IOT Water Meter Reading System Based on Multi-agent and Ah Hoc

Yonghua Wu[1(✉)] and Ruijuan Zuo[2]

[1] College of Electronic and Information Science, Fujian Jiangxia University, Fuzhou, Fujian 350108, People's Republic of China
wuyonghua@fjjxu.edu.cn

[2] College of Mathematics and Informatics, Fujian Normal University, Fuzhou, Fujian 350117, People's Republic of China

Abstract. Aiming at the shortcomings of traditional wireless meter reading system, such as difficulty in expansion, high deployment cost, and high power consumption during data transmission, this paper designs an IOT water meter reading system based on multi-agent and Ah hoc. The system can be automatically networked between nodes with LoRa, which is easy to expand. The system uses a multi-agent structure, each agent is responsible for different tasks, the complex system is divided into independent small systems, reducing the complexity of the system. In order to ensure the data security of the information in the water meter and transmission process, the Agent hardware design security module based on FMCOS-SE, the key information is encrypted and stored using SM4 algorithm.

Keywords: Wireless meter reading system · Ad hoc · Multi-agent · SM4 · IOT

1 Introduction

Micro-power wireless meter reading has been applied to the hydropower industry since the late 1990s. During more than 10 years of technical development, they have experienced star network, tree network, fixed frequency grid transmission, and have been partially developed to the fourth-generation technology. The fourth-generation technology focus on Ad-Hoc network data transmission mode with automatic frequency hopping and self-organizing network [1]. Ad hoc network applications have received little attention in the meter reading industry. Based on GPRS and ad hoc networks a novel design of a wireless ad hoc network remote meter reading system is proposed [2]. In order to facilitate the advanced measurement system with real-time interaction in smart grid and to satisfy the requirements for power quality management, a wireless ad hoc smart metering system for power quality using Internet of things (IoTs) technology is presented in the paper [3]. Typically, the electric power companies employ a group of power meter readers to collect data on the customers energy consumption. This task is usually carried out manually, which can lead to high cost and errors, causing financial losses, so in the paper [4], propose an architecture to the Automatic Meter Reading

Y. Chenggang et al. (Eds.): MobiMedia 2022, LNICST 451, pp. 15–30, 2022.
https://doi.org/10.1007/978-3-031-23902-1_2

(AMR) system using Unmanned Aerial Vehicles (UAV). These studies mainly focus on reducing the node's transmission power, detecting abnormal nodes, etc. The intelligence and coordination of the node itself are not considered, the receiving sensitivity is not good, and the meter reading speed is slow.

Agent theory and technology originated in the 1980s and are now gradually applied to industries, agriculture, and other fields [5, 6]. A multi-agent architecture is proposed. To exploit the advantages of multi-agent systemsmodelling for WSN services, network topologies and sensor device architectures [7]. These studies mainly focus on the accuracy of the data of the nodes without considering the networking capabilities of the nodes And low power consumption.

At present, the domestic and foreign wireless water meter reading network technologies include WIFI, HomeRF, Bluetooth BLE4.0, Zigbee, GPRS, micro-power wireless network, and low-power wide area network (LPWAN). WIFI, HomeRF, Bluetooth, etc. are not widely used in domestic water meter collection. Zigbee's communication technology is used more internationally [8]. With the rise of the Internet of Things, a low-power wide area network (LPWAN) came into being. NB-IoT and LoRa are among the best [9]. NB-IoT is currently not commercialized, and domestic research is very popular. The LoRa network has been piloted or deployed in many places abroad, but Lora has fewer applications in China and less in the collection of water meters [10].

Based on the current status of technology development at home and abroad, this paper uses the low-power LoRa transmission module currently on the market and integrates the Agent theory into various nodes of the meter reading system to build a self-organizing multi-hop Ad-Hoc network of nodes, which is used in the water meter collection and reading industry. Provide a three-dimensional perception system for the development of smart water services. The system is composed of multiple Agent structures, and each level of Agent can intelligently complete the corresponding tasks of data collection, communication, and summary. Using SX1278 LoRa as a communication module can have a longer communication distance and lower power consumption [11]. The nodes can self-organize to form an Ad-Hoc network. Any node can forward data for other nodes as a route, which has strong scalability and low deployment cost. The security module is embedded in various Agent hardware designs, and the key loaded in the module is used as the cornerstone to ensure the security of data communication, access, and storage. The encryption method uses the domestic SM4 algorithm [12, 13]. By introducing a ministerial key system, a three-level key management method for water meter application is established at the ministerial, project, and user levels.

