Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/090338

Virtual Token Passing Protocol Applicable to Manufacturing Sensor Networks

Ping Ren∗

Science and Technology on Electromagnetic Compatibility Laboratory, China Ship Development and Design Center, 430064 Wuhan, China

Received: 8 Aug. 2014, Revised: 9 Nov. 2014, Accepted: 10 Nov. 2014
Published online: 1 May 2015

Abstract: In this paper, a virtual token passing protocol has been proposed, in which sensor nodes join in the different subnets according to the received signal strength and the number of sensor nodes in the subnet to decrease the transmitting power to reduce energy consumption as far as possible. Secondly, router nodes adopt different RF to polling for new sensor node and neighboring subnets use different channels to realize internal communication, and this can not only improve the network capacity, but also reduce the interference between subnets and sensor nodes. Thirdly, the address of sensor nodes in subnet is allocated by the router in a unified way. By making full use of the continuity of address and the negotiation mechanism, sensor nodes impartially access the wireless channel according to the virtual token passing method, and this has greatly reduced the effect on network performance brought by token passing and maintenance. In addition, the introduction of node priority and second competition state make the higher sensor nodes have priority to access wireless channel and then send packet as soon as possible, and this will enhance the real-time performance and reliability further when there is an emergency happened. OPNET simulation experimental results show that the proposed MAC protocol has improved the throughput, increased the traffic load, decreased the network delay, reduced the amount of dropped packets and the wireless channel access delay, and this is of great importance to the wireless sensor network under manufacturing environment.

Keywords: Virtual token passing, Negotiation mechanism, Manufacturing environment, Wireless sensor networks

1 Introduction

With the development of computer technology and wireless network, especially along with the rising of Internet of things, wireless sensor network has being widely used in manufacturing environment as its characteristic of flexibility and distribution. Manufacturing WSN(Wireless Sensor Network), as a kind of control network, has high demand on the real-time performance and certainty of network delay, while the wireless channel access mode has a great effect on them. CSMA/CA is the most popular wireless channel access protocol, because of random backoff strategy, which can not guarantee the maximum network delay. Token passing method although can well make up the shortage of CSMA/CA, but it is proposed for wired network and not suitable for large-scale wireless network. On the other hand, as the poor transmission quality of wireless channel, too much interference will increase the amount of management messages brought by token maintenance and aggravate the network performance. Consequently, research on the new MAC protocol applicable to manufacturing WSN is of great significance.

In WSN, CSMA/CA (Carrier Sense Multi Access/Collision Avoidance) is the most popular protocol used to access wireless channel in MAC layer. In order to reduce the opportunity of collision, sensor node has to monitor the wireless channel and can not send data until the transmission medium is still available after withdrawing a random period of time. In addition, RTS-CTS (Request to Send-Clear to Send) handshake mechanism can guarantee that collision will not happen during the process of data transmission. However, CSMA/CA can not satisfy the requirement of the sensor network under manufacturing environment, because not only RTS-CTS will bring extra cost and delay, but also random backoff will make the channel access delay became uncertain and can not guarantee the maximum transmission delay. What was worse is that the transmission delay will increase rapidly and the network throughput will decrease sharply along with the

∗ Corresponding author e-mail: rp-2003@163.com

increasing of network traffic load and collision. Consequently, it is of great significance to propose a new kind of wireless channel access protocol which can guarantee the real-time performance.

Ye W, et al proposed S-MAC[1](Sensor Medium Access Control) protocol based on CSMA/CA, which adopts periodic monitoring/sleep method to reduce the energy consumption, but this will increase the network delay and decrease the throughput; Dam T V and Langendoen K proposed T-MAC[2](Timeout MAC)based on S-MAC, by introducing a TA slot time, which has reduced the idle monitoring time; Zheng T, et al proposed P-MAC[3](Pattern MAC) protocol based on S-MAC and T-MAC to adaptively adjust the sleep time according to the flow model and traffic load, which is hard to realize and has a high demand on sensor nodes hardware; Jamieson K, et al proposed Sift MAC[4]protocol based on event-driven and contention window mechanism, which is strict with clock synchronization and only suitable for part sensor network. From the analysis above can be seen that the CSMA/CA can not be used directly in manufacturing WSN.

IBM proposed a token ring network at 1980s, token is used to access transmission medium. Because token is passed orderly on the logical ring, and the access rights is impartial to all nodes, so it has a good performance when the traffic load is relatively heavy. The maximum delay of token passing can be estimated in advance and has some certainty, while the real-time performance can be further improved by adjusting the number of nodes in the token ring and the passing order or the number of frames can be sent when holding token, so it is suitable for the applications having high demand on real-time performance or demanding certainty on network delay. Form the analysis above, token has a great advantage in wired network, but it is hard to be applied to access wireless channel directly as the characteristic of wireless network, especially for the sensor network whose resources are restricted, the main reasons are shown as follows:

(1) The transmission condition of wireless channel is complex and adverse. The signal is not transmitted by a single path in wireless channel, and it is consisted of many reflected waves from multiple transmission paths. The different distance of various paths will result in their difference of arrived time and phase. Different-phase signals overlying will make the signal latitude change sharply and then result in fast fading; while the change of geographic position and meteorological condition will lead to slow fading; the frequency shifting brought by the mobility of sensor node require that we have to take the Doppler Effect on wireless communication into consideration; the openness of wireless channel will make it is more variable to the interference from other communication systems, it is more obvious especially when their frequencies are same and more or less; at the same time, obstacle will make the wireless signal fade rapidly and it is good at absorb long or short wave and high frequency signal. In summary, when compared with the stabilization of wired signal and the reliable transmission environment, the transmission condition of wireless signal is very complex and adverse, and it is highly variable to the environmental factors.

