WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. 2008; **8**:449–462
Published online 26 September 2006 in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/wcm.462

A load awareness medium access control protocol for single-hop wireless ad hoc networks

Chih-Min Chao[1*,†], Jang-Ping Sheu[2] and I-Cheng Chou[2]
[1] *Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan*
[2] *Department of Computer Science and Information Engineering, National Central University, Taiwan*

Summary

A contention-based wireless ad hoc medium access control (MAC) protocol, such as carrier sense multiple access with collision avoidance (CSMA/CA), has excellent efficiency when the system is light loaded. The main drawback of such protocols is their inefficiency and unbounded delay when the system load is heavy. On the other hand, a contention-free MAC protocol, such as token passing, has a better and fair throughput when the system is heavy loaded. The main drawback of such protocols is their inefficiency when only a small amount of users want to transmit. In this paper, we propose a new load awareness single-hop wireless ad hoc MAC protocol (which is called the *LA* protocol) that exploits the benefits of both contention-based and contention-free protocols. A contention-based MAC protocol is used when the system is light loaded and a contention-free one is used otherwise. Our *LA* protocol, which operates in a distributed fashion and is fully compatible with the IEEE 802.11 wireless local area network (WLAN) standard, can switch smoothly between the contention-based protocol and the contention-free one. Simulation results show that our protocol indeed extracts the better part of two kinds of protocols. Copyright © 2006 John Wiley & Sons, Ltd.

KEY WORDS: ad hoc networks; CSMA/CA; medium access control; token passing; wireless communications

1. Introduction

A wireless ad hoc network is formed by a cluster of mobile hosts without any pre-designed infrastructure of the base stations. In the IEEE 802.11 standard, all of the hosts in an ad hoc network are within each other's transmission range, which forms a single-hop (fully connected) ad hoc network. One of the main advantages of a wireless ad hoc network is that it can be rapidly deployed since no base station or fixed network infrastructure is required. Wireless ad hoc networks can be applied where pre-deployment of network infrastructure is difficult or impossible (e.g., in fleets on the oceans, armies on the march, natural disasters, battle fields, festival grounds, and historic sites). A single-hop ad hoc network is useful in a classroom, in a hall, or in a conference room, where students/participants turn on their laptops to form a network. Researches focus on single-hop networks can be found in References [1–6].

The design of MAC protocols for wireless ad hoc networks has received a great deal of attention recently. One of the most popular MAC protocols, the IEEE

*Correspondence to: Chih-Min Chao, Department of Computer Science and Engineering, National Taiwan Ocean University, No. 2, Beining Road, Keelung 20224, Taiwan (R.O.C.).
†E-mail: cmchao@ntou.edu.tw

802.11 WLAN standard [7], defines two mechanisms to access the channel—the distributed coordinated function (DCF) and the optional point coordination function (PCF). The DCF is a contention-based scheme which uses CSMA/CA as the access mechanism. The CSMA/CA protocol has the advantage of simple implementation. However, when the system load gets heavier, the performance drops dramatically because of increased collisions [8,9]. The PCF in IEEE 802.11 is a centralized polling scheme which is proposed to support collision-free and time-bounded services. The access point is responsible for polling the stations for transmissions. Such a centralized polling scheme suffers from poor performance when only a small amount of stations want to transmit [3,10]. This is because the access point will poll every station no matter it has packets to transmit or not. Thus unnecessary polls and delays incur. Such inefficiency is inevitable because, for fairness reasons, every station has to be polled in order to enable its transmission. Besides having poor performance during light loads, the centralized feature of the PCF does not fit the wireless ad hoc networks that are formed by a cluster of mobile stations without central access points.

Another way to provide contention-free channel access is to utilize the *token*. IEEE 802.4 Token Bus [11] and IEEE 802.5 Token Ring [12] are two well-known token passing MAC protocols that allow stations to transmit only when they hold a special control frame, the *token*. The token circulates around all the stations, thus every station has the chance to transmit. Both the Token Ring and Token Bus protocols are designed for wired networks. In a wireless environment, several contention-free protocols have also been proposed [5,13–16]. A more comprehensive review is in Subsection 1.1. Most of these contention-free protocols have the same problem as the 802.11 PCF does: suffer from poor performance when only few stations intend to transmit.

The problems mentioned above motivate this research work. In order to obtain better performance, a new MAC protocol with system load awareness is needed. In this paper, we propose a new distributed wireless ad hoc MAC protocol to achieve high performance all the time. The proposed load awareness (LA) protocol is based on the IEEE 802.11 standard. The fundamental contention-based DCF mode is unchanged but the contention-free mode is modified. The *LA* protocol can switch between contention-based mode and contention-free mode smoothly according to system load. The contention-based protocol is used if few stations want to transmit. Otherwise, the contention-free protocol is conducted. It is expected that our *LA* protocol can take the benefits of both contention-based and contention-free protocols and is fully compatible with the IEEE 802.11 standard. When we say compatible we mean that a host running IEEE 802.11 and a host running LA can operate in the same network concurrently.

1.1. Related Work

In Reference [13], a coordinator is responsible for passing the token to all the stations in turn. All data packets are first transferred to the coordinator and then relayed to the destination. The work in Reference [15] focuses on wireless LAN systems. Directional beam antennas are used while the service area is divided into 12 sectors. To facilitate data transmission in each sector, the *center module* transmits the token to every sectors one after another. Both [13] and [15] References adopt central controlled token passing mechanism, which has the drawback that data packets have to travel through the air twice: from the source station to the central control point and then to the destination.

In fact, token passing schemes need not to be centrally controlled. For instance, the Token Bus protocol is a fully distributed one. Another distributed token passing scheme can be found in Reference [16] where each station is responsible for correctly passing the token to the next station. Once a station, say X, passes the token, it will listen to the channel to see whether the next station begins to transmit or not. The token is retransmitted by X if no transmission is sensed within a predefined period. This token retransmission process will not stop until the token is successfully transferred. A wireless token ring protocol (WTRP) is proposed in Reference [14]. WTRP is a distributed protocol which includes station joining and leaving mechanisms in a multihop environment. However these schemes have some flaws. The token holder is responsible of deciding the station that can join the ring. The newly joined station is asked to send a join message to the station that is originally the successor of the token holder. This joining mechanism is inefficient since at most one station can join the ring for each invitation. Moreover, some stations will never join the ring because of the partially connectivity problem. For example, the token holder decides that a station (say, station G) is the one that can join the ring. However, the joining will fail if G cannot reach the successor of the token holder. A linear topology (stations form a chain and each one can only connect to its upstream and downstream stations) is another example that WTRP will fail. In general, a station

DOI: 10.1002/wcm

that is connected to only one of the ring members cannot join the ring. The problem of the station leaving scheme is that it may produce a linear topology which fails the WTRP. To conclude, we believe that it is difficult to design a complete contention-free protocol in a multihop environment due to its partially connectivity.

All these token passing protocols mentioned above, including central controlled and distributed ones, suffer from the same problem as the polling schemes do: inefficiency when the system is light loaded. The inefficiency results from the circulated token. In a light loaded situation, a host running a contention-based protocol has a large chance to access the channel immediately; however, a host running a token passing protocol has to wait for the token before transmission. This prolongs the access delay and reduces the efficiency.

A protocol called DBASE proposed in Reference [5] provides a contention-free period to transmit real-time traffic in wireless ad hoc environment. A station with real-time traffic must join the reservation table to reserve bandwidth. Contention is no longer needed to access the channel once the station successfully joins the reservation table. The DBASE protocol provides a good mechanism to support multimedia services in contention-free period. However, when the non-real-time traffic dominates the system, it performs similar to the IEEE 802.11 DCF. Our LA concentrates on the non-real-time traffic and intends to provide an efficient and fair channel access mechanism.