2 System Model Based on Multi-agent

2.1 System Architecture

Combining the idea of multi-agent system with Ad hoc self-organizing network technology, the wireless meter reading system model (see Fig. 1) is designed. From the topology diagram, the system is divided into three levels, with a collector agent, a concentrator agent, and a management center agent. Three different agents communicate with each other to complete the water meter collection task. The concentrator Agent node is connected to multiple water meter sensors, which can collect the readings of

multiple water meters in real time. The concentrator agent is responsible for managing the work of multiple collector agents. It can not only collect the data of the collector agent, but also issue instructions to the collector to control its running state. The management center agent manages multiple concentrator agent nodes, summarizes the data of each concentrator agent node, and can issue commands to the collector agent under it through the concentrator agent node. An Ad hoc network is formed between the Collector Agent and the Concentrator Agent. Although the concentrator agent is the central node of several collector agents logically, it is not necessary for the concentrator agent and collector agent to communicate directly. Any node in the network can forward packets for other nodes. The water meter data collected by the collector agent can be transmitted to the corresponding concentrator agent through multi-hops. Similarly, the control instructions of the concentrator agent can reach a certain collector agent in a multi-hop manner. Therefore, the Collector Agent and Concentrator Agent also have the ability to perceive the network topology and determine the data transmission path. The communication between the concentrator agent and the management center agent is performed via the 4G network using HTTP protocol. When the concentrator agent submits the data request, it will submit the data to the corresponding HTTP API of the management center.

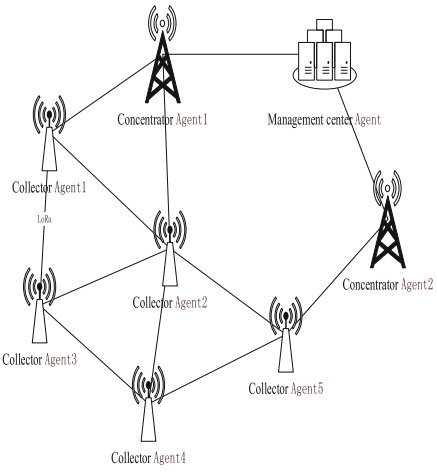


Fig. 1. Wireless meter reading system model

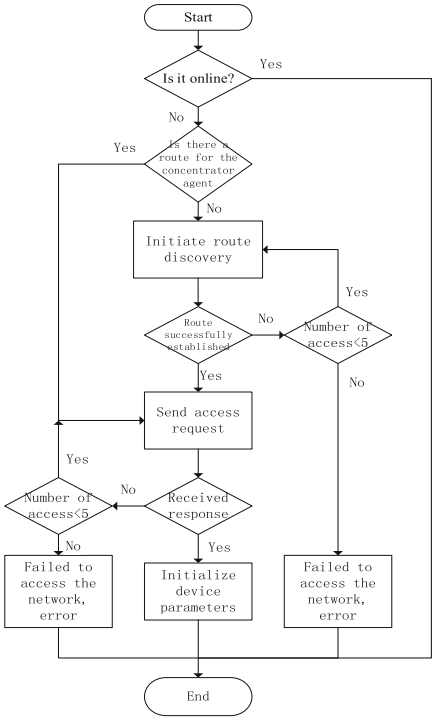


Fig. 2. The unconnected collector agent actively initiates a network access request to the concentrator agent

2.2 Coordination Mechanism Between Agents

2.2.1 Formation of Multi-agent Network

The network formation between the concentrator agent and the collector agent is initiated actively by the collector agent. The unconnected collector agent actively initiates a network access request to the concentrator agent (see Fig. 2).

The request may reach the concentrator node directly, or route through multiple nodes in the network (see Sect. 6 for detailed routing mechanism and protocol) to the concentrator agent. After confirming the network access request, the concentrator Agent sends basic system parameters to it. The parameters include the time and interval assigned to the node to initiate data upload. Different upload time points are used to avoid network congestion caused by multiple collector agents simultaneously uploading, and different time intervals affect the real-time performance and power consumption of data. The shorter the data upload interval, the better the real-time data, but the higher the communication frequency, the higher the average power consumption, the shorter the battery life; on the contrary, the longer the data upload interval, the more real-time data Poor, but the lower the average power consumption, the longer the battery life. After receiving the basic parameters of the system, the collector agent will update the configuration of its own node and respond to the concentrator to complete the network access. The concentrator agent uses the 4G module to access the management center agent to register and obtain the system configuration when it is first started.

