A WSN Nodes Access Mechanism and Directed Diffusion in Emergency Circumstances

Zhen Ni[1], Qianmu Li[1], Tao, Li[2],Yong Qi[1]
[1]School of Computer Science and Engineering,
Nanjing University of Science and Technology
Xiaolingwei.No.200, 210094 Nanjing, China
[2]School of Computer Science, Florida International University
11200 SW 8th Street Miami, FL 33199, U.S.A.
qianmu@mail.njust.edu.cn

Journal of Digital
Information Management

ABSTRACT: *When disaster strikes, the rapid deployment of Wireless Sensor Networks (WSNs) in the disaster area is helpful for real-time monitoring of environmental indicators and improving the efficiency and quality of emergency rescue. In the meanwhile, seveal factors such as the unpredictability of disaster, harsh environment and the urgency of network system put forward lots of special needs in network architecture, sensor nodes designing, and technical realization. This paper proposes a new routing framework for building WSNs in emergency circumstances. In particular, a mobile access mechanism based on the X-MAC protocol has been designed. An effective path of interest propagation strategy, where the WSN node positions have been used to guide the interest spread, has been proposed. Experimental results demonstrate that our proposed framework can significantly reduce the network traffic and energy consumption in directed diffusion.*

Subject Categories and Descriptors
C.2.1 [Network Architecture and Design]: Wireless Communication; **E.4 [Coding and Information Theory]**

General Terms: MAC Protocol Design, Routing Protocol Design

Keywords: WSN, Environmental Monitoring, Mobile Access, Directed Diffusion

Received: 19 January 2014, Revised 28 March 2014, Accepted 28 April 2014

1. Introduction

Wireless Sensor Network (WSN), one of the three high-tech industries forecasted by MIT, has been a hot research area in recent years. If the emergence of address-centered Internet has led to an explosive revolution in Information Sharing, the data-centered WSN that connects the natural entities in the real world into an information network through mobile sensors has already triggered a new transformation in information technology. This has been evidenced by the popularization of IOT (Internet of Things) and its wide-range of applications.

WSNs are generally application-oriented and their design and implementation need to carefully consider specific application requirements. The unique characteristics in emergency rescue, such as the harsh environment of the disaster area and the uneasy arriving of the rescue team, have generated many emergency-related application requirements in WSN implementation [1, 2, 3, 4, 5, 6]. Specifically these requirements are listed below.

(1) Usually, the occurrence of disaster is unpredictable. Sometime it is difficult to get the concrete geographic information of the disaster area. Probably, it is inconvenient even impossible for rescuer to arrive. So the senor nodes cannot be deployed manually, therefore, it is unable to achieve the deterministic coverage of the target area.

(2) In order to overcome the interference generated by noise, microwave, and obstruction, it is necessary to design effective communication mechanisms between

nodes, to solve the signal conflict of the wireless channel, to choose a reasonable path for data transmission, and to improve the stability of the network through the cooperation of the nodes.

(3) It is of great importance for emergency rescue systems to integrate individual sensors or other related things which carried by rescuers or mobile robots to the WSNs. Not only does the integration make the acquaintance of the on-site information of the target area more flexible and effective, but also can fill the blind monitoring point and increase the network coverage. To support the integration, the network function needs to be expanded and the access mechanism of mobile nodes and the dynamic network management technique need to be further investigated.

(4) Different from common environmental monitoring systems that gather information collected by sensors regularly, the system used under emergency circumstances often needs more quick reaction to events, and supports the function of querying the real-time situation of certain area or monitoring point and the function of querying the exception position of certain subject. Therefore, a real-time, query-based, efficient, and robust design of the routing strategy is needed. Only when the collected data exceeds the pre-defined threshold or a query request is received, will the data be uploaded to the Sink node. This would avoid the network congestion and the energy consumption caused by the transmission of a huge amount of data.

In order to meet the special requirements of the WSN monitoring systems in emergency circumstances, this paper designs a mobile access mechanism and proposes an effective stragtey for interest propagation in the directed diffusion routing algorithm. Our simulation experiments have compared traditional directed diffusion routing algorithm and improved directed diffusion routing algorithm and the results demonstrate the effectiveness of our proposed method.

The rest of the paper is organized as follows. Section 2 introduces the design of WSN system architecture and a mobile node access mechanism in emergency circumstances; Section 3 describes the design of the directed diffusion routing algorithm and our proposed effective strategy for interest propagation; Section 4 presents the experimental results; and finally Section 5 concludes.

2. The Design of WSNs System Architecture and Nodes Access Mechanism in Emergency Circumstances

2.1 System Architecture Design and the Choice of MAC Protocol

Assuming that the disaster area is a planar region, the general structure of emergency monitoring system can be shown in Figure 1 where a large number of sensor modes are deployed in the monitoring area at fixed

