*Journal of Network Intelligence*
**Taiwan Ubiquitous Information**

Volume **6**, Number **4**, November **2021**

# A TSP-over-LEACH Protocol for Energy-Efficient Wireless Sensor Networks

Chaur-Heh Hsieh

Fujian Provincial Key Laboratory of Big Data Mining and Applications, Fujian University of Technology
No.33, Xuefunan Road, University Town, Minhou, Fuzhou, 350118, China
College of Artificial Intelligence, Yango University, Fuzhou, 350015, China
chaoho1204@qq.com

Jianping Lin

College of Artificial Intelligence, Yango University, Fuzhou, 350015, China
jplin@ygu.edu.cn

Chih-Min Yu

College of Artificial Intelligence, Yango University, Fuzhou, 350015, China
hankycm7@gmail.com

Mao-Hsiung Hung*

School of Computer Science and Mathematics, Fujian University of Technology, Fuzhou, 350118, China
Corresponding author: mhhung0502@qq.com

Fenghua Huang

College of Computing and Informatics, University of North Carolina at Charlotte, Charlotte NC28223, USA
fenghuait@sina.com

Received June 2021; revised August 2021

---

Abstract. *Wireless sensor networks (WSNs) play as a way that associates the cybernetic digital world to the actual world. The clustering concept in WSNs can effectively prevent the unnecessary energy consumption in delivering packets to the sink by dividing the network into several groups or clusters. In LEACH protocol, cluster heads (CHs) among different clusters can aggregate sensed data and directly dispatch packets via single-hop transmission to the data sink. Hence, a new challenging issue is generated to reduce the energy consumption for all CHs transmissions since the multi-hop transmission among CHs can effectively reduce the total transmission distance than the direct transmission of CHs in the conventional LEACH. In this paper, a travelling salesman protocol (TSP) over LEACH (TSP-over-LEACH) is proposed based on the existing LEACH to minimize the total transmission distance among CHs and reduces the total power consumption of all CHs. The operation of TSP-over LEACH is divided into two stages. In the first stage, several CHs are determined randomly as the LEACH protocol. In the second stage, a shortest routing path is established for packet transmission along all CHs and the data sink to reduce the total transmission distance. As a result, the TSP-over-LEACH can calculate the minimum hop and distance to achieve the minimization of total energy consumption of all CHs. Simulation results show that the proposed TSP-over-LEACH can effectively reduce total energy consumption as the number of CHs increases especially when the sink node is far away and outside the operation area.*
**Keywords:** Wireless sensor networks, Cluster head, Energy consumption, LEACH, TSP

---

1. **Introduction.** Until now, it is about fifty billion intelligent devices are already connected by 2020 [1]. The number of persons essentially interconnecting may surpass the number of devices or machines virtually connected to them. This will lead enormous traffic volume where people may turn out to be the minority of producers and recipients of traffic volumes [2, 3]. This contributes the motivation for discovering Internet of Things (IoT) for different research regions due to its challenges and chances. Also, wireless sensor networks (WSNs) play as a way that links the cybernetic digital world to the real world. In WSNs, sensors or actuators interconnected with each other can sense and transmit the valuable detected parameters to the Internet. Also, WSNs are comprised sensor nodes that are deployed in a network operation field to supervise numerous physical and ecological factors. To achieve the energy-efficient networking, the routing path of information from the sensed nodes to the base station (BS) or sink node should be well planned since recharging the battery of sensor nodes is realistically impossible [4, 5].

The main objective for WSNs is to forward the accumulated data by each sensor and dispatch it to the BS. The straightforward method is the direct transmission scheme that each sensor nodes can transmit packets directly to the BS or sink node. However, if the communication distance between nodes and the sink is far away, the sensor nodes will run out their battery rapidly due to unnecessary power consumption [6]. The clustering concept in WSNs can effectively prevent the unnecessary energy consumption in delivering packets to the sink by dividing the network into several groups or clusters. Each cluster can be allocated with one or several CHs that disseminates data to the sink. As a result, a vital stage in the clustering scheme is the CH selection procedure that may achieve nearly even energy consumption distribution among the sensor nodes in each cluster [7, 8].

Reducing the power consumption becomes a main intending issue for designing WSNs. Recent research consequences have presented with different ideas to reduce energy consumption, achieve energy balance and thus improve network lifetime for appropriate utilization of energy resource [9-11]. As a result, routing protocols perform a critical role in the development of energy balanced WSNs. With clustering method, a hierarchy of clusters or groups for sensed nodes can be constructed that gathers and forwards the monitoring data to the particular group or cluster heads (CHs). Then, each CH processes the aggregated data and transmits the fused packets to sink node or BS which plays as the middleware between the end user and the WSNs. Among current clustering approaches, low energy adaptive clustering hierarchy (LEACH) is a traditional scheme that considers long term energy balance for hierarchical packet routing [12]. In LEACH, the network can be classified into several organized clusters, and the sensor nodes send their data to the corresponding CH in each cluster. For the system model, LEACH protocol divides the operation into rounds and the approach selects CHs randomly in a dynamically manner for each round. To collect the sensed data, each CH communicates with each sensor node in the associated cluster called member nodes. To efficiently collect sensed data, each CH allocates time division multiple access (TDMA) schedule for its associated cluster members. After obtaining the transmission timeslot, each member node can send packets during the assigned timeslot to avoid radio signal interference. As a result, the TDMA scheduling can efficiently avoid the packets collision among members in a cluster since the mutual interference among members is free. In addition, the gathered data in each CH is then verified for redundancy and compressed before forwarding to the sink node.