2.2.2 Communication Coordination Among Multiple Agents

Most of the time, the communication between the collector agent and the concentrator agent is initiated actively by the collector agent. The collector agent uploads data to the concentrator agent at the determined time interval based on the upload time point determined when accessing the network. The concentrator agent caches the data transmitted by the collector agent in local storage. The communication between the concentrator Agent and the management center Agent has two modes, real-time and non-real-time. In real-time mode, when the concentrator agent receives the data from the collector agent or meets a certain time interval, it will immediately initiate communication with the management center and submit the data to the management center. In non-real-time mode, the concentrator agent initiates communication only at fixed time intervals. When receiving the request from the concentrator agent, the management center agent checks whether there are any tasks not assigned to the agent in the task queue. If so, the corresponding task is delivered in the response. When the concentrator agent receives the task, it will actively contact the collector agent node that should actually execute the task and release the task.

3 System Hardware Design

3.1 Collector Agent

The hardware framework of the collector is mainly composed of PIC single-chip microcomputer, power supply module, LoRa wireless communication module, FMCOS-SE safety module, and pulse metering sensor module (see Fig. 3).

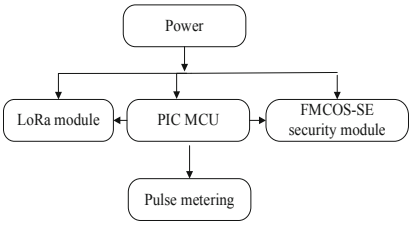


Fig. 3. The hardware framework of the collector agent

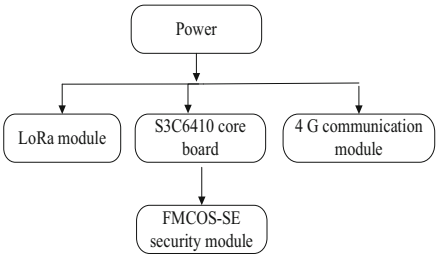


Fig. 4. The hardware framework of the concentrator agent

3.1.1 PIC Microcontroller Microcontroller Module

The microcontroller of the collector Agent uses Microchip's PIC24FJ128GA308 16-bit low-power microcontroller. The hardware module is responsible for sensor data reading, control signal output, data storage and communication. The microcontroller has a 16 × 16 hardware multiplier and a 32 × 16 hardware divider, which facilitates the processing of water meter data. At the same time, the current consumption of the microcontroller during sleep is 400 nA, which can run for a long time under battery power.

3.1.2 Power Module

The power supply switching circuit supports DC power supply and dry battery power supply separately. When the DC power supply and the battery are connected at the same time, the DC power supply is preferred. The storage module and the wireless communication module are respectively provided with 3.3 V power input by two separate HT7333 low dropout linear regulators. The on-off of the control circuit is controlled by a MOS field effect switch.

3.1.3 LoRa Wireless Communication Module

Use SX1278 LoRa wireless module from Semtech. The module is a long-distance, low-power wireless communication module that uses spread-spectrum technology, and has the characteristics of long communication distance, high receiving sensitivity, and low power consumption. The typical current consumption during sleep is 0.2 uA, the typical current consumption during reception is 10 mA, and when using 7 dm transmit power transmission, the typical current consumption is 2 mA. The maximum transmission distance in the city is about 3 km, suitable for long-distance low-power data transmission.

3.1.4 FMCOS-SE Security Module

The FMCOS-SE security module is a security module developed based on the FM1280 chip. It uses an ARM 32-bit security CPU and is equipped with a dedicated operating system. The FMSE security module encrypts some sensitive data related to the water meter, such as user password, user ID, card authentication data, ladder water price, water meter reading, valve control status, equipment root key, etc. The encryption algorithm

used is SM4 security algorithm. The SM4 algorithm was officially approved by the State Password Administration in 2012. It is the first commercial password algorithm for wireless LAN in my country. It has the characteristics of simple, safe and fast. SM4 is symmetric encryption, and the key length and packet length are both 128 bits.

3.2 Concentrator Agent

Based on the requirements of data processing and protocol conversion, the hardware of the concentrator agent is mainly based on the S3C6410 development board (see Fig. 4). The development board uses a SPI interface and a USB interface wireless communication module to connect to the 4G communication module. The concentrator agent obtains the system information, water meter information, valves, etc. encrypted by the FMCOS-SE transmitted from the collector agent through the LoRa wireless module, and uploads it to the server through the 4G communication module. The server completes the encryption and decryption of the data.