(2) The cost of token maintenance is huge, while the sensor node has restricted resources and needs to reduce the number and size of wireless frames. In order to make the token ring runs normally, maintain token well is the key point. Token maintenance consists of token generation, token passing, multiple token and token lost detection, polling for new station and so on. It is needed to generate a token according to a specific rule at the time of system initialization and when the token passing failed or the station received token invalidated; if there is an error happened during the communication or the process has not been coordinated well, maybe there are multiple tokens on the logical ring and result in collision, so every station has to detect the happening of this phenomenon in time and only reserve one station holding token or all stations give up token and then generate a new token. The station has to pass the token to the next station if has use token done or has no frame needed to send when holding token, and then the token can be passed circularly on the logical ring to make every node can access the transmission medium impartially; if the next station failed as fault or other reasons, it is needed to polling for a new next station; when token has been passed for a certain number of times, it is needed to polling the whole network to detect whether there are new stations waiting for joining in. From the analysis above can be seen that, the token maintenance is very complex and has a huge cost, and the traditional token ring can not be used directly for the sensor network and such restricted resources systems.

(3) The transmission condition of wireless channel is not very good, and this will aggravate the cost of token maintenance and make the radio of management messages in the whole messages increased, not only decrease the network traffic load, but also interrupt the transmission logical process frequently, and this will lead to uncertainty in access delay and waiting for service delay of sensor node. Consequently, the advantage of token ring in the aspect of real-time performance and traffic load will be weakened especially when the number of nodes is big and the traffic load is heavy. If there is an error happened in token passing and make the token can not been passed correctly to the next station and result in token lost, the station will send token again, if token passed successfully this time, maybe there are multiple tokens on the logical ring; if token passed unsuccessfully again, may be considered that the next station has quitted the logical token ring as failure or change of position, and this will easily lead to communication confusion and reliability decreasing. Token occupies the absolutely important position in the token ring network, the number and frequency of token passing are rather high, so there is no token or there are multiple tokens on the logical ring

will make the sensor node can not send frame or produce collision, while retransmission not only increase the end-to-end delay, but also decrease the network efficiency. Consequently, token ring can not be used directly in sensor network.

In this paper, a virtual token MAC protocol has been proposed according to the characteristic of manufacturing WSN and the nested cellular topology structure. The idea of the MAC protocol is that: make full use of the advantage of router node acting as a central node in subnet, virtual token is used to access wireless channel, namely the token is not truly exist, and this will reduce the risk of token lost and simplify the token maintenance; at the same time, control information is added to data frame by using integration method, and this will decrease the number of wireless frames and reduce the feasibility of error happened during transmission. In addition, the introduction of the second competition before token passing can satisfy the requirement of higher priority node, and improve the real-time performance and reliability, as well as provide extendibility for this MAC protocol.

At the time of system initialization or token lost, router broadcasts a control frame to appoint a sensor node to hold token, if the sensor node has no frame needed to send, and then broadcasts a frame to show that it has use token done; if the sensor node has sent a number of frames, and then adds a send frame done flag bit to the last frame, the next node begins to hold token when received this frame, so the token is passed according to the negotiation mechanism. Because the addresses of sensor nodes are allocated continuously in a unified way by the router, so the token is passed orderly in the light of address. Sensor node or router begins to monitor network after appointing address for node that is gong to hold token to ensure token passing successful. If the sensor node quits the subnet as energy exhausting or its fault, and then the previous node can not detect that the sensor node begins to use token and broadcasts a frame to make other nodes update the number of sensor nodes in subnet, and the sensor nodes whose addresses are bigger than that of the exit node have to update their addresses to keep the continuity of address in the whole network. Router node detects periodically whether there are new nodes waiting for joining in the subnet, while the router uses different RF and channels to polling for new sensor node, and this will not affect the virtual token passing in subnet and increase the number of management messages. When the router has detected that there is a new node joins in the subnet, and then allocates address and adds it to the logical virtual token ring, as well as broadcasts its information to other nodes and makes them update the number of sensor nodes in the subnet.

2 Protocol descriptions

2.1 State machine of sensor node

The state machine of sensor node is shown in figure 1.