The rest of the paper is organized as follows. Section 2 describes the details of our protocol. The system performance is analyzed in Section 3. Simulation results are in Section 4. Conclusions are drawn in Section 5.

2. Protocol Description

In this section, the details of our protocol are presented. We assume that the mobile stations communicate with each other without the assistance of central access points. Moreover, these mobile stations operate in a single-hop environment. This means that the frames sent by a station can reach all other stations. Data and control frames are transmitted on the same channel. Two or more simultaneously transmitted frames will cause a collision, which is not recoverable at the receiving stations.

2.1. Medium Access Mechanism

The basic idea of our load awareness protocol is to exploit the advantages of both contention-based and contention-free protocols. In the *LA* protocol, the contention-based scheme is used if the system traffic load is light while the contention-free scheme is used when the system load is heavy. In all traffic conditions, our intention is to pick the access scheme that outperforms the other. The concept can be illustrated in Figure 1 where the system traffic load is varied with time. In the light loaded environment, hosts contend to access the channel. As the traffic load goes higher than a predefined threshold *Threshold_A*, the access scheme is switched to the contention-free one until the traffic load falls below *Threshold_B*. In this example, the contention-free scheme is used between time A to B and between time C to D. The contention-based scheme is used otherwise. We define two different thresholds, Threshold_A and Threshold_B, to avoid ping-pong effect. This may cause a little performance degradation but more stable operations among hosts are achieved. Note that the information of system load is not available for the hosts in the network since our *LA* protocol is a distributed one. Thus, in this paper, we use the waiting time as the measurement of Threshold_A and Threshold_B since it is proportional to the system load.

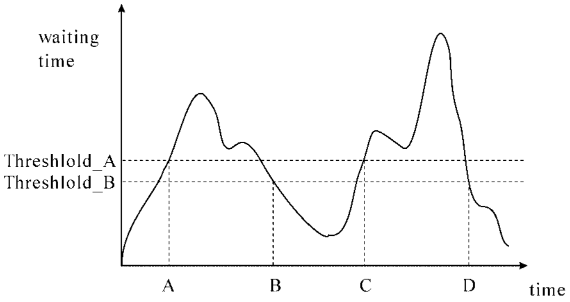

Fig. 1. The switching of contention-based and contention-free protocols.

We adopt IEEE 802.11 DCF as the contention-based scheme since it is a well-accepted standard in wireless environment. As for the contention-free scheme, we adopt token passing because it can be operated in a distributed manner. The main task of the *LA* protocol is the design of the contention-free part. Initially, all the hosts use the IEEE 802.11 DCF. When the system load is getting heavier, the channel access scheme is switched to token passing. Any station that seizes the channel and finds it has waited longer than Threshold_A (channel busy time excluded) will initiate the token passing scheme by sending a token at the end of its data. The frame format of the token is shown in Figure 2. The *Type* and *Subtype* fields can be used to identify the token frame while the *RA* field indicates the address of the station that the token will be

DOI: 10.1002/wcm

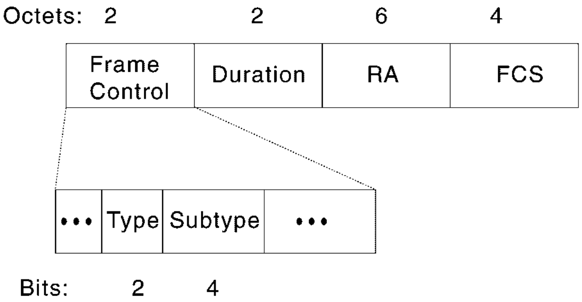

Fig. 2. The Token frame.

transferred to. The station that first transmit the token is called the 'token initiator.' By only allowing the mobile host that has already seized the channel to check if the token passing scheme should be started, we eliminate the possible contentions among hosts who want to be the token initiator.

Token initiator will transmit the CFP_START message at the beginning of data frames. All stations will enter contention free period (CFP) when they identify the CFP_START message. The CFP_START message contains the *active station list*, which is sorted by station ID and provides the token transmission order. Each station will maintain its own active station list. A station X adds another station, say Y, to its active list when it identifies that Y is involved in an active connection. The station Y will be deleted from X's active list when X detects that Y stops transmitting/receiving longer than a certain period of time. The active station list constructed by different stations may be different. To keep the list consistent in CFP, all users must follow the active station list of the token initiator. For those hosts that are not in the list of the token initiator, they can join later. These joins are activated by the invitation of any token holder. We will describe the details in Subsection 2.2. During the CFP mode, the token is circulated among all the active users according to the order provided in the active station list. Each user can start their data transmission when they hold the token. The operation of token passing is illustrated in Figure 3. Here we assume station 1 has packets to transmit and has waited for the channel longer than Threshold_A. When the channel returns to idle, station 1 will start its backoff process and RTS-CTS dialog after waiting DIFS. After successfully receiving the CTS sent from the destination (station 3), station 1 will transmit CFP_START followed by its data and the token. All stations will switch to CFP mode when they receive the CFP_START message. Afterwards, all active stations (six stations in this example) will take turns to transmit their packets. If a station receives the token but has no data to send, it simply sends out the token and the control is passed to the next station on the active list.

During the CFP mode, each station will calculate the access delay before it gets the token. Any station has the right to terminate the CFP mode if it receives the token and finds the access delay is lower than Threshold_B for successively *RT* (stands for Return Threshold) times. The access delay becomes lower means that few stations want to transmit and the IEEE 802.11 DCF will have better performance. We trigger the access scheme switching after recognizing lower access delay for successively *RT* times in order to keep our protocol stable (to avoid ping-pong effect). The token holder that decides to return to use the IEEE 802.11 DCF will cease the CFP mode by sending a CFP_END message. All stations will go back to run the IEEE 802.11 DCF when they recognize the CFP_END message. A host that does not run the *LA* protocol can still work properly by simply ignoring the newly introduced control frames (CFP_START, CFP_END, etc.). Note that the wireless channel is unreliable. It is possible that the token may be destroyed. We will describe the token maintenance and error recovery in Subsection 2.3.

The MAC switching algorithm of our *LA* protocol can be summarized as follows.

Initially, Medium Access Control (MAC) scheme is set to CSMA/CA
The following algorithm is executed once when a station gets the right to access the channel:

```
If (MAC is CSMA/CA)
    If (waiting time > Threshold_A)
        Transmit CFP_START (enter the CFP mode)
        MAC is set to Token Passing
Else
    If (waiting time < Threshold_B for successively RT times)
        Transmit CFP_END (exit the CFP mode)
        MAC is set to CSMA/CA
```

2.2. New Station Invitation

We assume the BEACON message is periodically broadcast both in the CFP and in the contention modes. In the contention period, the transmission of a BEACON follows the procedure of the IEEE 802.11 standard where all stations contend for transmitting one. In the CFP mode, token holders are responsible to broadcast a BEACON if they detect the beacon interval is expired. The BEACON packet contains the information whether the system is in the CFP mode or not. A new station must make sure in which mode

