Long, Hua

Research routing and MAC based on LEACH and S-MAC for energy efficiency and QoS in wireless sensor network

Research Routing and MAC based on LEACH and S-MAC for Energy efficiency and QoS in Wireless Sensor Network

Hua Long

A thesis submitted to the University of Huddersfield

in partial fulfilment of the requirements for

the degree of Doctor of Philosophy

The University of Huddersfield

October 2013

ABSTRACT

The wireless sensor is a micro-embedded device with weak data processing capability and small storage space. These nodes need to complete complex jobs, including data monitoring, acquisition and conversion, and data processing. Energy efficiency should be considered as one of the important aspects of the Wireless Sensor Network (WSN) throughout architecture and protocol design. At the same time, supporting Quality of Service (QoS) in WSNs is a research field, because the time-sensitive and important information is expected for the transmitting to to the sink node immediately. The thesis is supported by the projects entitled “The information and control system for preventing forest fires”, and “The Erhai information management system”, funded by the Chinese Government. Energy consumption and QoS are two main objectives of the projects. The thesis discusses the two aspects in route and Media Access Control (MAC).

For energy efficiency, the research is based on Low Energy Adaptive Clustering Hierarchy (LEACH) protocol. LEACH is a benchmark clustering routing protocol which imposes upon cluster heads to complete a lot of aggregation and relay of messages to the base-station. However, there are limitations in LEACH. LEACH does not suit a wide area in clustering strategy and multi-hop routing. Moreover, routing protocols only focus on one factor, combining the clustering strategy and multi-hop routing mechanism were not considered in routing protocol for performance of network.

QoS is supported by the MAC and routing protocol. Sensor MAC(S-MAC) makes the use of the periodically monitoring / sleeping mechanism, as well as collision and crosstalk avoidance mechanism. The mechanism reduces energy costs. Meanwhile, it supports good scalability and avoids the collision. However, the protocols do not take the differentiated services. For supporting QoS,A new route protocol needs to be designed and realized on embed platforms, which has WIFI mode and a Linux operation system to apply on the actual system.

This research project was conducted as following the steps: A new protocol called RBLEACH is proposed to solve cluster on a widely scale based on LEACH. The area is divided into a few areas, where LEACH is improved to alter the selecting function in each area. RBLEACH creates routes selected by using a new algorithm to optimize the performance of the network. A new clustering method that has been developed to use several factors is PS-ACO-LEACH. The factors include the residual energy of the cluster head and Euclidean distances between cluster members and a cluster head. It can optimally solve fitness function and maintain a load balance in between the cluster head nodes, a cluster head and the base station. Based on the “Ant Colony” algorithm and transition of probability, a new routing protocol was created by “Pheromone” to find the optimal path of cluster heads to the base station. This protocol can reduce energy consumption of cluster heads and unbalanced energy consumption. Simulations prove that the improved protocol can enhance the performance of the network, including lifetime and energy conservation. Additionally, Multi Index Adaptive Routing Algorithm (MIA-QR) was designed based on network delay, packet loss rate and signal strength for QoS. The protocol is achieved by VC on an embedded Linux system. The MIA-QR is tested and verified by experiment and the protocol is to support QoS. Finally, an improved protocol (SMAC -SD) for wireless sensor networks is proposed, in order to solve the problem of S-MAC protocol that consider either service differentiation or ensure quality of service. According to service differentiation, SMAC-SD adopts an access mechanism based on different priorities including the adjustment of priority mechanisms of channel access probability, channel multi-request mechanisms and the configuring of waiting queues with different priorities and RTS backoff for different service, which makes the important service receive high channel access probability, ensuring the transmission quality of the important service. The simulation results show that the improved protocol is able to gain amount of important service and shortens the delay at the same time. Meanwhile, it improves the performance of the network effectively

Key words: WSN, RBLEACH, PS-ACO-LEACH, MIA-QRP, SMAC-SD

ACKNOWLEDGEMENTS

I would like to express my most sincere appreciation and thanks to those who have helped me.

First of all, I would like to extend my heartfelt thanks to my supervisors, Professor Joan Lu and Professor Qiang Xu. Professor Joan Lu and Professor Qiang Xu have been a tremendous mentor for me. They are humble and approachable. Their minds are full of knowledge and academic rigor. I would like to thank them for encouraging my research in the process of topic selection and ideas of writing. In addition, their innovative mind and unique perspectives have profoundly inspired me in terms of my research and career.

A special thanks to my family. I am extremely grateful to my parents and my husband who have given me endless support.

The thesis is supported by the projects entitled “The information and control system for preventing forest fires”, and “The erhai information management system”, which come from the Chinese Government. Special thanks for the Fund Committee of YUNNAN Science and Technology Agency, Which is belong Chinese Government.

I thank for the Members of our group, especially Yubin Shao, Qin zhi Du, they give good suggest for experment simulations.

Finally, I would like to thank all the teachers who have given their kind assistance. Thank you all for your time, advice and hard work.

CONTENTS

Chapter 1 Introduction

Wireless Sensor Network (WSN) is a self-organizational Network constituted of hundreds of small-volume, low-electric energy and low-cost sensor nodes integrating sensing, data collection, processing and wireless communication ability. It aims at perceiving, collecting and processing the information of an object monitored in a geographic area covered by a network and transmitting the information to the background for data processing [1]. WSN has great potential for many applications in scenarios, such as military target tracking and surveillance [2,3], natural disaster relief [4], biomedical health monitoring [5,6], hazardous environment exploration, seismic sensing [7], intelligent agriculture, intelligent transportation[8,9], and etc.

A typical WSN includes sensor nodes, sink nodes, infrastructure network and sensor network management nodes. The nodes have resource constraints. The resource constraints include limited amount of energy, short communication range, low bandwidth and limited processing and storage in each node. Nodes transmit the data monitored to a sink node through other nodes in a multi-hop way. The design of communication protocol of WSN must be considered as follows: correctness, stability, fairness, as of the traditional computer network. Except for energy efficiency, simplicity should conform to the principles of WSN protocol. The design of the WSN protocol should be a minimum use of power and extend the life cycle. Meanwhile, Quality of Service (QoS) in WSNs is an on-going research field, due to the services differentiations. The protocol should be designed to support QoS.

Typical protocols include flat routing, hierarchical and routing based on geographic position. Optimal consumption of energy for WSN routing protocols is essential. Hierarchical is a well-known technique with special advantages in terms of scalability. There are numerous routings that have been developed for WSN data communication networks. The typical examples of the hierarchical routing protocol include:

Low Energy Adaptive Clustering Hierarchy(LEACH)[10], Power-Efficient GAthering in Sensor Information Systems(PEGASIS) [11], Tree based Energy Efficient protocol(TREEPSI)[12].

The three protocols represent typical WSN clustering routing algorithms of three different topological structures - cluster, chain and tree. PEGASIS is based on chain-based protocol. This proposal builds all sensor nodes to form a chain according to Greedy algorithm that the sum of edges must be minimum in wireless sensor networks. In PEGASIS, each node communicates only with a close neighbor and takes turns transmitting to the base station, thus reducing the amount of energy spent per round. TREEPSI is tree-based protocol in which WSNs select a root node in all the sensor nodes, the length of path form end leaf node to root/chain node in TREEPSI is the shortest. The data will not send for a longer path. Therefore, TREEPSI can reduce power consumption in data transmission less than the others. LEACH routing protocol is the first hierarchical routing protocol based on data aggregation. The initial idea is to allocate the energy load of the whole network to each sensor node on average through equal probability, random and cyclical selection of cluster heads, thus achieving the purpose of reducing network energy cost and extending the life cycle of the network. The advantage of LEACH is that each node has the equal probability to be a cluster head, which makes the energy dissipation of each node be relatively balanced. However, it requires nodes to have high communication ability and it has low expansibility. It is not appropriate for widely-scale networks [13, 14, 15, 16].

The recent research work [17,18,19] is focused on clustering strategy, and multi-hop routing mechanism. The former is responsible for the topology optimization of a network. The latter will be responsible for choosing the best path to transmit the data, which it senses in the network, to the base station by multi-hop routing mode. However, How to use the LEACH for widely area, Whether it is possible to combine clustering and routing to improve network performance? At the same time, if the swarm intelligence is introduced into the WSN, is there an advantage? This issues need more research.

Another aspect of research is focused on QoS [20]. Because WSN is limited by bandwidth delay, jitter, available bandwidth and packet loss. It is required to design and realize protocol, which supports QoS.

In the access control protocol in WSN, idle listening, collision, overhearing, control-packet overhead, traffic fluctuation cause energy consumption. IEEE802.11 [21], Time MAC (T-MAC)[22] and S-MAC[23] are proposed to decrease the energy costs and to support good scalability and avoid collision. S-MAC makes use of the periodically monitoring / sleeping mechanism and collision and crosstalk avoidance mechanism. However, the protocols do not include the differentiated services. Because WSNs are very different from traditional networks, supporting Quality of Service (QoS) in WSNs is still a largely unexplored research field. Based on S-MAC, an improved protocol SMAC-SD is proposed. The new protocol added the principle of distinction traffic, the mechanism of priority channel access based on traffic, and the mechanism of Multi-channel request mechanism.

The route is also influenced by QoS. How to choose a route based on QoS parameter is a research issue. The literatures [24,25,26,27] put forward these solutions. But most of the methods only consider a QoS parameter.

Over all, Energy efficiency and QoS will be studied in the thesis.

1.1 Motivations of this Study

The thesis is supported by the projects entitled “The information and control system for preventing forest fires”, and “The Erhai information management system”, which come from The Chinese Government. The projects have two main objectives for monitoring sensors: energy consumption and QoS. The thesis contains the two issues based on route and MAC.

1.1.1 Energy Efficiency

LEACH protocol is a clustering protocol, which is simple and easy to implement. However, the following problems should be taken into consideration:

1. How to use LEACH for a wide area? Due to the fact that the cluster head selection is randomly distributed, it will lead to a lack of uniformity in the energy distribution of sensor nodes in that the nodes, which are far away from the base station, will easily fail in a wide area.

2. Usually protocols only focus on one factor in terms of clustering strategy or multi-hop routing? For example, in researching multi-hop routing, the clustering strategy is simple. Equally, the cluster could be slightly neglected for route optimization. In fact, combining the clustering strategy and multi-hop routing mechanism will optimize the performance of network. This combination can be focused on clustering strategy or multi-hop routing.

3. LEACH routing protocol was put forward based on one parameter in WSN, such as hop counts or residual energy. Essentially, the route can be influenced by many factors, such as distance, energy and others. What if it could select multi-parameters as a judgment to select routes? What if combining Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO) is used for route?

1.1.2 QoS issue

1. Different technical communities may perceive and interpret QoS in different ways. In our project, information includes video, image and monitoring data. QoS is accepted as a measure of the service quality that the network offers to the applications. The purpose of MAC protocol is to focus on the underlying network, which provides applications to the QoS.

2. QoS is needed to support the routing protocol. How can we design and embed the routing protocol and realize these goals?

1.2 Contribution of this Study

1. A new protocol called RBLEACH is proposed to solve cluster on a widely scale. The widely scale divided into small scale and LEACH is improved to alter selecting function in each area. RBLEACH creates routes select by using a new algorithm to optimize the performance of network.

2. A new clustering method has been developed which uses several factors is PS-ACO-LEACH, the factors include the residual energy of cluster head, Euclidean distances between cluster members and a cluster head. Fitness function is optimally solved between cluster head nodes, a cluster head and the base station. It also maintain a load balance.

3. Based on the “Ant Colony” algorithm and transition of probability, a new routing protocol was created by “Pheromone” to find the optimal path of cluster heads to the base station. This protocol can avoid energy consumption of cluster heads and unbalanced energy consumption.

4. The Multi Index Adaptive Routing Algorithm (MIA-QR) was designed based on network delay, packet loss rate and signal strength. Protocol data formats are designed, and MIA-QR is achieved by Visual C++ (VC) on an embedded Linux system.

5. According to service differentiation, SMAC-SD is proposed based on S-MAC. It adopts an access mechanism based on different priorities. The protocol adjusts priority mechanisms of channel access probability, channel multi-request mechanisms, and configure waiting queues with different priorities. The protocol can make important service get high channel access probability and ensure the transmission quality of important service.

1.3 Thesis Outline

The thesis is organized as follows. In Chapter 2, it presents the main research related with the thesis. In Chapter 3, a method for improving LEACH protocol RBLEACH is proposed. In Chapter 4, PS-ACO-LEACH is proposed combining PSO and ACO, considering the combination between clustering and routing, and a complete mathematical analysis to the new protocol. In Chapter 5, based on the embedded platform that uses multi-QoS parameters, an MIA-QRP adaptive routing algorithm is put forward and the protocol is designed and implemented. In Chapter 6, improved SMAC-SD Protocol is proposed based on S-MAC. In Chapter 7, simulation and analyze of protocols are discussed for improved protocols. Chapter 8 is the summary of the thesis and overview of future works.

Chapter 2 Background

2.1 Architecture of WSN

WSN [21] nodes consist of managed nodes, aggregation and sensor nodes. A large number of sensor nodes are distributed in the monitoring region, and are responsible for the perception and acquisition of specific target temperature, humidity, density, light intensity, pressure and other physical characteristics, and then transmit these data to the aggregation node through a single-hop or multi-hop manner. The user releases monitoring tasks and data query through the management of node WSN network configuration and management. Typical WSN network structure is as shown in the Figure 2-1 [22][23]:

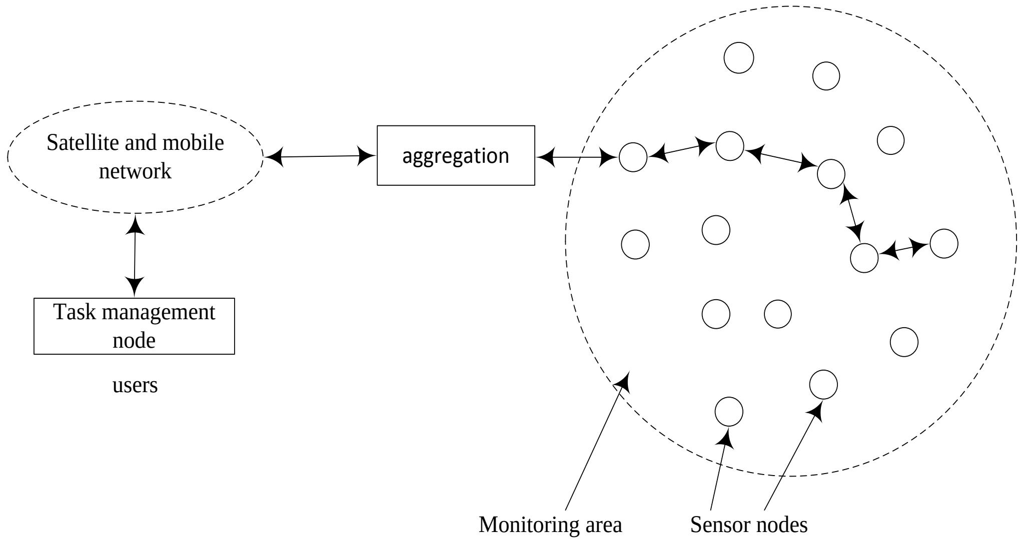


Figure2-1 Network structure of WSN

1.Wireless sensor nodes: WSN is composed of a large number of wireless sensor nodes[28], which are of a micro-embedded system, containing perception modules responsible for the perception of the external information, and are responsible for calculating the data processing module for processing data. A wireless communication module of sensor node is responsible for sending and receiving information.The energy module provides energy, and each of the wireless sensor nodes can be used as a network node terminal. The sensor nodes can also be used as a router for data perception, collection, storage, integration and forwarding.

2. Aggregation nodes: WSN system has to contain one or more node base stations (BS), also known as the aggregation node. The Aggregation node [29] is mainly responsible for transmitting data from sensor nodes for processing (such as compression, fusion), and then transfers it from the external network to the user. The data can be directly transmitted to the BS, or the BS in a multi-hop manner by the nodes. So it can be seen that the base station node is a transmission station for WSN and external network (users) to communicate with each other and that it can support two or more different protocol conversions between different protocols. The node base station typically has more computing power than ordinary sensors, more storage space and more energy reserves, and thus supports the general interaction of the entire WSN and external network (users).

3. Management node: Users manage and configure the wireless sensor node through the management nodes [30], publishing tasks, collecting data and inquiry data. On the contrary, the wireless sensor node will perceive and collect data passing to the convergence node in a single-hop or multi-hop manner, transmit the data from the Internet or a mobile network to a remote data processing center for processing or directly transmit them to the user.

4. From the perspective of network structure, it has a planar structure or hierarchical structure. In the planar structure [31], all nodes have the equal status with no difference in grades and levels. The network is divided into different levels with the selected node as the cluster head node and a cluster head perform as the communication backbone network, which is responsible for transmitting information in the network to the base station.

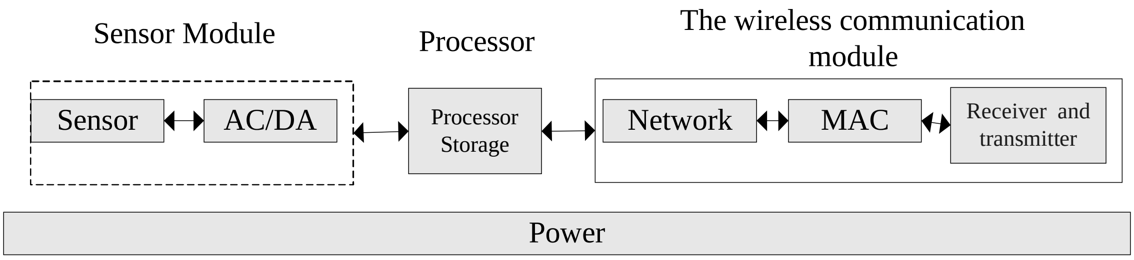


Figure 2.2 Wireless sensor network nodes module

The sensor nodes consist of four components: the sensor module, the processor module, wireless communication module and power supply module. Shown in Figure 2.2[32].

The converted information and data are collected and monitored by the sensor module it can store information.

Information is processed by processor.

Receiving and transmitting data from the own node to other nodes are undone by the wireless communication module.

The energy used by each node is supplied by energy modules.

WSN communication protocol architecture [33] is shown below, and can be divided into five layers: respectively; application layer, transmission layer, network layer, data link layer and physical layer. The horizontal management plane can be divided into the energy management plane, mobility management plane and task management plane. The following is the description of each of the specific functions.

WSN protocol stack is shown in Figure 2.3[34]:

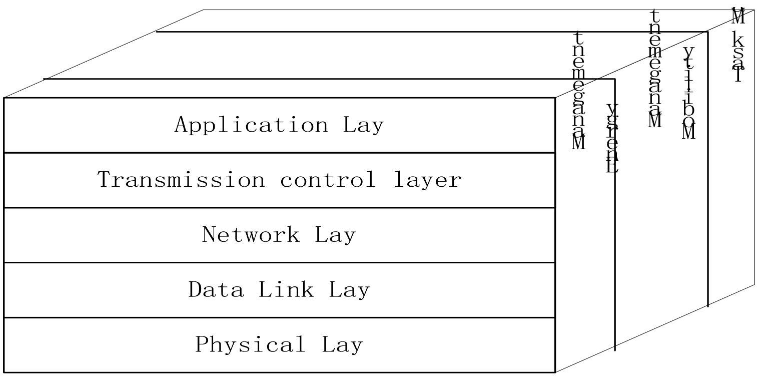


Figure 2.3 WSN Protocol

The physical layer addresses the needs of a robust modulation, transmission and receiving techniques.

Data link layer provides data framing, frame monitoring, media access and error control.

The network layer takes care of routing the data supplied by the transport layer.

The transport layer helps to maintain the flow of data if the wireless sensor network application requires it.

Depending on the sensing tasks, different types of application software can be set up and used on the application layer.

The power management plane manages how a sensor node uses its power and manages its power consumption among the three operations (sensing, computation, and wireless communications). The mobility management plane detects and registers the movement mobility of sensor nodes as a network control primitive. The task management plane (i.e., cooperative efforts of sensor nodes) balances and schedules the events' sensing and detecting tasks from a specific area.

2.2 Limitations of WSN

Limitations of WSN include:

1. Limitation of Power

Power limit sensor nodes are usually tiny with a low price, carrying limited energy[35][36]. There is no device transmitting external light, heat and tidal energy into electricity. Besides, it's impractical to change sensor nodes manually for the amount, distance and complex environmental reasons. As the precious energy is carried by sensors, its priority is to make full use of the energy and extend the life cycle of WSN. Due to the consumption of a vast majority of energy by the sensor in the wireless communication module design of WSN routing protocols, energy saving has become a need to focus on issues for consideration.

2. Limitation of Communication ability

It can be seen that there exists a positive correlation between the energy consumption of communicating nodes with the distance. The longer the distance is, the greater the energy consumption will be with a sharp increase. Therefore, under the premise of guaranteeing the communication link, it is required to try to reduce the distance of the single-hop communication, meanwhile, to design WSN routing one also needs to optimize the communication mechanisms to meet the communication needs of nodes in the network.

3. Limitation of computation and storage ability

The wireless sensor is a micro-embedded device, with weak data processing capability and small storage space. These nodes finish complex work, including the data monitoring, acquisition and conversion, the data processing [37]. For instance, one would need to address how to take full advantage of the node itself, the computing power and storage space and how to use the idea of working together to optimize computing and storage node challenged in the process of WSN routing design.

To sum up, the following problems need to be solved emphatically in WSN: (1) energy saving: due to a great number of nodes and wide distribution in the wireless sensor network, a battery supply is a widely used method. But the energy is limited and it is difficult to change and recharge the power for the battery supply. In order to make maximum use of the network and guarantee the working time, the energy should be saved as much as possible in the network; (2) network scalability: continuous invalidation would happen in network working due to a limited amount of node energy. The new nodes need to be added to enlarge the lifetime of the network. Thus, the topology of network is always changeable. WSN protocol needs to overcome this network scalability to adapt to this topological change; (3) network efficiency: the measurements to determine network efficiency include fairness, real-timing and utilization rate of the broad band etc.

2.3 Overview of research issues

In the case of WSNs, the following aspects must also be considered [38]: network topology control, network contract, information security, time synchronization, positioning technology, data fusion and management, developed on embedded operating system, application-layer technology

1. Network topology control

A good network topology is generated automatically by the topology control [39], it is possible to improve the efficiency of the MAC protocol for time synchronization, data fusion and targeting many aspects of the foundation, the sensor node can also save energy to extend the life cycle of the entire network. Under the premise of guaranteeing coverage to meet the communication link, the methods for forming network topology in order to ensure efficient data forwarding is the focus of current research.

2. Network contract

WSN has a dynamically changing topology; the nodes in the network are constantly changing, medium access control (MAC) protocol is an important factor to network contract. Network contract is time division multiple access (TDMA), frequence division multiple access and Coding division multiple access. Another method is competition-based MAC protocol, such as CSMA or SMAC [40,41].

3. Information security

As a task-based data-centric network, WSN not only collects data, but also needs to address, integrate and transmit data. Reliable and secure transmission and efficient data fusion on WSN is of paramount concern [42]. Information security should be paid attention to the problem, in order to ensure the message's authenticity, integrity, robustness, confidentiality, availability.

4. Time synchronization

Time synchronization is a new hot spot in the study of WSN technology. Many wireless sensor network applications require the sensor nodes to maintain clock synchronization. For WSN's own characteristics in the synchronization range, the synchronization accuracy and energy consumption have special requirements, so it is not applicable to make traditional synchronizations in WSN. In the design of WSN time synchronization mechanisms [43], it is required to take into account the stability, convergence, energy perception and scalability and other factors simultaneously. But because of the diversity of WSN applications, it is difficult to meet all application requirements for time synchronization mechanism.

5. Positioning technology

The location information is very important for the wireless sensors and the single collection of data [44], the majority of the data must be included for the location information in order to make it sense. Determining the data collection node location or a time position is one of the most basic functions of WSN. Deployed in the monitoring region of the wireless sensor nodes it must be able to get its own position, and positioning mechanisms need to consider self-organization, robustness, distributed computing and energy efficiency.

6. Data fusion

Due to the limited scope of the perception of a WSN, the data collected usually does not have a high degree of accuracy and redundancy. In order to improve the data accuracy and reduce the amount of data transmitted to save energy, it is needed to send and transmit data with WSN, use their computing power and storage capacity and realize relay data transmission fusion [45] to remove redundant information, so as to save node energy.

7. Data management

WSN can be seen as a distributed database. By simplifying the logical structure of data query management and database management [46] in WSN, WSN observers can achieve a logical view of the data stored in the network and network separation without hindering the specific implementation process.

8. Developed on embedded operating system

Each wireless sensor is a micro-embedded system containing simple data acquisition, process control [47], wireless communications and energy supply module with data processing algorithms input and data transfer protocol, application-specific support.

The new generation of WSN operating system needs to handle multiple applications concurrently, for control of hardware resources to respond to the multi-application, the question of how to efficiently use the wireless sensor nodes concurrency-intensive and high degree of modularity is a new challenge for WSN operating systems.

9. Application-layer technology

WSN application layer is the application by the individual-oriented software components, and publishes a variety of commands to perform a variety of specific tasks to WSN. WSN application level is focused on application system development and coordination between multi-tasking. Study of the application layer is only half completed: application-oriented system services, based on perceptual data understanding, decision making and actions of theory and technology [48,49].

10. QoS supporting

Different multimedia applications have different QoS requirements expressed in terms of end to-end QoS parameters in traditional network[50].QoS requirements generated by the applications of WSNs may be very different and traditional end-to-end. Some new QoS parameters are desired for the measurement of the delivery of the sensor data in an efficient and effective way. In WSN, The protocol need QoS routing, and QoS Medium Access Control (MAC)to support QoS, includes QoS model, QoS resource reservation signaling. They are current research issues.

The thesis is supported by the projects, which are provided financial aid by the Chinese Government “The information and control system for preventing forest fires ”, “Erhai information system” and etc.. The projects have two main problems for monitoring sensors: energy consumption, and QoS. The thesis will research the two issues based on route and MAC.

In conclusion, the thesis will focus on reduce energy consumption and ensure QoS. The issues regarding MAC and route protocol will be discussed.

2.4. WSN routing protocol

2.4.1 WSN routing protocol' characteristics

Routing protocols in WSN differ from traditional routing protocols in several ways [51]. For one, sensor nodes do not have Internet protocol (IP) addresses, so IP-based routing protocols cannot be used in a WSN. The design of network protocols in a WSN needs to be scalable. It should easily manage communication among many nodes and propagate sensor data to the base station. The protocol should meet network resource constraints such as limited energy, communication bandwidth, memory, and computation capabilities. By meeting these constraints, a sensor network's lifetime can be prolonged. Lastly, the protocol should address issues of efficiency, fault tolerance, fairness, and security.

WSN routing protocol has the following characteristics:

1. Energy priority. The Energy of a WSN node is limited, and prolonged survival of the entire network is an important goal, the energy consumption of nodes and balance of network energy is an important factor [52,53,54].

2. Based on local topology information. WSN uses multi-hop communication modes in order to save energy, nodes with limited memory resources and computing resources, cannot store large amounts of routing information. Because of local node topology information storage, how to implement a simple and efficient routing mechanism is a fundamental problem in wireless sensor network [55,56,57,58].

3. Data-centric. WSN has a large number of nodes deployed randomly; monitoring data is focused on the data forwarding path, which is importance. The

monitoring data have redundancy. Data-centric route finishes aggregation of data for the energy-efficient. [59]

4. Related-applications. WSNs are applied in different environments, data communication patterns are different, and there is no routing mechanism suitable for all applications, which is a manifestation of sensor network. Designers need to analyze the needs of each specific application with specific routing mechanisms and design a routing mechanism which can adapt to those needs.

For these characteristics of WSN routing mechanisms, depending on applications when designing routing mechanisms, it should meet the following requirements[55]:

1. Energy efficiency. WSN routing protocol not only needs to select the energy consumption of transmission paths, but also considers entire network considerations, chooses balanced energy consumption for the entire network and requires simple and efficient implementation transmission of information.

2. Scalability. In WSN, area ranges or different node densities are detected, resulting in different network sizes; if a node fails, a new node is added, node mobility, it will make the network topology change dynamically, requiring scalable routing mechanisms which can adapt to changes in the structure of the network.

3. Robustness. Routing mechanisms requires a certain fault tolerance because of the exhaustion of energy or environmental factors which may cause failure of sensor nodes, the surrounding environment also can affect the quality of wireless communication links.

4. Fast convergence. Routing mechanisms are required to quickly to adapt to the dynamic changes in network topology, limited node energy and communication bandwidth.

5. Quality of Service (QoS): dynamic configuration of the network resources in order to enable higher data efficiency issues from networking support and QoS considerations.

2.4.2 Routing Category

In general, routing in WSNs can be divided into flat-based routing, hierarchical-based routing, and location-based routing depending on the network structure [60]. In flat-based routing, all nodes are typically assigned equal roles or functionality. In hierarchical-based routing; however, nodes will play different roles in the network. In location-based routing, sensor nodes' positions are exploited to route data in the network. A routing protocol is considered adaptive if certain system parameters can be controlled in order to adapt to the current network conditions and available energy levels.

As figure2.4 shows, the network is divided into a group of clusters, each cluster selected a node as a cluster head, the job of each cluster head is to transmit information to the base station after it finishes aggregation of the data, and removes redundant information. Figure 2.4 shows the structure relationship between the various parts of WSN in the cluster [61,62,63].

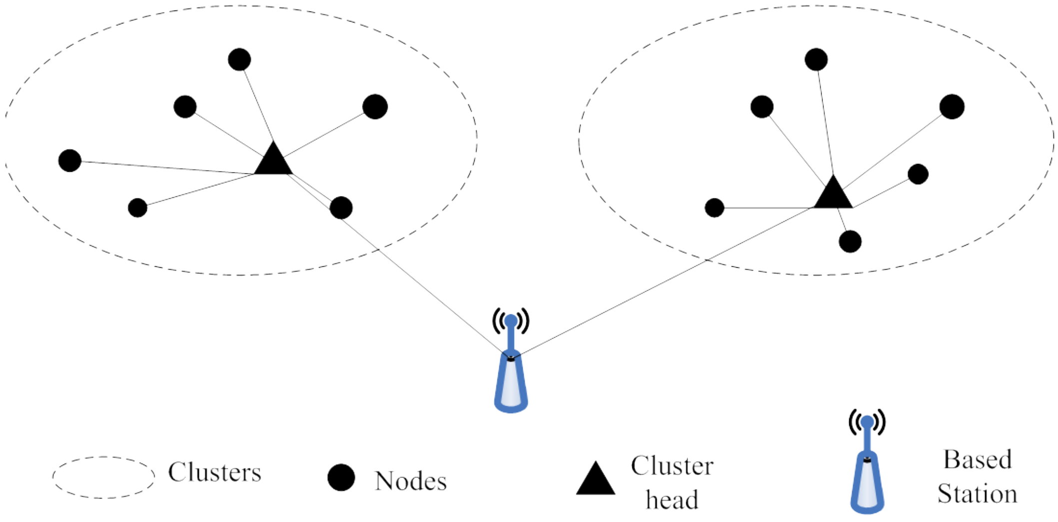


Figure 2.4 Structural relationships between nodes, cluster heads and base stations in WSN

After the network is clustered, cluster members are flexible, variable levels of network formation. Its advantages are [64,65]:

1. The storage space is reduced for routing table on a single node;

2. Clustering limits the scope of interaction within the cluster, avoids excessive exchange of information between the sensor nodes, and reduce the information stream in the broadband of communication;

3. Clustering can effectively stabilize the network topology, reduce topology maintenance overhead;

4. The sensors only need to focus on the connection between the cluster heads; the impact of inter-cluster heads doesn’t change the hierarchy;

5. The cluster head can be determined by optimal management mechanism, and further enhance network operation, extend battery life and individual nodes throughout the network life cycle;

6.The cluster head can schedule activities within a cluster, the nodes can wake up based on a low-power sleep mode to reduce the energy consumption rate, allowing the sensor nodes to run in web mode and determining the send and receive timing to avoid retry limit coverage redundancy to prevent an MAC layer of conflict [66].

7.The cluster head in a cluster can collect data, reducing the number [67] of the relay packets.

2.4.3 Clustering algorithm requires

Regarding applications of WSNs, clustering is proposed for different structures and design goals. The following are the structural parameters and the impact on network clustering.

1. Network dynamics: The nodes’ moving and the energy’s limitation cause topology change [68].

2. Network data processing: As the node may generate a lot of redundant data, similar data on multiple node aggregation packets reduces the amount of information

sent [10]; one must assign a cluster head for each cluster to achieve data forwarding.

3. Node Deployment: sensor nodes have the same energy, computing and communication capabilities when the nodes are randomly distributed; they are called isomorphic sensor network. Cluster heads communicate without sensors; the cluster head may not have the ability to reach the base station. The connectivity of a cluster head is an important part of the clustering mechanism [69].

2.4.4 Target of clustering protocol design

In order to meet different application requirements, various clustering algorithms goals are distinguished.Route hops in order to satisfy the delay-sensitive date, and the routing performances will be disscussed.

1. The maximum lifetime

A node starts working until its energy is depleted, combining clustering routing and adaptive clustering so as to maximize the lifetime of the network and streamline routing design goals[70][71].

2. Load balancing

Balance of node load to extend the lifetime of a network is the goal of clustering [72]. Load balancing is especially useful in energy constrained sensor network because the relative energy level of the nodes does affect the network lifetime more than their absolute energy level. When all sensors have equal initial energy and equal chances to become sources, network could maximize its lifetime if all sensor sensors dissipate energy at the same rate, since no loss of connectivity would result from node failure.

3. Fault tolerance

To avoid losing information, the cluster head should be fault tolerant [73]. Intuitive re-clustering is the role of the cluster nodes cluster head, rotation is also a tolerant approach and also has the advantage of balancing the load.

4. Enhanced connectivity to reduce delay

The purpose of communication is to ensure the existence of available paths from each cluster head to the point of convergence; connectivity becomes a design goal and constraint between clusters.

2.5 Typical clustering algorithm analysis and comparison

2.5.1 LCA

Mustapha Khiati, Djamel Djenouri proposed Linked cluster algorithm (LCA) [74]. The algorithm is to build a network topology that can effectively solve the problem of the movement of nodes. Every node broadcasts its ID and monitors the transmission of the other nodes. In the next round, the nodes broadcast the monitored the set of neighbors, and let every node know its 1-hop and 2-hop neighbors. Node x is defined as the cluster head if it has the highest ID amongst the neighbors, or if it does not have the highest in the near 1-hop neighbor but there is at least one node y in the neighbors making node x become the highest ID node in the 1-hop neighbor of node y. When nodes move, the cluster head can form a backbone for the network by means clustering, which allows the cluster members to connect. LCA algorithm is prepared to maximize the connectivity of the network.

2.5.2 RCC

K. Xu, M. Gerla proposed random competition based clustering(RCC) [75].The protocol is designed for a mobile WSN network, RCC is the clustering based on random competition. RCC algorithm focuses on the stability of the cluster and follows the rule of “first claim, first win”. After receiving the message of the first node broadcast, the neighboring nodes will join in the cluster as a member and give up the right of being a cluster head. In order to maintain the cluster, every cluster head will regularly broadcast the message of cluster head. The delay between message receiving and sending which may cause conflicts can force the neighboring nodes to broadcast the message simultaneously due to the fact that other nodes cannot sense the ongoing message. To avoid this problem, RCC makes judgments by using a random timer and node ID’s. Every node in the network will reset their time value randomly before broadcasting the message of cluster head. During a random time, a node will simply cancel its self-sent cluster head message if it receives the broadcasted message of cluster head from another node. Since the random timer cannot completely solve this problem, the nodes with a lower ID will become the cluster head if the conflict is upheld. Although frequent movements of the nodes directly affect the stability, RCC is more stable than a traditional clustering mechanism. A cluster head in the self-adaptive clustering mechanism gives up its own position when sensing a node with a lower ID; but a cluster head in the RCC gives up its own position only when a cluster head moves close to it.

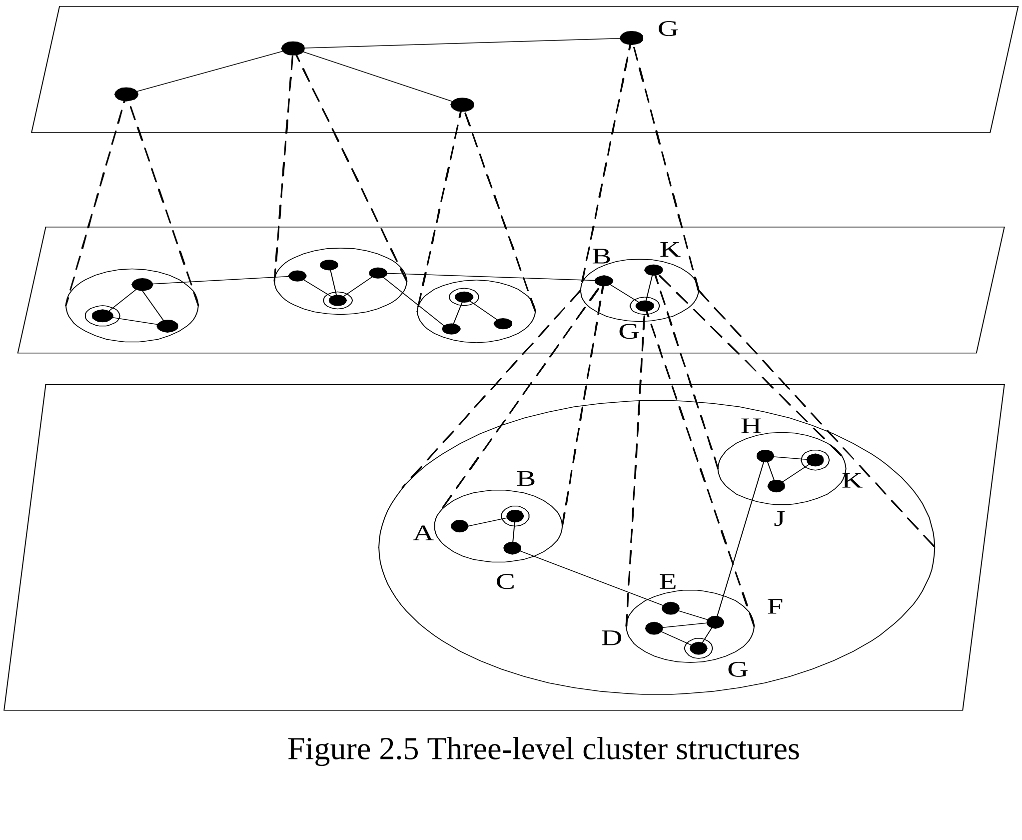


Figure 2.5 Three-level cluster structures

2.5.3 EEHC

S. Bandyopadhyay, E. Coyle proposed Energy Efficient Hierarchical Clustering algorithm (EEHC) [76] is the distributive clustering algorithm with the objective of maximizing the network survival time. The cluster heads collect the data picked up by the sensors in the clusters, and send the collected report to a focal point. In the stage of initialization (also called the single-stage clustering), every node claims itself as the cluster head with frequency p to the neighbor node in its communication range. These cluster heads claim themselves as the "volunteer" cluster heads. All cluster heads that are in the k-hop range of cluster heads receive the claims by direct communication or repost. Any cluster head will become the nearest cluster member if it is not the cluster head and receives the claims. The forced cluster head is neither the cluster head nor the node that belongs to the clusters. If the claim cannot get a node with the set time t, time t can be calculated by the duration when a message to the k-hop's node is received. If the claims are not in the any k-hop of the volunteer cluster head, this node is defined as the forced cluster head. In the second stage, the process is developed to allow the multi-level clustering, which is to build the h level cluster layers ,as shown in Figure 2.5. The process of recursive clustering repeats and forms an echoed level. The algorithm ensures the n-hop connection between cluster head and focal points. If the highest level is set as the h level, the sensor node will send the collected data to the higher level cluster head. The data at level-1 can be transferred and aggregated to level-2; the rest may be deduced by analogy. At the highest level of a clustering structure, the cluster head will send the data to the focal points.

2.5.4 HEED

O. Younis, S. Fahmy proposed Hybrid Energy-Efficient Distributed Clustering (HEED) [77]. The protocol can be selected from the deployment of sensor nodes. The energy and communication cost of HEED must be considered comprehensively in the selection of cluster head. This algorithm cannot select the cluster head node randomly, because only the nodes with residual energy can become the cluster head node. There are three main characteristics for this algorithm:

First, the probability of being a cluster head is low in the transmission range between two nodes. Second, the energy cost is not balanced for all nodes. Third, the connectivity between the cluster heads can be maintained by adjusting the selection probabilities for the given transmission range of nodes.

At HEED, every node can certainly shine upon the cluster, and communicate with the cluster head directly. The algorithm can be classified into three stages:

Initialization phases: Firstly, set the initial proportion C_{prob} of all nodes in the cluster head. This ratio is used to limit the initial cluster heads for other sensors declared. Each sensor in accordance with the formula (2-1) as a cluster head determines the probability CH_{prob}

$$CH_{prob} = C_{prob} \times E_{residual} / E_{\max} \qquad (2.1)$$

$E_{residual}$ is residual energy of the current node $E_{\max}$ is the maximum energy when the battery is fully charged. CH_{prob} is not allowed to fall below a certain threshold $P_{\min}$, $P_{\min}$ and $E_{\max}$ is inversed.

Repeat phase: In this phase, each sensor node goes through several iterations until the cluster head with minimum transmission power transmission is found, if not the cluster head is not heard, the cluster head node is allowed to send a message to its neighbors notifying of changes. Finally, each sensor CH_{prob}, is multiplied and it goes on into the next iteration. When it reaches 1, the stage is stopped. Therefore, the sensor nodes can advertise to their neighbors; there are two types of cluster head states:

Temporary Status: If $CH_{prob} < 1$, the sensor node becomes a temporary cluster head. If a lower power node cluster head is found, it can switch to the next iteration of general node status.

Final state: If CH_{prob} is 1, the node becomes permanently cluster head.

Final phase: In this phase, each sensor node according to their status as a final decision, with the selection of the least expense of a cluster head or declared itself as the cluster head.

2.5.5 DWEHC

P. Ding, J. Holliday, A. Celik put forward Distributed Weight-Based Energy-Efficient Hierarchical Clustering (DWEHC) [78], as shown in Figure 2.6. Every node calculates its' self-weight after locating the neighbor nodes. The weight is the function of the nodes energy and the proximity of the neighbors. In the neighborhood, the node with

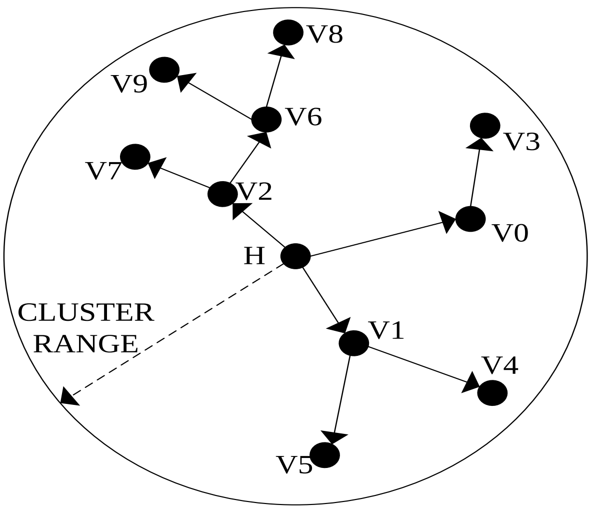


Figure 2.6 DWEHC cluster topology

maximum weight becomes the cluster head, and other nodes become the members. In this stage, since the nodes directly connect with the cluster head, they are defined as first-class members. In order to get the cluster head with the minimal energy, the nodes will keep adjusting the relations between members. The nodes will check the minimum power of non-cluster heads, and will judge them self to be a first level member or a second level member with a 2-hop to be the cluster head if the distance between the node to the neighbors is known. If the nodes can determine topology inside the cluster with the most effective energy use, the processing will stop. In order to limit the number of levels, every cluster is distributed in a range that each member node should give.

2.5.6 EEUC

Heinzelman W, Chandarkasan A, Balakrishnan H. proposed Energy Efficient Uneven Clustering EEUC [79]. The algorithm classifies the routing organization into two parts: intra-cluster communication and communication between the cluster heads and focal points. The intra-cluster communication uses single-hop, which is easy to achieve, while the communication between the cluster heads and focal points uses multi-hop to prevent energy waste caused by long-distance data transmission. EEUC algorithm uses non-uniform competitive radius so as to relatively decrease the number of cluster members that are closed to the focal points. Thus, the cluster head can save energy used when reposting the data in order to balance the energy cost of cluster heads. Moreover, not only is it important to consider the position of the candidate nodes to the focal points, but also the residual energy of candidate nodes when the cluster head selects the next hop nodes of its routing. The experiment results show that this routing algorithm can effectively solve the problems of non-uniform cluster head energy cost under multi-hop communication. This algorithm can also modify the energy cost of every node in the network and effectively prolong the lifetime of the network.

2.5.7 LEACH

Heinzelman W, Chandrakasan A, Balakrishnan H proposed Low Energy Adaptive Clustering Hierarchy [LEACH][10]. Based on the clustering, LEACH protocol is a low-cost protocol and clustering algorithm with the self-adaption. The cluster head nodes collect the data of sensor nodes from the clusters, and then the data is processed and sent to the focal points, which is the cluster head with a layered structure. It is very easy to select the information transmission path and save routing information without saving a large amount of information in complex functions. LEACH routing protocol can be mainly divided into two stages: building of the clusters and table processing.

The total time of these two stages is called a round. In order to decrease the cost of the protocol, the duration of the stable processing stage is longer than the building of clusters. However, very few nodes in LEACH usually die prematurely because of too much energy in the network. The sequence of the death is from the distant to the close. Thus, the communication of the region far away from the base station will be unresponsive early in the round and the functional region of the whole network decreases quickly while the life of network is strongly reduced.

This algorithm is one of the most popular clustering algorithms. In this thesis improvements to the LEACH algorithm are proposed and its detailed processing steps will be described in the next chapter.

To sum up, the comparison of various algorithms is as shown in Table 2.1[80, 81, 82].

Table 2-1 Comparison of various algorithms

Clustering approaches	Converg-ence time	Node mobility	Cluster overlap ping	Location awareness	Energy efficient	Failure recovery	Balanced clustering	Cluster stability
LCA	$O(n)$	Possible	No	Required	No	Yes	OK	Moderate
RCC	$O(n)$	Yes	No	Required	N/A	Yes	Good	Moderate
EEHC	$O(k_1 + k_2 + \cdots +$	No	No	Required	Yes	N/A	OK	N/A
HEED	$O(1)$	Stationa ry	No	Not required	Yes	N/A	Good	High
DWEHC	$O(1)$	Stationa ry	No	Required	Yes	N/A	Very good	High
EEUC	$O(1)$	No	No	Required	Yes	N/A	Good	High
LEACH	$O(1)$	Fixed BS	No	Not required	No	Yes	OK	Moderate

2.6 Analysis on LEACH algorithm

2.6.1 Network model

The network model uses the typical settings of the topology control in WSN, which is the same with LEACH. N nodes are randomly distributed in the region with the determined directions. The communication abilities of these isomorphic nodes are weak. The calculation abilities are relatively weak, and their energy is limited. These nodes will not move after being settled down, and they can automatically connect to each other to build the network without the manual help. There is only one base station in the whole network. The network which is built by the connections of nodes has the following properties [10]:

1) The energy consumption of the nodes in the network is different in every round

2) It is no need to know the detailed position of the nodes in the network and it is only needed to know the relative distance with the other nodes.

3) There is a network synchronization clock; each sensor node senses the monitoring parameter of the surrounding environment at a constant rate.

4) All sensor nodes in the network perceive the environment with a constant rate. Thus, there must be data information sent to the terminal.

5) The life cycle of the network is the duration from the operation of network to the first node death.

To sum up, it is clear that the design of the algorithm should uniformly distribute the energy cost of the network system into all nodes. The design also needs to guarantee scalability of the whole network and guarantee that the nodes can deal with the relative operations in different positions. Moreover, the design should reduce the negative effects to the network

The communication of the network uses both a symmetrical communication channel model and a free space model. In the environment of the network, the node energy cost of message sending with the constant distance threshold d is in proportion to the distance between the node sending and receiving. The node energy cost of a message sending can be calculated based on formula (2-2) and (2-3) by first order radio model [83].

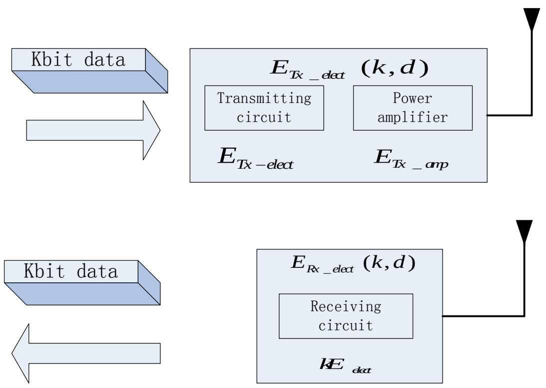


Figure 2.7 First order radio model

The energy cost produced in the data transmission of the receiving nodes is as shown in formula (2-2) [10,83]

$$E_{Tx}\left(k,d\right)=E_{Tx-elect}\left(k\right)+E_{Tx-amp}\left(k,d\right)$$

$$=\begin{cases} k*E_{elect}+k*\varepsilon_{fs}*d^2, d<d_0 \\ k*E_{elect}+k*\varepsilon_{mp}*d^4, d\geq d_0 \end{cases} \quad \ldots\ldots.(2\text{-}2)$$

$$E_{Rx}(k,d)=E_{elec}k \quad \ldots\ldots \quad \ldots(2\text{-}3)$$

Where k is the length of the data frame in the protocol, d is distance between the two nodes, E_{elec} *i*s the power consumption of sending and receiving, determined by the circuit itself, and ε_{amp} is the sending energy cost of an amplifier in the protocol, the transmission distance is less than threshold, the power amplifier ε_{fs} of free space model is adopted. Conversely, when the transmission distance is equal or greater than the value, the power amplifier ε_{amp} of multi-path attenuation model is adopted.

If the transmission distance is less than threshold d_0, the power amplifier *E*elec is the power consumption of sending and receiving, decided by the circuit itself.

$$d_0=\sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}} \quad (2\text{-}4)$$

2.6.2 Forming process of cluster

1. About “round”

The concept of the “round” has been introduced in LEACH [10]. The working process of the whole sensor network is divided into several rounds with two stages in each round: cluster creation stage and stable data communication stage. The cluster creation stage is mainly to send the control message without sending the actual sensor data. All nodes organize the clustering by broadcasting what is called the “short message”, one node in every cluster is set as the cluster head. After cluster formation, the cluster head is responsible for creating a TDMA program in the nodes. In the stage of clustering, all nodes broadcast the “short message” for communication by CSMA protocol. In the stage of stable data communication, the nodes send the data collected continuously by every frame to the cluster head nodes based on the TDMA program. Then the cluster head focuses the important data and sends them to the aggregation nodes. This is regarded as a recognizable method for reducing communication traffic. Figure 2.8 illustrates the above processes.

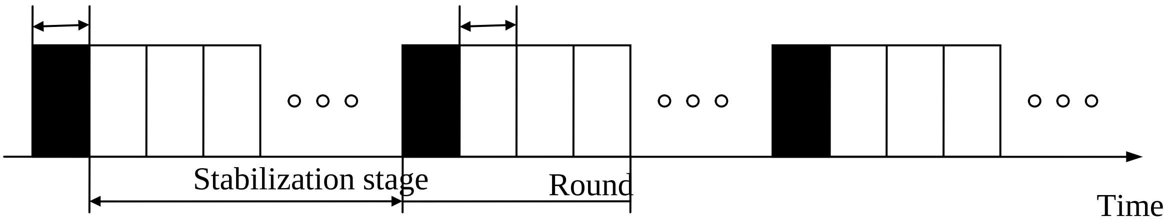


Figure 2.8Working process of LEACH protocol

2. Election method of cluster head.

In the creation stage, the sensor nodes create a random number from 0 to 1. If this number is lower than the threshold $T(n)$, the node will be the cluster head. $T(n)$ can be calculated based on formula (2-4)[12].

$$T(n)=\begin{cases}\dfrac{p}{1-p[r \bmod (1/p)]} & n\in G\\ 0 & other\end{cases} \tag{2-5}$$

Where, p is the percentage of the expected number of the cluster head in all nodes, which is the possibility of the nodes to be selected as cluster heads, r is the number of rounds. G is the set of all nodes not selected as the cluster head in the recent $1/p$ rounds. In every round, $T(n)$ is set as 0 if the nodes have been selected as the cluster head so that there is no node selected as the cluster head. For those sensor nodes not selected as the cluster head, they will be selected with the probability of $T(n)$. The threshold $T(n)$ of the residual nodes that will be selected as the cluster heads increases as more and more nodes are selected to be the cluster head. However, the random number percentage of the probabilities that the nodes creation is lower than the value of the $T(n)$ will increase. Thus the percentage of the nodes to be selected as the cluster head will increase. As there is only one node not selected as the cluster head, $T(n)=1$, which means this node certainly can be selected.