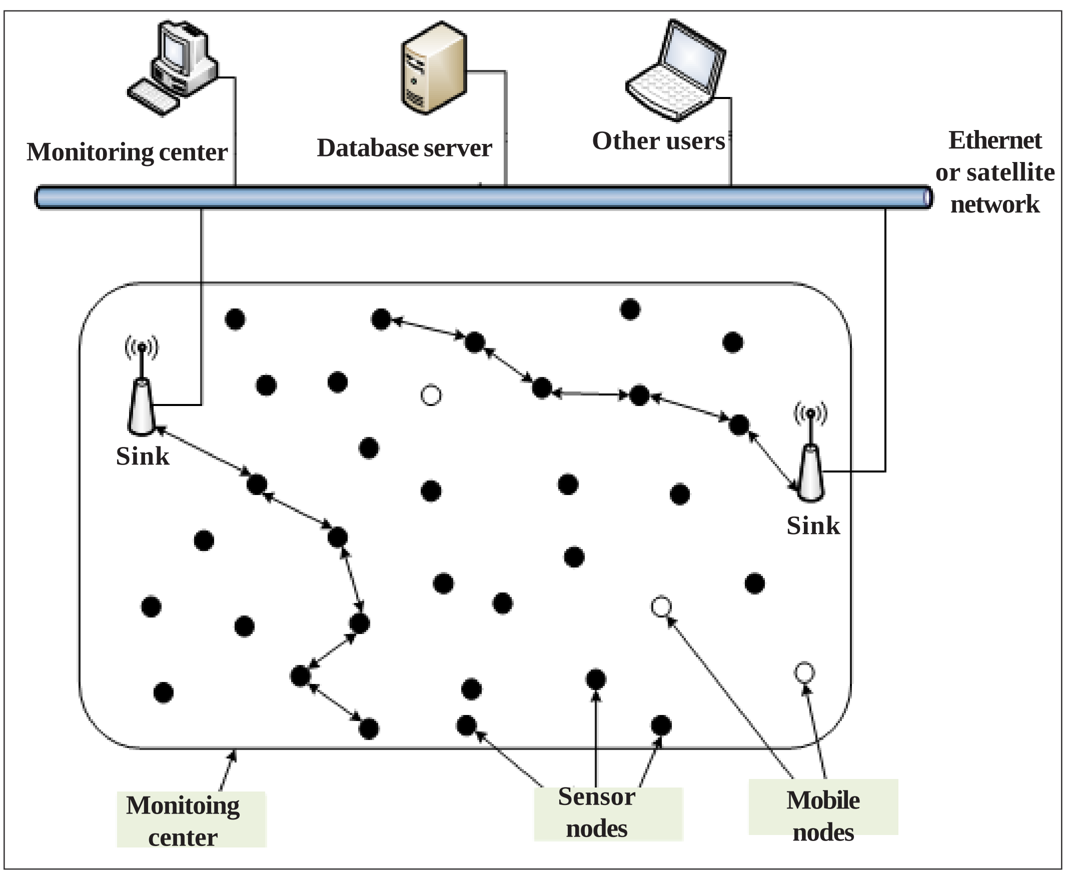

Figure 1. The general structure of the monitoring system

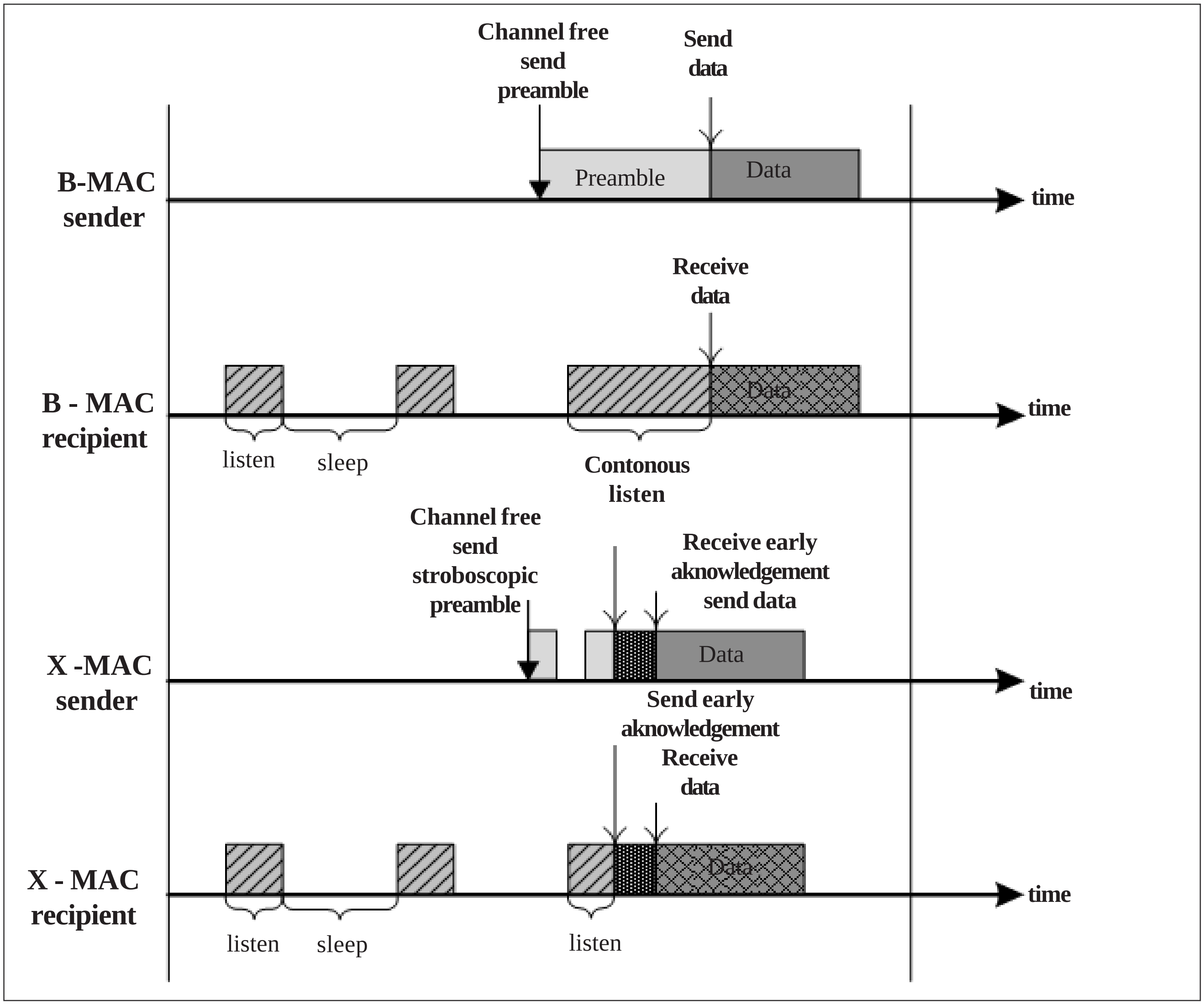

Figure 2. The sending and receiving process diagram of B-MAC protocol and X-MAC protocol

positions. There are also many mobile nodes (carried by the rescuers) that can move freely inside the monitoring network and communicate with other nodes. The whole monitoring system is formed by two components: the monitoring center (i.e., the computer/server on the top left) and WSN with the associated supporting servers. Among them, sensor nodes in WSN are responsible for collecting and uploading the environmental information within the effective sensing range. Usually, different kinds of sensor can be deployed in a sensor node simultaneously. The Sink node as the coordinator between WSNs and monitoring center is responsible for uploading information and transmitting instructions. The Sink node is responsible for gathering the data collected by sensors and for transmitting the data to the monitoring center through Ethernet or satellite. Meanwhile, it is also responsible for receiving various instructions like querying and managing and transmitting the data to the sensor nodes in the network.

The MAC protocol for WSNs can mainly be divided into three kinds [7, 8, 9,10]: the first is the allocation-based MAC protocol, like the MAC protocol which based on TDMA/FDMA/CDMA; the second is the competitive MAC protocol; the third is the hybrid MAC protocol. Instead of uploading data periodically, the sensor nodes in the network will upload the data only when there is an emergency (like monitoring value exceeds threshold) or they receive query instructions. So, it is appropriate to use the competitive MAC protocol.

There are several typical kinds of competitive MAC protocols in WSNs: S-MAC protocol [11], T-MAC protocol [12], B-MAC protocol [13], and X-MAC protocol [14]. Through comparing the overall performance on several aspects (such as node energy consumption, the network throughput, and the communication delay), X-MAC protocol shows significant advantages and can be easily realized on the nodes which support wireless transmitter with packet switching.

