OPTIMIZED SECURE CLUSTERING FOR DATA EXCHANGE IN WSNS

Ibrahim Alseadoon
College of Computer Science and Engineering, University of Hail, Kingdom of Saudi Arabia
Email: i.alsedon@uoh.edu.sa

ABSTRACT: *Smart technologies are widely applied in the fields of building, health, ecological monitoring, security, smart-home, vehicles, planes, and shipboard. Optimized secure clustering algorithms for wireless sensor networks (WSNs) are the fundamental concerns for smart technologies. Cluster-based WSN has a lot of boons including energy efficiency, less load, better network communication, better scalability, efficient topology management, and minimized delay. Consequently, clustering is a key research area in the WSN. This paper addresses a distributed clustering algorithm with minimum overhead. The algorithm is based on energy, distance, buffering, processing capabilities, and degree parameters for a better WSN performance. The performance measures of the proposed secure clustering algorithm are examined through simulation considering clustering efficiency, consumed energy, network lifetime, and resistance to attacks. The obtained results demonstrate the effectiveness of the proposed clustering algorithm in a constrained environment.*

Keywords: Clustering Algorithm, Cluster Head, Energy, IoTs , Network Lifetime, Wireless Sensor Networks

1. INTRODUCTION

Optimized secure clustering algorithms for wireless sensor networks (WSNs) became widely used due to their miscellaneous applications. The advantages of cluster-based WSN include energy efficiency, less load, better net-work communication, better scalability, efficient topology management, and minimized delay. Hence, clustering became a key research area in the WSN. Due to the importance of clustering in WSNs, there is an urgent need for proper nodes grouping, saving the sensor nodes' energy, and satisfying any operation deadline. At the same time, there is a lack of network security. Therefore, the problem could be summarized as developing a secure, optimized clustering in small and large-scale WSNs. Given a set of sensors S that are deployed randomly or using any structured methods, nodes are deployed in the monitored field. The deployment area (A) could be in any shape, and the environment obstacles (O) are ignored for simplicity. Sensors have a limited communication range (cr_i) and constrained sensing range (sr_i). Nodes are considered connected if the distance (d_{ij}) is less than or equal to the sum of the sensors s_i (cr_i) and s_j communication ranges (cr_j) where d_{ij} is computed as:

$$d_{ij} = \sqrt{(x_i, y_i)^2 + (x_j, y_j)^2} \qquad \forall 1 \leq \{i, j\} \qquad \{i, j\} \leq S$$

where (x_i,y_i) and (x_j,y_j) are the locations of s_i and s_j , respectively. Sensors are assumed to be deployed in unattended areas with some distribution. They collaborate to form a network where each sensor searches for its neighbors to communicate with, as shown in Figure 1. Sensors are assumed to send their sensed data to a sink node (SN). A sink node could be anywhere in the network. For instance, it is assumed that SN in Figure 1 is in the middle of the network.

Using a naive routing algorithm, it can be observed from Figure 1 that sensors will be energy depleted in almost no time due to extra required control messages, long paths, and the dropped messages. Therefore, a proper clustering technique is assumed to minimize the consumed energy per node, where each node will be sending its data to its nearest and efficient cluster head (CH_i). However, the purpose of sensors clustering is important. Many clustering techniques focus only on energy-saving, which is a critical requirement. However, focusing only on energy saving due to the communication will not make a reliable wireless sensor network.

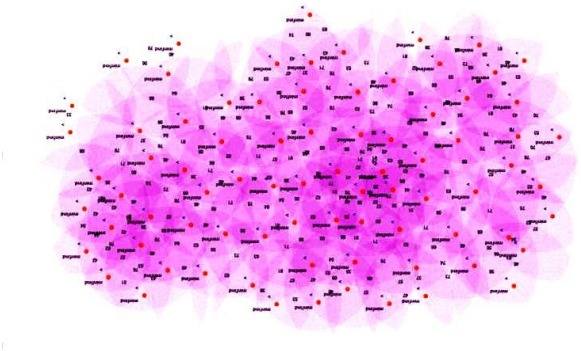

Figure 1. Random deployment to sensor nodes.