4. Cluster head number

The cluster head is randomly created in the region of the whole network in LEACH protocol, including the position and number of cluster head. This kind of random creation will lead to excessive cluster heads. In every round of LEACH protocol, the number of the selected cluster heads follows the binomial distribution. Assume that the percentage of the cluster head is $p=k/N$, the number of the selected cluster heads in every round is X. The formula (2-6) can be obtained:

$$P\{X=k\}=\binom{N}{k}p^{k}(1-p)^{N-k} \qquad (2\text{-}6)$$

5. Cluster head distribution

LEACH protocol randomly produces the cluster head in the whole region. This random distribution makes the size and scope of each cluster different, as shown in Figure 2.8. According to the analysis in Figure 2.9, it is known that this difference is caused by clustering distribution and will cause the prerequisites of LEACH protocol algorithm not to be ensured.

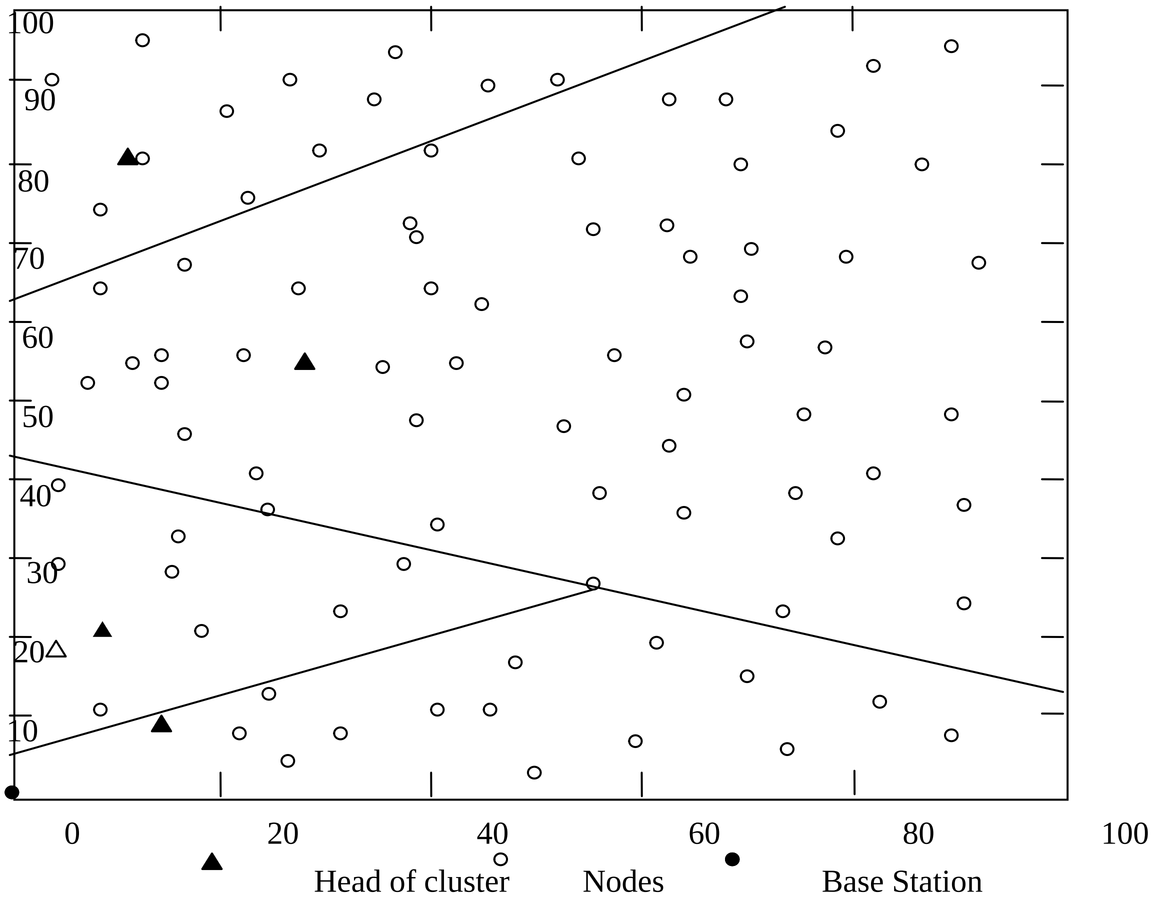


Figure 2.9 LEACH Cluster Distributions

The condition that LEACH protocol can effectively operate is described as follows: the first condition is the beginning of cluster formation. The energy of all nodes is the same at this moment. The second condition is cluster formation. The energy consumed is generally similar. In the first life cycle of the network, the first prerequisite is easily satisfied when the cluster head is selected in the first round. However, the second prerequisite cannot be satisfied if the range of the clustering is not constant. The network model is assumed as in section 2.61, that all the sensors perceive the surroundings. Therefore, the data is sent to the users. The nodes transmit the data at a constant rate, thus the clustering range affects the workload of the cluster head. As mentioned above, the nodes energy that is consumed by the range of cluster and the cluster position produced and distributed randomly by LEACH protocol has an obvious difference in data transmission. Meanwhile, there is a large difference between the contained nodes and the cluster head in terms of distance. Hence, the communication functions between the nodes have large differences. In the following round, the algorithm protocol will select a node that consumes more energy than the previous round as the cluster head, which will conversely accelerate the death of the nodes.

2.7 Extended LEACH

2.7.1 Extended LEACH

LEACH has been improved for various applications. Zuo Chen,Kai Chen proposed LEACH-MF, the protocol adopts the methods of multi-layer clustering and eliminates redundant information [84], B. Manzoora, N. Javaida, O. Rehmana, etl propose Quadrature-LEACH (Q-LEACH) for homogenous networks which enhances stability period, network life-time and throughput quiet significantly[85]. Thiemo Voigt proposed SLEACH [86], it provides a better network lifetime as compared to LEACH, some nodes are facilitated by solar power and these nodes act as CHs which mainly depend upon their solar status in LEACH. Farooq, M.O, Dogar, A.B. proposed Multi-Hop LEACH [87], it is more Energy efficient than LEACH. In Multi-Hop LEACH cluster-heads a long distance from Base station transmit data to next cluster-head closer to Base station instead of direct transmission to Base station. Wu Xinhua, Wang Sheng proposed LEACH-C [88] .To LEACH-C, at the initialization of every round, each node has to report its residual energy, resulting in copious energy consumption. Sunkara Vinodh Kumar and Ajit Pal proposed Assisted LEACH (A-LEACH) [89]; the protocol achieves lessened and uniform distribution of dissipated energy by separating the tasks of Routing and Data Aggregation. Mustapha Khiati, Djamel Djenouri proposed Broadcast over Duty-Cycle LEACH (BOD-LEACH)[90], which adds new common static and dynamic broadcast periods to support and accelerate broadcasting. This reduces broadcast latency and ensures scalability. JIANG

Yang， SUN Liu-lin[91]and others proposed a model to calculate the number of cluster head according to energy consumption. Hu Junping, Jin Yuhui, Dou Liang proposed LEACH-F [92], it makes some changes to the basis of LEACH. The formation of clusters is same as LEACH-C. The base station uses simulated annealing algorithms to generate clusters. Meanwhile, base stations generate a cluster head list for each cluster to indicate the order of selection of nodes for cluster heads in turn. Once a cluster is formed, its structure will no longer change. Compared to LEACH and LEACH-C, the greatest advantage of LEACH-F is that it is unnecessary to establish clusters in each cycle and the cost for establishing clusters is reduced. However, LEACH-F is not appropriate for real network applications, because it cannot process the addition, failure and motion of nodes dynamically and it increases signal interference among clusters. The generation of cluster heads in HYENAS[93] is basically the same as LEACH-C. It is generated by the base station with a centralized algorithm. However, it is necessary to determine whether to cluster again according to the similarity of the chosen clusters. The similarity of clusters can be completed according to the process of adaptive learning. Jing Chen, Hong Shen proposed HYENAS. It avoids the recombination of clusters and saves the cost for clustering in each cycle.

To conclude, LEACH protocol allows every node to have the chance to be the cluster head in the whole work cycle because of the expectations, making the load uniform, to some extent. However, the distribution and the number of cluster heads have some randomness and there are still some cluster heads that die prematurely, which cause a decrease in the life of the network. In order to prevent this phenomenon from happening, the nodes with high ability should be selected as cluster head as much as possible, and the energy used by the selected cluster head should be reduced as much as possible.

2.7.2 Reasons to select LEACH protocol as the improved object in the research

LEACH protocol is a low energy cost, self-adapting clustering routing protocol designed for WSN according to the layer routing. After LEACH protocol, many clustering protocols [85,86,87,88,89,90,91,92,93] are proposed and designed based on LEACH protocol. A lot of simulation experiments prove that this algorithm has a better stability and longer life cycle compared with the general plane routing algorithms and static clustering algorithms.

LEACH routing protocol has many characteristics in solving the problems of node life cycles in WSN. For example, it reduces the number of the node transmissions and the aggregation messages. The cluster head nodes are responsible for focusing the message sent from different nodes in the cluster, and send the collected message to the base station. The conflicts between or in the clusters are reduced by the MAC layer mechanism based on TDMA/CDMA[94]. The protocol is able to reselect the cluster head nodes to guarantee balanced use of energy in a WSN. However, there are still disadvantages of LEACH protocol [95,96]:

1. LEACH protocol cannot guarantee an even distribution of all cluster head nodes in the space within specified settings. In some cases, the cluster head nodes selected by the algorithm may concentrate in some narrow region, making some of the member nodes unable to join any cluster, or cause them to consume too much energy in the process of data communication, thus resulting in the premature death of those nodes, and even making it impossible to communicate with the cluster head nodes.

2. Asymmetrical distances between the cluster heads and the base station cause a non-uniform load to occur.

In LEACH protocol clustering algorithm, the cluster head is selected to produce a single-hop algorithm. The cluster nodes directly communicate with the base station after aggregating the data message sent from the other nodes in the cluster. In a small network scope, most communications which applied free space models between the cluster head and base station can be ensured, which can eliminate the energy differences consumed by the cluster head communication in different regions. However, once the covered regions in the network become larger, the differences of the energy cost between the nodes will become larger if the cluster head nodes select single-hop communication again. This can cause a situation to occur in which the nodes far from the base station die earlier than the nodes near the base station, which will influence the characteristics of the whole network.

Figure 2.10 is a screenshot of the experiment simulation of LEACH protocol. As shown in Figure 2.10, as the region scope of the whole network becomes larger, the nodes loads become uneven. The life cycle of the nodes near the base station are obviously longer, but the nodes far from the base station die prematurely because of the excessive energy cost caused by the communication between the nodes and the base station.

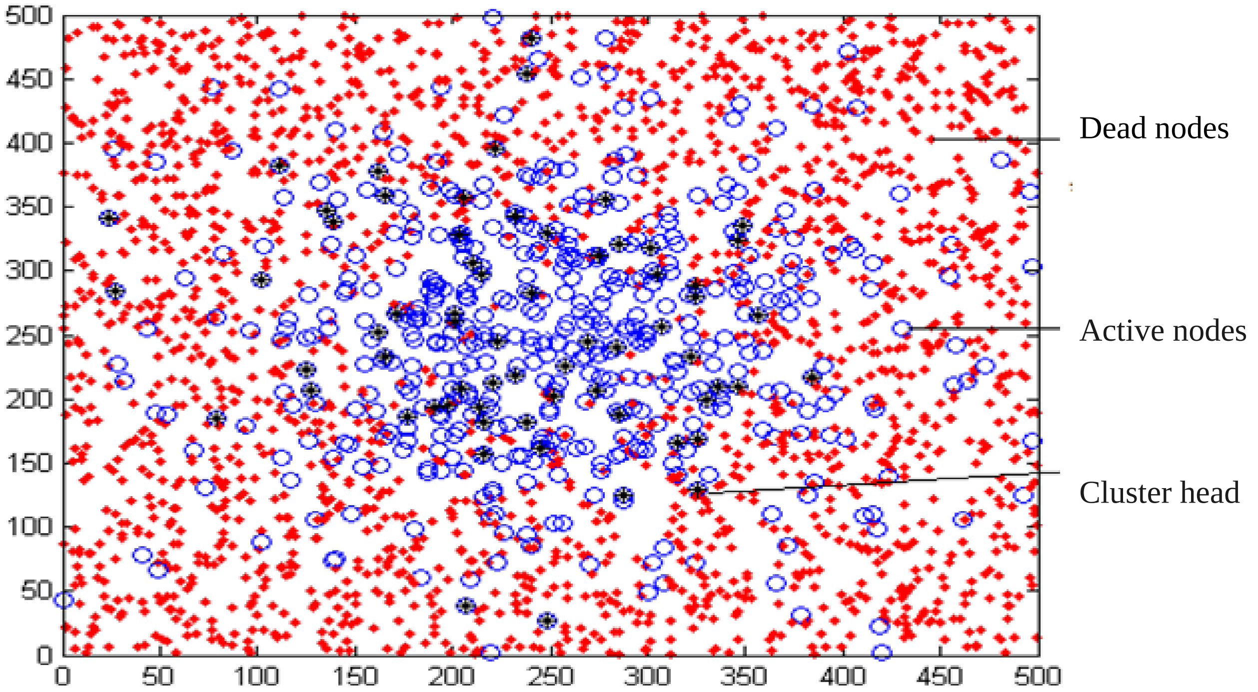


Figure 2.10 Network topology at round 400 in a region set at 500m*500m

However, if the base station is on the edge of the sensor nodes and the sensor nodes are in a wide range. The question which needs to be researched is “How to improve LEACH to be more suitable for current networks

2.8 Swarm intelligence and clustering algorithm

Swarm Intelligence (Swarm Intelligence, SI), is no intelligence or a simple intelligent individual without a centralized control case, by the simple act of a single individual, making the entire group exhibit some intelligent behavior, so as to solve some specific problems. Mark Millonas proposed to build a SI system which would meet five basic principles [97,98].

1. Proximity principle (Proximity Principle): the group of individuals can obtain information on the surrounding environment or an individual has the ability to be able to evaluate and execute a simple calculation on time or space;

2. Quality Principle: the group of individuals can respond to changes to key factors of the environment (Including other individuals within the group);

3. Principle of Diverse Response: different individuals in the group have different changes in response to the behavior exhibited by the diversity within the group;

4. Stability principle: not every change in the environment would lead to changes in behavior patterns of the entire group;

5. Adaptability Principle: environmental changes that occur in the event of changes in population worth paying opportunities, groups must be able to change their behavior patterns;

The ideas presented in SI provided a basic method to complex distributed problems in which there is not centralized control and does not provide a global model.

2.8.1 PSO's basic principles and mathematical models

Proposed Particle Swarm Optimization (PSO),[99,100] by Dr. Eberhart and Dr. Kennedy, is based on iterative optimization tools, the system is initialized within a group of random solutions, through an iterative search it finds the optimal solution.

1. The basic principles of PSO

Assuming a scenario as follows:

(1) A flock of birds in a random search for food.

(2) In this situation there is only one piece of food in the area.

(3) All the birds do not know where the food is.

(4) All the birds know their current location and how far away from the food they are.

The basic PSO algorithm, each optimization problem is a bird in the search space, called "particle." All particles have an optimized adaptation value (Fitness Value) function to determine, each particle has a flying speed and can determine their direction and distance. The particles follow the optimal particle current search in the solution space. Reynolds study found that birds flying only use a limited number of neighbors to track it, but the end result is the whole flock seems under control by a center, that complex global behavior is caused by the interaction of simple rules.

2. PSO mathematical model

Basic PSO algorithm is based on the parallel optimization to search technology. The population (Swarm) is constituted by the number of particles and the particles are known as population size or scale (Swarm Size). Each particle has a position vector and velocity vector, their number represents the number of problem solution space. If it is assumed that the search space is a problem in dimensional space, the position vector and the particle velocity vector as shown in Equation (2-7), (2-8), the position where the component represents dimensional position, vector represents the velocity vector the dimension velocity component.

$$X_i = [x_{i1}, x_{i2}, ..., x_{id}] \qquad (2\text{-}7)$$

$$V_i = [v_{i1}, v_{i2}, ..., v_{id}] \qquad (2\text{-}8)$$

The basic PSO algorithm initializes a group of random particles (random solutions), each particle "flies" in the search space through iterations to find the optimal solution. In the iterative process, the particles, by tracking, adjust their position to be updated by two "extremes" constantly. One extreme is the optimal solution found by the particle itself, this solution is called "individual extreme" or individual optimal solution, the individual particles of the extreme is $P_i = [p_{i1}, p_{i2}, ..., p_{id}]$; the other extreme is the entire population which currently has an optimal solution $P_g = [p_{g1}, p_{g2}, ..., p_{gd}]$, becomes global minimum or global optimal solution, they then find the optimal values of these two particles (2-9, 2-10) to update their velocity and the new position according to the formula:

$$v_{ij}(t+1) = wv_{ij}(t) + c_1 r_1 [p_{ij}(t) - x_{ij}(t)] + c_2 r_2 [p_{gj} - x_{ij}(t)] \quad (2\text{-}9)$$

$$x_{ij}(t+1) = x_{ij}(t) + v_{ij}(t+1) \quad (2\text{-}10)$$

$$1 \le i \le n, 1 \le j \le d$$

Where, c_1、c_2 are positive constants which is called the acceleration factor; r_1、r_2 are random numbers between $[0,1]$; w is called inertia factor. $j\ (1 \le j \le d)$ changes in the scope of the position $[-x_{j,\max}, x_{j,\max}]$ and velocity range $[-v_{j,\max}, v_{j,\max}]$, respectively, and the dimension (range translational processing by adding symmetry), iteration, if x_{ij} or v_{ij} is beyond their border, and or take the boundary values. The initial position and velocity of the particle swarm generates a random number, and then the formula (2-9, 2-10) to iterate until the condition is satisfied.

As shown from equation (2-9), the three factors represent the three parts of the particle velocity update.

(1) The first part reflects the influence of the next iteration, contacting the particles current state, combining inertial particle performance, the particles ability to balance global and local search. Therefore, it is called the inertia factor.

(2) The second part reflects the understanding of the particles “own experience", namely the impact of the particles memory, this part of the particles has a global search ability, to avoid falling into local minutia. Thus Venter and Socbeiski also defined this as "self-awareness” “(Self-Confidence)".

(3) The third part reflects the entire population of the "social experience”, this part helps to improve the global search ability of the particle, and therefore of the iterative process before considering the entire populations’ collective "experience", Venter and Socbeiski also define this as (Swarm-Confidence)".

At present, all particles are divided into several parts in the basic PSO algorithm, the particles are overlapping with neighbor particles, where the "neighbors" does not general position of the particle based Euclidean distance exhaustive, but rather refers to the number of particles adjacent to the neighbor relationship and this iterative process is typically remain unchanged. So each particle P_i and the neighboring historic optimal subgroups adjust their positions $P_l = [p_{l1}, p_{l2}, ..., p_{ld}]$, that formula (2-9, 2-10) exchanges according.

The basic PSO algorithm processes are shown as follows:

Begin

(1)The initialization of various random group velocities and the position of each particle;

(2) Calculate the fitness function of particles. The position of each particle and the fitness function are stored in an individual, the most optimal value of fitness function and position are stored in the global variable

While （Abort condition is not satisfied）do

According to the formula (2-9) and (2-10), Update the velocity and position of particles:

If the fitness value of particle is better than the current value ， updated to the current value of the current position and particle fitness function; If the particle fitness value than the current global values, with fitness function optimal particle position update global values;

End while

End

2.8.2 ACO's basic principles and mathematical models

Ant colony optimization (Ant Colony Optimization, ACO [101, 102]) algorithm is called the ant colony algorithm. It is proposed by Colorni, Dorigo and Maniezzo. The basic principle is analyzed based on a mathematical model.

1. Ant behavior description

Ants, although not communicating visually, are able to communicate. They release special secretions (Pheromones) along their path - to find their way [102].When they encounter an intersection which they cannot pass, they select a random path, and release (information) on the path. The longer the path of the ants, the smaller the amount of information is released. When the ants come again across this intersection, a larger amount of information on the path is secreted, thus a positive feedback mechanism is formed. The amount of information on the optimal path always grows, but the amount of information on other paths wills gradually abate. Ant colonies will eventually find the optimal path. Meanwhile the colony is also able to adapt to changes in the environment. For instance, if suddenly there is an obstacle on the path, ants can quickly navigate and find the optimal path. Although the capacity of a single ant is limited, the entire ant pheromone behavioral system has a high level of self-organization, the exchange of information between the paths of the ants, and optimal paths are found. Figure 2-11 illustrates further the search principle of a colony.

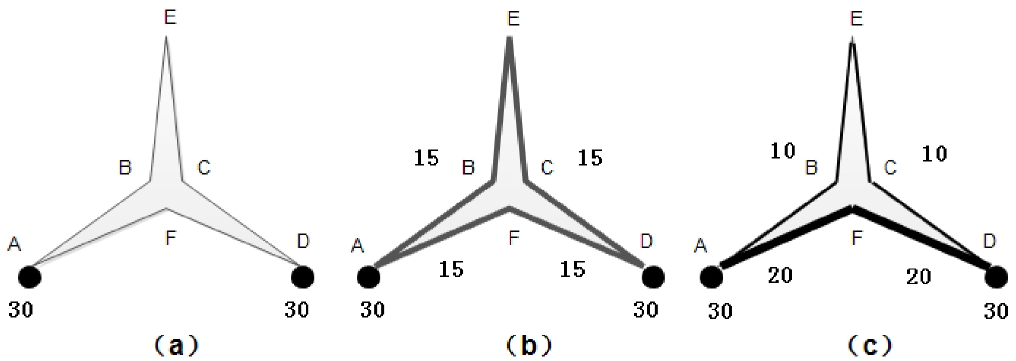


Figure2.11 Ant foraging Schematic

Figure 2.11, the set A point is a nest, D point is the food source, and the gray area of the triangle is an obstacle which cannot be passed. Because of the presence of obstacles, the Ant colony reaches D through E or F from A. The distance between the points is equal to that shown in Fig 2-11 (a).

Assuming that 30 ants reach point D from A, the amount of information is left as 1. For convenience, suppose the information residence time is 1unite time. In the initial moment, because no information exists on the path AB, BE, EC, CD, EC, AF, FD, located in A and D an ant can randomly select a path, from a statistical point of view and can be considered that an equal probability exists for ants to choose AB, AF, CD, FD, as shown in 2-11 (b), afteran unitnit of time, the amount of information in path ABECD, AFD path has two times the amount of information. After another period of time, there will be 20 ants who reached D from F, Fig 2-11 (c) shows, over time, more and more ants will probably select path AFD, eventually fully choosing path AFD, in order to find the shortest path from the nest to the food source.

2. The basic principle of the mechanism of ant colony algorithm

Simulated foraging behavior of an ant colony is a smart model. The algorithm is based on the following basic assumptions:

(1) Information and the environment are considered by communication between ant pheromones and each ant only responds to the local environment around them, they can only have an impact on its local surroundings.

(2）An ant’s response to the environment is decided by their internal model. Because ants are genetically modified organisms, ant behavior is actually an adaptive gene expression, that ants are reactive and adaptive.

(3) To a single ant, each ant is only making independent selections according to the environment; for the ant colony, they can form highly ordered behavior through self-organizational processes.

The above assumptions and analysis, the parade mechanism of a basic ant colony algorithm has two basic stages: adaptation stage and collaborative stage. In the adaptation phase, candidate solutions are continuously adjusted based on information accumulated in its structure, the more ants on the path leave a greater amount of information, so the paths are selected more; the amount of information that will decrease over time. In the collaborative stage, candidate solutions are produced through informational exchange. It is similar to the mechanism of automatic machine learning.

Self-organization mechanisms of ant colony algorithms are a dynamic process of entropy increase which is not affected by outside influences, the dynamic evolution is from disorder to order, its logical structure is shown in Figure 2.12.

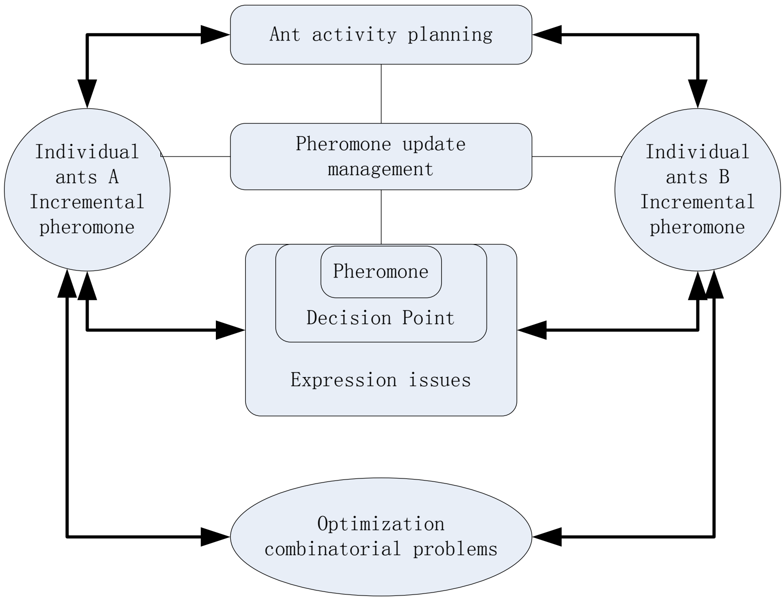


Figure 2.12 The logical structure of the basic ant colony algorithm

2. ACO mathematical model

Assuming that $b_i(t)$ is the number of ants at time t for element i ,the $\tau_{ij}(t)$ is the amount of information in t time on the path (i, j) , said scale TSP, the n is total number of ant colony, then; $m=\sum_{i=1}^{n} b_i(t)$ is $\Gamma=\{\tau_{ij}(t) | c_i, c_j \subset C\}$ the residual amount of information l_{ij} on the connection between two congregate city C at the t time . In the initial moments, the amount of information h is equal to each path and set up $\tau_{ij}(0)=const$, the basic ant colony is implemented by a directed graph $g=(C, L, \Gamma)$.

Ants $k(k=1,2,...,m)$ determine their transfer direction during movement according to the amount of information on each path. Taboo table $tabu_k(k=1,2,...,m)$ record the ants k with the currently traversed the city, their $tabu_k$ makes adjustments according to a dynamic evolutionary process. In the search process, the transition probability of ants is calculated based on the amount of information and the information of each path. $p_{ij}^k(t)$ is transition probability of element at the time from the elements (city) i to the element (city) j.

$$p_{ij}^k(t)=\begin{cases}\dfrac{\left[\tau_{ij}(t)\right]^{\beta} g[\eta_{ik}(t)]^{\beta}}{\sum\limits_{s\subset allowed_k}[\tau_{is}(t)]^{\alpha} g[\eta_{is}(t)]^{\beta}}, & if \quad j\in allowed_k \\ 0 \quad else & \end{cases} \qquad (2.11)$$

In formula (2.11), which $allowed_k=\{C\text{-tabu}_k\}$ allows the selection of the next city for ant k, α is a heuristic factor, it indicates the relative importance of the track, the larger the value is, the stronger the collaboration between ants; The more ants tend to choose the path that other ants travel; β shows the relative importance of visibility, reflecting the ants heuristic information in motion the process to select the path in the ant the degree of attention, the greater its value, the state transition probabilities closer greedy rule; $\eta_{ij}(t)$ as heuristic function, its expression is as follows

$$\eta_{ij}(t)=\frac{1}{d_{ij}} \qquad (2.12)$$

In the above formula, d_{ij} means the distance between the two adjacent cities. Ants k, the smaller d_{ij} is, $\eta_{ij}(t)$ and $p_{ij}^k(t)$ are greater. Obviously, this heuristic function, said the desired level which ants moved from i the elements (city) to the element (city) j the desired level.

In order to avoid submerged remnants heuristic information by too much residual pheromone, or at the completion of each ant has completed step traversal of all cities n (ie, the end of a cycle), the information should be updated to deal with the residue. This update strategy mimics the characteristics of the human brain memory, stored in the information system of the brain, while constantly on the information stored in the brain gradually fade over time, or even forgotten. Whereby the amount of information according to the following timing $t+n$ rules on the adjustment path (i, j)

$$\tau_{ij}(t+n) = (1-\rho)g\tau_{ij}(t) + \Delta\tau_{ij}(t) \qquad (2.13)$$

$$\Delta\tau_{ij}(t) = \sum_{k=1}^{m} \Delta\tau_{ij}^{k}(t) \qquad (2.14)$$

Formula (2.13, 2.14), ρ indicates pheromone evaporation rate, $1-\rho$ taking into account the residual pheromones, in order to prevent the accumulation of information which has no limit, the ρ range is $\rho \subset [0,1)$; $\Delta\tau_{ij}(t)$ is pheromone increments on the cycle path (i, j), $\Delta\tau_{ij}(0) = 0$ is the initial time, which $\Delta\tau_{ij}^{k}(t)$ means the amount of information on the first path left ant k in this cycle (i, j).

Depending on the pheromone update strategy, Dorigo M presents three different basic ant colony algorithm models [98], referred to as Ant-Cycle model, Ant-Quantity Model and Ant-Density model, the difference lies in the different methods of seeking $\Delta\tau_{ij}^{k}(t)$.

1.In Ant-Cycle model

$$\Delta\tau_{ij}^{k}(t) = \begin{cases} \dfrac{Q}{L_k} & \text{the ant } k \text{ in cycle (i, j)} \\ 0 & otherwise \end{cases} \qquad (2.15)$$

2. Ant-Quantity model:

$$\Delta\tau_{ij}^{k}(t)=\begin{cases}\dfrac{Q}{d_{ij}} & \text{the ant } k \text{ in cycle (i, j) form t to t}+1\\ 0 & otherwise\end{cases}\tag{2.16}$$

3. Ant-Density model:

$$\Delta\tau_{ij}^{k}(t)=\begin{cases}Q & \text{the ant } k \text{ pass (i, j) form t to t}+1\\ 0 & otherwise\end{cases}\tag{2.17}$$

Q is pheromone intensity, which affects the degree of convergence of the algorithm to a certain extent; L_k is ant k in this cycle as the total length of the path to go.

The difference between formula (2.15) and (2.16) (2.17), (2.16) and (2.17) are use of the local information, i.e., after the completion of the ant pheromone update path; the formula (2.15) is the overall utilization of the information, i.e., after the completion of a cycle Claim ant pheromone on all paths, better performance when solving TSP, so the commonly used formula is (2.15) as the basic model of ant colony algorithm.

2.9 Advantages of application of PSO and ACO in WSN

2.9.1 Advantages of application of PSO in WSN

There is growing concern about the application of PSO in the field of combination, optimization and network routes [103][104]. PSO is a swarm intelligence optimization algorithm simulating intergroup social behaviors of birds in the natural world and seeking optimal solutions through mutual cooperation among individuals. Due to the maturity, simple realization, good self-organization and adaptation of the PSO algorithm, it shows a strong vitality and potential in some classical combination optimization problems and routing problems. Compared to traditional optimization algorithms (such as linear programming and dynamic programming), it has the following characteristics:

1. All particles preserve the relevant knowledge of the optimal solution. In an environment with uncertainty, individuals constantly improve their own adaptability through learning and adapt to the environment better through cooperation and have good adaptation and self-organization.

2. Potential concurrency greatly improves the efficiency of searching and rate of convergence;

3. The algorithm has a strong applicability and effectiveness and good robustness in different environments.

Currently, PSO has been used in multicast routing and route optimization with QoS constraints. In WSN, PSO is mainly used in deployment optimization, network coverage and clustering routing optimization etc. Xue Wang, Jun-Jie Ma, Sheng Wang, and Dao-Wei Bi [105] puts forward a distributed energy efficiency coverage algorithm combining PSO and simulated annealing algorithm (SAA) which uses PSO and SAA to optimize energy consumption of SWN and obtain optimal deployment. The result shows that this distributed algorithm saves network energy after optimizing deployment. This algorithm improves network energy efficiency when applied in WSN target tracking. Santi P [106] puts forward a wireless sensor network routing algorithm based on effective avoidance of low energy or no energy areas PSO which converts routing problems to linear programming problems and uses PSO to solve the routing problem of low energy area avoidance on this basis. It has a good ability to adapt to any network deployment and meets the requirement of adapting to its environment. Hu et al. have proposed PSO-Traffic for topological planning for a real world traffic surveillance application [107]. Li et al. have proposed a mixture of stationary and mobile nodes and particle swarm genetic optimization (PSGO) as a remedy to coverage holes [108]. The PSGO hybrid is employed to determine redeployment positions of mobile nodes in order to improve average node density. Hong et al. have PSO Multi-Base for optimal positioning of multiple base stations in a two tier WSN

[109]. The two-tier network consists of nodes that can communicate only with the application nodes they are assigned to.

However, it is not applicable to networks with high requirements for real-time performance and its expansibility has certain limitations.

2.9.2 Advantages of application of ACO in WSN

Ant colony is a group composed of ant individuals with simple functions under certain rules. It is characterized by heuristic and distributed calculations etc [98].. Therefore, it is appropriate to use ant colony algorithms in routing algorithm design of WSN.

1. Individuals of ant colony algorithms only have simple functions, but can jointly complete complicated tasks according to simple rules. Therefore, it is feasible to use ant colony optimization algorithms to solve the design of WSN routing algorithms at this level.

2. Ant colony algorithm has a good superiority in solving dynamic problems. It completes a task through the work of each ant and their interactions. In the execution of ant colony algorithm, some individual factors will not influence optimal solutions. Other individuals in the group are not disturbed and operate according to predefined rules. Therefore, ant colony algorithm has a good ability to adapt to changes of network topology and can seek a new data path in a short amount of time.

3. Local work. Nodes in WSN only record relevant information of neighbor nodes. It is impossible to store the routing information of the whole network in each node. Traditional routing protocol is obviously not applicable to WSN. In network routing algorithms based on ant colony algorithm, each node achieves global routing through calculations and influence of local information.

4. Parameter association. In the design of network routing algorithms, part characteristic parameters of WSN such as link quality and residual energy of nodes and parameters in ant colony algorithm such as path pheromones, path distance and path

angle can be associated. WSN route selection can be realized through parameter matching of ant colony algorithm.

5. Multiple routing. Routing table of each node records the concentration of pheromones on the path with a neighbor node. Nodes select the next path through the use of a probability calculation based on the concentration of pheromones. The possibility of selection among multiple paths can be supported through parameter control. Routing designed with this idea has a good fault tolerance and stability of data transmission.

In recent years, the application of ACO in WSN routing has gradually become a hotspot:

Xin Guan, Guan L., Wang X.G., Ohtsuki introduces routing algorithms[110] based on ant colony system and uses multi-ant colony competitive mechanisms to solve the problem of energy balance and congestion control in the routing processes of WSN.

Ziyadi, M, Yasami, K., Abolhassani, B [111] uses adaptive clustering characteristics of ant colony to put forward a clustering protocol with energy awareness, which effectively reduces the energy consumption of data transmission and aggregation and greatly improves the network life cycle and energy consumption of data transmissions.

Salehpour A.A, Mirmobin. B, Afzali-Kusha A, Mohammadi S [112] puts forward an efficient WSN two-stage structural routing algorithm based on ant colony optimization. Member nodes in the first stage send data to cluster heads. Among cluster head nodes in the second stage, ant colony optimization algorithm is used to produce efficient routing. This algorithm has little delay and good performance in power consumption and load balance.

Ghasem Aghaei R. Rahman A.M. Rahman M.A, puts introduces the many-for-one data transmission routing protocol based on ant colony which generates the shortest path by using ant colony, implements congestion control mechanisms during many-for-one perception data transmission and reduces end-to-end time delay and loss of data package [113].

However, there are the following problems:

1. Single emphasis. Whether for clustering strategy or multi-hop routing, generally only one part is considered. For example, the research on multi-hop routing uses a simple clustering strategy, while the research on clustering neglects routing optimization.

2. Factors considered by clustering strategy are incomplete. Currently, many new ideas are introduced into the research on clustering strategy, such as solving “hotspot” problems based on graph theory and using non-uniform clustering thought, based on geographical location and energy awareness etc. However, these strategies generally only focus on considering some factors influencing clustering in WSN.

3. Clustering results mostly have randomness. Current clustering algorithms generally use the method of producing random numbers and setting threshold values to increase or decrease the weight of one or more factors determining cluster heads. Such cluster head selection is random and is not the optimal value.

4. The weight of each decision factor is not analyzed in detail when PSO is used to obtain the optimal cluster head. For example, in research using PSO to improve clustering algorithms such as literatures [113], they generally take the same value for the weight of each decisive factor or give a subject value.

2.10 Support QoS’ route and MAC protocol

Quality of Service (QoS, Quality of Service) is a comprehensive evaluation of the communication system; QoS can reflect a reasonable degree of distribution of network resources and information services strength for a communication system to carry. The definition of QoS in RFC2386 [114] (Request for Comments) is: QoS refers to a series of service requirements when transmitting the data stream in the network. Typical QoS parameters include delay, bandwidth, hops, packet loss rate and delay jitter.

2.10.1 Design requirements for ADHOC network QoS routing protocol

Adhoc is a self organization network, the following are requirements [115]:

1. Quick route discovery, because the network nodes have mobility characteristics, when moved to the network nodes, routing protocols should be able to protect the node and quickly establish communication with the network routing;

2. QoS parameter reasonable selection, the parameters should select the appropriate evaluation to optimize allocation of limited resources for different network environments

3. Algorithm is feasible for multi-index constraint routing strategy, processing algorithms should be able to draw meaningful optimal executable programs.

4. The routing protocol can perceive any dynamic changes in the network topology.

5. Low Bandwidth, ADHOC network bandwidth resources are limited, protocols should be compressed as much as possible to eliminate unnecessary overhead, using lower bandwidth resources;

6 .To reduce the overhead of host resources, ADHOC network nodes should be able to reduce the routing protocol transmission time and data transfer times while the use of efficient routing algorithms, reduce CPU overhead, memory and other resources;

2.10.3 Typical QoS routing protocols in ADHOC Network and Performance Analysis

Typical QoS routing protocols in ADHOC Network and Performance Analysis are researched by IETF MANET working group. Typical QoS routing protocols are described as follows:

1. P.Gupta, P.R.Kumar proposed STARA（system and traffic dependent adaptive routing algorithm)[116], it is a protocol with a minimum average path delay time as the QoS parameter index, is a table-driven proactive routing protocol. Each node needs to

periodically update the routing tables of the nodes and to have higher storage capacity requirements,

2. Anelise Munaretto, Hakim Badis proposed LS-QoS (Link State Base QoS Routing) [117]. The protocol selects routes by using the parameter of average survival time of the route and packets error rate. Network nodes periodically broadcast link state data to calculate the survival time, communication link and packet error rate, the routing table is in a dynamic state of adjustment. The protocol requires resources to periodically maintain link data, increasing the routing overhead and energy consumption of nodes and the need to take up storage space to save the link packet error rate and link lifetime.

3. Shigang Chen,Klara N proposed TBP（Ticket-Based Probing）[118].This protocol selects routes by the delay, bandwidth cost, it belongs to on-demand QoS routing protocol. The protocol dynamically changes the routing table by sending a number of packets (exploring packages) from the source node to the destination node. Each packet arrives at an intermediate node, according to the link status information and the neighbor status, the protocol determines the path to explore and discover the packet routing. If the exploring package finally reaches the destination node, the routing meets the QoS requirements of the path, the packet is sent by the destination node along the path in the reverse direction of resource reservation. If the source node does not receive the resource package, it indicates the establishment of QoS routing failure.

4.SHI JIAN, ZOULING proposed LBRM（Local Broadcast Routing Message）[119]. The protocol is a protocol which selects routing by delay, bandwidth and QoS parameters as indicators of cost, it is designed based on the TBP protocol, and belongs to on-demand QoS routing protocol. LBRM dynamically changes due to changes in network topology. The protocol applies changes slowly in the network topology.

5.Chenxi Zhu, M. ScottCorson proposed QAODV [120], the routing protocol selects the bandwidth of the QoS parameters as indicators, through improvements to

AODV protocol; it is also a flat-demand routing protocol. The protocol effectively reduces network latency and increases network throughput, mainly used in small-scale low-speed mobile networks.

6.Huangc, DA IF, WUJ proposed LTBR (Location-Aided Ticket-Based QoS Routing) [121], the protocol selects delay, bandwidth and QoS parameters as indicators of cost; it is a flat-demand routing protocols. The protocol is similar to the TBP protocol. Only the path information is a binding agreement in the choice of location information of nodes, effectively reducing the length of QoS routing.

7.Sivakumar, R.; Sinha, P.; Bharghavan, V. proposed CEDAR (Core Extraction Distributed ADHOC Routing)[122],the protocol is an on-demand hierarchical routing protocol with bandwidth. The protocol introduces the concept of core nodes to build a network through a core node, mainly used for small and medium ADHOC networks.

8. Prasun Sinha , Raghupathy Sivakumar , Vaduvur Bharghavan proposed MCEDAR (Multicast Core Extraction Distributed ADHOC Routing)[123] protocol is a protocol extension which comes from CEDAR, it still uses bandwidth as the QoS parameter index, and it is a hierarchical routing protocol. Through the expansion of the multicast protocol it establishes a hybrid multicast structure.

9. Wang jianxin, et al proposed QRME (QoS routing protocol based on maximum expiration time) [124], the protocol selects the maximum connection time as a parameter indicator. Mobile node location information is located by GPS and mobile information. It can effectively reduce the time and cost of connection establishment.

10、Li Layuan, Li Chunlin proposed HQMRP (Hierarchical QoS Multicast Routing Protocol) [125], the protocol selects delay and bandwidth as the QoS parameter indexes. It is a clustering, structure-based QoS multicast routing protocol which exchanges routing information between cluster head nodes by each cluster, the cluster node only needs to maintain routing information within the cluster. The protocol needs to consume some energy and take up some storage space.

Characteristics of each QoS routing protocol are shown in Table 2-2. According to Table 2-2 QoS analysis and comparison of various routing protocols, it shows that demand distributed QoS routing protocols direct its development, with the size of the structure, according to ADHOC network it can be used separately in plane distribution and hierarchical structure and relatively large network for general use clustering network topology. Referring to the different network application services, you can select different QoS parameter index routing protocols.

There are many routing protocols to support QoS, but most of the existing protocols usually use a single criterion based on node energy, bandwidth and delay QoS indicators. In this thesis, the average delay link, the average packet loss rate and signal strength indicators have been chosen as the node QoS parameters, to select the optimal route to meet specific requirements.

Table 2-2 Comparison of routing protocols

Protocol	Support Multicast	Active / demand	QoS	Distributed Operation	Network Topology
STARA	NO	Active	Delay	Yes	Flat
LS-QoS	NO	Demand	Packet rate, Survival time	Yes	Flat
TBP	NO	Demand	Delay, Bandwidth	Yes	Flat
LBRM	Yes	Demand	Delay, bandwidth	Yes	Flat
QAODV	NO	Demand	Bandwidth	Yes	Flat
LTBR	NO	Demand	Delay, bandwidth	Yes	Flat
CEDAR	NO	Demand	Bandwidth	Yes	Hierarchical
MCEDAR	Yes	Demand	Bandwidth	Yes	Hierarchical
QRME	Yes	Demand	Maximum connection time	Yes	Flat-based routing
HQMRP	Yes	Demand	Bandwidth, Delay	Yes	Hierarchical

2.10.4 Introduction to Embedded Linux routing modules

Linux operating system has powerful network functions, including network routing modules. Routing Linux kernel supports rule-based strategy [126,127], the rules include two selectors and an action: a selector chooses the format of the packet, including the source address, destination, Type of Service(TOS), etc.; while the action is defined by a specific treatment according to selector conditions. The action of core is divided into 5 classes: UNICAST, BLACKHOLE, UNREACHABLE, PROHIBIT and NAT. UNICAST which represents a routing table entry from the routing table; BLACKHOLE Drops packets; UNREACHABLE reports that the destination network is unreachable; PROHIBIT prohibits access; NAT expresses address translation. In addition, the network can match the kernel and creates three rules for all packets: local_rule (local rule), main_rule (main rule), and default rule (the default rule). The rule-based routing mechanism kernel shown in Figure 2-13, is set in accordance with local rules, custom rules, the main rule, the default rule followed by the implementation of the order.

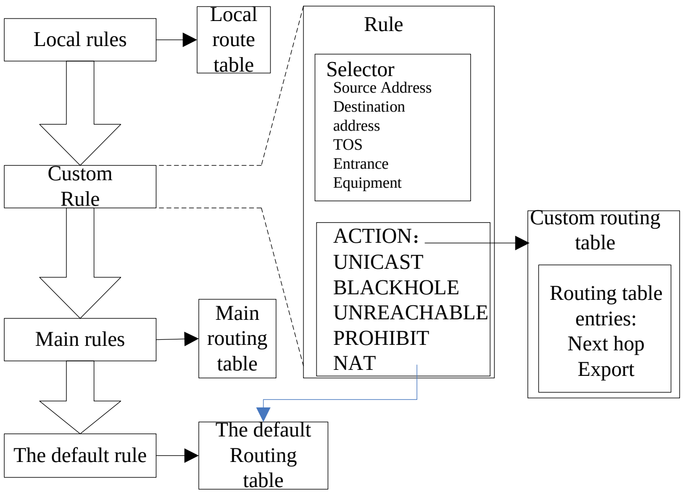


Figure 2-13 Rule-based routing mechanism

Rules for routing table management and routing table entries, Linux kernel provides a network interface to handle Net link rules in Net link mechanisms, and the routing information is related:: RTM_NEWRULE, adds routing rule entries; RTM_DELRULE, deletes the entries of a routing rule; RTM_NEWROUTE, adds a routing table entry; RTM_DELROUTE, deletes a routing table entry.

This technology provides a basis for achieving self-developed protocols on Linux-based embedded systems.

2.10.5 MAC Protocol of WSN to support QoS

The medium access control (MAC) is responsible for the resource distribution of the channel. The MAC can be classified into the time division multiple access, frequency division multiple access, and coding division multiple access. Another method is competition access control and the other types [128].

For WSN, MAC protocol has three reasons to cause energy consumption. The first reason is the collision. When a transferred data packet is abandoned because of the channel competition or transmission damage, the following re-transmission will increase the loss of energy. The second reason is the listening. A node listens if other nodes are sending the data. Listening will cause energy loss. The third reason is the energy cost of the control message.

The Time Division Multiple Access (TDMA) [129] distributes the individual data sending and receiving by time slot for the wireless sensor node. The data transmission does not need too much control information; the node can fall asleep in the free time slot. These characteristics make the WSN with TDMA mechanism avoid energy waste. Based on the applications of the wireless sensor, the ideal TDMA MAC protocol can be classified into the clustering networks based on TDMA type MAC protocol, DEANA protocol [130], TRAMA protocol [131] and DMAC [132], etc. However there are still some disadvantages in the TDMA mechanism, such as the strict time synchronization and the poor network scalability.

The competition-based MAC protocol uses the channel according to its needs. A node needs to use the channel by the competition to send the data. The sent data must be resent if a collision happens until the data is sent successfully or the data is abandoned directly. The typical competition-based MAC protocols are IEEE802.11 MAC protocol [133], S-MAC [23], T-MAC protocols [134] and so on.

Aiming at the shortfall of S-MAC protocol on the fixed duty cycle, the T-MAC protocol makes improvements. It adjusts activity time dynamically according to traffic on the basis of remaining the cycle’s length and sends messages with a burst mode, thus reducing idle listening time [135].

Sift protocol [136] is a MAC protocol based on the competition and oriented sensor networks aiming at even-driving. The main idea of this protocol is to use a fixed backoff window, and select the appropriate transmission probability distribution for nodes in different time slots, so that detecting a plurality of nodes that in a same event can send messages without collision in the time slots before the contention window. But it suffers from increased idle listening and system-wide time synchronization, which reduces its energy efficiency.

With the wide use of wireless sensor networks and the diversification of user needs, more and more services need adaption and satisfaction. In the case of an accident, fire, destruction of public facilities and other unexpected incidents, users expect the time-sensitive important information to be able to be transmitted to the sink node immediately.

S-MAC protocol makes use of the periodically monitoring / sleep mechanism and collision and crosstalk avoidance mechanism to reduce energy consumption. The protocol is to reduce energy consumption and to support a good scalability and collision avoidance. However, the S-MAC protocol uses the solid frame length and duty cycle. The frame length is limited by the delay requirement and the size of the cache. The active time of the nodes relies on the rate of the message. When the network load is very small, the long time of free monitoring will lead to serious transmission delay. Thus, the S-MAC is not suitable for the applications of the high requirement of real-time. It cannot identify the priorities of the transaction and it cannot supply the different access mechanism for the different transactions. Thus, under the conditions of limited channel, the S-MAC cannot guarantee that the data with high priority has the superiority in the channel competition, and it cannot ensure the timely and effective transmission of the important transactions.

2.11 Summary

1. When the sensor nodes are deployed in a widely range, LEACH protocol needs to be improved to ensure network performance, this is an issue to be studied;

2. Particle swarm and ant colony algorithm in line with the characteristics of WSN. Taking into account the combination of clustering and routing, PSO applied to the ant colony clustering and applies to routing and clustering considered together with route optimization to achieve improved routing algorithms for WSN research content.

3. There are a variety of supported QoS routing protocols. The actual development of the route requires practicality. The special focus of this study is how to design protocols for resource-constrained embedded systems.

4. S-MAC protocol widely used in the wireless sensor networks is unable to meet service differentiation. Due to the lack of S-MAC protocol, there is a need for improvement to satisfy distinct transmission services based on service differentiation in wireless sensor networks.

Chapter 3 RBLEACH PROTOCOL

As discussed in Chapter 2, analysis for LEACH protocol, cluster heads are selected according to random numbers, but communication cost and residual energy of cluster nodes are not considered, the nodes whose remaining energy the lowest can still be selected as the cluster heads, which means their lifetime is short; the network nodes are farther away from the base station which means the communication cost is more, resulting in unbalanced energy consumption; in the data transfer phase, due to data integration and data forwarding，nodes who consume more energy have an early death. LEACH is not suitable for wide areas. This thesis proposes RBLEACH protocol for widely area.

3.1 Assuming the network parameters

In this project, there is a scene, where a lot of sensors are distributed on a wide area and the Base Station is in the corner of the area, as Lake monitoring network.

The network model used is the same as in LEACH. It only limits region, which the nodes are randomly distributed in the square, BS is located at one end of the rectangle, according to the assumption §2.61. The network parameters are show as follows:

1. N nodes randomly distributed inside the area Q, Q is square (b*b).

2. The nodes are homogeneous, meaning nodes have the same initial energy, independent of the choice the communication distance.

3. The cluster heads can merge data according to data fusion rate δ .

4. The nodes are fixed and they can automatically constitute networks without artificial help.

5. There is only one Base Station (BS) in the whole network; BS is located at one end of the rectangle.

6. A node knows the relative distance between itself and the other nodes (including the base station).

7. There is a network synchronization clock; each sensor node senses the monitoring parameter of the surrounding environment at a constant rate.

8. Electromagnetic waves are transmitted by a first-order radio model (2.2)and (2.3), assume the distance is $d < d_0$

$$E_{Tx}(k,d) = E_{elec}k + \varepsilon_{amp}kd^2 \quad …….(2\text{-}2)$$

$$E_{Rx}(k,d) = E_{elec}k \quad (2\text{-}3)$$

3.2 Define divided area

Taking the location of the Base Station as the center of coordinate, sensors are distributed a rectangle on the first quadrant. The quadrant will be divided into arc areas by the radius $R_i = An_i$, as shown in Figure 3-1, which A is the unit length split from side b.