Both B-MAC protocol and X-MAC protocol use the LPL (low power listening) mechanism. Unlike B-MAC protocol, X-MAC protocol uses several shorter stroboscopic preambles to replace the long consecutive preamble (as shown in Figure 2) and utilizes the handshaking

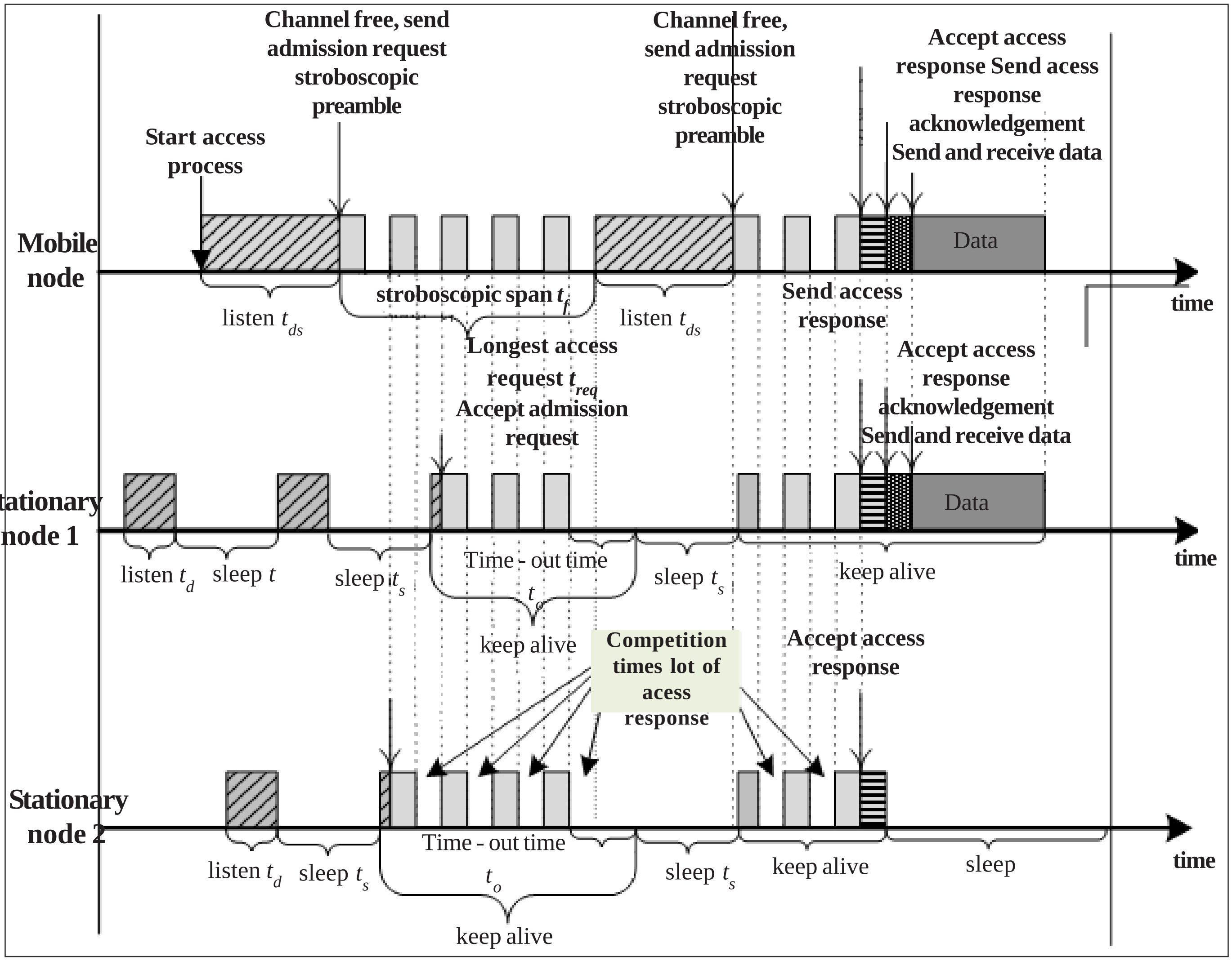

Figure 3.The accessing process of mobile nodes

mechanism to further reduce the energy consumption caused by the transmission of the preamble. When the target node receives the preamble transmitted by the sending node, the target node will send "*early acknowledgement*" information to the sending node using the break between different stroboscopic preambles, and the sending node will stop sending stroboscopic preambles and transmit the real data immediately after receiving the "*early acknowledgement*" message. Thus, the unnecessary energy consumption and communication delay caused by the continuous sending of stroboscopic preamble are avoided. Meanwhile, the transmitted preamble contains the identification of the target node and non-target nodes will drop the preamble and turn into the sleep state when receives the preamble. In this paper, we use X-MAC protocol and also design, extend, and implement the access mechanism of the mobile node and the maintenance of the mobile link.

2.2 The Design of Node Access Mechanism

There are mainly two types of methods for mobile nodes to access the network: passive access and active access .Typical passive access methods (e.g., Eavesdrop and Register (EAR) algorithms) need the stationary node to broadcast the invitation periodically to establish the connection with mobile nodes. The time delay of this type of methods depends on the time span of the broadcast invitation sent by the stationary node. And the time span is usually set to be a large value (a few seconds to tens of seconds) by the MAC protocol due to the energy conservation. Therefore, it is not proper to use passive access in applications that need fast response. In active access, mobile nodes will broadcast the admission request to the nearby stationary nodes. The stationary nodes that receive the message will send back the response message to establish the connection. This mechanism has a smaller time delay with lower energy consumption because the stationary nodes do not need to broadcast the invitation message periodically. But the mobile nodes must confirm that the channel is free before broadcasting the admission request, thus, will not interrupt the normal communication among other nodes.

In emergency monitoring systems, individual sensors carried by rescuers, moving fast inside the network, have higher requirements on response time. Therefore, this paper uses the active access method for node access and the maintenance of mobile link. The concrete process is described below.

Stage 1: The accessing process of mobile nodes

Figure 3 shows the accessing process of mobile nodes. Mobile nodes will listen if the channel is free (The monitoring time is t_{dm}); If the channel is free, the admission request message will be broadcasted. And the admission request message is broadcasted in the way of stroboscopic preamble. The stroboscopic interval is t_f and the longest duration of one admission request is t_{req}. If a mobile node has not received any access response message within t_{req}, then it will test whether the channel is free and enter the next "*listening-admission request broadcasting*" cycle.

Thus, the long-time occupation of the channel resources can be avoided and the communication among other nodes will not be affected. If a mobile node receives the access response message sent by other nodes, then it will send the acknowledgement message to the source node. Afterwards, a connection will be established and the data transmission can be performed.

When receiving the admission request message from a mobile node, a stationary node will send the access response message and wait for the acknowledgement message. To prevent multiple nodes from sending the access response message simultaneously after receiving the admission request message, a collision-avoiding mechanism is needed. This paper uses the following back-off strategy: Each stationary node generates a random number R between 0 and 1 and compares the result with a default value R_m. If $R \le R_m$, then the node will send the access response message in the current timeslot. Otherwise, it will wait for the next timeslot to repeat the process. If a stationary node does not receive any admission request messages within t_o while waiting for the next timeslot, it will turn into the sleep state to avoid over monitoring. If a stationary node receives the access response message sent by other nodes, it will quit the competition and turn into the sleep state immediately. If a mobile node receives more than one access response message sent by different stationary nodes, it will drop these messages and continue to send the admission request message. To guarantee the channel is free, the longest duration of an admission request t_{req} has to be longer than ($t_d + t_s$) the "*listening-sleeping*" cycle of a stationary node, and the stroboscopic time span t_f has to be shorter than t_d the monitoring time of a stationary node. To guarantee the channel would not turn into the sleep state too early, the stationary node monitoring timeout t_o has to be longer than the stroboscopic time span which caused by the mobile node's transmission of the preamble t_f .

