Adaptive Routing Protocol for Reliable Sensor Network Applications

Jiann-Liang Chen[1], Yu-Ming Hsu[2] and I-Cheng Chang[2]

[1]Department of Electrical Engineering, National Taiwan University of Science & Technology, Taipei, Taiwan.

[2]Department of Computer Science & Information Engineering, National Dong Hwa University, Hualien, Taiwan.

Corresponding Author: Jiann-Liang Chen *Lchen@mail.ntust.edu.tw*

Abstract- The existing routing protocol for sensor networking can be divided into proactive routing protocol, reactive routing protocol and hybrid routing protocol. Each routing protocol has its merits and shortcomings. The lifetime will end when the working routing protocol can no longer support the whole wireless sensor network. An adaptive method based on redundancy node and dual routing protocol was proposed in the study. Redundancy node, when wireless sensor network is being deployed, can divide the wireless sensor network into operating and sleeping modes, and can use the different routing protocol. Dual routing protocol individually designs two kinds of different routing protocols in the sensor node, using the merits of these two different kinds of routing protocols to accomplish the mission of sending the data. The scenario set up is when the wireless sensor network has been used for a long time; the power kept in these sensor nodes is different. It is possible that some sensor nodes contain lower power because the heavy load of work, and some with more power because of less work load. After we send a query to the source node and unfortunately find out there is more than one wireless sensor in the routing path, and if there is power shortage, we can only query a message to send the sink to the source node. At the meantime, the source node will judge the storing condition of the power in all the sensor nodes when sending the query from the sink to the source node. Then the target wireless sensor will send a broadcast to all the neighbors. If there is a sleeping node in the neighbor and run a second kind of routing protocol, the sleeping wireless sensor will wake up. The woken sensor node will build up a path to ensure the data get sent from the source to the sink. Simulation results showed that the proposed mechanism is about 44% of packet delivery ratio can be increased compared to existing proactive/reactive routing protocol.

Keywords: Wireless sensor network, proactive routing protocol, reactive routing protocol, network lifetime

1. Introduction

Wireless sensor networks consist of a large-number of sensor nodes. A Senor node is composed of transceiver, processing unit, sensing unit, mobilizer, location finding system and power unit. In recent years, advance in micro-electro-mechanical-system (MEMS) and nano technologies [1,2]. Let us can make low-cost and low-power of sensor nodes. It has sensing, communication and processing information of the ability. The Sensor networks collection information depends on the original design routing protocol and return to the sink, as ***Figure 1***. Sensor networks have a lot of applications. For examples, it can be used in home protection, against natural disaster and so on.

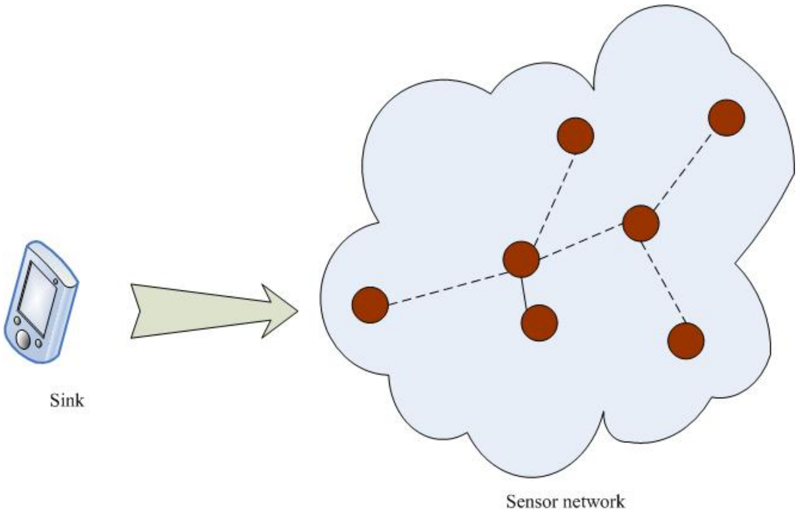


Figure 1: Architecture of Wireless Sensor Network

Sensor networks collect the environmental information by a huge-number of distributed sensor nodes and wireless communication each other. Because of the sensor node is small, the number of nodes may be form hundreds or thousands and transmission range from few meter to the few kilometer. Consequently, the sensor networks management is a very important problem and relation factor is divided, as follows:

Self Organization The self organization of wireless network doesn't need additional network device to help them [3]. These nodes through protocol stack and distribute algorithm to coordinate themselves. Once the nodes booting, they can autonomous to form a network rapidly.

Classification The sensor networks are divided into threes classifications: micro-sensor networks, interior sensor networks and outside sensor networks. The micro-sensor networks can be used in monitor temperature of the human body. The interior sensor networks may be application, such as sensing bridges or building to understand status. The outside sensor networks can be application on wilderness or forest and dangerous region. Depending on situation, the design fit of the sensor networks.

Scalability Sensor network has large scalable, the number from hundreds to several thousands. Depending on the application increase the number of the sensor nodes and they will not affect the performance. It is big challenge for the routing protocol.

Management The sensor nodes is large, so that they need integrate and analyze the data if they responsible for the same of the task by group such as monitor the enemy in the battlefield or trace the animal movement in forest. When the object moves that the group of the sensor nodes will change, and the trace the multi-object is also an interesting issues for management and traffic overhead.

Security It is fundamental design that traditional networks avoided for eavesdropping, injection, and modification of packets or modification routing protocol, and the sensor networks design also should have the capability. It is very important for built a security protection outside of sensor networks communication [4]. But the sensor nodes energy has limited, the key establishment need easy and scale as a guideline. It thus appears that the level of security protection with key establishment according to cost and application.

Fault tolerance Fault tolerance is a major issue in any networks. Because of sensor nodes is large, prevent not expect sensor nodes fault or networks interference. It should not affect the whole of sensor networks.

The large of number of sensor nodes are deployed in a fixed geography area, no external power supply and cannot charge therefore only usage embedded battery, the sensor node is small. They collection information and communication with neighbor or sink use radio. Thus, the power management for sensor networks becomes very important. Since sensor networks design of every component must be consider integrated power management from the base design of sensor node hardware with select of component, routing protocol, and group management and so on, and relation the lifetime of sensor networks. The design of routing protocol must adaptation the scale feature of sensor networks and will not reduce performance.

According to relate research that the dropped energy resource in communication. First, when the sensor nodes deployment densely, it will be collision that nodes collect information need to transmission to the other node. It occurs that the all of node are transferring or multiple nodes are delivering to same node. When the data collision occurs, it will be to repeat data transfer and waste energy. Secondly, the nodes are transmitting packet and the neighbor also received. It will be to waste power because the neighbors of eavesdrop. Thirdly, the sensor network random deployment, sink to node is multi-path routing, and then according to reliability and QoS and power will select a routing path. Selecting the different routing contain different energy waste. Beside, a sensor node has three statuses, it is divided into transmitted, receive and idle. No matter in any status it still power consumption. As shown in ***Figure 2***.