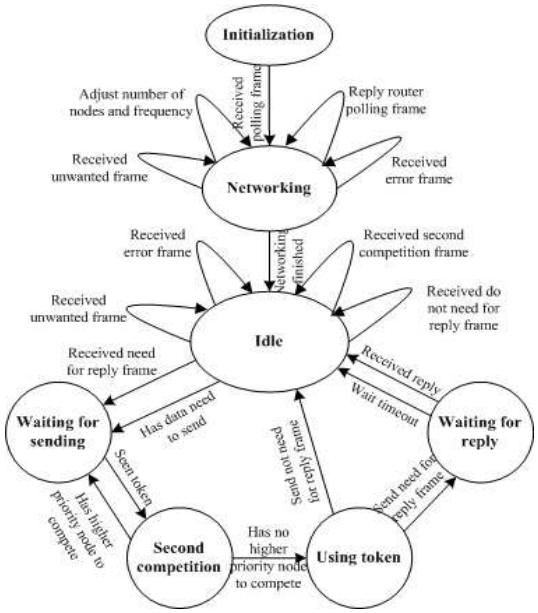

Fig. 1: State machine of sensor node

The state machine consists of seven states: Initialization, Networking, Idle, Waiting for sending, Second competition, Using token and Waiting for reply. Initialization is mainly responsible for parameter setting of sensor nodes software and hardware and memory space allocation, this is the first state sensor node enters into after power on. Networking is in charge of choosing router for sensor node according to the received signal strength, geographic position, and the number of sensor nodes in subnet, and then the sensor node joins in the subnet in which the router acting as a transmitting node. Idle is the default state when sensor node has chosen a neighboring router as its central node, and then determines to enter into which state according to the received frame and other conditions. Waiting for sending is the state in which sensor node has data needed to send or received a need to reply frame when holding no token. Second competition is an especially introduced state after the previous node has use token done and before the next node begins to use token, which is aim at the sensor network under manufacturing environment, such control network has a high demand on real-time performance. It is very effective to prevent timeout from happening as waiting for token and then prolong the waiting for service delay when sensor node has emergent frame needed to send, and reduce the threat to the safety of manufacturing

environment. Token using is the state in which sensor node sends data on its own initiative when holding token and having no higher priority sensor nodes participating in wireless channel competition. In waiting for reply, sensor node has sent a need to reply frame and then waits for reply from the destination node.

At the time of system initialization, all sensor nodes work at the same fixed frequency, router nodes send polling frames in a certain interval to search the neighboring sensor nodes, and then add them into the subnet in which they act as central nodes. Sensor node begins to receive polling frame when it has finished initialization. If sensor node has received polling frame and does not received it from other routers in the coming specific time, this shows that the sensor node is only covered in the communication range of one router. If sensor node has received multiple polling frames from different routers simultaneously, this shows that there are multiple routers in the communication range of this sensor node. Sensor node chooses one router of them as its central node according to the signal strength of router and the number of sensor nodes in the subnet, then joins in it by replying the received polling frame, and switches to the communication frequency of the subnet. Consequently, the networking process has finished.

If sensor node has received a frame not sent to itself in networking state or received an error frame, this shows that there is an error happened during the communication, and then drops the frame and stay in networking state. Sensor nodes enter into idle when finished networking, if received do not need to reply frame, and then process the frame and stay in the state; if received second competition frame, not belong to this node frame or error frame, and then drop it and stay in the state; if received a need to reply frame or need to send frame initiatively, and then enter into waiting for sending state, if found that the previous sensor node has use token done, this shows that the node should hold token and enter into second competition state to avoid there are sensor nodes having high priority frames waiting for sending; if do not received second competition frames from other sensor nodes in specified time, and then the sensor node can use token to send data; if there are higher priority sensor nodes participating in wireless channel competition, and then pass the token to the highest priority sensor node; if there are more than one higher priority sensor nodes participating in wireless channel competition simultaneously, the token should be passed orderly between them to ensure that the emergent messages can be sent out as soon as possible; if sensor node sends a need to reply frame, and then enters into waiting for reply state, if received need to reply frame ACK or waiting for reply timeout, and then return to idle state, other wise enter into idle state.

The proposed virtual token MAC protocol has been well realized by the above seven states and their shift between them. The most important characteristic of the MAC protocol is that which can not only guarantee the maximum network delay, but also the sensor node can hold token to gain the usage rights of wireless channel as soon as possible when there is emergency happened. Consequently, the high priority frames can be sent out preferentially and timely as far as possible, and this is of great significance to the control network. In order to realize this goal, priority mechanism of sensor node and second competition state have been introduced. Generally speaking, all sensor nodes are in the same priority, they access and possess wireless channel impartially. If one sensor node has emergent message needed to send, and then promote it to be the highest priority dynamically, this makes that the sensor node can send second competition frame to hold token and then send frame when the next station enters into second competition state after the sensor node has use token done. If there is more than one sensor nodes need to send emergent messages, they hold the virtual token and then send frames orderly. Consequently, the proposed MAC protocol has a good real-time performance and reliability, while the introduction of second competition state can not only solve the problem that the emergent messages can not be sent out timely in normal token ring network, but also provide extendibility for the MAC protocol, and make full use of this state to realize dynamically token passing in subnet and adaptively bandwidth allocation.