Stage 2: The maintenance of the mobile link

A mobile node can communicate with a stationary node after the connection between them has been established through the mobile accessing process. If the mobile node keeps moving, it may make the received signal strength indication (RSSI) with the stationary node drop to some certain degree. At that time the mobile node will send the disconnected message to the stationary node to disconnect the connection. Next, the mobile node will start another mobile access process and establish the connection with another stationary node.

3. The Design of Directed Diffusion Routing Algorithm for WSNs in Emergency Circumstances

3.1 Communication Features and The Improved Routing Algorithm

In emergency circumstances, instead of uploading data periodically, the sensor nodes in the network will upload data only when there is an emergency (like monitoring value exceeds threshold) or receiving query instructions. As a result, it is suitable to use the data-centered, query-based directed diffusion (DD) routing protocol as the routing protocol for WSNs in emergency circumstances. Emergencies and query requests that need to be monitored will be encapsulated into the interest packet. Then, the interest packet will be diffused to a specified network area. Thus, a sensor node in the specified area can upload the data to the Sink node using the gradient established in the interest broadcasting stage when it captures an event matching the interest.

For the large amount of data transmission and the high energy consumption caused by the default interest broadcasting to the whole network in traditional DD protocol, an effective interest propagation strategy, where node positions have been used to guide the interest spread, has been propose in this paper to avoid broadcasting interest to the whole network. As shown in Figure 4, the improved routing algorithm can still be divided into three stages: interest diffusion, data dissemination, and path enforcing. This paper mainly focuses on the interest diffusion stage (including the interest encapsulation) as the other two stages are similar as the traditional DD protocol. The details of the algorithm are described as follows.

3.2 Interest Diffusion

Interest, using a set of key-value pairs to represent, is injected into the network through the Sink node. The keys include task type (type), data upload interval, target area (rect), Sink node identification (sinkID), coordinate of Sink node (sinkLocation), timestamp when interest generated (timestamp), term of validity of the interest (expiresAt), data matching conditions (matchCond) and so on. In particular, "*task type*" is the type monitored by a sensor node, such as temperature, moisture, the concentration of certain chemical gases, the speed of certain moving thing; "*data matching conditions*" is used to describe certain emergency (e.g., the temperature raises to more than 100^{o}C, the speed is higher than 20m/s, the

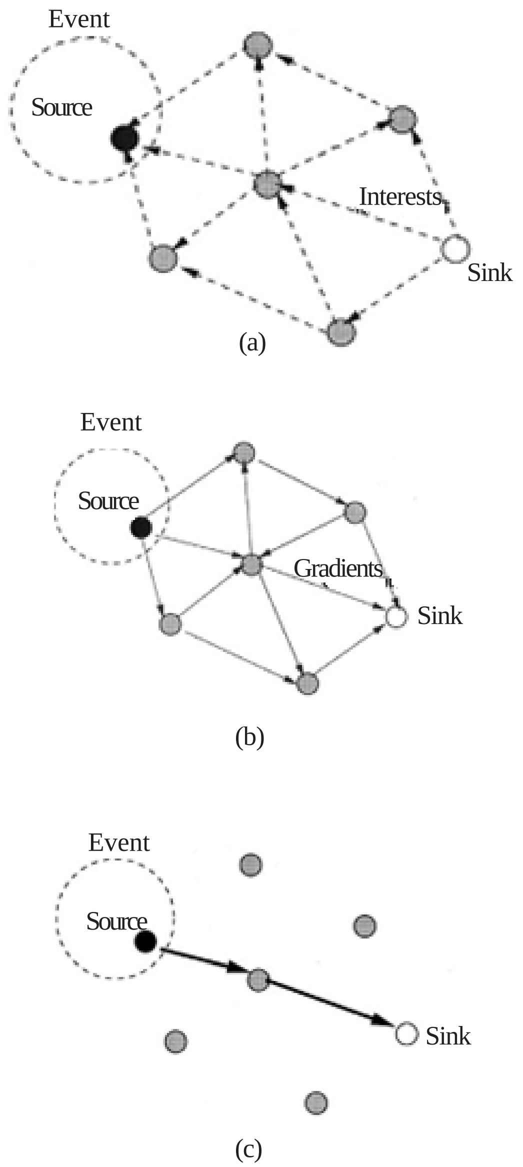

Figure 4. The diagram for the principle of the DD protocol: (a) Interest diffusion, (b) Data dissemination, (c) Path enforcing

concentration of sulfur dioxide in atmosphere exceeds 0.56mg/m3, etc.). This paper uses the combination of three keys, [type, rect, sinkID] to identify a unique interest. In other words, if the three fields of two interests are the same, then, the two interests will be considered as identical.

An example of interest is listed as below.

type = "*temperature*"

interval = 20ms //upload data collected every 20ms

rect = [100, 200, 300, 500] //target rectangle [x1, y1, x2, y2], Coordinates can be used too.

sinkID = "*SinkA*" //MAC address can be used to identify a node too, here is just for convenient.

sinkLocaion = [50, 50]

timestamp = 2012-12-01 08:30:30 //yyyy-MM-ddHH:mm:ss

expiresAt = 2012-12-01 09:30:30

matchCond = ">100^{o}C"

Interest is encapsulated in interest packets (messages) to transmit among network nodes. Besides the aforementioned fields, an interest packet also contains the information about the identification of the previous node (preNodeID) and the location of the previous node (preNodeLocation). Interest is broadcasted into the network by the Sink node.

The initial interval value in an interest packet is large (the data upload frequency is small), and it will be used to sniff the network to find whether there is any event matches the interest. The periodically broadcasting process is used to maintain the routing path between the Sink node and the source node in the WSNs whose topology is dynamically changing. Each node maintains an interest cache whose entry is associated to a unique interest.

In addition to the fields of interest, the cache contains the timestamp (lastRecvTimestamp) which represents the last time when received a message matching the interest. The cache also contains a gradient table corresponding to the interest. A gradient table contains several gradients; each gradient corresponds to a neighbor node that sends the interest packet. The gradient field contains: the identification of neighbor node (neighborID), the data rate required by the neighbor (dataRate, time interval, corresponding to the interval field in interest), the start time (timestamp, corresponding to the timestamp field in interest) and the end time (expiresAt, corresponding to the expiresAt field in interest) of the term of validity, etc. When the validity term of a gradient terminates, the corresponding entry will be removed from the gradient table. An interest will be removed from the interest cache when the corresponding gradient table is empty.