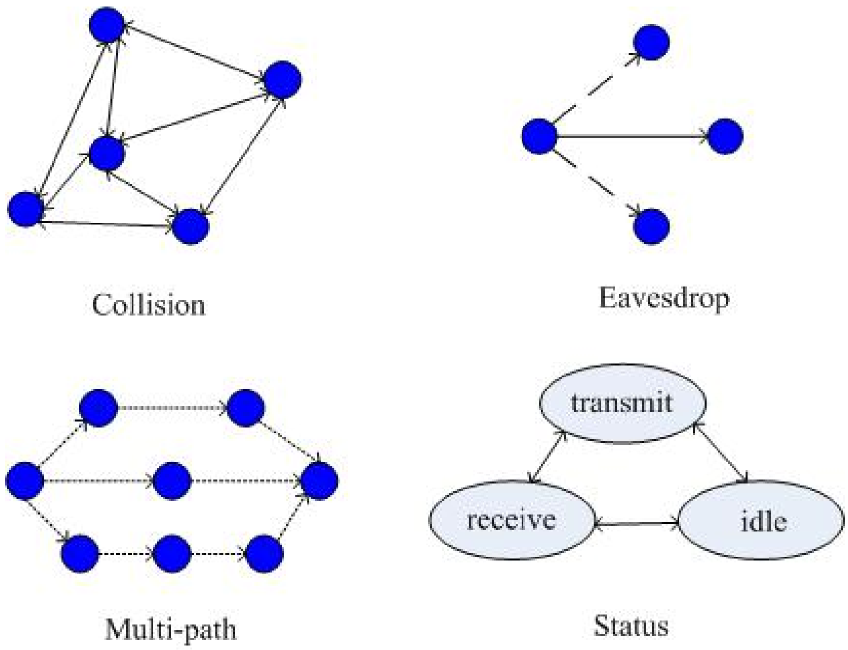


Figure 2: Four Cases of Power Waste and Consumption

In order to extend sensor networks lifetime by decrease power consumption, not only consider the design of routing protocols. For examples, let sensor networks periodically wake-up and sleep with decrease power waste. If no any scheme, energy consumption soon. With the MAC layer technology [5-10] cut down collision problem such as FDMA (Frequency Division Multiple Access) [9], each nodes have two bandwidth which of one is transmit and the other is receive that avert. With TDMA [5-8] time-slot management avoid data collision and decrease energy consumption. The design of dynamic power management with the sensor networks clock or suspend some of task decrease wastes.

Power management for sensor networks is very important problem. If the sensor networks want to extend life, then may be try recharge power supply by itself for future besides use battery of limited energy. Recently years in MEMS (Micro-Electro-Mechanical Systems) development is fast. For the MEMS in power generator and transducer technology can recharge with itself by the environment heat energy or solar power energy. A lot of researchers focus on the issues. However, both power management and refresh the power technology is important. In the paper, we don’t discuss the issues.

Recently in wireless communication technology of progress has embedded inside of sensor node, used wireless communication with each other. Because of a lot of sensor node have hundreds or thousands of nodes and much more. It need a routing protocol with management sensor networks, then sense information may be accuracy transmit information.

The wireless communication technology contains two classes:

Infrastructure networks Infrastructure networks are the base station management group of node. The sensor nodes communicate with the neighbors of node by base station.

Ad-hoc networks The sensor nodes can be communication each other without via base station, and the sensor networks application may be one of method or combine two kinds of methods. For example, LEACH [5] in categorization of the sensor nodes into many cluster, and accord to algorithm select one of cluster head of them. The cluster head will be management and process of the nodes of cluster, then communication between node and sink. The cluster head is like a base station.

Consider the design of power management and routing protocol of the sensor networks is important. In the situation, the most less of power consumption, the sensor networks can complete the work and extend life of the sensor networks. The classification of the Sensor networks transmit is divided into flooding, unicast and multicast [11]. Flooding is rebroadcast the packet, when the sink send data to the sensor nodes, that packet received by all of the node neighbors. Each sensor node will rebroadcast the packet, at least the packet received in the whole sensor networks. The method is simple, and the cost is expensive for the power wastes. For unicast according to the design of the routing protocol, the data transmit from a single node to the next node, and the data will be delivered accuracy to the object node. This way is less energy than flooding, design is more complex. In multicast, it can group the sensor nodes into several clusters and each cluster contains a cluster head of cluster. The sink transmits information to one of the cluster heads, and sends information to the sensor by the cluster head.

As the sensor node is limited in both energy and resource. To decrease power wastes is the design guideline of routing protocol. Filtercast solve flooding problem, for data repeat broadcast problem, suggest a method. Filtercast set a threshold for the sensor node received packet, when exceed the number of times to no longer receive. With this method decrease power consumption, to avoid flooding caused the sensor networks traffic load and energy wastes. The LEACH design can decrease power, with the average consumption of the sensor networks extend the networks life. Besides, the sleep and wake up scheme application in the sensor networks. The scheme can less power consumption by sleep and wake up periodically. Altogether, exports the sensor networks life is optimal.

We improved the routing protocol in the past or design of the new routing protocols. However, the major design guidelines based on decrease power consumption. When initiation a sensor networks, one of the routing protocol is to begin until it can't work. This indicates that the sensor networks have already died. But it has a problem, for the original of routing protocol is not suitable in sensor networks, or it reaches to expect the life. But it is just to can't support the sensor networks again, can't indicate all of sensor nodes have already died. Thus, this paper treats the issues, when the original of routing protocol through long-time activity, to each sensor nodes save power will be different. But the original of routing protocol was not suitable in sensor networks. At last the sensor networks died. Therefore, it will change routing protocols to try adapting to the new conditions. The new routing protocol can extend the sensor networks life by change the old routing protocol.

The rest of this paper is organized as follows. In the first part of this paper, we introduce the concept about wireless sensor networks and our motivation. The next section reviews the background knowledge of the routing protocol, management for Wireless Sensor Networks, and related work. Section 3 describes the proposed method. Section 4 elucidates the simulation environment and analyzes the results, and Section 5 summarizes and draws conclusion.

2. Background Knowledge and Related Work

Before bringing up our method, in this section we will briefly introduce the relative knowledge of wireless sensor networks. The background knowledge of wireless sensor network is very important. We extend our concept of design through the illustration of the basic knowledge.

2.1 Sensor Network Architecture

The architecture of sensor network management could be divided into two parts. One is Hierarchical Network Architecture and the other is Flat Network Architecture [12,13].

The original design of Hierarchical Network Architecture is to separate the sensor network into several clusters, and each cluster has its cluster-head to take charge of the sensor node to which it belongs (as shown in ***Figure 2.1***). Besides managing the node from the bottom layer, cluster-head obtains the ability of data aggregation and data fusion. Furthermore, sink could query information by using the cluster-head layer. While applying the management of cluster-head layer, we deal with the information collected from the layer and return it to the sink. With the use of hierarchical network architecture, we can affectively manage a large of the sensor node, as well as to economize the consumption of power. However the routing protocol with this kind of design is more complex. Several researches of hierarchical network architecture have already taken place and many related articles have been published.

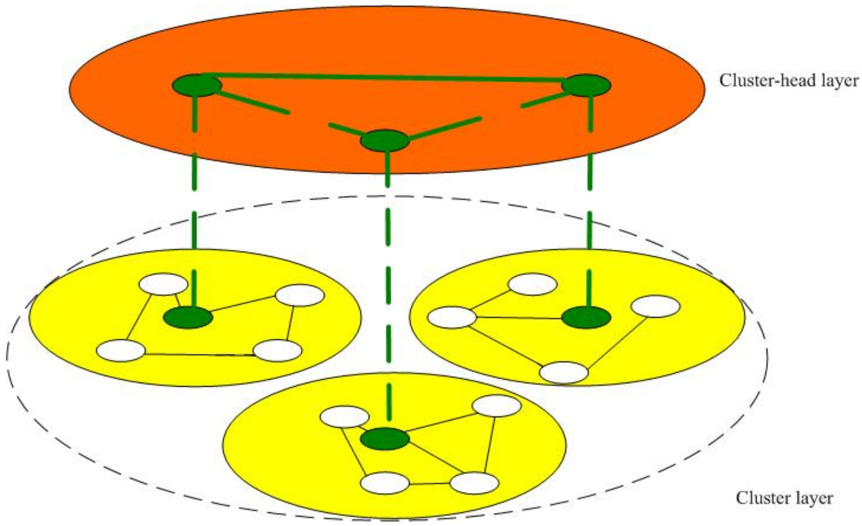


Figure 2.1 Hierarchical Network Architecture

Flat Network Architecture is a peer-to-peer technique (as shown in ***Figur***e ***2.2***). Each node is on the same level and can communicate with each other directly. So it is not necessary to reach the purpose of communication with the help of cluster. If the target is far way, the system adapts the way of multi-hop.

