A Load Awareness Medium Access Control Protocol for Wireless Ad Hoc Network

Chih-Min Chao, Jang-Ping Sheu, and I-Cheng Chou
Department of Computer Science and Information Engineering
National Central University, Taiwan

Abstract— **A contention-based wireless ad hoc medium access control (MAC) protocol, such as carrier sense multiple access with collision avoidance (CSMA/CA), has the excellence of simple and efficient when the system is light-loaded. The main drawback of such protocols is their inefficiency and unbounded delay when system load is heavy. On the other hand, a contention-free MAC protocol, such as token passing, has 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 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 system is light-loaded and a contention-free one is used otherwise. Our LA protocol, which operates distributed and is fully compatible with 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 and performs well in all system loads.**

Keywords: Ad hoc network, CSMA/CA, medium access control, token passing, wireless communication.

I. Introduction

A wireless ad hoc network is formed by a cluster of mobile hosts without any pre-designed infrastructure of the base stations. A host in a wireless ad hoc network can roam and communicate with other hosts, at will. Two mobile hosts may communicate with each other either directly (if they are close enough) or indirectly, through intermediate mobile hosts that relay their packets, because of transmission power limitations. A main advantage 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 (for example, in fleets on the oceans, armies on the march, natural disasters, battle fields, festival grounds, and historic sites).

The design of MAC protocols for wireless ad hoc networks has received a lot of attention recently. One of the most popular MAC protocols, the IEEE 802.11 WLAN standard [2], 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 that it is simple to implement. However, when system load is getting heavier, the performance drops dramatically because of increased collisions [3]. 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 [9]. It is because the access point will poll every station, no matter it has packets to transmit or not, thus unnecessary polls and delays are incurred. Such inefficiency is inevitable because, for fairness reasons, every stations has to be polled in order to enable its transmission. Besides the poor performance at light load, the centralized feature of the PCF does not fit the wireless ad hoc networks that is 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 and IEEE 802.5 Token Ring 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 wireless environment, several contention-free protocols have also been proposed [4], [6], [7], [8]. In [4], 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 [6] focuses on wireless LAN systems. Directional beam antennas are used while the service area is divided into twelve sectors. To facilitate data transmission in each sector, the *center module* transmits the token to every sectors one after another. Both [4] and [6] 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 central controlled. For instance, the Token Bus protocol is a fully distributed one. Another distributed token passing scheme can be found in [7] where each station is responsible for correctly passing the token to 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. All these token passing protocols mentioned above, including central controlled and distributed ones, suffer from the same problem as the polling schemes do: inefficient when system is light-loaded. A protocol called DBASE proposed in [8] 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. No contention is needed any more to access the channel once the station successfully join 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 IEEE 802.11 DCF mode.

The problems mentioned above motivate this research. 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 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

This work was supported by the National Science Council of the Republic of China under Grant NSC 91-2213-E-008-025.

0-7803-7802-4/03/$17.00 © 2003 IEEE

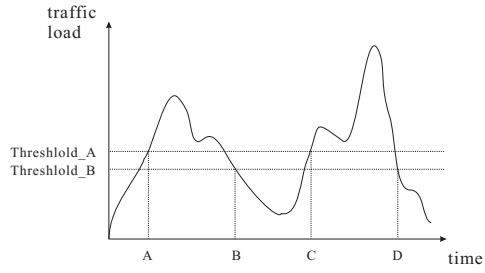

Fig. 1. The switching of contention-based and contention-free protocols.

loads. 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.

The rest of the paper is organized as follows. Section II describes the details of the protocol. Simulation results are in Section III. Conclusions are drawn in Section IV.

II. Protocol Description

We assume the mobile stations communicate with each other without the assistance of central access points. Moreover, these mobile stations operate in a fully-connected environment. It means 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.

A. Medium Access Mechanism

The basic idea of our load awareness (LA) 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 and the contention-free scheme is used otherwise. In all traffic conditions, our intention is to pick the access scheme that outperforms the other. The concept can be illustrated in Fig. 1 where the system traffic load is varied with time. At 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 scheme until the traffic load is down to another threshold $Threshold\_B$. 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 thresholds Threshold_A and Threshold_B to avoid ping-pong effect. This may cause a little performance degradation but more stable operations among mobile hosts are achieved. The information of system load is not available for the hosts since our LA protocol is a distributed one. Thus, in this paper, we use waiting time as the measurement of Threshold_A and Threshold_B since waiting time is proportional to system load.