In LEACH protocol, CHs can directly transmit packets to BS or data sink. Hence, the power consumption in sending data from CHs to BS will be huge as compared to the communication in each cluster. Therefore, the CHs will deplete their energy more quickly than the member nodes. Multi-hop communication can be one of the solutions to overwhelm this challenging issue for single-hop transmission among CHs. Currently, LEACH has been reworked by researchers to enhance the network lifetime performance. Researchers are promoting energetically in enhancing present schemes for better performance for the IoT applications [13]. For WSN-based IoT, an energy-efficient trust derivation approach is also examined in [14]. The method exploits risk policy analysis to decrease network overhead by getting an optimal number of recommendations and reduces the packet latency of networks. A time-based CH election called TB-LEACH is offered in [15] that groups well-distributed clusters and improves the lifetime by 20% to 30%. Also, the distance between nodes and BS are all investigated for threshold-based CH election that expands lifetime by 10% in [7].

From the above research, the main power consumption part in LEACH protocol is the CH transmission to the data sink since the single-hop communication may be far away from the sink. Also, the energy consumes more as the number of CHs increases. Therefore, a new challenging issue is generated for how to reduce the energy consumption for all CHs transmissions. Currently, the multi-hop transmission among CHs can effectively reduce the total transmission distance than the direct transmission of CHs in the conventional LEACH [5] and [8]. This motivates us to propose a TSP-over-LEACH protocol, and the main contributions of this manuscript are summarized as follows.

1) To reduce the total transmission distance and then save the energy consumption of all CHs, a travelling salesman protocol applied for the existing LEACH called TSP-over-LEACH is proposed to minimize the total transmission distance among CHs.
2) Also, the TSP-over-LEACH can iteratively calculate and determine the minimum hop and distance to achieve the minimization of total energy consumption for the data transmissions among all CHs.
3) Simulation results show that the proposed TSP-over-LEACH can efficiently decrease total energy consumption as the number of CHs increases especially when the sink node is far away and outside the operation area.

## 2. Proposed Methodology.

### 2.1. Network Model.

The fast expansion in population density in metropolitan regions needs up-to-date infrastructures with appropriate provisions to connect the requirements of the city occupants. Thus, modern developments in information technology, such as Internet of Things (IoT) allows in requirement to deliver a framework for the advance of smart cities. The proposed network model presents an ecological supervising scenario that exploits wireless sensor networks (WSNs) as an essential portion of IoT. The sensor nodes are clustered in four diverse areas to construct clusters as shown in Fig.1. Assume that there are eight sensor nodes in each area and only one candidate node can turn out to be the cluster head (CH) with red circle in each operation area. The base station (BS) or sink node can collect data from each CH in each operation round of each area and sends the merged information for the end user in the Internet.

For the network model, several assumptions have been developed as underneath.

1) Each sensor node is static and homogeneous with initial energy 0.5 J and is distributed in different operation areas to supervise the required parameters, such as sound, temperature, humidity, and brilliance.
2) The BS/sink is located at an assigned area and can be fixed in the middle or outside of the network operational area.
3) Sensors deployment are assigned by the uniform random distribution and transmit their data intermittently.

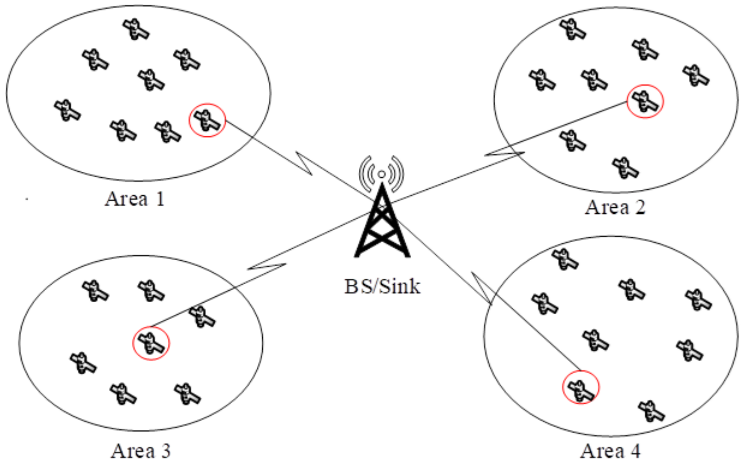


FIGURE 1. An ecological supervising configuration for WSNs

4) Each area can select a CH that communicates with the BS/sink either in the single hop or the multi-hop transmissions.
5) The designated BS/sink collects the information from all CHs and fuses data to the cloud.