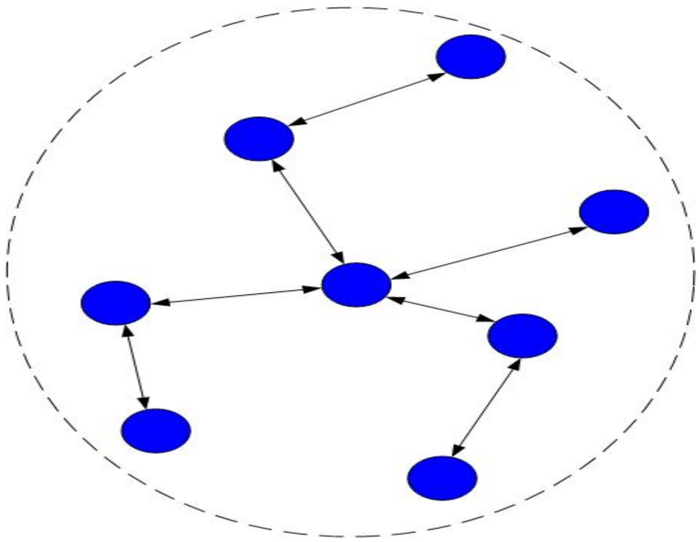


Figure ***2.2*** Flat Network Architecture

2.2 Routing Protocol

The wireless routing protocol can be divided into three types, and they are proactive routing protocol, reactive routing protocol, and hybrid routing protocol [14]. Proactive routing protocol (also named Table-driven), by means of broadcast, updates the routing table in an extinctive circumstance. Different proactive routing protocols take different methods to update the routing table, but they update the time and base themselves on the routing table. Reactive routing protocols (that is on-demand or demand-driven) establish a routing path when there is a necessity. Reactive routing protocols are quite suitable in the usage of mobile wireless sensor node. Hybrid routing protocols are the routing protocols integrated with the merits of proactive routing protocols and reactive routing protocols. The paper brings out new ideas on the basis of proactive routing protocols and reactive routing protocols. Therefore, the following is the description of each distinctive routing protocol on the three types of routing protocols.

2.2.1 Proactive Routing Protocol

The most convincible theory of proactive routing protocols was brought up by Perkins—DSDV (Dynamic Destination-Sequence Distance-Vector Routing Protocol) [14,15]. This is a table-driven routing protocol. The memory of every sensor node has a forwarding table and an advertise one. Forwarding table is a routing table, which contains destination-node field, next node field, hop-number field, sequence-number field and time-adjustment field. The value of sequence-number will multiply and its main function is to indicate the new and old condition. Thus the value stored in sensor is always the largest, which ensures the routing path is the newest. Advertised table sustains the records of links. As long as the status changes, the documents inside advertised table will vary. Different proactive routing protocols have different methods to update the routing table. However the mutual feature is that it maintains the routing table in a specified time. In ***Figure 2.3***, the wireless sensor network is composed of seven nodes; each maintains a forward table and an advertised table. Let's take node 3 for example; the forwarding table and advertised table maintained are illustrated in ***Table 2.1*** and ***Table 2.2***.

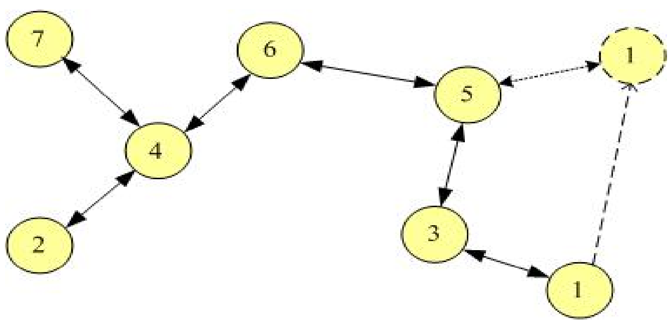


Figure 2.3 DSDV Routing Protocol

Table 2.1 Forwarding Table

Destination	Next	Hop	Sequence	Time
1	3	1	ID50-1	T01-3
2	5	4	ID36-2	T01-3
3	3	0	ID28-3	T01-3
4	5	3	ID46-4	T01-3
5	5	1	ID15-5	T01-3
6	5	2	ID70-6	T01-3
7	5	4	ID62-7	T02-3

Table 2.2 Advertised Table

Destination	Hop	Sequence
1	1	ID50-1
2	4	ID36-2
3	0	ID28-3
4	3	ID46-4
5	1	ID15-5
6	2	ID70-6
7	4	ID62-7

The chance for outing table update is when the node moves. For instance, node 1 is originally right next to node 3; however, if the circumstances call for it, it will move around node 5. Now, the routing table of every node has to update the relevant information. Take node 3 in account, the routing table updates the red area of ***Table 2.3*** and ***Table 2.4***. We change the next of destination node 1 from 3 to 5; hop number from 1 to 2, sequence number and time are thereby updated. The content of forwarding routing table has been modified and the advertised table is simultaneously updated.

Table 2.3 Forwarding Table

Destination	Next	Hop	Sequence	Time
1	5	2	ID75-1	T07-3
2	5	4	ID36-2	T01-3
3	3	0	ID28-3	T01-3
4	5	3	ID46-4	T01-3
5	5	1	ID15-5	T01-3
6	5	2	ID70-6	T01-3

7	5	4	ID62-7	T02-3

Table 2.4 Advertised Table

Destination	Hop	Sequence
1	2	ID75-1
2	4	ID36-2
3	0	ID28-3
4	3	ID46-4
5	1	ID15-5
6	2	ID70-6
7	4	ID62-7

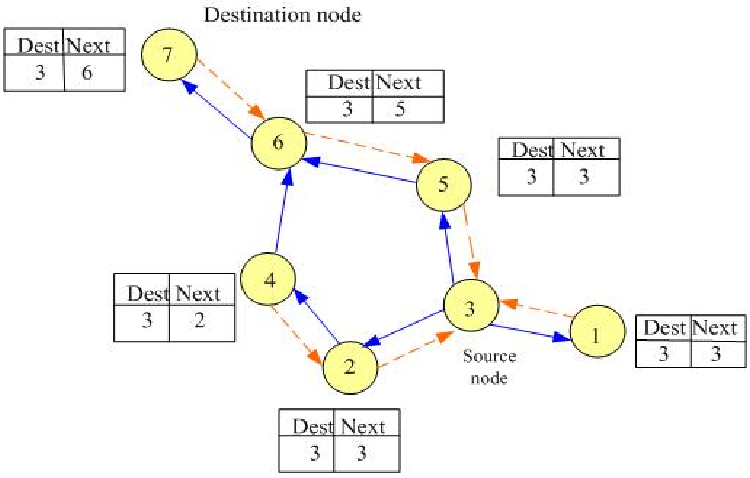
The merit of proactive routing protocol is when the sensor node forwards the data to the destination node, the data can be sent to the destination node according to the routing table restored in each node. This way, we can minimize the delayed time when sending the data, and elevate the stability when sending the information in a wireless environment.