3.2.1 Processor

Use Samsung S3C6410 processor. This is a core based on ARM1176JZF-S, including 16 KB instruction data cache and 16 KB instruction data TCM.

3.2.2 Power Supply

In order to maintain long-term continuous operation, the power supply on the concentrator Agent board is provided by the DC power supply.

3.2.3 LoRa Wireless Communication Module

Use the same SX1278 LoRa wireless module as the collector Agent, and connect to the CPU with SPI interface.

3.2.4 4G Communication Module

This system uses U8300C 4G wireless module, it is a wireless terminal product suitable for TDD-LTE/TD-SCDMA/UMTS/EVDO/EDGE/GPRS/GSM/CDMA multiple network standards and GPS positioning services. While providing high-speed data access and GPS positioning services, the U8300C can provide functions such as SMS and address book, and can be widely used in products such as mobile broadband access, video surveillance, handheld terminals, and car equipment. The system uses the serial port UART of the ARM embedded system S3C6410 to complete the control of the U8300C 4G module. Drive the transistor S8050 through the S3C6410 GPIO pin to reset the 4G module. The concentrator agent remotely transmits user data, channel information, water meter dial data, valve control data and other related data to the background database through the U8300C 4G wireless module, enabling centralized management and monitoring of multiple concentrator agents.

3.2.5 FMCOS-SE Security Module

Use the same FMCOS-SE security module as the collector Agent, and connect with the S3C6410 embedded processor with SPI interface.

4 FMCOS-SE Security Module File Structure Design

The security module is a special security encryption chip designed based on the requirements of the ISO7816 specification, and supports the watch to realize the security protection of sensitive data. The product uses a dedicated domestic cryptographic algorithm chip as a hardware platform and is equipped with a dedicated operating system. The security module has adopted perfect security protection measures during hardware design, such as anti-tampering, anti-attack and other functions, and the operating system has also designed and implemented a perfect software security mechanism, using domestic cryptographic algorithms to meet the storage and storage of key data. Encryption protection. The security module contains the water meter application, and the application directory is MF. The following (see Fig. 5) shows the file structure of the Collector Agent and Concentrator Agent security modules.

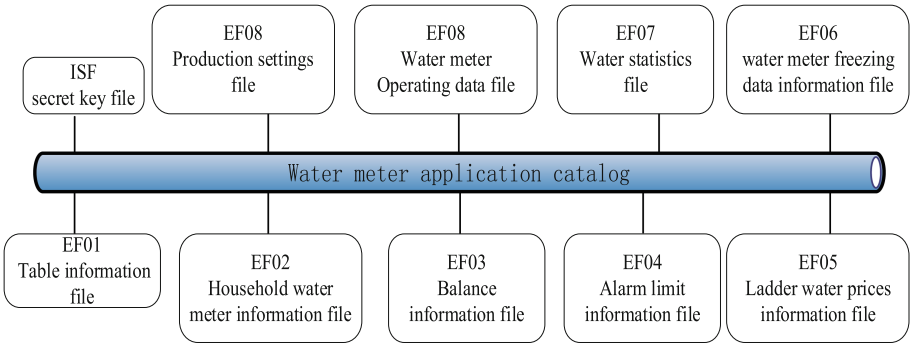


Fig. 5. File structure of the collector agent and concentrator agent security modules

5 Agent Communication Protocol Design

According to the characteristics of LoRa hardware and the actual application scenarios, the communication protocol between collector agent and concentrator agent is designed. The communication between the collector Agent, the concentrator Agent and the server/handheld terminal interacts in the form of data packets. A complete command packet consists of the start identification unit, packet length, command 1, command 2, command 3, command unit and check unit end character, see Table 1.

5.1 Command 1

Represents the source device: 53H (V) represents the server, 57H (W) stands for handheld terminal/Bluetooth, 55H (U) stands for serial debugger, 52H (R) represents the collector, 4DH (M) stands for concentrator.

Table 1. Common format of the information interaction command packet of server, concentrator and collector

Packet header	Packet length	Command 1	Command 2	Command 3	Data	Check code
55 99 2 bytes	1 byte	Source device 1 byte	Terminal device 1 byte	1 byte	JSON format	CRC 2 bytes

5.2 Command 2

On behalf of the terminal equipment: 53H (V) on behalf of the server, 57H (W) stands for handheld terminal/Bluetooth, 55H (U) stands for serial debugger, 52H (R) represents the collector, 4DH (M) stands for concentrator.