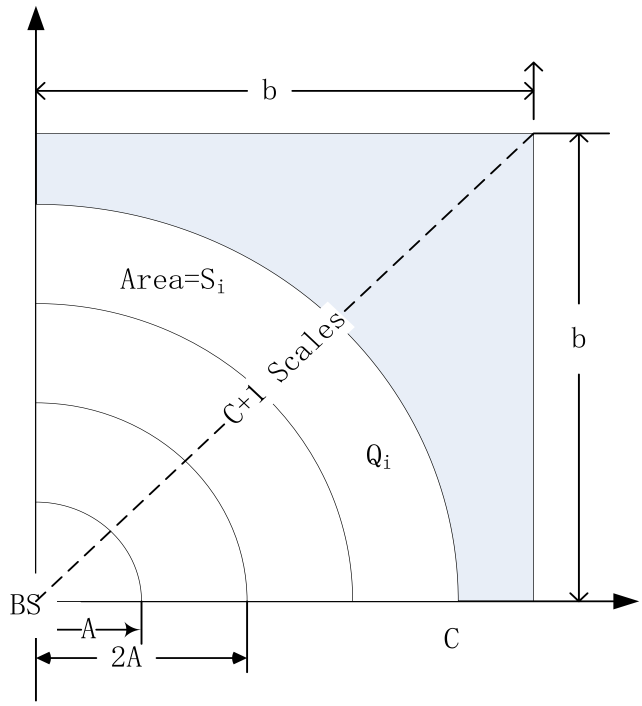


Figure 3.1 Divided areas

$n_i = 1,2,3.....C \quad 0 \le R_i \le b$ (3-1)

Shown in Figure 3.1, the entire network area is divided into $C+1$ region:

$C = \lceil b/A \rceil$ (3-2)

Q_i is i_{th} region which is divided.

$Q_i \in Q$

$Q = \sum_{i=1}^{C+1} Q_i$,

$S_i = \pi(R_{i+1}^2 - R_i^2)/4 \quad (i \ne C)$ (3-3)

$S_i = b^2 - \pi R_c^2 / 4 \ (i = C)$

The distance between a node to the Base Station in region i is r_i in Q_i,

$R_i \le r_i \le R_{i+1}$

Definitions:

$\overline{R_i} = \frac{R_{i+1} + R_i}{2}$ (3-4)

N_i is the number of the The distance between a node to the Base Station in region nodes in Q_i

3.3 Define the number of cluster heads assigned

3.3.1 The Energy Consumption Calculation

As shown in figure 3.1,

N_CH_j is the number of the cluster heads in Qi

($j = 1,2,3....$)

In regional $i = 1$, the nodes are directly connected to the base station;

$N\_CH_j^{'} = 0$

2. $i \geq 2$, cluster heads has N_CH_j

Consider the energy consumption of the nodes when data is transmitting, the energy consumed by the power amplifier and receiving data according to (2.2)

The average number of nodes is $N_i / N\_CH_j - 1$ except cluster head in a cluster,

Each cluster members to send 1bit data in one round, a k data fusion energy consumption is E_{DA}, Data fusion rate is η, When the data need to transmit, The amount of data after fusion is:

$$K = \eta * k * N_i / N\_CH_j \tag{3-5}$$

Then the energy consumption of the cluster head in a round is

$$E_{CH} = k * E_{elect} * (N_i / N_{i\_}CH_j - 1) + k * E_{DA} * N_i / N_{i\_}CH_j + K * E_{elect} + K * \varepsilon_{amp} * R_{toBS} \tag{3-6}$$

Then the energy consumption of the cluster number in a round is

$$EN_{NO\_CH} = KE_{elect} + K * \varepsilon_{fs} * R_{toBS} \tag{3-7}$$

The total energy consumption of cluster nodes and the cluster head is

$$E_{total} = \sum_j N_{i\_}CH_i * \{E_{CH} + (N_i / N_{i\_}CH_j - 1) * E_{NO\_CH}\} \tag{3-8}$$

The average size for each cluster node is $\frac{S_i}{N_{i\_}CH_i}$, Node density $\rho = \frac{1}{S_i / N_{i\_}CH_i}$

(3-9)

The Mathematical expectation of the square of the distance between and BS is

$$R_{toBS} = \iint r^2 \rho(r,\theta) d\theta dr$$

$$0 \leq \theta \leq \pi/2, \quad An_i \leq r \leq An_{i+1} \tag{3-10}$$

The expectation square distance from node to the cluster head is :

$$E(R_{toCH}) = \iint \rho r^2 dr d\theta = \frac{S_i}{8\pi N_i\_CH_j} \qquad (3\text{-}11)$$

Combining (2.2), (3-11) and (3-8),

$$\frac{\partial E_{total}}{\partial N_i\_CH_j} = 0 \qquad (3\text{-}12)$$

The optimal number of cluster heads:

$$N_{i\_}CH_{jbest} = \frac{\sqrt{N_i}}{4\sqrt{2\pi}}\sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{amp}}}\frac{\sqrt{S_i}}{R_{tobs}^2} \approx \frac{\sqrt{N_i}}{4\sqrt{2\pi}}\sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{amp}}}\frac{\sqrt{S_i}}{R_i^2} \qquad (3\text{-}13)$$

3.3.2 Energy Monitoring

After the first cluster head is selected based on region, for the region Qi , each round, the sink node will calculate the remaining average energy of each cluster

Assuming there are numbers of cluster heads $N\_CH_j = l$

Assuming the residual energy of each cluster is:

Definition：

$$E_{avgi} = \frac{E_{avgi1} + E_{avgi2} ..... + E_{avgim}}{l} \qquad (3\text{-}14)$$

E_{avgi} Represents the remaining energy in the region Qi

3.4 Cluster head selection

3.4.1 Energy parameters

In order to make the nodes with the highest energy be elected as the cluster head, thus introducing energy parameters:

Definition:

E_{ij} Is the remaining energy of j node in Q_i, its normalized value of the remaining energy.

$$\beta_j = \frac{E_{ij}}{E_{avgi}} \qquad (3\text{-}15)$$

Definition:

The relative distance from the node to the base station

$$R(i) = 1 - \frac{\overline{R_i}}{\sqrt{2}b} \qquad (3\text{-}16)$$

3.4.2 Selected the cluster head

Cluster head Selection is based on two things: First, the optimal number of nodes in the network, Second the number of nodes in the front wheel in the diagram n was selected as cluster head.

That is, each node according to a formula (3-17). The first round of random r calculated values associated with the energy and the distance of the value between 0-1.

Definition: The cluster head selection

$$TQ_i = [\alpha_1 \beta_i + \alpha_2 R(i)] * [\frac{p}{1 - p(r \bmod \frac{1}{p})}] \qquad (3\text{-}17)$$

Is the corresponding weight value α_1 *and* α_2

$(\alpha_1 + \alpha_2) = 1$

TQ_i is calculated and arranged $\alpha_1 > 0, \alpha_2 > 0,$ by order of size, G is a node set which has not been selected in the cluster head which determines the number of clusters by format.

3.5 The formation of clusters

After the selection of the cluster head, the cluster N_CH_j head broadcasts “SMS” to all nodes using MAC protocol of CSMA.

N_j is the nodes in Q_i

If

$E_{Rx_j}(L, d_j) = E_{elect} L \le E_{RThreshod}$,

Node N_i belongs to the i cluster

If N_i is at the boundary of Q_i and Q_j ,

If

$E_{Rx_j}(L_j, d) > E_{Rx_i}(L_i, d)$ N_i Belongs to the i cluster

$E_{Rx_j}(L_j, d) < E_{Rx_i}(L_i, d)$ N_i Belongs to the j cluster

Else if

$E_{Rx_j}(L_j, d) = E_{Rx_i}(L_i, d)$ Nodes can randomly select the i cluster or the j cluster.

3.6 Multi-hop data transmission among clusters

In the stage of data transmission of LEACH protocol, the communication between the head of cluster and base station is the single-hop, which is data transmission from each head of cluster to the base station. As shown in Figure 3.2, all the heads of clusters focus the data, which come from all member nodes in the clusters and transfer the data to the base station. However, it is obvious that this single-hop method does not work. The head of cluster far away from the base station needs to consume much energy to send the data to the base station, thus causing early death of nodes.

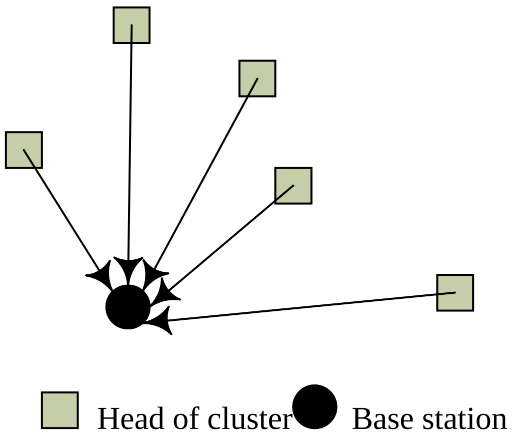


Figure 3.2 Single-hop of the head of cluster and base station

The single-hop does not work based on the analysis in Figure 3.2, so the multi-hops should be considered in RBLEACH. With the multi-hops, each head of cluster does not need to transfer the data with a long distance, and the energy cost of the sensor nodes can be reduced to elongate the life cycle of the networks. Thus, in this thesis, the multi-hops data transmission between the head of clusters is employed. The transmission between the sensor nodes is as shown in Figure 3.3.

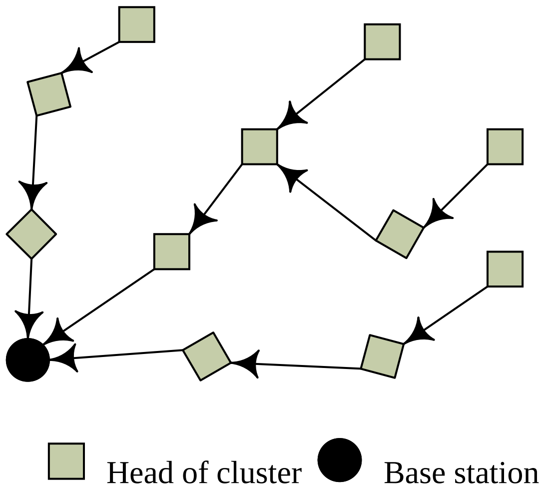


Figure 3.3 Transmission between multi-hops in the head of clusters

Compare Figure 3.2 and Figure 3.2, it is known that the data is not transferred to the base station directly from each head of cluster. The selected head of clusters in each round connects to each other to form a link with several branches. The data collected from each head of cluster is transferred and aggregated in this link. Finally, all the data is fused and aggregated, ready to be sent to the base station.

This thesis contributes the relative analysis based on following analysis:

In the process of data transmission, the table of all sensor nodes contains $T\left(T=M+K\right)$ time slots. Each node member (except the cluster head) transmits data collected to cluster head nodes at time slot $i\left(i\leq M\right)$. Cluster head nodes aggregate data received and then integrate them. At the former *M* time slots, the transmission of data in all clusters is completed. At subsequent *K* time slots, cluster head data is transmitted. Cluster head nodes integrate data received from other cluster head nodes and data saved by itself and send data obtained after integration to the next hop of cluster head nodes at time slot $M+j$ until all data in base station nodes is fully integrated.

The current cluster head maintains the energy list $\left\{E\left(CH_1\right),E\left(CH_2\right),\cdots,E\left(CH_m\right)\right\}$ of a neighbor cluster head, where refers to the residual energy of cluster head of the i^{th} cluster at the current moment. Assume that $CH_1,CH_2,\cdots,CH_m$ are neighbor cluster heads around CH_k (When cluster head CH_k has data information to be transmitted to the base station, first, it is required to calculate whether the base station is in the communication scope (radius) of its cluster head; if it is, it will directly transmit data to the base station; otherwise, it will give the process of transmitting data to the next hop, i.e. the process of cluster head jump. The residual energy of neighbor cluster head nodes and the distance between this cluster head node and base station should first be considered. To cluster head CH_j , P_j is called the probability of cluster head jump. Its calculation is shown in formula (3-11).

$$P_j=[\frac{E(CH_j)}{E_{\max}}]^{\alpha}[\exp(-R_i)]^{\beta} \qquad (3\text{-}20)$$

In formula (3-11), $E_{\max}$ refers to highest residual energy among all neighbor cluster heads of cluster head CH_k; α and β are two factors used to control the energy and position of cluster heads. After the calculation of relative probability of different neighbor cluster heads being selected, the one with a higher probability value will become the jump cluster head of this node. Therefore, it is obvious that, the more the residual energy there is and the closer it is to the base station, the higher the probability of being selected as jump cluster head will be. However, the cluster head node selected as a routing hole does not have the chance of being selected as a jump cluster head. Therefore, such path selection mode obtained based on the residual energy of neighbor cluster head nodes and the distance between this cluster head node and base station.

3.7 Summary

This chapter proposed the performance of the RBLEACH algorithm. The regional division, selection of cluster head and path depend on residual energy and distance, these changes can improve the performance of the protocol, such as prolongs the lifetime of each sensor node and death of the nodes, the simulation results are showed in chapter 7.

RBLEACH is used in wide area,but it only focus on cluster select, it is need to conside

(energy and distance as criteria for selecting head

Chapter 4 PS-ACO-LEACH

4.1 Main problems

Clustering strategy or multi hop routing are research hot issues. However, protocols only focus on one factor. For example, in researching multi-hop routing, the clustering strategy is simple; conversely, the cluster could be slightly neglected for route optimization. RBLEACH is used in the wide area,but it only focuses on the selection of the cluster head, whether is the performance of network combining the clustering strategy and multi hop routing mechanism to be optimized? Based on these problems, in this chapter, a WSN clustering routing protocol is proposed, which is based on the particle swarm optimization and ant colony optimization (PS-ACO-LEACH).

4.2 Assumptions of PS-ACO-LEACH clustering routing protocol

The default scene of this protocol is a process, which is to randomly distribute the wireless sensor nodes into a limited square area and then send the data collected from the nodes to the base station.

The following assumptions are made of the networks considering the networks model except §2.61

1. All sensor nodes send the solid bits of data to the head of the cluster every time. The bits will not increase or decrease because of data amount. The information (position, residual energy and whether being the head of cluster or not) of the sensor nodes are all contained in the data packets with a solid length. The sensor nodes will not send the extra data.

2. The base station uses the external power supply and the energy will not be exhausted.

3. The setting information sent from the base station is very simple and short.

There is no energy cost when the sensor receives this information.

4. The radio communication models used by WSN is the same with that in section 2.6

4.3 Design of PS-ACO-LEACH clustering routing protocol

4.3.1 Clustering strategy of PS-ACO-LEACH

The clustering part of the PS-ACO-LEACH uses the centralized control strategy, which executes the algorithm at the base station which has inexhaustible energy. The protocol applies to the same ideas with the literature [8,45]. There are two rounds in each round: creation of the cluster and steady-state stage. The creation of the cluster can be implemented by the following three steps:

(1) The base station collects the nodes' information

(2) The basic PSO is applied to find out the optimized solution of the fitness function adjudged on the multi-factors, so as to find out the optimized clustering.

(3) The base station publishes the clustering information to the head of the cluster, and the head of the cluster publishes the clustering information to the nodes in the clusters.

LEACH considers the impact of the node in the cluster. Based on these two judgment factors, in this thesis, the Euclidean distance to the head of the cluster and the Euclidean distance from the head of the cluster to the base station are also considered in order to improve the distribution of the cluster.

According to the energy information of all nodes, the base station calculates the average energy of the node. The node whose node energy is more than or equal to the average energy, is selected as the head of the cluster node. The candidate for the head of the cluster node is set to narrow the selection range of the head of the cluster to guarantee that the head of the cluster node finally selected has sufficiently large amounts of energy and has the ability to play the role of head of the cluster.

Assume that there are N nodes in the network, Kth node is selected as the head of the cluster, and there are M candidates for the head of the cluster (M>>K). Thus, in total there are $Q = C_M^K$ probabilities for the head of the cluster combinations.

Modify the problem and describe it as: decide a group as the optimized solutions (K solutions) in M candidate head of cluster nodes to make the value of the optimized solutions minimal.

$$\cos t = \alpha f_1 + \beta f_2 + \lambda f_3 + \eta f_4 \tag{4-1}$$

Where f_1、f_2、f_3 and f_4 are the evaluation factors considered in the selection of the head of the clusters. α, β, λ and η represent the weights of each judgment factor in the fitness function respectively. Formulas (4-2) to (4-5) are the mathematical formula for the judgment factors

$$f_1 = \max_{k=1,2,\ldots,K} \left\{ \sum_{\forall n_i \in C_{p,k}} d(n_i, CH_{p,k}) / \left(\left| C_{p,k} \right| * d\left(BS, NC\right) \right) \right\} \tag{4-2}$$

$$f_2 = \sum_{i=1}^{N'} E(n_i) / \sum_{k=1}^{K} E(CH_{p,k}) \tag{4-3}$$

$$f_3 = \max_{k=1,2,\ldots,K} \left\{ d\left(BS, CH_{p,k}\right) / d\left(BS, NC\right) \right\} \tag{4-4}$$

$$f_4 = \max_{k=1,2,\ldots,K} \left\{ \left| \min_{\substack{e=1,2,\ldots,K \\ e \neq k}} \{ d(CH_{p,k}, CH_{p,e}) \} - l \right| / d\left(BS, NC\right) \right\} \tag{4-5}$$

Table 4-1 shows the parameters explanations from Formulas (4-2) to (4-5). It should be noted that $d\left(BS, NC\right)$ plays the role of dimensionless elimination. $d(\text{parameter1}, \text{parameter2})$ is the Euclidean distance between two parameters.

Table 4-1 The meaning of parameters in fitness function

k	Head of cluster ID	K	Head of cluster Amount
N	Amount of nodes	$N^{'}$	Amount of current active nodes
i	Nodes ID	n_i	Node i
$C_{p,k}$	Cluster k in the particle p	$\lvert C_{p,k} \rvert$	Amount of the nodes contained by cluster k in the particle p
$CH_{p,k}$	Head of cluster of cluster k in the particle p	BS	Base station
NC	Networks region center	$CH_{p,e}$	E head of cluster in the particle p
l	Idea value of the distance between the nearest clusters		

Table 4-2 The meaning of fitness function factors

f_1	Compact cluster judgment factor: calculate the maximal average Euclidean distance from the nodes in the each cluster to the corresponding cluster heads. The longer distance, the worse compact.
f_2	Head of cluster energy judgment factor: it equals to the summation of the current residual energy of all sensor nodes divided by the summation of the current residual energy of head of cluster nodes.
f_3	"Hot zone" Related judgment factor: equals the maximal Euclidean distance from the head of cluster to the base station divided by the distance from Base station to the region center. The less value of the distance, the larger probabilities that the head of cluster concentrate in to the hot zone.
f_4	Clustering uniformity judgment factor: calculate the Euclidean distance from each cluster head to the nearest cluster head, and calculate the difference between the value of this Euclidean distance and the ideal distance. The less difference, the more uniform distribution of the cluster.

Based on the definition of the fitness function, the clustering method corresponded with the minimal fitness value should be satisfied by the following:

(1) The average Euclidean distance from the nodes to the corresponding cluster head should be short, which is shown by the compact distribution of the nodes in the cluster that is quantified by f_1

(2) The summation of the cluster head energy is large, and is quantified by f_2

(3) The cluster head is close to the base station, and is quantified by f_3

(4) The distribution between the cluster heads is reasonable, and is quantified by f_4

This type of network clustering can minimize the energy cost in the clusters, balance the energy cost and reduce the probabilities that the nodes far from the base station become the cluster heads in order to maximally elongate the life of the nodes and the networks.

Flow chart of the PS clustering algorithm is as shown in Figure 4-1

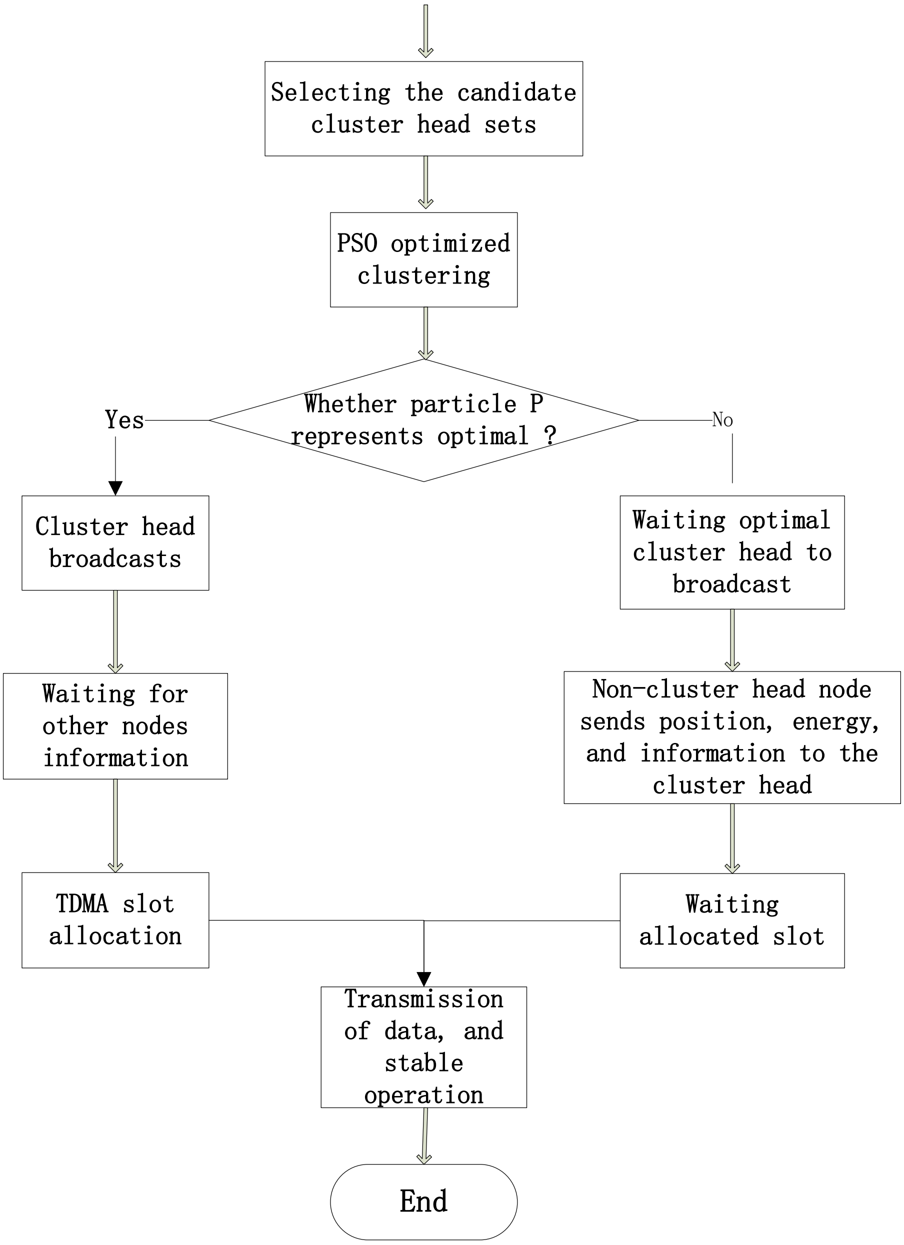


Figure 4-1 Flow chart of the PS-based clustering algorithm

4.3.2 Weight analysis of the judgment factors

The judgment factors are analyzed based on the idea: the weight analysis of each judgment factor needs to compare the difference on a relative fair “Platform”. The “fair” means that each judgment factor has a similar influence to the selection of the cluster head in some ideal networks environment and in the initial state.

Assume this scene: all nodes and all cluster heads in the networks are distributed uniformly, as shown in Figure 4-2. This kind of network topology and clustering are considered temporarily to be ideal.

Calculate the initial value of each judgment factor in the above-mentioned network environment and adjust the weight parameter of each factor accordingly to make the final calculating value of each factor the same. Adjust slightly the value of each weight parameter and observe the life cycle for different value cases.

Analyze the results according to the rationality and influence of the simulation results for the judgment factor.

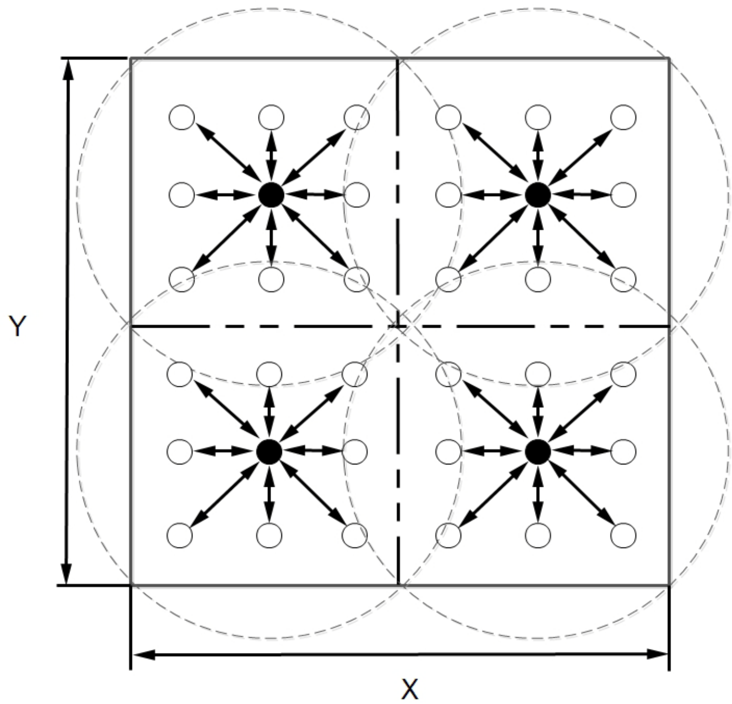


Figure 4-2 Network topology of the nodes uniform distribution

The following is the analysis of the initial value of four judgment factors under an ideal network environment.

1. For f_1, each cluster head is responsible for a rectangular area under the assumptions shown in Figure 4-2. The area of the region should follow formula (4-6). The number of the cluster members in the region should follow formula (4-7)

$$S = (X * Y) * p \qquad (4\text{-}6)$$

$$A = N * p - 1 \qquad (4\text{-}7)$$

Where S is the area that each cluster head is responsible for, A is the node number of a cluster, X is the length of the network region, Y is the width of network region, and P is the percentage of cluster heads. Assume that no matter what the value of X or Y, the region that the cluster head is responsible for is close to the square which means the length along the side is $l = \sqrt{S}$. The nodes in the cluster are distributed uniform. If the nodes are moved around the center diagonally with some degrees, as shown in Figure 4-3, all nodes in the cluster are distributed uniformly along the diagonal. The distance from the nodes to the head of cluster is $\overline{d(n_i, CH_{p,k})} = \frac{\sqrt{2}}{4} * l$. Assume that the coordinate of the base station is (x_{bs}, y_{bs}), $d(BS, NC) = \sqrt{\left(\frac{X}{2} - x_{bs}\right)^2 + \left(\frac{Y}{2} - y_{bs}\right)^2}$ can be obtained. Thus, formula (4-8) can be concluded:

$$f_1 = \overline{d(n_i, CH_{p,k})} / d(BS, NC)$$

$$= \left(\frac{\sqrt{2}}{4} * \sqrt{(X * Y) * p}\right) / \sqrt{\left(\frac{X}{2} - x_{bs}\right)^2 + \left(\frac{Y}{2} - y_{bs}\right)^2} \tag{4-8}$$

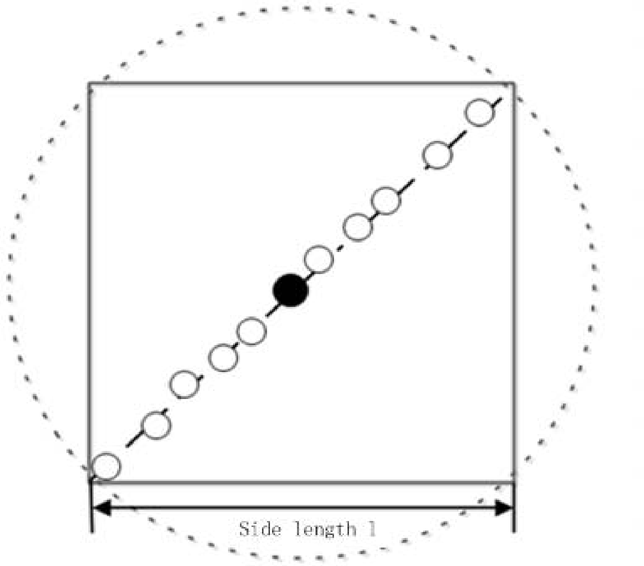


Figure 4-3 Equivalent position of cluster members in evenly distributed nodes

2. For f_2, the energy of all nodes is equal to the initial condition. Based on formula

(4-3), the value of f_2 is same with the reciprocal of cluster head probabilities.

$$f_2 = \frac{1}{p} \qquad (4\text{-}9)$$

3. For f_3, the distribution of cluster heads is assumed to be uniform. There are $N * p$ cluster heads in the region, in which there are A cluster heads on the long side and B cluster heads on the short side. The value of $d\left(BS, CH_{p,k}\right)$ and $d\left(BS, NC\right)$ in formula (4-4) is analyzed. The base selection is selected in different locations because of different application environments and purposes. The location might be in the center of the region, at the edge of the region or someplace far away from the region. The location of the base station is assumed as $\left(x_{bs}, y_{bs}\right)$, then the solutions for formula (4-11) to solve values of A and B can be obtained:

$$\begin{cases} A * B = N * p \\ \dfrac{A}{B} = \dfrac{X}{Y} \end{cases} \qquad (4\text{-}10)$$

$$\begin{cases} A = \left[\sqrt{(N * p) * \dfrac{X}{Y}} \right] \\ B = \left[\sqrt{(N * p) * \dfrac{Y}{X}} \right] \end{cases} \qquad (4\text{-}11)$$

The location of the base station is set as (0,0) , and it can be concluded that the coordinate of x of the farthest cluster head to the base station in the current network is $\left(X - \frac{1}{2} * \frac{X}{A} \right)$, the coordinate of y is $\left(Y - \frac{1}{2} * \frac{Y}{B} \right)$. According to formula (4-4), the value of f_3 can be obtained as:

$$f_3 = \sqrt{\left(\left(X - \frac{1}{2} * \frac{X}{A} \right) - x_{bs} \right)^2 + \left(\left(Y - \frac{1}{2} * \frac{Y}{B} \right) - x_{bs} \right)^2} \,/\, d\left(BS, NC\right)$$

$$= \frac{\sqrt{\left(\left(X-\frac{1}{2}*\frac{X}{\left[\sqrt{(N*p)*\frac{X}{Y}}\right]}\right)-x_{bs}\right)^2+\left(\left(Y-\frac{1}{2}*\frac{Y}{\left[\sqrt{(N*p)*\frac{Y}{X}}\right]}\right)-x_{bs}\right)^2}}{\sqrt{\left(\frac{X}{2}-x_{bs}\right)^2+\left(\frac{Y}{2}-y_{bs}\right)^2}} \tag{4-12}$$

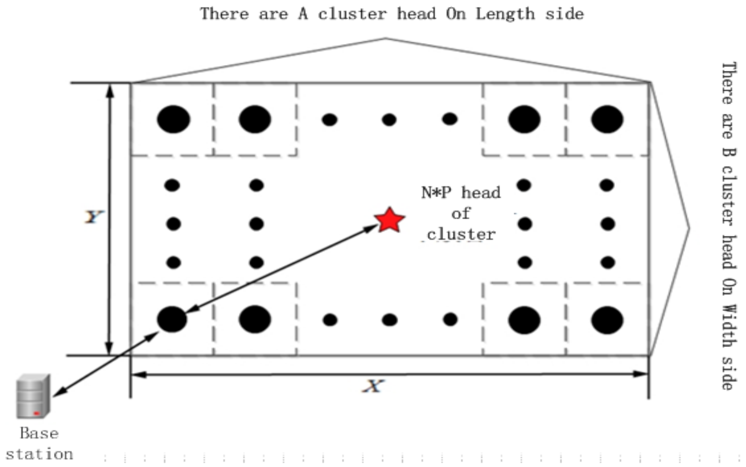


Figure 4-4 Cluster head node distribution in uniformly distributed nodes

4. For f_4, the optimal distance between the clusters is $l=\frac{X}{A}$, as shown in Figure 4-4. However, because the distance between the clusters in the ideal environment are all optimized value, $f_4=0$.

The network environment is assumed and shown in Table 4-3. (It is named as the first category environment). Based on the formulas 4-11, 4-12 and 4-15, the value of f_1, f_2, f_3 and f_4 can be obtained as: $f_1=0.15$, $f_2=10$, $f_3=2$, $f_4=0$. In order to make the proportions closer, the difference between the late $d(CH_{p,k},CH_{p,e})$ of the WSN life cycle and l is assumed as 20. This means that the value of f_4 in the late $d(CH_{p,k},CH_{p,e})$ is approximately 0.5. It is easy to set the least common multiple of $f_i(i=1,2,3,4)$ to be 30. The result of f_i multiplying weight is 30, and the values in Table 4-5 can be concluded.

Table 4-3 Parameter settings of network environment.

X region length	100 (m)	Y region width	100 (m)
Location of base station	(0,0)	N amount of the sensor nodes	100
ε_{fs} energy cost ε_{fs} of the free space channel model	$10*10^{-12}$ (J/bit/m^2)	ε_{mp} energy cost ε_{mp} of the free space channel model	$0.0013*10^{-12}$ (J/bit/m^4)
Initial energy of the nodes	0.1(J)	nodes distribution type	uniform

Table 4-4 Weight Value of the judgment factors

α	200	β	3
λ	15	η	60

The value in Table 4-5 can be obtained by normalizing the values in Table 4-4. In Table 4-5, ρ_k is the weight of the corresponding factor f_k, and the value of k can be ranged as $k = 1, 2, ..., m$ where m is the number of the factors in the self-set fitness function. The fitness function probably selects more different factors that will influence the clusters because of the different applications and considering development in the future.

$$\rho_k = \frac{\rho_k}{\sum_{i=1}^{m} \rho_i}, (k = 1, 2, ..., m) \tag{4-13}$$

Table 4-5 Normalizing the weight of judgment factors

α	0.71	β	0.02
λ	0.05	η	0.22

As shown in Table 4-5, it is unreasonable to set the value of weights as the same or set the weights to be subjective, which probably would cause the completely failure of one or more judgment factors

After the creation of a fair “platform”, the value of each weight should be adjusted to be 5 times or 20 times more. Then the difference of the simulation results between the adjusted weight combination and the initial weight combination is observed to determine which judgment factor is more important. It is noted that the simulation mentioned is to peel off the multi-hops routing mechanism that the cluster head transfer the data to the base station with single-hop like LEACH, and the networks nodes are distributed randomly. The purpose is to determine if the judgment factors joining the PS-ACO-LEACH are reasonable, and to analyze the importance of each judgment factor in the fitness function.

In Figure 4-5, the solid line indicates the rising curve of the dead nodes when the values of the weight parameter α, β, λ, η of the judgment factors are averaged. The dotted line indicates the rising curve of the dead nodes when the values of the weight parameters are taken in the following Table 4-5. The region indicated by the arrow is enlarged for the comparison of two simulation curves. It is observed that the life cycle of weight parameters calculated by formulas (4-8), (4-9) and (4-12) is improved. It is noted that the simulation curves straight up when the number of dead nodes is close to 90, which is caused by the added settings in the program. When the proportion of the dead nodes is close to 90%, WSN is invalid. This will result in the rapid death of residual nodes. The following simulation figure is set with the same assumptions.

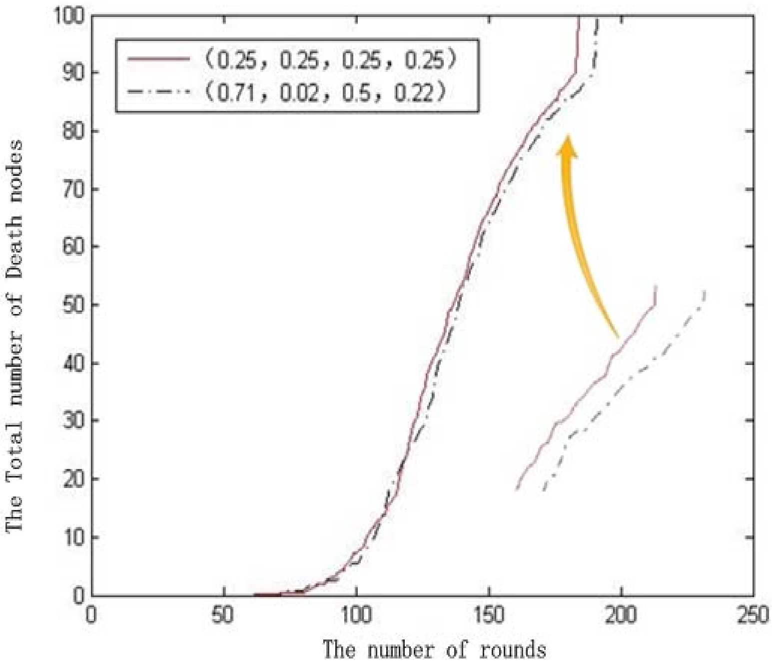


Figure4-5 Comparison of weight parameters

Figures 4-5 to 4-8 show the simulation results that increase the values of α , β , λ and η by 5 times and 20 times. Compared with the parameters in Table 4-5, the following can be concluded:

(1). The simulation curves have a high degree of coincidence, but their separations are not obvious, they need to be enlarged to see the tiny differences

(2) The value of the solid line is decided based on Table 4-4. Its life cycle is the longest, demonstrating that considering the four judgment standards in this thesis comprehensively and evenly is better than considering some judgment factor solely.

(3) The simulation curve in Figure 4-5 and Figure 4-8 has a high degree of coincidence in the former and latter parts of the WSN statement, demonstrating that the cluster compact judgment factors and "hot zone" relative judgment has a large influence on the selection of the cluster head.

(4) The solid lines in Figure 4-5 and Figure 4-7 are always on the right side, demonstrating that the cluster head energy judgment factors and the clustering uniformity judgment factors have few influences on the cluster head. The separation in Figure 4-9 is a little larger, demonstrating that the cluster head energy judgment factors

have a minimal influence in this network environment.

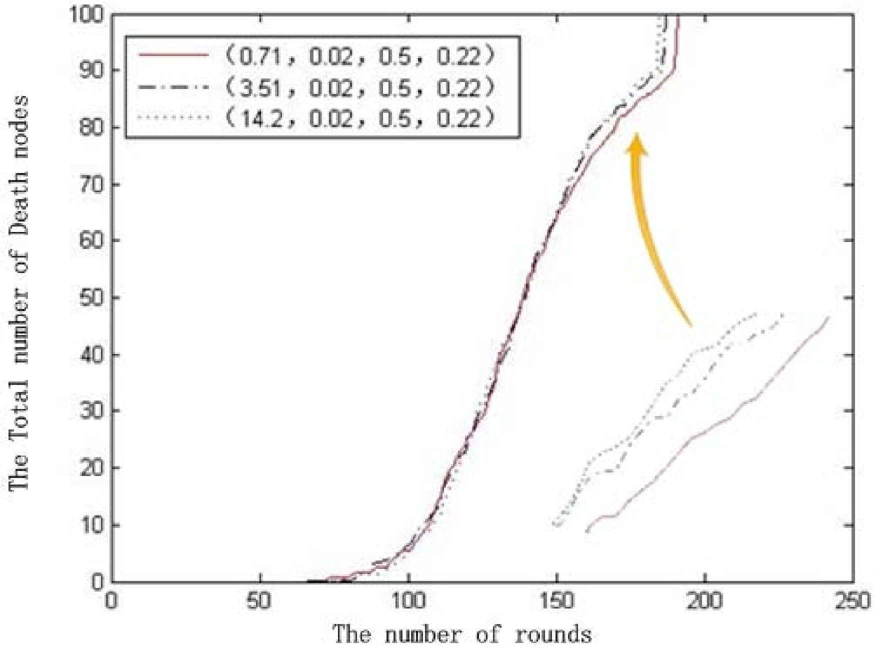


Figure 4-6 Comparison of weight parameters

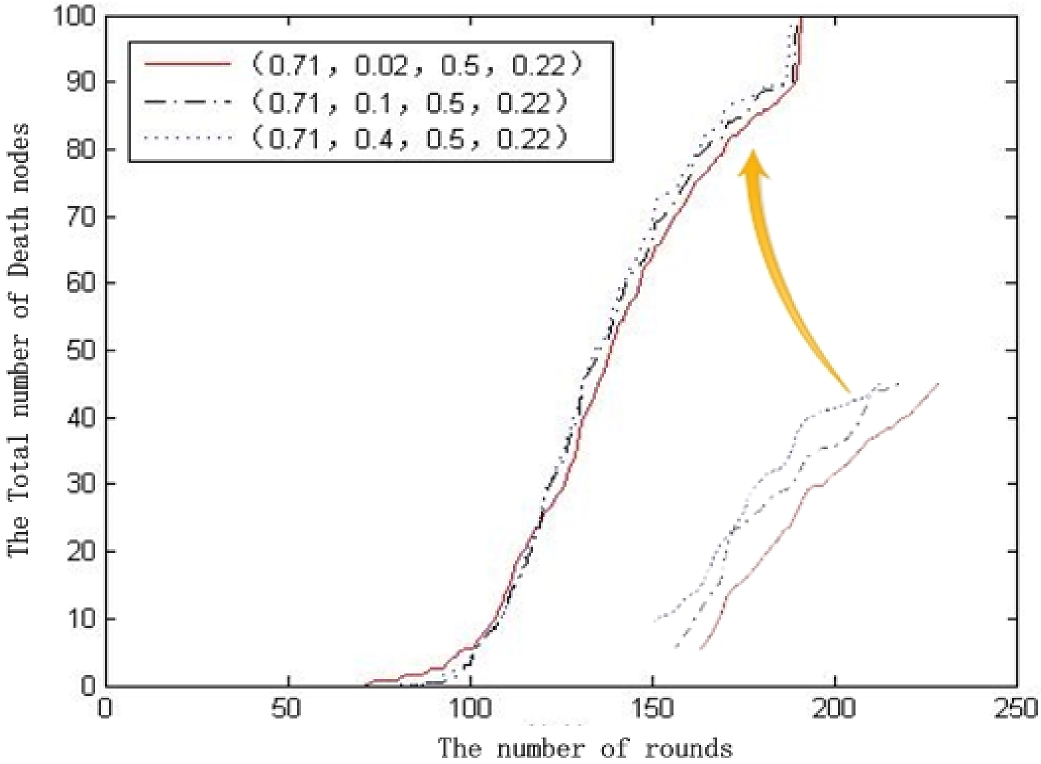


Figure4-7 Comparison of weight parameters

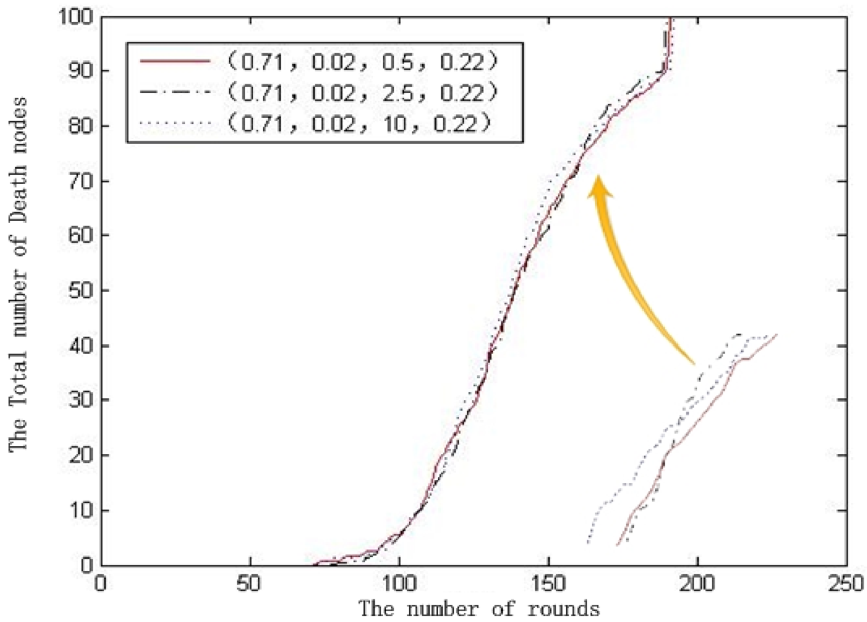


Figure 4-8 Comparison of weight parameters

Conclusions for the above analysis:

(1) Two judgment standards proposed in this thesis are feasible, effective and have a positive influence on the elongation of the life cycle of proposed networks.

(2) In this thesis, the methods of analysis for the weight of judgment factors and the weight parameters obtained based on the analysis methods are optimized in the network environment. The analysis methods are universal and can be used to compare the weight parameter of each judgment in the different network environments.

(3) In this network environment, the influence of each judgment is ranked from high to low: $f_3 > f_1 > f_4 > f_2$

4.3.2 Routing process of PS-ACO-LEACH

PS-ACO-LEACH uses the basic ant colony algorithm [46-48] to select the shortest path from the cluster head to the base station. According to ACO, The transition probability is computed by

$$p_{ij}^{k}(t)=\begin{cases}\dfrac{[\tau_{ij}(t)]^{\alpha}+[\eta_{ik}(t)\}^{\beta}}{\sum\limits_{s\in allowed_k}[\tau_{ij}(t)]^{\alpha}+[\eta_{ik}(t)^{\beta}}, & j\in allowed_k\\ 0 \quad else \end{cases}$$ (4-14)

$\alpha\, and \quad \beta$ have to be discussed.

$allowed_k=\{C\text{-tabu}_k\}$ is all the states allowing ant k th to select for the next step.

$$\eta_{ij}(t)=\frac{1}{d_{ij}}$$ (4-15)

η_{ij} is the heuristic information, d_{ij} is the distance between the two adjacent cities.

The information system is similar to a human's brain, because the information will fade with time, and even be forgotten. The amount of information on path (i,j) will be expressed in the moment of $t+n$:

$$\tau_{ij}(t+n)=(1-\rho)\tau_{ij}(t)+\Delta\tau_{ij}(t)$$ (4-16)

$\Delta\tau_{ij}(t)$ is carried over the amount of information for k th ant in this cycle path. ρ is a pheromone evaporation coefficient.

The flow chart is shown in Figure 4-9.

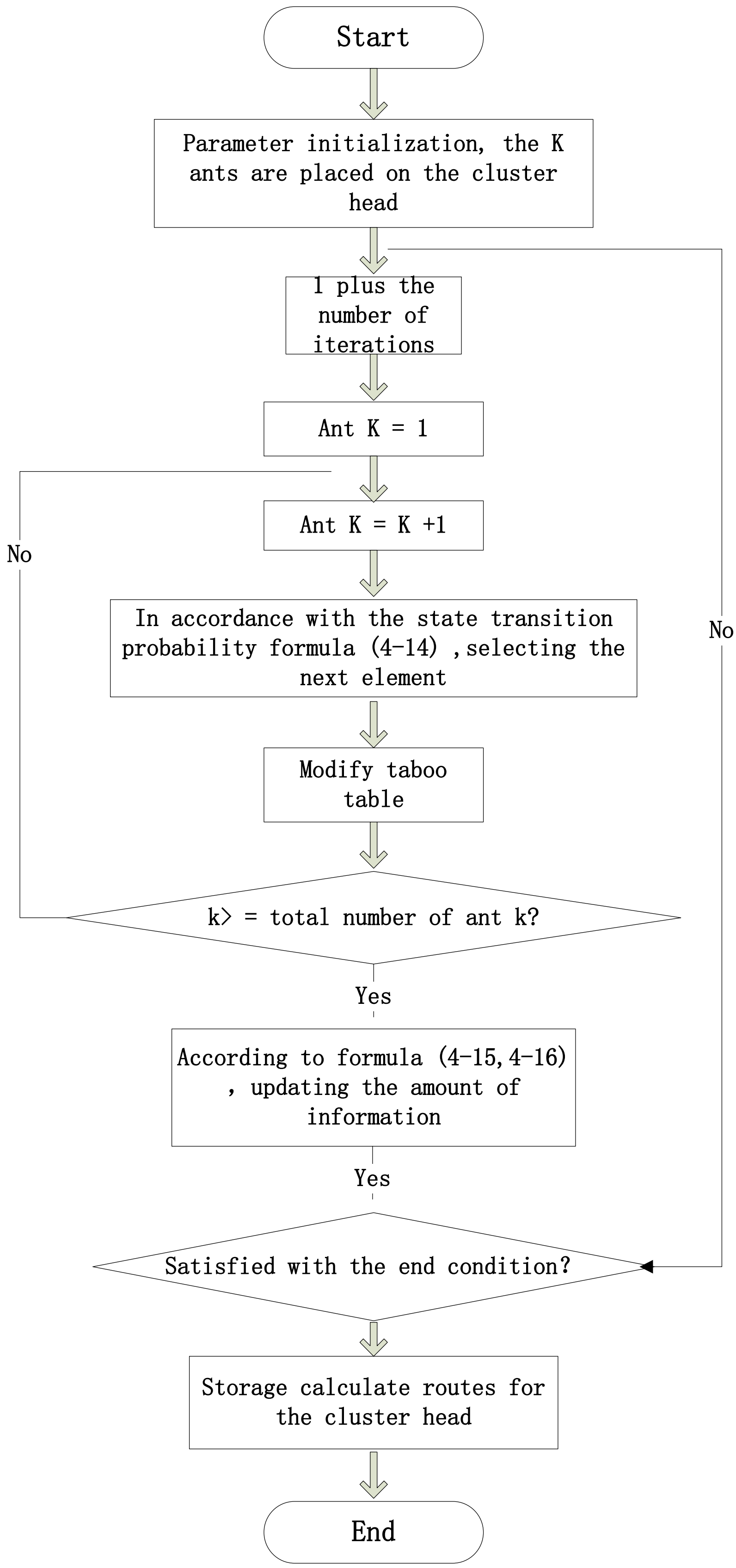


Figure 4-9 Flow chart of using basic AC to find optimized path

4.3.3 Routing maintenance and strategy for routing failure

Affected by the environment and energy, the topology of WSN is changing frequently. Both the death of the old nodes due to energy depletion and addition of the new ones will contribute to changes in topology of the networks so that the routing process fails. The PS-ACO-LEACH protocol uses the artificial ants to construct the path, which can deal with the addition of new nodes and death of the old ones conveniently. As a new node enters the network, the ants can rapidly construct new communication paths according to the developed probability transmission regulation. As an old node dies because of energy depletion or for other reasons, its previous hop-node will find the death caused by the data transmission time-out. Then the information consistence of this path will decrease to zero to prevent continuous visits to the dead node. All the characteristic information of the dead node in its near nodes list will be deleted. Finally, the next hop-node will be calculated according to the probability transmission regulation.

4.5 Summary

According to the characteristics of WSN and in combination with two kinds of swarm intelligence algorithms, PS-ACO-LEACH is proposed. Firstly, it improved particle swarm fitness function in the clustering stage, considering the residual energy of cluster head, Euclidean distance of a cluster member to a cluster head, Euclidean distance between clusters, cluster head nodes to base station of the Euclidean distance to optimize the cluster head configuration; Secondly, in the routing phase of ant colony algorithm to find the best route from nodes to the base station of cluster head, cluster head along this path transmission data have been collected.

Chapter 5 MIA-QRP protocol implementation

5.1 Introduction to MIA-QRP protocol

The network is Adhoc, which can origanize the network itself without relying on a pre-existing infrastructure. This network is one kind of WSN. RBLEACH and PS-ACO LEACH are used for ADHOC, but the route protocls don’t consider QoS. The routing protocols of Adhoc support the ones of the QoS [111-123], but most of the existing protocols are criticized by one factor among the node energy, the bandwidth, the delay and the other single QoS indexes. In this thesis, the average link delay, the average package loss rate and the node signal strength are selected as the parameters of QoS for the special requirements. Multiple Indicator Adaptive QoS Routing protocol (MIA-QRP) is suggested.

Classified by routing strategy, MIA-QRP belongs to table-driven routing protocol [117], which can support at most two-hops. During the operation of the protocol, each node maintains a network topology table. The nodes obtain the link relation by exchanging the topology routing information. When the topology is updated, it will use the routing algorithm to select the optimized path. The stored information of node topology table is as shown in Table 5-1.

Table 5-1 Node list information structure

Mac	IP	ParentMac	ParentIP	Lost	Delay	Quality	TTL	Link_state

The definition of each field is as follows:

MAC means the MAC address of nodes.

IP means the IP address of nodes.

Parent Mac means the parent MAC of nodes

Parent IP means the parent IP of nodes

Loss means the package loss rate parameters of the link formed by the nodes and parent nodes.

Delay means the delay parameters of the link formed by the nodes and parent nodes.

Quality means the nodes' signal strength of receiving the parent node signal

TTL means the live time of nodes.

Link_statie means the link condition between the nodes and parent nodes.