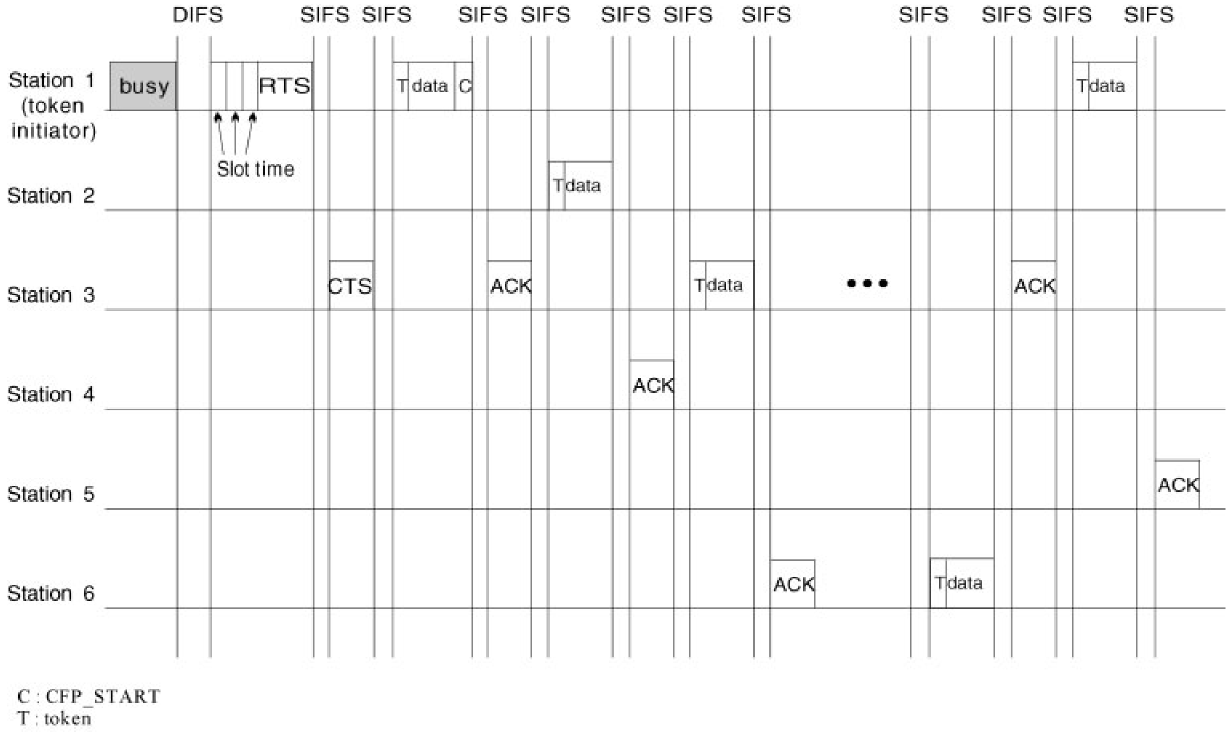

Fig. 3. The operation of token passing.

the system is before transmitting data. In the CFP mode, a station not belonging to the active station list does not have the chance to access the channel. If an inactive station has data packets to send, it must first become an active station by the invitation of a token holder, and then, wait for the token to start its transmission.

A token holder will invite new stations to join the CFP mode when it did not hear the CFP_INVITE message for more than a predefined interval. The CFP_INVITE message should be transmitted periodically and can be issued by any token holder. This CFP_INVITE carries the maximal number of stations, INVITE_NUM, that can join the CFP operation in each invitation. After correctly receiving this CFP_INVITE message, a station that wants to join the CFP mode will wait for a backoff time between 1 and INVITE_NUM before it can reply its CFP_JOIN message. Since the expected number of stations that want to join the CFP mode is small, the value of INVITE_NUM is set to eight. The probability of two or more successful transmissions in eight slots is higher than 86% if the number of stations waiting to join is no more than 10 [17]. At the end of the invitation, the token holder will broadcast a CFP_ACCEPT message, which carries a list of the stations that have successfully joined the CFP mode.

The newly joined stations will be inserted at the end of the active station list. After the invitation, the token holder will transmit its data and pass the token to next station as usual. If there are collisions or transmission failures during the invitation process, the next token holder will trigger another round of invitation. Such invitation is continued until there is no new station waiting to enter the CFP mode.

The frame formats of CFP_INVITE, CFP_JOIN, and CFP_ACCEPT are shown in Figure 4. The *RA* and *TA* fields represent destination and source addresses, respectively. The *DATA* field is used to carry the specific data for three different frames.

Although the number of stations that want to join the CFP mode is considered to be small, it is still possible that a large number of stations want to be in the CFP mode at the same time. To handle such a situation, we can enlarge the value of INVITE_NUM. When all the CFP_JOIN messages are collided or incurred

Octets: 2	2	6	6	4
Frame Control	DATA	RA	TA	FCS

Fig. 4. Management frame format.

DOI: 10.1002/wcm

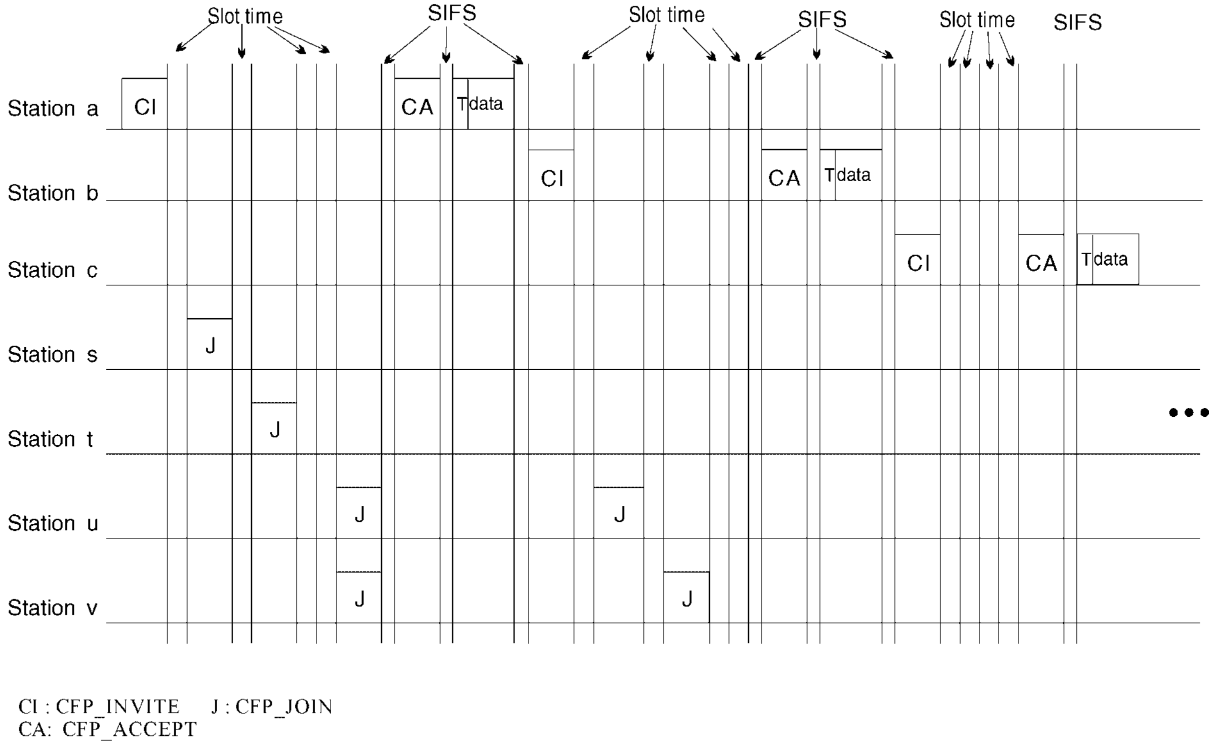

Fig. 5. An example of new stations joining into CFP (INVITE_NUM = 4).

transmission failures[‡] in a particular insertion round, the INVITE_NUM will be doubled at the next round of insertion. This collision resolution strategy is similar to that of the IEEE 802.11. We double the INVITE_NUM since we cannot obtain the exact number of stations that cause the collision. An example of invitation with the INVITE_NUM equals to four is shown in Figure 5. Stations a, b, and c are in the CFP mode while stations s, t, u, and v want to join them. In the first round invitation, which is activated by station a, stations s and t join the CFP mode successfully while the CFP_JOIN messages sent by stations u and v collide with each other. Station b will trigger the second round of invitation and both stations u and v join the CFP mode successfully. The invitation process ends when no new station wants to join the CFP mode. Since we assume a single-hop environment, all other active stations will be aware of the insertions of new members. The invitation scheme is a robust one since all the active stations are responsible for inviting new stations. Failure of stations will not cause any damage to the invitation scheme. Lastly, the new station insertion algorithm of our *LA* protocol is summarized below.