2.2.2 Reactive Routing Protocol

The routing path will establish only when it is necessary. This is the main feature of reactive routing protocols (that is on-demand routing protocol or demand-driven). DSR (Dynamic Source Routing) by Johnson and Maltz, as well as AODV (Ad Hoc On-demand Distance Vector Routing) [16,17] are two convincible reactive routing protocols. And here we take AODV as an illustration.

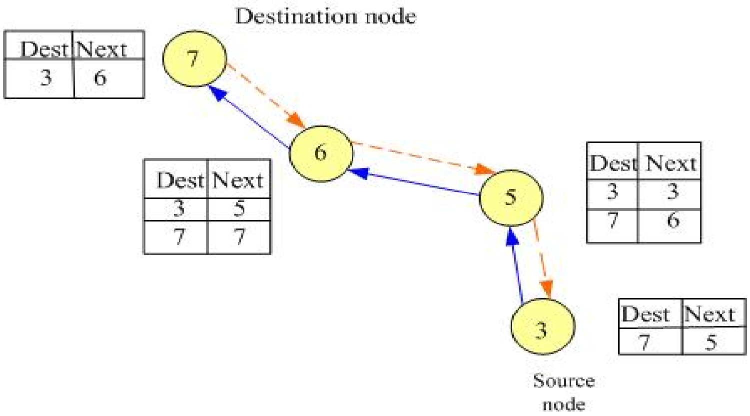
The main design of AODV (Ad Hoc On-demand Distance Vector Routing) focuses on the dynamic network topology, establishing and maintaining the routing path in need. AODV distinguishes the two methods-unicast and multicast. We illustrate the part of unicast here. There are three procedures in the unicast, which includes the route request, route reply, and the route maintain.

Route Request The route discovery of AODV varies in two sessions—route request and route reply. As there is a packet in the source node to be sent to the destination node, the source node will first check if its own routing table forwards to the next node in the destination node. If there is any valid record in the routing table, the source node starts the process of route request right away. Source node broadcasts the control packet of RREQ (Route Request) by flooding; the packet contains source node IP, destination node, destination node IP and broadcast ID. Broadcast ID is an increased series number maintained within each node. After each node broadcasts a RREQ, it adds one to broadcast ID. So the combination of broadcast ID and source node IP can make sure the node that receives RREQ to only identify the RREQs sent at the same time. Prevent the repetitive procedure to the same line of RREQs. As the source node finishes delivering RREQ, we set the timer to wait for the RREP (Route Reply.) One important mission to send RREQ is to establish the reverse route, to make the RREP return the source node in alliance with the reverse route. The sending procedure of RREQ, node 3 for example, is shown in ***Figur**e **2.4***.



Figur**e **2.4 Propagation of RREQ through Network

Route Reply During the sending process, if any of the routing table within the node reaches the information of the destination, then this node can be used to respond to RREP in accordance with the reverse route, to wait until RREQ arrives at the destination node, the destination node responds to RREP in person. RREP sends the files by the way of unicast. During the process it will establish the forward route. The purpose of forward route is to let the source send the packet. The sending of RREQ is illustrated in ***Figur**e **2.5***.



Figur**e **2.5 Response of RREP

Routing path maintain The routing path maintain can be divided into two kinds—routing table maintain and routing path broken. The maintenance of routing table refers to the fact when one routing path is not in use for a time period or it is updating, the path will be removed from the routing table of the node. There are two ways to handle the routing path crack. One is to directly send RERR (Route Error) back to the source node. The node RERR passes will delete the relevant information in sequence. After RERR returns to the source node, the source node reestablishes one routing path to the destination node. The second kind is the local repair. It is when the broken node gets near the destination node, and the broken node directly sends RREQ to search for the destination node. If this RREQ can reach the destination node, then RREP can maintain the broken link.

The main feature of reactive routing protocols is to establish routing path when there is a need to send the information. Reactive routing protocols can be divided into two usages. First, when performing routing discover, routing information will be sent along with the control packet. Then it saves the routing path information in the routing table of the sensor node at last. This is called the source routing. Second, the routing information is contained in each node, and every node only records the next node that that gets to be sent. This way is called the distance vector. Anyhow, the feature of reactive routing protocols is that it is not necessary to maintain the routing table of the node information in the network. This way we can diminish the extra power consumption caused by the communication. Especially for the mobile node, it is very important to efficiently use the power.

2.2.3 Hybrid Routing Protocol

The design of hybrid routing protocols is to combine the merits of proactive routing protocols and reactive routing protocols. Let’s take ZRP (Zone Routing Protocol) [18-20] brought by Hass and Peralman for example. In the cluster, every node adapts the proactive routing protocol to send the information. If it needs to send the information to the cluster out of range, we will deal with the situation with reactive routing protocol. Other related hrbrid routing protocols include DDR (Distributed Dynamic Routing algorithm) [21], and HCBM (Hierarchical Cellular-Based Management) [22].

2.3 Other Related Protocols

Within the design of the routing protocol, basically there are two kinds—proactive routing protocols and reactive routing protocols. There are still other routing protocols, the routing protocols that base on geographic information or base on mobility prediction. We design of the sensor network, the most practical concern is to evaluate and adjust to the local geographical environment. We can application the different types of routing protocols to the real-life different needs.

3. Proposed Mechanism

In the previous section, we have introduced the basic knowledge we need to know. We will put our idea into practice with this background knowledge. The mechanism we brought up is mainly realized by the two different types of applications—proactive and on-demand routing protocols. The section will be divided into three parts for illustration. First we mention a new concept. Second is the illustration of function. Third we discuss the merits of this method.

3.1 Backup Routing Path

In the wired network, in order to make sure the data gets sent in an accurate way from the source node to the destination node, we set several routing paths. It is to prevent when there is a malfunction in the main path, and that we could switch to the backup path manually or the system itself. By means of this kind of mechanism, we can ensure the fluency to forward the data. In a wireless environment, we can also use the routing protocol to find out the multi-path. If one of the routing paths has encountered obstacles, we can still use other paths to secure the fluency from the source to the destination. However, the above methods do not apply to the wireless sensor network. It is because the sensor node often relies on the battery itself while functioning individually. If the middle node in a certain path malfunctions, power shortage for example, then it means that the path is no longer in use. Generally speaking, we generate another routing path in the multi-path to make sure the communication between the sink and source node is working fine. But two more questions arrive.

Inconclusive After applying the sensor network for a long time, the power stored in all of the nodes might be different. It might occur when the routing path in use malfunctions and stops, switching to another path. However another routing path might have contained the malfunctioned node, which disables the communication between the sink to source node.

Select_backup_Node If the node which is forwarding the information finds out that the source node is not able to complete the forward function, certain routing protocol gives permission to find the nearby node in order to establish the routing path, by passing the broken node to maintain the fluency of the path. However, if the system is not able to find an appropriate node to forward the data, the data will not be able to send to the destination.

Our study can figure out the solutions of the above two problems. The idea is to apply

Redundancy node and **Dual routing protocol.** Redundancy node is used when we deployment the sensor network, it can be divided into two parts while using different routing protocols. One part is the routing protocol that the sensor network stations in the first place. The other part is the sleeping node, which will be wakening only when it is necessary. Dual routing protocol is the design that puts two different types of routing protocols in the sensor node of both parts. By adapting the merits of these two different types of routing protocols, we manage to accurately complete the mission of forwarding the data.