5.3 Command 3

The command includes up to 100 commands such as querying the agent information of the collector, serial port setting, water meter information and valve information setting, Ad-Hoc network channel type and frequency setting.

5.4 Check Unit

a) Check the "command data" in the protocol. From the first byte of "Command 1" to the last byte of the data area;
b) A 16-bit CRC check polynomial x16 + x2 + 1 (0×8005) is used to generate a 2-byte CRC checksum (high byte in the back, low byte in the front);
c) The sender should generate a two-byte CRC checksum according to the "command unit". After receiving the complete data packet, the receiver should generate a new CRC checksum according to the "command unit";
d) The new CRC checksum is equal to the received checksum, indicating that the data packet is valid.

6 Routing Protocol Design

6.1 Ad Hoc routing protocol

Routing protocol provides the path selection for communication between collector node and concentrator node. Ad Hoc routing protocols are divided into active routing and on-demand routing. Active routing is similar to traditional routing protocols. Each node in the network needs to maintain a routing table to other nodes, Periodically broadcast routing packet information is exchanged and routing table updates are maintained. On-demand routing is the opposite of table-driven routing. Each node makes routing requests only when needed, and instead of establishing and maintaining routing information to other nodes, it creates routing tables temporarily based on communication needs.

In this design, for the acquisition Agent, The data finally flows to the corresponding concentrator Agent. A collector Agent node will not take other collector Agents as the destination node for communication, so there is no need to maintain the routing information to all other nodes in the network, so Table - driven routing protocol should not be used. In addition, the location of collector Agent and concentrator Agent in this design is relatively fixed, so the items in the routing table will not change frequently and the frequent changes of node topology need not be considered. The concentrator Agent can broadcast its routing information and save the routing request cost generated by the node.

6.2 Four Basic Messages Design

In this design, Ad Hoc protocol is designed based on on-demand protocol, and has four basic messages (see Fig. 6): Routing request message, Router response message.

The concentrator agent broadcast message and Routing error message.

The fields of each message are described below:

Version: The version number of the protocol currently in use
Type: Message type
TTL: Time to live, A counter used to limit packet lifetime. Each time the message goes through the route forward, TTL-1, When the TTL decays to 0, the packet is discarded.
Hops: The number of hops a message passes through a router

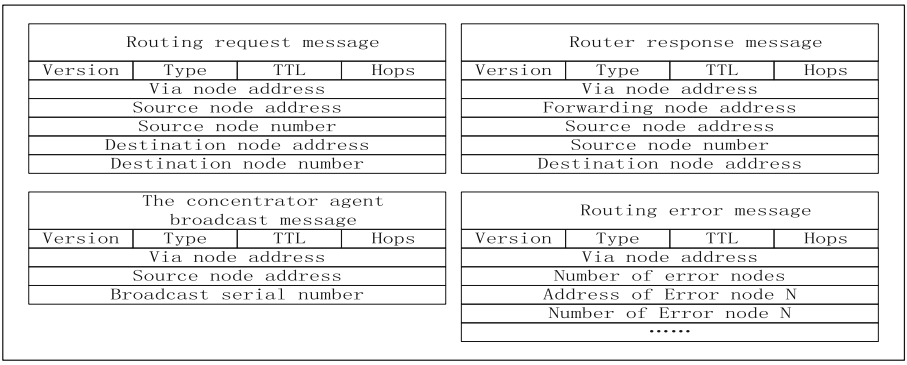


Fig. 6. Four basic messages design

1) The concentrator agent broadcast message
① Via node address: The address of the node through which the broadcast message is currently passing
② Concentrator Agent source node address: Address of the concentrator Agent node issuing the broadcast
③ Broadcast serial number: Broadcast serial number maintained by a source

2) Routing request message
① Via node address: The address of the routing request message currently passing through the node
② Source node address: The address of the routing request originating node
③ Source node number: The sequence number maintained by the source node, indicating the order of the request
④ Destination node address: The address of the destination node
⑤ Destination node number: The sequence number maintained by the destination node, indicating the order of the response
3) Router response message
① Via node address: The address of the current routing response message passing through the node
② Forwarding node address: Specifies the address of the node to forward this message
③ Source node address: The address of the node sending the routing response message
④ Source node number: The sequence number maintained by the source node, indicating the order of the response
⑤ Destination node address: The destination node address of the routing response message
4) Routing error message
① Via node address: The address of the node at which the current routing error message is routed
② Number of error nodes: The number of error nodes contained in the message
③ Address of Error node N: The address of the Nth node at which a connection error occurred
④ Number of Error node N: When an error occurs, the sequence number of the error node in the routing table cache