When a token holder X determines that a new station insertion is need, the following operations are executed:

1. *Broadcast the CFP_INVITE message.*
2. *Listen to the channel and count the successful CFP_JOIN message.*
3. *At the end of the insertion, broadcast the CFP_ACCEPT message.*
4. *Pass the token and transmit data packets, if any.*

The token holder that follows station X will repeat above four steps with two further considerations:

A. *If all the CFP_JOIN messages are collided or incurred transmission failures, doubles the INVITE_NUM.*
B. *If there is no CFP_JOIN message is sent by any new station, ends the new station insertion process.*

[‡] Note that a node cannot distinguish a collision from a transmission failure due to link errors. Here we treat them equally: the INVITE_NUM will be enlarged when either situation happens.

DOI: 10.1002/wcm

When a new station tries to join the CFP mode, the following operations are executed:

1. *Listen to the channel, count the successful CFP_JOIN messages.*
2. *Backoff before transmitting its CFP_JOIN message.*
3. *Transmit the CFP_JOIN message.*
4. *At the end of the invitation, determine if the join is successful or not according to the CFP_ACCEPT message sent from the token holder.*

2.3. Token Maintenance

If a station with the token is out of function or the token is destroyed during transmission, all other stations will detect this *token lost* event after the channel is idle for longer than SIFS (recall that a station receives the token must respond after SIFS). To solve this problem, the stations that are behind the failure station will coordinate to recirculate the token. Each station will have to wait for a duration, which is proportional to the transmission difference with the failed station, before it tries to generate a new token. For example, if it is the third station that holds the token and fails, the fourth station will wait $4 - 3 = 1$ time slot before it tries to send its data packet; the fifth station will wait $5 - 3 = 2$ time slots before it tries to send its packets. All the stations will follow this rule to wait for its turn to transmit. As long as one station succeeds to transmit its packet, the token will be regenerated at the end of the data packet, and thus, the token lost event is resolved. Note that this scheme can solve both individual station failure and multiple (continuous) stations failures. Also, the situation that a token is destroyed during transmission (due to poor wireless channel condition) can be considered as the station that transmits the token fails. The algorithm to solve the token lost problem is listed below.

> *All the stations monitor the channel. When the channel is idle for longer than SIFS, i.e. a particular station Y is failed, each station S waits for a particular period of time before it tries to regenerate the token. The duration for each station to wait is determined as follows:*

Time slots to be waited for station S

= the difference between station Y and station S

in the active station list.

Besides the token maintenance, the LA protocol relies on the CFP_START and CFP_END to switch medium access protocol protocols. It is important to handle the loss of such messages. Fortunately, missing these two messages does not produce a serious problem. If a CFP_START is lost, all the stations except the token holder remain operational using the CSMA/CA protocol. Later on, the token frame transmitted by the token holder will simply be discarded. A CFP_END loss can be regarded as a token lost event. Without correctly receiving the CFP_END, all the active stations still expect a token. However, the token holder will not generate a token since it has transmitted a CFP_END, thus, all the other stations will detect a token lost event and corresponding recovering procedure will be triggered.

3. Performance Analysis

The average cycle time and average access delay in contention-free mode are analyzed in this section. It is assumed that the packets arrive to each station according to a Poisson distribution. The packet length is the same for all the stations. Some notations that are used in the analysis are listed below:

- M : the number of stations.
- N_{p} : the average number of packets a station will transmit in a cycle time.
- L : the length of a packet (bits).
- L_{t} : the length of the token (bits).
- R : the capacity of the channel.
- λ : the average arrival rate.
- S : the interframe space (including delay in physical layer).
- T_c : the average cycle time.

The relationship between the access delay and the cycle time is shown in Figure 6, where a rectangle labeled as i means station i is being served. The cycle time is defined as the interval between two successive access of the channel for the same station. The average cycle time is the summation of the packet transmission time, token transmission time, and the interframe space, which can be expressed as [18]

$$T_c = M\left(\frac{N_{\mathrm{p}} \times L}{R} + \frac{L_{\mathrm{t}}}{R} + S\right) \tag{1}$$

where N_{p} is the average number of packets a station will send in one cycle time, which equals

$$N_{\mathrm{p}} = \lambda T_c \tag{2}$$

DOI: 10.1002/wcm

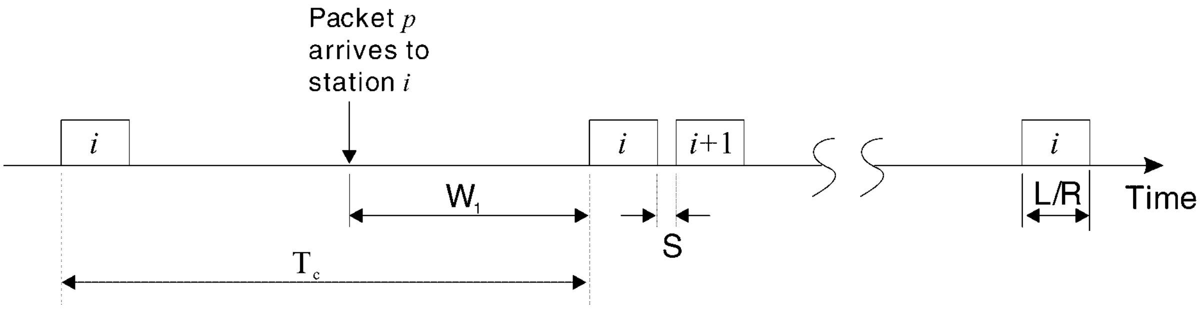

Fig. 6. The relationship of the waiting time and the cycle time.

Combining Equation (1) and Equation (2), we get

$$T_c = \frac{M\left(\frac{L_t}{R} + S\right)}{1 - \frac{ML\lambda}{R}} \tag{3}$$

Note that Equation (3) holds when $N_p < 1$ since at most one packet is allowed to send whenever a station holds the token. That is,

$$N_p = \lambda T_c < 1 \Rightarrow T_c < \frac{1}{\lambda} \tag{4}$$

Substitute Equation (4) into Equation (3), we get the necessary condition for Equation (3):

$$\lambda < \frac{R}{M(L_t + L + RS)} \tag{5}$$

When $N_p \geq 1$, all stations have data to transmit thus, from Equation (1), we have the maximum cycle time

$$T_c = M\left(\frac{L}{R} + \frac{L_t}{R} + S\right) \tag{6}$$

To conclude, according to Equations (3) and (6), the average cycle time is

$$T_c = \begin{cases} \frac{M\left(\frac{L_t}{R}+S\right)}{1-\frac{ML\lambda}{R}} & \text{if } \lambda < \frac{R}{M(L_t + L + RS)} \\ M\left(\frac{L}{R} + \frac{L_t}{R} + S\right) & \text{otherwise} \end{cases} \tag{7}$$

The access delay is defined as the time interval between a station has a packet to send and the time the particular station successfully access the channel. When $\lambda < \frac{R}{M(L_t+L+RS)}$, the access delay is equal to half of the idle time (denoted as W_1 in Figure 6), which is given by

$$\text{access delay} = \frac{T_c - \frac{T_c - MS}{M}}{2} = \frac{T_c - \frac{T_c}{M} + S}{2}, \quad \text{if } \lambda < \frac{R}{M(L_t + L + RS)} \tag{7}$$

where $T_c - MS/M$ is the busy duration of one station.