To effectively utilize the network energy, the environment supervising applications require the suitable packet routing for sensed data from sensor nodes. When a sensor node with fewer residual energy is elected as CH in one of the areas, the CH will escort to the depletion of packet transmission from the operation area. As this moment, the BS/sink will not receive whole information to monitor the environmental situations. To effectively evaluate the energy consumption of sensor nodes, the radio model used in Equation (1) has been took into account to examine the behavior among all sensors of the proposed network model. Within each area, the free-space model for short distance communication is considered between sensors and CHs. For long distance communication, free-space model or the multipath fading model can be considered between CHs and sink that is dependent on the distance $d_0$. In addition, the symmetrical propagation channel is assumed for both short and long distance communication. To consider the energy consumption of a packet, the relationship of power consumption in transmitting l bits of data and the communication range d meters can be expressed as below.

$$E_{tx}(l,d) = \begin{cases} E_{elec} \times l + E_{fs} \times l \times d^2 & \text{if } d \leq d_0 \\ E_{elec} \times l + E_{mp} \times l \times d^4 & \text{if } d > d_0 \end{cases}, \; E_{rx}(l) = E_{elec} \times l \qquad (1)$$

where $E_{elec}$ is the bit energy consumption by the receiver or transmitter, $E_{fs}$ is for the free-space model, and $E_{mp}$ is the propagation parameter for multipath fading model.

LEACH protocol is an original single-hop clustering configuration that can conserve a massive amount of energy as compared to flat or non-clustering schemes. Once the sensor nodes are adopted, sensors are arranged together to construct clusters for data collection with one nearest CH in each cluster. Also, the LEACH protocol is realized in operation rounds. The clusters are constructed dynamically and the CHs are voted randomly to balance the energy consumption among sensor nodes. Each node in the cluster can have the identical probability or the different weight to be nominated as the CH which aims to make the energy dissipation rate balance. Usually in LEACH, the residual energy in each sensor node is checked persistently by the BS/sink until the lifetime of all sensor nodes are terminated, i.e., from a sensor node run out its energy until all sensor nodes deplete out their battery power.

Let there be $m$ CHs and $n$ sensor nodes in the operational area. In the LEACH scheme, $q$ denotes the probability for a sensor node to act as a CH in an operational round $r$. In the initiation of the first round, each sensor node $i$ can produce a random number between the interval $[0, 1]$. If the number in a sensor node is less than a threshold value $K(n)$ known by Equation (2), then the node will turn out to be a CH for the operation round.

$$K(n) = \begin{cases} \frac{q}{1-q\left[r \bmod (1/q)\right]} & \text{for all } n \in G \\ 0 & \text{otherwise.} \end{cases} \quad (2)$$

In each operation round, the CH alters based on the nominating probability which means that all sensor nodes in each cluster have the same likelihood to be selected as CHs. This in return ensures fair distribution of power in the network and thus enhancing network lifetime.

After all CHs and their associated members are determined in LEACH, the timeslot is assigned by the CH for each node to avoid packet collision and then the packet transmission to CHs can be occurred. In each timeslot, only the transmitting sensor node stays active and all other nodes in the cluster may turn off its radio power to save battery capacity. After all sensor nodes have completed packet transmission in each cluster, each CH will start to handle the collected data. Then, each CH accumulates and examines the information to eliminate any redundancy parts and compress the data as much as possible to achieve the maximum utilization of bandwidth. Finally, all CHs dispatch the data to the BS/sink in either single-hop or multi-hop communications.

2.2. **Proposed Method.** The proposed methodology can be divided into two stages namely random CH selection stage and inter-CHs transmission stage. In CH selection stage, a LEACH based algorithm is exploited to randomly determine the CH candidates. In the inter-CHs transmission stage, the shortest distance routing paths to connect CHs is generated first by the Travelling Salesmen Protocol and each CH forwards its gathered data from sensor nodes to the BS/sink via its neighboring CHs. As a result, the TSP-over-LEACH is presented.

In the random CH selection stage, the sensor nodes are randomly deployed in the network and are grouped into clusters that is responsible by a CH to collect data from sensed nodes. The aggregated data is processed by the CH to decrease the data size by eliminating the unnecessary bits. In the beginning, the clusters and CHs are constructed by using standard LEACH algorithm, where CHs are chosen according to Equation(2).

Once the CHs for each operation round are nominated, each CH sends the CH request information to its member nodes in the corresponding cluster. The sensed nodes check the received signal strength indication of the request message and decide which CHs has the strongest signal strength for joining the cluster. Also, each member replies confirm message to its affiliated CH. Then, the CH broadcasts TDMA slot schedules for the affiliated member nodes to transmit data in different time slots and avoid data collision. The procedure is persisted for the rest of the operation rounds until all nodes deplete all their energy in the network.