In this paper, some parameters other than energy are utilized for better WSN performance. For instance, distance, processor speed, degree, and buffering could be other important parameters to be considered during the clustering process. The distance between a node and its cluster head (CH) is important due to the required communication energy, as it will be explained in the following section. Besides, processing speed and node's buffering are other important parameters due to the deadline of applications. The nodes' degree is another factor to be considered, especially in clustering, which is an indicator of the connectivity of the given node. The proposed clustering method considers those parameters. Also, sensor networks suffer from security where sensors are tiny, and regular cryptography algorithms are not suitable. Intrusion and malware became life-threatening issues in sensor networks. Therefore, considering security during the clustering phase helps network operations to be executed appropriately. Also, due to the frequent change of the WSN structure, it is hard to build a secure WSN. The proposed method evolves security issues during the clustering. That makes the network work efficiently without a threat.

The organization of this paper is as follows. Section 2. provides the state-of-the-art methods, Section 3. hints the energy model, Section 4. illustrates the proposed approach, Section 5. discusses the obtained results, and Section 6. concludes the paper.

2. STATE-OF-THE-ART METHODS

The wireless sensor network (WSN) is comprised of a huge number of small and cheap devices known as sensor nodes. A key issue in WSN is to select a set of sensors to join sensing tasks under some physical resource constraints while achieving a required information accuracy [1, 2]. A system of interconnected devices and sensors with the Internet of Things (IoTs) standards can communicate independently with less or no human inter-action [3]. All sensor nodes have limited power supply and have the capabilities of information sensing, data processing and wireless communication. The sensor nodes communicate together with wireless techniques. These communication techniques are powered by routing protocols. The performance of WSN mainly depends on the application based routing protocols. Based on network structure, routing protocols in WSNs can be roughly classified into flat routing and hierarchical routing. In a flat routing protocol, all nodes do identical tasks and have identical functionalities in the network. Data transmission is done hop by hop normally using the form of flooding. The well-known flat routing protocols include Flooding and Gossiping [4], Sensor Protocols for Information via Negotiation (SPIN) [5], Directed Diffusion (DD) [6], Rumor [7], Greedy Perimeter Stateless Routing (GPSR) [8], Trajectory Based Forwarding (TBF) [9], Energy-Aware Routing (EAR) [10], Gradient-Based Rout-ing (GBR) [11], and Sequential Assignment Routing (SAR) [12]. Flat routing protocols are relatively effective in small scale networks. But it is relatively undesirable in large-scale networks due to resource restriction. In a hierarchical routing topology, nodes do various tasks and usually are organized into lots of clusters based on fixed requirements or metrics. Commonly, each cluster consists of a leader named as CH and other member nodes. The cluster heads can be classified into different hierarchical levels. Nodes with higher energy act as a CH and do the task of data processing and information transmission. But nodes with low energy act as member nodes and do the task of information sensing. The well-known clustering routings protocols include low-energy adaptive clustering hierarchy (LEACH) [13], hybrid energy-efficient distributed clustering (HEED) [14], distributed weight-based energy-efficient hierarchical clustering protocol (DWEHC) [15], position-based aggregator node election protocol (PANEL) [16], two-level hierarchy LEACH (TL-LEACH) [17], unequal clustering size (UCS) model [18], energy-efficient clustering scheme (EECS) [19, 19], energy-efficient uneven clustering (EEUC) algorithm [20], algorithm for cluster establishment (ACE) [21], base-station controlled dynamic clustering protocol (BCDCP) [22], power-efficient gathering in sensor information systems (PEGASIS) [23], threshold sensitive energy-efficient sensor network protocol (TEEN) [24], two-tier data dissemination (TTDD) [25], adaptive threshold sensitive energy-efficient sensor network protocol (APTEEN) [26], concentric clustering scheme (CCS) [27], and hierarchical geographic multicast routing (HGMR) [28].

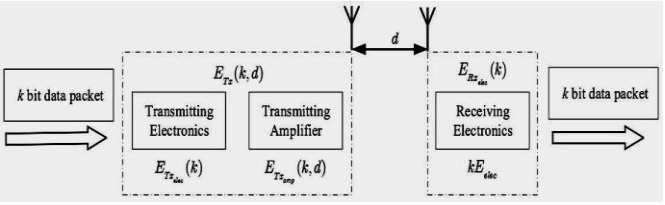

Figure 2. Wireless sensor node energy model [29].