When $\lambda \geq \frac{R}{M(L_t+L+RS)}$, a station always has packets waiting to be sent, thus, the access delay is equal to the average cycle time minus the transmission time, which is

$$\text{access delay} = M\left(\frac{L}{R} + \frac{L_t}{R} + S\right) - \frac{L}{R}, \quad \text{if } \lambda \geq \frac{R}{M(L_t + L + RS)} \tag{8}$$

The analysis of access time is used to verify our simulation results in next section.

4. Simulation Results

We have implemented a simulator based on the GloMoSim library [19] to evaluate the performance of the proposed protocol. The hosts are randomly placed within an area of 200 × 200 m. The transmission range for each mobile host is about 377 m and the channel capacity is 2 Mbps. Packets arrived at each mobile host in a Poisson distribution with arrival rate λ packet/s. A spot in the figures are the average of 10 simulations each simulates 600 s. There are 75 hosts in the area. For each packet arriving at a sender, we randomly choose a recipient host as the destination. The *LA* protocol is built on top of the IEEE 802.11, the system parameters are summarized in Table I. For the *LA* protocol, a host failure rate of 0.5 host/s is imposed and the new station invitation procedure is executed every 100 ms

DOI: 10.1002/wcm

Table I. Experimental parameters.

Parameters	Value
Slot time	20 μs
SIFS	10 μs
DIFS	50 μs
Length of PHY's preamble	144 μs
Length of PHY's PLCP header	48 μs
Length of RTS	160 bits
Length of CTS	112 bits
Length of ACK	112 bits
Length of token	112 bits
Length of CFP_INVITE	160 bits
Length of CFP_ACCEPT	160 bits
Length of CFP_JOIN	160 bits
INVITE_NUM	8
Retry limit of RTS	7
CW_{min}	31
CW_{max}	1023
RT (return threshold)	2

when the *LA* protocol operates in the CFP mode. The active station list is maintained in each host in a linked list structure which facilitates the station insertions and deletions.

In order to achieve better performance, we must first determine the values of Threshold_A and Threshold_B. It is reasonable to switch to the CFP mode when the access delay a host experienced in the contention-based mode is longer than that in the contention-free mode. Thus, we set Threshold_A to the average cycle time of the token passing scheme when $\lambda < \frac{R}{M(L_t+L+RS)}$, which equals to $M(\frac{L}{R}+\frac{L_t}{R}+S)$ according to Equation (7). The choice of Threshold_B is a design issue. If Threshold_B is far smaller than Threshold_A, it takes a long time for our LA to react to the traffic load changes. If Threshold_B is equal to Threshold_A, our LA protocol may switch between the token-passing scheme and the IEEE 802.11 DCF frequently. If Threshold_B is larger than Threlhold_A, after switching to the token passing scheme, the LA will never switch back to use the IEEE 802.11 DCF. To keep our LA function correctly, Threshold_B is set to 0.9 × Threshold_A. The standard deviations for the results are also reported. The maximum and average standard deviations are about 4% and 2%, respectively.

Below, we compare the *LA* protocol to the IEEE 802.11 DCF and the token passing schemes from seven aspects.

(A) *Average access delay*: Figure 7 shows the average access delay of the three protocols (*LA*, IEEE 802.11 DCF, and token passing). We also draw the curve of the theoretical results of the average access delay of the token passing scheme. The access delay is defined as the duration between the time a station has a packet to transmit and the time the station gets the right to access the channel. For the token passing scheme, the average access delay is given by Equations (8) and (9). As we can see, the *LA* protocol indeed takes advantage of the other two protocols in all of the three packet sizes. Our *LA* protocol and the IEEE 802.11 DCF

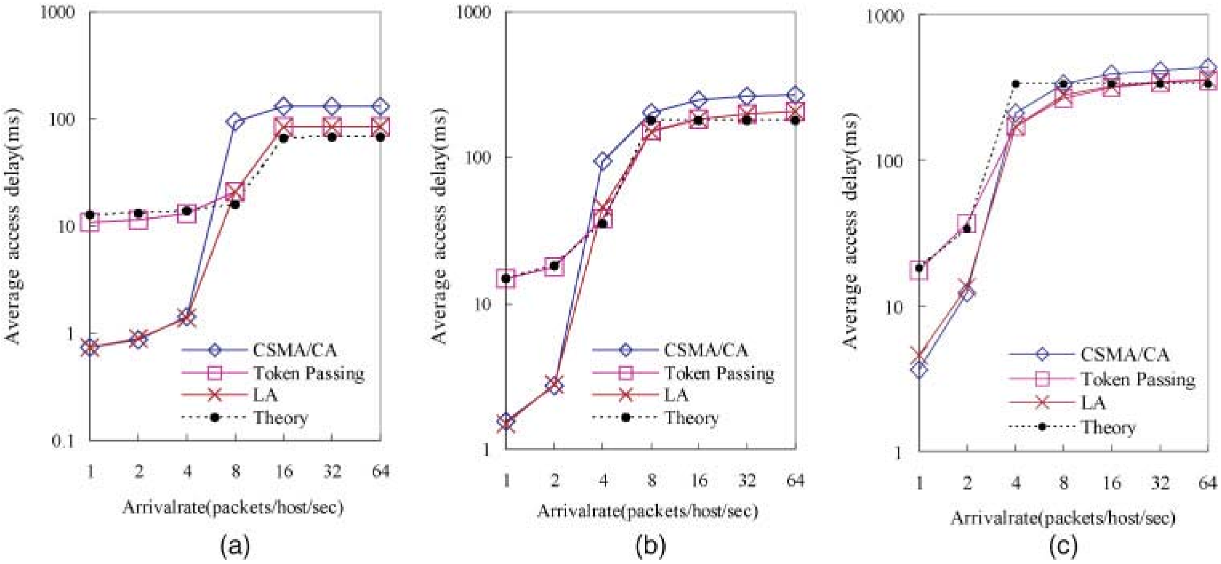

Fig. 7. The comparison of average access delay for packet size (a) 64, (b) 512, and (c) 1024 bytes.

DOI: 10.1002/wcm

have a similar delay which is much lower than that of the token passing scheme when the system is light loaded. Longer delay of the token passing scheme results from the token circulation and maintenance overhead. When the system is heavy loaded, the delay of the IEEE 802.11 becomes larger than the other two schemes. For example, when $\lambda = 32$ with packet length 512 bytes, delay time for 802.11, token passing, and *LA* are 265, 201, and 200, respectively.