The relative definitions in this protocol are described as follows:

In order to manage the nodes information normally and conveniently, the first stored information of the topology table is set with the relative information of each node. The MAC and IP in the table fill the MAC address and the IP address of the each node respectively. The parent nodes MAC and the parent nodes IP fill the 00-00-00-00-00-00 and the Loop address 127.0.0.1. The value of the lost is 0, value of the delay is 0, value of quality is 1, value of TTL is 0 and that of the link state is 2.

Relay nodes: in a communication link, if the data communication between node A and node C should be finished by the data transmission of node B, then node B is the relay node of node A and node C.

Parent nodes: In a communication link, if node B is the relay node of the link from node A to node C, then node B is the parent node of node C, and node A is the parent node of node B.

Direct neighbor nodes: other nodes which are in the direct communication distance range of node A are the direct neighbor nodes of node A. The topology information of the direct neighbor nodes sets the parent MAC and the parent IP to be the MAC address and the IP address of node A respectively.

Line of sight: the communication link built with the direct neighbor nodes is the line of sight.

Multi-hop path: the communication link between the indirect neighbor nodes is multi-hop path.

Two-way link: If node A and node B can receive a signal from each other, then the communication link between node A and node B is two-way link.

One-way link: If only one node can receive the signal from the other node, the communication link between the two nodes is one-way link.

All nodes maintain their own network topology table. The nodes obtain each path to communication with other nodes, and finish the selection of their optimized path and the division of the alternate path by combining the path selection algorithm programs. Finally, the settings of the nodes routing table are finished. All node information in this protocol is operated and maintained by this network topology table.

The operations of this protocol are finished by the cooperation of seven types of messages, namely, “hello”, “response”, “update”, “rsreq”, “reqack”, “Ack” and “delete”. The hello message is a broadcast message, in which the nodes will first send this message to the surrounding nodes as they start up. During the operations of the protocol, the nodes will regularly broadcast the hello message to the surrounding nodes to maintain their own network topology information. The surrounding nodes will response to the response message when they receive the hello message to determine the direct neighbor nodes to form the line of sight. When one node has a new path, it will send the updated message to the neighbor nodes directly so that the neighbor nodes can update the network topology table in time. In order to guarantee the efficiency of the node information, this protocol sets a detection timer to regularly maintain each node. Once an expired node is found, the “delete” message will be sent to the neighbor nodes. The nodes detect their own network topology table after receiving the delete message and delete the information of the expired nodes. In order to prevent routing loops, an “rsreq” path detection message and a “reqack” path confirmation message are designed. The “ack” message is to finish the verification of the two-way link to ensure that the protocol can construct all two-way linked networks.

5.2 Design of protocol message

As described in 5.1, this routing protocol is finished by the cooperation of five types of messages, “hello”, “response”, “update”, “ack” and “delete”. The functions of each message are exhibited in Table 5-2

Table 5-2 Function of protocol message

Hello message	Claim self-existence by broadcasting to the surrounding nodes
Response	Send the node network topology information to the nodes of sending “hello” message
Update	Send the updated information of the network topology to the direct neighbor nodes
Delete	Send the routing deletion information to the direct neighbor nodes
Ack	Detect the message in the adjacent nodes to remove the one-way link

5.2.1 Common head of protocol message

Seven types of message in this protocol have the similar format, which is called the common head of the protocol message

<table>
<tr><td>0</td><td>7</td><td></td><td>15</td><td>31</td></tr>
<tr><td>Command（6、7）</td><td>Version1</td><td></td><td>F</td><td>Length（16）</td></tr>
<tr><td colspan="5">Ipv4 address</td></tr>
<tr><td colspan="5">MAC</td></tr>
<tr><td colspan="4">MAC(cont’)</td><td></td></tr>
<tr><td colspan="5">Source IPv4 Address（ip_src）</td></tr>
<tr><td colspan="5">Destination IPv4 Address（ip_dest）</td></tr>
</table>

Figure 5-1 Public radical format of protocol messaging

Value definitions of each field command: This field indicates the type of message, which occupies eight bits. The value of this field is 1, which means it is a “hello” message. The rest may be deduced by analogy, when the values of the fields are 2,3,4,5,6 and 7, the fields are response message, update message, delete message, ack message, rsreq message and reqack message.

Version: This field shows the protocol version of this field, which occupies 4 bits and is designed for the upgrading of the protocol. In this thesis, the value of the first version in this protocol is 1.

F: This field indicates the mark field. When the value of the command field is 5, the value of this field is significant. If the value of the F field is 1, it means it needs the other side to send the “ack” message for the confirmation. The value of the F field is 2, which means it does not need confirmation.

Length: This field indicates the total length of the protocol message, including the length of the protocol head, which occupies 2 bits.

Ipv4 address: This field indicates the ipv4 address of this node, which occupies 4 bits.

MAC: This field indicates the physical address of the node, which is actually the MAC address of the NIC and occupies 6 bits.

5.2.2 Format of the “hello” message

The format of the “hello” message is the same as the public radical of the message. It just needs to give the relative value to each field. The value of the command is 1, the value of version is 1, the value of F is 1, the value of length is 16, and the IPv4 and MAC fields fill the IP address and the MAC address of this node respectively, as shown in Figure 5-2:

0 7 15 31

<table>
<tr><td>Command</td><td>Version.1</td><td></td><td>F</td><td>Version.（16）</td></tr>
<tr><td colspan="5">Ipv4 address</td></tr>
<tr><td colspan="5">MAC</td></tr>
<tr><td colspan="4">MAC(cont’)</td><td></td></tr>
</table>

Figure 5-2 Format of “hello” message

5.2.3 Format of “response” message

The “response” message is the response to the “hello” message. The node receiving the “hello” message supplies the network topology information to the node sending the “hello” message so that the node that sends the “hello” message can create its own network topology table as soon as possible. The message format is shown in Figure 5-3

0	7		15	
Command（2）	Version1		F	Length（16）
Ipv4 address				
MAC				
MAC(Cont’)				
n routing entries				

5-3 Format of the “response” message

In the “response” message, the radical of the message command field value is 2. There are “n” routing entries after the public radical. Each routing entry indicates the path information from one node to one of its direct neighbor nodes. The format of each routing entry is shown in Figure 5-4

0 7	15 31
Ipv4 address	
Link_state	Delay
Lost	Quality

Figure 5-4 Routing entry format

The length of each routing entry is 12 bits, including IPv4 address, link state, delay, package loss rate and signal strength. The definition of each field is described as follows:

IPv4 address (IP) occupies 4 bits and indicates the IP address of the direct neighbor nodes.

Link state occupies 2 bits. It is used to express the link state between direct neighbor nodes and the original node. This field can supply criteria for routing selection in the routing algorithm. If the value is 0, it means that the link between the nodes is broken. If the value is 1, it means that the link between the nodes is one-way link. If the value is 2, it means that the link between the nodes is two-way link.

Delay occupies 2 bits. It shows the statistical average value of the communication delay between the original node and the direct neighbor nodes, including processing delay and transmission delay.

Package Loss Rate occupies 2 bits. It shows the average value of the communication package loss rate between the original node and direct neighbor nodes.

Signal strength (quality) occupies 2 bits. It shows the signal strength of the direct neighbor nodes detected by the original node at its location.

It is known from the definitions of the message format that the total length of the message minus the length of the message public radical is equal to the length of the entry part of the routing. Each routing entry occupies 12 bits. Thus, the number N of the routing entry in each response message can be calculated with the following formula:

$$N = \frac{len - 16}{12} \tag{5-1}$$

Where len is the length of the whole message, 16 is the length of the public radical of the protocol message and 12 is the length of one routing entry.

5.2.4 Format of update message

The “update” message is used to report the finding of a new path or the updating of a path to the direct neighbor nodes. It is an important part of the path updating and maintenance. Each “update” message contains a path condition, and each condition is expressed by one routing entry. The “update” message has a length of 28 bits and the value of command field is 3. The message format is shown in Figure 5-5.

0 7 15 31

Command(3)	Version(1)		F		
IPV4(Address)					
MAC (Address)					
MAC Address					
IPV4(Address)					
Link_state C				Delay C	
Lost C				Quality C	

Figure 5-5 Formate of update message

5.2.5 Format of delete message

The “delete” message format is similar to the “response” message format. Both of them contain public message radicals and “n” routing entries. Its command value is 4. The detailed message format is shown in Figure 5-6

0 7 15

Command（2）	Version1		F	Length（16+12n）
Ipv4 address				
MAC				
MAC(Cont’)				
n routing entries				

Figure 5-6 Format of the “delete” message

The routing entry in the “delete” message is the routing entries that need to be deleted. Most of them are expired node paths.

5.2.6 Format of “ack” message

The “ack” message is mainly used for protocol message confirmation between the neighbor nodes. The neighbor nodes confirm a two-way link based on the “ack” message. The length and the format of the message are similar to the “request” message. But the value of the command field is 5. The format of the “ack” message is shown in Figure 5-7

0 7 15 31

Command	Version.1		F	Length.（16）
Ipv4 address				
MAC				
MAC(cont’)				

Figure 5-7 Format the of “ack” message

5.3 Path discovery

In this protocol, the path discovery mechanism includes positive path discovery and negative path discovery. The positive path discovery means that the nodes send the “hello” message to the neighbor nodes to require positive routing information. The negative path discovery means nodes receive the “update” message from the neighbor nodes, in which the path is constructed based on the “update” message. The positive path discovery is the base of the negative path discovery.

5.3.1 Active path discovery

The active path discovery of nodes includes three steps: perception of new nodes to the path, confirmation of link state, and perception of the neighbor nodes to the new nodes. The network topology is shown in Figure 5-9. The distance between the neighbor nodes is in the one-hop, but the distance that is between the non-neighbor nodes is beyond the direct communication range. It is assumed that nodes B, C and D can communicate with each other directly, and the network topology shown in Figure 5-8 has been formed. Setting node A as an instance, the path active discovery of the protocol is described as follows:

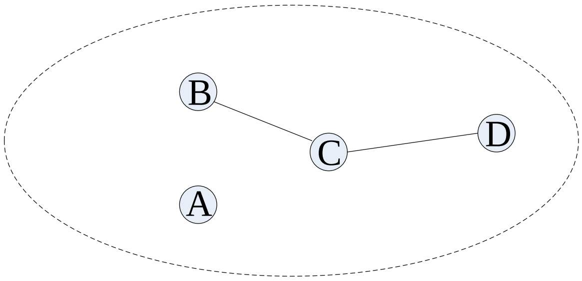


Figure 5-8 Nodes network topology

After the switch of node A’s hardware, node A first initializes self-hardware, then it operates the content of this protocol. Node A first broadcasts a “hello” message to the neighborhood the content of this message is shown in Figure 5-9. After sending the “hello” message, node A is in the condition of loop waiting. After receiving the protocol message from the other nodes, node A will operate the relative messages.

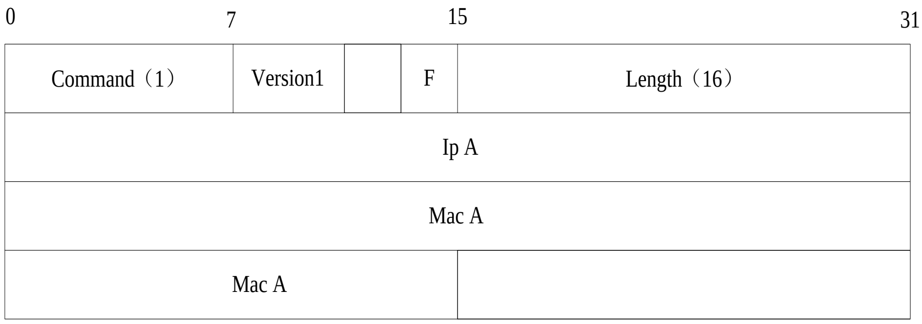


Figure 5-9 Content of the “hello” message

Based on the node network topology in Figure 6-10, node B and node C will receive the “hello” message sent from node A. According to the construction regulation of the direct path, node B and node C will create the corresponding network topology information based on the received “hello” message. The received “hello” message can only confirm the one-way communication between the Link A-B and Link A-C. The link state field is set as 1, the detailed generated network topology information is shown in Figure 5-10.

Node MAC	Node IP	Parent node MAC	Parent node IP	Packet loss rate	Delay	Signal strength	Living time	Link state
Mac A	IP A	Mac B	IP B	-	-	-	0	1
Mac A	IP A	Mac B	IP B	-	-	-	0	1

Figure 5-10 Topology information content of node B and node C

The rules of one-way direct path constructed by the "hello" message are described as follows:

The nodes MAC address in the radical of the MAC and of the "hello" message

The nodes IP address in the radical of the IP and "hello" message

Parent node MAC, filling in the MAC address of this node

Parent node IP, filling in the IP address of this node

Package loss rate, because there is no two-way link confirmed. The measured data is not generated.

Delay, because there is no two-way link confirmed, the measured data is not generated.

Signal strength, because there is no confirmed two-way link, the measured data is not generated.

Life time, because the path is just constructed, 0 is filled in.

Link state, because the "hello" message is just received, 1 is filled in to express the one-way link.

After node B and node C generate their own one-way topology information table, node B and node C will check self-network topology information tables, and extract and package the corresponding node information to the response message, which will be sent to node A. The routing entry of the response message must be a two-way direct path. The response message sent from the node B and node C to node A are shown in Figure 5-11 and figure 5-12.

<table>
<tr><th>0</th><th>7</th><th></th><th>15</th><th>31</th></tr>
<tr><td>Command(0x02)</td><td>0x01</td><td></td><td>F</td><td>Lenght（28）</td></tr>
<tr><td colspan="5">Ip B</td></tr>
<tr><td colspan="5">Mac B</td></tr>
<tr><td colspan="4">Mac B</td><td></td></tr>
<tr><td colspan="5">Ip C</td></tr>
<tr><td colspan="4">link_state C</td><td>Delay C</td></tr>
<tr><td colspan="4">Lost C</td><td>Quality C</td></tr>
</table>

Figure 5-11 Response message of node B

<table>
<tr><th>0</th><th>7</th><th></th><th>15</th><th>31</th></tr>
<tr><td>Command（0x02）</td><td>0x01</td><td></td><td></td><td>F Length（16）</td></tr>
<tr><td colspan="5">Ip C</td></tr>
<tr><td colspan="5">Mac C</td></tr>
<tr><td colspan="4">Mac C</td><td></td></tr>
<tr><td colspan="5">Ip B</td></tr>
<tr><td colspan="4">link_state =2</td><td>Delay B</td></tr>
<tr><td colspan="4">Lost B</td><td>Quality B</td></tr>
<tr><td colspan="5">Ip D</td></tr>
<tr><td colspan="4">link_ state =2</td><td>Delay D</td></tr>
<tr><td colspan="4">Lost D</td><td>Quality D</td></tr>
</table>

Figure 5-12 “Response” message of node C

After node A receives the “response” message sent from node B and node C. The network paths are constructed based on the message content and two direct paths and three multi-hop paths are obtained, as shown in Figure 5-13

Node MAC	Node IP	Parent node MAC	Parent node IP	Packet loss rate	Delay	Signal strength	Living time	Link state
Mac B	IP B	Mac A	IP A	Lost B	Delay B	Quality B	0	2
Mac C	IP C	Mac A	IP A	Lost C	Delay C	Quality C	0	2

Figure 5-13 Direct path information of node A

Rules of construction of the direct path:

Node MAC, the MAC address in the “response” message radical

Node IP, the IP address in the “response” message radical

Parent MAC, the MAC address filled in node A

Parent IP, the IP address filled in node A

Package loss rate, node A measures the statistical average value of package loss rate of the communication between node A and the node related to the “response” message.

Delay, node A measures the statistical average value of the delay of communication between node A and the node related to the “response” message

Signal strength, node A measures the signal strength value of the node related to the “response” message.

Life time, as the path is just constructed, 0 is filled in.

Link state, because the “response” message is just received, 2 is filled in to express the two-way link.

Meanwhile, according to the “response” message entry message, node A can construct three multi-hop paths. The content of network topology information content is shown in Figure 5-14.

NodeMAC	NodeIP	parent node MAC	parent node IP	packet loss rate	Delay	Signal strength	Living time	link state
Mac B	IP B	Mac A	IP A	Lost B	Delay B	Quality B	0	2
Mac C	IP C	Mac A	IP A	Lost C	Delay C	Quality C	0	2
Mac C	IP C	Mac B	IP B	Lost C	Delay C	Quality C	0	2
Mac B	IP B	Mac C	IP C	Lost B	Delay B	Quality B	0	2
Mac D	IP D	Mac C	IP C	Lost B	Delay B	Quality B	0	2

Figure5-14 Network topology information of node A

The construction rules of the multi-hop paths are described as follows:

Node mac, mac is filled in 00-00-00-00-00-00-00 because it is not the direct path.

Node IP, extracted from the routing entry information of the response message.

Parent mac, the mac address of the response message radical

Parent IP, the IP address of the response message radical

Package loss rate, the nodes related to the response message radical measure the statistical average value of the package loss rate of the communication between the nodes and the relative routing entry nodes delay, the nodes related to the response message radical measure the statistical average value of the delay of communication between the nodes and relative routing entry nodes

Signal strength, the nodes related to the response message radical measure the signal strength of relative routing entry nodes.

Living time, because the path is just constructed, 0 is filled in

Link state, the response message is promised to merely send the two-way path information, thus 2 is filled in.

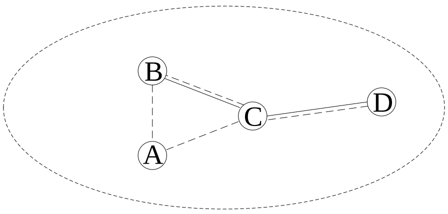


Figure 5-15 Network topology structure of node A

Node A receives the “response” message by sending a “hello” message to the neighbor nodes. Based on the detailed content of the “response” message, node A can obtain the network topology structure of the neighbor nodes, and modify the network topology structure information table of node A to create the communication path with the neighbor nodes. The network topology structure of node A is shown in the dotted line in Figure 5-15.

After node B and the node C receive the “hello” message from node A, they can only confirm the link A-B and link A-C as one-way paths, but not as the complete communication path between nodes B, C and node A. In order to modify the network topology information table of node B and node C, after node A finishes the operation of the “response” message, it needs to feedback the “ack” path confirmation message to node B and node C so that the direct neighbor nodes can confirm the creation of two-way path. As node A has already confirmed the communication link as a two-way link, it just needs to send the “ack” link confirmation message to the direct neighbor nodes. The value of the field F of the message radical is 2, which means that the direct neighbor nodes do not need to reply to the “ack” message for link confirmation. The detailed “ack” message content sent from node A is shown in Figure 5-16.

<table>
<tr><td>0</td><td>7</td><td></td><td></td><td>15</td><td>31</td></tr>
<tr><td>Command（5）</td><td>Version(1)</td><td></td><td>2</td><td colspan="2">Length（16）</td></tr>
<tr><td colspan="6">Ip A</td></tr>
<tr><td colspan="6">Mac A</td></tr>
<tr><td colspan="4">Mac A</td><td colspan="2"></td></tr>
</table>

Figure 5-16 Content of “ack” message

After receiving the “ack” link confirmation message, node B and node C will correct the link state field of the information related to network information topology table of the nodes, and correct 1 to 2 expressing the two-way link. They will also call the package loss rate, delay and signal strength of the relative link obtained from the link measurement program. The content of the corrected network topology information table is shown in Figure 5-17.

NodeMAC	NodeIP	parent node MAC	parent node IP	packet loss rate	Delay	Signal strength	Living time	link state
Mac A	IP A	Mac B	IP B	Lost A	Delay A	Quality A	0	2
Mac A	IP A	Mac C	IP C	Lost A	Delay A	Quality A	0	2

Figure 5-17 Network topology information of the node B and the node C

After the “ack” link confirms the completion of message operations, the network topology information tables of node A, node B and node C are modified, and the communicated network topology between nodes is created. However, node D does not update its own network topology information table, thus it does not have the multi-hop path information to node A. This routing protocol also designs an updated routing renewing message, by which node D modifies the topology information table of the nodes. The update process of the network topology information table of node D is introduced as follows:

5.3.2 Process of negative path discovery

Based on the network topology shown in Figure 5-8, after node C finishes the “ack” link confirmation message and modifies its own network topology information, it will send the updated routing message to the neighbor nodes. As the constructed C-D link cannot be confirmed as a two-way link, the value of link state of the network topology information will be corrected to 1 when node C sends the “update” message to node D in order to confirm the C-D link state again. The content of the “update” routing message sent from node C to node D is shown in Figure 5-18.

0	7		15	31
Command（3）	Version1		F	Length（28）
Ip C				
Mac C				
Mac C				
Ip A				
link_state=2				Delay A
Lost A				Quality A

Figure 5-18 Content of the “update” message

After node D receives the update routing message, it will create a D-C-A multi-hop path from node D to node A according to the message content and to the multi-hop path construction rules. Because the link state of path C-D needs to be updated, the value of the link state of the created network topology information table will be set as 1. The content of network topology information table created by node D is shown in Figure 5-19

NodeMAC	NodeIP	parent node MAC	parent node IP	packet loss rate	Delay	Signal strength	Living time	link state
Mac C	IP C	Mac D	IP D	Lost C	Delay C	Quality C	0	1
Mac A	IP A	Mac C	IP C	Lost A	Delay A	Quality A	0	1

Figure 5-19 Network topology information of node D

After node D updates the path topology information based on the “update” message, it needs to send the “ack” link state request confirmation message to confirm the D-C path as a two-way link. Because node D needs node C to feed back the “ack” link confirmation message, the value of F field is set as 1. The content of the “ack” message sent is shown in Figure 5-20.

0	7		15	31
Command（5）	Version1		1	Length（16）
Ip D				
Mac D				
Mac D				

Figure 5-20 Content of “ack” request message sent by node D

After node C receives the ack link state request message from node D, it modifies its network topology information table first, and corrects the value of the link state of the relative routing information from 1 to 2. It also marks the relative path as a two-way available path. After modification of the information, node C will feed back the ack link state confirmation message to node D. The value of the F field in the message is set as 2. The detailed content is shown in Figure 5-21.

0	7		15	31
Command（5）	Version1		2	Length（16）
Ip C				
Mac C				
Mac C				

Figure5-21Ack confirmation message sent from node C

After node D receives the ack link state confirmation message, it will correct the value of the path state of the network topology information based on the message content, and set the value of link state of relative D-C link and D-C-A link as 2 to express the relative path as the two-way path. The corrected topology information is shown in Figure 5-22.

Node MAC	Node IP	Parent node MAC	Parent node IP	Packet loss rate	Delay	Signal strength	Living time	Link state
Mac C	IP C	Mac D	IP D	Lost C	Delay C	Quality C	0	2
Mac A	IP A	Mac C	IP C	Lost A	Delay A	Quality A	0	2

Figure5-22 Topology information content of node D

After the update path message is completed and the network topology information table of node D is modified by the ack link confirmation message, the node topology shown in Figure 3-10 obtains updated communicated topology, in which there is accessible topology path information between each node and the path discovery is completed. The final network topology is shown in Figure 5-23.

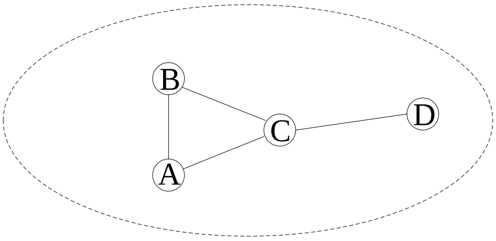


Figure 5-23 Network topology of nodes

5.4 Path maintenance

This routing protocol is based on the table-driven routing protocol. Each node needs to regularly maintain self-routing table information. This routing protocol implements the work of nodes routing table maintenance, mainly by setting the node timing, updating the timer and the node inquiring timer. The nodes update the timer mainly through the real-time effectiveness of self-node maintenance, and by regularly claiming the existence of the self-nodes. The nodes inquiring timer is used to regularly inquire the content of the network topology information table, and timely delete the expired invalid node information.

5.4.1 Regular updating strategy of routing

In this ADHOC network, the nodes can randomly move. The network topology is characterized by dynamic change. The network topology information created between the nodes can be changed at any time. The routing protocol needs to, on a timely basis, determine the effectiveness of each link to guarantee the feasibility of network communication.

This routing protocol implements the update of routing information by designing the regular updating timing of nodes to guarantee the path effectiveness between the nodes. Each communication node has a regular updating timer. Once the prescribed amount of time elapses, the node will regularly broadcast the “hello” message to the surrounding nodes to claim the existence of the nodes. Due to different application conditions of the ADHOC networks, the external influences on the nodes are different, and the moving conditions of the nodes are different. The detailed interval is set according to the specific circumstances.

When the time of the timer comes, the nodes will not only send the “hello” message, but also update the value of the lifetime field of each path in the network topology information table of the nodes. The nodes will also set regular intervals to achieve the objective of recording the lifetime of a path. When receiving the “hello” message, the surrounding nodes will timely correct the relative path lifetime of the path information, which is reset to 0, based on the content of the “hello” message, and mark the effectiveness of the link.

5.4.2 Routing deletion strategy

In order to timely update the invalid routing information of the nodes in the node network topology information table, an inquiry timer is designed in this protocol. The nodes regularly travel through the network topology information table to check the recorded value of the path lifetime field, and to judge if the lifetime of each path exceeds the set maximum lifetime. If the lifetime of each path exceeds the set maximum lifetime, the path is judged as an expired invalid path, and the corresponding node is the invalid node. This node will delete the corresponding routing information in the network topology information, and package the invalid nodes into the “delete” message sent to the surrounding direct neighbor nodes. The surrounding direct neighbor nodes will timely update the network topology information table according to the “delete” message to remove the invalid routing information contained by the expired nodes.

Node D in Figure 5-24 is assumed to be an invalid node, and the deletion process of the path is described. If node D does not have failing node, the set request timer will detect the maximum value that the C-D path lifetime exceeds the set value in the network topology information table after a while. Meanwhile, node C judges node D as an invalid one and deletes the routing information related to node D in the network topology information table of self-node. The network topology information of node C is shown in Figure 5-24.

Node MAC	Node IP	Parent node MAC	Parent node IP	Packet loss rate	Delay	Signal strength	Living tim	Link state
Mac A	IP A	Mac C	IP C	Lost B	Delay B	Quality B	TTL	2
Mac B	IP B	Mac C	IP C	Lost A	Delay A	Quality A	TTL	2
Mac B	IP B	Mac A	IP A	Lost B	Delay B	Quality A	TTL	2
Mac A	IP A	Mac B	IP B	Lost A	Delay A	Quality A	TTL	2

Figure 5-24 Network topology information of node C

After deleting the information of the invalid node D, node C will package node D into the “delete” message and send it to the direct neighbor nodes. The state value of the link in the routing entry contained in the “delete” message is set as 0, which indicates an invalid link. The content of the “delete” message is shown in Figure 5-25.

0	7			15 31
Command(4)	Version(1)		F	Length(28)
IP C				
MAC C				
MAC C				
IP D				
Link_state =2			Delay D	
Lost D			Quality D	

Figure5-25 Deleted message sent by the nodes

After node A and node B receive the "delete" message, the lifetime of path A-C and path B-C will be set to 0 according to the message content. The information of the invalid nodes in the nodes network topology information table, which is the recorded information of node D, will be deleted. After the deletion, the topology information of node A and node B are shown in Figure 5-26 and Figure 5-27.

NodeMAC	NodeIP	parent node MAC	parent node IP	packet loss rate	Delay	Signal strength	Living time	link state
Mac B	IP B	Mac A	IP A	Lost B	Delay B	Quality B	TTL	2
Mac C	IP C	Mac A	IP A	Lost C	Delay C	Quality C	TTL	2
Mac C	IP C	Mac B	IP B	Lost C	Delay C	Quality C	TTL	2
Mac B	IP B	Mac C	IP C	Lost B	Delay B	Quality B	TTL	2

Figure 5-26Network topology information of node A

Node MAC	Node IP	Parent node MAC	Parent node IP	Packet loss rate	Delay	Signal strength	Living tim	Link state
Mac A	IP A	Mac B	IP B	Lost A	Delay A	Quality A	TTL	2
Mac C	IP C	Mac B	IP B	Lost C	Delay C	Quality C	TTL	2
Mac C	IP C	Mac A	IP A	Lost C	Delay C	Quality C	TTL	2
Mac A	IP A	Mac C	IP C	Lost A	Delay A	Quality A	TTL	2

Figure 5-27 Network topology information of node B

After node A, node B and node C complete the update of the network topology information table, they will delete the expired path information of node D. The network topology structure is shown in Figure 5-28.

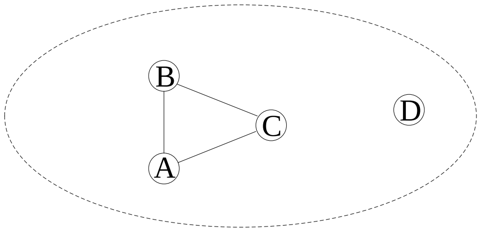


Figure 5-28 Network topology structure

5.5 Finite-state machine mode of protocol

Many protocol modes always involve the Finite-state machine (FSM) [137], which makes an accessible analysis by the state transmission and detects all kinds of mistakes in the protocols and the standards. The FSM of the protocol is shown in Figure 5-30. From the view of the form, the FSM mode of this protocol can be regarded as a triad (S,M,T).

In this triad,

S indicates all possible states set in the protocol;

M indicates the setting initializing the transmission of the protocol state;

T indicates the setting of the transmission between protocol states.

The event trigger mode is used in the design of this protocol. As a protocol event comes, the protocol transfers from the free state to the events processing state. After the processing is done, the protocol will transfer to a free state.

The events that initiate the state transmission (Figure 5-29).

Protocol initiation

Protocol exit

Regular sending of “hello” message

The path lifetime exceeds the maximal living time

Regular deletion of the link QoS parameter index

Receiving the hello message

Receiving the response message

Receiving the update message

Receiving the delete message

Receiving the ack message

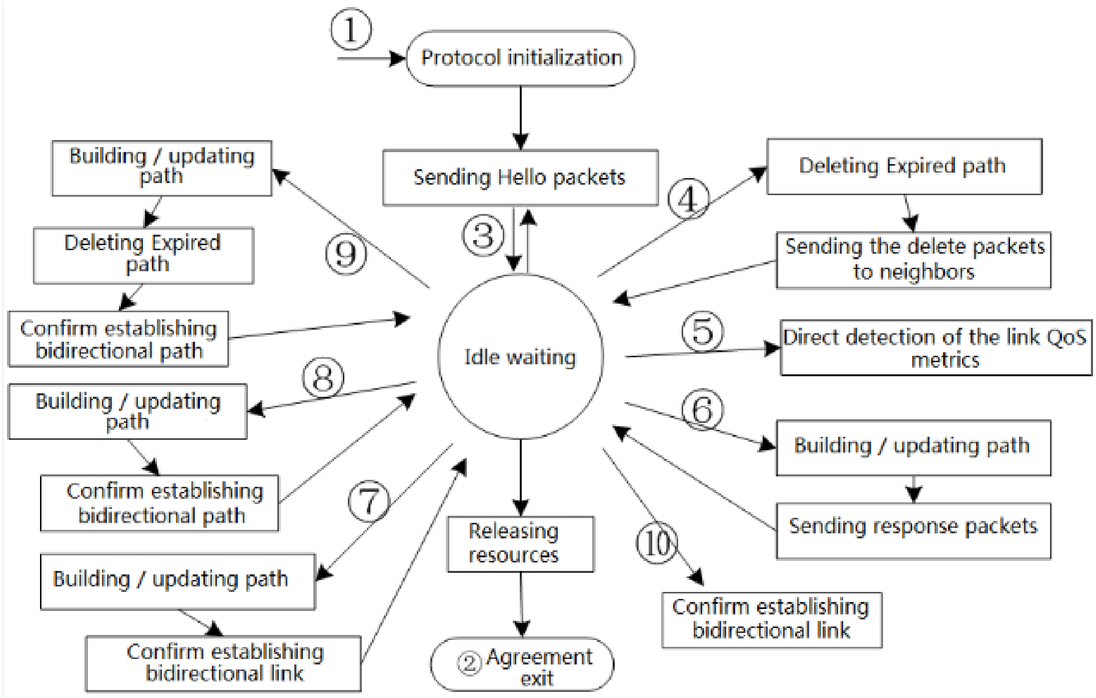


Figure 5-29 FSM mode of protocol

Protocol state set:

Over all, there are two states in this protocol: free waiting state and protocol event processing state. In the free waiting state, the protocol machine does nothing and waits for the coming events that initiate the protocol state transmission. The protocol event processing state is a brief busy state of the protocol machine to process all kinds of the protocol events. The detailed protocol events processing states are described as follows:

- Protocol initiation
- Protocol message packaging
- Protocol message sending
- Protocol message transferring

□New path construction

□Path information updating

□ deleting the path

□Two-way link confirmation

□Protocol resource releasing

The core of this protocol is the processing of the protocol message. The protocol machine makes the relative processing based on the received message. It returns to the waiting state after processing. The two timers use the interrupt mechanism. After the interruption mechanism, the interruption processing is done, and then the protocol retunes to the waiting state. From the FSM mode mentioned above, the protocol always repeats wait for the mission-processing when the mission returns back to the waiting state, and there is no deadlock in the protocol mode. Thus, the protocol has no mistakes in flow-processing design.

5.6 Routing algorithm

5.6.1 Routing algorithm classification and design requirements

The routing algorithm can be classified into two types: self-adaptive routing algorithm and non-self-adaptive routing algorithm [138]. The self-adaptive routing algorithm can feel the change of the networks and change the routing strategy according to the measurements and estimates. In the non-self-adaptive routing algorithm, the routing information has already been downloaded to the local when the networks are launched. When the network topology or other networks statistics changes, the nodes won't change the routing strategy according to the network change.

These two routing algorithms have their own advantages and disadvantages. The self-adaptive routing algorithm can timely change the routing strategy according to network change, but it is very complex to calculate with this algorithm and has a high consumption. Although the flexibility of non-self-adaptive routing algorithm is low the calculation is simple and the consumption will be low [139].

ADHOC networks are characterized by randomized moving of the nodes and a dynamic change of network topology. The radio channel will constantly change, which is influenced by the environment. Qos routing should timely select an optimized network topology path based on the link condition in order to supply the reliable QoS assurance. In order to implement the dynamic aesthesia to the change of the networks, self-adaptive routing algorithm is used in this protocol, which can improve an effective QoS routing assurance routing to ADHOC networks.

5.6.2MIA-QRP routing algorithm

ADHOC networks are mainly used for emergency communication and military communications. Now, there are many routing protocols supporting the QoS, but most of them use the node energy, with bandwidth, delay and some single QoS indicator as the judgments. In this protocol the average delay of link, average package loss rate and node signal strength are selected as the judgment standards to select the optimized routing that can satisfy the special requirements.

1． QoS

(1) Delay

The delay is the time needed to transfer a message or a grouping from a node to another in the network. It includes sending delay, broadcast delay, processing delay and queuing delay (delay = sending delay + broadcast delay + processing delay + queuing delay). The average delay index is regarded as one of the link judgment indices [140] [141]. For the multi-hop ADHOC networks, the total average delay of the link equals to the accumulation of the average delay of each single-hop link. The average delay reflects the effectiveness of network transmission. The less the delay is, the more effective it is. Especially for voice packages, too much delay will badly influence the quality of communication.

$$delay = \sum_{i=1}^{n} delay_i \qquad (5\text{-}2)$$

(2) Package loss rate

Package loss rate (loss) is the proportion of lost data packages in the total sent data packages during the link transmission. For the multi-hop ADHOC networks, the total average package loss rate of the link is the product of average package loss rate of each single-hop link. The package loss rate is related to the length of the data package and the sending frequency it also reflects network reliability. The less the package loss rate is, the more reliable it will be.

$$lose = \prod_{i=1}^{n} lose_i \qquad (5\text{-}3)$$

(3) Signal strength index

The signal strength [142] indicates the signal strength of the nodes in the relative surrounding points, which can reflect the communication quality of nodes and the condition of residual energy, and is regarded as one of the QoS judgment indexes in order to increase the stability of the routing.

$$\overline{strength} = \frac{1}{n}\sum_{i=1}^{n} strength_i \qquad (5\text{-}4)$$

2. MIA-QRP judgment mode

In this routing protocol a Multiple Indicator Adaptive QoS Routing (MIA-QRP) is proposed to improve the network service quality [143,144,145] by comprehensively balancing delay, package loss rate and signal strength of the nodes, the MIA-QRP can overcome the defects of a single consideration of the QoS index in the traditional algorithm, and select the optimized path timely by a self-adaptive algorithm determining the weight of each index with the entropy weight coefficient method.

For the original node S and the destination node D, the delay, package loss rate and the signal strength of each link can be calculated by the formula (5-2), the formula (5-3) and the formula (5-4) respectively. The set of the judgment indexes of the S and

D, which is R_j={ R_{j1}, R_{j2}, R_{j3}| j =1,2, ……, n }, can be obtained by combining each link. R_{j1} is average delay index, R_{j2} is link loss packets index, R_{j3} is the link signal strength index. Due to magnitude and dimension problem of each index, the judgment indexes matrix R_j is standardized as follows:

$$B_{jk} = \begin{cases} \dfrac{R_{jk} - \min R_{jk}}{\max R_{jk} - \min R_{jk}} & \text{For signal strength index} \\ \dfrac{\max R_{jk} - R_{jk}}{\max R_{jk} - \min R_{jk}} & \textit{For} \quad \text{average delay index and ink loss packets index} \end{cases}$$

(5-5)

$$R = \begin{bmatrix} R_{11} & R_{12} & R_{13} \\ R_{21} & R_{22} & R_{23} \\ R_{31} & R_{32} & R_{33} \end{bmatrix} \Rightarrow B = \begin{bmatrix} B_{11} & B_{12} & B_{13} \\ B_{21} & B_{22} & B_{23} \\ B_{31} & B_{32} & B_{33} \end{bmatrix} \qquad (5\text{-}6)$$

After the standardization, the value of the non-dimension and the magnitude is from 0 to 1. Assume that the relative weight of each index is $\omega_1 \geq 0$、$\omega_2 \geq 0$、$\omega_3 \geq 0$, and $\omega_1 + \omega_2 + \omega_3 = 1$, then the weighted assessment mode of each path is shown as follows:

$$u_j = \omega_1 H_{j1} + \omega_2 H_{j2} + \omega_3 H_{j3} \qquad (5\text{-}6)$$

where $H_{jk} = -B_{jk} \log B_{jk}, k = 1,2,3$

After the weight of each index is determined, the weighted assessment value of each path can be calculated. Thus the path with the highest assessment value can be selected.

3. Decision of weight

Based on the extreme property of entropy, when each system condition has the same probabilities, which is $P_j = \dfrac{1}{n}, j = 1,2\ldots\ldots, n$, the maximum value of the entropy is:

$$H_{\max} = \lg n = H\left(\frac{1}{n}, \frac{1}{n}, \ldots\ldots \frac{1}{n}\right) \tag{5-7}$$

When the entropy of one index gets larger, the difference of the relative index value between each link is less. Then the effects of the judgment index are less, and its weight value is less. The weight value of the judgment index mentioned above can be determined based on the characteristics of the entropy.

According to the standardized matrix B produced by judgment index matrix R, the close degree mode of each judgment index can be determined:

$$d_{jk} = \frac{D_{jk}}{\sum_{j=1}^{n}\sum_{k=1}^{3} D_{jk}} \tag{5-8}$$

$$D_{jk} = \begin{cases} \dfrac{B_{jk}}{\max\{B_{jk}\}} & \text{For signal strength index} \\[2ex] \dfrac{\min\{B_{jk}\}}{B_{jk}} & \text{For average delay index and ink loss packets index} \end{cases} \tag{5-9}$$

According to the definition of entropy, the importance of each judgment index can be measured by the following condition entropy:

$$H_k = -\sum_{j=1}^{n} \frac{d_{jk}}{d_k} \lg\left(\frac{d_{jk}}{d_k}\right) \tag{5-10}$$

$$d_k = \sum_{j=1}^{n} d_{jk}, k = 1,2,3$$

The H_k is normalized by the $H_{\max}$ based on the extreme property of the entropy to get the assessment importance entropy that characterizes the judgment index:

$$h_k = \frac{H_k}{H_{\max}} = -\frac{1}{\lg n}\sum_{j=1}^{n} \frac{d_{jk}}{d_k} \lg\left(\frac{d_{jk}}{d_k}\right), \quad k = 1,2,3 \tag{5-11}$$

In order to comprehensively evaluate each index, the comprehensive weights of the judgment indexes can be determined by h_k:

$$\omega_k = \frac{1-h_k}{\sum_{k=1}^{3}(1-h_k)} \quad 0 \le \omega_k \le 1 \qquad \sum_{k=1}^{3}\omega_k = 1$$

(5-12)

Thus, the judgment weights of the delay, package loss rate and the signal strength ω_1、ω_2、ω_3 can be determined. Related to the path weighted assessment mode, the nodes can select the path with the highest judgment to be the optimized path from the original node S to the destination node D by calculating the judgment value of each path.

5.7 Design and implementation of MIA-QRP protocol

5.7.1Embedded development condition

1. Hardware resources

Development mainframe: CPU Frequency 3.0GHz, Memory 1GB, Hard disk 512G

Target board: The friendly Arm mini development developed board, arm 9 Processor, 256M and flash

Wireless transceiver: 802.11xUSB Wireless network card, which uses the link rt73 USB Wireless LAN chip and supports 802.11a, b, g protocol.

2. Software resource

Fedora 10.0 Linux Operating system, Linux 2.6.25-14 Kernel version

Vmware7.0; Vmware7.0 Virtual machine software

The target board operates the embedded Operating system mirror, Linux 2.6.32.2 Kernel version.

Rt73 Wireless network card chip driver source code

5.7.2 Design and transplantation of wireless NIC driver

As shown in Figure 5-30, based on the TCP/IP network layer mode, the system structure of the Linux networks driver can be divided into 4 layers [146], namely network protocol interface layer, network device interface layer, device driven function layer and network device and media layer.

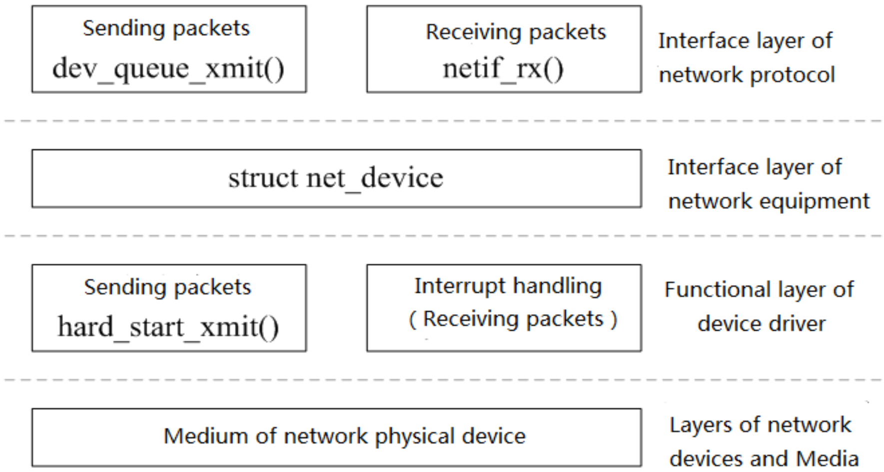


Figure 5-30 Architecture of network device driver

The network device and media layer is in the lowest layer of the network device driver structure. It supplies directly the driver to access the physical network device. The function of device driven function layer is to improve the operator interface to access the outside device for the upper program, and to implement the driver of the device. It starts the sending operation by the function of hard_start_xmit(), and implements the operations by the interrupt trigger in the network device. The network device interface layer improves an unified structure net_device, which is used to describe the characteristics and operations of detailed network device to the network protocol interface layer. This structure is the container of each function in the networks protocol interface layer. The network device interface layer is responsible for macro plan of device driven function layer of the hardware. The network protocol interface layer improves an unified sending and receiving interface to the networks layer protocol without considering the upper protocol. The dev_queue_xmit() function is used to send the data, the netif_rx() function is used to receive the data. The design of this layer makes it is unnecessary to consider the detailed implementation of the protocol for the last layer of the protocol.

5.7.3 Drive function and main data structure of network device

1. Drive function of network device

The main functions achieved by the network device driver include system initialization, data package sending and receiving etc. The system initialization is implemented by defining the initialization function init() in the data structure net_device. The initialization function init() will detect the hardware information of the device to determine whether to arrange the resource spaces to this device or not. After deletion, the initialization function will fill the information of this device into the data structure net_device and add this new device to the new device list.

The data package sending and receiving is the most important content in the design of the network device driver. Whether the programming of this driver is good or not will directly influence the overall quality of the driver. The sending of network device needs to use the dev_queue_xmit() function in the protocol interface layer, by which the pointer of the hard_header function in the data structure net_device is adjusted, the data in the socket buffer saved in the sk_buff will be read, and the data will be sent to the physical device. The receiving of the data package is always a netif_rx() function. When driver programs of lower layer hardware receive the data package, the hardware will create an interrupt signal. Then, the data in the socket buffer sk_buff will be queued in the upper protocol queue by the netif_rx_schedule function for the convenience of the following processing.

2. Main data structure of the networks driver

All network devices are abstracted as an unified interface in the Linux, which is the network device interface. It expresses the operation condition of the network device in the kernel by the structure variables of the structure net_device type, including loopback devices and hardware network device interface. The kernel administrates the entire network device from the device list in which the dev_base is the head pointer.

sk_buff structure is used to administrate the back T structure and plays an important role in the sending and receiving of data package. The data of each network layer in the Linux is sent by the sk_buff. In the network protocol interface layer, both kernel functions the dev_queue_xmit() and the netif_rx() use the sk_buff as the parameters.

3. Design and analysis of rt73 wireless network card driver

In the Linux, most of the drivers are based on the development approach of the module, and they can be loaded and unloaded freely. The design of this network card driver is developed according to the module, which sets the module_init as the driver entrance and sets the module_exit as the driver exit.

The main tasks to be completed by the design of the network device driver include network device registration, network device initialization, processing of data sent and received etc. It is also required to make the immediate processing in case of timeout and breakage of transmission.

(1) Initialization of the network device driver

The work of module_init is to register the rtusb driver to the kernel USB Drive chain. The corresponding program is return usb_register(&rtusb_driver), where the definition of the rtusb_driver is described as follows:

```
struct usb_driver rtusb_driver = {
#if LINUX_VERSION_CODE < KERNEL_VERSION(2,6,15)
    .owner = THIS_MODULE,
#endif
    .name="rt73",
    .probe=usb_rtusb_probe,
    .disconnect=usb_rtusb_disconnect,
    .id_table=rtusb_usb_id,
```

#ifdef CONFIG_PM

.suspend = rt73_suspend,

.resume = rt73_resume,

#endif

};

The usb_rtusb_probe function is the most important, and is mainly used for device detection and initialization of the needed kernel resource. The rt73_suspend and the rt73_resume are related to the power administration, such as how to work when it receives the suspension, and how to recover at the resumption. The usb_rtusb_disconnect will call the interface after the usb device is removed from the system. The rtusb_usb_id is the usb devices ID lists driven by the rtusb_usb_id.

After the module initialization and registration to the system, the driver will scan the system bus to check if the relative devices of this driver are on the bus. If there are devices on the bus, the probe function will be called, or the device is inserted to the system after the initialization of the driver.

According to the design of network device driver, most members in the net_device structure need to be instantiated. The relative content of this network card driver is defined as follows:

```
netdev->priv_flags = INT_MAIN;
    netdev->open = usb_rtusb_open;
    netdev->hard_start_xmit = usb_rtusb_sendpkt;
    netdev->stop = usb_rtusb_close;
netdev->do_ioctl = rt73_ioctl;
```

(2).Sending of network data package

According to the instantiated code content of the net_device structure, the data sending of the networks card is finished by calling the usb_rtusb_sendpkt, which will call the RTMPSendPackages function to finish the sending of the data. The dev->hard_start_xmit is a callback function, and its value is set as dsr_dev_start_xmit.

This function is not called by the drive layer, but it is called by the upper protocol. For example, when the IP or ARP layer needs to message, it can decide use which network device (net_dev) to transfer the data according to the destination IP address, and it will call its hard_start_xmit callback function. The call and control of the TCP/IP protocol stack will have been finished in the kernel, and they will use the callback function until the data comes to the device. This is the principle of the driver implementation. The network drive is the same as other drivers.

For the network card, the true data sending is finished by the USB. The RTUSBKickBulkOut function will be called in the RTMP Send Package function to finish the data sending.

(3) Receiving of the networks data package.

In the process of data package receiving, an interrupt will be generated when the data packages arrive at the network device, and inform the driver to receive the data packages. The interrupt processing program will apply for a period of addresses to the system as the sk_buff buffer to save the received data. After the received data is saved to the buffer, it is still needed to fill in the other parts information, such as the structure of specified devices, data frame types and link layer data types. Finally, by using the protocol interface layer function netif_rx() calling the RTUSBRxPackage(data) function sending the data packages to the upper layer for processing.

There is 802.11 protocol stack processing in the RTUSBRxPackage function. After the USB part receives the data, it will call the receiving function of network card driver for simple protocol stack processing and copy the data to the upper data layer.

4. Compilation and transplantation of the wireless LAN driver

After the design of network card driver, the network card needs to be recompiled in order to use the network card driver on the embedded Linux platform. This driver uses the arm-linux-gcc-4.3.2 cross-compiler based on the mini2440 development board for the compilation. The processing of compilation to the driver is described as follows:

Correct the compilation files

Enter “2010_0817_RT73_Linux_STA_v1.1.0.4/Moude” catalog and open the “Makefile” file under the catalog. Make the following corrections:

Correct the platform settings, use the embedded platform, PLATFORM= CMPC

(2) Correct the compiler settings, use cross-compiler and link tools CC :=arm-linux-gcc , LD :=arm-linux-ld

(3) Correct the kernel compiled head file catalog, LINUX_SRC = /root/linux-2.6.32.2, this catalog is the saving path of the kernel head file.

2. Compilation

(1) Execute the command “make old config && make prepare && make modules_prepare” to make preparation for the compilation of the kernel module.

(2) Enter the catalog “2010_0817_RT73_Linux_STA_v1.1.0.4/Moude”, and execute “make -C /root/linux-2.6.32.2 M=`pwd` modules” to compile the networks card driver. After the compilation, the driver kernel module files are generated finally: rt73.bin, rt73.koand rt73sta.dat. The network card can be used on the destination board if these files are downloaded and installed on the destination board.

5.8 Architecture of protocol software

There are two modes of design of embedded Linux based software, namely kernel module design and user application software design. The kernel module development program usually begins to run into the kernel state with the start of the operation system. The development requirements of kernel program are high, which needs to completely consider the calling mechanism of the kernel program. Designed for the safety and convenience, this protocol applies the user application program so that the users can design and administrate the program easily.

5.8.1 Software layers model

According to the OSI design mode, layer modular design is also used in this routing protocol to divide the protocol into four layers, each of which implements the relative function. The layers call each other by the interface, and complete the function of the routing protocol with help of each other. As shown in Figure 5-31, starting from the top, this routing protocol software model can be divided into routing algorithm execution layer, protocol event processing layer, protocol message analysis layer and original network data package capture layer.

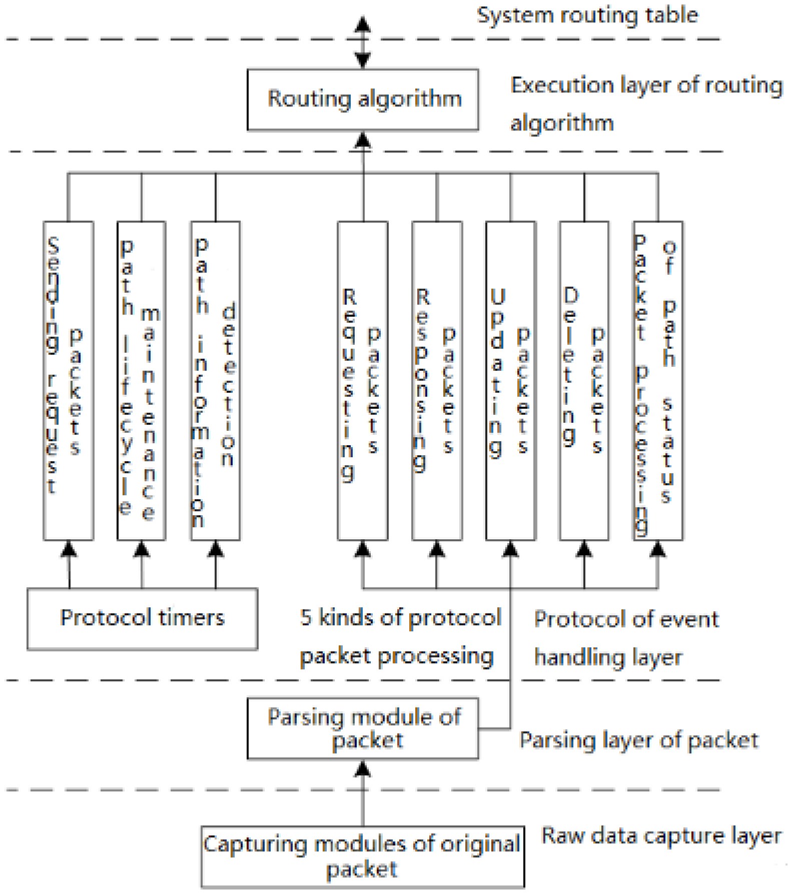


Figure 5-31 Model of protocol layers

1. Original data package capture layer.

This is the bottom layer in the protocol layer model, mainly responsible for supplying the original data related with this protocol to the upper layer. The function of this layer is implemented according to the function of the OSI based data link layer.

