and forward to the random nodes. The major drawback for gossiping is delay.

- Data Diffusion [33, 34]:

Data diffusion is defined as the process of dividing the sensor nodes into groups based on the data generated. When the query is posted in the network, all the nodes gather the data for aggregation process. As a next step, the aggregated data is forwarded to the base station. The base station checks the aggregated data and sends to the neighboring nodes. The nodes verify the received data and collect the data accordingly. The major drawback of this protocol is data redundancy.

- Sensor Protocols for Information via Negotiation [32]:

This protocol is efficient in terms of reducing redundancy and preserving the energy. The protocol predicts that all the nodes in the neighboring region may contain the similar data. Therefore, the protocol compares the aggregated data with received data from the base station. The nodes with low redundant data are selected and forwards to the base station. This protocol is efficient and simpler to implement.

3.3 Location-Based Routing Protocols

In general, WSNs consists of thousands of sensor nodes, and they are not organized with any IP-based addressing scheme. Therefore, to locate the sensor nodes, their location information is considered. The location-based routing protocols use global positioning system (GPS) to collect the location information of the sensor nodes, but this process leads to the energy consumption [35].

- Minimum Energy Communication Network (MECN) [36]:

MECN is the efficient routing mechanism in location-based routing protocols. This protocol discards the weak nodes and reconfigures the network by regrouping. MECN utilizes minimum energy for data forwarding and also it finds the relay nodes in the network to transfer the data instead of direct transmission.

- Small Minimum Energy Communication Network (SMECN) [37]:

SMECN is the advanced version of the MECN, where it contains minimum number of sensor nodes to form the group. SMECN consumes less energy compared to the MECN due to the smaller network, but the network overhead will be high for searching the subnetwork with limited number of sensor nodes.

- Geographic and Energy-Aware Routing (GEAR) [38]:

GEAR is a major routing protocol in WSNs and it is treated as the alternative to the GPS usage in location prediction. The major motive of the proposed protocol is to decrease the energy consumption of the network and increase the network lifetime. The function of the GEAR is to collect the data from the sensor nodes according to the query and sends the data to the particular location where the data is required.

- Geographic Adaptive Fidelity(GAF) [39]:

GAF is practically designed for routing in the MANETs, and then it is extended to use in the WSNs. The basic principle of GAF is to create the virtual grid based on the nodes location information. This protocol utilizes the GPS location of the sensor nodes for cluster formation. GAF preserves the energy of the network by making the idle nodes into inactive state, and also, it increases the lifetime of the sensor nodes. It uses the dynamic resource routing in WSNs.

4 Secure Routing in WSNs

In WSNs, the sensor nodes are deployed in different regions to collect information, and this information is sent to the sink nodes where it can be used by the application [40]. This type of sensor nodes generally gathers the information and transfers to the base station. This type of information gathering in the distributed environment is called as data aggregation and requires aggregation of data from same occurrences. The major motive of data aggregation is to maximize the network lifetime with the help of minimizing the resource utilization of the nodes such as bandwidth, energy consumption, and battery power. To achieve the increment in network lifetime, an efficient routing protocol is necessary. The routing protocols should address the QoS metrics such as fault tolerance, latency, data accuracy, and security.

In the data aggregation process, the design of architecture for WSNs plays a crucial role. There are a number of protocols which provides routing and data aggregation at the same time. These protocols are divided into two types: cluster-based routing protocols and tree-based routing protocols. In [41, 42], the authors made contributions by developing the shortest path tree-based structures. But the disadvantages are not addressing the resource constraints of WSN. In [43], the data aggregation protocol is presented along with the security enhancement. This is because malicious nodes can compromise the data aggregation results.

In WSNs, security is one of the major requirements to protect the nodes from malicious attacks. Some of the characteristics of sensor nodes will compromise the security features when they are deployed in remote environments. The wireless medium is the primary target of the attackers, which is open to everyone. The attackers had the advantage to access the transmitted packets easily by compromising the sensor nodes. The second one is, sensor nodes which are deployed in the WSN environment have limited resources, and therefore it is difficult to implement robust security mechanisms [44–46].