We adopt IEEE 802.11 DCF as the contention-based scheme since it is a well-accepted standard in wireless environment. As to 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, the system is running under IEEE 802.11 DCF mode. 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 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 mobile hosts who want to be the token initiator.

Token initiator will transmit the CFP_START message in the front 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. And station Y will be deleted from X's active list when X detects that Y stop 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 into the CFP later. The joins are activated by the invitation of any token holder. We will describe the detailed join operations in next subsection. In 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 Fig. 2. Here we assume station 1 has packets to transmit and has waited the channel for 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 in 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 twice successively. 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 two successively lower access delay in order to keep our protocol stable (to avoid ping-pong effect). The token holder that decides to return to IEEE 802.11 DCF mode will cease the CFP mode by sending a CFP_END message. All stations will go back to IEEE 802.11 DCF mode when they recognize the CFP_END message.

B. New Station Invitation

We assume the BEACON message is periodically broadcast both in CFP and non-CFP modes. 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 the system is before transmitting data. A token holder will broadcast the BEACON message if it detects the beacon interval is expired. In the CFP mode, a station not belonging to the active station list does not have the chance to access the channel. If a non-active 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

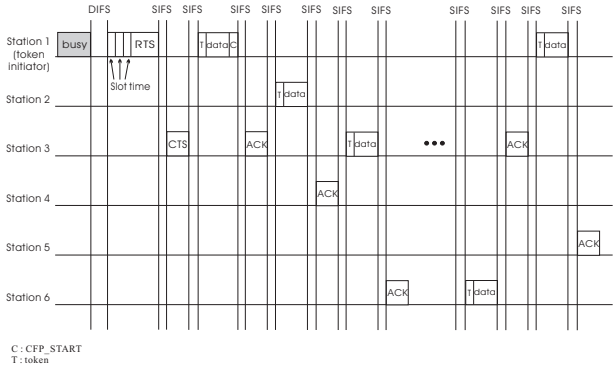

Fig. 2. The operation of token passing.

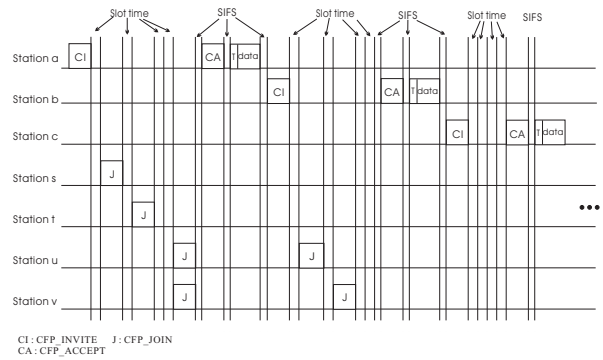

Fig. 3. An example of new stations joining into CFP (INVITE_NUM=4).

predefined interval. The CFP_INVITE message should be transmitted periodically and can be issued by any token holder. This CFP_INVITE carries the number of stations, INVITE_NUM, that can join the CFP operation. 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 [5]. Note that a host which sends a CFP_JOIN message doesn't know whether its message is correctly received by the token holder or not. This problem is solved here by the cooperation of all stations and the token holder. All the stations that want to join the CFP mode will listen to the channel and record the number of the CFP_JOIN messages being successfully received. Let n_i denote the CFP_JOIN message successfully received by station i. At the end of the invitation, the token holder will broadcast a CFP_ACCEPT message, which carries the number of CFP_JOIN messages that have been correctly received (denoted as N). The stations that just sent a CFP_JOIN message can determine whether they have successfully join the CFP mode by comparing n_i to N. The CFP_JOIN message sent by station i is correctly received by the token holder if $N = n_i + 1$, which means station i has successfully joined the CFP mode. That is, for any station i

$$\begin{cases} \text{station } i \text{ successfully joins the CFP,} & \text{if } N = n_i + 1 \\ \text{station } i \text{ fails to join the CFP,} & \text{otherwise.} \end{cases} \quad (1)$$

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 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 for entering the CFP mode.

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 in a particular insertion round, the INVITE_NUM will be doubled at the next round of insertion. An example of invitation with the INVITE_NUM equals to four is shown in Fig. 3. 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 fully-connected environment, all other active stations will be aware of the insertions of new members. After the invitation, the token holder transmit its data packets and pass the token as usual. 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.

C. Token Maintenance

If a station with the token is out of function, 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 wait for a duration 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 slots 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 thus the token lost event is resolved. Note that this scheme can solve individual station failure and continuous station failures.