2.2 Token passing and maintenance

The proposed MAC protocol dose not use real token to access wireless channel, but broadcasts management information using the advantage of router acting as a central node and updates the addresses of sensor nodes in subnet dynamically to keep their continuity, to realize a similar token passing network by negotiating and competing between sensor nodes, this will reduce the cost of communication and computing brought by token maintenance as far as possible, it is very important to the wireless sensor network whose transmission medium is complex and unstable. On the other hand, the maximum wireless channel access delay of sensor node can be guaranteed, and it has a high real-time performance and the capability to deal with burst data.

(1) Token passing

In the traditional token ring network, the token is commonly passed according to the order of station address. When the station holding token has no data needed to send or has sent specified number of frames, the token has to be passed to the next station, so the token is passed circularly on the logical ring orderly. With regard to wired network, because the transmission medium is reliable and stable, this kind of token passing method has a good performance, but when it comes to wireless network, it is easily lead to token lost or been retransmitted for multiple times, the network performance will be effected consequently. The proposed MAC protocol makes full use of star and ring mixed network

topology structure and allocates address when there is a new sensor node joins in subnet, the address scope is from 1 to 127, while 0 will be allocated to the router. When some sensor nodes leave the subnet, the sensor nodes whose addresses is bigger than that of the exit node will subtract 1from their addresses respectively to ensure the continuity of address. The router broadcasts a frame to inform other sensor nodes that the number of sensor nodes has changed.

At the time of subnet initialization, the router whose address is 0 will hold token and send data firstly, it will set the flag bit to show that the sending process has finished when sending the last frame. If the router has no data needed to send and then sends an empty frame containing flag bit. When number 1 sensor node monitored flag bit, it is able to hold token and begins to send data if there is no higher priority sensor nodes competing wireless channel in specified time, and then deal with the token according to the same way with the previous node when the token has been used done. Other sensor nodes will act like that to finish the token passing between them. By keeping the continuity of address and monitoring the token using status of the previous sensor node, as well as the second competition, this negotiation mechanism has reduced the sending times of token frame and the risk of token lost due to the transmission quality of wireless network, consequently decreased the effect on network performance brought by token retransmission, token lost and token generation.

(2) Token generation

In the proposed MAC protocol, the token is always generated by the lowest sensor node, namely it will be generated by the router all the time to ensure that it is impossible to be generated by more than two sensor nodes at the same time. The router is the first station of token passing and be in the same place with sensor node in this sense. As central node of the subnet, its invalidation means the invalidation of the whole subnet.

(3) Token lost detection

If there is a communication error when the sensor node holding token sends the last frame or sends an empty frame containing specific flag bit when there is no frame needed to send, and then the next sensor node can not detect that the previous node has use token done, and this will result in token lost. The previous sensor node resends an empty frame containing flag bit and then monitors network, if the next sensor node has began to send data and this shows that the token has been passed successfully, if there is still no data monitored on the network when resending specific times of empty frame and this shows that the next sensor node has left the subnet because of fault or change of geographic position and transmitting power, and then report this situation to the router. When the router received this message, it broadcasts a frame containing the address of the exit sensor node, the sensor nodes in the subnet whose address is bigger than that of the exit node subtract 1 from their address and then update the number of sensor nodes in the subnet.

2.3 Parameters definition

(1) Frame format

The frame format is shown in figure 2. The frame format is composed of frame head, source address, destination address, data length, data, flag bit and frame tail. Frame head and tail can be adjusted flexibly according to the application background. Frame head commonly includes preamble synchronous code, and frame tail consists of parity bit, encryption information and so on, while the flag bit is used to indicate that whether the token has been used done.

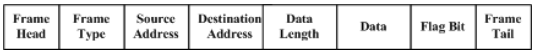

Fig. 2: Frame format

(2) Frame type

I have defined the following wireless frame types:

1) *Polling_for_Sensor_Node*, which is sent out by router periodically and used to add sensor nodes moving to the edge of router or new power on sensor nodes to the subnet. This frame includes the number of sensor nodes in subnet, communication frequency, and wireless signal strength and so on, and provides basis for sensor node to choose an appropriate subnet when it is covered in the range of multi-routers;

2) *Need_to_Reply_Frame*, when sensor node or coordinator has high priority data needed to send, and then it is needed to send this frame to ensure that whether the destination node has received the frame correctly;

3) *Do_Not_Need_to_Reply_Frame*, when sensor node or coordinator has normal priority data needed to send and the drop of the frame will not affect the system heavily. In order to decrease the traffic load of network and save the energy of sensor node, it is needed to send this frame;

4) *Token_Use_Done*, if there is no frame needed to send when sensor node holding token, it is needed to send this frame to inform the next station or router and then give up holding token, and this will gain opportunity and authority for the next sensor node;

5) *High_Priority_Node_Compete_Medium*, when some sensor nodes have emergent messages needed to send, which can send this frame to compete the wireless channel for the second time before the token has been passed to itself when the previous station has use token done;

6) *Polling_for_Sensor_Node_ACK*, when sensor node enters into networking state after finishing initialization, and then chooses a appropriate router according to the number of sensor nodes and signal strength in the

received polling for sensor node frame, and sends this ACK frame to switch channel and join in the subnet;