3. ENERGY MODEL

An energy consumption model involved in the interaction is provided in Figure 2 [29] to determine the efficiency of cluster maintenance in WSNs. Remember that this analysis does not include energy wastage in measurement and processing. The communication capacity of nodes in WSNs requires energy consumption in data transmission and receiving, respectively. When sending data, energy consumption requires the energy consumed by the radio frequency transmitter circuit and the signal amplifier circuit. The receiving circuit only requires energy consumption when receiving information. Among them, signal amplifier power consumption can be measured by the free-space path or multi-path fading model according to the distance between the sender and receiver sides. For the free-space path fading model, the path loss exponent is two. It means that the energy loss is proportional to the squared distance. While the path loss exponent for the multipath fading model is four. Suppose the communication channel is symmetrical. If k bit information is transmitted through the distance d system, the $E_{T\,x}$(k; d) transmission energy consumption may be given as follows:

$$E_{Tx}(k,d) = E_{Tx_{map}}(k) + E_{Tx_{map}}(k,d)$$
$$= K\,E_{elec} + K\,\varepsilon_{fs}\,d^{r}$$

where $E_{Txelec(k)}$ and E_{elec} are transceiver k bit energy consumption and single-bit information, respectively. $E_{Txamp}(k,d)$ is the power amplifier energy consumption for k bit information a distance d. The ϵ_{fs} is the power consumption of the amplifier in the free space path fading for each bit of data transmission. R is a wireless channel constant determined by the signal distance d($r = 2$ *if* $d < d_0$, *else* $r = 4$), and d_0 is the transmission distance threshold defined as [29]:

$$d_0 = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}}$$

where ε_{mp} is the power amplifier's energy consumption in the multi-path fading model. The receiving side's energy consumption can be calculated as follows:

$$E_{Rx}(k) = E_{Rx_{elec}}(k) = k\,E_{elec}$$

where $E_{Rx(k)}$ is the wireless receiver circuit's energy consumption for k bit data.

Table 1. Parameters priority.

Parameter	Energy (E)	Distance (D)	Buffering (B)	Processing capabilities (P)	Degree (Ge)
Priority	1	2	3	4	5
Weight	30	10	20	15	25

5. THE PROPOSED APPROACH

In this section, the proposed distributed clustering algorithm with minimum overhead is discussed. The algorithm consists of two phases namely setup and clustering.

4.1 Setup Phase

In this phase, sensors cooperate to know their neighbors by exchanging hello messages, including their IDs, energy level, location information, processing speed, and buffer size. Sensors are assumed to have a GPS location identification feature. Once a node identifies its neighbors, it computes the distance to all of them. A node forms a table with all of its neighbors' parameters for future use. The setup phase costs only one message to be sent from each node. Any node hears from others, will keep track of these messages.

4.2. Clustering Phase

Actual clustering takes place after the setup phase process, where the head of the cluster declares itself in a separate message. Furthermore, there are two methods for construction namely priority-based and weighted-based. Every parameter is given a priority to be considered first in the priority-based approach. Every parameter is given a weight in the weighted-based approach, and the clustering is formed accordingly based on the specified weights.

4.2.1. Priority-Base Clustering

Here, the idea is that each node has a priority to be considered; therefore, a node sorts the parameters according to the given priority. For example, if the nodes' parameters are prioritized as in Table 1, it sorts the given information according to the highest priority parameter first followed by the next highest, and so on.

4.2.2. Weighted-Base Clustering

In this type of clustering, each parameter is given a weight, which represents its importance. It differs from the priority-based clustering in the way that parameters were handled with weights, wherein priority-based all of the parameters have the same weight, and the priority is just an indicator to which parameter to start with. In weighted-base clustering, the weight is an indicator of the priority as well as the value.

According to the previous two methods, nodes sort their collected data, including itself, according to either the priority or the weight. If the node found itself on the top of the sorted list, it announces itself as the CH. The distance will play no role in the CH formation phase since the node has a zero distance to itself. When a neighbor hears a CH, it decides to join or not based on its collected parameters about the announced cluster heads. If a node hears only from a single CH, it joins it; otherwise, it applies the concept of either priority selection or weighted selection. A node in a priority selection sorts the cluster heads parameters according to the given priority. On the other hand, a node may select the CH to join according to the given parameters' weight. In this case, distance plays a major role in the selection of the CH.

4.3. Security Issues

It is important to secure communication between nodes and their CH as well as cluster heads and sink nodes. It is assumed that the sink node can increase its power to reach the farthest CH. Besides, it is assumed that there is no communication between cluster heads. Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. This study proposes to use ECC due to the algorithm signature and its performance. The simplicity of the ECC makes it possible to be used in the clustered networks where every node generates its public and private keys, including the cluster heads and the sink node. One round of broadcasting, the public key of the CH reaches its nodes, and nodes now know each other public key.