When node A receives an interest packet P broadcasted by its neighbor node B, A will take different actions based on different situations: If there are no matched interests in the interest cache TB, A will use the proposed interest propagation strategy (the details will be described in the next paragraph) to judge whether A is on the effective path. If A is on the effective path, an interest entry and the corresponding gradient table (only contains one gradient) will be added to the TB. The value of all fields in the interest entry and the gradient is obtained from P. The preNodeID and preNodeLocation fields will be updated with the information of A and the updated P will be broadcasted. Otherwise, P will be dropped; (2) If there is a match in the TB and the corresponding gradient of B exists in the gradient table, then the algorithm checks whether the timestamp in P is latter than the timestamp in this gradient. If it is, P will be considered to be an updating interest packet. First, certain fields of the interest entry like lastTimestamp, timestamp, expiresAt and certain fields of corresponding gradient like dataRate, timestamp, expiresAt will be updated if necessary. Then, the preNodeID and preNodeLocation fields of P will be updated with the information of A and the updated P will be broadcasted. Otherwise, P is dropped to avoid the possible message loop in the network.

When node A receives an interest packet P from its neighbor B, A will use the proposed effective path of interest propagation to check whether the old effective path of the interest, $Sink \rightarrow ... \rightarrow B$, is still an effective path after adding node A ($Sink \rightarrow ... \rightarrow B \rightarrow A$). The strategy works as follows: First, A will get the location of the Sink node in P (sinkLocation field), the Location of the target rectangle (rect field, As the rectangle CDEF shown in figure 5) and node B, then perform the following checks: (1), if A is in rect (this can be tested from the coordinate of A and the diagonal point coordinate of rect), A is then considered to be in the effective path of interest, and the decision process is over. Otherwise, turn to procedure (2); (2), The longest and shortest lengths between node A, node B and the four corners of the rectangle rect need to be calculated respectively(the rectangle CDEF shown in Figure 5 is an example) by using the coordinate of each point.

$$d_{a\text{-}min} = min\ \{d_{ac}, d_{ad}, d_{ae}, d_{af}\}$$

$$d_{a\text{-}max} = max\ \{d_{ac}, d_{ad}, d_{ae}, d_{af}\}$$

$$d_{b\text{-}min} = min\ \{d_{bc}, d_{bd}, d_{be}, d_{bf}\}$$

$$d_{b\text{-}max} = max\ \{d_{bc}, d_{bd}, d_{be}, d_{bf}\}$$

Then compare $d_{a\text{-}min}$ with $d_{b\text{-}min}$, $d_{a\text{-}max}$ with $d_{b\text{-}max}$, if ($d_{a\text{-}min} < d_{b\text{-}min}$) || ($d_{a\text{-}max} < d_{b\text{-}max}$), turn to (3). Otherwise, A is not on the effective path of interest, and the decision process is over; (3), The max length $d_{s\text{-}max}$ from the Sink node to the four corners of rect and the length d_{sa} from the Sink node to node A is calculated. If $d_{sa} \leq d_{s\text{-}max}$, A is on the effective path of interest; Otherwise, A is not, and the decision process is over. Figure 5 shows the diagram of interest propagation which uses the proposed effective path of interest propagation strategy.

3.3 Data Dissemination

With the propagation of interest, the gradient of data dissemination will be established (along the opposite direction of the interest propagation path). A sensor node will check its local interest cache when an event is monitored in the network. If there is no match, it will drop the event; otherwise, it will first check the corresponding gradient table of the matched interest and the max reporting data rate (Data-Rate) of all gradients in the table, and then perform data collection (at the Data-Rate) and data transmission to the neighbor nodes (at a rate proportion to the reporting data rate in the gradient). For the intermediate nodes whose reporting data rates of their neighbors are no less than their own receiving data rates, they will use the receiving data rate to transmit data to their neighbors. For those intermediate nodes whose reporting data rates of their neighbors are lower, they will transmit data to their neighbors proportionally. For any forwarded packet, there will be a copy and a record of forwarding time in the transmit data buffer of the node.

3.4 Path Enforcing

When interest spread to the source node, a data transmission link (along the opposite direction of the interest propagation path) between the source node and the Sink node will be established, and the source node

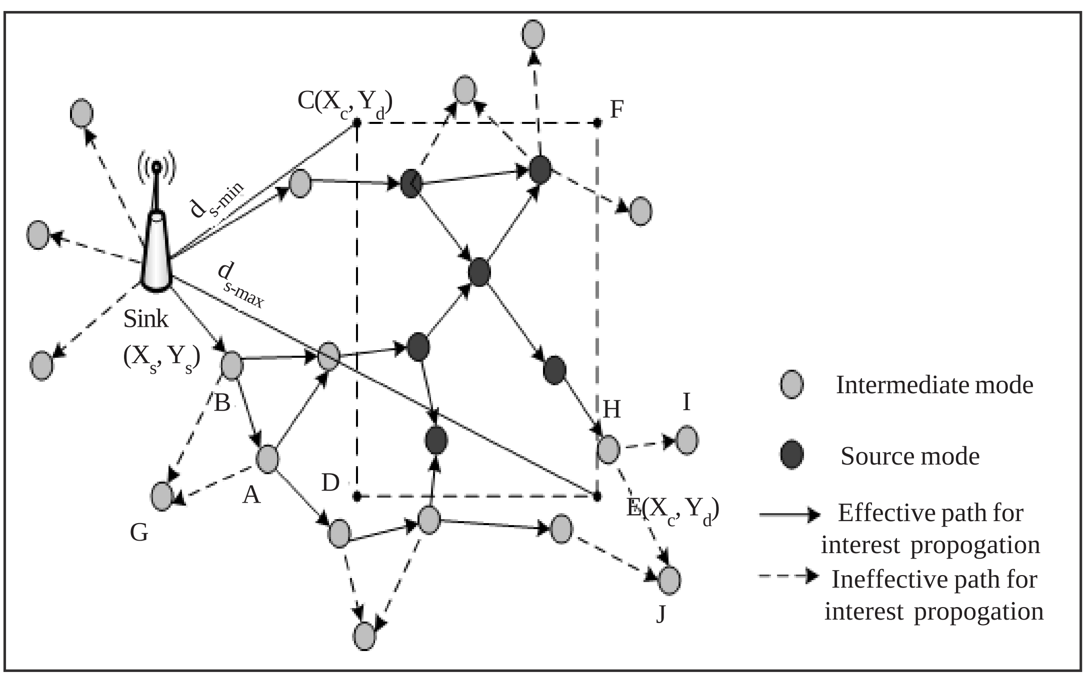

Figure 5. Interest diffusion diagram of the improved algorithm

will upload data to the Sink node at a low speed first. The Sink node will begin to enforce one of the transmission paths with the source node when receiving the data uploaded by the source node, and enlarge the uploading data rate on this enforced path. The Sink node will choose the neighbor node from which it receives the data packet first as the first hop, send the path enforcing message, and increase the reporting data rate in the path enforcing message. A node will update the reporting data rate in the corresponding gradient of the interest cache when receiving the path enforcing message. If the value of this reporting data rate is the biggest among the ones in the gradient of the corresponding interest, this node will choose the neighbor node from which it first receives the data packet as the first hop, and send the path enforcing message. The whole system will repeat the process above until the data transmission link between the source node and the Sink node is established.