The captured original data is the MAC frame data of the link layer, which has the transparent and reliable data characteristics. The data captured by this layer will be saved to the buffer of the original data for the use of the upper layer. Meanwhile, in order to obtain the QoS parameter index of the link, this layer implements the statistics function for the link average package loss rate and the average delay and the detection function of the nodes signal strength to integrate the captured data and the detected data, which is regarded as the basic data processed by the upper layer routing.

2. Protocol message analysis layer.

This layer is mainly responsible for extracting the data related to this protocol from the original data buffer saved from the original data package capture layer, and saves the data to the protocol data buffer for the calling of the upper layer. As the data captured from the lower layer are all Ethernet data frames captured from the data link layer, in addition to the data message types of this protocol, there are still other networks protocol data frame types, such as IP, ARP data, PPP data. Thus, the type mark field data of the message in this protocol needs to be designed.

Based on the Ethernet format, the types of Ethernet are marked and distinguished according to the value of Length/EtherType field. The different value indicates the different types of the data frame. When the value of the Length/EtherType field is more than or equal to the hexadecimal 0x0600, it indicates the MAC client computer. For example, the value of 0x0800 means IP datagram; the value of 0x0806 means the ARP datagram, and the value of 0x8863 indicates PPPoE protocol datagram. In order to mark the datagram type of this protocol, the value of the Length/EtherType field in the Ethernet is set as 0x6c6c, this layer just needs to analyze the data frame with the value of the type marked field, which equals to 0x6c6c, in the original networks data buffer. The other types of data frame will be abandoned directly.

3. Protocol event processing layer.

This layer is the core of this routing protocol. It creates and maintains the network topology path table, generates and updates the path information, and supplies the foundation for the routing algorithm. This layer consists of two modules: protocol message processing and timing clock event processing. The protocol message-processing module is responsible for confirming the communication link, path findings, path maintenance, and inquiry and confirming path state. The clock provides basic timing for the protocol, and assists the nodes to accomplish the regular message request, position update service and maintenance of life cycle. This layer consists of four parts: update timer module, deletion timer module, path findings module and path maintenance module, which work together to accomplish the processing of the protocol message and calculate the optimized path to the destination nodes.

4. Routing algorithm execution layer.

The assignment of this layer is to calculate the optimized path to the destination node according to the content calling routing algorithm in the network topology information table. Meanwhile, it is responsible for maintaining the system kernel routing table and adding the optimized path to the system kernel routing table and deleting the expired path.

5.8.2 Threading model

Based on the protocol layers model, this protocol applies the technologies of the multi-threading which designs three threading and three timers to accomplish the basic work of the protocol. The three basic threading models are the original network data package capture threading, the protocol data package analysis threading and the protocol message processing threading. These three threads keep working with the start of the protocol and will be destroyed until this protocol quits.

In this protocol, the method of creating the temporary threading is used to implement the function of three basic timers. When the time of the timer comes, a temporary threading will be created to implement the corresponding assignment. This threading is destroyed after the assignment is accomplished. The creation of the timer starts with the beginning of the protocol, and the timer will stop until the protocol quits.

The routing selection algorithm of this protocol is designed as a call function. The part processing assignments of the protocol message processing threading is called in need to save the cost and improve the performance. The model of the protocol threading is shown in Figure 5-32.

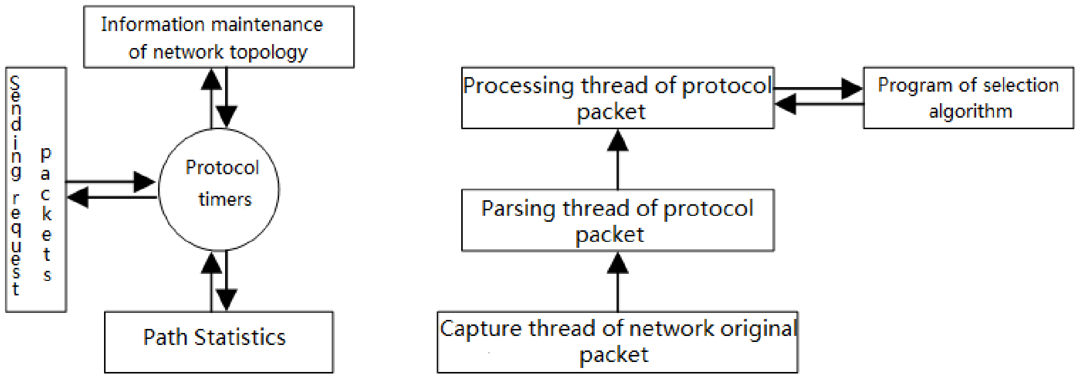


Figure 5-32 The model of the protocol threading

5.8.3 Data stream of protocol

According to the protocol layers design model, the data stream of this protocol is shown in Figure 5-33.

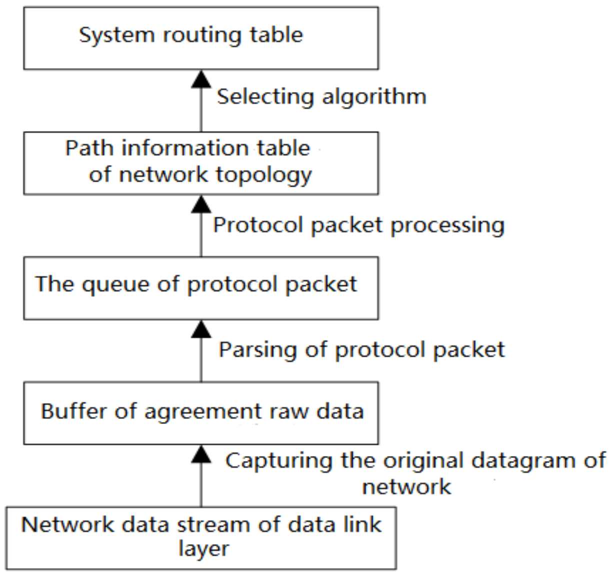


Figure 5-33 Data stream of protocol

The data of this protocol is captured and obtained according to the networks data stream of the data link layer. The obtained data frame is saved to the protocol original data buffer by the processing of the networks original data package capture layer. The protocol data analysis layer will extract the data of this protocol from the original data buffer to save the data to the protocol message buffer queue. The protocol message-processing layer will make the further process to the protocol message buffer queue to generate the network topology path information table. Finally, the protocol message processing threading selects the optimized path of the network topology by calling the routing algorithm, and the selected optimized path is added to the system kernel routing table.

5.8.4 Design of the key module and Process flow

1. Synchronization of multi-threading

In the process of protocol data stream, the networks original data capture threading will timely extract the networks data frame and save it to the networks original data buffer. Meanwhile, the protocol message analysis threading will timely extract the data in the networks original data buffer to extract and filter this protocol message. The protocol threading makes a shared access to the data in the networks original data buffer. If there is no relative threading synchronization, the unforeseen data accessing errors will be generated. There is a shared access to the protocol message buffer queue between the protocol message analysis threading and the protocol message processing threading.

The Linux provides several process methods for the synchronization of multi-threading, but the usual methods are mutual exclusion, condition variable and semaphore. This protocol implements the data synchronization of the multi-threading by the method that combines the mutual exclusion and the condition variable, and implements the gradual visit of the multi-threading to the shared resource by using the mutual exclusion. This protocol also combines a condition variable to control the access and the dormancy of threading in case of multi-threading access blocked caused by only using the mutual exclusion, and increases the resource utilization and the code execution efficiency.

The mutual exclusion and the condition variable used in this routing protocol are defined as follows:

pthread_mutex_t raw_lock;

pthread_mutex_t pro_lock;

pthread_mutex_t topo_lock;

prthread_cond_t cond_raw;

prthread_cond_t cond_pro;

Where the mutual exclusion raw_lock and the condition variable cond_raw are used for synchronization shared access of the network original capture threading and the protocol message analysis threading to the networks original data buffer. The mutual exclusion pro_lock and the condition variable cond_pro are used for the synchronization shared access of the protocol message analysis threading and the protocol message processing threading to the protocol message buffer queue.

Where the mutual exclusion and the condition variable are used, mutual exclusion locked and unlocked function, condition dormancy and the wake-up function are described as follows:

pthread_mutex_lock(pthread_mutex_t *mutex), the mutual exclusion locked function

pthread_mutex_lock(pthread_mutex_t *mutex), the the mutual exclusion unlocked function

pthread_cond_wait(pthread_cond_t *cond,pthread_mutex_t *mutexz, Consition waiting, which leads the threading to the freedom waiting state

pthread_cond_broadcast(pthread_cond_t *cond), condition activation, which wakes up the free waiting threading

The threading synchronization flow used by the mutual exclusion and the condition variable is shown in Figure 5-34.

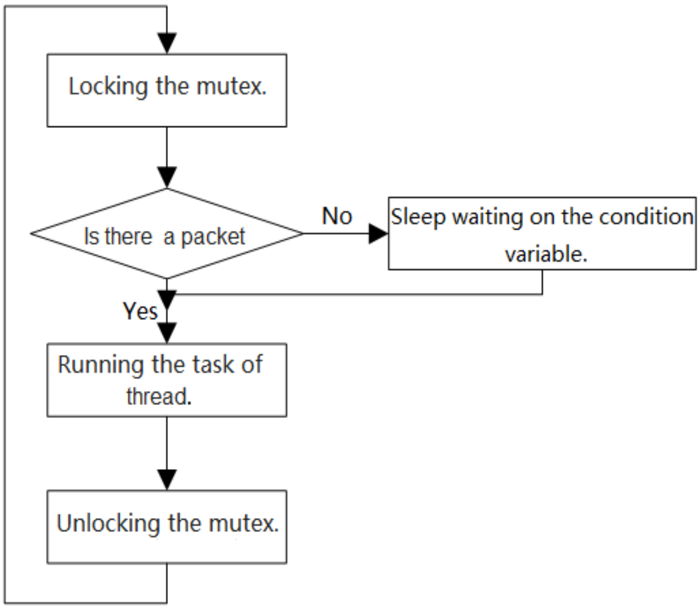


Figure 5-34 Synchronization flow chart of multi-threading

2. Data buffer queue

Because this protocol needs to timely receive the networks data package and processes the protocol message, it is needed to design a data buffer for this protocol in case of loss of data received and processed. The design can effectively process the saved data in case of the data lose.

The data buffer of this protocol, which applies to the loop queue, is implemented by the structure. The saving unit of the loop queue consists of saving data and data length. The detailed data structures are defined as follows:

```
typedef struct raw_package_unit{
unsigned char data[1518];
unsigned short len;
}raw_unit,*praw_unit;
```

3. The sending and receiving of the data package

All original data of this protocol is captured by the data link layer. In the condition of Linux, the libpcap data package and the creation of the socket are used to implement the capture of the networks data frame, where the libpacap is the open source implementation code of the network's programming on the Linux stage [147]. Based on the practical experience of the author to the Linux networks programming, this protocol is implemented by applying the creation of socket under the Linux. The direct access of the data in the networks data link layer is implemented by creating the networks original socket to capture the networks original data package.

The function prototype of the Linux networks socket interface is the int socket (int domain, int type, int protocol. In order to directly access the data in the data link layer, the parameters are set as follows:

Domain is socket field, and is set as PF_PACKAGE

"Type" is the type of the socket. The usual types are the stream socket (SOCK_STREAM), the data gram socket (SOCK_DGRAM) and the original socket (SOCK_PACKAGE. The socket is set as SOCK_PACKAGE in this protocol.

The protocol is the socket protocol, and is set as htons (0x0003) in this protocol.

The data in this protocol capturing the threading needs to timely catch the networks data, and set the networks socket as the non-blocked state. Then the function fcntl (s, F_SETFL, O_NONBLOCK) is called to finish the settings.

After the creation and settings of original socket, the function send to() and recvfrom() is used to implement the access the data in the data link layer. The prototype of the function interface is described as follows:

sendto(int sock, const void *buf, size_t len, int flags, const struct sockaddr *to, socklen_t tolen);

int recvfrom(int sockfd,void* buf,int len,unsigned int flagsstruct sockaddr* from,int* fromlen).

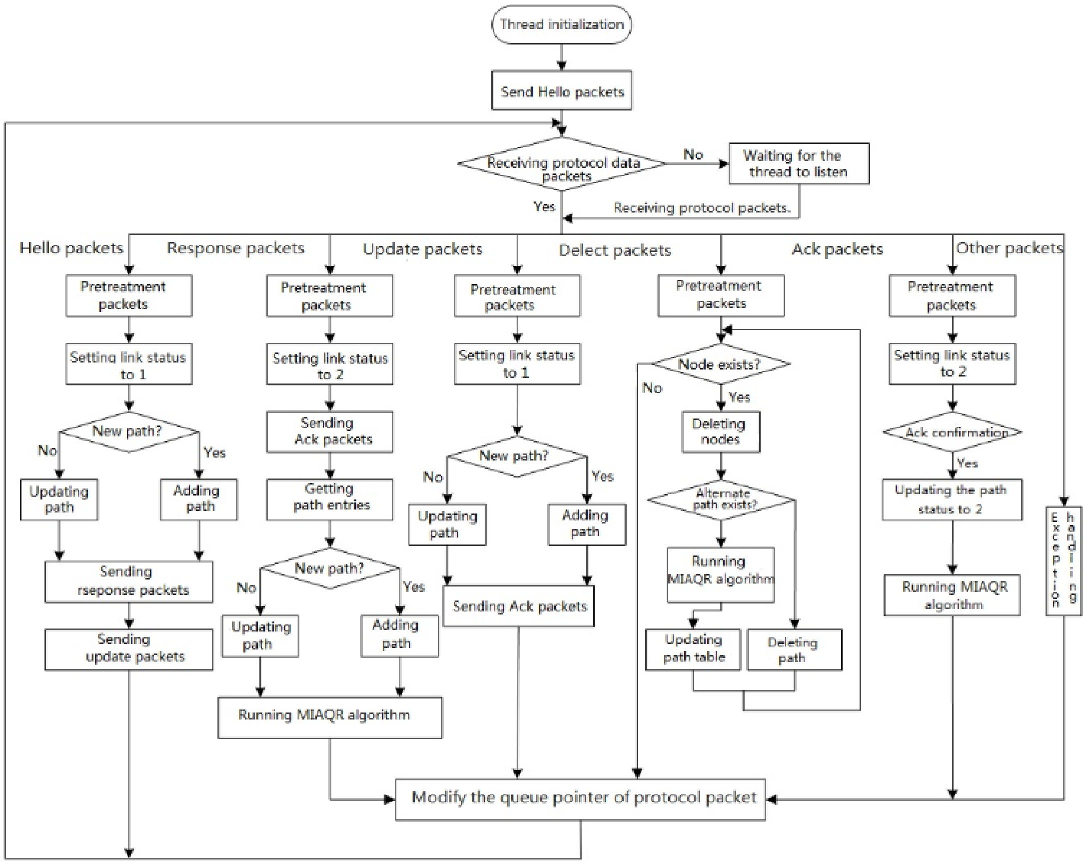


Figure 5-35 Flow chart of protocol message processing

4. Processing flow of protocol message

The path findings and maintenance in this protocol are implemented by the effective processing of the protocol event process layer to this protocol message. The processing protocol message is the key to process the data in this protocol. The message processing flow in this protocol is shown in Figure 5-36.

According to the protocol message processing flow chart, this routing protocol extracts the protocol message one by one from the protocol message buffer queue first. Then the protocol runs the switch branching processing based on the type of the message, and calls different message processing programs to implement the message processing.

The protocol message processing designed in the protocol has a pretreatment. Each type of the message processing branches firstly constructs a piece of network topology information by the pretreatment of the message. Then the network topology table is inquired to detect if there is the same network topology information. If no, a new piece of topology information will be added in the network topology information, otherwise, the content of the network topology information table is updated according to the message content. The protocol message pretreatment procedures are shown in Figure 5-36.

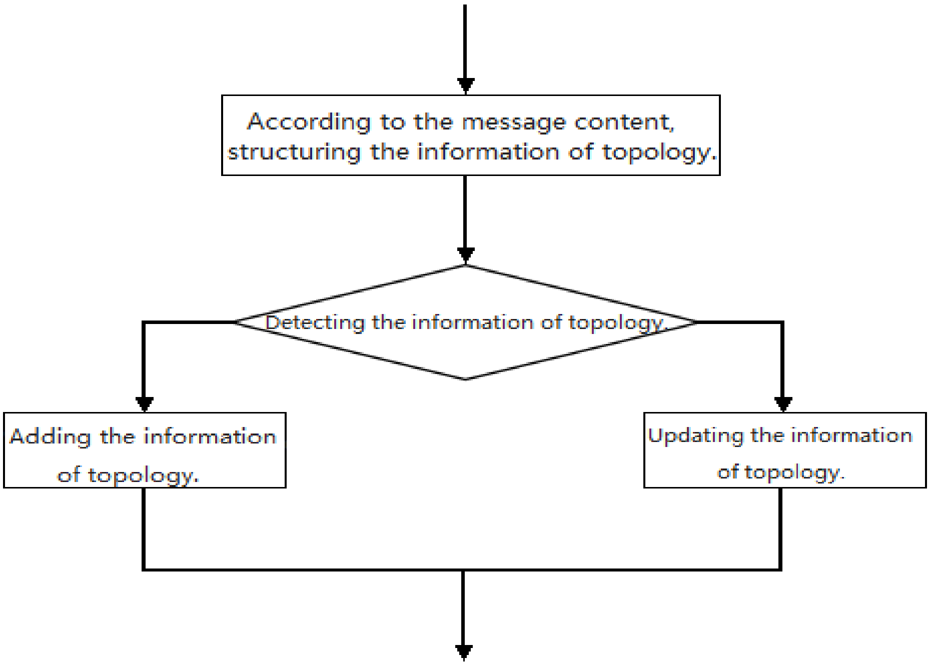


Figure 5-36 Message pretreatment procedures

In this protocol, an optimized path selection algorithm is designed. According to the protocol threading model, the routing algorithm will call in the message processing as needed

5. Protocol timer

In this protocol, three modules are designed which accomplish the periodical sending of node broadcast message, expired path information detection and link parameter indexes detection respectively. The function of each timer has been described in the last section. Now the operations of the timers are described as follows:

Linux arranges three internal timers for each assignment [148]. When the time comes, the ITIMER_REAL real-time timer will send the SIGALRM signal to the process, ITIMER_VIRTUAL timer will send the SIGVTALRM signal to the process and the ITIMER_PROF timer will send the SIGPROF signal to the process. An initial value is given to the timer, which decreases with time and sends the signal to the process until it decreases to 0, and then it will return to its initial value. The ITIMER_REAL real-time timer is used for the implementation of this protocol, which can timely send the SIGALRM signal to the process and run the relative functions.

Linux uses timers, which need the initialization works and relative signal processing mechanism. In the design of this protocol, the initialization and signal processing mechanism of the timers are accomplished by calling the corresponding function. The prototype of each function is:

int setitimer(int which, const struct itimerval *value, struct itimerval *ovalue)

The set timer function is used to accomplish the timer initialization. Each parameter is set as follows:

Which is the type of the timer, which is set as ITIMER_REAL

Interval value of the timer. The detailed interval of the timer can be set by this structure, which can be accurate to a microsecond.

ovalue is used to save the previous value. It is not used usually, and is set as the NULL here.

int sigaction(int signum,const struct sigaction *act ,struct sigaction *oldact)

The sigaction function is used to create the signal processing mechanism of the timers. Each parameter is set as follows:

signum is the signal type, which is set as the SIGALRM signal type sent from the ITIMER_REAL timer act is the structure type. The call function of the SIGALRM signal processing can be set by the member sa_handler of the structure.

The object pointed by the old act is used to save the processing to the old corresponding signal, which is set as NULL.

In the design of the timer, the Linux system calls the timer signal to execute the function by the method of creating the temporary threading, and accomplishes the operation assignments of the timer. After completion of assignment, the threading resource is released.

6. Design of routing algorithm program.

According to the protocol-threading model designed in this protocol, the routing algorithm of this protocol runs the calling the execution by the protocol message processing the threading to decrease the recourse cost largely, and improve the executive efficiency of the program. The core idea of this protocol algorithm design is to calculate the optimized path from the original node to the destination node according to the path information in the network topology information table and the MIA-QRP algorithm theory, and to improve a reliable QoS security service to the AD HOC networks.

In the program of protocol message processing, after execution of the "response" message and "ack" message, the function executed by the routing algorithm will be called. The execution procedures of routing algorithm is shown in Figure5-37.

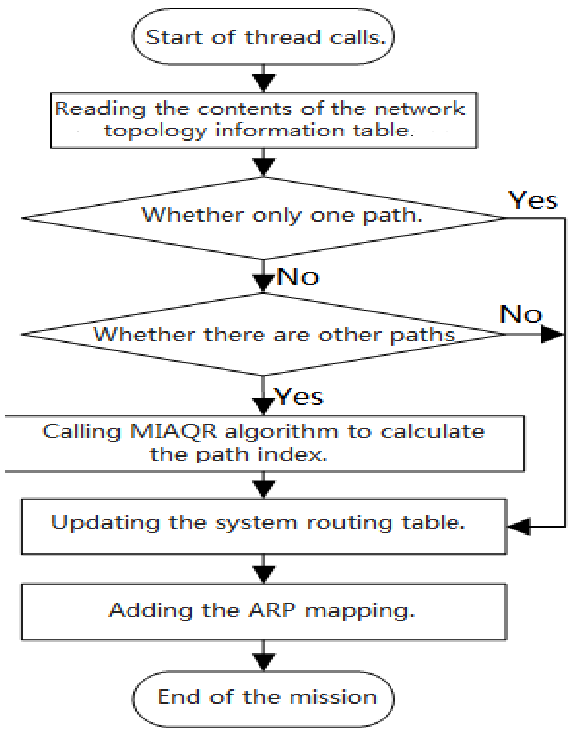


Figure 5-37 Execution procedures of routing algorithm program

When the routing algorithm program is called, it will first read the path information between the original nodes to the destination node from the network topology information table in order to detect if there is only one accessible path. If there is only one path, then it will be directly added to the system routing table, otherwise all the accessible information will be collected from the topology information table to calculate the optimized path in all accessible paths by calling MIA-QRP path selection algorithm, and to update the system routing table and ARP table. When all the path information of the nodes is processed, the assignment is over and will quit.

7. System routing table and ARP table operation

The network communication routing selection of Linux system is implemented by the inquiry operation of system routing table. The path information obtained from this protocol is applied by the other networks program, and is added to the system routing table. Thus, the system() function is further called to update and maintain the system routing path.

The operation of using system() function to the system routing table[148] is described as follows:

For example, add it to 192.168.1.170 direct routing

system ('route add –host 192.168.1.170')

add it to 192.168.1.171 routing and forwarded by the 192.168.1.170

system ('route add –host 192.168.1.171 gw 192.168.1.171')

delete 192.168.1.170 direct routing to the nodes

system ('route del –host 192.168.1.170')

delete the 192.168.1.171 routing and forward it by 192.168.1.170

system ('route del –host 192.168.1.171 gw 192.168.1.171')

In the Linux system, the kernel routing table accomplishes the routing function with the connection of the ARP table. The corresponding relation between the IP address and the hardware address can be inquired by the ARP table. The ARP table is also used in the networks address analysis. The ARP table information should be updated when the routing table is added. The operation of the system ARP table is described as follows:

Assume that the IP address of the direct routing node is 192.168.1.170, its MAC address is D8:5D:4C:7C:13:DF

system (’arp –s 192.168.1.170 D8:5D:4C:7C:13:DF’)

system(’arp –d 192.168.1.170 D8:5D:4C:7C:13:DF’)

If the IP address of the node is 192.168.1.171, the next hop from this node to the next destination node is 192.168.1.170

add the corresponding ARP table: system(’arp –s 192.168.1.171 D8:5D:4C:7C:13:DF)

Delete the corresponding ARP table: system(’arp –d 192.168.1.171 D8:5D:4C:7C:13:DF’)

5.9 Summary

According to the multiple QoS parameters including delay, loss of package and quality, a new routing algorithm is proposed. This routing protocol is implemented by five kinds of protocol messages, including network route discovery and maintenance, and through the programming, it is to realize link parameters acquisition, selection of optimal path and update of system routing table. In the development of protocol implementation, wireless network card driver is analyzed. According to the design principle of the protocol, the software architecture of the protocol is given in this chapter. The protocol is designed in detail.

Chapter 6 SMAC-SD Protocol

6.1 The improved SMAC protocol

Route protocol need to be supported by MAC,S-MAC protocol can guarantee the nodes to be periodical monitoring/sleeping mechanism to reduce the energy cost. However, in order to satisfy differentiated Services in WSN, S-MAC protocol should be improved .The thesis proposed an improved protocol: SMAC-SD.

The main principles of the SMAC-SD protocol are: it follows the periodical monitoring/sleeping mechanism of S-MAC protocol, the message transmission mechanism and the selection and maintenance scheduling, and the time synchronizations and NAV mechanism. Its improvements include principle of the differentiated services; priority mechanism based on service queue; channel multi-requirements mechanism.

6.2 Mechanisms of SMAC-SD Protocol

1. Secure transport mechanism of the service differentiation.

(1). Principle of the differentiated Services

The standard of the differentiated services is related to the traffic of application lay.

From the point of view of network QoS, how the data is delivered to the sink and corresponding requirements are concerned. Generally, there are three basic data delivery models, i. e. , event-driven, query-driven, and continuous delivery models [149]. Before presenting the application requirements, some factors that characterize are provided as follows:

Real-time voice, image, or video data: Real-time data is delay-constrained and has a certain bandwidth requirement. Packet losses can be tolerated to a certain extent.

Non-real-time data: The sink may want to collect periodic data from the sensor field.

In this project, information of time-sensitive will be taken in consideration.

This protocol defines two transaction classes: important transaction and general transaction.

Important Transaction: low tolerance to the delay and high priority in the networks transmission. It has a higher priority access channel queue mechanism.

General Transaction: high tolerance to the delay, and low priority in the networks transmission.

For the different WSN, the users can define which transaction is the important transaction depending on the actual demand of using.

(2) Probability priority mechanism based on service queue

SMAC-SD defines two queues of access category (AC), and each queue has different priorities of the data transmission.

Assume:

The minimal backoff windows are CW_{min}; maximal backoff window is CW_{max} and the Arbitration Interframe Space is (AIFS).

CW_{min} [1], CW_{max} [1], and AIFS [1] are for the high priority access class;

CW_{min} [0], CW_{max} [0] and AIFS [0] are for the low priority access class

where CW_{max} [0] $\geq$ CW_{max} [1], CW_{max} [0] $\geq$ CW_{max} [1] , AIFS[0] $\geq$AIFS[1].

Two transmission queues are arrayed in the base station. Every sequence supports an access classification, and its behavior is similar to DCF mechanism [145]. Every queue runs a DCF function. The bigger backoff windows is, the lower the priorities of access control is.

The access classifications are divided into two types. It is assumed that there are n active base stations in the WSN and every base station has the complete two queues, there are 2n queue object, which means there are 2n base stations, their channel compete by IEEE802.11DCF, as figure 6-1.

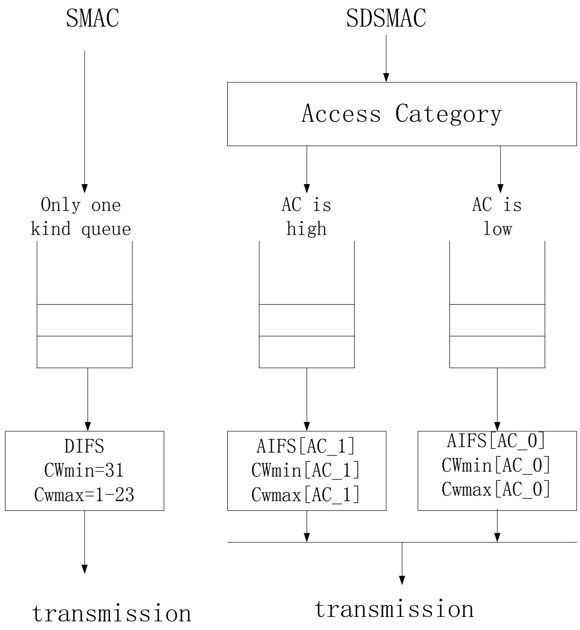


Figure 6-1 Flow Chart of the Probability priority mechanism of the Channel Access

3) Channel multi-requirements mechanism

SMAC-SD protocol uses the probability priority mechanism of the channel access, which can guarantee the higher efficiency of accessed data to the channel compare with the general transaction. However, the probability of accessing the channel is not completely equal to the successful probability of accessing the channel. The successful probability of accessing the channel for the important transaction is related to the data stream of the general transaction. The successful probability of accessing the channel for a priority transaction in the nodes is [150,151,152]:

$$P_{si} = n\tau_i(1-\sum_{i\in m}\tau_i)^{n-1}\prod(1-\tau_i) \qquad (6\text{-}1)$$

P_{si} is the successful probability of accessing the channel of the transaction data with the priority i, n is the number of the nodes, τ_i is the access probability of the transaction with the priority i, and m is the number the access transaction.

With the analysis, the general transaction will influence the important transaction by the following aspects: the data packet of the general transaction collides with the important transaction; generally, the channel occupied time after the successful sending in the general transaction makes the delay to the channel of the data access in the important transaction. This will lead the channel competition advantages of the data stream of the important transaction to be reduced by the large existed data stream of the general transaction under the intense condition in the networks.

According to the probability priority mechanism of channel access, the channel multi-requirements mechanism improves the handshake mechanism of the queues with high priority.

The access mechanism of all transactions in the SMAC protocol is RTS-CTS-DATA-ACK. RTS-CTS means Request To Send/Clear To Send. Based on the principle of the differentiated services. Access of channel supplies one more passing RTS frame requirement. The mechanism is showed:

1. Important transaction: the interFrame space of the waiting queues with high priority in the important transaction is adjusted as follows:

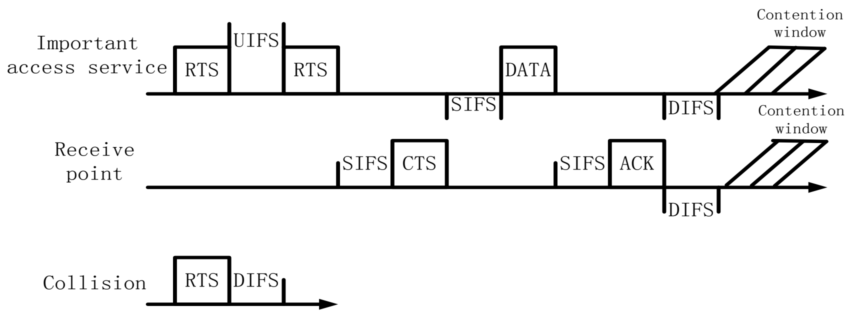


Figure 6-2 Access and RTS/CTS mechanisms for Important Transaction

If a node requires sending RTS request frame is successful, the receivers will immediately responds to agree to send the CTS frame, and the senders begin to send the data after receiving the CTS.

If the first requirement is failed, then it will resend the RTS requirement with the UIFS interval, UIFS=SIFS+2*slot time. If the requirement is successful at this time, the receivers will responds CTS frame, and the senders begin to send the data after receiving. If the requirement is failed again, it turns into the backoff process.

2. General transaction: the timing chart of the waiting queues with low priority in the important transaction is adjusted as follows:

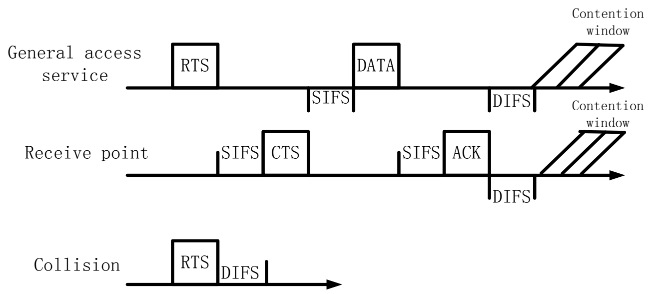


Figure 6-3 Access and RTS/CTS mechanisms for General Transaction

For the data stream of the general transaction with the low priority, Access and RTS/CTS mechanisms is showed by figure 6-3.

If a node requires sending RTS request frame is successful, the receivers will immediately responds to agree to send the CTS frame, and the senders begin to send the data after receiving the CTS.

If the first requirement is failed, then it turns into the backoff process.

The flow chart of the multi-appointments mechanism based on the service differentiation is shown as follows:

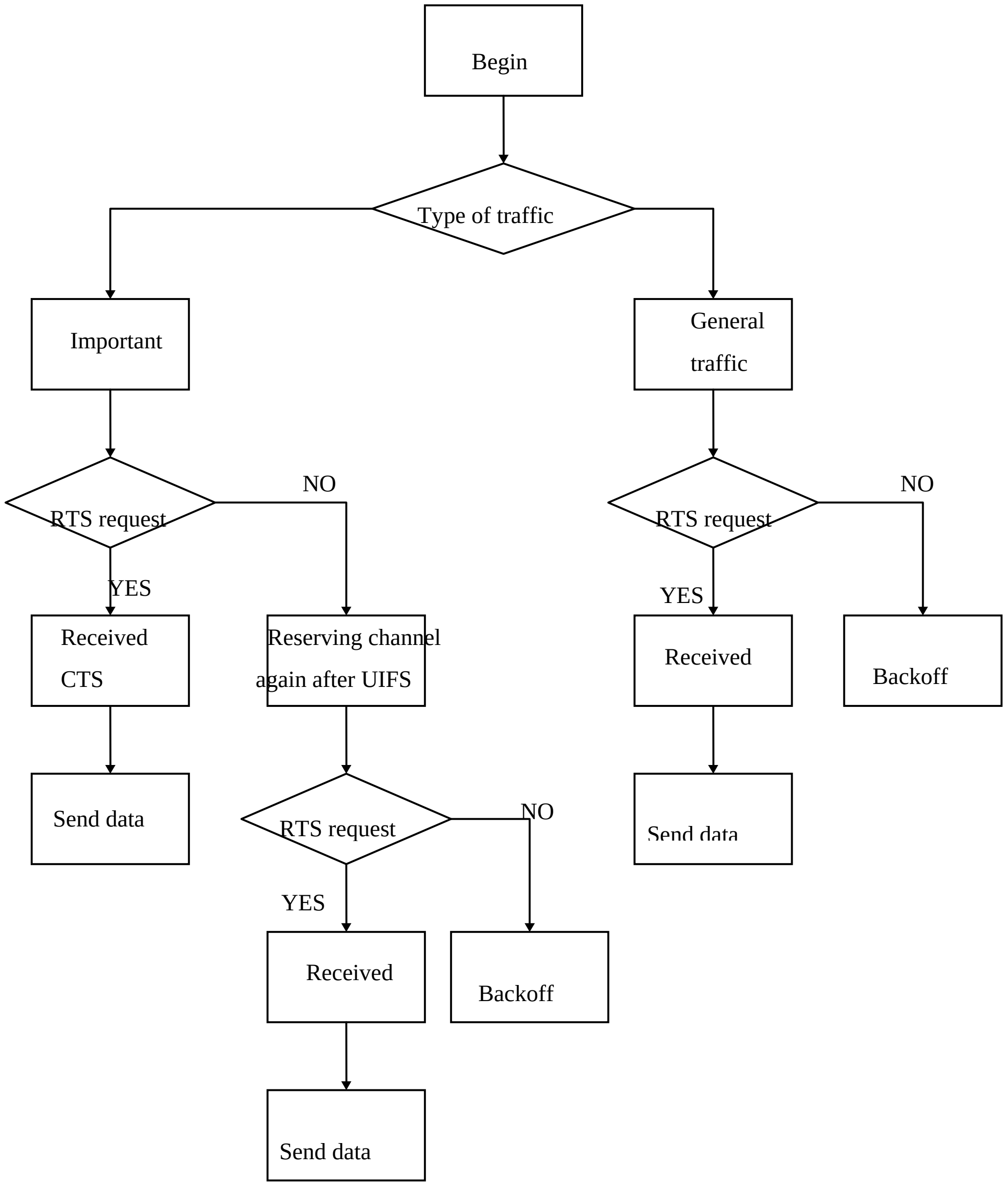


Figure 6-4 Multi-channel request mechanism flowchart

6.3 Theoretical analysis of the SMAC-SD

Assume that there are n nodes in the WSN sharing a radio channel without considering the problems of the hidden terminal and channel fading. For the channel access process of a node, set $s(t)$ as the back off level of the node at the moment, the range of the value is $[0, m]$, where m is the value of maximal back off. The $b(t)$

stands for the value of back off counter at t moment, the range of the value is $[0, W_{i-1}]$ where $W_i = 2iW$, the range of i is $[0, m]$; $W = CW_{\min}$, $CW_{\max} = 2mW$. The two random processes described by $s(t)$ and $b(t)$ are obviously not the Markov process. Regard these two non- Markov random process as an entirety and use two-dimensional random process $\{s(t), b(t)\}$ to demonstrate the channel competition process of this node. The status transmission is shown in Figure 6.5.

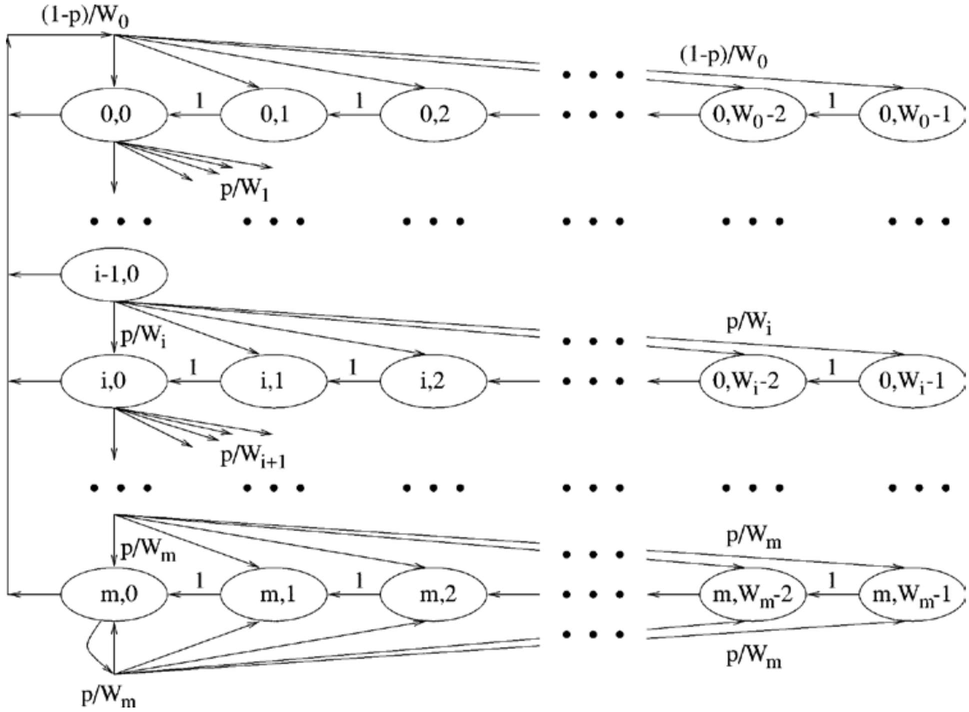


Figure 6-5 Flow chart of the two-dimensional Markov process

Assume the probabilities of data frame collision are not related to the former collision numbers, and the collision probability p is constant and independent. At the status $\{s(t+1), b(t+1)\}$ of $t+1$ moment, two-dimensional random process is only related to the former status {s(t)，b(t)} at t moment. It has no relationship with former status such as {s(t-1)，b(t-1)}, and the time and the status are discrete. Above all, the random process $\{s(t), b(t)\}$ is a two-dimensional Markov chain. To simplify the analysis, set the transmission probability as:

$$P\{i_1, j_1 \mid i_0, j_0\} = P\{s(t+1) = i_1, b(t+1) = j_1 \mid s(t) = i_0, b(t) = j_0\} \tag{6-2}$$

$$P\{i, j \mid i, j+1\} = 1 \qquad 0 \le i \le m, \quad 0 \le j \le W_i - 2 \tag{6-3}$$

$$P\{i+1, j \mid i, 0\} = p \big/ Wi+1 \qquad 0 \le i \le m-1, 0 \le j \le W_{i+1} - 1 \tag{6-4}$$

$$P\{m, j \mid m, 0\} = p \big/ W_m \qquad 0 \le j \le W_m - 1 \tag{6-5}$$

$$P\{0, j \mid i, 0\} = (1-p)W_0 \qquad 1 \le i \le m, 0 \le j \le W_0 - 1 \tag{6-6}$$

Formula (6.2) shows that the backoff counter will subtract 1 immediately when the backoff begins. Formula (6.3) shows that the backoff level will add 1 if the backoff level does not achieve the maximal value m and if the sending of the data frame is failed. The probabilities of the value of the counter is obtained randomly from the range of $[0, W_{i+1} - 1]$; Formula (6.4) shows that when the backoff level get to the maximal value m, the value of the backoff level keeps constant and the probabilities of the value of the counter is obtained randomly from the range of $[0, W_i - 1]$ if the sending of the data frame is failed. Formula (6.5) shows that the backoff level value will migrate to the minimal value 0 if the sending is successful at any backoff level.

It is defined:

$$b_{i,j} = \lim P\{s(t) = t, b(t) = j\} \qquad 0 \le i \le m, 0 \le j \le W_i - 1 \tag{6-7}$$

Based on the Figure 6-5, the following status transmission formula can be obtained:

$$\begin{cases} b_{i-1,0}\,p = b_{i,0} & 0 < i < m \\ b_{m-1,0}\,p + b_{m,0}\,p = b_{m,0} & i = m \end{cases} \tag{6-8}$$

$$\begin{cases} b_{i,0} = p^i b_{0,0} & 0 < i < m \\ b_{m,0} = p^m \big/ 1 - p b_{0,0} & i = m \end{cases} \tag{6-9}$$

From Figure 6-5, it is concluded:

For any $j \in [0, W_i - 1]$

$$b_{i,j} = \frac{w_i - j}{w_i} \begin{cases} (1-p)\sum_{k=0}^{m} b_{k,0} & i = 0 \\ pb_{i-1,0} & 0 < i < m \\ p(b_{m-1,0} + b_{m,0}) & i = m \end{cases} \qquad (6\text{-}10)$$

All $b_{i,j}$ can be shown by $b_{0,0}$ and p. From Figure 6-5, it can be known that

$$\sum_{i=0}^{m} \sum_{W_I}^{W_I - 1} b_{i,j} = 1$$

Because

$$b_{i,j} = \frac{W_i - j}{W_i} b_{i,0}$$

Thus,

$$b_{0,0} = \frac{2(1-2p)(1-p)}{(1-2p)(W+1) + pW[1-(2p)^m]} \qquad (6\text{-}11)$$

The probability of sending data frame at any moment is:

$$\tau = \sum_{i=0}^{m} b_{i,0} = \sum_{i=0}^{m} p^i b_{0,0} = \frac{1-p^{m+1}}{1-p} b_{0,0} \qquad (6\text{-}12)$$

Formula (6.11) can be used for all priority transaction data.

For the transaction with different priorities, the probability of sending the data frame at any moment from the nodes of the real-time transaction with high priorities is:

$$\tau_1 = \frac{2(1-p_1)(1-p_1{}^{m=1})}{W_1[1-(2p_1)^{m+1}](1-p_1) + (1-p_1)(1-p_1{}^{m+1})} \qquad (6\text{-}13)$$

The probability of sending the data frame at any moment from the nodes of the general transaction with low priority is:

$$\tau_2 = \frac{2(1-p_2)(1-p_2{}^{m+1})}{W_2[1-(2p_2)^{m+1}](1-p_2) + (1-p_2)(1-p_2{}^{m+1})} \qquad (6\text{-}14)$$

Where W_1 and W_2 are the minimal competition window of the real-time transaction and the general transaction, respectively. P_1 and P_2 are the collision probabilities of sending frame of the transaction stream of the important transaction and the general transaction, respectively.

From formula (6.11), the probability of sending the data frame of the nodes at any moment is τ, which is decided by the collision probabilities p. The channel status of sending the collision event of a node is: in the transmission networks with the node numbers n, the collision happens in the data frame of a node. This collision happens when there is at least one node sending the data in the $n-1$ nodes. Set the probabilities of sending the data frame of every node as ι, then,

$$p = 1 - (1-\tau)^{n-1} \qquad (6\text{-}15)$$

For the transactions with different priorities, the probabilities that there is a collision taking place on the nodes n1 of the real-time transaction with high priority is:

$$p = 1 - (1-\tau_1)^{n_1 - 1} \qquad (6\text{-}16)$$

The probabilities that there is a collision taking place on the nodes n2 of the real-time transaction with low priority is:

$$p = 1 - (1-\tau_1)^{n_1} (1-\tau_2)^{n_2 - 1} \qquad (6\text{-}17)$$

Analysis for the Throughput

In this protocol, S means the throughout of the system, which is defined as following:

$$S = \frac{E[\text{Load of one slot}]}{E[\ \text{Time of slot}]} \qquad (6\text{-}18)$$

Before the analysis the throughput, the following parameters regionalized

Set P_{tr} as the probabilities when the channel is busy. The busy of channel means that there is at least one node sending the data during the channel competition process of all nodes with the priority transaction. Thus:

$$P_{tr} = 1 - (1-\tau_1)^{n_1} (1-\tau_2)^{n_2} \qquad (6\text{-}19)$$

P_{s1} and P_{s2} are the data frame successful sending probabilities of the important transaction and the general transaction, respectively; P_{s11} and P_{s12} are the data frame successful sending probabilities of the important transaction and the general transaction without the collision, respectively; P_{c1} is the collision probability between the real-time transaction data frames, P_{c2} is the collision probability between the general transaction data frames when there is no transaction; P_{c11} is the collision successful probability between the real-time transaction data frames, P_{c12} is the collision failed probability between the real-time transaction data frames.

$$P_{s1} = P_{s11} + P_{s12} + P_{c11} \tag{6-20}$$

$$P_{s11} = n_1\tau_1(1-\tau_1)^{n_1-1}(1-\tau_2)^{n_2} \tag{6-21}$$

$$P_{s12} = n_1\tau_1(1-\tau_1)^{n_1-1}[1-(1-\tau_2)^{n_2}] \tag{6-22}$$

$$P_{s2} = n_2\tau_2(1-\tau_1)^{n_1}(1-\tau_2)^{n_2-1} \tag{6-23}$$

$$P_{c1} = 1-(1-\tau_1)^{n_1} - n_1\tau_1(1-\tau_1)^{n_1-1} \tag{6-24}$$

$$P_{c11} = (\frac{1}{2})^{n_1} P_{c1} \tag{6-25}$$

$$P_{c12} = [1-(\frac{1}{2})^{n_1}]P_{c1} \tag{6-26}$$

$$P_{c2} = (1-\tau_1)^{n_1}[1-(1-\tau_2)^{n_2} - n_2\tau_2(1-\tau_2)^{n_2-1}] \tag{6-27}$$

T_{s11}, T_{s12}, T_{s2}, T_{c11}, T_{c12}, T_{c2} response to the channel time of successful sending data and the conflict.

$$T_{s11} = RTS + 3SIFS + CTS + DATA + ACK + DIFS \tag{6-28}$$

$$T_{s12} = 2RTS + 4SIFS + 3slottime + CTS + DATA + ACK + DIFS \tag{6-29}$$

$$T_{s2} = RTS + 3SIFS + CTS + DATA + ACK + DIFS \tag{6-30}$$

$$T_{c11} = 2RTS + 4SIFS + 3slottime + CTS + DATA + ACK + DIFS \tag{6-31}$$

$$T_{c12} = 2RTS + SIFS + slottime + DIFS \tag{6-32}$$

$$T_{c2} = RTS + DIFS \tag{6-33}$$

Based on the above analysis, the saturation throughput of the important transaction and the general transaction are:

$$S_1 = \frac{P_{s1}E[data]}{(1-P_{tr})\theta + P_{s11}T_{s11} + P_{s12}T_{s12} + P_{s2}T_{s2} + P_{c11}T_{c11} + P_{c12}T_{c12} + P_{c2}T_{c2}} \tag{6-34}$$

$$S_2 = \frac{P_{s2}E[data]}{(1-P_{tr})\theta + P_{s11}T_{s11} + P_{s12}T_{s12} + P_{s2}T_{s2} + P_{c11}T_{c11} + P_{c12}T_{c12} + P_{c2}T_{c2}} \tag{6-35}$$

where θ is the duration of an empty slot, $E[data]$ is the average payload time of transmission. It is known from analysis formulas (6-15) and (6-16), that the failure probabilities caused by collision will be influenced by the transaction data stream with higher priorities. From the formulas (6-19) and (6-22), when the probabilities of sending frame and the number of nodes of the real-time transaction with high priorities and the general transaction with the low priorities are same, the successful probabilities of the real-time transaction is higher than the one of the general transaction. Thus the similar conclusion can be obtained for the saturation throughput

Under the collision between the data stream of the important transaction and the general transaction, the delay of data stream of the important transaction with the successful sending (TSs12)

$$TDs12 = RTS + 2*SIFS + floor(2.999*rand)*slottime + ACK \tag{6-36}$$

Under the collision between the data streams of the important transaction, the delay of data stream of the important transaction with the successful sending (TDc12)

$$TDc11 = Tc11 \tag{6-37}$$

Under the collision between the data streams of the important transaction, the delay of data stream of the important transaction with the failed sending (TDc12)

$$TDc12 = Tc12 \tag{6-38}$$

Under the collision between the data streams of the general transaction, the delay of data stream of the general transaction with the successful sending (TSs12)

$$TDc2 = Tc2 \tag{6-39}$$

6.4 summary

A new protocol SMAC-SD is proposed to support QoS. It includes service distinction, priority mechanism based on service queue, and channel requests service differentiation mechanisms constituting secure transport mechanism. The SMAC-SD protocol ensured the network's context of the high-quality transmission on diverse business, at the same time to establishing the analytical model by formula deduction to verify the correctness of the theory.

Chapter 7 Simulation and analysis

7.1 Simulation analysis of RBLEACH protocol

7.1.1 The parameters and settings of the simulation

Simulation process:

1. The simulation starts and the simulation programs begin. The simulation scene is set and each energy parameter is added into the settings.

2.Initialization settings of the whole system.