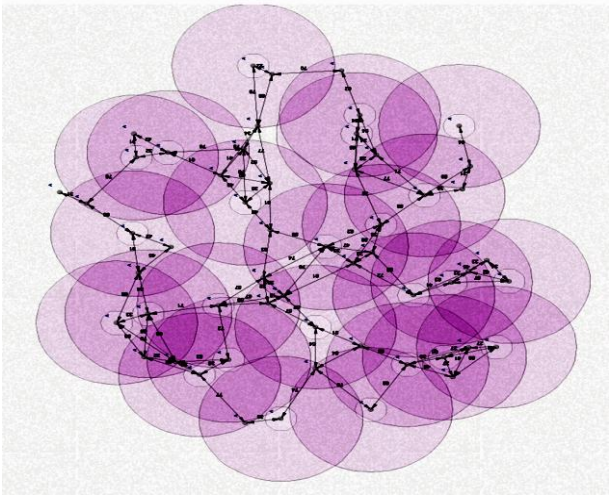

Figure 3. Random deployment of 55 sensor nodes.

4.4. CH Replacement

This occurs in two cases, CH disappears, or its battery goes below a certain threshold. In such cases, nodes within this cluster need to start the clustering process once more. Nodes broadcast their parameters' information, and a qualified CH announces its desire to be a cluster. This broadcasting process is done through a secure channel encrypted using ECC. Therefore, if there is an attacker, it will not be able to know the CH as well as the transmitted messages.

6. RESULT AND DISCUSSION

The performance of the proposed secure clustering approach is measured through four measures namely (i) clustering efficiency, (ii) consumed energy, (iii) network lifetime, and (iv) resistance to attacks. Those measures are examined through simulation. CupCarbon [30] is a simulator for Wireless Sensor Networks (WSNs) and IoTs. It enables to create environments scenarios such as fires, gas, and mobiles. Therefore, it is suitable to test the proposed approach. Besides, it allows the generation of different protocols and modifications using SenScript language.

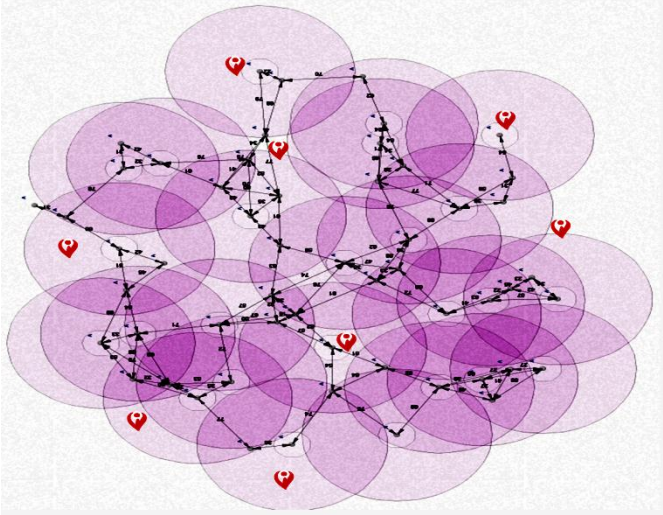

Figure 4. Random deployment of 55 sensor nodes with gas event.

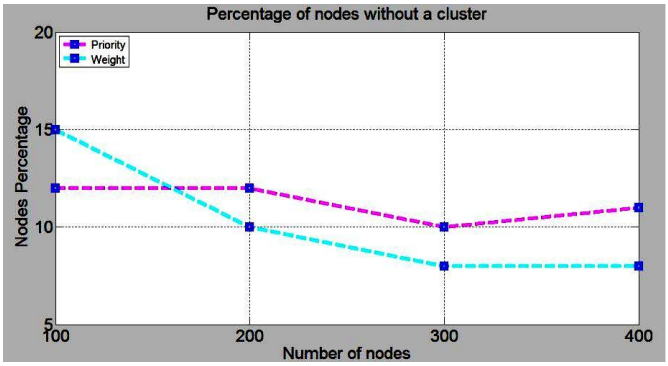

Figure 5. Performance of the clustering algorithms.

7.