6.3 Route Discovery

Each node maintains a routing table (see Fig. 7). The routing table contains the address of the next node to go through to reach a node and the number of hops needed to reach that node. The ordinal fields represent the order of the data and are used to route updates and avoid loops. There are three ways for a node to discover the route to other nodes: address broadcast, passive acquisition, and on-demand request. The address broadcast mode can only be initiated by the concentrator Agent, which is mainly used to convey its route to the accessible nodes in the network at the initial stage of network establishment. When address broadcasting is used, the concentrator Agent will broadcast its address to neighboring nodes. The node receiving the broadcast will update its routing table and forward the broadcast packet to its neighboring nodes. In the form of flooding, the routing information of the concentrator Agent will be transmitted to all reachable nodes in the network. After address broadcasting is completed, the initial nodes at the time of network establishment will establish a routing item to the concentrator Agent node. Passive acquisition means that during communication, a node retrieves the route to a node in reverse. Suppose that a newly added collector Agent node A obtains the route to concentrator Agent node C by on-demand request, but node C does not know the route of node A. When node A sends data message to node C via node B routing, node C will add

node B to the routing item to node A. Before sending data to a node that is not recorded in the routing table, any node will request a route to a destination to its neighbor node on demand. This is typically used when a newly added node starts communicating with the concentrator agent, when one node has a network unreachable failure and the other nodes need to update the routing table. The following sections describe the detailed steps of address broadcasting and on-demand.

Destination	Next hop	Hops	Destination ID
0x00000001	0x00000004	3	3

Fig. 7. Node routing table

6.3.1 Address Broadcast Mode

(1) Launch of broadcast

The broadcast message initiated by the concentrator Agent contains three elements: < via address, source address, source serial number >. Where, the address of the source address is written to the concentrator Agent, and the source serial number is written to a set of increasing serial Numbers maintained by the concentrator initiating the broadcast to identify the order of the broadcast message. Fill the TTL according to the size of the broadcast and set the hops to 0.

(2) Broadcast reception

After the neighbor node receives the broadcast message of the concentrator Agent, it first checks whether the TTL is greater than 0. If it is greater than 0, it continues to check whether the address of the concentrator Agent node in the broadcast message is equal to the address of the concentrator to which it belongs. If so, it checks whether there is a route to the concentrator node in the routing table. If the routing table meets one of the following conditions: ① The routing table does not contain the node; ② The ID number of the node in the routing table is less than t the ordinal numbe in the message; ③ The ID number of the node in the routing table is equal to the ordinal numbe in the message, and the number of hops is greater than the number of hops in the message, the routing table is updated and the message is forwarded.

(3) Routing table update:

The address and ID of the source node in the received message are filled in destination node field and the serial number field of the destination node, the via node field in the message is filled in the next hop field, and the hops number in the message is added by one to fill in the hops field.

(4) Message forwarding:

When forwarding the message, fill the node address into the via node field, and subtract 1 from TTL and add 1 to the hop number.

The solid node is the concentrator Agent with address D, and the hollow node is the collector Agent with addresses A, B, and C respectively (see Fig. 8). Nodes directly connected by solid lines are neighbor nodes. In the figure, A, B and C are neighbor, C and D are neighbor, while A,B and D are not. Address broadcast is initiated by concentrator Agent node D, and the serial number of broadcast is 1. The arrow in the figure shows the propagation path of the address broadcast. The address broadcast issued by A and B is omitted. When broadcast to all reachable nodes in the network, each node caches the next hop path to D in the routing table. Node C can directly transfer data to Node D, while nodes A and B will transfer data to node C, which will then transfer data to node D. After the broadcast, Node D is not aware of the existence of other nodes. Only when other nodes initiate communication to node D, can node D establish a reverse route by passive acquisition.