In recent years, some of the secure data aggregation routing protocols are presented. These protocols are not completely sufficient to address the vulnerabilities of the WSN, but they will provide an overview of possible mechanisms for securing data aggregation.

In [47], Jacques et al. proposed the end-to-end encryption mechanism for secure data aggregation which uses the smaller key size and elliptic curve cryptography. This approach restricts the usage of two same texts for the cryptography and also does not allow the usage of a large number of operations over the ciphertext. The major advantage of this encryption scheme is it allows the small asymmetric encrypted keys that are crucial for sensor nodes. The drawback of the end-to-end encryption mechanism is time delay between the packet deliveries which will ultimately affect the network performance.

In [48], Prakash et al. presented the data aggregation model along with privacy-preserving scheme. The approach is simply called as cluster-based private data aggregation. The main feature of this protocol is to preserve the security at the time of data aggregation. This approach will provide less communication overhead over the WSN. The proposed method does not guarantee the fault tolerance, which is a primary concern for secure data aggregation.

In [49] Saut et al. presented the authentication and aggregation model for sensor motes (DAA). This model integrated the functionalities of authentication, data aggregation, and false data detection. The data aggregator node performs the data aggregation and performs data validation with authentication codes for their corresponding nodes. This approach follows the data confidentiality among the nodes by sending the encrypted data. Due to the utilization of encrypted keys, the network overhead is high in this approach.

Roy et al. [50] surveyed the problem of security in WSNs. One compromised sensor node will render the whole network useless and untruthful. They developed secure data aggregation protocols are strong against the intruders and the public key compromises. But the major issue in this protocol is that every time the size of the aggregated data is expanded when it was forwarded to the intermediate nodes.

Othman et al. [51] developed a secure data aggregation protocol to manage the queries over the data collected by the sensor nodes. The proposed protocol is designed especially for securing the computation at the time of data aggregation. However, this protocol manages to provide the data authentication. But still, the data sent from the sensor nodes to the data aggregator is a plaintext. It means the protocol fails to provide security at the time of data transmission.

Rezvani et al. [52] proposed the protocol to address the collusion attacks in WSNs. This protocol follows the iterative filtering algorithm to restrict the unwanted traffic in the network. The proposed protocol is robust against the collusion attacks, but the communication overhead is high in the network. Ouada et al. [53] developed lightweight-based authentication protocol for preserving the energy and providing the security in the wireless sensor networks. This protocol uses identity-based encryption in order to reduce the energy from the public key certificate management. This protocol achieved satisfying results in providing the security. The drawback of this protocol is it concentrates on the energy

Table 1 .

Protocols	Encryption approach	Data confidentiality	Data integrity	Drawbacks
Prakash et al. [48]	End-to-end symmetric	Yes	No	Does not have fault tolerance approach
Jacques et al. [47]	End-to-end symmetric	Yes	Yes	Time delay between the packet deliveries
Suat and Hasan [49]	End-to-end symmetric	Yes	Yes	Network overhead is high
Roy et al. [50]	Hop-to-hop	Yes	Yes	Size of the aggregated data is more
Othman et al. [51]	End-to-end symmetric	Yes	Yes	Lack of security at the time of data transmission
Rezvani et al. [52]	No	Yes	Yes	Communication overhead is high
Ouada et al. [53]	No	Yes	Yes	No encryption mechanism is applied for the data transfer

consumption and the data encryption is not employed to preserve the security. The comparison of secure data aggregation protocols is given in Table 1.

By observing the above-discussed protocols, it can be stated that the behavior of the sensor networks makes the sensor nodes prone to the different type of attacks. Therefore, an efficient data aggregation scheme is necessary to address the data security, energy consumption, data accuracy, and propagation delay.