(B) *Throughput*: Next, we investigate the throughput of the *LA* protocol. As shown in Figure 8(a), when the packet size is 64 bytes, these schemes coincide with each other if the system is light loaded. When the system load is higher than 8 packets/host/s, the *LA* protocol has the same throughput as the token passing and both outperform the IEEE 802.11 DCF. Figure 8(b) and (c) show the same simulation with the packet size set to 512 and 1024 bytes, respectively. Similar results can be found. This experiment indicates that the token passing protocol performs well on throughput. Its drawback is the high waiting time when the system is light loaded. Our *LA* protocol has both lower delay when the system is lighted loaded and high throughput (as good as the token passing scheme) when heavy loaded.

(C) *Dropped packets*: A packet that has not been correctly acknowledged will be retransmitted if the number of retransmission for the particular packet is less than the retry limit (a predefined system parameter). If the number of retransmission exceeds this limit, the packet will be discarded (dropped). A protocol that produces dropped packets is unstable because hosts running such a protocol may encounter many collisions before a successful transmission. This is undesirable from the users' point of view. In general, a contention-based scheme will suffer from such an unstable feature but a contention-free one will not. In Figure 9(a), (b), and (c), our protocol performs as well as the token passing scheme and outperforms the IEEE 802.11 DCF. This experiment verifies that our protocol, combined with a contention-based scheme and a contention-free one, does not suffer from the same unstable phenomenon as a contention-based protocol does.

(D) *Effect of time-varied traffic load*: In this experiment, we verify the performance of our protocol in a practical way: the traffic load is time-varied and is changed irregularly. As shown in Figure 10, where the packet size is 512 bytes and the arrival rates are changed every 40 s with the values 2, 4, 8, 1, 4, 32, 2, 1, 8, 64, 2, 16, 8, 1, and 2, respectively. We can see our *LA* protocol, switching between the token passing and the CSMA/CA schemes, takes advantage of the two protocols and achieves similar performance as the higher one all the time. It also indicates that we made a good selection of threshold_A and threshold_B such that our

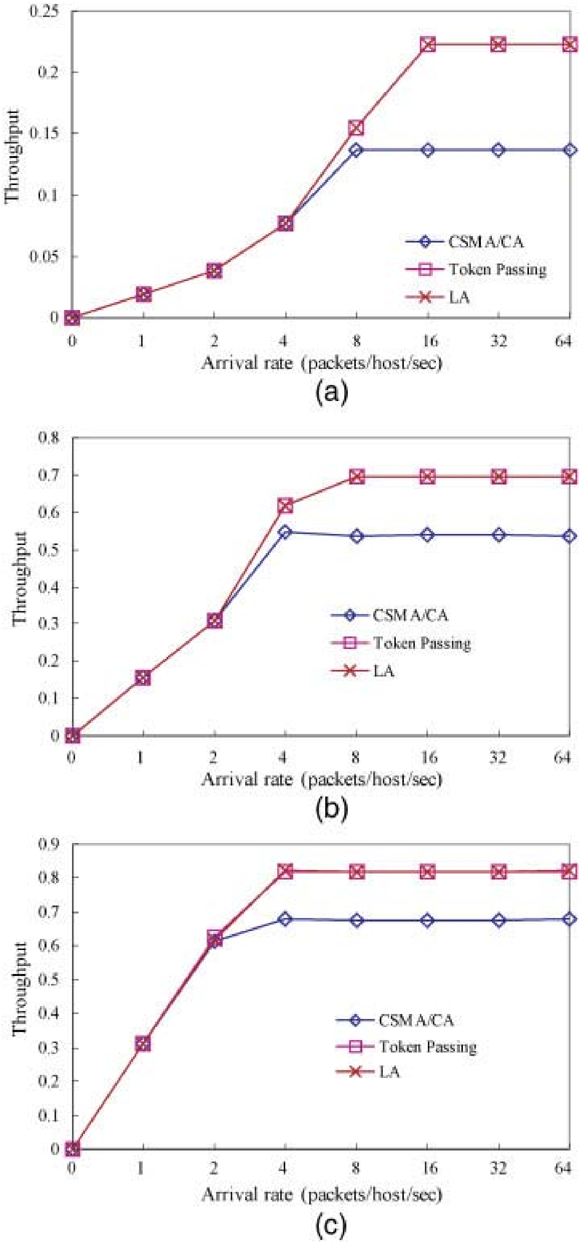

Fig. 8. The comparison of throughput for packet size (a) 64, (b) 512, and (c) 1024 bytes.

DOI: 10.1002/wcm

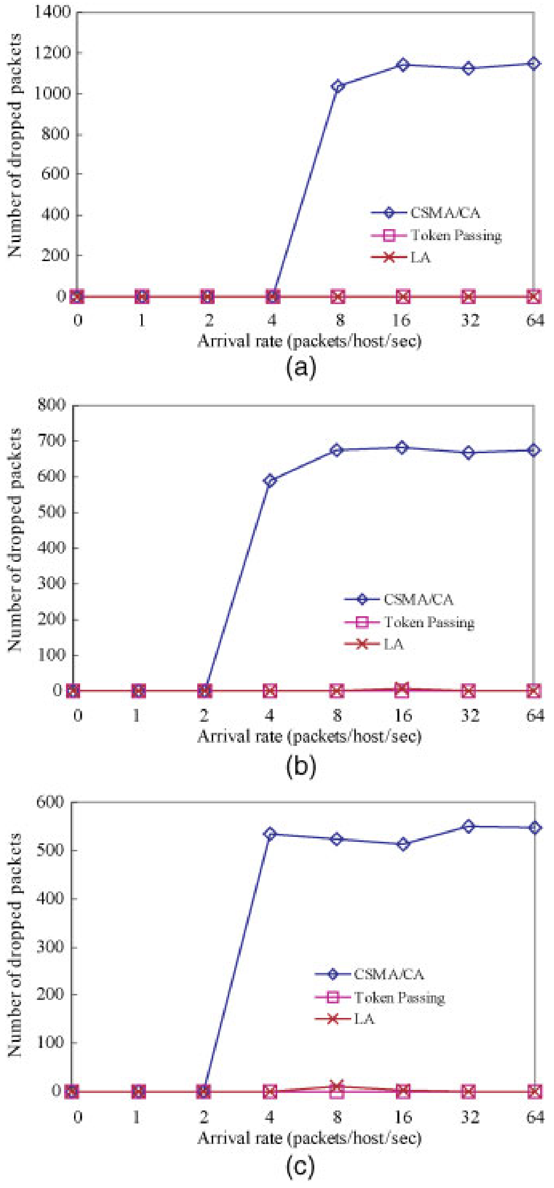

Fig. 9. The comparison of dropped packets for packet size (a) 64, (b) 512, and (c) 1024 bytes.

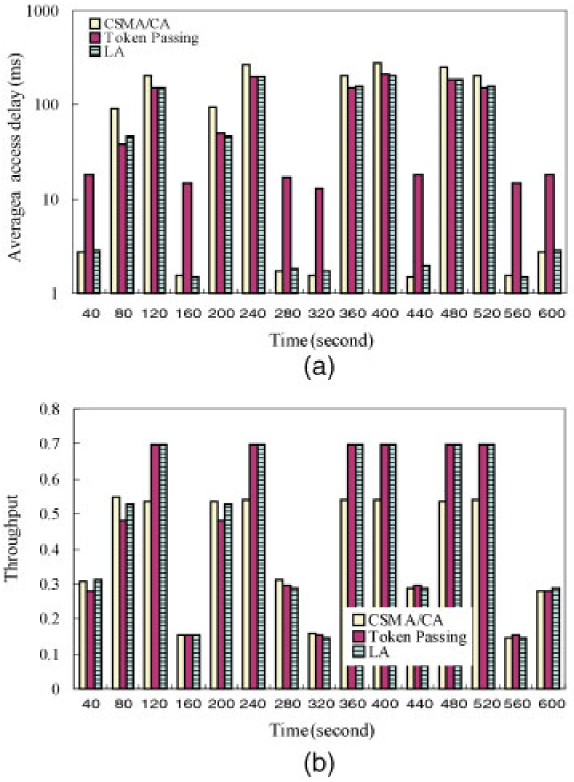

Fig. 10. Effect of irregularly time-varied system load over (a) average access delay and (b) throughput.

protocol can switch between two different schemes properly.