During the inter-CHs transmission stage, tangible data routing appears where the gathered data is dispatched to the BS/sink by the CHs in the network. After the selection of CHs, a new routing scheme with travelling salesman protocol is presented to interconnect all CHs together and deliver packets efficiently. Based on the travelling salesman protocol, the total distance among CHs is computed to determine the shortest distance path for packet transmission. The proposed scheme aims at the minimization of the total transmission distance as *dist* by interconnecting all CHs in Equation (3).

$$dist = \min \sum_{i=1}^{m} (d_i) \tag{3}$$

where $m$ is the number of CHs, and $d_i$ is the distance between any CHs. After the TSP-over-LEACH protocol is executed, many paths or trajectories are essential to be planned and determined. The routing path is the sequence of CHs, the order and distances are required to be computed and compared to finally determine the routing paths of CHs as shown in Fig.2. As a result, the total path length should be the shortest path to minimize the transmission distance by the TSP protocol, which results in the minimization of power consumption and delay minimization with the shortest path along the selected CHs and the data sink. The detailed operational flows involved for each operational round in TSP-over-LEACH protocol is presented in the flowchart provided in Fig.3.

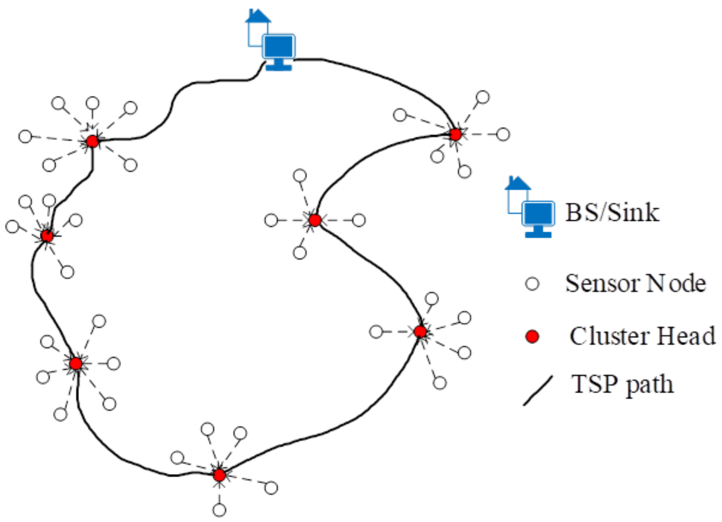


FIGURE 2. The routing path to interconnect all CHs for the TSP-over-LEACH

3. **Simulation results.** Taking into account for a deployment area of 100 × 100 square meters and a uniform random distribution is implemented for the placement of 100 nodes. The BS/sink can be located at the center or outside the operation area. The number of cluster heads is ranging from 5, 10, 15, ..., 50 and the initial energy at each sensor node is 0.5 joules (J). Table I presents the main parameters considered for the packet transmission among CHs. In the LEACH protocol, each CH transmits packets to sink directly. To reduce the energy consumption among inter-CHs communication, the proposed TSP-over-LEACH forwards packets via its nearest neighboring CHs according to the computed routing paths.

With Equation(2), computer program is written in MATLAB to determine the required number of CHs randomly. After the CHs are selected, the affiliated members are determined for each cluster. Then, each CH can merge and forward to the sink via one-hop transmission. Fig.4(a) shows the selected CHs transmissions for a center sink in the LEACH network and Fig.4(b) shows the selected CHs transmissions for a center sink in the TSP-over-LEACH network. In Fig.4(a), ten CHs are generated and they can directly transmit packets to the sink. During transmission in LEACH protocol, the propagation distance will be increased if the CHs are located far from the sink since the CHs are randomly selected for energy balance. In the TSP-over-LEACH network, Fig.4(b)

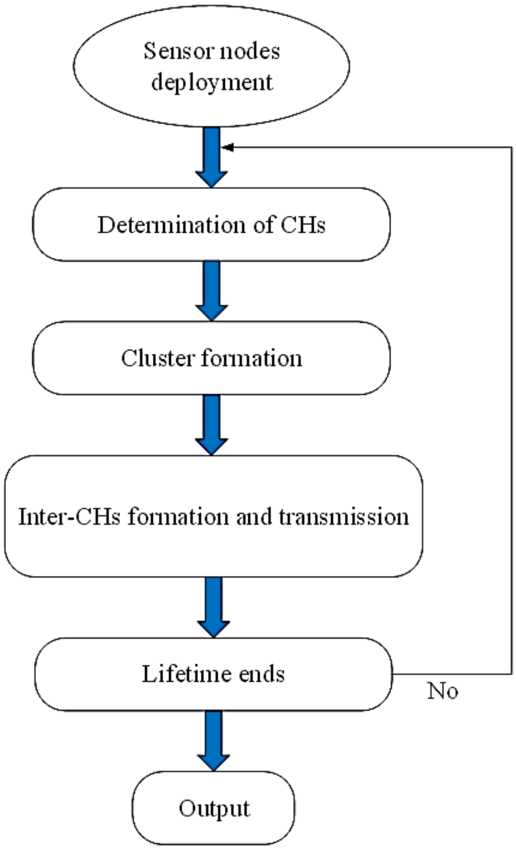


Figure 3. The flows involved in each operational round of TSP-over-LEACH.