7) *New_Sensor_Node_Join_Subnet*, when sensor node monitors that a new node has joined in the subnet and then broadcasts this frame including the address of this sensor node, and other sensor nodes update the number of sensor nodes in the subnet;

8) *Sensor_Node_Quit_Subnet*, when some sensor nodes quit the subnet as the change of location or their fault, and then broadcast this frame including the address of the exit node, while other sensor nodes will update the number of nodes in the subnet. In addition, in order to maintain the continuity of address, the sensor node whose address is bigger than that of the exit node will subtract 1 from its address;

9) *Subnet_Die_Out*, when the number of sensor node in some subnet is less than the minimum threshold, and then the subnet loses the necessity of existing. By sending this frame, the sensor nodes in this subnet can join in other neighboring subnets to save the channel resources and improve network efficiency;

10) *Need_to_Reply_Frame_ACK*, by sending this frame to reply the need to reply data frame and then establish a handshake between the source node and the destination node to guarantee a reliable communication.

(3) Variables definition

In order to realize the proposed MAC protocol and complete its defined functions, we have defined the following variables:

1) *T*S(This Station), the address of sensor node in subnet;

2) *N*S(Next Station), the address of the next station of token passing;

3) *P*S(Previous Station), the address of the previous station of token passing;

4) *Nnumber_of_Sensor_Node*, the number of sensor nodes in subnet, which will be updated instantaneously according to the information collected from router;

5) *Ffrequence_of_Subnet*, the communication frequency of sensor subnet, which is assigned by the coordinator in a unified way when the establishment of subnet. Sensor node switches to the channel of the subnet when finished networking to ensure that the sensor nodes in the subnet can communicate directly with each other;

6) *Tpoll_for_Sensor_Node_Interval*, the interval of router polling sensor node, which can be adjusted dynamically according to the movement speed of sensor node and single hop distance, its default value is 50ms;

7) *Ntoken_Retry_Times*, the maximum times of token retransmission, when the router or sensor node uses token done and then has to pass token to the next station, this variable shows the maximum retry times if failed, its default value is 3;

8) *Twait_for_Token_Use*, the maximum delay to determine whether the token has been passed successfully, the router or sensor node starts to monitor the network after passing token to the next station, if there is no data monitored on the network in the time defined by this variable shows that the token passing failed. Its value is 30ms and can be determined dynamically according to the processing speed of sensor nodes processor and the time of transceiver needed to send data;

9) *Thigh_priority_Request_for_Medium*, the maximum delay of wireless channel competition when the sensor node seen token and has data need to send, if there is no other higher priority sensor nodes to complete the wireless channel in the time defined by this variable, and then the station holding token begins to send data. Its default value is 20ms and can be adjusted dynamically according to the processing speed of sensor nodes processor and the time of transceiver needed to send data as well, but it has to be less than Twait_for_Token_Use;

10) *Nmaximum_Frame_Send*, the maximum number of frames sensor node can send when holding token, which should be determined by the traffic load of sensor node and its interval of generating frame, if the value is too big will prolong the time of token passing for a circle and increase the wireless channel access delay of single node, if the value is too small will easily lead to the token passing for non-data when the sensor nodes network traffic load is heavy and distributed unevenly to reduce the network performance, its default value is 1;

11) *Twait_for_Time_out*, the maximum delay sensor node needs to wait for reply after sending a frame needed to reply, if over this value and then regard as timeout. Its default value is 200ms and need to be adjusted according to the average end-to-end service delay in specific network to realize optimal performance, if its value is too big will make the sensor node waits for too long time, while if its value is too small maybe received the reply frame after regarding as timeout to reduce the network reliability and efficiency;

12) *Twait_for_Another_Poll_Frame*, the maximum delay of waiting for polling frame from other routers when sensor node received polling frame from one router. This variable is mainly designed to avoid the interference caused by neighboring sensor nodes when networking and choosing, because the polling interval of every router is same and sensor node maybe received the poling frame from the further router and this is not good for network optimization, its default value is 70ms and can be adjusted slightly according to the network condition to ensure that there is enough time to receive other polling frames and do not receive repeatly polling frame from the same router.

2.4 Advantages of the proposed protocol

In this proposed MAC protocol, sensor nodes have been divided into three priorities according to the emergency degree of the waiting for being sent messages: normal, important, emergent. The priority of sensor node is determined by the emergency of messages and they can transform between each other, the goal of that is to ensure the high priority messages can be sent out as soon as

possible, and this is be of great practical significance to the sensor network under manufacturing environment.