3. Preset function is set based on the relative theories and the cycle setting is done.

4. Implement the results and the simulation is ended.

The settings of the simulation scene are described as follows:

The 400 sensor nodes are randomly distributed into the network region with the area of $200m \times 200m$ .The preventing position of the base station is $(0,0)$

Table 7.1 Used parameters in the simulation

Parameter	Value
Network size	$(200m \times 200m)$
Base station position	$(0,0)$
Amount of nodes	400
Expected percentage of the head of cluster P	0.1
Fusion probability	0.6
E_0 initial energy of single node	$0.05J$
E_{TX} transmission energy cost	$50*0.000000001J/bit$
E_{RX} receiving energy cost	$50*0.000000001J/bit$
E_{fs} channel model of the free space	$10*10^{-12}J/bit/m^2$
E_{mp} channel model of the Multipath fading	$0.0013*10^{-12}J/bit/m^4$
E_{DA} energy cost of the data fusion	$5*10^{-12}J/bit$
d_0 border Threshold	84
(α_1, α_2)	(0.6,0.4)
(α, β)	(0.6,0.4)

Figure7.1 shows a network of 400 nodes randomly produced according to the above parameters

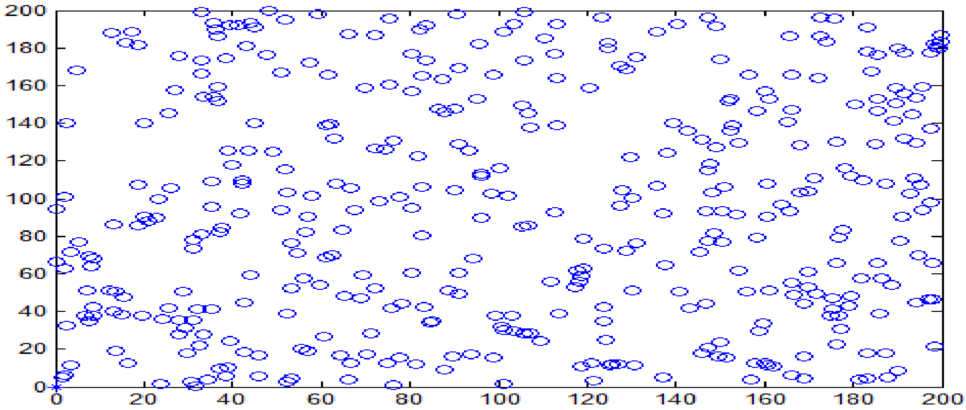


Figure 7.1 Random networks of 400 nodes

7.7.2 Performance indicator of simulation

The network simulation needs to set many performance indicators based on practical situations, and to set a realistic parameter to these performance indicators. All indicators and parameters are implemented by the implementation of the simulation objectives initially set that need to be solved by the new protocols. In this experiment, the results of the simulation are to prolong the life cycle of the networks. The energy cost of nodes decreases in each round, and the energy cost of sensor nodes of data collection and transmission can be balanced in the whole network. In order to achieve this objective, the simulation implements LEACH algorithm and RBLEACH algorithm; then compare the performance of the two algorithms. The standards to evaluate the RBLEACH algorithm are described as follows:

1. Network life: duration from the first dead node to the last one.
2. Proportion of the amount of cluster heads.
3. Comparison of residual energy in each round.
4. Comparison of energy cost of cluster heads in each round.

7.7.3 Experiment results of simulation and comparison of relative work

1. Comparison of network life

Figure 3.8 demonstrates the relation between the amount of dead nodes and the network working time (rounds). Compared with LEACH, RBLEACH proposed in this thesis can greatly prolong the life cycle of a network because every sensor node in the cluster shares the energy cost evenly. Meanwhile, the node with more energy is first selected as the cluster head, and the proportion of cluster head distribution is balanced in the cluster head selection. It synchronizes the energy cost of each sensor node and delays the moment of the first death of a node. The RBLEACH algorithm prolongs the life of nodes 30% more than when using LEACH algorithm.

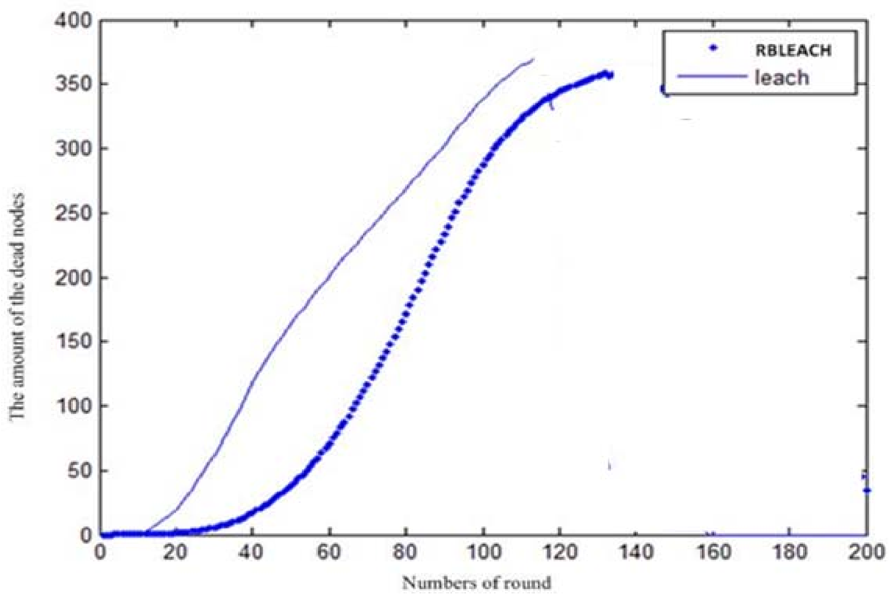


Figure 7.2 Comparison of amount of dead nodes

Figure 7.2 shows the death rate of sensor nodes. It is known from the first death of a node that the death of all nodes will be concentrated in the last 40 rounds when using RBLEACH algorithm, which is better than the death rate when using LEACH algorithm, illustrating that the algorithm can balance the energy used by the nodes and that the networks can supply high quality service.

2. Comparison of cluster head amounts

Figure 7.3 shows the number of cluster heads selected with different rounds in the LEACH protocol and RBLEACH protocol. It is obvious that the amount of the live sensor nodes in RBLEACH protocol is more than that of LEACH protocol. The amount of the cluster heads selected with proportion of RBLEACH protocol is less than that of LEACH protocol. Thus, the energy cost in the process of transmission in RBLEACH protocol is reduced, achieving the objectives of reducing energy cost.

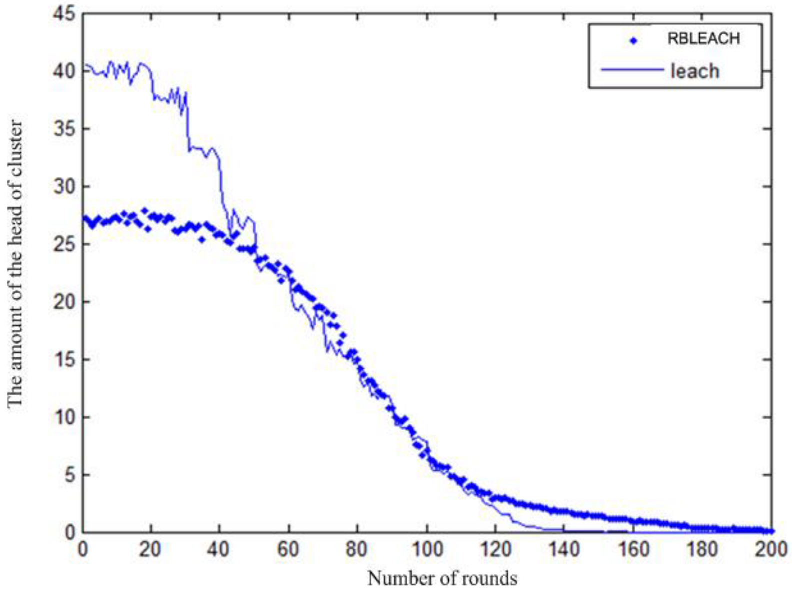


Figure7.3 Comparison of amount of cluster heads

3. Comparison of residual energy for each round

Figure 7.4 shows the comparison of total residual energy when using LEACH protocol and when using RBLEACH protocol for each round. It can be known from Figure 3.10 that the total residual energy when using RBLEACH protocol is much more than that of LEACH protocol, illustrating that the life cycle of the whole network when using RBLEACH protocol is much longer than that when using LEACH protocol.

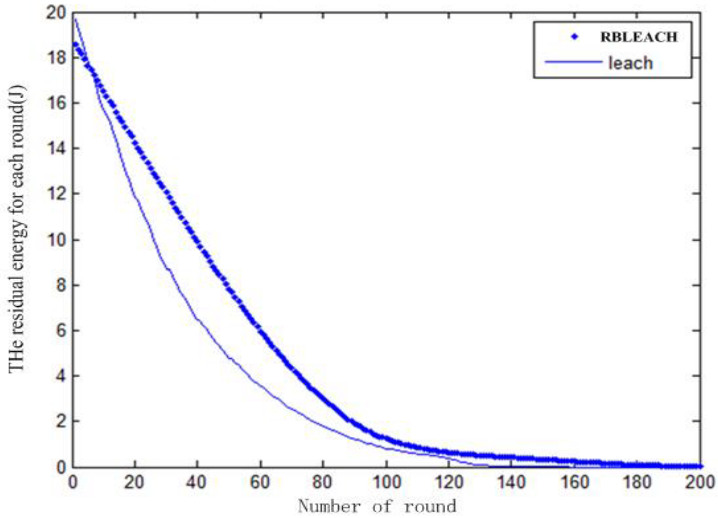


Figure7.4 Comparison of residual energy for each round

4. Comparison of the energy cost of the cluster heads for each round.

Figure 7.5 shows the simulation results of cluster head energy cost of LEACH protocol and RBLEACH protocol for each round. It's shown in Figure 7.5that the maximum value of the cluster head energy cost of RBLEACH protocol is less than the minimum value of the cluster head energy cost of LEACH protocol for all rounds. Thus, under the condition where the same initial energy is supplied, the cluster head energy cost of RBLEACH protocol is less than that of LEACH protocol. Therefore, the life cycle of RBLEACH protocol can be prolonged.

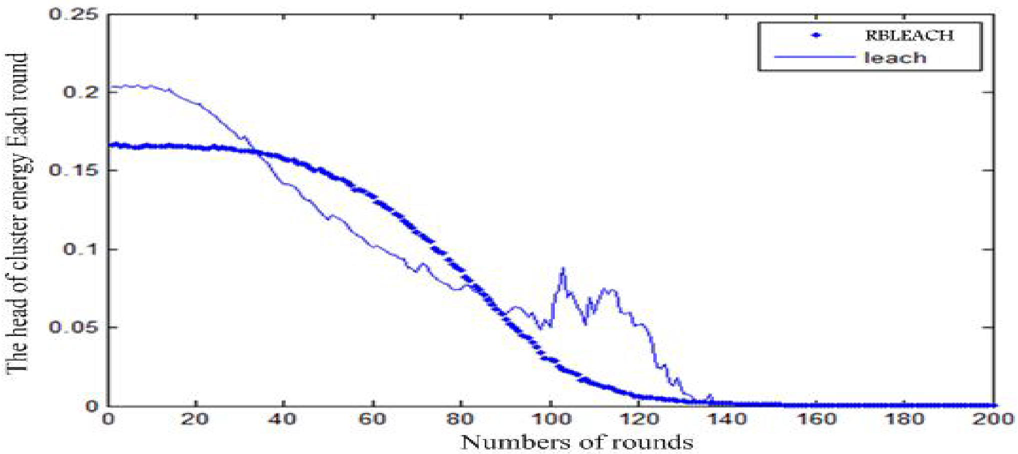


Figure 7.5 comparisons of the residual energy for each round

In conclusion, whether examining the lifetime or total residual energy of the sensor nodes in the networks, RBLEACH protocol is better than LEACH protocol. In

RBLEACH protocol, the whole network is divided into several regions and the cluster heads are selected by proportion, which obviously contributes to a more uniform distribution of the cluster heads in the network. The node energy cost of the data transmission from the member nodes to the cluster head and from the cluster head to the base station is lower, resulting in a longer life for each node in the network. Compared with LEACH protocol, the multi-hops selected by the cluster head in the clusters are used for data transmission to save energy between the sensor nodes. This relatively improves the lifetime of each sensor node in the network.

7.2 Simulation analysis of PS-ACO-LEACH

7.2.1 Performance indicator

Throughout this thesis, the performance of the PS-ACO-LEACH is analyzed from the following aspects:

1. Load balance: the routing protocol of WSN should distribute the network load to each node evenly as much as possible and prevent few nodes or some region nodes dying too early, which can affect the networks performance. This chapter is to analyze the protocol based on the distribution of dead nodes.

2. Life cycle: the duration from the operation of the networks to the death of the nodes is shown as “round”, which can be expressed by two durations: duration from the first death and duration of the death of half the nodes, if there are half of the sensors exhausting their energy, the WSN is considered to be dead.

3. Energy cost: the routing protocol of WSN should be good to save the energy of the nodes in the networks and prevent the unnecessary consumption. This chapter contributes to the analysis from the total residual energy of the nodes in each round.

7.2.2 Simulation results and evaluations

1. Design of simulation environment.

In order to compare the performance difference between LEACH and PS-ACO-LEACH in different ranges, the simulations are operated in two different scenes respectively. The area of scene 1 is 100m*100m, and the coordinate of the base station is (0, 0). The nodes of scene 2 are distributed into the region with an area of 200m*200m, and the coordinate of the base station is (0, 0). The relative parameters are shown in Table 7-2, and the detailed physical definitions are described in 4.2.2.

Table 7-2 The detailed parameters of the network environment

Experimental parameters	Scene 1	Scene 2
Region area	100m*100m	200m*200m
nodes amount	110	440
Location of the base station	(0, 0)	(0, 0)
initial energy	0.1J	0.1J
p	0.1	0.1
length of the data packet	4000 bit	4000 bit
E_{elect}	$50nJ / bit$	$50nJ / bit$
ε_{fs}	$10 pJ / bit / m^2$	$10 pJ / bit / m^2$
ε_{mp}	$0.0013 pJ / bit / m^4$	$0.0013 pJ / bit / m^4$
E_{DA}	$5nJ / bit$	$5nJ / bit$
d_0	87m	87m

7.2.3 Evaluations for simulation performance indicator

1. Load balance

Assume that the area of the region is 200m*200m, there are 400 nodes and the base station is located at (0,0). Figure 7-6 and Figure7-7 show the distribution of dead nodes of the WSN operation in the LEACH protocol and PS-ACO-LEACH in early-term. Figure 7-8 and Figure 7-9 show the distribution of the dead nodes to these two protocols in medium-term. The nodes far away from the base station begin to die first due to single-hop routing used in LEACH protocol. Moreover, the distribution of the cluster heads are more reasonable and the energy cost is less because of improved clustering strategy and the multi-hop mechanisms used in PS-ACO-LEACH protocol, thus the dead nodes are distributed evenly. LEACH protocol has a considerably large part of its region that cannot be covered in the medium-term and late-term of the network operation which means the network will fail. However, PS-ACO-LEACH protocol can cover a large part of the region in the medium-term and late-term of the networks operation. Thus, the PS-ACO-LEACH protocol is better than LEACH protocol when considering the load balance.

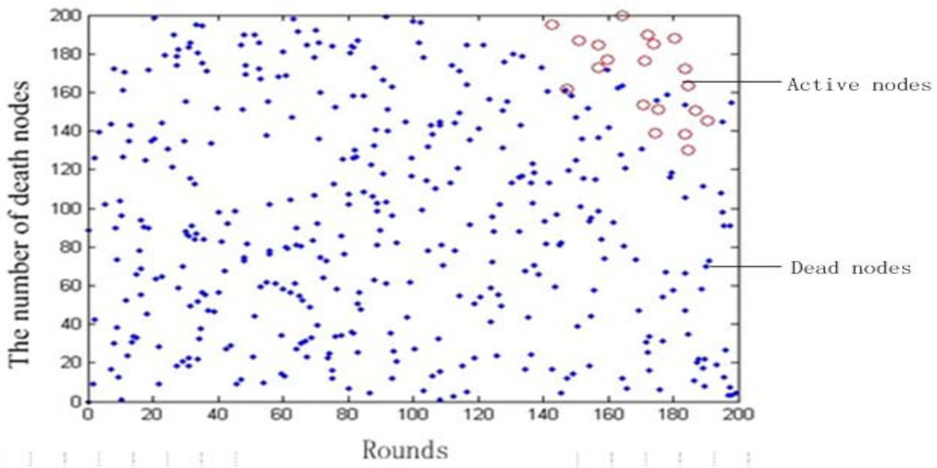


Figure 7-6　Distribution of dead nodes in early term of LEACH

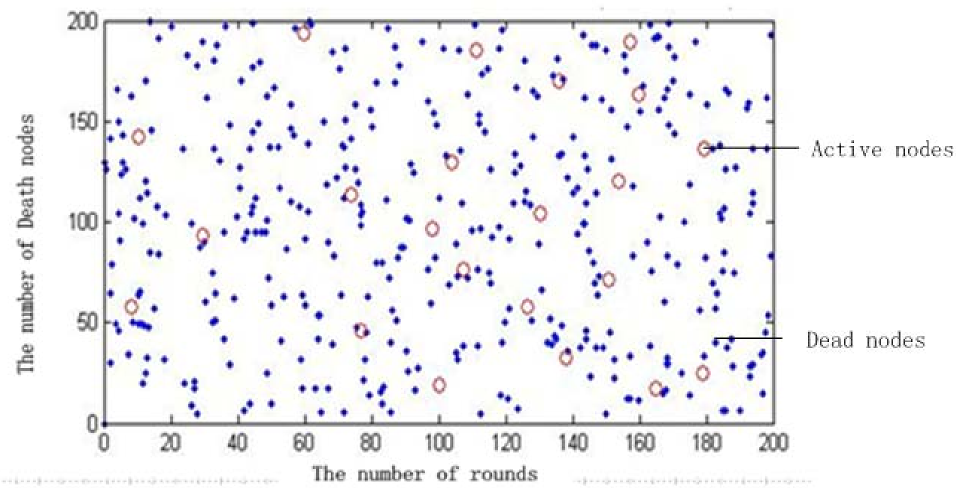


Figure 7-7 Distribution of dead nodes distribution in early term of PS-ACO-LEACH

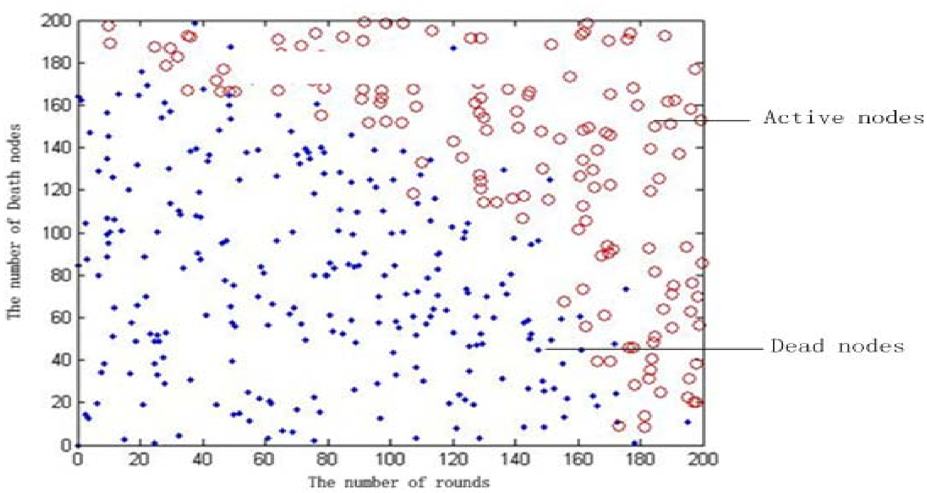


Figure 7-8 Distribution of dead nodes in the medium term of LEACH

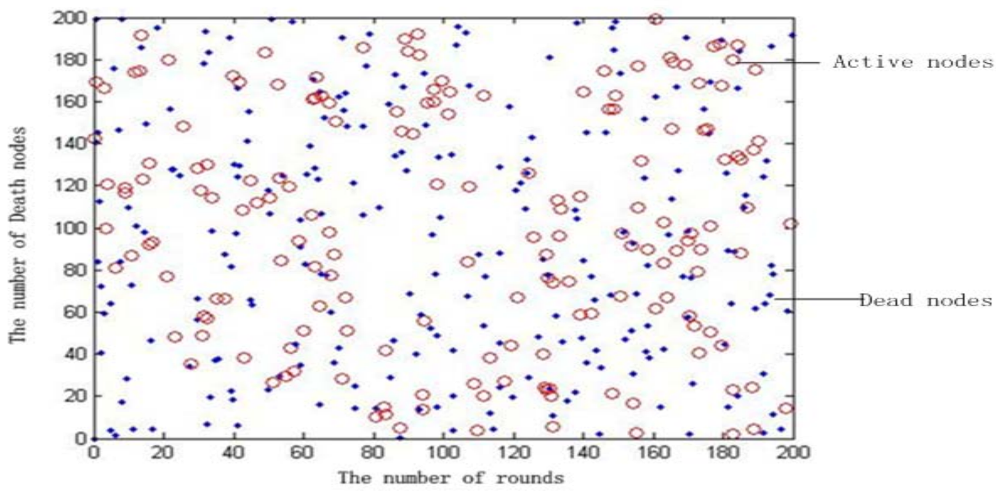


Figure7-9 Distribution of dead nodes distribution in the medium term of

PS-ACO-LEACH

2. Life cycle

Figure 7-10 shows the network life cycle in the 100m*100m scenario. The dotted line represents the rising curve of dead nodes in the CRP-PSAC protocol, and the solid line represents the rising curve of dead nodes in the LEACH protocol. In scenario 1, the moment of the first nodes death (FND) in the CRP-PSAC is the 200th round and that of the LEACH is the 166th round. For the half node death (HND) moment, the CRP-PSAC is the 200th round and the LEACH is the 225th round, illustrating that that the CRP-PSAC can distribute the energy cost more evenly into all the nodes to prevent early death of a single node due to energy loss.

Figure7-11 shows the network life cycle in the 200m*200m scenario. In scenario 2, the advantages of the CRP-PSAC are further expressed. The moment of its FND and HND are the 186th round and the 267th rounds respectively. The moment of LEACH's FND and HND are the 29th round and the 131st round respectively. This is because the communication distance between the cluster head and the base station increases in the LEACH protocol under the large scenario environment, and the single communication energy loss of the cluster heads increases. However, in the CRP-PSAC protocol, the communication between cluster heads and the base station uses a multi-hop routing method, thus the single communication energy loss will not increase with the increase of the area. Moreover, the PS-ACO-LEACH protocol considers the judgment standard for multiple cluster heads to distribute network energy amongst all the sensors as much as possible.

It is noted that the all curves are drawn by repeating the simulation 100 times to calculate the average value in order to make the simulation results convincing. The number of network nodes is set to the 110th and the 440th rounds respectively because of programming needs. However, the curves are cut at the 100th and the 400th round in the figures.

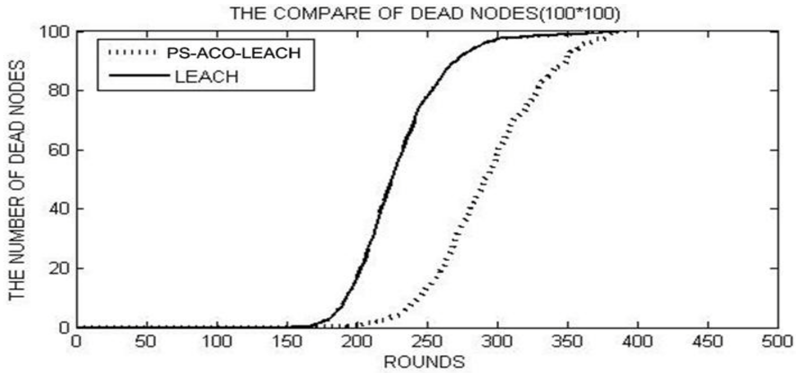


Figure 7-10 Relation between dead nodes and time in the 100m*100m scene

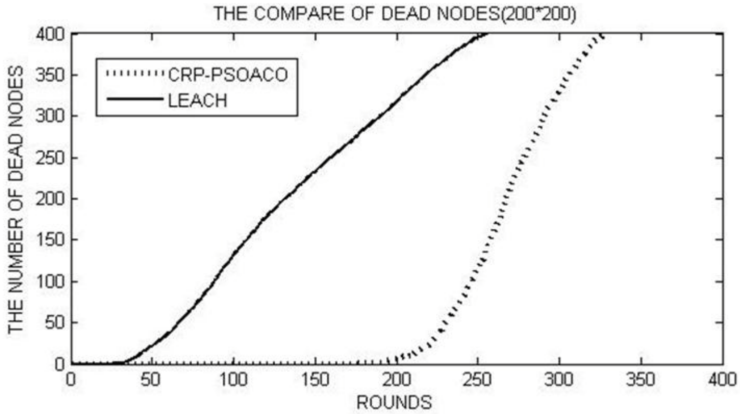


Figure 7-11 Relation between dead nodes and time in the 200m*200m scene

3. Energy cost

Figure 7-12 and Figure 7-13 show the relation between network energy cost and time in the LEACH and the PS-ACO-LEACH protocol under the 100m*100m and the 200m*200m environments respectively. The figures intuitively show the relation between the networks residual energy and time. As shown in the figures, PS-ACO-LEACH can save the network residual energy costs compared with LEACH. The rate of the energy cost decreases, and the total residual energy of the PS-ACO-LEACH is lower than that of LEACH at any moment. This is because most of the nodes in LEACH have died over time, but there are still many live nodes in the PS-ACO-LEACH. Thus, in LEACH, the covered area of the cluster head is larger, the collected information is more, and the energy cost is relatively more.

When the area of the network region becomes larger, the energy-saving effects of PS-ACO-LEACH are more obvious, which can be explained in the same way as was explained in Figure 7-11

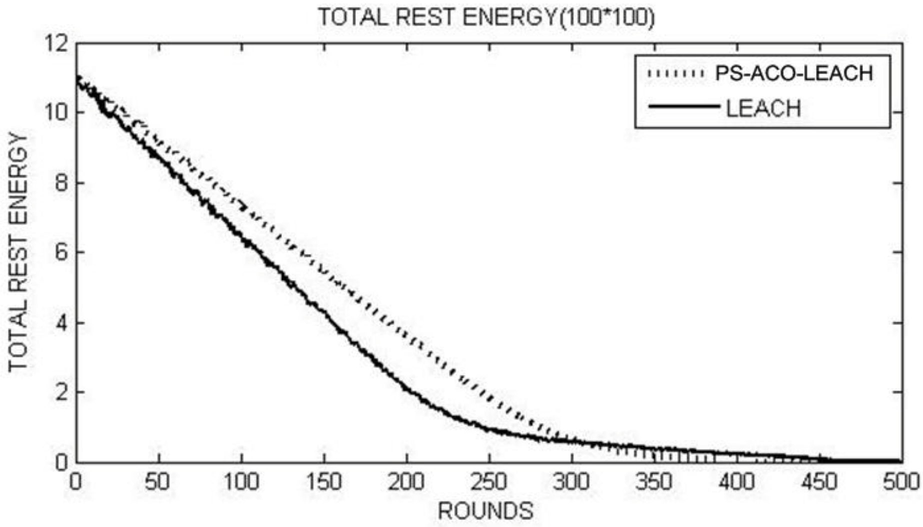
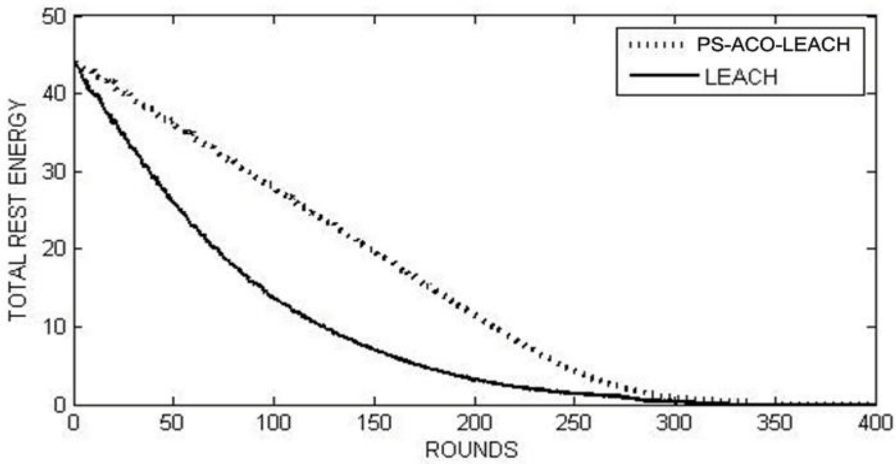


Figure 7-12 Relation between network residual energy and time in the 100m*100m scene



Fiure 7-13 Relation between network residual energy and the time in 200m*200m scene

7.3 Emulation of MIA-QRP

7.3.1 Creation of protocol testing environment

To test the operation of this protocol, verify the correctness of routing protocol and the good characteristics of protocol performance, it is not only needed to accomplish the software design of the protocol and drive design and compilation of wireless LAN, but also to set the forward of the data package supported by the destination machine and to set the node networks card.

7.3.2 Support setting of nodes to data package for forwarding

The ADHOC network is characterized by moving multi-hops, and the nodes can randomly move in the networks. In the process of the network communication, each node functions as both the client and router. When one node becomes the forwarding node of one communication link, it needs to supply the forwarding of data package for the network data communication between the original node and the destination one. Thus, to test this protocol needs to modify the routing function of nodes, so that the node can forward the data package.

There is a complete TCP/IP protocol stack in the Linux, which supports the data package forwarding. The Linux operation system has a powerful service, and has functions of the network service of the client computer and the data package forwarding of the router. However, the Linux is just used as the client computer in the default condition without using the forwarding of the Linux to the data package. To meet the need of this routing protocol testing, the destination machine regarded as the nodes; need to start the forwarding function. The following are the detailed setting commands:

sysctl -w net.ipv4.ip_forward=1

After start of the Linux system, imputing the above setting commands can accomplish the forwarding of system to the network data package. As Linux operation system does not start this function in the default condition, the data forwarding will be shut down when the system is restarted. To reduce the repetition of data forwarding configuration of system set in the each testing, the data package forwarding settings can be written into system files to read the configuration file itself to start the forwarding. The correction methods of the system configuration files are described as follows:

First, open the configuration files, the command is: # vim /etc/sysctl.confined the configuration item and correct “the net.ipv4.ip_forward = 0” to “net.ipv4.ip_forward = 1”. After correction, save it and quit. In order to make the set configuration come into effect timely, the command line needs to be input as “# sysctl –p” Input the command “# sysctl net.ipv4.ip_forward” to check if the data forwarding starts.

7.3.3 Network configuration of testing nodes

The friendly arm company development board mini2440 is used for the testing nodes in this protocol use. There are three tested nodes, and the networks card of each node use rt73 USB wireless LAN. Each nodes target board needs to install the compiled network card driver. The installation steps of the Rt73 USB wireless LAN are described as follows:

First, download the compiled files to the mini2440 development board and execute the following commands:

```
# mkdir /etc/Wireless
# mkdir /etc/Wireless/RT73STA
# cp rt73.bin /etc/Wireless/RT73STA/rt73.bin
# dos2unix rt73sta.dat
# cp rt73sta.dat    /etc/Wireless/RT73STA/rt73sta.dat
# /sbin/insmod rt73.ko
```

After the above operation, the compiled driver is successfully installed to the system, and the networks card can work generally.

After load of the networks card driver, it is need to start the networks and configure network nodes. The basic configuration information of the network nodes is described as follows:

Table 7-3 Node configuration

Node name	IP address	MAC address
A	192.168.1.172	D8:5D:4C:7C:15:2F
B	192.168.1.171	D8:5D:4C:7D:95:1F

The node configuration and the network settings are described as follows:

(1)start the networks card: if config rausb0 up, rausb0 is the name of the networks card interface

(2)set the IP address of the nodes: the IP address corresponding to the if config rausb0.

(3) set the networks card to ad-hoc networks mode: iwconfig rausb0 mode ad-hoc

(4) set SSID for the node: iwconfig rausb0 essid “dsh”, which improves the security of the networks

(5) download the protocol sdap to the development board and correct the competence: chmod +x sdap

(6) execute the protocol modul./sdap

Through the above settings, the neighbor nodes have the function of data transmission of using USB wireless LAN.

7.3.4 Protocol performance testing

There are many indexes to measure the performance of the routing protocol. This thesis is mainly to judge the protocol by the primary path finding velocity, path maintenance effectiveness, data package forwarding and protocol cost etc.. The performance testing and the results of the analysis are provided.

1. Path findings testing

Due to limited resources, testing networks consist of the three networks nodes. The distribution of the network node is shown in Figure 7-14

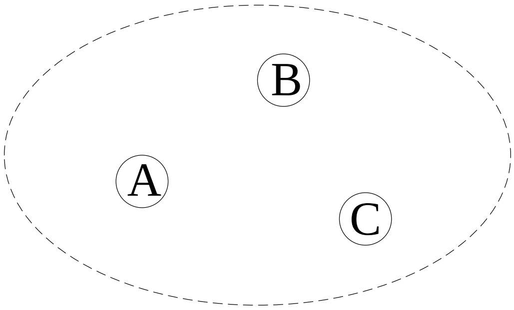


Figure 7-14 Distribution of testing node network

Based on the testing results of nodes, the operation of this protocol is described. Start node B and node C before testing node A, and build path topology between node B and node C. According to the design theory of this routing protocol, node A will build a network topology information table with node B and node C after it starts to form the A-B and the A-C two direct path and form the A-B-C and the A-C-B two multi-hop path. Then the routing algorithm is called to select a optimized path between the nodes to be added to the system routing table.

The network topology information of node A can be printed, as shown in Figure 7-15, after it starts and operates the routing protocol for a while.

```
the total node number is:5
mac:d8-5d-4c-7c-15-2f ip:192.168.1.172 parent ip:127.0.0.1
mac:d8-5d-4c-7d-95-1f ip:192.168.1.171 parent ip:192.168.1.172
mac:d8-5d-4c-7d-13-df ip:192.168.1.170 parent ip:192.168.1.172
mac:00-00-00-00-00-00 ip:192.168.1.170 parent ip:192.168.1.171
mac:00-00-00-00-00-00 ip:192.168.1.171 parent ip:192.168.1.170
```

Figure 7-15Network topology information of node A

As shown in Figure 7-15, there are 5 pieces of information in the network topology information table of node A. The first one is the network information of node A itself, which is designed and produced according to this protocol and has no corresponding path. The second one and the third one are the direct path topology information, which is related to the nodes networks configuration information in Table 7-3. It is known that the second one and the third one record the topology information of path A-B and path A-C respectively. The mac address recorded in the fourth one and the fifth one is 00-00-00-00-00, which records the multi-hop path information and corresponds to topology information of the path A-B-C and the path A-C-B, respectively. The network topology information produced in node A is in compliance with the design theory of this protocol.

In order to inquire the selected final routing information of this protocol by the MIA-QRP routing selection algorithm, the system routing table and the ARP table information of the node A can be observed by using the routing information and arp address analysis table information of the output system of the command route and command arp respectively, as shown in Figure 7-16and Figure 7-17.

```
[root@FriendlyARM /]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.170   *               255.255.255.255 UH    0      0        0 rausb0
192.168.1.171   *               255.255.255.255 UH    0      0        0 rausb0
192.168.1.0     *               255.255.255.0   U     0      0        0 rausb0
```

Figure 7-16 System routing table information

```
[root@FriendlyARM /]# arp
? (192.168.1.1) at <incomplete>  on rausb0
? (192.168.1.171) at d8:5d:4c:7d:95:1f [ether] PERM on rausb0
? (192.168.1.170) at d8:5d:4c:7c:13:df [ether] PERM on rausb0
```

Figure 7-17 System ARP table information

According to the recording of system routing table information, path A-B and path A-C are finally selected in the routing algorithm designed in this routing protocol finally as the optimized path for communication between node A and nodes B,C. Meanwhile, the system ARP table records the physical address corresponded to the IP address of node C and node B, which corresponds to the system routing table information recording. The network topology structure of node A is as show in the dotted line in Figure 7-18.

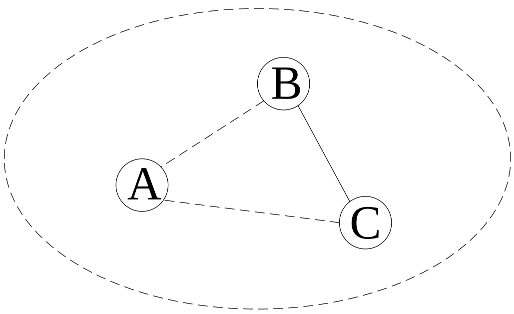


Figure 7-18 Network topology structure.

2. Path maintenance testing

Based on the distribution of the nodes in the networks shown in Figure 7-14, each node has produced the network topology path information after the routing protocol operation. Now shut down the main computer of node C, and further observe the change of the network topology information of node A. The printed and outputted network topology information of the A after shutdown of node C and waiting for a while is shown in Figure 7-19.

```
the total node number is:2
mac:d8-5d-4c-7c-15-2f ip:192.168.1.172 parent ip:127.0.0.1
mac:d8-5d-4c-7d-95-1f ip:192.168.1.171 parent ip:192.168.1.172
[root@FriendlyARM /]# _
```

Figure 7-19 Network topology information of node A

Based on the topology path information of node A, node A only has the information record of the direct path that arrives at node B. The network topology information produced before or related to node C has been deleted, which is in compliance with the results of this routing protocol design. The system routing table and the ARP table information of the node A, as shown in the Figure 7-20 and the Figure7-21 respectively, are examined by the route command and arp command.

```
[root@FriendlyARM /]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.171   *               255.255.255.255 UH    0      0        0 rausb0
192.168.1.0     *               255.255.255.0   U     0      0        0 rausb0
```

Figure 7-20 System routing table information of node A

```
[root@FriendlyARM /]# arp
? (192.168.1.171) at d8:5d:4c:7d:95:1f [ether] PERM on rausb0
? (192.168.1.1) at <incomplete>  on rausb0
```

Figure 7-21 ARP table information of node A

Based on the information between Figure 7-16 and Figure7-20 and by comparing the ARP table information between Figure 5-44 and Figure 5-46, the node C becomes invalid after it is shut down. Node A maintains and deletes the network topology information related to node C after the routing, and updates the system routing table information and ARP table information. There is only path information record of the path A-B left. Based on this, node A can effectively run dynamic perception to the network topology, timely update the network topology information, delete the expired nodes and maintain the path.

3. Multi-hop path selection testing

The tested nodes are redistributed by using the T-shaped corridor in the laboratory building, as show in Figure 7-22. The direct communication link between node A and node C is influenced by the wall, so the signal strength of node C tested by node A is largely decreased. Meanwhile, the commutation delay between node A and node C and the package loss rate are influenced with different degrees. However, node B is set at a corner, so there is no any blocking between node B and nodes A, C. The design of this distribution is mainly to test if node A and node C can select the multi-hop path that regards node B as the relay node by the routing selection algorithm.

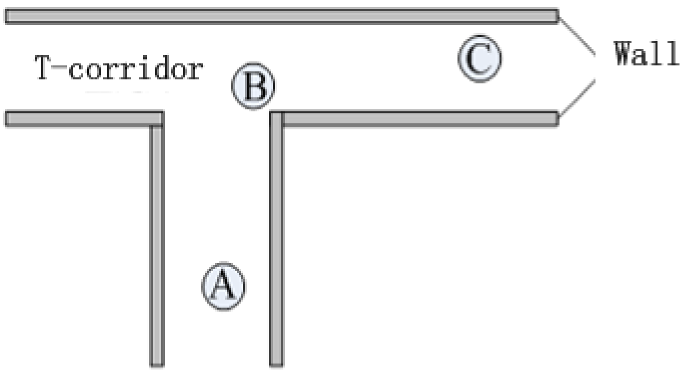


Figure 7-22 Distribution structure of nodes

Start the mechanism of node B and node C and build the network topology path of node B and node C, then start the mechanism of node B. Export the network topology information of node A after the operation for a while, as shown in Figure 7-23.

```
the total node number is:5
mac:d8-5d-4c-7c-15-2f ip:192.168.1.172 parent ip:127.0.0.1
mac:d8-5d-4c-7d-95-1f ip:192.168.1.171 parent ip:192.168.1.172
mac:d8-5d-4c-7d-13-df ip:192.168.1.170 parent ip:192.168.1.172
mac:00-00-00-00-00-00 ip:192.168.1.170 parent ip:192.168.1.171
mac:00-00-00-00-00-00 ip:192.168.1.171 parent ip:192.168.1.170
```

Figure 7-23 Network topology information of node A

It is known from Figure 7-24 that node A has captured the network topology information of node B and node C, and created a two-way direct path and two multi-hop paths with each node. The system routing table and ARP table information of node A, as shown in Figure 7-24 and Figure 7-25 respectively, are examined by the route command and arp command.

```
[root@FriendlyARM /]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.170   192.168.1.171   255.255.255.255 UGH   0      0        0 rausb0
192.168.1.171   *               255.255.255.255 UH    0      0        0 rausb0
192.168.1.0     *               255.255.255.0   U     0      0        0 rausb0
```

Figure 7-24 System routing table information of node A

```
[root@friendlyARM /]# arp
? (192.168.1.170) at d8:5d:4c:7c:95:1f [ether] PERM on rausb0
? (192.168.1.171) at d8:5d:4c:7c:95:1f [ether] PERM on rausb0
? (192.168.1.1) at <incomplete> on rausb0
```

Figure 7-25 ARP table information of node A

They are shown from the system routing table information that the path from node A to node C (IP address is 192.168.1.170) needs to go through the gateway (IP address of node B). The physical address corresponding to the networks IP address of node C is recorded as D8:5D:4C:7D:95:1F (MAC address of node B). This can completely demonstrate that this routing protocol sets the multi-hop path A-B-C as the communication path between node A and node C, and node B plays the role of relay node.

4. Multi-hop path performance testing

For multi-hop path A-B-C formed in Section 5.2.3, each index and performance of the link can be detected and the data forwarding of the node B can be supported by using ping command on node A. First, the simple ping command is used to test the link connectivity.

From the testing results shown in the Figure 7-26, the communication data package between the node A and the node C is implemented by the forwarding of the node B. The response data package received from the node A is sent back from 192.168.1.171 (that is the IP address of the node B). Thus this can verify that node B has the function of data package forwarding and the function to be the gateway router and it can be the relay node of node A and node C.

```
[root@FriendlyARM /]# ping 192.168.1.170
PING 192.168.1.170(192.168.1.170): 56 date bytes
From 192.168.1.171: seq=0 Redirect Host(New nextop: 192.168.1.170)
64 bytes from 192.168.1.170: seq=0 ttl=64 time=23.4ms
From 192.168.1.171: seq=1 Redirect Host(New nextop: 192.168.1.170)
64 bytes from 192.168.1.170: seq=1 ttl=64 time=21.6ms
64 bytes from 192.168.1.170: seq=2 ttl=64 time=26.0ms
From 192.168.1.171: seq=3 Redirect Host(New nextop: 192.168.1.170)
64 bytes from 192.168.1.170: seq=3 ttl=64 time=22.5ms
From 192.168.1.171: seq=4 Redirect Host(New nextop: 192.168.1.170)
64 bytes from 192.168.1.170: seq=4 ttl=64 time=23.8ms
64 bytes from 192.168.1.170: seq=5 ttl=64 time=34.6ms
From 192.168.1.171: seq=6 Redirect Host(New nextop: 192.168.1.170)
64 bytes from 192.168.1.170: seq=6 ttl=64 time=22.3ms
From 192.168.1.171: seq=7 Redirect Host(New nextop: 192.168.1.170)
64 bytes from 192.168.1.170: seq=7 ttl=64 time=21.5ms
```

Figure 7-26 Ping command-testing results

In order to further detect the communication link delay between node A and node C and the package loss rate performance, the statistic data can be obtained by the extended instruction of ping command. The experiment tests the link performance by changing the ping package number and the ping package sizes. The ping commands used are described as follows:

#ping –q –c package number n –s package size m

The ping package number set in this testing are 50, 100, 300, 500, 700, 1200 and 1500. The ping package sizes are 1KB, 10KB and 50KB. The testing results under the condition that the ping package number sent by the node A is 50 and the ping package size sent by the node A is 1KB is shown in the Figure 7-27.

```
[root@FriendlyARM /]# ping 192.168.1.170 -q -c 50 -s 1024
PING 192.168.1.170 (192.168.1.170): 1024 date bytes

--- 192.168.1.170 ping statistics ---
50 packets transmitted, 48 packets received, 4% packet loss
round-trip min/avg/max = 20.825/21.254/36.943
[root@FriendlyARM /]#
```

Figure 7-27 Link performance testing results

After the testing, the final testing results can be counted. The statistic results of the link delay are shown in Figure 7-27.

According to the testing results, for the two-hop A-B-C link, the communication delay of the link is stabilized at about 11ms when the sizes of the sent data package are

1KB and 5KB, and the package loss rate is stabilized less than 5%. The link performance is tending towards stability and the fluctuation is slight. However, when the sent data package size increases to 50KB, the communication delay of the link will increase with the increasing of the data package number, and the package loss rate increases to higher than 10%. Every aspect of the performance decreases greatly.

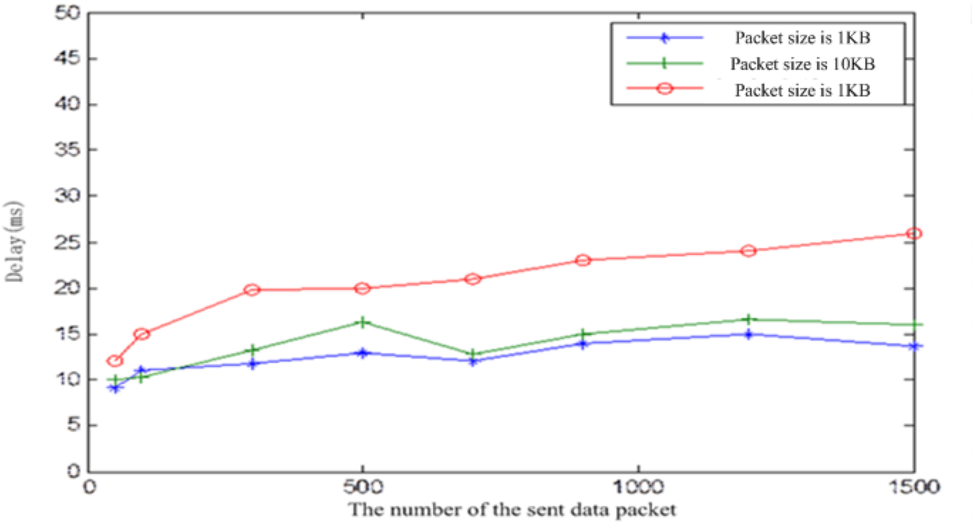


Figure7-28 Statistic results of link delay

5. Protocol cost

During operation of the protocol, using the top command can examine the real-time occupation condition of protocol to the system CPU and the memory. The results are shown in Figure 7-29.

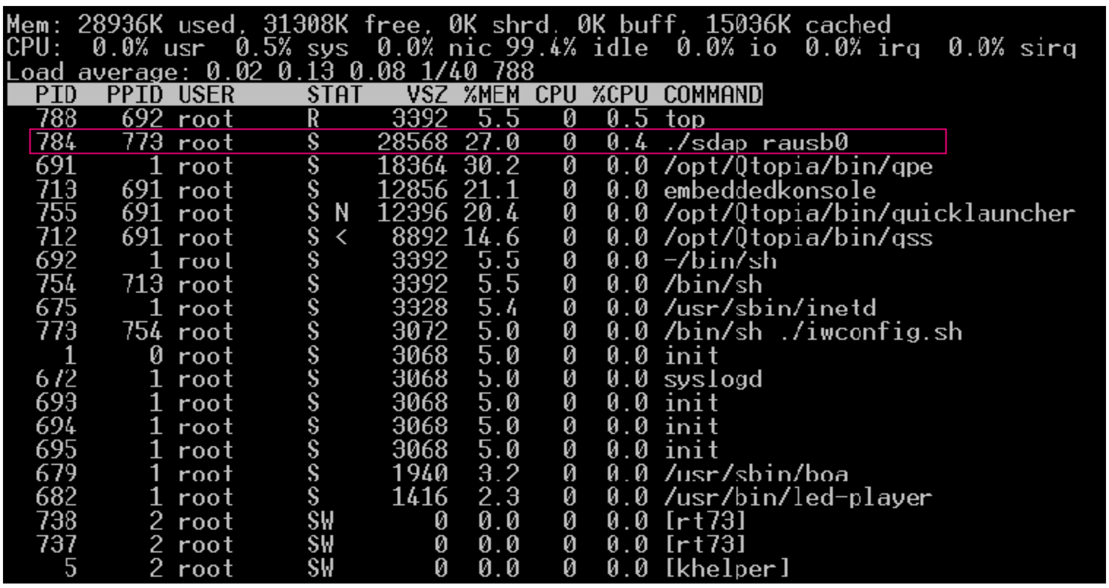


Figure 7-29 Protocol CPU and memory cost

It is shown in Figure 7-29 that the utilization of the protocol to the system CPU and the memory are 0.4% and 27.0% respectively. Through the testing of protocol cost, the occupation of this protocol to the system CPU is small. The occupation of this protocol to the memory resource is up to 27%, including a buffer space of 15036K. But this protocol is based on the mini2440 testing platform. The total memory size is 64M. Thus, the memory cost of this protocol is small so that it can adapt to the using of the selected development environment.

7.3.5 Compare with QoS protocol

Literature [153] reported the QoS protocol realization on Linux. According to zhu Lin’s work, the performances of QoS are compared:

Test environment

Three nodes A,B,C, their IP address are set:

A(192.168.0.1),

B(192.168.0.2)

C((192.168.0.3)

Embedded nods A has a WIFI interface, it is used access the public network. IN WIFI model, the Qos parameters are set according to the

Table 7.4 QoS parameters

Downlink Bandwith	90kbit/s
Maximum download Bandwith	24kbit/s
Maximum Uplink Bandwith	24bit/s
Minimum Bandwith	16kbit/s

Let A,B,C access the FTP server, and it will get average download speed:

Table 7.5 QoS testing result1

Node	average download speed For literature	average download speed for MIA-QRP
A	41kbit/s	43kbit/s
B	25kbit/s	32 kbit/s
C	24bit/s	31 kbit/s

Let B,C access the FTP server, A is not work, B,C' average download speed

Table 7.6 Table QoS 7.6 testing result 2

Node	Average download speed For literature [148]	Average download speed MIA-QRP
B	25kbit/s	32 kbit/s
C	24bit/s	32 kbit/s

The result shows MIA-QRP has more accurate flow control on every IP than literature [153].

7.4 Simulation of SMAC-SD protocol on the NS2

7.4.1 Realization of the SMAC-SD protocol

The SMAC-SD protocol is used to improve the S-MAC protocol. The realization of the new protocol in the NS2 needs the finishing of the C++ protocol code and the tcl debugging code. Compared to the code of the S-MAC protocol, the improvement is made.

The modified sdsmac.h file and the sdsmac.cc file in the new SMAC-SD protocol will add the file into NS2.

Simulation scene and parameter setting, tel sript in order to analyze the performance, 20 nodes and two data streams of the different transaction with different original node and destination node are set in the experiment. The protocol uses the

AODV routing protocol and control the network traffic by the data transmission rate. Related parameters are described as follows:

Table 7.7 Simulation parameters

Parameter	Value	Parameter	Value
Routing protocol	AODV	maximal window	1024
data stream	CBR	minimal window	32
agency protocol	UDP	size of the data packet	512
simulation time	100s	Slot duration	20us

7.4.2 Simulation scene and Parameter settings

1.Simulation objective: the SMAC-SD protocol is simulated by the Low-load network and high-load network, respectively. By analyzing the throughput and the system delay, the improved SMAC-SD protocol is proved to supply a effective transmission for the important transaction.

2. Simulation scene: In the using of WSN, the basic communication model collects the data for the nodes of the sensor, and then sends to the aggregation nodes which will send the data to the users. Because the nodes will self organize the wireless networks and the users are in the limited networks, the nodes of sensor cannot communicate with the users directly. Thus, the combination of the wireless networks and the limited networks is involved. In order to be closer to the using reality, the basic simulation scene of the SMAC-SD protocol is described as shown in Figure 30:

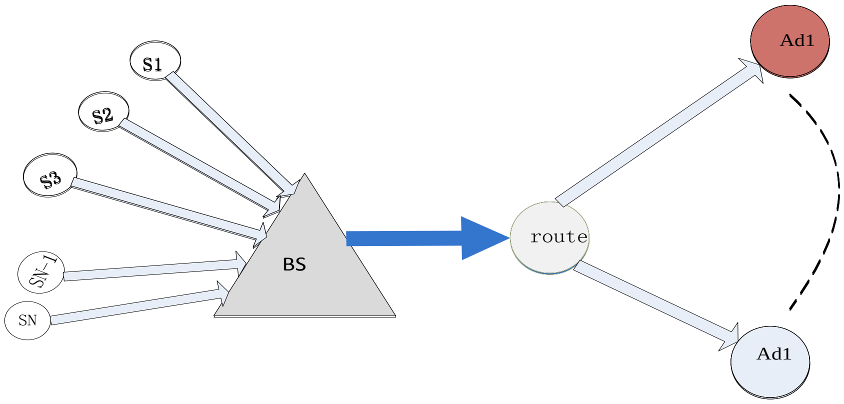


Figure 7-30 Basic simulation scene of SMAC-SD Protocol

3. Simulation experiment: in the basic simulation scene of SMAC-SD Protocol, based on the Implementation requirements of the simulation objectives, this simulation consists of the experiment one and the experiment two. The SMAC-SD protocol performance is proved to meet the design objective by comparing the experiment one and the experiment two.