Table 1. Simulation parameters

| Simulation parameters | Values |
|---|---|
| Target area | $100 \times 100m^2$ |
| Number of nodes | 100 |
| Position of sink | $(50, 50)$ or $(50, 150)$ |
| Initial energy | 0.5 J |
| $E_{elec}$ | 50 nJ/bit |
| $E_{fs}$ | 10 pJ/bit/$m^2$ |
| $E_{amp}$ | 0.0013 pJ/bit/$m^4$ |
| $E_{DA}$ | 5 nJ/bit |
| Packet size | 4000 bits |
| Number of CHs | $5, 10, 15, ..., 50$ |

interconnects all CHs and the sink into a chain with the minimum total distance for transmitting packets to sink. The packet transmission distance can be reduced than that of LEACH protocol since each CH only needs to propagate packets to its neighboring nodes instead of direct transmission to the sink.

Fig.5(a) shows the selected CHs transmissions for an outside sink in the LEACH network and Fig.5(b) shows the cascade CHs transmissions for an outside sink in the TSP-over-LEACH network. In Fig.5(a), ten CHs are generated and they can directly transmit packets to the sink. During transmission in LEACH protocol, the power consumption will be increased than that of Fig.4(b) since each CH will utilize more propagation distance to reach the data sink. In the TSP-over-LEACH network, Fig.5(b) interconnects all CHs and the sink into a routing chain with the minimum total distance for transmitting packets

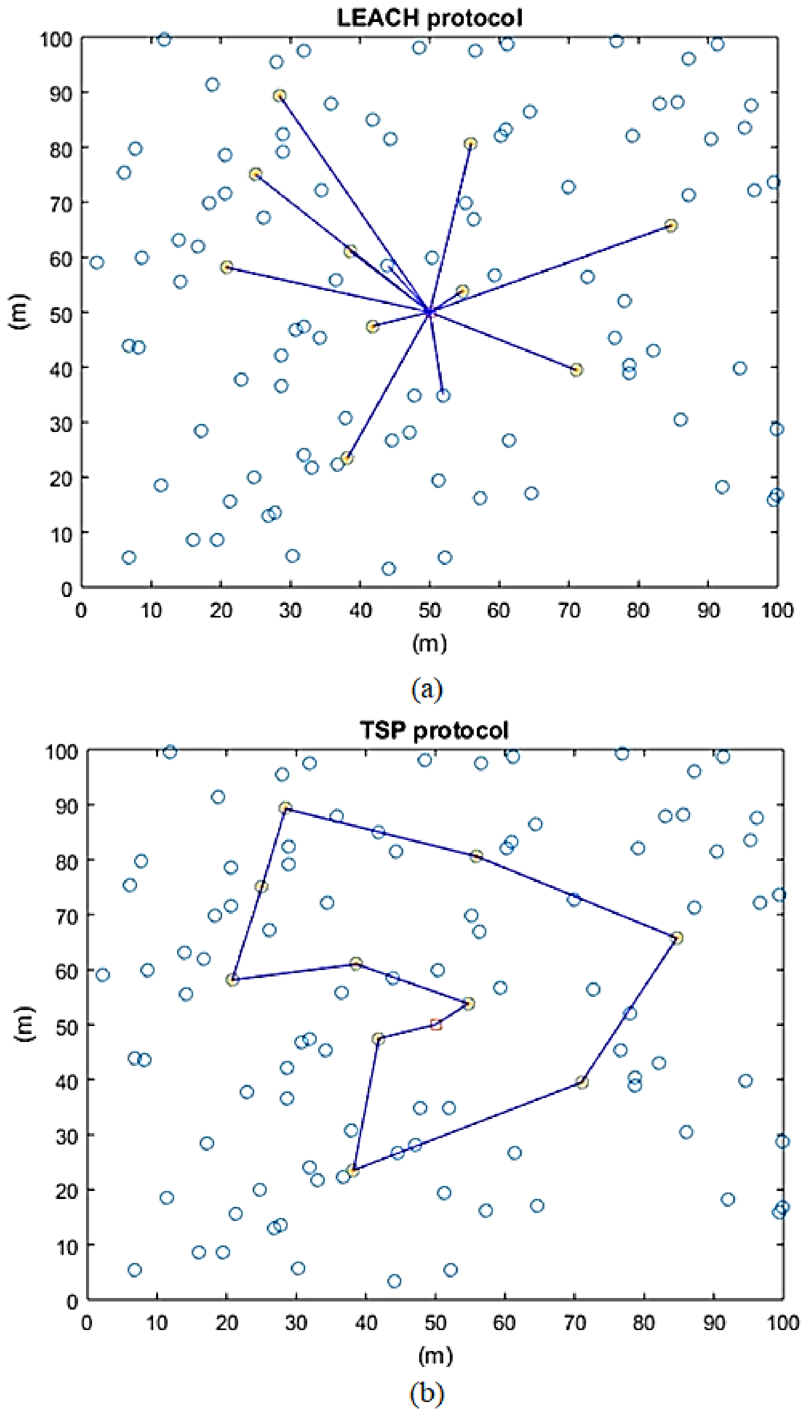


Figure 4. (a) The selected CHs transmissions for a center sink in the LEACH network (b) The cascade CHs transmissions for a center sink in the TSP-over-LEACH network.

to sink. The packet transmission distance can be reduced than LEACH in Fig.5(a) since each CH only needs to propagate packets to its neighboring CH nodes. From the observation in Fig.5(a), only two CHs are required to transmit packets to sink directly instead of 10 CHs in Fig.5(a). As our expectation, the proposed TSP-over-LEACH protocol will save more propagation energy than the conventional LEACH protocol.