5 Conclusion

Routing in wireless sensor networks is a new research filed with increasing set of research results with limited flexibility. In this paper, we made a comprehensive survey on conventional routing mechanisms as well as secure routing mechanisms. All the routing mechanisms have the common motive of extending the lifetime of the nodes, while not compromising the security parameters. Overall, the routing mechanisms are classified into three categories such as hierarchical, location-based, and data-centric routing protocols. We highlighted the challenges and future scope of each routing techniques. Although all the routing protocols promising in the sensor networks, still there is need to address many challenges.

References

1. Jiang X, Dawson-Haggerty S, Dutta P, Culler D (2009) Design and implementation of a high-fidelity ac metering network. In: The 8th ACM/IEEE international conference on information processing in sensor networks, San Francisco, California, USA, pp 253–264

2. Kim Y, Schmid T, Charbiwala ZM, Friedman J, Srivastava MB (2008) Nawms: nonintrusive autonomous water monitoring system. In: 6th ACM conference on embedded networked sensor systems, Raleigh, North Carolina, USA, pp 309–322
3. Ceriotti M, Mottola L, Pietro G, Murphy AL, Gun S (2009) Monitoring heritage buildings with wireless sensor networks: the torreaquila deployment. In: ACM/IEEE international conference on information processing in sensor networks, San Francisco, California, USA, pp 277–288
4. Xu N, Rangwala S, Chintalapudi KK, Ganesan D (2004) A wireless sensor network for structural monitoring. In: Conference on embedded networked sensor systems, Baltimore, MD, USA, pp 13–24
5. Beutel J, Gruber S, Hasler A, Lim R, Meier A, Plessl C, Talzi I, Thiele L, Tschudin C, Woehrle M, Yuecel M (2009) Permadaq: a scientific instrument for precision sensing and data recovery in environmental extremes. In: The 8th ACM/IEEE international conference on information processing in sensor networks, San Francisco, USA, pp 265–276
6. Tolle G, Polastre J, Szewczyk R, Culler D, Turner N, Tu K, Burgess S, Dawson T, Buonadonna P, Gay D, Hong W (2005) A macroscope in the redwoods. In: 3rd international conference on embedded networked sensor systems, San Diego, California, USA, pp 51–63
7. Werner-Allen G, Lorincz K, Johnson J, Lees L, Welsh M (2006) Fidelity and yield in a volcano monitoring sensor network. In: The 7th USENIX symposium on operating systems design and implementation, Seattle, Washington, pp 381–396
8. Cerpa A, Elson J, Estrin D, Girod L, Hamilton M, Zhao J (2001) Habitat monitoring: application driver for wireless communications technology. In: 2001 ACM SIGCOMM workshop on data communications
9. Hu W, Bulusu N, Chou CT, Jha S, Taylor A, Tran VN (2009) Design and evaluation of a hybrid sensor network for cane toad monitoring. ACM Transac Sensor Netw 5(1):4:1–4:29
10. Zhang P, Sadler CM, Lyon SA, Martonosi M (2004) Hardware design experiences in zebranet. In: Conference on embedded networked sensor systems, Baltimore, MD, USA, pp 227–238
11. Blough DM, Santi P (2002) Investigating upper bounds on network lifetime extension for cell-based energy conservation techniques in stationary ad hoc networks. In: The 8th international conference on mobile computing and networking, Atlanta, Georgia, US, pp 183–192
12. Kodialam M, Lakshman TV (2000) Minimum interference routing with applications to mpls traffic engineering. In: Nineteenth annual joint conference of the IEEE computer and communications societies, vol 2, pp 884–893. Tel Aviv, Israel, IEEE
13. Watts JD, Strogatz HS (1998) Collective dynamics of small-world networks, Nature © Macmillan Publishers, New York, USA, vol 393, pp 440–442, June 1998
14. Diestel R (2010) Graph theory. Springer-Verlag, Berlin, Heidelberg, Electronic Edition, 4th edn, vol 173
15. Lin C et al (2006) An energy efficient dynamic power management in wireless sensor networks. In: Proceedings of the 5th international symposium on parallel and distributed computing, IEEE 2006
16. Zhong JH, Zhang J (2011) Energy-efficient local wake-up scheduling in wireless sensor networks. In: 2011 IEEE congress on evolutionary computation (CEC), pp 2280–2284, 5–8 June 2011. https://doi.org/10.1109/cec.2011.5949898
17. Jiang B, Ravindran B, Cho H (2008) Energy efficient sleep scheduling in sensor networks for multiple target tracking. In: Distributed computing in sensor systems, lecture notes in computer science, vol 5067, pp 498–509
18. Sthapit P, Pyun JY (2013) Medium reservation based sensor MAC protocol for low latency and high energy efficiency. Telecomm Syst 52:2387–2395. https://doi.org/10.1007/s11235-011-9551-z
19. Fulkar S, Kapgate D (2014) Energy efficient resource allocation in wireless sensor networks. Int J Comput Sci Mob Comput 3(5):887–892, May 2014