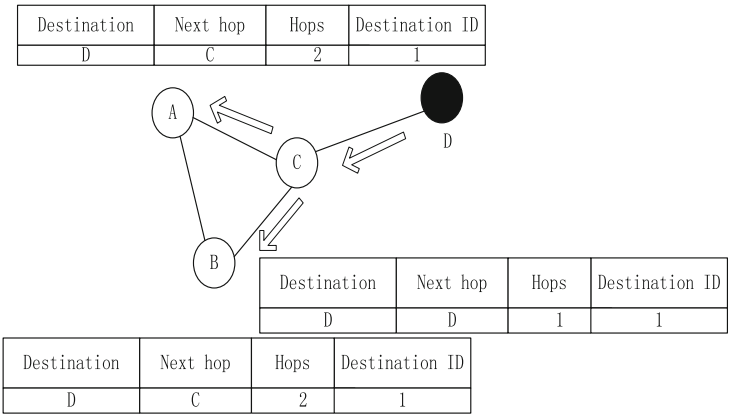


Fig. 8. Address broadcast mode

6.3.2 Request on Demand

(1) Initiate routing request

Routing request message contains five elements: via node address, source node address, source node serial number, destination node address, and destination node serial number. The node that initiates the routing request fills the address of the node into the address field of the source node and the address field of the routing node, fills the address of the destination node into the address field of the destination node, and fills the self-increasing ordinal number maintained by the node into the ordinal number field of the source node. The destination node field fills in the latest serial number of the known destination node. If the destination node has never been found by the node, fill in -1.

(2) Processing of routing requests

The node receiving the routing request message first determines whether the TTL of the message is 0. If not, it continues to determine whether the message is sent by the node itself. If not, detects whether it has received a request containing

the same source node address and source node number in a certain time◦ if not then check if the nodes in the routing table and orderly, is greater than the packet destination node in the serial number of the record, if any, is issued a response message routing, if not then start the timer, and set up a in the routing table for packet source node as the destination node in routing record, will jump under the node address fill in the address field, will jump Numbers to add 1 in the packet, fill in the jump number, from the source node number fill in the destination node number field. After completing the routing table, the node fills its serial number into the routing field of the received message, and forwards the message after subtracting 1 from TTL and adding 1 to the hops.

(3) Initiate routing response

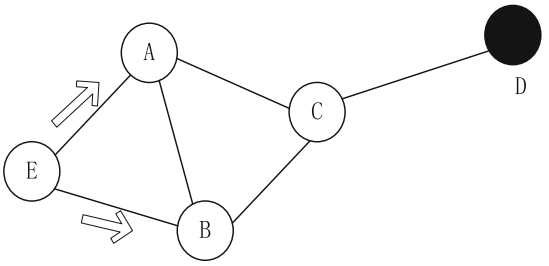
When a node receives a valid routing request message, if the node is the destination of the request or the routing record of the request node is in the routing table of the node, and the node ordinal number in the record is greater than that in the request message, then the routing response message is issued. The node sending the response fills the destination address and serial number in the request message into the address and serial number fields of the source node in the routing response message, fills the address of the node itself into the address field of the routing node, fills the hopping number into the hopping number section, and fills the address of the originating node in the routing request message into the address field of the destination node. The via node address is filled in the forward node field, the source node address is filled in the destination node address field, and the TTL value is reset.

(4) Processing of routing response

The node receiving the routing response message checks whether the TTL value in the message is 0. If not, it continues to check whether the current node matches the destination node in the message. If it is, and the serial number of the source node in the message is greater than that in the routing table, then the address of the source node, the serial number of the source node, and the address of the routing node in the response message are updated into the address of the destination node, the serial number of the destination node, and the address of the next hop in the routing table respectively, and the number of hops is added by 1 to fill in the hopping number segment. If the destination node address of the received message does not match the address of the current node, check whether the address of the node itself matches the forwarding node field in the message. If so, update the routing table and fill the forwarding node address field with the next-hop node address of the routing item in the routing table. Fill its address into the via node field, subtract 1 from the number of hops and TTL, and then forward the response message.

New node E joins the existing network. Where A, B, C and D are nodes in the existing Agent network (see Fig. 9). After running for A certain time, A, B, C and D have all learned the next hop route to other nodes in the network. Only the routing tables of Nodes A and B that are directly connected to E are listed in the figure. Node E broadcasts routing requests to node D to neighboring nodes. Since node E knows nothing about node D, the destination node in the request message is numbered −1.

Destination	Next hop	Hops	Destination ID
D	C	2	2
B	B	1	2
C	C	1	2



Destination	Next hop	Hops	Destination ID
D	C	2	2
A	A	1	2
C	C	1	2

Fig. 9. Request on demand

Since routing entries to D are in routing tables of A and B, and their Ordinal Numbers are greater than −1, both A and B will issue routing response to E (see Fig. 10). Since the number of hops to D in both A and B routing tables is 2, and the last known Node D saved in the routing table also needs to be the same, node E will update the information in the response message that arrives first into the routing table, ignoring the information in the message that arrives later.