The different number of sensors are randomly deployed into an environment of 1000 1000 m with similar and different parameters, including the sensing and communication ranges, and initial energy. The initial deployment sample for 55 nodes is shown in Figure 3, where the connection between the nodes is illustrated. The gas simulation is already embedded in the CupCarbon simulator, which makes the sensor network operation more accurate. Figure 4 demonstrates that 55 nodes with gas events are deployed.

The clustering efficiency is measured based on the number of nodes left without a cluster. Both priority and weight methods are examined with 20 deployment trails with different numbers of sensors 100, 200, 300, and 400.

The average efficiency value is computed and recorded for the 20 trails. Also, the priorities and weights are generated randomly where the priority for each sensor parameter is limited to 5 (1 be the highest), and the sum of the weights has to be 100. As can be seen in Figure 5, the average performance of the performance of both algorithms (priority and weight) is very similar to a large number of deployed sensors. However, the weight algorithms seem not to perform well with a small number of nodes. To examine the lifetime of the deployed network, 200, 300, and 400 nodes are deployed based on weight-based clustering, and the ECC cryptography algorithm is implemented on each node. Each node is assigned with public and private keys at the setup phase, and nodes neighbors' information is collected per neighbor. Besides, the clustering operation is performed, and the CH energy is monitored, and 30% energy threshold is used to change the CH. The gas event is adjusted to generate events every 1ms. The network operated till the first node dies and the lifetime of the network after that. Figure 6 demonstrates the lifetime of the network based on 200, 300, and 400 nodes.

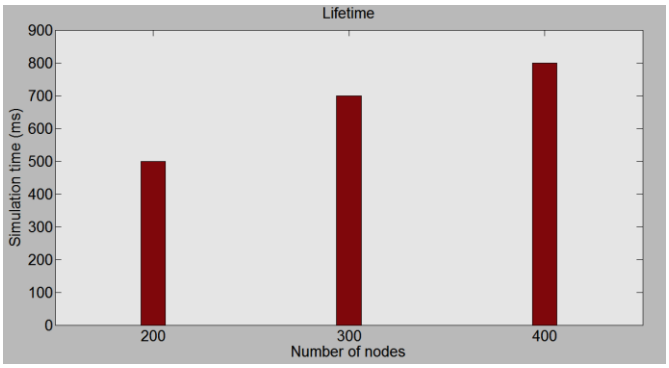

Figure 6. Network lifetime versus a different number of nodes.

6. CONCLUSION

This study proposed a distributed clustering algorithm with minimum overhead. It was based on energy, distance, buffering, processing capabilities, and degree parameters for a better WSN performance. The performance measures of the proposed clustering approach were examined through simulation by considering clustering efficiency, consumed energy, network lifetime, and resistance to attacks. Obtained results showed the effectiveness of the proposed clustering algorithm in a constrained environment.

7. REFERENCES

[1] H. Li, S. Jiang, and G. Wei, "Information-accuracy-aware jointly sensing nodes selection in wireless sensor networks," in Mobile Ad-hoc and Sensor Networks, J. Cao, I. Stojmenovic, X. Jia, and S. K. Das, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 736–747, (2006).

[2] M. H. Sharif, "An eigenvalue approach to detect flows and events in crowd videos," Journal of Circuits, Systems and Computers, vol. 26, no. 7, pp. 1 750 110:1–50, (2017).

[3] M. H. Sharif, I. Despot, and S. Uyaver, "A proof of concept for home automation system with implementation of the internet of things standards," Periodicals of Engineering and Natural Sciences, vol. 6, no. 1, pp. 95-106, (2018).

[4] Z. J. Haas, J. Y. Halpern, and L. Li, "Gossip-based ad hoc routing," in Proceedings of Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3. IEEE, pp. 1707–1716, (2002).

[5] J. Kulik, W. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," Wireless networks, vol. 8, no. 2/3, pp. 169-185, (2002).

[6] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking," IEEE/ACM Transactions on Networking (ToN), vol. 11, no. 1, pp. 2–16, (2003).

[7] D. Braginsky and D. Estrin, "Rumor routing algorthim for sensor networks," in Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications. ACM, pp. 22–31, (2002).

[8] B. Karp and H.-T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in Proceedings of the Annual International Conference on Mobile Computing and Networking. ACM, pp. 243–254, (2000).

[9] D. Niculescu and B. Nath, "Trajectory based forwarding and its applications," in Proceedings of the 9th annual international conference on Mobile computing and networking. ACM, pp. 260–272, (2003).