20. Parvatkar S, Gore D (2014) Energy efficient protocol for heterogeneous wireless sensor network using ant colony optimization. (IJCSIT) Int J Comput Sci Inf Technol 5(3): 3454–3456
21. Heidemann J, Silva F, Intanagonwiwat C, Govindan R, Estrin D, Ganesan D (2001) Building efficient wireless sensor networks with low-level naming. In: Proceedings of the Symposium on Operating Systems Principles, Lake Louise, Banff, Canada, Oct 2001
22. Luo Z, Zhang Y, Pang Z (2013) Research on energy-efficient intelligent method for WSN. J Convergence Inf Technol (JCIT) 8(1), Jan 2013. https://doi.org/10.4156/jcit.vol8.issue1.12
23. Niculescu D (2005) Communication paradigms for sensor networks. IEEE Comm Mag
24. Lindsey S, Raghavendra CS (2002) PEGASIS: power-efficient gathering in sensor information systems. In: Proceeding of IEEE aerospace conference, vol 3, pp 1125–1130
25. Pei G, Chien C (2001) Low power TDMA in large wireless sensor networks. In: Military communications conference (MILCOM 2001), vol 1, pp 347–351, Vienna, VA, Oct 2001
26. Gerla M, Kwon T, Pei G (2000) On demand routing in large ad hoc wireless networks with passive clustering. In: Proceedings of IEEE WCNC 2000, Chicago, Illinois, Sept 2000
27. Heinzelman WR, Chandrakasan A, Balakrishnan H (2002) An application specific protocol architecture for wireless microsensor networks. IEEE Wireless Comm 1(4):660–670
28. Yang Y, Wu H, Chen H (2006) SHORT: shortest hop routing tree for wireless sensor networks. In: Proceedings of the IEEE international conference on communications, Istanbul, Turkey, pp 3450–3454
29. Lotf J, Bonab M, Khorsandi S (2008) A novel cluster-based routing protocol with extending lifetime for wireless sensor networks. In: Proceedings of the 5th international conference on wireless and optical communications networks, Surabaya, India, pp 1–5
30. Satapathy SS, Sarma N (2006) TREEPSI: tree based energy efficient protocol for sensor information. In: Wireless and optical communications networks 2006, IFIP international conference, pp 11–13, Apr 2006
31. Manjeshwar A, Agrawal DP (2001) TEEN: a routing protocol for enhanced efficiency in wireless sensor networks. In: Parallel and distributed processing symposium (IPDPS'01), San Fransisco, USA, pp 2009–2015
32. Heinzelman W, Kulik J, Balakrishnan H (1999) Adaptive protocols for information dissemination in wireless sensor networks. In: The 5th annual ACM/IEEE international of the first workshop on sensor networks and applications (WSNA). Altlanta, GA, USA
33. Sohrabi K, Gao J, Ailawadhi V, Pottie G (2000) Protocols for self-organization of a wireless sensor network. IEEE Personal Communication 7(5):16–27
34. Su W, Sankarasubramaniam Y, Cayirci E, Akyildiz IF (2002) A survey on sensor networks. IEEE Comm Mag 102–114
35. Gerla M, Kwon T, Pei G (2000) On demand routing in large ad hoc wireless networks with passive clustering. In: Proceedings of IEEE WCNC 2000, Chicago, Illinois, Sept 2000
36. Rodoplu V, Meng TH (1999) Minimum energy mobile wireless networks. IEEE J Sel Areas Commun 17(8):1333–1344
37. Li L, Halpern JY (2001) Minimum-energy mobile wireless networks revisited. Proceedings IEEE ICC'01. Helsinki, Finland, pp 278–283
38. Yu Y, Govindan R, Estrin D (2001) Geographical and energy aware routing: a recursive data dissemination protocol for wireless sensor networks. Technical Report UCLA/CSD-TR-01–0023, UCLA Computer Science Department, May 2001
39. Xu Y, Heidemann J, Estrin D (2001) Geography-informed energy conservation for ad-hoc routing. In: Proceedings ACM/IEEE MobiCom'01, Rome, Italy, pp 70–84, July 2001
40. Peter S, Westhoff D, Castelluccia C (2010) A survey on the encryption of converge cast traffic with in-network processing. IEEE Trans Dependable Secure Comput 7(1):20–34
41. Zheng J, Xu X, Wang G (2011) Energy efficient data aggregation scheduling in wireless sensor networks. In: IEEE 10th international conference on trust, security and privacy in computing and communications, pp 1662–1667
42. Chaudhary S, Singh N, Pathak A (2012) Energy efficient techniques for data aggregation and collection in WSN energy. IJCSEA 2(4):37–47