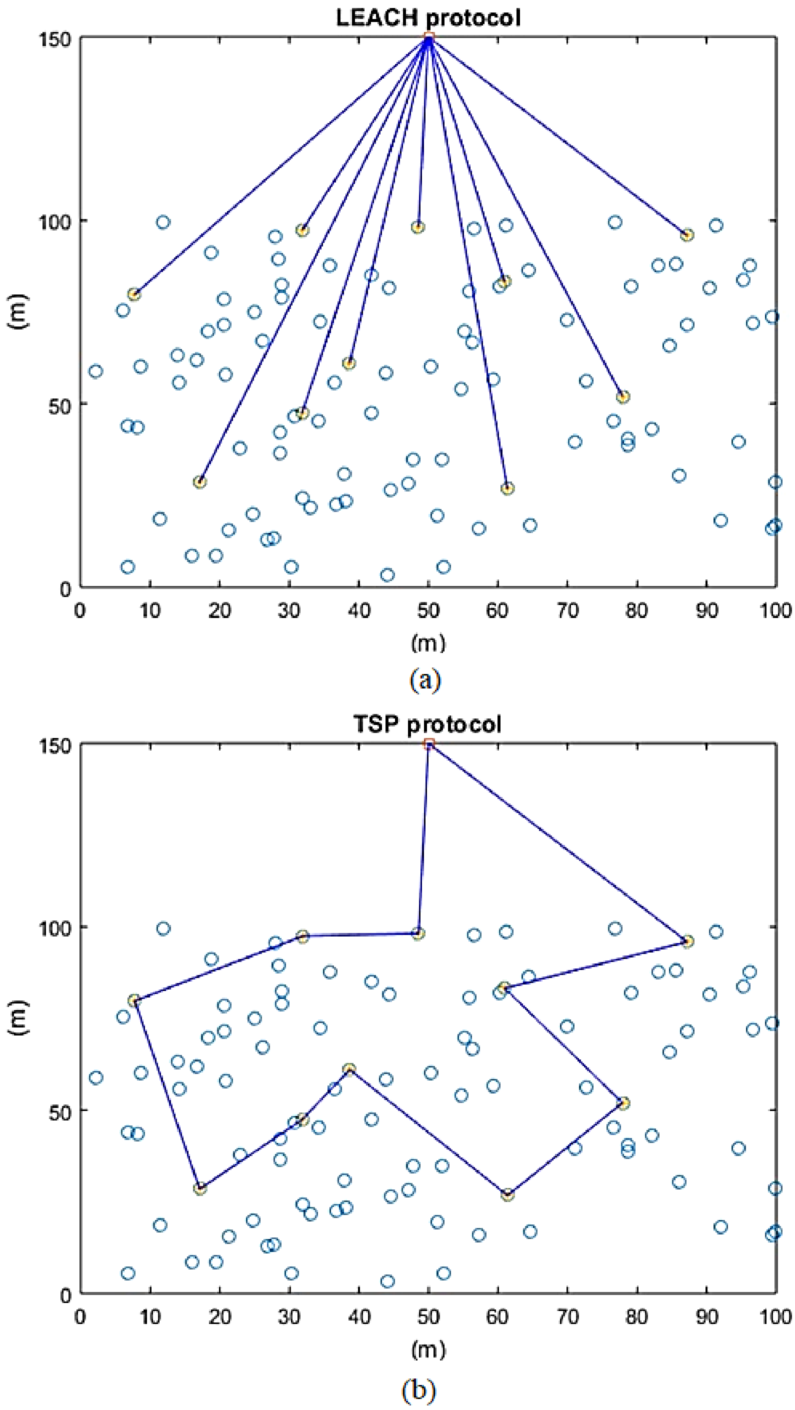


FIGURE 5. (a) The selected CHs transmissions for an outside sink for the LEACH network (b) The cascade CHs transmissions for an outside sink in the TSP-over-LEACH network

With Equation (1), the power consumption of transmission and reception are computed for the LEACH and TSP-over-LEACH protocols respectively. Fig.6(a) exhibits the total energy consumption among CHs to a center sink for both the LEACH and TSP-over-LEACH protocols. The TSP-over-LEACH achieves less energy consumption among CHs than the conventional LEACH since the TSP can effectively reduce the propagation path length in terms of distance than the LEACH protocol. The average energy consumption for the LEACH case is 0.0225 J and the average energy consumption for the TSP-over-LEACH case is about 0.0175 J. As a result, the power consumption of TSP-over-LEACH can be reduced about 22% in average than that of LEACH and the expected network lifetime can be improved for WSNs.