When certain node (assume it is node B) on the enforced path discovers that the data transmission rate of the next hop node A drops significantly, it will deduce that link $A \rightarrow B$ lose efficacy, send the path fading message, and decrease the reporting data rate of A to B. Then a new path will be enforced by the method mentioned above.

4. Simulation Experiment

4.1 The Environment of Simulation Experiment

In the experiments, we simulated the interest diffusion stage of the directed diffusion routing algorithm and compared the traditional directed diffusion routing protocol (directed diffusion, DD), and the directed diffusion routing protocol using our proposed effective path of interest propagation (directed diffusion with decision rules, DDwDR) in terms of the number of transmitted interest messages in the same simulation environment. In addition, we also evaluated the influence of the network scale (node numbers) on the two algorithms by varying the node number in the simulation. Finally, the statistical results of two algorithms are compared, analyzed, and displayed graphically. To make the empirical study more convincing, all statistical results are computed as the average results of 100 algorithm trials (the nodes are redeployed each time) under the same conditions.

The Simulation scene is a square area of $500m \times 500m$ size, where nodes are randomly deployed in the square area and the Sink node is selected randomly among to encapsulate interest packets and broadcast packets to the network. Communication radiuses of all nodes are set to be 90m and the models for radio propagation are regular spheres. The diagram of node distribution in one of the experiments is shown in Figure 6 (where 100 nodes are deployed). In the diagram, star * represents the Sink node, circle O represents the ordinary node, and the red dotted line indicates the target area of the interest diffusion (the source node). The corresponding neighbor relationship diagram of the distribution showed in Figure 6 is shown in Figure 7. In Figure 7, * and O correspond to the Sink node and ordinary node in Figure 6, respectively. The blue short line in Figure 7represents that the connected two nodes can communicate with each other through the wireless channel, in other words, they are neighbor nodes of each other.

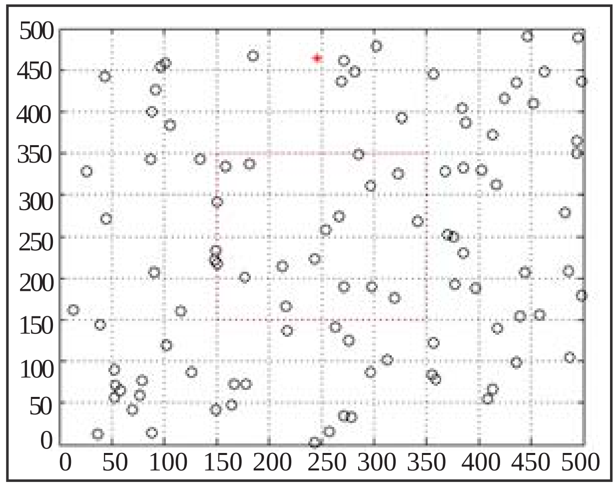

Figure 6.The diagram of nodes deployment

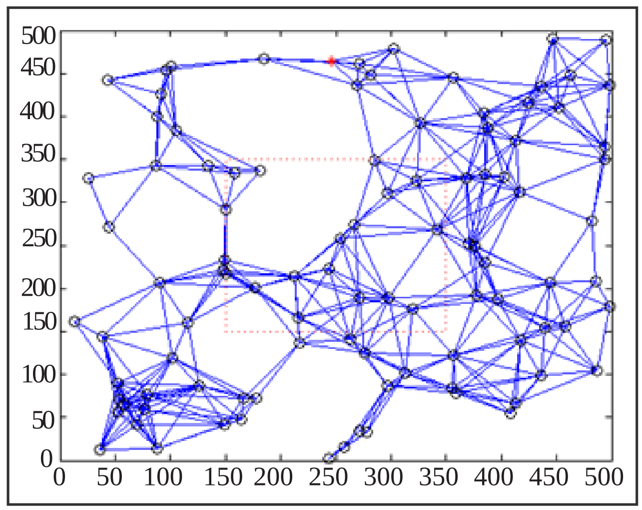

Figure 7. The diagram of the node’s neighbour relationship

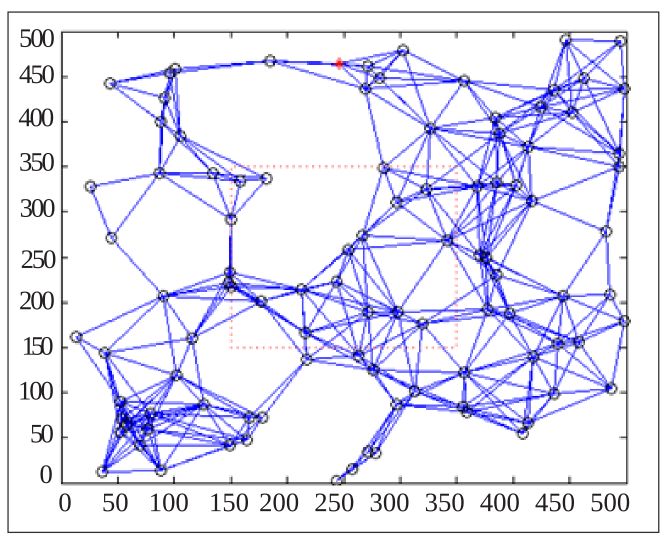

Figure 8. The visual interest diffusion diagram of the DDwDR routing algorithm

4.2 The Comparison of the Interest Diffusion Between the Two Routing Algorithms

For the node distribution in Figure 6, the visual diagrams of the interest diffusion of both routing algorithms (DDWDR and DD) are shown in Figure 8 and Figure 9, respectively. Figure 8 and figure 9 show that the traditional DD routing algorithm makes the interest diffusion in the whole network, and consequentially forward more packets; The DDwDR routing algorithm uses the effective path of interest propagation and only diffuses interest in part of the network. As a result, DDwDR forwards less packets and interest can be spread to all nodes in the target area.

4.3 The Relationship Between the Interest Packets Forwarded and the Network Size (Total Number of Nodes) of the Two Routing Algorithms

Figure 10 shows the statistical results of the number of packets forwarded for the two routing algorithms when the total number of nodes increased gradually according to the following sequence

[60, 80,100,120,140,160,180, 200, 220, 240, 260, 280,300]

As can be observed from Figure 10, under the same conditions, compared with the traditional DD routing algorithm, the DDwDR routing algorithm using the effective path of interest propagation can significantly reduce the interest packets forwarded in the network. When the total number of nodes increases, the number of forwarded interest packets will increase sharply in the traditional DD routing algorithm. However, the increase in the improved routing algorithm DDwDR is relatively smaller and more stable.