43. Maraiya K, Kant K, Gupta N (2011) Wireless sensor network: a review on data aggregation. Int J Sci Eng Res 2(4):1–6
44. Sethi H, Prasad D, Patel RB (2012) EIRDA: an energy efficient interest based reliable data aggregation protocol for wireless sensor networks. IJCA 22(7):20–25
45. Nithyakalyani S, SureshKumar S (2012) Optimal clustering algorithm for energy efficient data aggregation in WSN. Eur J Sci Res 78(1):146–155
46. Mathapati BS, Patil SR (2012) A reliable data aggregation forwarding protocol for wireless sensor networks. IJCSNS 12(5):90–95
47. Jacques MB, Christophe G, Abdallah M (2010) Efficient and robust secure aggregation of encrypted data in sensor networks. In: 10th proceeding of the 2010 4th international conference on sensor technologies and applications, (SENSORCOMM), Washington, DC, USA
48. Prakash GL, Thejaswini M, Manjula SH, Venugopal KR, Patnaik LM (2009) Secure data aggregation using clusters in sensor networks: world academy of science. Eng Technol 51:32–35
49. Suat O, Hasan C (2010) Integration of false data detection with data aggregation and confidential transmission in wireless sensor networks. IEEE/ACM Trans Netw 18(3):736–749
50. Roy S, Conti M, Setia S, Jajodia S (2012) Secure data aggregation in wireless sensor networks. IEEE Trans Inf Forensics Secur 7(3):1040–1052
51. Othman SB, Trad A, Youssef H, Alzaid H (2013) Secure data aggregation in wireless sensor networks. In: Ad Hoc networking workshop (MED-HOC-NET), 2013 12th annual mediterranean, pp 55–58. IEEE, 2013
52. Rezvani M, Ignjatovic A, Bertino E, Jha S (2015) Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks. IEEE Trans Dependable Secure Comput 12(1):98–110
53. Ouada FS, Omar M, Bouabdallah A, Tari A (2016) Lightweight identity-based authentication protocol for wireless sensor networks. Int J Inf Comput Secur 8(2):121–138