Fig.6(b) exhibits the total energy consumption among CHs to an outside sink in both the LEACH and TSP-over-LEACH protocols. The TSP-over-LEACH significantly reduces energy consumption among CHs than the conventional LEACH since the TSP can effectively reduce the total propagation distance than the conventional LEACH protocol. The average energy consumption for the LEACH case is 0.124 J and the average energy consumption for the TSP-over-LEACH case is about 0.022 J. As a result, the power consumption in WSNs can be significantly reduced about 77% and the TSP can operate better among CHs transmission when the sink location is outside or far away from the operation area.

4. **Conclusions and Future Work.** In this paper, a travelling salesman protocol (TSP) over the LEACH called TSP-over-LEACH is proposed based on the existing LEACH to minimize the total transmission distance among CHs and reduces the total energy consumption of all CHs. The operation of TSP-over LEACH is divided into two stages. In the first stage, several CHs are determined randomly based on the LEACH protocol. In the second stage, a shortest routing path is established among all CHs and the data sink to reduce the total transmission distance. As a result, the TSP-over-LEACH can calculate the minimum hop and distance to achieve the minimization of total energy consumption of all CHs since this is the main part to consume energy in LEACH protocol. Simulation results show that the proposed TSP-over-LEACH can effectively reduce total energy consumption as the number of CHs increases for both the simulation configurations of sink located at the center or outside the network. Also, the power consumption of TSP-over-LEACH can be reduced about 22% and 77% in average than that of LEACH protocol for the location of sink that is at the center or outside the network, respectively. As a result, the proposed TSP-over-LEACH can effectively reduce the total energy consumption among CHs and the expected network lifetime can be improved in WSNs.

In the future, we will consider the security issues of WSN including the three-factor authentication protocols [16-18], the certificate-based aggregate signature [19], the data integrity [20], etc. While the wireless transmission medium of WSNs is vulnerable to network attacks, and the sensor node cannot carry out complex encryption operations due to limited energy supply, thus it is very necessary to design energy-efficient approaches to protect the network security in WSNs.

**Acknowledgment.** Acknowledgment. This work was supported in part by Fujian University of Technology, Granted KF-X18009; and in part by Fujian Province Young and Middle-aged Teacher Education Research Project, Granted JAT200851.

## REFERENCES

[1] J. Chase, The evolution of the internet of things, Texas Instrument. Inc., Dallas, TX, USA, 2013.

[2] D. Bandyopadhyay and J. Sen, Internet of things: Applications and challenges in technology and standardization, *Wireless Personal Communication*, vol. 58, no. 1, pp. 49-69, 2011.

[3] B. Pourghebleh and V. Hayyolalam, A comprehensive and systematic review of the load balancing mechanisms in the internet of things, *Cluster Computing*, vol. 23, pp. 641-661, 2019.

[4] L. Xu, R. Collier, and GMP O'Hare, A survey of clustering techniques in WSNs and consideration of the challenges of applying such to 5G IoT scenarios, *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1229-1249, 2017.