(1) When compared with CSMA/CA protocol, this protocol has the characteristic of certainty in the aspect of network delay, especially when the network traffic load is heavy; it has a good performance and can well satisfy the real-time requirement of manufacturing network. If ignoring the transmission time and processing time of wireless packet, then the maximum network delay has the following inequality,

$$Tmaximum\_Delay\_Time \leq Ntoken\_Retry\_Times * Twait\_for\_Token\_Use + Thigh\_priority\_Request\_for\_Medium$$

It can be seen from this that, the maximum network delay can be controlled in about 100ms and has a high performance;

(2) When compared with normal token ring network, this protocol has decreased the complexity of token maintenance, and can better adapt the characteristic of wireless link and satisfy the requirement of restricted resource of sensor node;

(3) When compared with wireless token ring network, this protocol has effectively prevent the network performance from decreasing brought by the frequently updated token passing order, which is due to the failure of token passing as the location movement of sensor nodes;

(4) By introducing the second competition mechanism before the next node using token, and combining the priority hierarchy of sensor node, the emergent messages can be sent out in time as far as possible to guarantee the high reliability and real-time performance of network;

(5) Sensor node joins in the network is completed by the other wireless channel and RF transceiver of router, this has effectively reduced the huge cost of the periodical polling new sensor node and can better reduce the effect brought by the change of topology structure as the location movement of sensor node.

3 Simulation experiments and results analysis

In order to validate the feasibility of the proposed protocol and evaluate its network performance, we make a set of simulation experiments adopting different MAC protocols under the same network condition in OPNET, and then contrast their network performance[5]. By analyzing the experimental data, it can be got that whether there is an improvement in network performance from different aspects and their amplitude, and this is be of great significance to further adjust and optimize the network parameters.

3.1 Simulation model

According to the characteristic of the proposed MAC protocol and the present condition of the wireless sensor network, we have made a set of simulation experiments adopting three MAC protocols: WTRP (Wireless Token Ring Passing), Sensor network based on CSMA/CA and virtual token protocol, and then analyze their network performance from throughput, wireless access delay, traffic load, network delay and amount of dropped data. The network simulation parameters are shown in table 1.

Table 1: Network simulation parameters

Number of sensor nodes	10	**Simulation time**	1200s
Number of router	5	**Number of protocols**	3
Number of RF on router	2	**Number of channels**	16

Assume that the sensor node has a weak mobility and every sensor node can always communicate with one neighboring router directly at least, the sensor node will not fail during the simulation process. Every router node adopts two wireless transceivers simultaneously. One of them is used to communicate with the sensor nodes in subnet, and the other one is responsible for sending data from subnet to the coordinator directly or by other routers. The simulation environment of virtual token passing, CSMA/CA and wireless token ring protocol is shown in figure 3.

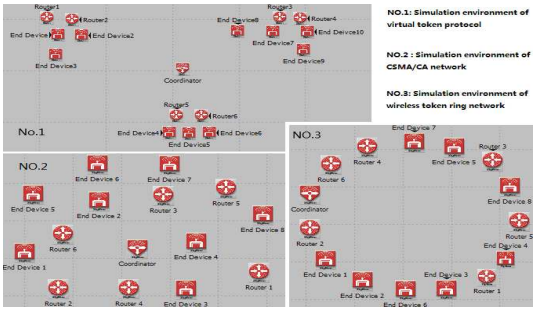

Fig. 3: Simulation environment of virtual token protocol

OPNET[6] is a large-scale communication and computer network simulation software developed by OPNET Technology Company in United States. Modeler provides a wide range of editors to help users to accomplish network modeling and simulation.

3.2 Results analysis

(1) Comparison of throughput between three MAC protocols is shown in figure 4.

It can be seen from the figure that, the fluctuation of MAC throughput of them is relatively small and keeps at a same level. When adopting CSMA/CA, its MAC