Our environment is set when the sensor network is applied for a long time, and the power within the sensor node is not equal. Possibly there are too many missions for some node while the power is rapidly consumed and the working load is low for other nodes while they contain higher power. If there is more than one node in the routing path of the source node that we query, it might be because the power runs short, and it could only afford to forward the query information from the sink to the source node. At the same time, the source node will depend on the situation according to the power stored in the nodes of this path while the system forwards the query information from the sink to the source node. If the estimation says that the destination node is unable to use the original routing path and send the information back to the sink, then the source node will broadcast a beacon-request packet to the nearby node. If within the nearby nodes, there is a sleeping node which runs the second type of routing protocol, then the sleeping node will be waken. The awaken sensor node will establish a routing path to make sure the source node forward back data to the sink.

Figure 3.1 and ***Figure 3.2*** indicate the station of both grid and random sensor networks. When the power of a node is below the threshold in the original routing path, and it is unable to return the data in the original path, then the source node will trigger the second type of network and return the data to the sink in safety.

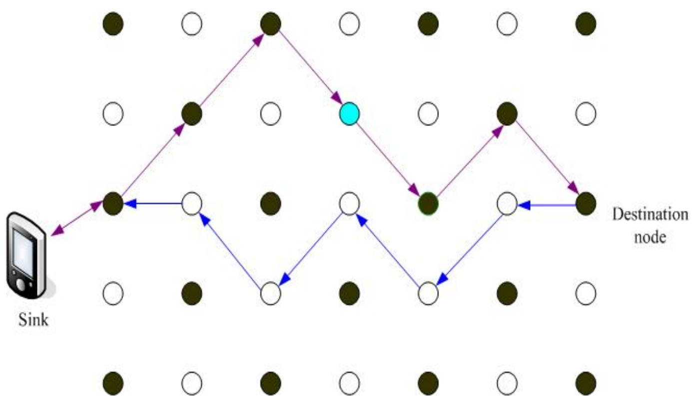


Figure 3.1 Grid Sensor Network

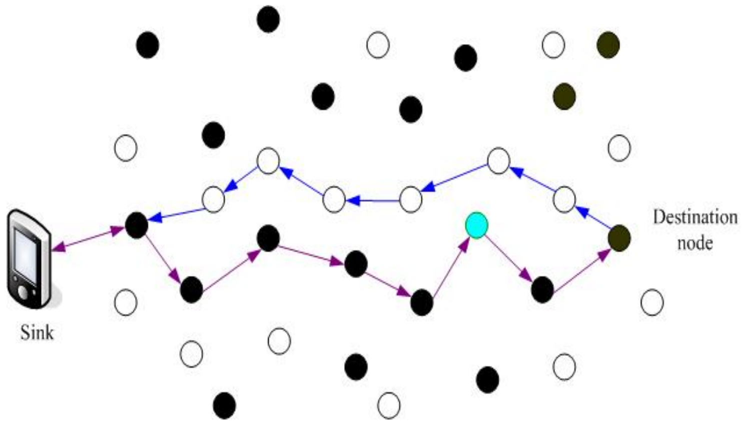


Figure 3.2 Random Sensor Network

3.2 Redundancy Node and Dual Routing Protocol

Redundancy node We can set some part of the node in the sensor network into the sleeping condition. Since it is in sleeping condition, the power is seldom consumed. Therefore these redundancy nodes could be seen as backup or emergency nodes. We then can apply these redundancy sensor nodes evenly distributed in the whole sensor network to establish a safe and reliable routing path, so that the source node can return the query information to the sink. It is necessary to establish the idea of redundancy node in the important stations in the sensor network. The main purpose is that the query delivered by the sink can make sure the data gathered by the source node return to the sink.

Dual routing protocol After we divide the sensor network into two groups, two different types of routing protocols are installed in the sensor network of these two groups. The sensor network of the first group will install the proactive routing protocol, for the merit of table-driven routing protocol is that as the sink sends data to the source node; the data is forwarded in a fast speed, with a fairly low delayed time. The second group installs the on-demand routing protocol. For the sensor node of the second group is in sleeping condition. Only when the request is received will it wake up and establish the routing path. The merit of demand-driven routing protocol will be in need, so the discovery routing exists. The feature corresponds with the role of the sensor node in the second group. With the combination of redundancy node and dual routing protocol, we can return the data back to the sink.

3.3 Source Node and Destination Node

More than one sensor node will be used to forward the query in the path from the sink to the source node. There are two very important nodes in this whole routing path. Both of them are source node and destination node.

Source node When the sink makes a query to the remote node, the sink will send out the source-request packet surrounding the sensor network from the beginning. The purpose is to find out if there is an appropriate sensor node to take as a sink (or so-called gateway). Node is responsible for the role of source node. Besides the fact that the ability of the node itself has to function properly, the most important is to have the highest power. In other words, the mission the sink sends out the source-request packet to the surrounding node is to find out the sensor node which contains the highest power, as it shows in ***Figure 3.3***, because the source node is in charge of the communication between the sink and the routing path. When the backup path is established, in order to make a routing discovery, we need to make the source node as our searching object. If the sink finds out the power shortage at the start, the establishment of the backup path will fail.

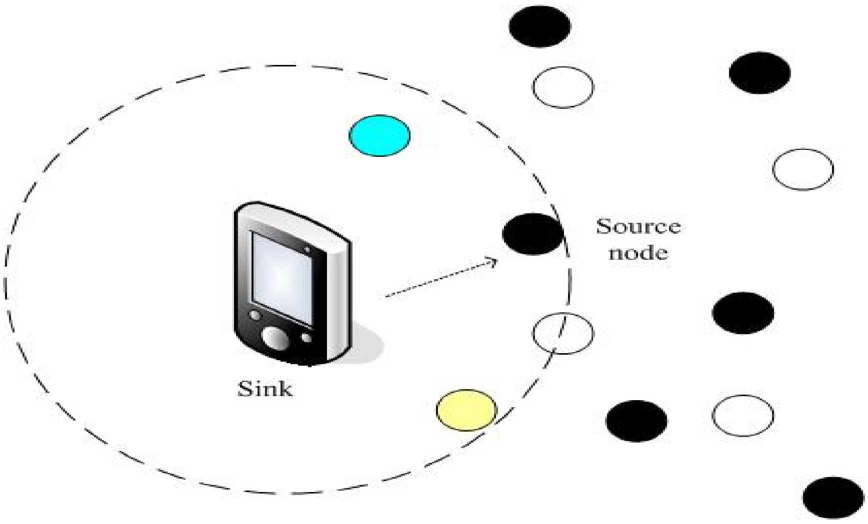


Figure 3.3 Sink Search for Source Node

Destination node There are two functions in the destination node. The first one is to apply the original path and return the gathered data. The second one is that the destination node will distinguish if the original path is applied to return the data according to the power data resembled in each node when the query-request packet passes. If it does not work, then the destination node will send out the beacon-request packet to the nearby node, wakening the node in the second group. If there are several nodes in the second group in the surrounding, then the destination node will find out the node closest to the original path according to the direction of the original path. It returns the data of the query back to the sink, as it shows in ***Figure 3.4***.