(1) Simulation experiment one: simulation of SMAC-SD Protocol at the low-load networks.

(2) Experiment one: By the simulation model and the supporting settings of the parameters, the networks is set in the low-load networks. The SMAC-SD protocol is simulated.

(3) Simulation scene of the experiment one: set four mobile wireless nodes, one base station and three wired nodes (one of them is set as the routing). The four wireless nodes are the original nodes, which can set two data streams of the different transactions. The wired nodes are objective nodes, and different objective nodes receive the different transaction data stream. The original nodes 0,1 send the important transaction data stream, which is received by the objective node 1. The original nodes 2,4 send the general transaction data stream, which is received by the node 2. The wireless node 0 is responsible for the routing. The topology of the simulation scene of the experiment one is shown as figure 7-31 :

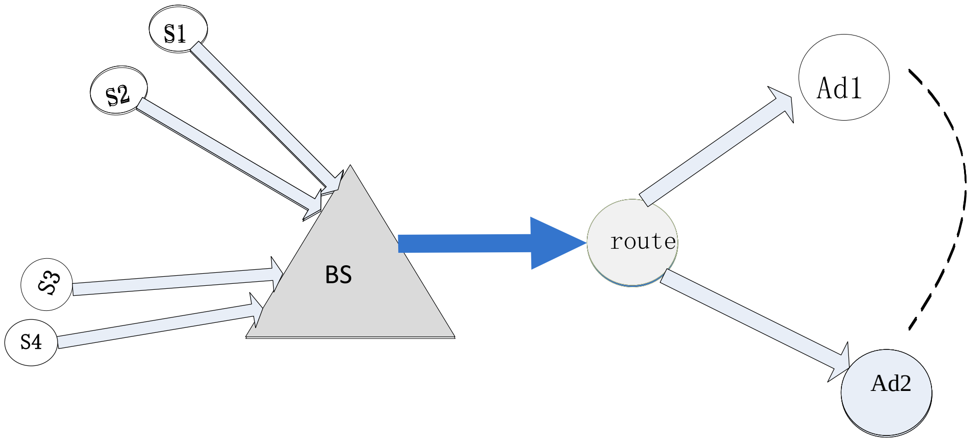


Figure 7-31 Topology of Low-load simulation experiment Scene

The related simulation parameters of the important transaction data stream are shown as table 7.8:

Table 7.8 Simulation parameters

Parameter	Value	Parameter	Value
Routing protocol	DSDV	maximal window	7
data stream	CBR	minimal window	15
agency protocol	UDP	size of the data packet	256
Priority	0(High)	Send packet rate	100Kb
AIFS	2	Simulation time	50s

The related simulation parameters of the general transaction data stream are shown as table 7.9:

Table 7.9 Simulation parameters

Parameter	Value	Parameter	Value
Route	AODV	maximal window	15
Data Flow	CBR	minimal widow	31
Protocol agent	UDP	size of the data packet	256
Traffic priorities	1（low）	Send packet rate	100Kb
AIFS	2	Simulation time	50s

(4). Simulation experiment two: simulation of SMAC-SD Protocol at the high-load networks

Experiment two: By the simulation model and the supporting settings of the parameters, the networks are set in the high-load networks. The SMAC-SD protocol is simulated.

Simulation scene of the experiment two: set 8 mobile wireless nodes, one base station and three wired nodes (one of them is set as the routing). The 8 wireless nodes are the original nodes, which can set two data streams of the different transactions. The wired nodes are objective nodes, and different objective nodes receive the different transaction data stream. The original nodes 0,1, 2, 3 send the important transaction data stream, which is received by the objective node 1. The original nodes 4, 5, 6, 7 send the general transaction data flow, which is consider receiving by the node 2. The wireless node 0 is responsible for the routing. The topology of the simulation scene of the experiment two is shown in Figure 30and Figure 31:

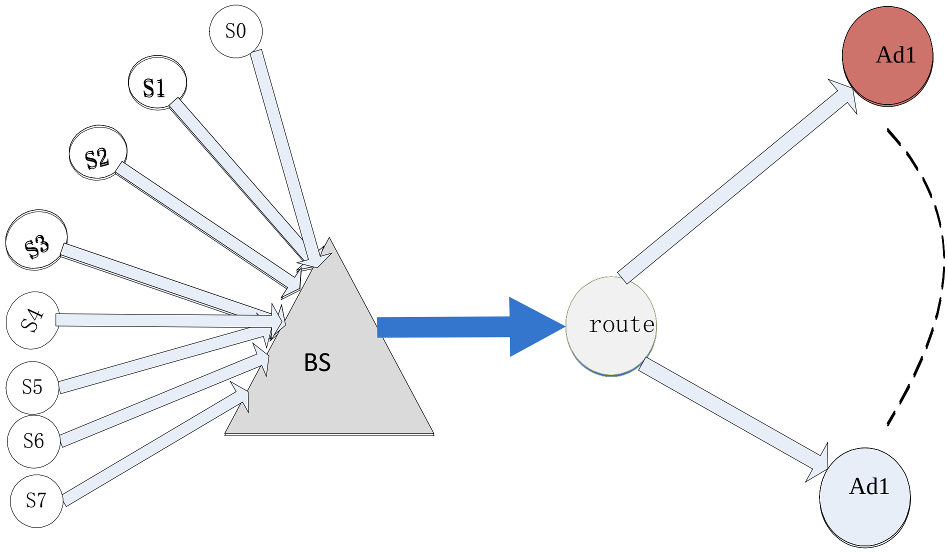


Figure 7-32 Topology of High-load simulation experiment Scene

The related simulation parameters of the important transaction data stream and the general transaction data stream are same with table 7.8 and table 7.9.

7.4.3. Performance Analysis of Low-load Protocol

In this simulation experiment, the wired link is set as 10 M, the wireless link is set as 1m, the sending rate of every wireless nodes are 100kb, and there are 4 wireless nodes. The network is in the condition of relax facing to the load. The trace file is obtained after the simulation. The following results are obtained by the analysis of the AWK tool:

1. Throughput

Due to the large amount of the obtained data, the data analyzed by awk needs to be treated to be shown with the graphic. Take the low-sdsmac-through as an example. There are 7626 rows data in the original file of sdmac-put-important. In order to show the change trend of the throughput with the time, and value of the throughput is set equidistantly with the probability of 0.01. One group is taken out every 100 rows. There are totally 76 groups of data.

Under two transactions, the chart of the throughput as a function of time in the SMAC-SD protocol at the low-load and the chart of the throughput as a function of time in the S-MAC protocol at the low-load are shown respectively as follows figure:

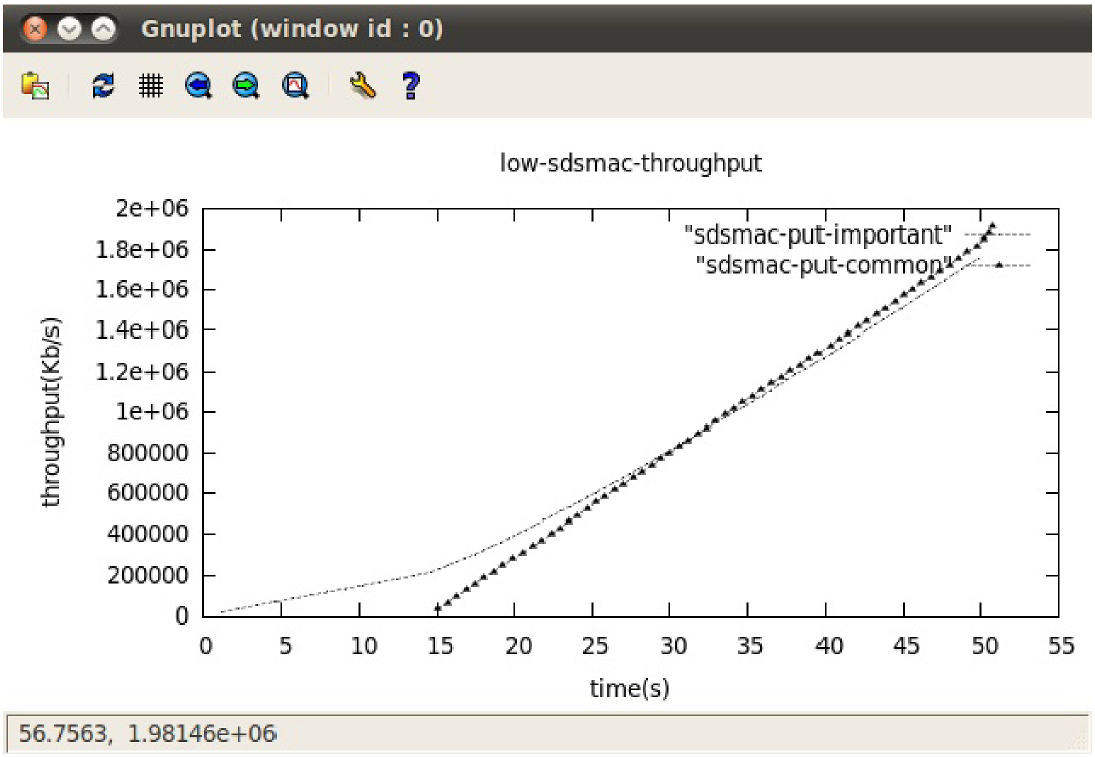


Figure 7-33 Throughput of the Low-load SMAC-SD protocol in the Different Trnasactions

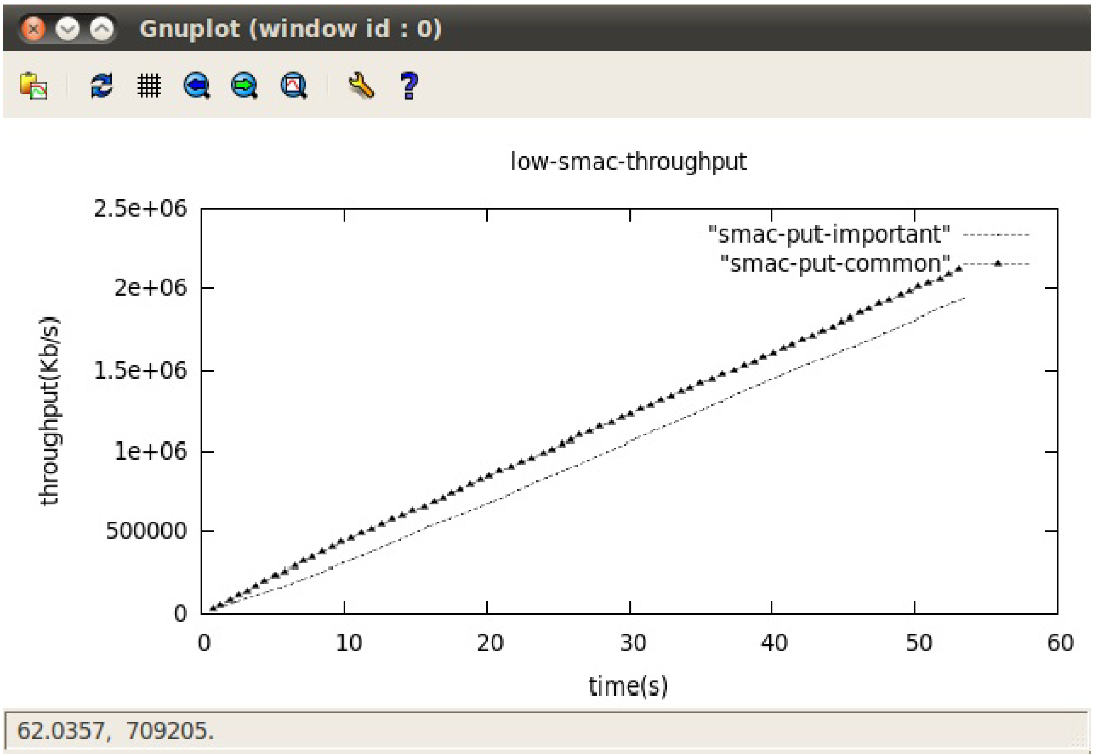


Figure 7-34 Throughput of the Low-load S-MAC procotol in the Different Transactions

In the simulation, set the bandwidth wireless link as 1M, there are 4 wireless nodes, the rate of sending is 100 kb/s, the percentage of load is less than 40% of the maximal load of the channel. The channel is in the low-load condition with the reasonable competition. It can be concluded from analyzing the above two figures at the low-load:

In the SMAC-SD protocol, the important transaction is set as the high priority 0, the general transaction is set as the low priority 1. The effective transmission of the important transaction is guaranteed by different size of the competition window and by channel request mechanism of multi-sending RTS frames in the access slot. As shown in the Figure 7-33, the important transaction almost uses all channel resources from 0 to 15s. However, the general transaction begins to receive the data packet from the 15s, and there is no obvious difference throughput between the important transaction and the general transaction after 15s. Thus, the ability to seize the channel of the important transaction data is better than the general transaction data. Under the premise of good transmission of the data for the two transactions, the SMAC-SD protocol can firstly ensure the transmission of the important transaction.

S-MAC protocol does not divide the priority of the transaction, all types of the transactions compete fairly for the channel. As illustrated in the Figure 7-33 and 7-34, the data Throughputs of different types of transactions are similar, and the slight error can be omitted.

3. System delay

The time interval of the system delay data that is analyzed by awk is small, the jitter amplitude is large, and the drawn pictures are not clear. In order to show the performance of the system delay, low-sdsmac-delay is set as an example. SMAC-SD delay-important original data is valued equidistantly with 0.01 probabilities, one group is taken out every 10 rows.

Under two transactions, the chart of the throughput as a function of time in the SMAC-SD protocol at the low-load and the chart of the throughput as a function of time in the S-MAC protocol at the low-load are shown respectively as follows

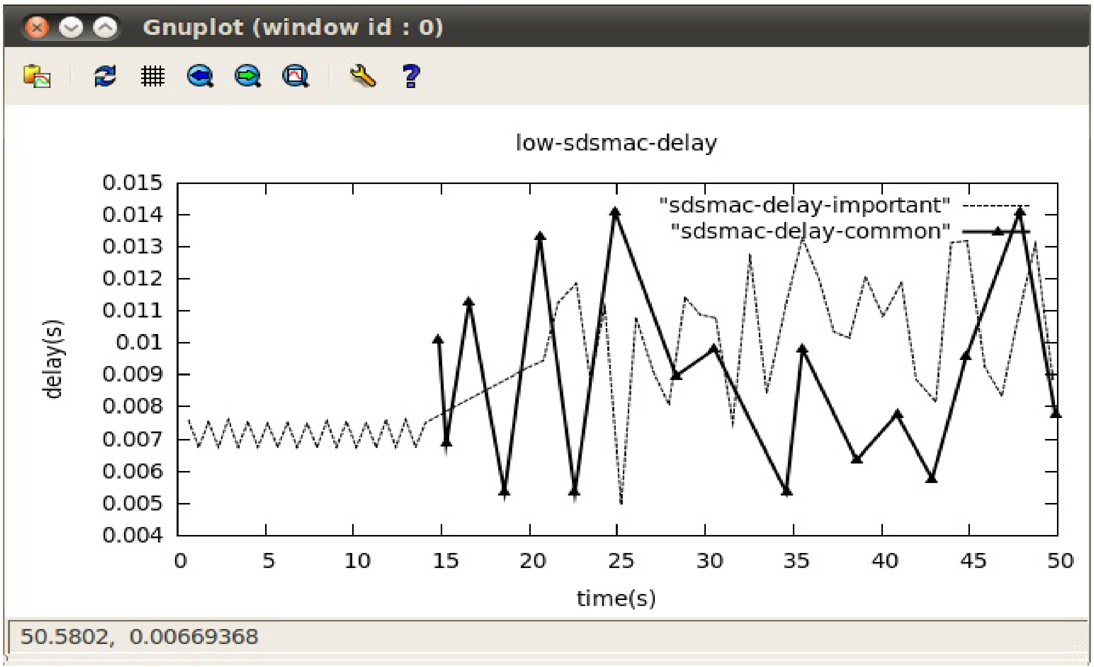


Figure 7-35 System Delay of the Low-load SMAC-SD protocol in the Different Transactions

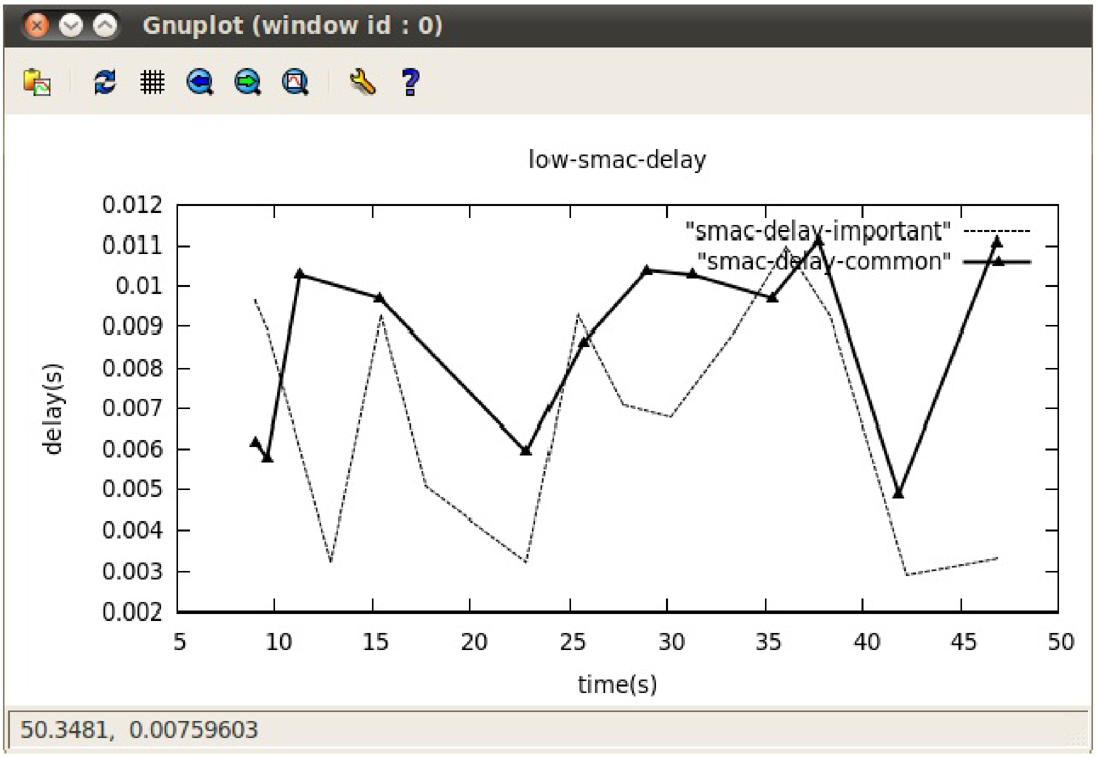


Figure 7-36 System Delay of the Low-load S-MAC protocol in the Different Transactions

Under the condition of low-load, it is known from the above the two figures7-35 and 7-36:

In the SMAC-SD protocol, from 0s to 15s, the system delay of the important transaction data stream is concentrated with 0.0072s and is waved constantly with the margin of 0.0003s. After 15s, the entire of the delay increases to be concentrated with 0.008s and is waved with the margin of 0.004s. In the general transaction, there is no transmission before 15s, and the system delay is empty. After 15s, the system delay is concentrated with 0.010s and is waved inconstantly with the margin of 0.005s. Thus, the wave range of the important transaction is lower than the one of the general transaction in the SMAC-SD. The delay in the important transaction is more stable, which can ensure the effective transmission of the important transaction.

In the S-MAC protocol, there is no big difference of the system delay between the important transaction and the general transaction. Both of them is concentrated with 0.009s and is waved with the margin of 0.005s.

4. Packet loss rate

Table 7-10 Packet loss rate of the different transactions at low-load in the SMAC-SD protocol and S-MAC protocol

Protocol type	Important transaction		General transaction	
	Packet loss number	Packet loss rate	Packet loss number	Packet loss rate
SMAC-SD	1285	0.144418	2672	0.299820
S-MAC	1314	0.147442	1146	0.128591

From the data in the Table 7-10, it shows:

Under the condition of the same load of the important transaction and general transaction in the SMAC-SD protocol, the packet loss number of the important transaction is 1285, the packet loss number of the general transaction is 2672; the packet loss rate of the important transaction is 14.45%, the packet loss rate of the general transaction is 29.98%. The packet loss rate of the important transaction is about 50% of the one of the general transaction, but the packet loss probabilities of two transactions are small. Thus, under the condition of the low load, the SMAC-SD protocol can effectively ensure the transmission of the different transactions, but it will firstly ensure the transmission of the important transaction. The performance of the important transaction is better.

Under the condition of the same load of the important transaction and general transaction in the S-MAC protocol, the packet loss number of the important transaction is 1314, the packet loss number of the general transaction is 1146; the packet loss rate of the important transaction is 14.74%, the packet loss rate of the general transaction is 12.86%. Thus, the packet loss probabilities of the different data are similar in the S-MAC protocol. The slight error can be omitted.

7.4.4 Performance Analysis of high-load Protocol

In this simulation experiment, the wired link is set as 10 M, the wireless link is set as 1m, the sending rate of every wireless nodes are 125kb, and there are 8 wireless nodes. The network is in the condition of full-load. The trace file is obtained after the simulation. The following results are obtained by the analysis of the AWK tool:

1.Throughput

Due to the large amount of the obtained data, the data analyzed by awk needs to be treated to be shown with the graphic. Take the high-sdsmac-through as an example. There are 10180 rows data in the original file of sdmac-put-important. In order to show the change trend of the throughput with the time, and value of the throughput is set equidistantly with the probability of 0.01. One group is taken out every 100 rows. There are totally 101 groups of data.

Throughout two transactions, the chart of the throughput as a function of time in the SMAC-SD protocol at the high-load and the chart of the throughput as a function of time in the S-MAC protocol at the high-load are shown respectively as figure 7-37 and figure 7-38

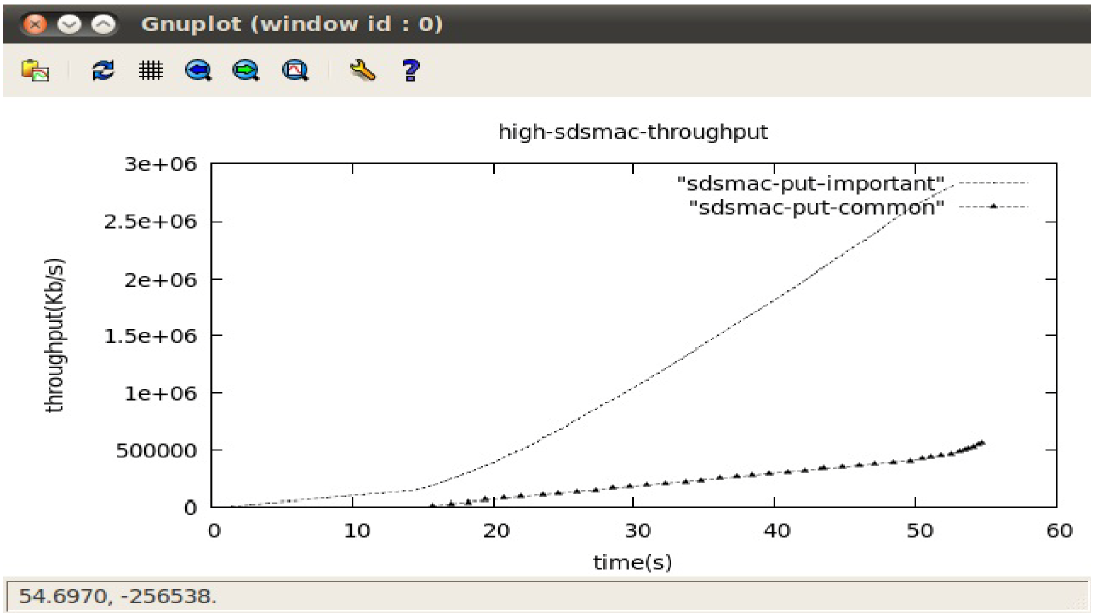


Figure 7-37 Throughput of the high-load SMAC-SD protocol in the Different Transactions

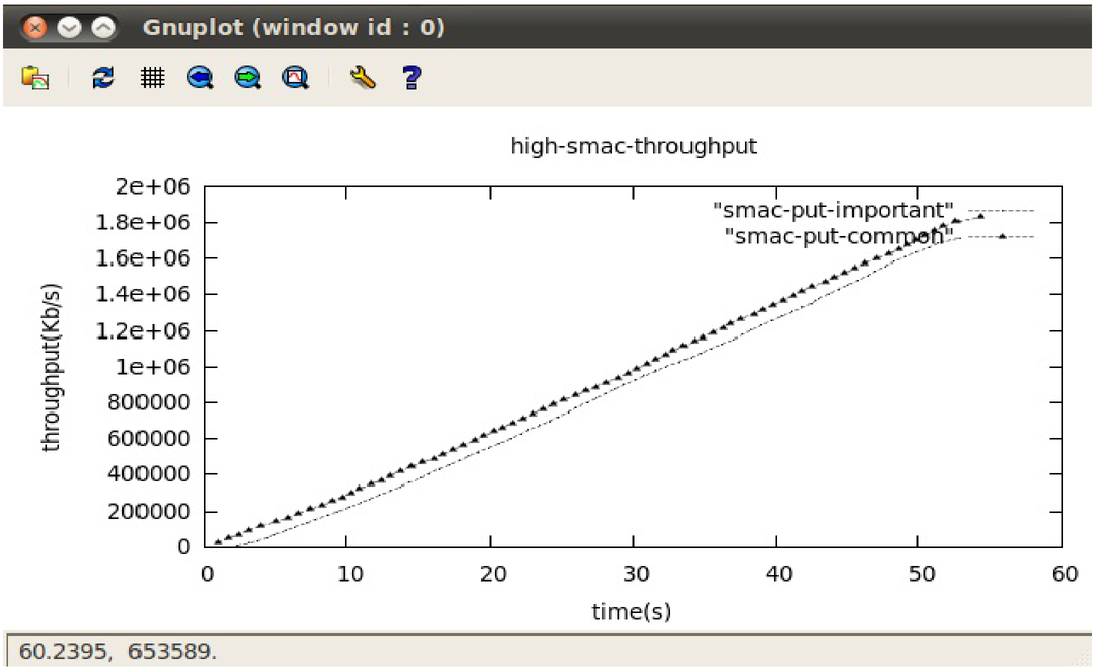


Figure 7-38 Throughput of the high-load S-MAC protocol in the Different Transactions

It can be concluded from analyzing the above two figures at the low-load:

In the SMAC-SD protocol, the important transaction is set as the high priority 0, the general transaction is set as the low priority 1. The effective transmission of the important transaction is guaranteed by different size of the competition window and by channel request mechanism of multi-sending RTS frames in the access slot. As shown in the Figure 5-9, the important transaction almost uses all channel resources from 0 to 15s. After 15s, the throughput of the important transaction remains as much as five times than the one of the general transaction. However, the general transaction begins to receive the data packet from the 15s, and the throughput increases slowly after 15s. Thus, the ability to seize the channel of the important transaction data is better than the general transaction data considering the full-load and the channel competition. There is large difference throughput between the important transaction and the general transaction. The excellent performance of the important transaction is ensured by sacrificing the transmission performance of the general transaction. At the same time, under the extreme conditions of the full-load system, the general transaction can seize the channel to ensure that there is no transmission hunger in the general transaction and ensure the basic requirement of the transmission.

S-MAC protocol does not divide the priority of the transaction, all types of the transactions competite fairly for the channel. As illustrated in the Figure 5-10, the data Throughputs of different types of transactions are similar, and the slight error can be omitted.

2. System delay

The time interval of the system delay data that is analyzed by awk is small, the jitter amplitude is large, and the drawn pictures are not clear. In order to show the performance of the system delay, high-sdsmac-delay is set as an example. There is 2712 rows of data in the sdsmac-delay-important original data. It is valued equidistantly with 0.02 probabilities. One group is taken out every 50 rows and there 54 rows of data being obtained.

Under two transactions, the chart of the throughput as a function of time in the

SMAC-SD protocol at the full-load and the chart of the throughput as a function of time in the S-MAC protocol at the full-load are shown respectively as figure 7-39 and figure 7-40.

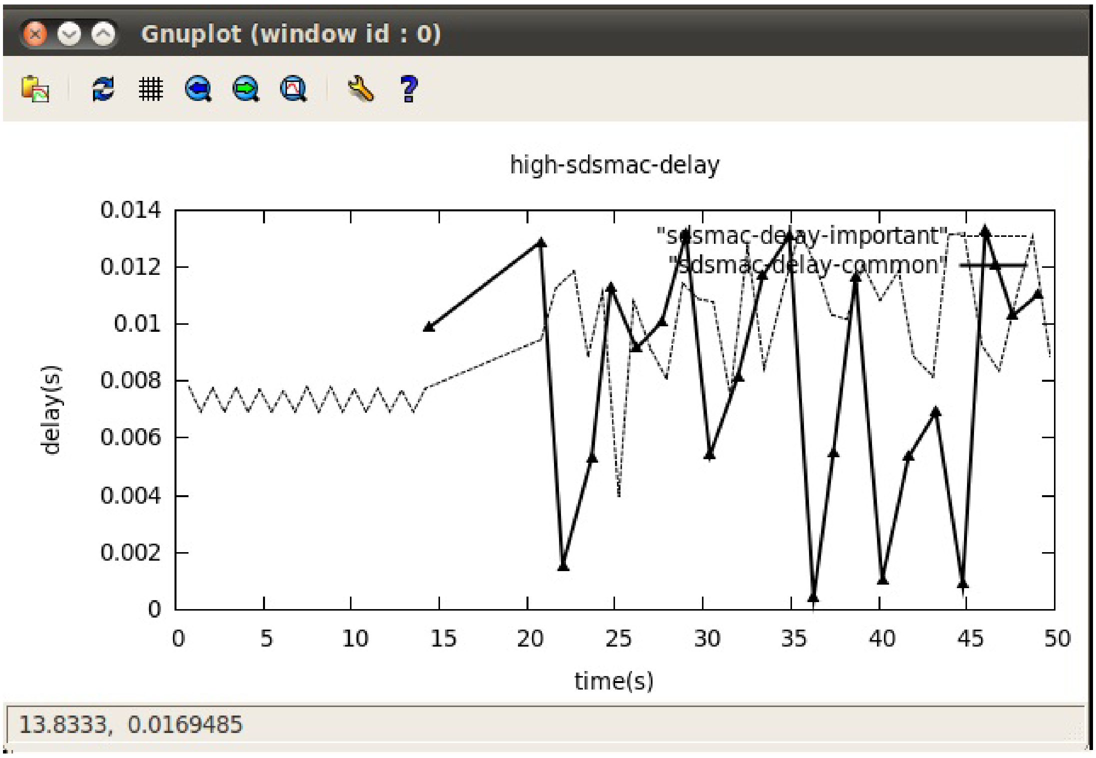


Figure 7-39 System Delay of the high-load SMAC-SD protocol in the Different Transactions

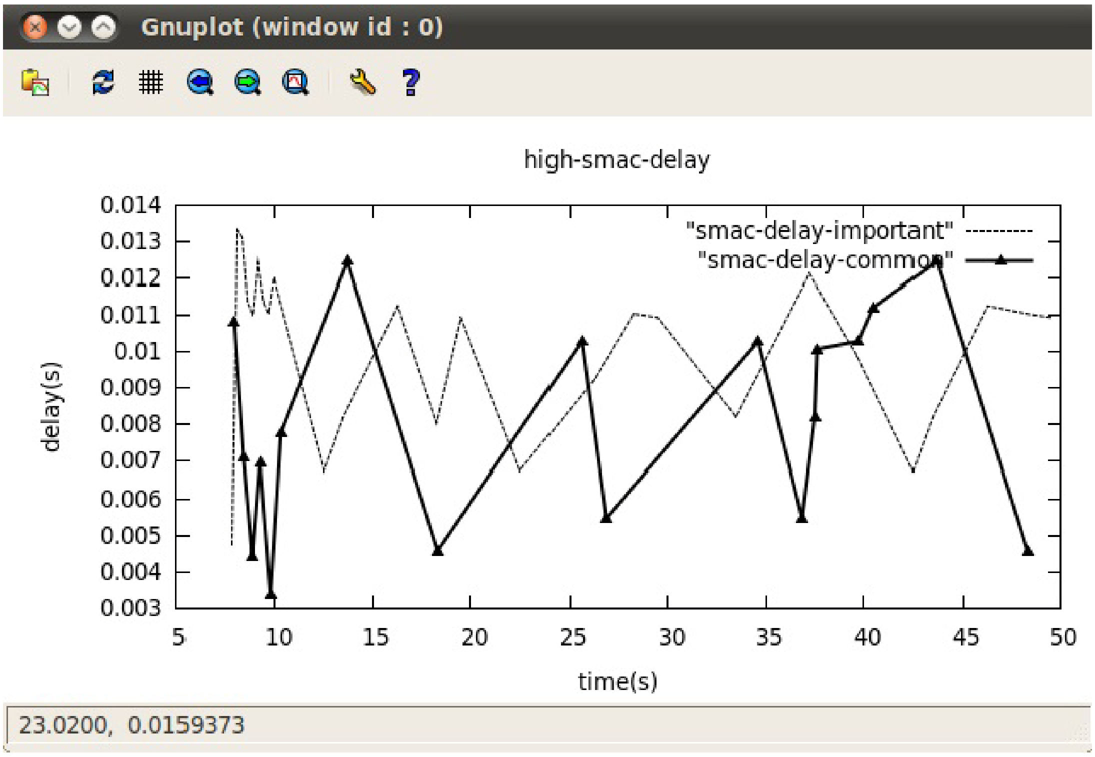


Figure 7-40 System Delay of the high-load S-MAC protocol in the Different Transactions

Comparing the figure 7-39 and figure 7-40, it shows: in the SMAC-SD protocol with high-load networks, from 0s to 15s, the system delay of the important transaction data stream is concentrated with 0.0075s and is waved with low margin, which is shown in Figure 5-11. After 15s, the entire of the delay begins to increase. After 20s, it is concentrated with 0.01s and waved. The margin of waving is 6 times more than the one from 0s to 15s. In the general transaction, there is no transmission before 15s, and the system delay is empty. After 15s, the system delay is concentrated with 0.070s and is waved inconstantly with the margin of 0.007s. The reason for the empty delay of the first 15s in the general transaction is shown in Figure 5-9. The channel is used for the transmission of the important transaction in the first 15s, and there is no data transmission for the general transaction during this time. Thus, the concentration of the delay and the wave range of the important transaction are lower than the ones of the general transaction in the SMAC-SD. The delay in the important transaction is more stable, which can ensure the effective transmission of the important transaction in the

SMAC-SD protocol.

In the S-MAC protocol, there is no big difference of the system delay between the important transaction and the general transaction. Both of them is concentrated with 0.0085s and is waved with the margin of 0.0005s.

3.Packet loss rate

Table 7-11 Packet loss rate of the different transactions at high-load in the SMAC-SD protocol and S-MAC protocol

Type of protocol	Important transaction		General transaction	
	packet	Loss packet	packet	Loss packet
SMAC-SD	4671	0.314503	3583	0.482494
S-MAC	3349	0.225491	3385	0.488738

In the full-load SMAC-SD protocol, the packet loss number of the important transaction is 4671, the packet loss number of the general transaction is 3583; the packet loss rate of the important transaction is 31.45%, the packet loss rate of the general transaction is 48.25%. The packet loss rate of the important transaction is about 60% of the one of the general transaction. The packet loss number of the important transaction is lower. Thus, the full-load SMAC-SD protocol can effectively ensure the transmission of the important transaction and basically ensure the transmission of the general transaction.

Under the condition of the same load of the important transaction and general transaction in the S-MAC protocol, the packet loss number of the important transaction is 2849, the packet loss number of the general transaction is 3885; the packet loss rate of the important transaction is 22.55%, the packet loss rate of the general transaction is 48.87%. Thus, there are no differed priorities in the transactions of the S-MAC. The packet loss rate is random.

7.4.5 General Analysis

It is concluded by analyzing the general performance of the SMAC-SD protocol and the S-MAC protocol without dividing the types of the transactions:

1.Total throughput of the system

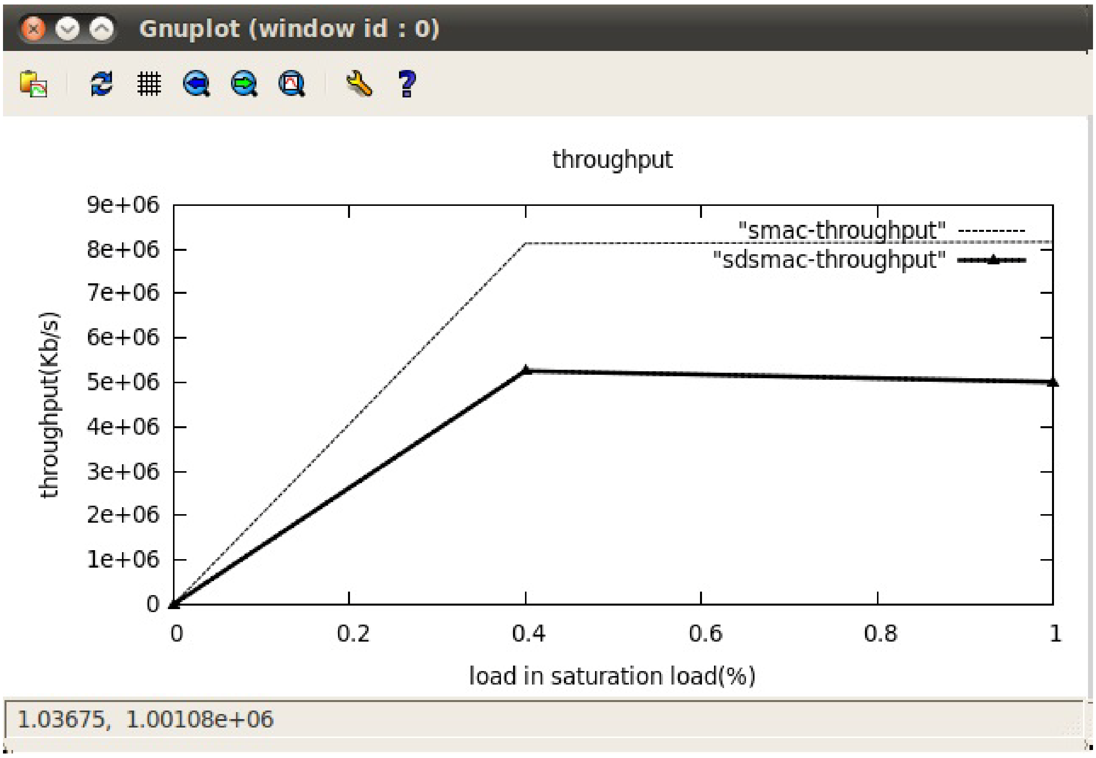


Figure 7-41 Change Trend of the Throughput as a function of the load in the SMAC-SD protocol and the S-MAC protocol

From Figure 7-41, the total throughput of the SMAC-SD protocol is lower than the one of the S-MAC protocol, and both of them slightly decrease with the increasing of the load. There are two reasons leading to this change: (1) SMAC-SD protocol focuses on the assurance for the performance of the important transaction. The performance of the important transaction is higher than all other transactions in the SMAC-SD protocol. However, the performance of the general transaction decreases. Thus, the system performance of the SMAC-SD decreases slightly. (2) the access slot and the competition window of the SMAC-SD protocol increases, which lead to the increasing of the free timing. To sum up, the total throughput of the SMAC-SD protocol system decreases slightly.

2.System packet loss rate

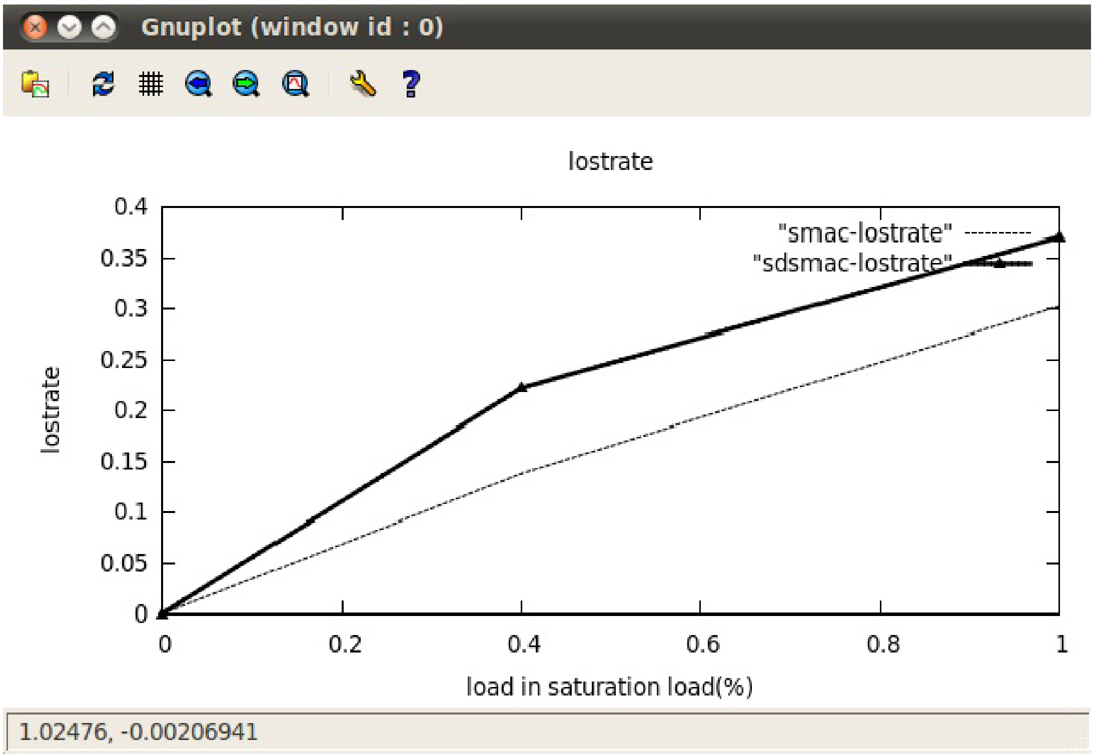


Figure 7-42. The change of the packet loss rate as a function of the load in the SMAC-SD protocol and the S-MAC protocol

Figure 7-42 shows the result of simulation, because the throughput of the SMAC-SD protocol is slightly lower than the one of the S-MAC protocol, the packet loss rate of the SMAC-SD is slightly higher than the one of the S-MAC protocol.

3.Average system delay

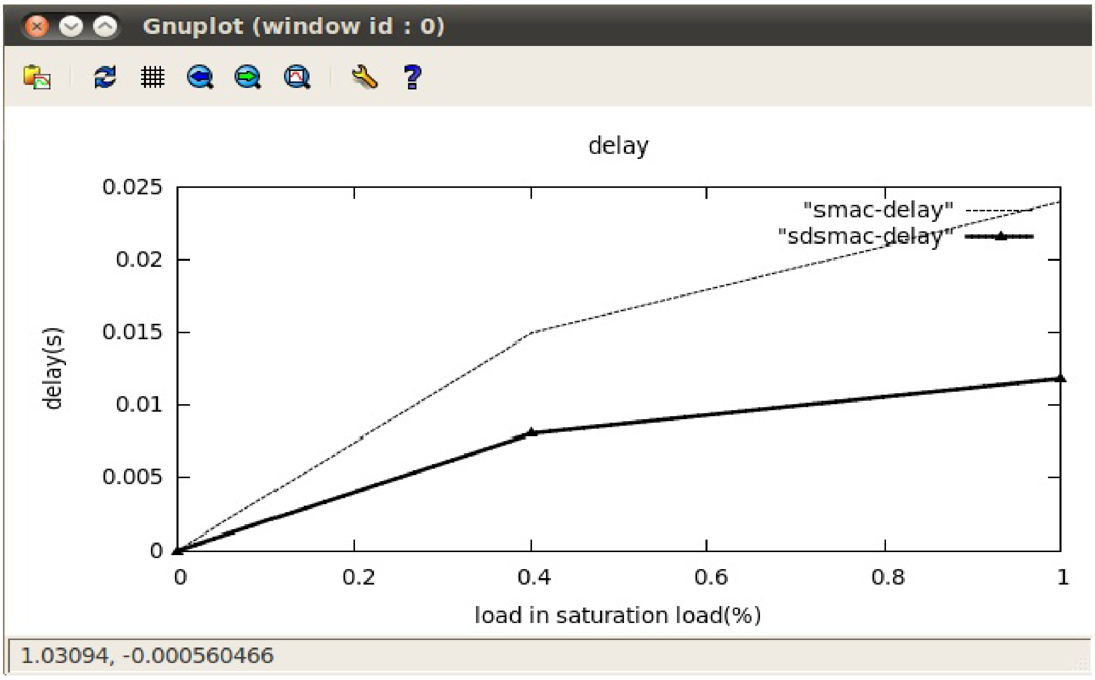


Figure 7-43 the change of the packet loss rate as a function of the load in the SMAC-SD protocol and the S-MAC protocol

From the Figure 7-43, the average system delay of the SMAC-SD protocol is lower than the one of the S-MAC protocol. For the data that is sensitive to the delay, SMAC-SD protocol is better

To sum up, although the total throughput of the SMAC-SD protocol slightly decreases compared with the one of the S-MAC protocol, the throughput of the important transaction is higher than all transactions in the S-MAC protocol. At the same time, the average delay of the SMAC-SD protocol increases badly compared with the one of the S-MAC protocol. Moreover, the delay of the important transaction in the SMAC-SD protocol is much better than the average value.

Under the condition of the intense competition in the channel, the SMAC-SD protocol can effectively protect the transmission of the important transaction, which is in accordance with the objectives.

7.5 summary

1. To RBLEACH, it can be concluded from the results of the experimental simulation that RBLEACH has largely prolongs the lifetime of each sensor node. It also solves the problem of the premature death of the nodes in LEACH protocol caused by the far-to-close death and by the premature communication paralysis in the region far away from the base station.

2. To PS-ACO-LEACH, Simulation results show that this protocol can avoid network node energy consumption and energy consumption imbalance, which is caused by unsatisfactory cluster head selection or poor routing paths. Compared with LEACH, PS-ACO-LEACH improves the robustness of the network more effectively, promotes balance of network energy consumption and enhances the network life cycle effectively.

3. To MIA-QRP , it select route based on the multiple QoS parameters, including delay, loss of package and quality. The test results show that the protocol can find a path quickly and maintain the path effectively.

4.To SMAC-SD, the new protocol was verified by the NS2 simulation platform. The simulation results show that the improved protocol can gain the throughput of vital service and shorten the delay at the same time, and improve the performance of network effectively.

Chapter 8 Conclusions and Future Work

8.1 Conclusions

1. Comparing the RBLEACH algorithm and the LEAHC algorithm, the energy cost of communication between each member node, head of cluster and base station is less, the life cycle of the networks is elongated, and the multi-hop data transmission between the clusters largely save the energy of each sensor node compared with the LEACH protocol.

2. PS-ACO-LEACH protocol prevents too much energy cost or non-balanced energy cost caused by the unsatisfactory selection of head of cluster or poor routing path. Compared with LEACH, PS-ACO-LEACH protocol effectively improves the network scalability, contributes to the balanced energy cost of network, and elongates the life cycle of networks effectively.

3. MIA-QRP self-adaptive routing algorithm can rapidly find the path and make effective maintenance to the path. The optimized path to the destination node can be calculated according to the MIA-QRP self-adaptive routing algorithm. This protocol supports multi-hop forwarding and occupies few system resources.

4. According to service differentiation, SMAC-SD adopts an access mechanism based on different priorities. It can adjust priority mechanism based on service queue and channel multi-request mechanisms, and configure waiting queues with different priorities and RTS retries for different service with different priorities, which can make vital service get high channel access probability and ensure the transmission quality of vital service. The simulation results show that the improved protocol can gain the throughput of vital service and shorten the delay at the same time, and improve the performance of network effectively.

8.2 Future work

1. In this thesis, the clusters are designed with the proportioned selections and communication path between clusters in a special divided area. However, in actual condition, there is possible difference density in the distribution of sensor nodes in the network. The distributions do not show the uniform and random assumed in this thesis. Thus, the division for the network should be judged by the density, which makes the problem more complex. In the future, a clustering algorithm with optimized function should be considered in order to adapt to all the changing factors.

2. For PS and ACO, in this thesis, the PS optimization clustering just uses the basic PS with a slow convergence rate, high-energy consumption of nodes, and a massive consumption of time. This basic PS also possibly results in the part optimization, not the overall optimization. In the future, a more detailed research for the PS should be developed to apply to the improved PS, so as to optimize the clustering. The basic ACO is also used in the stage of multi-jumping routing. Simply seeking for the shortest routing in the ESN routing protocol is not the best program. In the future, an improved AC should be developed in this part and should be connected with energy, location and other information to optimize the routing selection in order to decrease the energy consumption of routing and elongate the lifetime of the network. Meanwhile, because of large amount of weight parameters and complex relation between each parameter in the PS fitness function, it is a very complex problem to decide the best parameters to optimize the settings of clustering groups. In this thesis, a calculation method for the optimized parameters is concluded for the random distribution of the nodes. However, this method is not universal, and cannot be applied for the non-uniform distribution of the nodes (e.g. random Gaussian distribution). The author will further research the optimized weight parameters combination in the fitness functions.

3. In this thesis, the MIA-QRP self-adaptive QoS routing protocol just considers

the delay of link, package loss rate and strength of the node signal, which can be only adaptive for the network application of the part QoS protection and needs. According to the application prospects of the WSN, The networks should dynamically perceive the networks application and the QoS service demands, and comprehensively evaluate the QoS service guarantee. Moreover, because the limited resource can only build a simple testing environment, the protocol function cannot be evaluated currently in the conditions with a large amount of nodes.

4. For QoS, since WSNs have to interact with the environment, their characteristics can be expected to be very different from other conventional data networks. Thus, while WSNs inherit most of the QoS challenges from general wireless networks, including severe resource constraints, unbalanced traffic, data redundancy, multiple sinks, packet criticality and so on, it will is studied how to design MAC protocol to satisfy QoS. .

References

[1] Anna Hac. Wireless Sensor Network Designs [M].Hoboken, NJ: John Wiley & Sons Ltd,2003.

[2] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal. Wireless sensor network survey [J].Computer Networks, 2008: 2292–2330.

[3] J. Yick, B. Mukherjee, D. Ghosal, Analysis of a Prediction-based Mobility Adaptive Tracking Algorithm, in: Proceedings of the IEEE Second International Conference on Broadband Networks (BROADNETS), Boston, 2005.

[4] M. Castillo-Effen, D.H. Quintela, R. Jordan, W. Westhoff, W. Moreno, Wireless sensor networks for flash-flood alerting, in: Proceedings of the Fifth IEEE International Caracas Conference on Devices, Circuits, and Systems, Dominican Republic, 2004.

[5] T. Gao, D. Greenspan, M. Welsh, R.R. Juang, A. Alm, Vital signs monitoring and patienttracking over a wireless network, in: Proceedings of the 27th IEEE EMBS Annual International Conference, 2005.

[6] G. Wener-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees, M. Walsh, Deploying a wireless sensor network on an active volcano, Data-Driven Applications inSensor Networks (Special Issue), IEEE Internet Computing, March/April 2006.

[7] F. Ehlers, D. Sofge, M. Chitre and J. Potter, "Distributed Mobile Sensor Networks for hazardous Applications", International Journal of Distributed Sensor networks, vol. 2012, **(2012)**, pp. 1-3.

[8] Vivek Katiyar,Prashant Kumar,Narottam Chand,An Intelligent Transportation Systems Architecture using Wireless Sensor Networks,International Journal of Computer Applications (0975 – 8887) Volume 14– No.2, January 2011

[9]KSHITIJ SHINGHAL,WIRELESS SENSOR NETWORKS IN AGRICULTURE: FOR POTATO FARMING,International Journal of Engineering

Science and Technology,Vol. 2(8), 2010, 3955-3963

[10] Heinzelman W, Chandrakasan A, Balakrishnan H. Energy-efficient Communication Protocol for Wireless Microsensor Networks[C]. In Proceeding of the 33rd,Annual Hawaii Int'l Conf.on System Sciences. Maui：IEEE Comoputer Society, 2000: 3005-3014.