(E) *Effect of number of nodes*: In earlier experiments, we limited the number of transmitters to 75, but now we allow more users to transmit to observe the effect. Figure 11 shows the throughput comparison of 150 hosts and 75 hosts. We find the performance is almost the same for the token passing scheme when the system is heavy loaded. For the CSMA/CA, better performance is achieved when there are fewer hosts in the system. Again, our protocol takes the better part of the token passing and the CSMA/CA protocols, performs well in all system loads.

(F) *Effect of legacy 802.11 hosts*: Since the existence of legacy 802.11 hosts affects the performance of the LA protocol. This experiment verifies the effectiveness of our LA in an environment that

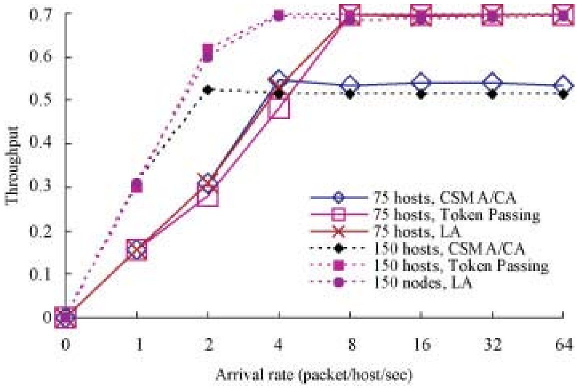

Fig. 11. Effect of number of hosts.

DOI: 10.1002/wcm

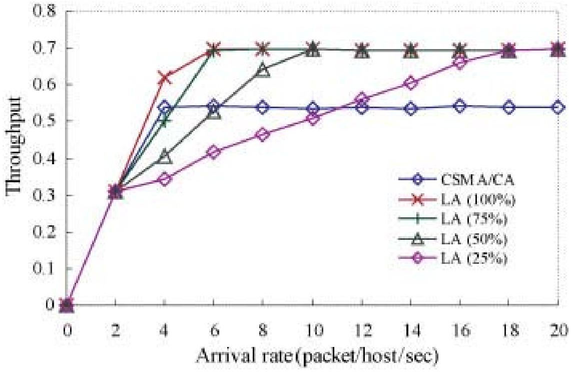

Fig. 12. Effect of legacy 802.11 hosts. The values in the parentheses are the percentage of hosts that implement the LA.

there are some legacy 802.11 hosts[§]. We simulate 75 hosts where 100%, 75%, 50%, or 25% of them have implemented the LA protocol (denoted as LA-capable hosts). The packet size is set to 512 bytes. Figure 12 shows the results. In all arrival rates, the best performance occurs when all of the hosts are LA-capable. In the cases that only some hosts are LA-capable, these LA-capable hosts find the waiting time exceeds threshold_A when the arrival rate is equal to or higher than 4 packets/host/s. Thus, they will switch to use the token passing scheme. However, since the legacy hosts do not realize LA-related management frames, they are unable to transmit in the CFP mode. Thus, fewer hosts than expected will be involved in transmission and the LA-capable hosts will switch back to use the CSMA/CA after recognizing the waiting time is below threshold_B. These frequent switches between the token passing and the CSMA/CA schemes produce some overhead. When these LA-capable hosts' traffic load is not heavy enough to compensate such overhead, pure CSMA/CA will be a better choice. For example, in this experiment, when the arrival rate is 4 packets/host/s, the CSMA/CA scheme has better performance than our LA if the LA-capable hosts occupy 75% or below; when the arrival rate is 8 packets/host/s, it only outperforms our LA protocol when 25% of the hosts are LA-capable; when the arrival rate is 12 packets/host/s or higher, even though there are only 25% of the hosts that are LA-capable, the throughput will improve if our LA protocol is applied.

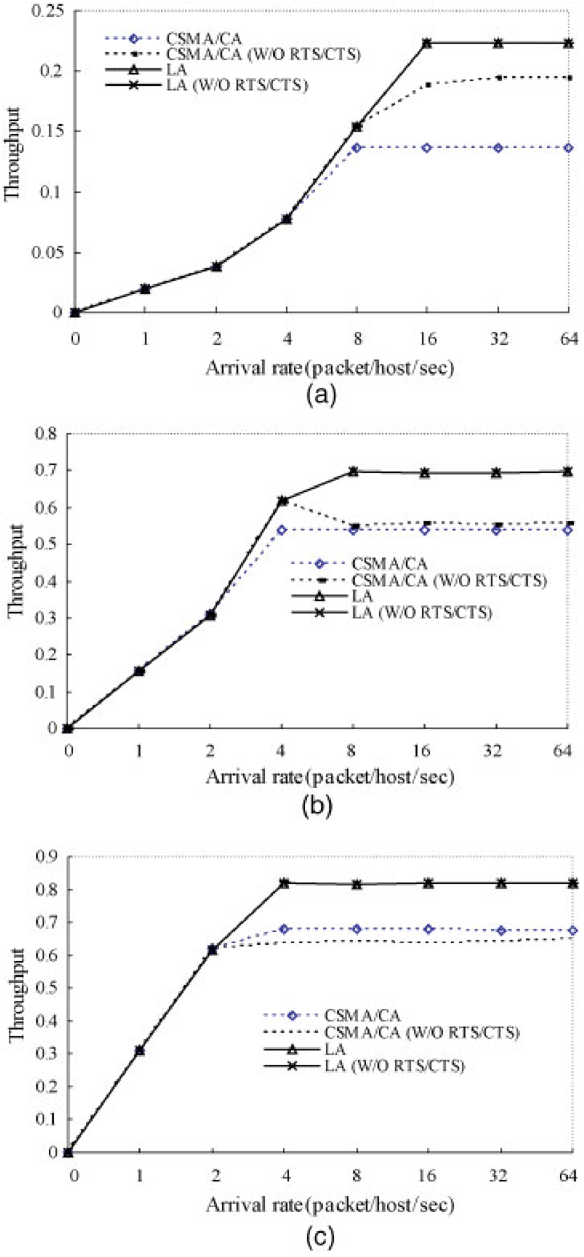

Fig. 13. Effect of with/without RTS and CTS packets for (a) 64, (b) 512, and (c) 1024 bytes.

(G) *Effect of RTS/CTS*: In this experiment, we test if RTS/CTS plays an important role on performance. In a single-hop network, the exchange of RTS and CTS only performs a fast collision check because there is no hidden terminal

[§] A legacy host will also appear in the active station list since hosts cannot distinguish which host is legacy host. There are legacy hosts in the active station list which is not a problem. A legacy host does not recognize token/token-embedded frame and thus it will not send a token as a LA-capable host does. However, it is just a token lost event and the associated token maintenance mechanism can handle it.