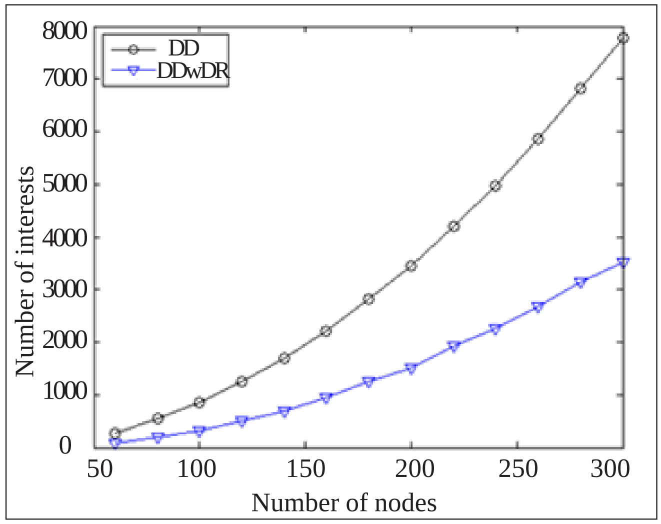

Figure 10. The relationship between the interest packets forwarded and the total number of the nodes of the two routing algorithms

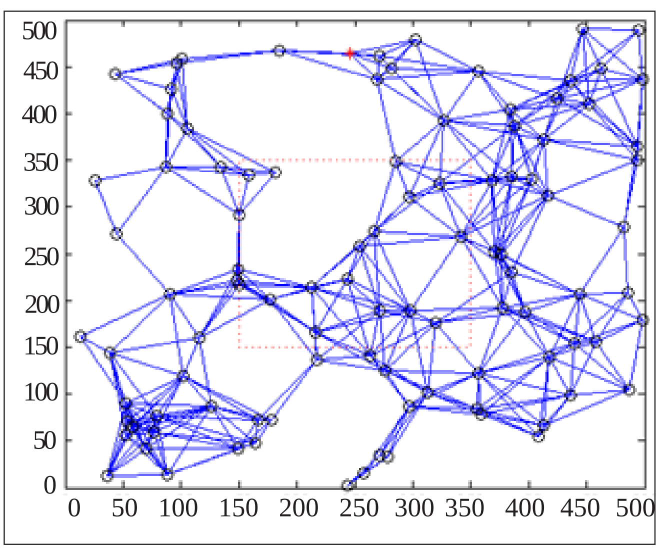

Figure 9. The visual interest diffusion diagram of the DD routing algorithm

4.4 The Performance Analysis of Improved Algorithm

By using the effective path of interest propagation, the improved DDwDR algorithm limits the blind dissemination of the interest in the network successfully, reducing both the amount of data to be transmitted in the network and the energy consumption. Because the data diffusion has a clear direction, the number of message loop has been decreased, and the data transmission delay is also significantly reduced. For example, in Figure 5, the propagation path $B \to A$ is an effective path, but the propagation path $A \to B$ is not effective. Hence the propagation path $A \to B$ does not exist (Not shown in the diagram), and the $B \to A \to B$ message loop is avoided. In addition, DD protocol establishes more than one transmission path from the source node to the Sink node by the diffusion of interest, this makes the whole system has a good performance in fault tolerance in complex harsh emergency circumstances and improves the reliability of data transmission.

4.5 Simulation for the Validity of Node Access

In this set of experiments, 20 nodes are used to simulate the validity of access in emergency circumstances, each group will be experimented for 5 times, and the average value will be computed. Mobile nodes will access the cluster that consists of the neighboring stationary nodes. The experimental results of six groups are shown in Figure 11. It can be observed from Figure 11 that the number of cluster heads has not changed, indicating that the node access strategy is effective.

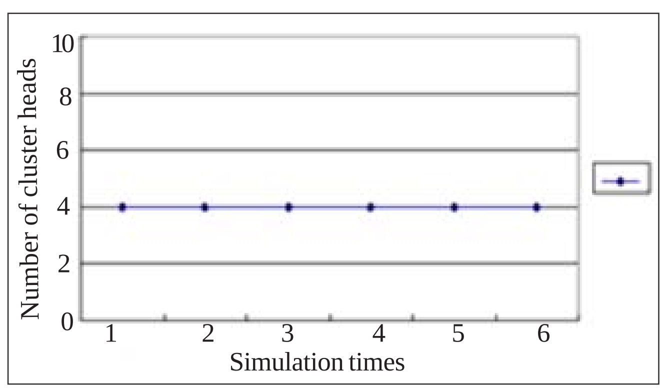

Figure 11. The validity experiment of mobile node access

In the following studies, the vehicle testing field in Tangshan military experimental center of Nanjing University of Science and Technology is used as a real-world scenario to verify the access method of mobile nodes in emergency circumstances. The experimental site covers about twenty Km^2. The following hardware elements were deployed in this area, including 8 stationary nodes (Transceiverÿ30-55MHz), an emergency signal simulation interferometer (batch-type), two emergency mobile vehicles (ID: 1, 2; Transceiver, 30-55MHz; GPS; network control access recording system). The first set of experiments is the ten trials of mobile node test, tracking the emergency vehicle from the start to accessing the stable test data, as shown in Figure 13, where the batch-type interference signal was set in the 2^{th}, 3^{th}, 5^{th}, 6^{th}, 7^{th}, 8^{th}, 9^{th} test. The second of experiments considers different scenarios of the mobile node access. In particular, the access of five groups of new mobile nodes was simulated, the exit of five groups mobile node which caused by signal interruption was simulated, and the sudden damage of ten groups of stationary nodes was simulated. Each group has been experimented for 5 times, and the average result is shown in Figure 14.

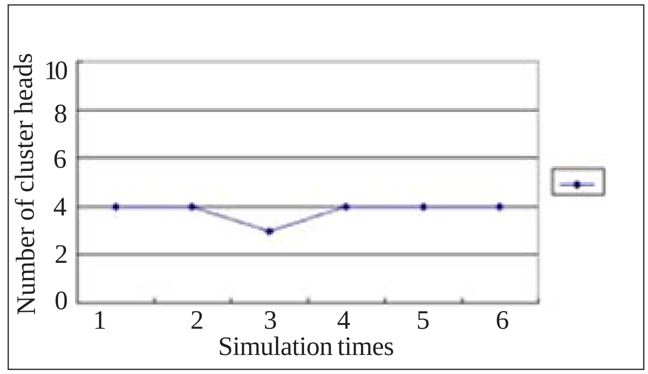

Figure 12. The validity experiment of mobile node exit

Figure 13 shows that, using the proposed routing method, mobile nodes can access the network when in batch-type interruption, and can remain relatively stable. In addition, an even better performance can be achieved when there is no environment interference. Figure 14 shows that, in the condition which simulates the real situation, the access and exit of the mobile nodes have no effects on the structure of the network; When stationary nodes are damaged, short adaptation will occur in the network.