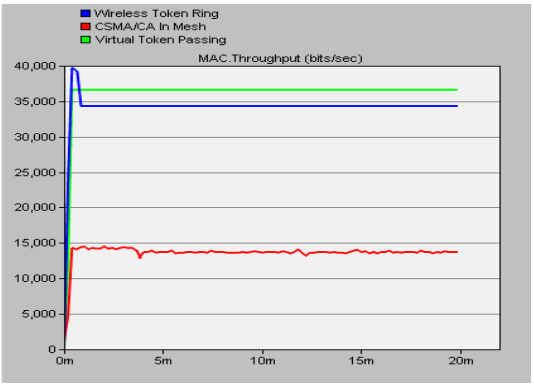

Fig. 4: Comparison of throughput

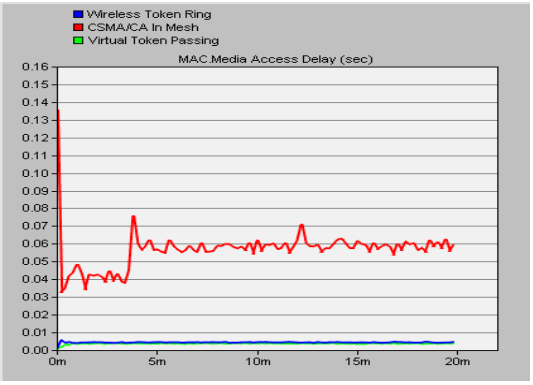

Fig. 5: Comparison of media access delay

throughput is smallest. The throughput of wireless token ring and virtual token passing network is same and double that of CSMA/CA. It is caused by the following reasons: CSMA/CA adopts single handshake and random backoff strategy to realize the access control of wireless channel, not only has increased the uncertainty of network delay, but also sensor node can not send data when there is collision happening, especially when there are more sensor nodes being in the single hop communication distance, the chance of collision will get bigger and the situation will be more obvious. On the other hand, the more times of collision happening, the longer backoff time, and this will decrease the duty ratio and reduce the network throughput heavily; Wireless token ring network uses token to access wireless channel, in which sensor nodes send data according to the order of token passing in sequence, and effectively avoid the happening of collision and the random backoff delay brought by this to improve the networks duty ratio and throughput; (3) Virtual token passing protocol has reduced the computing complexity and communication traffic by consultation mechanism of continuous address and topology structure which is similar to star network, not only has the advantage of wireless token ring, but also reduced the amount of network management message. Consequently, virtual token passing protocol has a good network performance. It has increased the duty radio as the reduced network delay by avoiding collision each other, and reduced the amount of network management message evidently through consultation mechanism between sensor node and router node.

(2) Comparison of media access delay between three MAC protocols is shown in figure 5.

It can be seen from the figure that, the sensor network using CSMA/CA has a maximum access delay and comes through a obvious jump, while the access delay of wireless token ring and virtual token passing network are almost same, and the latters change process is merely more stable. The jump of delay is caused by the following reasons: when it comes to CSMA/CA, because of the different sensor nodes power on time and their discrepancy in capability, there is not much nodes sending data simultaneously and the competition or collision is small relatively at the beginning of network initialization; When the network comes to steady gradually and enters into formal working state, many sensor nodes need to send data at the same time will lead to the sharply increasing of collision, in order to reduce the probability of collision, only have to withdraw longer time to prolong the time of node having wireless channel usage rights. While the latter two MAC protocols realize the access control of wireless channel through token, their channel access methods are same and only have a slight difference in token expression and passing method, but this does not affect the single nodes channel access delay. Even when some sensor nodes do not being in their communication radius each other, but the reduction of management message can well make up the extra delay caused by router transmitting token. Consequently, virtual token passing protocol has an advantage in the length of media access delay and stability, and this is mainly owing to the tokens certainty in media access delay and the virtual expression form of token.

(3) Comparison of MAC traffic load between three MAC protocols is shown in figure 6.

It can be seen from the figure that, the sensor network adopting CSMA/CA has a smallest network load; Wireless token ring network takes the second place and is probably 2.3 times that of CSMA/CA network; Virtual token passing networks traffic load comes to maximum and has a slight difference with that of wireless token ring, and that the traffic load of the three network shows linear distribution and parallels each other. It is caused by the following reasons: the main factors affecting network load consist of the wireless channel access delay of sensor node, the maximum service delay one packet can tolerate and the length of input queue. When the influencing factors are fixed, network traffic load has an approximately same trend with network throughput.

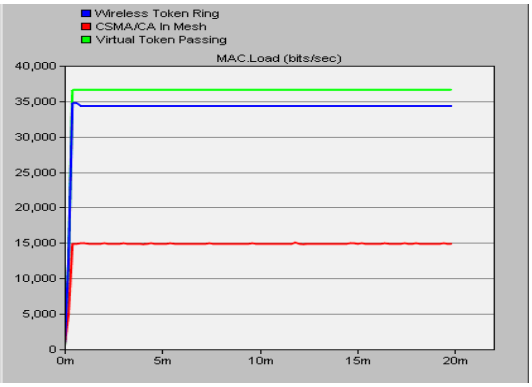

Fig. 6: Comparison of MAC traffic load

(4) Comparison of MAC delay between three MAC protocols is shown in figure 7.

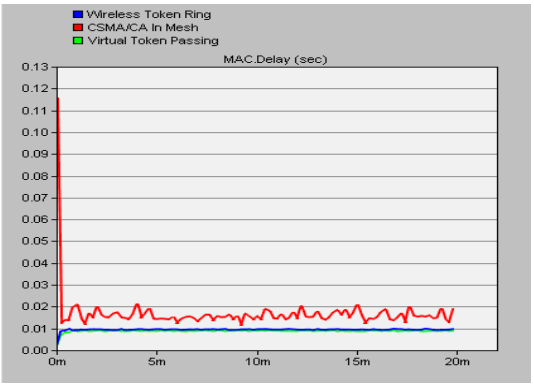

Fig. 7: Comparison of MAC delay

It can be seen from the figure that, at the beginning of network initialization, sensor network adopting CSMA/CA has a big pulse, when the network runs smoothly by degrees, its MAC delay keeps at a low value but fluctuates heavily; MAC delay in wireless token ring and virtual token passing network takes on a basically same trend and has improved the performance for about 50% when compared with CSMA/CA. It is caused by the following reasons: Sensor network is a self-organized and multi-hop communication network, it will take a long time to establish a reliable communication link between sensor nodes, while the moving of sensor node will lead to the change of network topology structure and make the network transmission delay being uncertainty; Wireless token ring and virtual token passing network make use of token to access transmission media, every sensor node uses wireless channel impartially and keeps a stability in the aspect of access delay; When compared with CSMA/CA, token protocol has reduced the network delay caused by single handshake and random backoff when encountering collision, so it has a good network performance.