[10] R. C. Shah and J. M. Rabaey, "Energy aware routing for low energy ad hoc sensor networks," in 2002 IEEE Wireless Communications and Networking Conference Record. WCNC 2002 (Cat. No. 02TH8609), vol. 1. IEEE, 2002, pp. 350–355, (2002).

[11] C. Schurgers and M. B. Srivastava, "Energy efficient routing in wireless sensor networks," in 2001 MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force (Cat. No. 01CH37277), vol. 1. IEEE, pp. 357–361, (2001).

[12] K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie, "Protocols for self-organization of a wireless sensor network," IEEE personal communications, vol. 7, no. 5, pp. 16–27, (2000).

[13] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in Proceedings of the 33rd annual Hawaii international conference on system sciences, (2000).

[14] O. Younis and S. Fahmy, "Heed: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," IEEE Transactions on mobile computing, no. 4, pp. 366–379, (2004).

[15] P. Ding, J. Holliday, and A. Celik, "Distributed energy-efficient hierarchical clustering for wireless sensor networks," in International conference on distributed computing in sensor systems, pp. 322–339, (2005).

[16] L. Buttyan´ and P. Schaffer, "Position-based aggregator node election in wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 6, no. 1, p. 679205, (2010).

[17] V. Loscri, G. Morabito, and S. Marano, "A two-levels hierarchy for low-energy adaptive clustering hierar-chy (tl-leach)," in IEEE vehicular technology conference, vol. 62, no. 3. IEEE; 1999, 2005, p. 1809, (2005).

[18] S. Soro and W. B. Heinzelman, "Prolonging the lifetime of wireless sensor networks via unequal cluster-ing," in 19th IEEE international parallel and distributed processing symposium. (2005).

[19] M. Ye, C. Li, G. Chen, and J. Wu, "Eecs: an energy efficient clustering scheme in wireless sensor networks," in PCCC 2005. 24th IEEE International Performance, Computing, and Communications Conference, 2005. IEEE, pp. 535–540, (2005).

[20] C. Li, M. Ye, G. Chen, and J. Wu, "An energy-efficient unequal clustering mechanism for wireless sensor networks," in IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, (2005).

[21] H. Chan and A. Perrig, "ACE: An emergent algorithm for highly uniform cluster formation," in European workshop on wireless sensor networks. Springer, 2004, pp. 154–171, (2004).

[22] S. D. Muruganathan, D. C. Ma, R. I. Bhasin, and A. O. Fapojuwo, "A centralized energy-efficient routing protocol for wireless sensor networks," IEEE Communications Magazine, vol. 43, no. 3, pp. S8–13, (2005).

[23] S. Lindsey, C. Raghavendra, and K. M. Sivalingam, "Data gathering algorithms in sensor networks using energy metrics," IEEE Transactions on Parallel & Distributed Systems, no. 9, pp. 924–935, (2002).

[24] A. Manjeshwar and D. P. Agrawal, "Teen: Arouting protocol for enhanced efficiency in wireless sensor networks." in ipdps, vol. 1, (2001).

[25] H. Luo, F. Ye, J. Cheng, S. Lu, and L. Zhang, "Ttdd: Two-tier data dissemination in large-scale wireless sensor networks," Wireless networks, vol. 11, no. 1-2, pp. 161–175, (2005).

[26] A. Manjeshwar and D. P. Agrawal, "Apteen: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," in IPDPS, 2002, p. 0195b, (2002).

[27] S.-M. Jung, Y.-J. Han, and T.-M. Chung, "The concentric clustering scheme for efficient energy consump-tion in the pegasis," in The 9th international conference on advanced communication technology, vol. 1. IEEE, 2007, pp. 260–265, (2007).

[28] D. Koutsonikolas, S. M. Das, Y. C. Hu, and I. Stojmenovic, "Hierarchical geographic multicast routing for wireless sensor networks," Wireless networks, vol. 16, no. 2, pp. 449–466, (2010).

[29] B. Li, W. Wang, Q. Yin, H. Li, and R. Yang, "An energy-efficient geographic routing based on cooperative transmission in wireless sensor networks," SCIENCE CHINA Information Sciences, vol. 56, no. 7, pp. 1–10, (2013).

[30] CupCarbon, "CupCarbon U-One 4.1," http://cupcarbon.com/, 2019, [Online; accessed 13-November-2019].