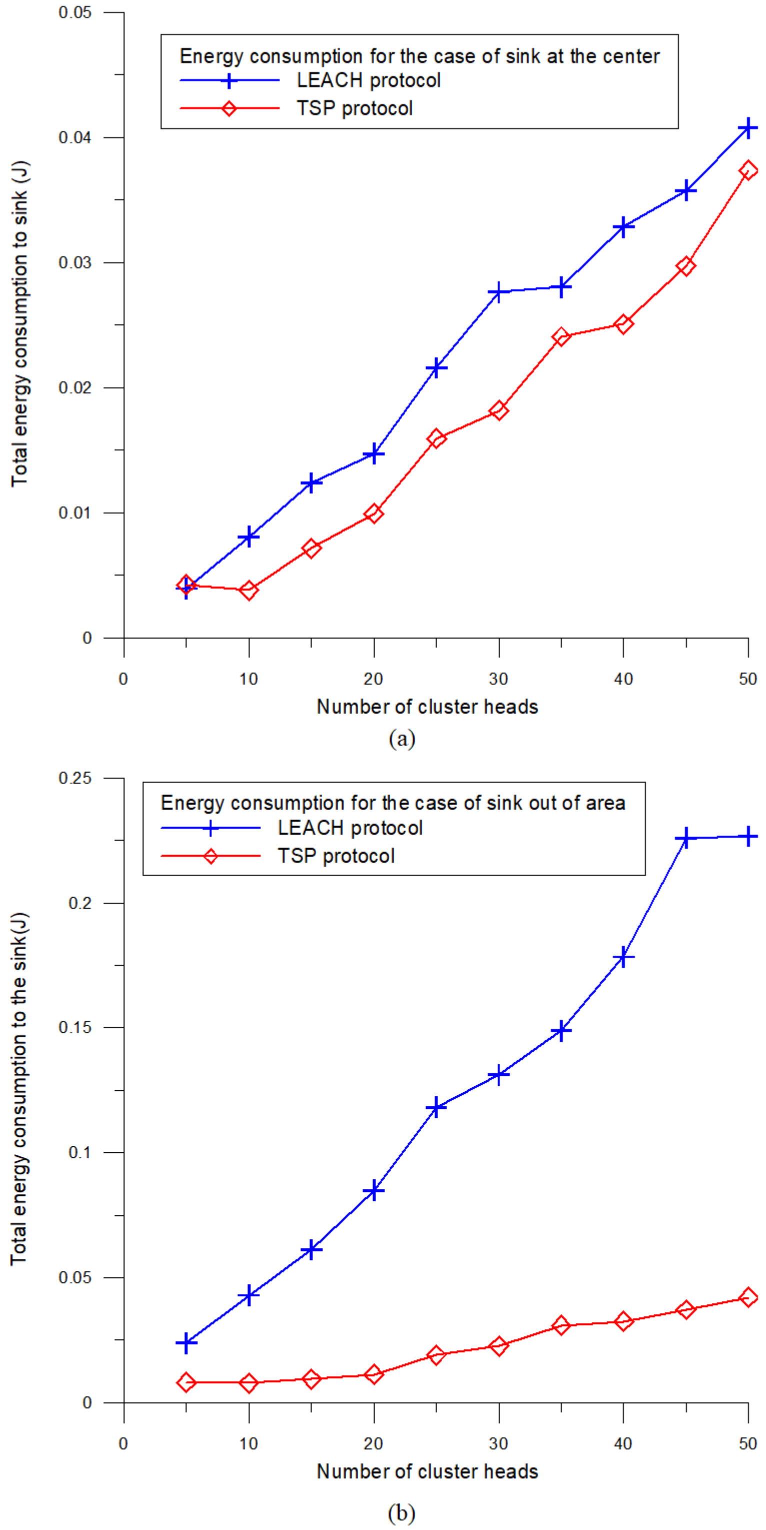


FIGURE 6. (a) The total energy consumption among CHs to a center sink in both the LEACH and TSP-over-LEACH protocols (b) The total energy consumption comparison for an outside sink in both the LEACH and TSP-over-LEACH protocols.

[5] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, An application-specific protocol architecture for wireless microsensor networks, *IEEE Transactions on Wireless Communication*, vol. 1, no. 4, pp. 660-670, 2002.

[6] M. C. M. Thein and T. Thein, An energy efficient cluster-head selection for wireless sensor networks, *International Conference on Intelligence System Model Simulation (ISMS)*, pp. 287-291, 2010.

[7] S. H. Kang and T. Nguyen, Distance based thresholds for cluster head selection in wireless sensor networks, *IEEE Communication Letters*, vol. 16, no. 9, pp. 1396–1399, 2012.

[8] T. M. Behera et al., Residual energy-based cluster-head selection in WSNs for IoT application, *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5132-5139, 2019.

[9] C.-M. Yu, M.-L. Ku, and L.-C. Wang, Joint topology construction and hybrid routing strategy for BLE load balancing networks, *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 7101-7102, 2021.

[10] C.-M. Yu, M.-L. Ku, and L.-C. Wang, BMRHTA: Balanced multi-path routing and hybrid transmission approach for lifecycle maximization in WSNs, *Accepted by IEEE Internet of Things Journal*, 2021, doi: 10.1109/JIOT.2021.3085597.

[11] K. Wang, C.-M. Yu and L.-C. Wang, DORA: A destination oriented routing algorithm for energy-balanced wireless sensor networks, *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 2080-2081, 2021.

[12] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, Energy-efficient communication protocol for wireless microsensor networks, *33rd Annual Hawaii International Conference on System Sciences*, vol. 2, pp. 1-10, 2000.

[13] J. A. Stankovic, Research directions for the internet of things, *IEEE Internet Things Journal*, vol. 1, no. 1, pp. 3–9, 2014.

[14] J. Duan, D. Gao, D. Yang, C. H. Foh, and H.-H. Chen, An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications, *IEEE Internet Things Journal*, vol. 1, no. 1, pp. 58–69, 2014.

[15] H. Junping, J. Yuhui, and D. Liang, A time-based cluster-head selection algorithm for LEACH, *IEEE Symposium. Computers a Communications (ISCC)*, pp. 1172–1176, 2008.

[16] T.-Y. Wu, Y. Lei, Z. Lee, S.-C. Chu, S. Kuari, S. Kumar, A provably secure three-factor authentication Ppotocol for wireless sensor networks, *Wireless Communications and Mobile Computing*, vol. 2021, 5537018, 2021.

[17] K. Renuka, S. Kumar, S. Kumari, C.-M. Chen, Cryptanalysis and improvement of a privacy-preserving three-factor authentication protocol for wireless sensor networks, *Sensors*, vol. 19, no.21, 4625, 2019.

[18] C.-M. Chen, B. Xiang, T.-Y. Wu, K.-H. Wang, An anonymous mutual authenticated key agreement scheme for wearable sensors in wireless body area networks, *Applied Sciences*, vol. 8, no. 7, 1074, 2018.

[19] J.-N. Chen, F. Zou, T.-Y. Wu, Y. Zhou, A new certificate-based aggregate signature scheme for wireless sensor networks, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 9, no. 5, pp. 1264-1280, 2018.

[20] C.-M. Chen, Y.-H. Lin, Y.-C. Lin, H.-M. Sun, RCDA: Recoverable concealed data aggregation for data integrity in wireless sensor networks, *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 4, pp. 727-734, 2011.