[11] Lindsey S, Raghavendra C S. Pegasis: Power-efficient Gathering in Sensor Information Systems[C]//Proc. of IEEE Int'l Conf. on Computer Systems. San Francisco, USA: [s. n.], 2002.

[12] S.S. Satapathy and N. Sarma, TREEPSI: tree based energy efficient protocol for sensor information ,Wireless and Optical Communications Networks 2006, IFIP International Conference 11-13,April 2006 .

[13] Rajesh Patel,Sunil Pariyani,Vijay Ukani,Energy and Throughput Analysis of Hierarchical Routing Protocol (LEACH) for Wireless Sensor Network,International Journal of Computer Applications (0975 – 8887),Volume 20– No.4, April 2011

[14] Renold, A.P. ; Poongothai, R. ; Parthasarathy, R. , Performance analysis of LEACH with gray hole attack in Wireless Sensor Networks, Computer Communication and Informatics (ICCCI), 2012 International Conference on, Date 10-12 Jan. 2012

[15] Ravneet Kaur, Deepika Sharma2 and Navdeep Kaur, Comparative Analysis Of Leach And Its Descendant Protocols In Wireless Sensor Network, International Journal of P2P Network Trends and Technology- Volume3Issue1- 2013,P51-54

[16] Qian Liao, Hao Zhu, An Energy Balanced Clustering Algorithm Based on LEACH Protocol, Proceedings of the 2nd International Conference On Systems Engineering and Modeling (ICSEM-13)

[17] Nguyen Duy Tan, Longzhe Han, Nguyen Dinh Viet, and Minho Jo,An Improved LEACH Routing Protocol for Energy-Efficiency of Wireless Sensor Networks,Smart Computing Review, vol. 2, no. 5, October 2012,P360-390

[18] Rajashree.V.Biradar , Dr. S. R. Sawant , Dr. R. R. Mudholkar, Dr. V.C .Patil, Multihop Routing In Self-Organizing Wireless Sensor Networks IJCSI International

Journal of Computer Science Issues, Vol. 8, Issue 1, January 2011 155 ISSN (Online): 1694-0814,P155-164

[19]Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. IEEE Communications Magazine, 2002,40(8): 102−114

[20] R.Sumathi and M.G.Srinivas,A Survey of QoS Based Routing Protocols for Wireless Sensor Networks,J Inf Process Syst, Vol.8, No.4, December 2012,http://dx.doi.org/10.3745/JIPS.2012.8.4.589

[21]LAN MAN Standards Committee of the IEEE Computer Society, Wireless LAN medium access control (MAC) and physical layer (PHY) specification,IEEE, New York, NY, USA, IEEE Std 802.11-1997 edition, 1997.

[22] van Dam T, Langendoen K. An adaptive energyefficient mac protocol for wireless sensor networks. In: Proc. of the 1st ACM Conf. on Embedded Networked Sensor Systems (SenSys). New York: ACM Press, 2003. 171−180.

[23] Ye W, Heidemann J, Estrin D. An energy-efficient MAC protocol for wireless sensor network. In: Proc. of the INFOCOM 2002. San Francisco: IEEE Computer Society, 2002.

[24]Vithya, G. ; St. Joseph"s Coll. Of Eng., Chennai, India ; Vinayagasundaram, B.Actuation sensor with adaptive routing and QOS aware checkpoint arrangement on Wireless Multimedia Sensor Network, Recent Trends in Information Technology (ICRTIT), 2011 International Conference on 3-5 June 2011 Page 444 - 449.

[25]Jafarzadeh, S.Z. ; Dept. of Comput. Eng., Ferdowsi Univ., Mashhad, Iran ; Moghaddam, M.H.Y. Design of energy-aware QoS routing protocol in wireless sensor networks using reinforcement learning,Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on 4-7 May 2014 page1 - 5

[26]Rui Dai ; Broadband Wireless Networking Lab., Georgia Inst. of Technol., Atlanta, GA, USA ; Pu Wang ; Akyildiz, IF. Correlation-Aware QoS Routing With Differential Coding for Wireless Video Sensor Networks,Multimedia, IEEE Transactions on (Volume:14 , Issue: 5)page 1469 - 1479.

[27]Jing Feng ; Inst. of Meteorol., PLA Univ. of Sci. & Technol., Nanjing, China ; Xiaoxing Yu ; Zijun Liu ; Cuihan Wang,A QoS Enhanced Routing Protocol in Wireless Sensor Networks,Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on July 31 2011-Aug. 4 2011,page 1 - 6

[28] Akyildiz I，Su W, Cayirci E. Wireless sensor network [J]. Computer Networks. 2002，vol.38: 393-422.

[29] Jiming Chen, Linrui Zhong, SUN You-Xian, wireless sensor networks Communications System [J]. Sensing Technology,2006,19(4):1290-1295.

[30] Edgar H. Callaway. Wireless sensor networks: Architectures and protocols[M]. BocaRaton: CRC Press, Jan.2004.

[31] Yongxin Liu,Zhaoxia Wang,Junqi Zhao,Zhenda Sun,A wireless sensor network node design based on ZigBee protocol,Automatic Control and Artificial Intelligence (ACAI 2012), International Conference on 3-5 March 2012,P:325 – 328

[32] Considine, J.; Li, F.; Kollios, G. & Byers, J. (2004). Approximate aggregation techniques for sensor databases, In Proceedings of ICDE, pp. 449-460, April, 2004.

[33] T.H. Kim and S. Hong, “Sensor Network Management Protocol for State-Driven Execution Environment,” in Proc. ICUC Conf., Oct. 2003

[34] I.F. Akyildiz, J.N. and A. E. Kamal , “Routing techniques in wireless sensor networks : A survey”, IEEE Wireless Communications , vol.11, no.6, pp.6-28, 2004.

[35] Jiming Chen, Linrui Zhong, SUN You-Xian, wireless sensor networks Communications System [J]. Sensing Technology,2006,19(4):1290-1295.

[36] Edgar H. Callaway. Wireless sensor networks: Architectures and protocols[M]. BocaRaton: CRC Press, Jan.2004.

[37] Nets-noss: Creating an architecture for wireless sensor networks.

[38] C-Y. Chong, S.P. Kumar, Sensor networks: evolution, Opportunities, and challenges, Proceedings of the IEEE 91 (8) (2003) 1247–1256.

[39] Eliana Stavrou, Wireless Sensor Networks, part 2: Limitations,Web Hosting Articles

[40] W. Ye, J. Heidemann, and D. Estrin, “Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks,” IEEE/ACM Trans. Net., vol. 12,no. 3, June 2004, pp. 493–506.

[41] A. El-Hoiydi, “Spatial TDMA and CSMA with Preamble Sampling for Low Power Ad Hoc Wireless Sensor Networks,” Proc. ISCC 2002, July 2002, pp. 685–92.

[42] Al-Sakib Khan Pathan,Hyung-Woo Lee,Choong Seon Hong,Security in Wireless Sensor Networks: Issues and Challenges,Feb. 20-22, 2006 ICACT2006

[43] Jeremy Elson and Deborah Estrin, Time Synchronization forWireless Sensor Networks, In Proceedings of the First Workshop on Hot Topics in Networks (HotNetsI),2829,October 2002, Princeton, New Jersey, USA.http://www.acm.org/sigcomm/HotNetsI

[44] Mohammad Reza Gholami, Positioning Algorithms for Wireless Sensor Networks, Communication Systems Group Department of Signals and Systems chalmers university of technology,Gothenburg, Sweden 2011

[45] Sasikala V and C. Chandrasekar, Energy Efficient Multipath Data Fusion Technique for Wireless Sensor Networks, ACEEE Int. J. on Network Security , Vol. 03, No. 02, April 2012

[46] Haiying Shen; Fayetteville, AR ;Ting Li,Data Management of Wireless Sensor Networks,Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE

[47] David E. Culler , Arch Rock Corp. TinyOS: Operating System Design for Wireless Sensor Networks, Networking & Communication

[48] KAZEM SOHRABY,DANIEL MINOLI,TAIEB ZNATI,WIRELESS SENSOR NETWORKSTechnology, Protocols, and Applications,A JOHN WILEY&SONS,INC. PUBLICATION

[49] Gyanendra Prasad Joshi, Seung Yeob Nam and Sung Won Kim, Cognitive Radio Wireless Sensor Networks: Applications, Challenges and Research

Trends,Sensors 13, no. 9: 11196-11228.

[50] Dazhi Chen and Pramod K. Varshney,QoS Support in Wireless Sensor Networks:A Survey, International Conference on Wireless Networks - ICWN , pp. 227-233, 2004

[51] Shamsad Parvin,Muhammad Sajjadur Rahim,Routing Protocols for Wireless Sensor Networks: A Comparative Study,International Conference on Electronics, Computer and Communication (ICECC 2008),PP891-894

[52] G. Gupta, M. Younis. Load-balanced clustering in wireless sensor networks[C]. Proceedings of the International Conference on Communication (ICC 2003), Anchorage, Alaska, 2003.

[53] D. J. Baker and A. Epheremides, “The Architectural Organization of a Moblie Radio Network via a Distributed Algorithm,” IEEE Transactions on Communications, vol. Com-29, no. 11, November 1981.

[54] P. Tsigas, “Project on Moblie Ad Hoc Networking and Clustering for the Course EDA390 Computer Communcation and Distributed Systems,” Manual for University Course.

[55] A. Amis, R. Prakash, T. Vuong, and D. Huynh, “Max-Min D-Cluster Formation in Wireless Ad Hoc Networks,” IEEE INFOCOM, March,2000

[56] K. Akkaya, M. Younis. A survey on routing protocols for wire less sensor networks[J]. Journal of Ad Hoc Networks, 2005, 3(3):325-349.

[57] M. Younis, M. Youssef, K, Arisha. Energy-aware management in cluster-based sensor networks[J]. Computer Networks, 2003, 43(5):649-668.

[58] Y. T. Hou, Y. Shi, H. D. Sherali. On energy provisioning and relay node placement for wireless sensor networks[J]. IEEE Transactions on Wireless Communications, 2005,4(5):2579-2590.

[59] G. Jolly, M. Younis. An energy efficient, scalable and collision less MAC layer protocol for wireless sensor networks[J]. Wireless Communications and Mobile Computing, 2005, 5(3):285-304.

[60] Qianfeng Jiang,Manivannan D,"Routing.Protocol for Sensor Network"[A]. In:Consumer Communciations and Networking Conference[C].2004.93-98

[61] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy

Efficient Communication Protocol for Wireless Micro Sensor Networks,” Proceedings of IEEE HICSS, Jan 2000.

[62] C. F. Chiasserini, I. Chlamtac, P. Monti, and A. Nucci, “Energy Efficient Design of Wireless Ad Hoc Networks,” Proceedings of European,Wireless, Feb 2002.

[63] S. Bandyopadhyay and E. J. Coyle, “An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks,” IEEE INFOCOM,April 2003.

[64] K. Dasgupta, K. Kalpakis, P. Namjoshi. An efficient clustering-based heuristic for data gathering and aggregation in sensor networks[C]. Proceedings of the IEEE Wireless Communications and Networking Conference(WCNC 2003), New Orleans, LA, 2003.

[65] Jianping Pany Y. Thomas Houz Lin Caiy Yi Shiz Sherman X. Sheny,Topology Control for Wireless Sensor Networks,MobiCom’03, September 14–19, 2003, San Diego, California, USA.p286-299

[66] Yao Liang Rui Liu,Routing Topology Inference for Wireless Sensor Networks,ACM SIGCOMM Computer Communication Review,Volume 43, Number 2, April 2013

[67] T. Zhao, W. Cai, and Y. Li. MPIDA: A sensor network topology inference algorithm. In Proc. Int.Conf. on Computational Intelligence and Security,PP 451-455, 2007.

[68] Y. Yang, Y. Xu, and X. Li. Topology tomography in wireless sensor networks based on data aggregation. In Proc. Int. Conf. on Communications and Mobile Computing, pages 37{41, 2009.

[69] Bhaskar Krishnamachari, Deborah Estrin, Stephen Wicker, Modelling Data-Centric Routing in Wireless Sensor Nwetwork,

[70] Kemal Akkaya, Mohamed Younis,A survey on routing protocols for wireless

sensor ,Ad Hoc Networks 3 (2005) 325–349

[71] Jae-Hwan Chang, Maximum lifetime routing in wireless sensor networks, Browse Journals & Magazines > Networking, IEEE/ACM Transaction Volume:12 Issue:4

[72] Jianmin Zhang, Load-balanced Route Discovery for Wireless Sensor Networks, JOURNAL OF NETWORKS, VOL. 5, NO. 9, SEPTEMBER 2010,p1060-1067

[73] Hai Liu, Amiya Nayak, and Ivan Stojmenovi´c, Fault-Tolerant Algorithms/Protocols in Wireless Sensor Networks, S. Misra et al. (eds.), Guide to Wireless Sensor Networks, Computer Communications and Networks, DOI: 10.1007/978-1-84882-218-4 10,p261-291

[74] D. J. Baker, A. Ephremides. The architectural organization of a mobile radio network via a distributed algorithm[J]. IEEE Transactions on Communications, 1981, 29(11):1694-1701.

[75] K. Xu, M. Gerla, A heterogeneous routing protocol based on a new stable clustering scheme[C]. Proceeding of IEEE Military Communications Conference (MILCOM 2002), Anaheim, CA, October 2002.

[76] S. Bandyopadhyay, E. Coyle. An energy efficient hierarchical clustering algorithm for wireless sensor networks[C]. Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), San Francisco, California, 2003.

[77]O. Younis, S. Fahmy.: A Hybrid, Energy-Efficient, Distributed clustering approach for Ad Hoc sensor networks[J]. IEEE Transactions on Mobile Computing, 2004, 3(4):325-349.

[78]P. Ding, J. Holliday, A. Celik, Distributed energy efficient hierarchical clustering for wireless sensor networks, in: Proceedings of the IEEE International Conference on Distributed Computing in Sensor Systems(DCOSS’05), Marina Del Rey, CA, June 2005.

[79]Heinzelman W,Chandarkasan A,Balakrishnan H.Energy-efficient

Communication Protocol for Wireless Microsensor Networks[C].In Proceeding of the 33rd Annual Hawaii Int'l conf. on System Science. Maui: IEEE Computer Society,2000:3005-30

[80]M. Ettus. System Capacity, Latency, and Power Consumption in Multihop-routed SS-CDMA Wireless Networks. In Radio and Wireless Conference (RAWCON '98), pages 55–58, Aug. 1998

[81]X. Lin and I. Stojmenovic. Power-Aware Routing in Ad Hoc Wireless Networks. In SITE, University of Ottawa, TR-98-11, Dec. 1998

[82]T. Meng and R. Volkan. Distributed Network Protocols for Wireless Communication. In Proc. IEEEE ISCAS, May 1998.

[83]Wendy Beth Heinzelman. Application-Specific Protocol Architecture for Wireless Networks. PhD thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 2000.

[84] Zuo Chen,Kai Chen,An improved Multi-hop Routing Protocol for Large-Scale Wireless Sensor Network Based on Merging Adjacent Clusters,JOURNAL OF SOFTWARE, VOL. 8, NO. 8, AUGUST 2013,pp2080-2085.

[85] B. Manzoora, N. Javaida, O. Rehmana, etl,Q-LEACH: A New Routing Protocol for WSNs,The 4th International Conference on Ambient Systems, Networks and Technologies (ANT 2013), the 3rd International Conference on Sustainable Energy Information Technology (SEIT-2013),Volume 19, 2013, Pages 926–931

[86] Thiemo Voigt, Hartmut Ritter, Jochen Schiller,Adam Dunkels, and Juan Alonso. Solar-aware Clustering in Wireless Sensor Networks. In Proceedings of the Ninth IEEE Symposium on Computers and Communications, June 2004.

[87] Farooq, M.O, Dogar, A.B. ; Shah, G. MR-LEACH: Multi-hop Routing with Low Energy Adaptive Clustering Hierarchy, Sensor Technologies and Applications (SENSORCOMM), 2010 Fourth International Conference on 18-25 July 2010

[88] Wu Xinhua ,Wang Sheng, Performance Comparison of LEACH and LEACH-C Protocols by NS2, Distributed Computing and Applications to Business Engineering and Science (DCABES),

2010 Ninth International Symposium on 18-25 July 2010

[89] Sunkara Vinodh Kumar and Ajit Pal ,Assisted-Leach (A-Leach) Energy Efficient Routing Protocol for Wireless Sensor Networks, *International Journal of Computer and Communication Engineering, Vol. 2, No. 4, July 2013*

[90] Mustapha Khiati, Djamel Djenouri,BOD-LEACH: broadcasting over duty-cycled radio using LEACH clustering for delay/power efficient dissimilation in wireless sensor networks, International Journal of Communication Systems,24 SEP 2013

[91] JIANG Yang，SUN Liu-lin，AO Wen-jun，YUAN Min,Research on optimal cluster-head number of LEACH routing protocol for WSN,Application Research of Computers,Vol. 27 No. 11Nov． 2010

[92] Hu Junping, Jin Yuhui, Dou Liang. A Time-based Cluster-Head Selection Algorithm for LEACH[J]. Computers and Communications,2008.ISCC 2008.IEEE Symposium on, 2008,1172-1176

[93]. Jing Chen, Hong Shen. MELEACH-L: More Energy-efficient LEACH for Large-scale WSNS[J]. Wireless Communication and Sensor Networks,2008.WCSN 2008.Fourth International Conference on, 2008, 1-6.

[94] Rajendran V，Obraczka K，Garcia-Luna-Aceves J． Energy-efficient，collision-free medium access control for wireless sensor networks． Embedded Networked Sensor Systems，November 2003，LosAngeles，CA． 181-192

[95] Mortaza Fahimi Khaton Abad, Mohammad Ali Jabraeil Jamali,Modify LEACH Algorithm for Wireless Sensor Network,IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 1, September 2011,ISSN (Online): 1694-0814

[96] Lan Tien Nguyen, Xavier Defago, Razvan Beuran,Yoichi Shinoda,An Energy Efficient Routing Scheme for Mobile Wireless Sensor Networks,IEEE ISWCS 2008,pp568-572

[97] E. Bonabeau, M. Dorigo, and G. Theraulaz. Swarm Intelligence: From

Natural to Arifical Systems. New York：Oxford University Press，1999.

[98] Ajith Abraham, et.al. Swarm Intelligent Systems[M]. Studies in Computational Intelligence,Volume 26: 3-25

[99] Kenndy J, Eberhart R.C. Paricle Swarm Optimization. In: IEEE International Conference on Neural Networks, IV. Piscataway, NJ: IEEE Service Center,1995.1942-1948.

[100] Shi, Y.; Eberhart, R.C. (1998). "A modified particle swarm optimizer". Proceedings of IEEE International Conference on Evolutionary Computation. pp. 69–73.

[101] Marco Dorigo, Vittorio Maniezzo, Alberto Colorni. The Antsystem: Optimization by a Colony of Cooperating Agents [J]. IEEE Transactions on Systems, Man, and Cybermetrics, 1996, 26 (1):1-13.

[102] Marco Dorigo, Luca Maria Gam bardella. Ant Colony System: A Cooperative Learning Approach to the Traveling Salesman Problem [J]. IEEE Transactions on Evolutionary Computation, 1997, 1 (1): 53-66.

[103]Marco Dorigo, Ant System: Optimization by a Colony of Cooperating Agents,IEEE TRANSACTIONS ON SYSTEMS,MAN, AND CYBERNETICS-PART B:CYBERNETICS,VOL,26,NO,1,February 1996

[104] Raghavendra V. Kulkarni, and Ganesh Kumar Venayagamoorthy, Particle Swarm Optimization in Wireless Sensor Networks: A Brief Survey,IEEE TRANSACTION ON SYSTEM,MAN AND CYBERNETICS-PART C:APPLICATIONS AND REVIEW

[105] Xue Wang,Jun-Jie Ma, Sheng Wang,Dao-Wei Bi,Distributed Particle Swarm Optimization and Simulated Annealing for Energy-efficient Coverage in Wireless Sensor Networks,Sensors (Basel). 2007 May; 7(5): 628–648

[106] Santi P Silence is folden with high probability: maintaining a connected backbone in wireless sensor networks [A].In; Proc. of 1st European Workshop on Wireless Sensor Networks[C].Betlin,2004

[107] J. Hu, J. Song, M. Zhang, and X. Kang, "Topology optimization for urban traffic sensor network," Tsinghua Science & Technology, vol. 13,Apr 2008.

[108] J. Li, K. Li, and W. Zhu, "Improving sensing coverage of wireless sensor networks by employing mobile robots," in Proceedings of the International Conference on Robotics and Biomimetics (ROBIO), 2007,pp. 899–903.

[109] T. P. Hong and G. N. Shiu, "Allocating multiple base stations undergeneral power consumption by the particle swarm optimization," in Proceedings of the IEEE Swarm Intelligence Symposium (SIS), 2007,pp. 23–28

[110]Xin Guan, Guan L., Wang X.G., Ohtsuki, A Novel Routing Algorithm based on Ant Colony System for Wireless Sensor Networks[C]. Proceedings of 18th International Conference on Computer Communications and Networks(ICCCN 2009), 2009: 1-5.

[111] Ziyadi, M, Yasami, K.,Abolhassani, B, Adaptive Clustering for Energy Efficient Wireless Sensor Networks based on Ant Colony Optimization [C]. Seventh Annual Communication Networks and Services Research Conference (CNSR '09), 2009: 330-334.

[112] Salehpour A.A, Mirmobin. B, Afzali-Kusha A, Mohammadi S. An Energy Efficient Routing Protocol for Cluster-Based Wireless Sensor Networks Using Ant Colony Optimization[C].International Conference on Innovations in Information Technology (IIT 2008), 2008: 455-459.

[113] Ghasem Aghaei R. Rahman A.M. Rahman M.A, Gueaieb W. Ant Colony-Based Many-to-One Sensory Data Routing in Wireless Sensor Networks[C]. International Conference on Computer Systems and Applications (AICCSA 2008), 2008: 1005-1010.

[114] http://www.rfc-base.org/rfc-2386.html

[115] Prasun Sinha, QoS Issues in Ad-Hoc Networks, Ad Hoc Networks,2005, Publisher:Springer US, pp 229-247

[116] P.Gupta, P.R.Kumar. A System and traffic dependent adaptive routing

algorithm for ad hoc networks.The 36th Conference on Decision and Control.San Diego,California,1997:2375-2380.

[117] Anelise Munaretto, Hakim Badis, Khaldoun Al Agha, Guy Pujolle, A Link-state QoS Routing Protocol for Ad Hoc Networks, Mobile and Wireless Communications Network, 2002. 4th International Workshop on 2002

[118] Shigang Chen,Klara N.Distributed quality-of-service routing in Ad hoc networks.IEEE Journal on Selected Areas in Communications,1999,17(8):1488-1505.

[119]SHI JIAN, ZOULING, A QoS based distributed multicast routing algorithm in Ad Hoc networks, JOURNAL OF CHINA INSTITUTE OF COMMUNICATIONS, 2003, 24(6)

[120] Chenxi Zhu, M. ScottCorson. QoS routing for mobile ad hoc networks. INFOCOM,2002,6(2): 958-967

[121] HUANG C, DA IF, WUJ. On-Demand location-aided QoS routing in ad hoc networks. In：Proc．Of the Int’l Conf．On Parallel Processing(ICPP)．2004:502—509.

[122] Sivakumar, R.; Sinha, P. ; Bharghavan, V.,CEDAR: a Core-Extraction Distributed Ad hoc Routing algorithm, Selected Areas in Communications, IEEE Journal on (Volume:17 , Issue: 8)

[123] Prasun Sinha , Raghupathy Sivakumar , Vaduvur Bharghavan, Multicast Core-Extraction Distributed Ad hoc Routing, In Proc. of the Wireless Communications and Networking Conference, 1999

[124] Wang jianxin,et al,A quality of service routing protocol based on mobility prediction in mobile ad hoc networks, Journal CSUT Vol 10, No1, 2003: 53—57.

[125] Li Layuan, Li Chunlin, A QoS multicast routing protocol for mobile ad-hoc networks, Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on 4-6 April 2005

[126] Wang Lei. Research and implementation of Linux data packet capture technology based on Gigabit network. Ji'nan: Shandong University,2007

[127] Chang Feng Meng Zhuanliang ,Based on ARM-Linux network driver designs. Communication technology.2012.6(45):32-35.

[128]Yigitel M A，Ozlem Durmaz Incel，Cem Ersoy．QoS-aware MAC protocols for wireless sensor networks：A survey〖J]. Computer Networks，2011(SUPPL)：l-23．

[129] http://onlinelibrary.wiley.com/doi/10.1002/0470867787.ch6/summary.

[130] Bao L, Garcia-Luna-Aceves J J. A new approach to channel access scheduling for ad hoc networks.[C] In: Proc 7th Annual Int’l Conference on Mobile Computing and Networking,(MobiCOM 2001), Rome, Italy, July 16-21, 2001. 210~221

[131] Rajendran V, Obracazka K, Garcia-Luna-Aceves J J.Energy-efficient, collision-free medium access control for wireless sensor networks[A]. Proc 1st Int’l Annual Joint Confon Embedded Networked Sensor Systems (SenSys)[C], Nov.5-7,2003, Los Angeles, CA. 181~192

[132]Lu G, Krishnamachari B, Raghavendra C. An adaptive energy-efficient and low-latency MAC for data gathering in wireless sensor networks.[C] In: Proc 18th Int’l Parallel and Distributed Processing Symp (IPDPS’04), April 26-30, 2004,Santa Fe, New Mexico. 224~230

[133] IEEE Computer Society LAN MAN Standards Committee. IEEE Std 802.11-1999, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. 1999

[134]Langendoen K, Van Dam T. An adaptive energy-efficient MAC protocol for wireless sensor networks.[C] In: Proc 1st Int’l Annual Joint Conf on Embedded Networked Sensor Systems (SenSys), Nov. 5-7,2003, Los Angeles, CA. 2003

[135] Langendoen K, Van Dam T. An adaptive energy-efficient MAC protocol for wireless sensor networks.[C] In: Proc 1st Int’l Annual Joint Conf on Embedded Networked Sensor Systems (SenSys), Nov. 5-7,2003, Los Angeles, CA. 2003

[136]Jamieson K, Balakrishnan H, Tay Y C. Sift: A MAC protocol for event-driven wireless sensor networks.[J],MIT-LCS-TR-894, 2003.

[137] Lee, David Y. AT&T Bell Labs, Murray Hill, NJ, USA Yannakakis, Mihalis.Principles and methods of testing finite state machines-a survey.Proceedings of the IEEE.Aug 1996:1090-1123.

[138] Matthias Grossglauser, David N.C. Tse, Mobility Increases The Capacity of Wireless Ad Hoc Networks. INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, Volume: 3, 2001. Page(s): 1360 -1369 vol.3.

[139]Schult N,Mirhakkak M,LaRocca D, Strater J, Routing in mobile Ad Hoc networks, Military Communications Conference Proceedings, IEEE, Volume: 1,1999: 10 -14 vol.1.

[140] Wang, Yunbo Dept. of Comput. Sci. & Eng., Univ. of Nebraska - Lincoln, Lincoln, NE, USA Vuran, Mehmet C.; Goddard, Steve.Cross-Layer Analysis of the End-to-End Delay Distribution in Wireless Sensor Networks.Networking, IEEE/ACM Transactions on. Feb.2012:305-318.

[141] Xing Yang, Li zhicun, Gao qian, A Delay guaranteed QoS routing protocol. Microcomputer Information. 2012.5(28):127-129.

[142] Wang S Y,Liu J Y,Huang C C.Signal strength-based routing protocol for mobile ad hoc networks, Proceedings of the 2005 IEEE International Conference on Advanced Information Networking and Applications, 2005:17-20.

[143]Xiuqin Yi,Xiaotong Zhu.Application of Entropy Weight Coefficient Method to the Evaluation of the profitability of listed firms.Computer Application and System Modeling (ICCASM), 2010 International Conference on.Oct.2010:108-110.

[144]Jinbo Song, Yan Liu, Danrong Song.Multi-grade Fuzzy Comprehensive Evaluation of BOT Projects Service Quality Based on Fuzzy Entropy Weight Coefficient Method.2012 Fifth International Conference on Business Intelligence and Financial Engineering (BIFE).Aug.2012:556-560.

[145]FengKong,Zhiguang Zhang,Ying Liu.Research on improvement of grey relation analysis method based on ideal points.Computing, 2007. WiCom 2007.

International Conference on Wireless Communications, Networking and Mobile.Sept.2007:5717-5720.

[146] CHANG Feng,MENG Chuan-liang,development of Network Driver Program based on Embedded Linux,Communications Technology,2012, 45(6):32-35.

[147] Wang yang, Zhuchaoxia,Research on Linux Multithread Synchronization Based on Semaphore, COMPUTER AND DIGITAL ENGINEERING,2004,4:20-22.

[148] Ye Dun-fan, Zhou Fe fan; Min Liang-liang.Design and Implementation of High-Precision Timer in Linux.Computer Science and Information Engineering.2009 WRI World Congress on Volume:7 Digital Object Identifier:10.1109/CSIE.2009.277.Publication Year:2009,Page(s): 341- 345.

[149] Sung-Ju Lee and Mario Gerla,A Simulation Study of Table-Driven and On-Demand Routing Protocols for Mobile Ad Hoc Networks,IEEE Network July/August 1999,p48-54

[150] G. Bianchi, “IEEE 802.11: saturation throughput analysis,” IEEE Commun.Lett., vol. 2, pp. 318-320, Dec. 1998.

[151] G. Bianchi, “Performance analysis of the IEEE 802.11 distributed coordination function,” IEEE J. Select. Areas Commun., vol. 18, pp. 535-547,Mar. 2000.

[152] Yang Xiao． Performance Analysis of IEEE802.1le EDCF Under Saturation Condition[C] ． Proceedings of 2004 IEEE International Conference on Communications． IEEE，June2004： 170-174

[153] Zhu Lin,Research and Implementation OnWireless Router Based on Embedded Linux,Chengdu University of Technology in Communications and information technology, Master’s thesis,2009.

Appendix1

Published papers

1.Hua Long, Qian Lei , Joan Lu ,A New RSSI-based Centroid Localization Algorithm Using Virtual Reference Tags, INFOCOMP2013

2. Hua Long, Joan Lu, S .Chao, Jim Yip, Handoff algorithm improvement and its analysis for mobile networks. In: Proceedings of the 2007 International Conference on Communications. CSREA Press, pp. 66-71. ISBN 1-60132-030-2

3.Hua Long， Joan Lu, , Yip, J.; Hua Long Jiang, An Improved Access Scheme Based on Multiple-Hop Priority and Cross-Layer Design in 802.11e , Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference

4.Hua Long, Joan Lu,Yubin Shao, Guantao and Yip, Yau Jim (2007) A Clustering Algorithm for Block Mobility in Ad-hoc Network. Communications of SIWN, 5. ISSN 1757-4439

5.Hua Long, Joan Lu, Yubin Shao ,Guantao and Yip, Yau Jim ， A new backoff scheme based on channel state for IEEE 802.11e WLANs，Proceedings of the fifth annual meeting of China Institute of Communications,ISBN:9787121059261, PRESS：Publishing House of electronics industry, 2008-2-1

6.Y Che, Hua Long, Joan Lu, YJ Yip,An investigation in self-similar study and implication of 3G mobile traffic, 01/2007; In proceeding of: Proceedings of the 2007 International Conference on Communications in Computing, CIC 2007, June 25-28, 2007, Las Vegas, Nevada, USA,Source: DBLP

Appendix2

kernel program

1．RBLEACH algorithm

```
clear all    %
close all    %
clc          %
%% Simulation parameters
MC  = 100;          % Monte Carlo simulation times
%xm=100;            %x
%ym=100;            %y
 %
xm=200;             %
ym=xm;              %
%sink.xd=0.5*xm;%
%sink.yd=0.5*ym;%
% Base stations are placed in the region boundary, is arranged in the corner
sink.xd=0;%BS x
sink.yd=0;% BS y
N=400;              %  NUMBEROF SENSORS
p=0.1;              % The percentage of the expected cluster head
Cc=0.6 % The fusion rate;
rmax=200; %Toll rounsa
Rmax=200 % the total number of rounds;
CM=32; % The size of the control information
CM=32;% control message size
```

DM=4000; % Data size

DM=4000;% data size

E0=0.05; % Single node initial energy

The initial energy of single node E0=0.05;%

ETX=50*0.000000001; % Transport energy consumption（J/bit）

ETX=50*0.000000001;% transmission energy consumption (J/bit)

ERX=50*0.000000001; % Receive energy consumption（J/bit）

ERX=50*0.000000001;% acceptance of energy consumption (J/bit)

Efs=10*10^(-12); %（free space）Channel model（J/bit/m^2）

Efs=10*10^ (-12);% free space (free space) channel model (J/bit/ meters square)

Emp=0.0013*10^(-12); %（multipath fading）Channel model（J/bit/m^4）

Emp=0.0013*10^ (-12);% multipath attenuation (multipath fading) channel model (4 J/bit/ m)

EDA=5*10^(-12); % Data fusion energy consumption（J/bit）

EDA=5*10^ (-12); energy consumption data fusion (J/bit)

do=sqrt(Efs/Emp); %Efs and EmpBoundary threshold

Do=sqrt (Efs/Emp); demarcation threshold%Efs and Emp, value is 84

Dead = zeros(1,rmax); % Death of nodes per round

Dead = zeros (1, Rmax);% the death of nodes for per round

CH_Num = zeros(1,rmax); % Cluster heads for per round

CH_Num = zeros (1, Rmax);% every wheel cluster characteristic

R_total = 0; % Survival Round

R_total = 0;% survival number of rounds

R_first = 0;% the first death round number

E_left = zeros (1, Rmax);% total residual energy per round

E_CH = zeros(1,rmax); %Each cluster head energy consumption

E_CH = zeros (1, Rmax);% each cluster head energy consumption

for mc = 1:MC

```
    %% The initialization of scene
    figure(1)
    hold off
    for i=1:N
        S(i).xd=rand(1,1)*xm;
        S(i).yd=rand(1,1)*ym;
        S(i).G=0;
        S(i).E=E0;
        S(i).type='N';
        plot(S(i).xd,S(i).yd,'o');
        hold on;
    end
    plot(sink.xd,sink.yd,'x');
Plot (sink.xd, sink.yd,'x');
network area
Partition%% network area
Partition%% network area
QN = 6; % The numbers of area
 QN = 6;% number region division
QN = 6;% number region division
QN = 6;% number region division
QN_num=zeros (1, QN);% of the number of nodes in each region, survival
QN_num=zeros (1, QN);% of the number of nodes in each region, survival
QN_num=zeros (1, QN);% of the number of nodes in each region, survival
CN_num=zeros (1, QN);% of each region the number of cluster heads
CN_num=zeros (1, QN);% of each region the number of cluster heads
Rc=zeros (1, QN);% cluster head ratio of each region
Sqn=zeros (1, QN);% of the area of each region
```

```
R = xm/ (QN-1);% zone radius
R = xm/ (QN-1);% zone radius
R = xm/ (QN-1 zone radius);%
dd=R/10;
Dd=R/10;
Dd=R/10;
Dd=R/10;
% is calculated for each area
Sqn(1)=1/4*pi*R^2;
Sqn (1) =1/4*pi*R^2;
Sqn(QN)=xm*ym-1/4*pi*(QN*R-R)^2;
Sqn (QN) =xm*ym-1/4*pi* (QN*R-R) ^2;
for qn=2:QN-1
for qn=2:QN-1
     Sqn(qn)=1/4*pi*(qn*R)^2-1/4*pi*(qn*R-R)^2;
Sqn (QN) =1/4*pi* (qn*R) ^2-1/4*pi* (qn*R-R) ^2;
end
end
% calculated for each node which belong to the area
for i=1:N
 for i=1:N
        qn = min(floor(distance(sink,S(i))/R),5);
        QN_num(qn+1)=QN_num(qn+1)+1;
        S(i).Q=qn+1;
 end
end
% of each region the number of cluster heads
CN_num(1)=0;
```

```
CN_num (1) =0;
CN_num(2)=1;
CN_num (2) =1;
for qn=3:QN
  for qn=3:QN
    CN_num(qn)=floor(Sqn(qn)/Sqn(1));
    CN_num (QN) =floor (Sqn (QN) /Sqn (1));
  end
end
% painting area division map
alpha=pi/2:-pi/32:0;
Alpha=pi/2:-pi/32:0;
Xround=zeros(QN-1,length(alpha));
Xround=zeros (QN-1, length (alpha));
Yround=zeros(QN-1,length(alpha));
Yround=zeros (QN-1, length (alpha));
for qn=1:QN-1
  for qn=1:QN-1
                for i=1:length(alpha)
                        Xround(qn,i)=R*qn*sin(alpha(i));
                        Yround(qn,i)=R*qn*cos(alpha(i));
                end plot(Xround(qn,:),Yround(qn,:),'r')
Plot (Xround (QN, Yround, (QN:),:),'r')
  end
end
he cluster head ratio of each area%
Disp ('each region of the cluster head ratio');
disp ('region of 1: 0');
```

```
Disp (0 'region of 2: (fixed 1 cluster head)');
    for r=1:rmax
            figure(1);
            hold off;      % Round picture redrawn
            plot(sink.xd,sink.yd,'x');% Draw the base station
            hold on;
              for qn=1:QN-1
                    plot(Xround(qn,:),Yround(qn,:),'r')
              end
            dead=0;          %  The  initial death nodes 0
end
            %% Death statistics node
            QN_num=tttemp;
            for i=1:N
                if(S(i).E<=0)      % If the energy is equal to 0
                    S(i).type='D';
                    plot(S(i).xd,S(i).yd,'r.');
                    QN_num(S(i).Q)=QN_num(S(i).Q)-1; % A surviving node is
calculated for each region
                    dead=dead+1; % Cumulative mortality nodes
                        if(dead==1)    % If the node is the first death occurred
                                if(flag_first_dead==0)
                              first_dead=r;    % Record the first round of death
node
                            flag_first_dead=1;
                        end
                    end
                else
```

```
                S(i).type='N';
                plot(S(i).xd,S(i).yd,'o');
            end
        endflag_first_dead=0;%
Flag_first_dead=0;% the first death node flag variables
Cid=zeros(2/p,rmax);
Cid=zeros (2/p, Rmax);
Cnum=zeros(2/p,rmax);
Cnum=zeros (2/p, Rmax);
tttemp=QN_num;
Tttemp=QN_num;
for r=1:rmax
 for r=1:rmax
figure(1);
Figure 1.
 Round picture redrawnHold off;% every wheel picture re
Plot (sink.xd, sink.yd,'x');% drawing base station
hold on;
Hold on;
for qn=1:QN-1
For qn=1:QN-1
plot(Xround(qn,:),Yround(qn,:),'r')
Plot (Xround (QN, Yround, (QN:),:),'r')
 end
End
dead=0; %
 Dead=0;% initial death node number is 0
statistical dead node%%
```

QN_num=tttemp;

QN_num=tttemp;

for i=1:N

for i＝1：N

if(S(i).E<=0) %

If (S (I).E<=0)% if the energy is less than or equal to 0

S(i).type='D';

S (I).Type='D';

plot(S(i).xd,S(i).yd,'r.');

Plot (S (I).Xd, S (I).Yd,'r.');

QN_num(S(i).Q)=QN_num(S(i).Q)-1; %计算每个区域的存活节点

QN_num (S (I) =QN_num (.Q) S (I).Q) -1;% of each region was calculated survival nodes

Dead=dead+1;% cumulative death of nodes

If (dead==1)% if it is the first death of nodes

if(flag_first_dead==0)

If (flag_first_dead==0)

First_dead=r;% records first appeared dead node sequence

flag_first_dead=1;

Flag_first_dead=1;

end

end

end

end

else

Else

S(i).type='N';

S (I).Type='N';

```
plot(S(i).xd,S(i).yd,'o');
Plot (S (I).Xd, S (I).Yd,'o');
            end
        end
Dead (R) = Dead (R + dead/MC);% record each round of death of nodes
If (dead > = 0.95*N)% of all death exit the loop node
break;
Break;
end
End
%% each region to select cluster head -Leach protocol
% no cluster head region 1, region 2 only 1 cluster head
cluster=0;
Cluster=0;
CN_num=zeros(1,QN);
CN_num=zeros (1, QN);
CN_num(1)=0;
CN_num (1) =0;
CN_num(2)=1;
CN_num (2) =1;
Ptemp=floor(QN_num(2)*rand)+1;
Ptemp=floor (QN_num (2) *rand) +1;
Temp=0;
C2_id=0;
C2_id=0;
for i=1:N
For i=1:N
if(S(i).type ~= 'D' && S(i).Q == 2)
```

```
If (S (I).Type ~ ='D'& & S (I).Q = = 2)
% 2 regional cluster head selection
temp=temp+1;
Temp=temp+1;
if (Ptemp == temp)
If (Ptemp = = temp)
cluster=cluster+1;
Cluster=cluster+1;
S(i).type='C';
S (I).Type='C';
C (cluster).Xd=S (I).Xd;% will this node as cluster head logo
C(cluster).yd=S(i).yd;
C (cluster).Yd=S (I).Yd;
C(cluster).Next=0;
C (cluster).Next=0;
Plot (S (I).Xd, S (I).Yd,'k*');% mapping of this cluster head
C(cluster).distance=distance(sink,S(i));
C (cluster).Distance=distance (sink, S (I));
C (.Id=i cluster);% this cluster head ID
C2_id=i;
C2_id=i;
C(cluster).Q=S(i).Q;
C (cluster).Q=S (I).Q;
Packet_To_Bs (=1 cluster);% and transmitted to the base station data packet
number 1
end
End
end
```

End

% of other regional cluster head selection

if(S(i).type ~= 'D' && S(i).Q > 2)

If (S (I).Type ~ ='D'& & S (I).Q > 2)

p=Rc(S(i).Q);

P=Rc (S (I).Q);

if(rand<= p)

If (rand<= P)

cluster=cluster+1;

Cluster=cluster+1;

S(i).type='C';

S (I).Type='C';

C (cluster).Xd=S (I).Xd;% will this node as cluster head logo

C(cluster).yd=S(i).yd;

C (cluster).Yd=S (I).Yd;

C(cluster).Next=0;

C (cluster).Next=0;

Plot (S (I).Xd, S (I).Yd,'k*');% mapping of this cluster head

C(cluster).distance=distance(sink,S(i));

C (cluster).Distance=distance (sink, S (I));

C (.Id=i cluster);% this cluster head ID

C(cluster).Q=S(i).Q;

CN_num(S(i).Q)=CN_num(S(i).Q)+1;

packet_To_Bs(cluster)=1;% The number of packets sent to the base station for 1

end

end

end

```
            CH_Num(r)=  CH_Num(r)  + duster/MC;        %
            for i=1:N
                if(S(i).type=='N'&&S(i).E>0)%
                    if (S(i).Q == 1)
                        Er1=0;
                        Et1=ETX*DM+Efs*DM*distance(S(i),sink)^2;    % Free
space fading
                    elseif (S(i).Q == 2)
                        Er1=ERX*CM;

Et1=ETX*(CM+DM)+Efs*(CM+DM)*distance(S(i),S(C2_id))^2;    %By the spatial
fading                     else
                        Er1=ERX*CM*CN_num(S(i).Q)*0.5;
                        min_dis = 999999;
                        Pcc=0;
                        for cc=1:cluster
                            if (C(cc).Q==S(i).Q)
                                if (distance(C(cc),S(i))<min_dis)
                                    min_dis=distance(C(cc),S(i));
                                    Pcc=cc;
                                end
                            end
                        end
                        if(min_dis==999999)
                            Et1=ETX*DM+Efs*DM*distance(S(i),sink);    %
                        elseif (min_dis>do)
                            packet_To_Bs(Pcc)=packet_To_Bs(Pcc)+1;
```

```
Et1=ETX*(CM+DM)+Emp*(CM+DM)*min_dis^4;    %
                        else
                            packet_To_Bs(Pcc)=packet_To_Bs(Pcc)+1;

Et1=ETX*(CM+DM)+Efs*(CM+DM)*min_dis^2;    %
                        end
                    end
                    S(i).E=S(i).E-Er1-Et1*0.8;% Residual energy
                end
            end
            %% Computing cluster head routing - greedy algorithm
            for c1=1:cluster
                if (C(c1).Q>2)
                    min_dis=9999;
                    pmin=0;
                    flag=1;
                    qq = C(c1).Q;
                    while (flag)
                        qq = qq-1;
                        for c2=1:cluster
                            if (C(c2).Q==qq)
                                if (distance(C(c2),C(c1))<min_dis &&
distance(C(c2),C(c1))<0.8*distance(sink,C(c1)))
                                    min_dis=distance(C(c2),C(c1));
                                    pmin=c2;
                                end
                            end
                        end
```

```
if (min_dis ~= 9999)
    plot([C(pmin).xd C(c1).xd],[C(pmin).yd
C(c1).yd],'g');
    C(c1).Next=pmin;
    if (qq==2)

packet_To_Bs(pmin)=packet_To_Bs(pmin)+packet_To_Bs(c1)/2;
    else

packet_To_Bs(pmin)=packet_To_Bs(pmin)+packet_To_Bs(c1)/10;
    end
    flag=0;
elseif (qq==2)
    flag=0;
end
        end
    end
end
for cc=1:cluster
    if (C(cc).Next == 0)
        plot([C(cc).xd sink.xd],[C(cc).yd sink.yd],'g');
    end
end
%% Calculate the residual energy of cluster head
for c=1:cluster
    CEr1=ERX*CM*(packet_To_Bs(c)-1);% Cluster members to
receive information about energy consumption
CEr2=ERX*DM*(packet_To_Bs(c)-1);% Cluster members received information on
```

```
energy consumption data                    CEt1=ETX*CM+Efs*CM*R*R;% cluster
head broadcast energy clusters                       if (C(c).Next ＝ 0)
CEt2=(ETX+EDA)*DM*packet_To_Bs(c)+Efs*DM*cc*packet_To_Bs(c)*dd^2;    %
Decline of free space
                    else

CEt2=(ETX+EDA)*DM*packet_To_Bs(c)+Efs*DM*cc*packet_To_Bs(c)*dd^2;    %
Decline of free space
                    end
                    S(C(c).id).E=S(C(c).id).E-CEr1-CEr2-CEt1-CEt2;%此
E_CH(r) = E_CH(r) +(CEr1+CEr2+CEt1+CEt2)/MC;
                end
                for i=1:N
                    if (S(i).type=='N' && S(i).E>0 )
                        E_left(r) = E_left(r) + S(i).E/MC;
                    end
                end
            end
            R_total = R_total + r/MC;
            R_first = R_first + first_dead/MC;
    end

    save RcLeach Dead CH_Num R_total R_first E_left E_CH
```

2.PSO-LEACH

```
%% Cluster head selection algorithm - PSO -Leach
clear all
```

```
close all
clc
%% simulation parameters
%xm=100;%x axis range
%ym=100;%y axis range
% because of the larger values of do, modify the range
Xm=200;%x axis range
Ym=200;%y axis range
% sink.xd = 0.5 * xm;% base x-axis
% sink.yd = 0.5 * ym;% y-axis base
% Stations are generally on regional boundaries, located on the corner
sink.xd = 0;% base x-axis
sink.yd = 0;% y-axis base
N = 200;% number of sensors
p = 0.1;% expected percentage of cluster head
cc = 0.6;% fusion rate
rmax = 1000;% of total number of rounds
CM = 32;% the size of the control information
DM = 4000;% data size
E0=0.05; % The initial energy of single node
ETX=50*0.000000001; % Transport energy consumption（J/bit）
ETX=50*0.000000001;% transmission energy consumption (J/bit)
ERX=50*0.000000001; % Acceptable energy consumption（J/bit）
ERX=50*0.000000001;% acceptance of energy consumption (J/bit)
Efs=10*10^(-12); % free space’s Channel model（J/bit/M）
Efs=10*10^ (-12);% free space (free space) channel model (J/bit/ meters square)
Emp=0.0013*10^(-12); %    multipath fading’s Channel model（J/bit/米的4次方）
Emp=0.0013*10^ (-12);% multipath attenuation (multipath fading) channel model
```

(4 J/bit/ m)

```
EDA=5*10^(-12); % Data fusion energy consumption（J/bit）
EDA=5*10^ (-12); energy consumption data fusion (J/bit)
do=sqrt(Efs/Emp); %Efs和Emp’ Boundary threshold，值越为84
Do=sqrt (Efs/Emp); demarcation threshold%Efs and Emp, value is 84
%% scene initialization
figure(1)
for i=1:N
    S(i).xd=rand(1,1)*xm;
    S(i).yd=rand(1,1)*ym;
    S(i).G=0;
    S(i).E=E0;
    S(i).type='N';
    plot(S(i).xd,S(i).yd,'o');
    hold on;
end
plot(sink.xd,sink.yd,'x');
%% Each round of iteration
flag_first_dead=0;% The first sign of the variable node death
Cid=zeros(2/p,rmax);
Cnum=zeros(2/p,rmax);
for r=1:rmax
    hold off;    % Round picture redrawn      disp(r)
    figure(1);
plot(sink.xd,sink.yd,'x');%
    hold on;
    dead=0;        %
    %% Death statistics node
```

```
for i=1:N
    if(S(i).E<=0)     %
        S(i).type='D';
        plot(S(i).xd,S(i).yd,'r.');
dead=dead+1; % Cumulative  mortality  nodes
if(dead==1)    %
            if(flag_first_dead==0)
                first_dead=r;    %
                flag_first_dead=1;
            end
        end
    else
         S(i).type='N';
         plot(S(i).xd,S(i).yd,'o');
    end
end


Dead(r)=dead;              %
if(dead ==  N)             % All died out of the loop node
    break;
end
%%select head of cluster
%f the number of rounds is precisely an integer multiple of a cycle, is set
S1(i).G=0
if(mod(r-1, round(1/p) )==0)
    for i=1:N
        S(i).G=0;
    end
```

```
            end
            [C,S]=GroupHead(S,N,dead,sink,p,r);
            num_cluster=length(C);    %
            CH_Num(r)=length(C);        %
            %% Assigned to each cluster head node and compute the energy
consumption of cluster members
            for i=1:N
                if (S(i).type ~= 'D')
                    if num_cluster >0
                        min_dis=distance(S(i),sink);
                        min_dis_cluster=0;
                        for c=1:num_cluster
                            temp=distance(S(i),C(c));
                            if(temp<min_dis)
                                min_dis=temp;
                                min_dis_cluster=c;
                            end
                        end
                        if (min_dis_cluster>0)
                            C(min_dis_cluster).ptb=C(min_dis_cluster).ptb+1;          %
This node to join the cluster head plus a number of packets
Er1=ERX*CM*(num_cluster+1);                    % This cluster head node receives
control information of each energy                              else
                            min_dis=distance(S(i),sink);
                            Er1=0;
                        end
                    else
                        min_dis=distance(S(i),sink);
```

```
                Er1=0;
            end
            % This node sends a join message and transmit energy
consumption data
            if (min_dis>do)
                Et1=ETX*(CM+DM)+Emp*(CM+DM)*min_dis^4;    %
            else
                Et1=ETX*(CM+DM)+Efs*(CM+DM)*min_dis^2;    %
Multipath fading
            end
            S(i).E=S(i).E-Er1-Et1;                                %
Residual energy
        end
    end
    %% Cluster head routing decisions made for each cluster head to the base
station of the information required for the path
    C=HeadRoute(C,sink);
    %% Computing cluster heads energy consumption
    for c=1:num_cluster

CEr1=ERX*CM*(C(c).ptb-1);                                          %
Cluster members to receive information about energy consumption

CEr2=ERX*DM*(C(c).ptb-1);                                          %
Cluster members received information on energy consumption data
        if (N-dead<=num_cluster)
            CEt1=0;
        else
```

```
CEt1=ETX*CM+Efs*CM*(sqrt(xm*ym))*(sqrt(xm*ym));                    %
Information broadcast cluster head energy clusters
            end
            % headof cluster sent to the base station after fusion energy
            if (min_dis>do)

CEt2=(ETX+EDA)*DM*C(c).ptb+Emp*DM*cc*C(c).ptb*C(c).distance^4;     %
Multipath fading
            else

CEt2=(ETX+EDA)*DM*C(c).ptb+Efs*DM*cc*C(c).ptb*C(c).distance^2;     %
Decline of free space
            end

S(C(c).id).E=S(C(c).id).E-CEr1-CEr2-CEt1-CEt2;                   % After this
round of the node residual energy
            Cid(c,r)=C(c).id;
            Cnum(c,r)=C(c).ptb;
        end
    end
```