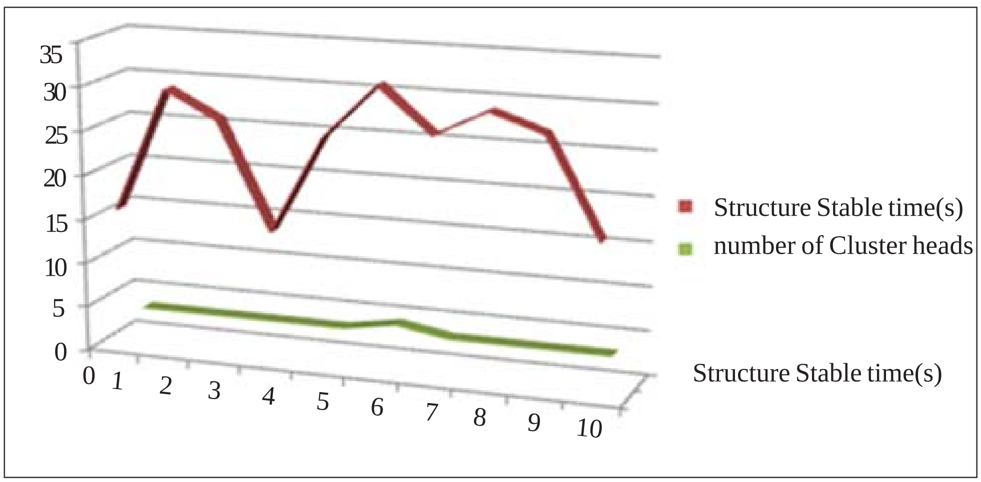

Figure 13. The validity experiment in emergency circumstances

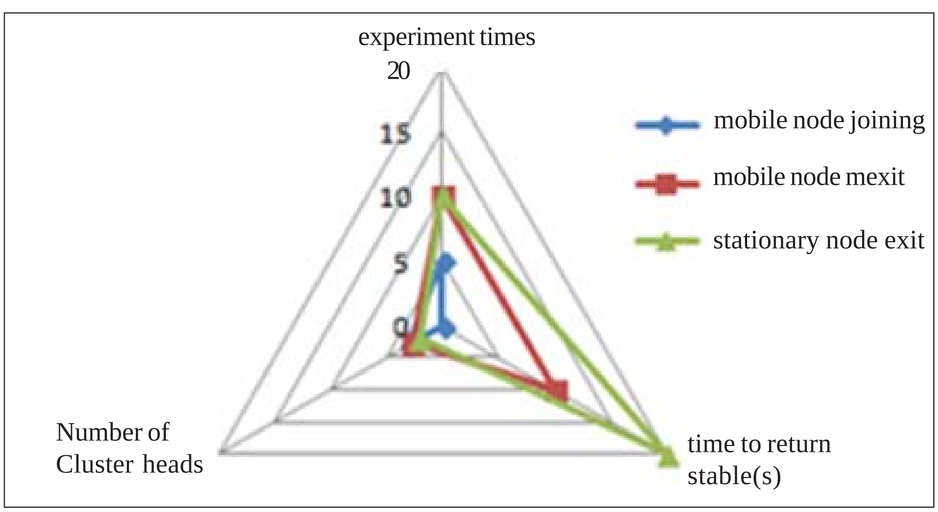

Figure 14. The stability test for access in emergency circumstances

5. Conclusion

This paper studies the access mechanism of mobile nodes and the query-based directed diffusion algorithm. After analyzing and comparing several existing common MAC protocols for WSNs and the characteristics and application scenarios of the routing algorithms, this paper designs a mobile node access mechanism based on X-MAC protocol for emergency circumstances. To reduce the data transmission and energy consumption caused by the default interest network-wide broadcasting in traditional directed diffusion routing algorithm, the paper proposes an effective path of interest propagation strategy using the node location information to ensure that the interest diffusion has a more clear direction. The paper also performs simulation studies to verify and analyze the real influence on the performance of directed routing when using the proposed strategy. The experimental results indicate that the improved routing algorithm can significantly reduce the forwarding interest packets in the network, reduce the message loop, and save network energy. Compared with the tradition directed diffusion routing, the performance of the proposed algorithm has been greatly improved.

6. Acknowledgements

This research was funded by a grant (61272419) from the National Natural Science Foundation of China, a grant (BK2011370, BK2011023) from Jiangsu Natural Science Foundation, a grant (2012M521089) from China postdoctoral Foundation, a grant (1201044C) from Jiangsu Postdoctoral Foundation and a grant (BY2012022) from Research Union Innovation Fund of Jiangsu Province.

References

[1] Bertand, A., Szurley, J., Ruckebusch, P., et al. (2012). Efficient calculation of sensor utility and sensor removal in wireless sensor networks for adaptive signal estimation and beamforming. *IEEE Transactions on Signal Processing Journal*, 60 (11) 5857-5869.

[2] He, S. B., Chen, J. M., Cheng, P. et al. (2012). Maintaining quality of sensing with actors in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems Journal*, 23 (9)1657-1667.

[3] Qian-mu Li, Hong Zhang. (2012). Information security risk assessment technology of cyberspace: a review. *Information- an International Interdisciplinary Journal*, 15 (11) 4677-4684.

[4] Qian-mu Li, Mulitiple, QoS. (2011). Constraints finding paths algorithm in tmn. *Information an International Interdisciplinary Journal*, 14 (3) 731-738.

[5] Xiao Yang, Peng Miao, Gibson, J., et al. (2012). Tight performance bounds of multihop fair access for mac protocols in wireless sensor networks and underwater sensor networks. *IEEE Transactions on Mobile Computing Journal*, 11 (10) 1538-1554.

[6] Xiao-xing LV, Bai-hai Zhang. (2013). Research on Transmission Based on Collaboration Coding in WSNs. *Journal of Digital Information Management*, 11 (6) 441-445.

[7] Qian-mu Li, Jia Li. (2012). Rough outlier detection based security risk analysis methodology, *China Communications*, 5 (7) 14-21.

[8] Qian-mu Li, Hai-yan Mao, Hong Zhang. (2012). The design and cost analysis of dcp algorithm based on directional circle. *International Journal of Radio Frequency Identification and Wireless Sensor Networks*, 2 (2) 1-7.

[9] Si-yuan Chen, Min-su Huang, Shao-jie Tang. et al. (2012). Capacity of data collection in arbitrary wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems Journal*, 23 (1) 52-60.

[10] Wei Ye, Heidemann, J., Estrin, D. (2002). An energy-efficient mac protocol for wireless sensor networks. *In*: Proceedings of the 21st Int'1 Annual Joint Conf IEEE Ccmputer and Communications Societies (INFOCOM2002), p. 1567-1576.

[11] Van, D. T., Langendoen, K. (2003). An adaptive energy-efficient mac protocol for wireless sensor networks. *In*: Proceedings of the 1st Int'1 Conference on Embedded Networked Sensor Systems (SenSys'03), p. 171–180.

[12] Polastre, J., Hill, J., Culler, D. (2004). Versatile low power media access for wireless sensor networks. In: Proceedings of the 2nd International conference on Embedded Networked Sensor System (ACM SenSys'04), p. 95-107.

[13] Buettner, M., Yee, G. V., Anderson, E. et al. (2006). X-mac:a short preamble mac protocol for duty-cycled wireless sensor networks. *In*: ACM SenSys'06 Proceedings, p. 307-320.

[14] Qian-mu Li, Guo-shen Zhan, Jun Hou. et al. (2012). A trusted mobile interaction in ubiquitous networks. International *Journal of Advancements in Computing Technology*, 4 (15) 346-353.