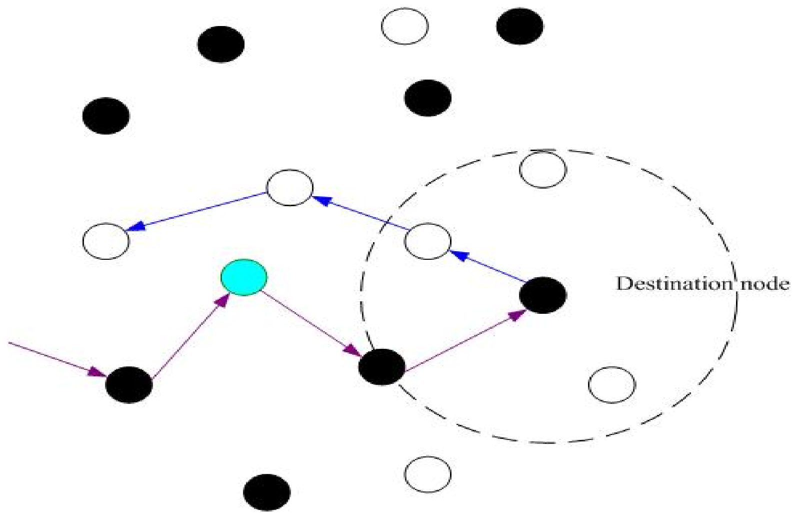


Figure 3.4 Destination Node Search for Backup Node

We take the source node and destination node as the basis and establish a safe and secured routing path. When the original path malfunctions, we can adapt different methods to establish a stable routing path. This way we can prevent the data from getting lost during the communication.

3.4 Advantages

Our idea of **Redundancy node** and **Dual routing protocol** is not something new or renewed routing protocol, but a new concept brought up especially for a specific application. Take the war or the fire protection for example. Under this kind of circumstance when every minute counts, we need a stable sensor network to offer accurate information to leave the user with the best to deal with the condition. The following is the four advantages of our method.

Reliability We set another sensor network as backup. When there is a need, the other sensor node is generated. With the application of these backup nodes, we are able to forward the reliable data.

Integrity The establishment of redundancy node can mend the shortcoming of mono-network design. For instance, for prevention, if the original routing path malfunctions, then there is an influence over the forwarding data.

Fault tolerance This method can be a precaution because when the routing path of the mono-routing protocol has a problem, we cannot make a query to the remote area.

Lifetime With the application of the sensor network that the two groups design, we can lengthen the life of the sensor network.

4. Simulation Analysis and Discussion

In this section, the simulation was performed based on NS2 (Network Simulator, version 2) network simulator. NS2 takes C++ and OTcl as to develop a simulated environment. The main of OTcl (Tool Command Language) is to edit the simulated network environment. NS2 will unscramble the written OTcl script and then come up with the simulation result. We will estimate the average latency of the redundancy node and dual routing protocol, the delivery radio and the life time. The differences between our method and the existed well-known DSDV will be compared.

4.1 Scenario

Of all the natural disasters, volcanoes have the most momentarily destruct power. Besides gushing a stream of lava hazardous to the lives and personal savings of surrounding neighborhood, a large scale of gas such as volcanic ashes, carbon dioxide, sulfur dioxide, H_2S can more likely affect the quality of air and visibility within a region, and further, do harm to our respiratory system. In addition, the oxysulfide bursting from the volcano will take form of acid rain, hindering the crops or plants from growing. To forecast a volcanic activity, the researchers need to gather massive statistic data; though the mission is quite dangerous and difficult to complete. Nonetheless, the statistic analysis can not only help forecast the future volcanic activities but also ease the danger brought by the volcanic eruptions. Therefore, we can adapt the qualities of sensor network to monitor the volcanic action in a long run. The network can gather information concerning the volcanic incline or inflation, the shifting magnetic field and temperature, the changing gas formation, and the constant earthquakes. We can deploy the sensor network at the crater and the surrounding area where the volcanic information can be inducted. We deploy our second backup sensor network in the important region to avoid the route path from breaking owing to the power shortage, and to elevate reliability and lifetime of the network.

4.2 Simulation Environment

In the simulation, the network consisted of 50,200 sensor nodes in a 1500(m)*500(m) rectangle. These nodes with radio coverage of 250 meters were grid placed in the sensor field. The size of each packet size was 64 bytes and the traffic type was CBR (Constant Bit Rate). Sources generated one data packet per second and simulation time lasted for 300 seconds. The distributed coordination function (DCF) of the IEEE 802.11 standard was used as the Medium Access Control (MAC) layer protocol for wireless sensor networks.

4.3 Average Latency

The average latency is the average delay time of a packet between transmission from the sink and receipt at the destination. ***Figure 4.1*** indicates, with 50 nodes, there is a difference of average latency between two kinds of routing protocols. Within the single protocol, the average latency of DSDV is about 0.12 seconds. When (DSDV+AODV) routing protocol is run, after 100 seconds, it occurs when the data can not return to the path of the DSDV routing protocol, so AODV and the second set of nodes are enabled. It takes AODV a very long time to look for the path; in consequence, the average latency of AODV will be much higher than that of DSDV. Its average latency can reach as high as 0.56 seconds, and then drop about 0.15-0.17 seconds. ***Figure 4.2*** shows our comparison of the average latency of both routing protocols when the nodes go up to 200. With 200 nodes, the average latency of DSDV routing protocol is about 0.47 seconds. When (DSDV+AODV) routing protocol can not return the data, its average latency is at the highest 2 seconds or so, and then drops gradually down to 0.6 seconds. Only when the highest delay time is 2 seconds may we accept the result.