DOI: 10.1002/wcm

problem. Since no RTS/CTS is transmitted in the token passing scheme, we focus our attention on the CSMA/CA and LA protocols. The results are shown in Figure 13. Our LA still has better performance. In general, the RTS/CTS exchanges that affect the throughput when the network is heavy loaded. For the LA protocol, no matter RTS/CTS is transmitted or not, the performance is almost the same since the token passing scheme is applied when the network is heavy loaded. For the CSMA/CA scheme, without RTS/CTS achieves higher throughput when the packet size is small (64 and 512 bytes). It indicates that the benefit of the fast collision check does not compensate for the generated overhead. However, when the packet size increases, as we can see in Figure 13(c), the advantage of RTS/CTS exchanges appears. It verifies the design principle of RTS/CTS: it is not necessary to enable RTS/CTS transmission for short data packets.

5. Conclusions

We propose a new MAC protocol, *LA*, that combines a contention-based (IEEE 802.11 DCF) access scheme and a contention-free (token passing) one. The proposed protocol switches between these two schemes according to traffic load. The IEEE 802.11 DCF scheme is used when the system is light loaded and the token passing scheme is used otherwise. Such combination takes advantage of both access schemes and at the same time avoids the shortcomings of them. The most challenging tasks in designing a token passing protocol in an ad hoc network are the transmission and maintenance of the token over unreliable wireless links. Our token passing scheme is robust since it cannot only handle the station insertions and deletions but also resolve the token lost situation, which are critical issues for a token passing scheme in the wireless environment. Simulation results show that the proposed protocol can switch between the contention-based and the contention-free schemes smoothly, and thus takes advantage of both schemes.

References

1. Chao C-M, Sheu J-P, Chou I-C. An adaptive quorum-based energy conserving protocol for IEEE 802.11 ad hoc networks. *IEEE Transactions on Mobile Computing* 2006; **5**(5): 560–570.
2. Huang L, Lai TH. On the scalability of IEEE 802.11 ad hoc networks. In *Proceedings of the third ACM International Symposium on Mobile Ad Hoc Networking & Computing*, Lausanne, Switzerland, June 2002; pp. 173–182.
3. Sharon O, Altman E. An efficient polling MAC for wireless LANs. *IEEE/ACM Transactions on Networking* 2001; **9**(4): 439–451.
4. Sheu J-P, Liu C-H, Wu S-L, Tseng Y-C. A priority MAC protocol to support real-time multimedia traffic in ad hoc networks. *ACM Wireless Networks* 2004; **10**(1): 61–69.
5. Sheu S-T, Sheu T-F. A bandwidth allocation/sharing/extension protocol for multimedia over IEEE 802.11 ad hoc wireless LAN. *IEEE Journal on Selected Areas in Communications* 2001; **19**(10): 2065–2080.
6. Sobrinho JL, Krishnakumar AS. Quality-of-service in ad hoc carrier sense multiple access wireless networks. *IEEE Journal on Selected Areas in Communications* 1999; **17**(8): 1353–1368.
7. IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11*, 1999.
8. Bianchi G. IEEE 802.11–Saturation Throughput Analysis. *IEEE Communication Letter* December 1998; **18**: 318–320.
9. Bianchi G. Performance analysis of the IEEE 802.11 distributed coordination function. *IEEE Journal on Selected Areas in Communications* 2000; **18**(3): 535–547.
10. Sobrinho JL, Brazio JM. Proposal and performance analysis of a multiple-access protocol for high-speed wireless LANs. *Computer Networks and ISDN Systems* 1996; **28**: 283–305.
11. IEEE 802.4: Token-Bus Access Method. *IEEE Std 802.4*, 1985.
12. IEEE 802.5: Token-Ring Access Method. *IEEE Std 802.5*, 1985.
13. Davies RL, Watson RM, Munro A, Barton MH. Ad-hoc wireless networking: contention free multiple access using token passing. In *Proceedings of IEEE Vehicular Technology Conference* 1995; pp. 361–365.
14. Lee D, Attias R, Puri A, Sengupta R, Tripakis S, Varaiya P. A wireless token ring protocol for intelligent transportation systems. In *Proceedings of IEEE Intelligent Transportation Systems* 2001; pp. 1152–1157.
15. Miura S, Nakamura H, Kamienoo M, Araki K. Radio control method by using radio token in high speed wireless LAN system. In *Proceedings of IEEE Globecom* 1998; pp. 1811–1816.
16. Muriithi N, Burr AG. A robust token passing protocol for peer-to-peer radio LANs. In *Proceedings of IEE Colloquium on Radio LANs and MANs* 1995; pp. 6/1–6/6.
17. Hsu C-S, Sheu J-P. Design and performance analysis of leader election and initialization protocols on ad hoc networks. *Journal of Wireless Communication and Mobile Computing* 2003; **3**(4): 487–502.
18. Hammond JL, O'Reilly PJP. *Performance Analysis of Local Computer Networks*. Addison-Wesley: Boston, MA, 1986; 202–207.
19. UCLA parallel computing laboratory and wireless adaptive mobility laboratory. *GloMoSim: A Scalable Simulation Environment for Wireless and Wired Network Systems*, http://pcl.cs.ucla.edu/projects/glomosim/index.html

Authors' Biographies

Chih-Min Chao received his B.S. and M.S. degrees in Computer Science from Fu-Jen Catholic University and National Tsing-Hua University in 1992 and 1996, respectively, and his Ph.D. in Computer Science and Information Engineering from National Central University in January of 2004. He was with SENAO International in 1996. He was an assistant professor at the TamKang University, Taiwan from 2004 to

DOI: 10.1002/wcm

2005. Since 2005, he has been an assistant professor with the Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan. His research interests include mobile computing and wireless communication.

Jang-Ping Sheu received his B.S. degree in computer science from Tamkang University, Taiwan, Republic of China, in 1981, and the M.S. degree and Ph.D. in Computer Science from National Tsing Hua University, Taiwan, Republic of China, in 1983 and 1987, respectively. He joined the faculty of the Department of Electrical Engineering, National Central University, Taiwan, Republic of China, as an associate professor in 1987. He is currently a professor of the Department of Computer Science and Information Engineering and Director of Computer Center, National Central University. He was a chair of Department of Computer Science and Information Engineering, National Central University from 1997 to 1999. He was a visiting professor at the Department of Electrical and Computer Engineering, University of California, Irvine from July 1999 to April 2000. His current research interests include wireless communications, mobile computing, and parallel processing. He was an associate editor of *Journal of the Chinese Institute of Electrical Engineering* from 1996 to 2000. He was an associate editor of *Journal of Information Science and Engineering* from 1996 to 2002. He was an associate editor of *Journal of the Chinese Institute of Engineers* from 1998 to 2004. He is an associate editor of the *IEEE Transactions on Parallel and Distributed Systems* and *International Journal of Ad Hoc and Ubiquitous Computing*. He has served as a program chair and vice program chair for a number of international conferences including IEEE ICPADS'02, ICPP'03, and IEEE MSN'05. He received the Distinguished Research Awards of the National Science Council of the Republic of China in 1993–1994, 1995–1996, and 1997–1998. He received the Distinguished Engineering Professor Award of the Chinese Institute of Engineers in 2003. He received the Distinguished Professor award of the National Central University in 2005. Dr Sheu is a senior member of the IEEE, a member of the ACM, and Phi Tau Phi Society.

I-Cheng Chou received his B.S. degree in Computer Science from National Chengchi University in 2001, and received his M.S. degree in Computer Science and Information Engineering from National Central University in 2003, respectively. He worked for the Askey Computer Corp. as a senior engineer from 2003 until now. His research domains include wired and wireless local area network communication, broadband network communication. He currently focuses on gigabit passive optical network (GPON) development.

DOI: 10.1002/wcm