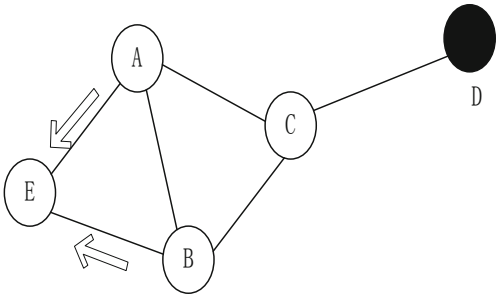


Fig. 10. Node E update routing table

7 Conclusion

This paper combines LoRa wireless networking technology and FMCOS-SE security module into the meter reading system to implement an Ad hoc network water meter collection and reading system based on multi-agent. This system combines the advantages of the current mainstream wireless meter reading technology, and has the characteristics of low deployment cost, low power consumption and strong scalability. This system adopts a highly modular design, which can be widely used for the collection and monitoring of various meter data such as user electric meters, water meters, gas meters, etc. This system provides a basic IoT perception layer for smart water services, provides accurate water data for water management, obtains all available information such as water quality at any time, achieves water saving and energy saving goals, and better manages water supply and drainage facilities throughout, Improve the efficiency of asset operation and maintenance management, promote the modernization of city management, and accelerate the construction of a "smart city".

Acknowledgments. This work was funded by Natural Science Foundation of Fujian Province (Grant Number 2021J011221);

Conflict of Interest. The authors declare that they have no conflict of interest.

References

1. Yin, J., Wei, L., Sun, H., et al.: An incentive mechanism for mobile crowd sensing in vehicular ad hoc networks. J. Transp. Technol. **12**(1), 15 (2022)
2. Shen, X., Li, C., Li, M., Feng, Y.: Design and implementation of wireless ad hoc smart metering system for power quality. Int. J. Sci. **3**(12), 84–90 (2016)
3. Sajan, R.I., Christopher, V.B., Kavitha, M.J., et al.: An energy aware secure three-level weighted trust evaluation and grey wolf optimization based routing in wireless ad hoc sensor network. Wirel. Netw. **28**(4), 1439–1455 (2022). https://doi.org/10.1007/s11276-022-02917-x
4. Muntean, M.V.: Multi-agent system for intelligent urban traffic management using wireless sensor networks data. Sensors **22**, 208 (2021)
5. Qin, J., Fu, W., Gao, H., et al.: Distributed k-means algorithm for sensor networks based on multi-agent consensus theory. IEEE Trans. Cybern. **47**(3), 772–783 (2017)
6. Alsboui, T., Qin, Y., Hill, R., et al.: An energy efficient multi-mobile agent itinerary planning approach in wireless sensor networks. Computing **103**, 2093–2113 (2021)
7. Xu, B., Lu, M., Zhang, H., et al.: A novel multi-agent model for robustness with component failure and malware propagation in wireless sensor networks. Sensors **21**(14), 4873 (2021)
8. Qi, M., Pan, J., Song, S.: The design of user meter reading system based on ZigBee and GSM. In: 2020 12th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA) (2020)
9. Lil, Y., Yan, X., Zeng, L., Wu, H.: Research on water meter reading system based on LoRa communication. In: IEEE International Conference on Smart Grid and Smart Cities, vol. 248–251 (2017)

10. Kumari, P., Mishra, R., Gupta, H.P., et al.: An energy efficient smart metering system using edge computing in LoRa network. IEEE Trans. Sustain. Comput. **PP**(99), 1 (2021)
11. Wu, Y.H., Zuo, R.J., Jiang, H.: The two-level group network meter reading system based on SX1278. In: Proceedings of SPIE International Conference on Optical Communications and Networks, vol. 11048 (2019)
12. Bai, K., Chuankun, W.: A secure white-box SM4 implementation. Secur. Commun. Netw. **9**(10), 996–1006 (2016)
13. Hu, X., Qin, X., Mou, H.: Secure measuring and controlling methods embedded SM4 algorithm for smart home. In: Deng, Z., Li, H. (eds.) Proceedings of the 2015 Chinese Intelligent Automation Conference, vol. 336, pp. 179–187. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46469-4_19