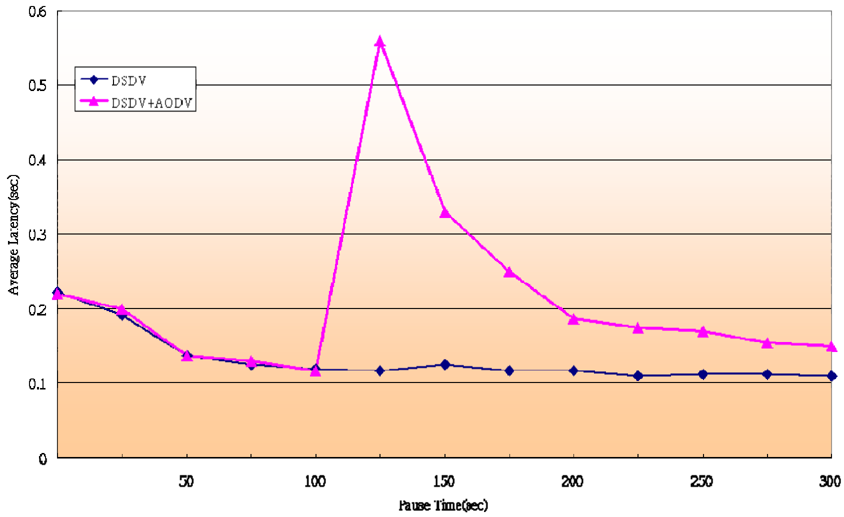


Figure 4.1 Average Latency with 50 Nodes

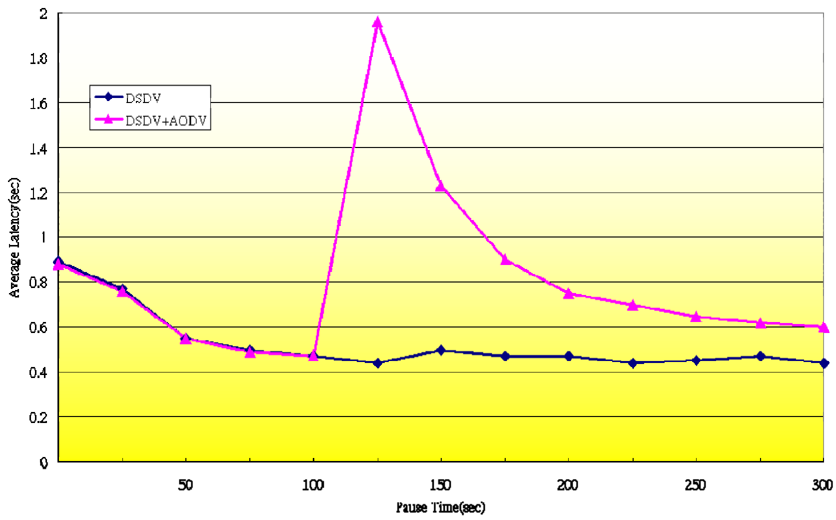


Figure 4.2 Average Latency with 200 Nodes

4.4 Packet Delivery Ratio

The packet delivery ration represents the rate between numbers of data packets received by the destination and the number sent by the source. We compare DSDV and (DSDV+AODV) individually according to the pause time. (Illustrated in ***Figure 4.3***) As the DSDV routing protocol is used alone, its packet delivery ratio is quite stable, approximately between 0.8~0.82. Prior to 100 seconds, since there is no broken of the path running (DSDV+AODV); therefore, we run the DSDV routing protocol. However after 100 seconds, there is a routing path broken; consequently, AODV routing protocol and the second set of node have been started. Now that AODV is a reactive routing protocol, it will be looking for the path when there is a need. Thus, after 100 seconds, the packet delivery ratio has gone down to 0.55. Nonetheless, after 200 seconds, the delivery ratio is raised up to around 0.9.

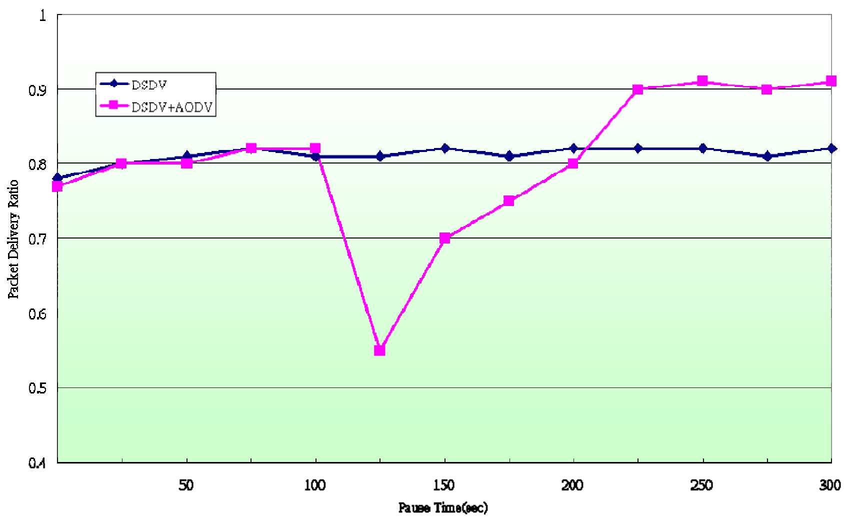


Figure 4.3 Packet Delivery Ratios with 200 Nodes

4.5 System Lifetime

Lifetime is how long the sensor networks last. Of course there are merits and shortcomings of the existing routing protocols, and the mechanism we bring up combines the merits of the proactive routing protocol and the reactive routing protocol. ***Figure 4.4*** illustrates the DSDV routing protocol after 100 seconds. The power of the route path is insufficient, so the data can not be returned, thus, the packet delivery ratio is down to 0. After we run (DSDV+AODV) for 100 seconds, AODV will be looking for another set of sensor node. Right then the packet delivery ratio will be the lowest around 0.55. After AODV routing protocol establishes the route path, the packet delivery ratio is about 0.9. Our mechanism can continually having a query with the destination area.

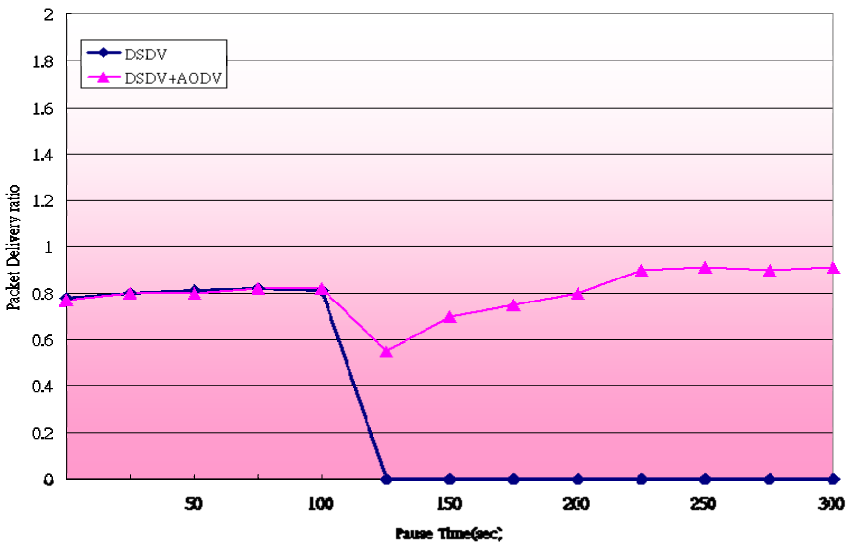


Figure 4.4 Packet Deliver Ratio with Lifetime

5. Conclusion

This method applies the technique of the redundancy node and the dual routing protocol. Redundancy node means when sensor network is deployed, we can divide the sensor network into two parts, and adapt different routing protocol. One part is the routing protocol functioning as soon as the sensor network is deployed. The other part the sleeping node, only when there is a need will the sleeping nodes be awake. In this case, we get to avoid the power shortage of the node when the sink gives out a query. We can make sure the data sent from the sink query can be returned by using the node of the second group. As the result of simulation suggests, the lifetime of our method is longer than that of sensor network routing protocol. Most importantly, this method can ensure the return of such important data. Our method has been proved feasible through the simulation. We will test the method by implementing it under the real-life sensor network in the near future, to understand the problems we will face.

6. Acknowledgement

This paper is a partial result of project no. NSC95-2218-E-259-001 and NSC95-2219-E-259-003 conducted by National Dong Hwa University under the sponsorship of the National Science Council, ROC.

References

[1] I.F. Akyildiz, W.Su, Y. Sankarasubramaniam and E. Cayirci, “Wireless Sensor Networks: a Survey,” *Computer Networks*, Vol.38, No.4, pp.393–422, 2002.

[2] I.F. Akyildiz, W.Su, Y. Sankarasubramaniam and E. Cayirci, “A Survey on Sensor Network,” *IEEE Communications Magazine*, Vol.40, pp.102-114, August 2002.

[3] M. Kochhal, L. Schwiebert and S. Gupta, “Role-base Hierarchical Self Organization for Wireless Ad hoc Sensor networks,” *Proceedings of the 2nd ACM International Conference on Wireless Sensor networks and Applications*, pp. 98-107, September 2003.

[4] A. Perrig, J. Stankovic and D. Wagner, “Security in Wireless Sensor Networks”, *Communications of the ACM on Wireless sensor networks SPECIAL ISSUE*,” Vol.47, pp.53–57, June 2004.

[5] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, “Energy-Efficient Communication Protocol for Wireless Microsensor Networks,” *Proceedings of the Hawaii International Conference on Systems Science*, Vol.2, pp.1-10, January 2000.