(5) Comparison of dropped packet amount between three MAC protocols is shown in figure 8.

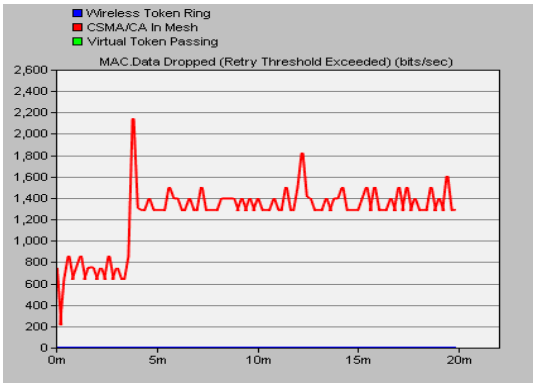

Fig. 8: Comparison of dropped packet amount

It can be seen from the figure that, the packet drop ratio of wireless token ring and virtual token protocol is very low, while the sensor network adopting CSMA/CA has a bigger packet drop ratio and present an obvious stability owing to the major jump. It is caused by the following reasons: wireless channel access delay in the network adopting token passing algorithm has a small value and be of predictability, when the network traffic load is not heavy, the packets can be sure to send out in the specified maximum network delay; CSMA/CA has a long wireless channel access delay as the introduction of random backoff strategy, especially when the traffic network load is relatively heavy, some packets has to be dropped because they can not be sent out in the specified time; CSMA/CA has a great uncertainty in the aspect of wireless channel access delay and result in the amount of packets having no service in unit time has a great fluctuation.

4 Conclusions

In this paper, we have proposed a MAC protocol based on virtual token passing mechanism. Network management cost as token maintenance has been reduced effectively by making full use of the advantage of router node as central node and the characteristic of node addresss continuity, as well as the introduction of token passing negotiation mechanism. OPNET simulation experimental results show that this MAC protocol has decreased the effect of wireless channel access delays uncertainty and satisfy the requirement of control networks maximum network delay when compared with CSMA/CA; on the other hand, the proposed MAC protocol has reduced the cost of management message and improved the use ratio

of wireless network when compared with regular token passing protocol, so it has a good network performance in the aspect of real-time and reliability especially, and be capable of meeting the requirement of the sensor network under manufacturing environment. Consequently, the proposed protocol has significant theory value and broad application prospect.

Acknowledgement

This work was supported by the Fund of the Key Laboratory of Science and Technology on Electromagnetic Compatibility.

References

[1] Ye W, Heidemann J, Estrin D. An energy-efficient MAC protocol for wireless sensor networks. In: Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies. New York, USA: IEEE, 15671576(2002).
[2] Dam T V, Langendoen K. An energy-efficient MAC protocol for wireless sensor networks. In: Proceedings of the 1st International Conference on Embedded Networked Sensor Systems.. California, USA: ACM, 171180(2003).
[3] Zheng T, Radhakrishnan S, Sarangan V. P-MAC: An adaptive energy-efficient MAC protocol for wireless sensor networks. In Proc. of the Parallel and Distributed Processing Symp. Piscataway: IEEE Computer Society, 237247(2005).
[4] Tae Rim Park, Myung J. Lee, Junehyung Park, and Jaehyun Park. FG-MAC: Fine-Grained Wakeup Request MAC for Wireless Sensor Networks, IEEE COMMUNICATIONS LETTERS, Vol.11 (No.12), 10221024(2007).
[5] Ping REN, A Nested Cellular Topology Applicable to Wireless Sensor Networks, ICCT2010, Nanjing, China, Nov.(2010).
[6] Min CHEN. OPNET Network Simulation. Beijing: Tsinghua University Press, 1216(2004).
[7] RANIWALA A, CHIUEH T C. Architecture and algorithm for an IEEE 802.11-based multi-channel wireless mesh networks [EB/OL](2008).
[8] Pradeep K, Vaidya NH. Routing and link-layer protocols for multi-channel multi-interface ad hoc wireless networks. ACM SIGMOBILE Mobile Computing and Communications Review, 3143(2006).
[9] Ahn GS, Miluzzo E. Funneling-MAC: A localized, sink-oriented MAC for boosting fidelity in sensors networks. In: Proc. of the 4th ACM Conf. on Embedded Networked Sensor Systems (Sensys 2006). Boulder: ACM Press, 293306(2006).
[10] BENENSON Z, et al. An algorithmic framework for robust access control in wireless sensor networks [A].2nd European Workshop on Wireless Sensor Networks (EWSN) [C].Istanbul, 15816(2005).

Ping Ren who was born in Sichuan province, China, in September 1982. He earned bachelor, master and doctor degree of engineering from Wuhan University of Technology, Wuhan, China in 2005, 2008 and 2011 respectively, and studied in Cardiff University, UK as a Joint-PHD student between 2009 to 2011, and work in China Ship Development and Design Center now. His major field of study is wireless industrial network.