[6] D. Estrin, L. Girod, G. Pottie and M. Srivastava, “Instrumenting the World with Wireless Sensor Networks,” *Proceedings of IEEE International Conference*, Vol.4, pp.2033-2036, 2001.

[7] K. Sohrabi, J. Gao, V. Ailawadhi and G. J. Pottie, “Protocols for Self-organization of A Wireless Sensor Network,” *IEEE Personal Communications*, Vol.7, pp.16-27, October 2000.

[8] K. Sohrabi, G. Pottie, “Performance of a Novel Self-organization Protocol for Wireless Ad-hoc Sensor Networks,” *Vehicular Technology Conference*, Vol.2, pp.1222-1226, 1999.

[9] C. Schurgers, M. Srivastava and V. Tsiatsis, “STEM: Topology Management for Energy Efficient Sensor Networks,” *Proceedings of the IEEE Aerospace Conference*, Vol.3, pp.1099-1108, 2002.

[10] W. Ye, J. Heidemann and D. Estrin, “An Energy-Efficient MAC Protocol for Wireless Sensor Networks”, *In Proceedings of INFOCOM2002*, April 2002.

[11] S. Tilak, A. Murphy, W. Heinzelman, “Non-uniform Information Dissemination for Sensor

Networks", *Proceedings of IEEE International Conference*, pp.295–304, November 2003.

[12] J. Macker and S. Corson, "Mobile Ad hoc Networks (MANET)", *IETF WG Character.* http://www.ietf.org/manet-charter.html.

[13] T. Hou and T. Tsai, "Adaptive Clustering in a Hierarchical Ad hoc Network," *Proceedings of the Workshop on Computer Networks,* December 1998.

[14] E. Royer and C. Toh, "A Review of Current Routing Protocols for Ad hoc Mobile Wireless Networks," *IEEE Personal Communications Magazine*, pp.46-55, April 1999.

[15] C. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," *Proceedings of the ACM SIGCOMM'94*, pp.234-244, October 1994.

[16] C. Perkins, E. Royer and S. Das, "Ad Hoc On-demand Distance Vector(AODV) Routing," *Internet Draft*, draft-ietf-manet-adov-13.txt, February 2003.

[17] C. Perkins and E. Royer, "Ad hoc On-Demand Distance Vector Routing," *Proceedings of IEEE WMCSA*, February 1999.

[18] Z. Haas and M. Pearlman, "The Performance of Query Control Schemes for the Zone Routing Protocol," *ACM/IEEE Transactions on Networking*, Vol.9, No.4, pp.427-438, August 2001.

[19] M. Pearlman and Z. Haas, "Determining the Optimal Configuration for the Zone Routing Protocol," *IEEE Journal on Selected Areas in Communications*, Vol.17, No.8, pp.1395-1414, August 1999.

[20] Z. Haas and M. Pearlman, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," *Internet Draft*, draft-ietf-manet-zone-zrp-02.txt, June 1999

[21] N. Nikaein, H. Labiod and C. Bonnet, "DDR-Distributed Dynamic Routing Algorithm for Mobile Ad hoc Networks," *Proceedings of IEEE Mobile and Ad Hoc Networking and Computing*, pp.19–27, August 2000.

[22] Y. Chang, T. Chang and T. Hsieh, "Hierarchical Cellular-based Management for Mobile Hosts in Ad-hoc Wireless Networks," *Proceedings of IEEE International Conference on Information Networking*, pp.843 -848, February 2001.

[23] S. Coleri and P. Varaiya, "Fault Tolerance and Energy Efficiency of Data Aggregation Schemes for Sensor Networks," *Proceedings of the IEEE 60th Vehicular Technology Conference*, Vol.4, pp.2925-2929, 26-29 September 2004.

[24] D.B. Johnson and D.A. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks," *IETF Draft*. July 2004.

[25] F. Bertocchi, P. Bergamo, G. Mazzini and M. Zorzi, "Performance Comparison of Routing Protocols for Ad-hoc Networks," *Proceedings of the IEEE Global Telecommunications Conference*, Vol.2, pp.1033-1037, December 2003.

[26] K. Seada and A. Helmy, "An Overview of Geographic Protocols in Ad Hoc and Sensor Networks," *Proceedings of the 3rd ACS/IEEE International Conference on Computer Systems and Applications*, pp.62-69, 2005.

[27] M. Hempel, H. Sharif and P. Raviraj, "HEAR-SN: A New Hierarchical Energy-Aware Routing Protocol for Sensor Networks," *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, pp.324-331, January 2005.

[28] Z.W. Zheng, Z.H. Wu and H.Z. Lin, "Clustering Routing Algorithm using Game-theoretic Techniques for WSNs," *Proceedings of the 2004 International Symposium on Circuits and Systems*, Vol.4, pp.904-907, May 2004.

[29] J. Hornsberger and G.C. Shoja, "Geographic Grid Routing for Wireless Sensor Networks," *Proceedings of the IEEE Networking, Sensing and Control Conference*, pp.484-489, 19-22 March 2005.

[30] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed Diffusion for Wireless Sensor Networking," *IEEE/ACM Networking Transactions,* Vol.11, No.1, pp.2-16, February 2003.

[31] H. Sabbineni and K. Chakrabarty, "Location-aided Flooding: An Energy Efficient Data Dissemination Protocol for Wireless Sensor networks," *IEEE Transactions on Computers,* Vol.54, No.1, pp.36-46, January 2005.

[32] R.C. Luo, L.C. Tu and O. Chen, "Auto-Deployment of Mobile Nodes in Wireless Sensor Networks Using Grid Method," *Proceedings of IEEE International Conference on Industrial Technology,* pp.359-364, 14-17 December 2005.

[33] F. Ye, H. Luo, J. Cheng, S. Lu and L. Zhang, "Sensor Networks: A Two-Tier Data Dissemination Model for Large-scale Wireless Sensor Networks," *Proceedings of the 8th Annual ACM/IEEE International Conference on Mobile Computing and Networking,* pp.148-159, September 2002.

[34] S. Kim, S.H Son, J.A. Stankovic, S. Li and Y. Choi, "SAFE: A Data Dissemination Protocol for Periodic Updates in Sensor Networks," *Proceedings of 23rd International Conference on Computing Systems,* pp.228-234, 2003.

[35] H.L. Xuan and S. Lee, "A Coordination-based Data Dissemination Protocol for Wireless Sensor Networks," *Proceedings of the Intelligent Sensors, Sensor Networks and Information Processing Conference,* pp.13-18, 14-17 December 2004.

[36] Q. Li and D. Rus, "Global Clock Synchronization in Sensor Networks," *IEEE Transactions on Computers*, Vol.55, No.2, pp.214-226, February 2006.

[37] N. Bulusu, J. Heidemann and D. Estrin, "Gps-less Low Cost Outdoor Localization for Very Small Devices," *IEEE Personal Communications Magazine*, Vol.7, No.5, pp.28-34, October

2000.

[38] J. Albowicz, A. Chen and L. Zhang, "Recursive Position Estimation in Sensor Networks," *Proceedings of IEEE International Conference on Network Protocols (ICNP'01)*, pp.35-41, November 2001.

[39] Y. Xu, J. Heidemannn and D. Estrin, "Geography-informed Energy Conservation for Ad Hoc Routing," *Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Rome, Italy, pp.70-84, 16-21 July 2001.

[40] M. Mamun-Or-Rashid, C.S. Hong and C.H. In, "Passive Cluster Based Clock Synchronization in Sensor Network," *Proceedings of Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resources*, pp.340-345, July 2005.