III. Simulation Results

We implemented a simulator based on the GloMoSim library [1] to evaluate the performance of the proposed protocol. The mobile hosts are randomly placed within an area of 200 meter $\times$ 200 meter. The transmission range for each mobile host is about 377 meters and the channel capacity is 2 Mbps. Packets arrived at each mobile host in an Poisson distribution with arrival rate λ packet/sec. A spot in the figures are the average of 10 simulations each simulates 300 seconds. There are 75 hosts in the area. For each packet arriving at a sender, we randomly chose a recipient host as the destination. The LA protocol is built on top of IEEE 802.11, the system parameters are summarized in Table I. For the LA protocol, a host failure rate of 0.5 host/sec is imposed and the new station invitation procedure is executed every 100 ms when the LA protocol is in CFP mode.

TABLE I

EXPERIMENTAL PARAMETERS.

Parameters	Value
slot time	20 μs
SIFS	10 μs
DIFS	50 μs
length of RTS	160 bits
length of CTS, ACK, and token	112 bits
length of CFP_INVITE, CFP_ACCEPT, and CFP_JOIN	160 bits
INVITE_NUM	8
retry limit of RTS	7
CW_{min}	31
CW_{max}	1023

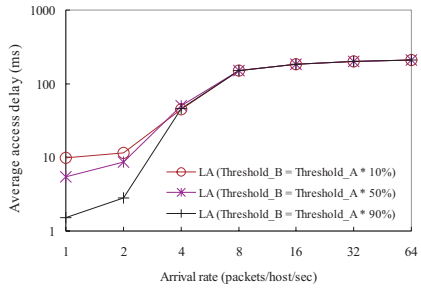

Fig. 4. The effect of Threshold_B with packet size 1024 bytes.

In order to achieve better performance, we must first determine the values of Threshold_A and Threshold_B. It is reasonable to switch to CFP mode when the access delay a host experienced in contention-based mode is longer than that in contention-free mode. Thus, we set Threshold_A to the average access delay of the token passing scheme when the system is fully-loaded, which equals $M(\frac{L}{R} + S)$ where M is the number of stations, L is the length of a packet, R is the capacity of the channel, and S is the interframe space. The effect of different Threshold_B's is shown in Fig. 4. It is obvious that the lowest delay happened when Threshold_B equals 0.9 $\times$ Threshold_A. We will use this setting of Threshold_B in the following simulations.

We make comparisons of the LA protocol to the IEEE 802.11 DCF and token passing schemes from four aspects.

A) Average access delay: Fig. 5 shows the average access delay of the LA protocol, IEEE 802.11 DCF and token passing. As we can see in both Fig. 5(a) and Fig. 5(b), the LA protocol indeed take advantages of the other two protocols. In Fig. 5(a) where the packet size is 512 bytes, our LA protocol and IEEE 802.11 DCF have similar delay and is much lower than that of the token passing scheme when the system is light-loaded. The longer delay of token passing is produced by the token circulation and maintenance overhead. When the system is heavy-loaded, the delay of IEEE 802.11 becomes larger than the other two schemes. Similar simulation is shown in Fig. 5(b). Again, the LA protocol switches between the other two protocols and gets the benefits of them.

B) Throughput: Next, we investigate the throughput of the LA protocol. As shown in Fig. 6(a), when the packet size is 512 bytes, LA, CSMA/CA and token passing coincide with each other if the system is light-loaded. When the system load is higher than 4 packets/host/second, the LA protocol have the same throughput as the token passing and both outperform the CSMA/CA. Fig. 6(b) shows the same simulation with the packet size 1024 bytes. Similar results can be found.

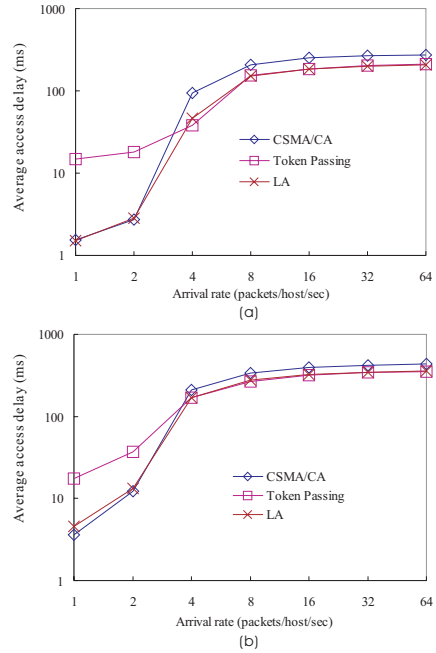

Fig. 5. The comparison of average access delay for packet size (a) 512 bytes and (b) 1024 bytes.

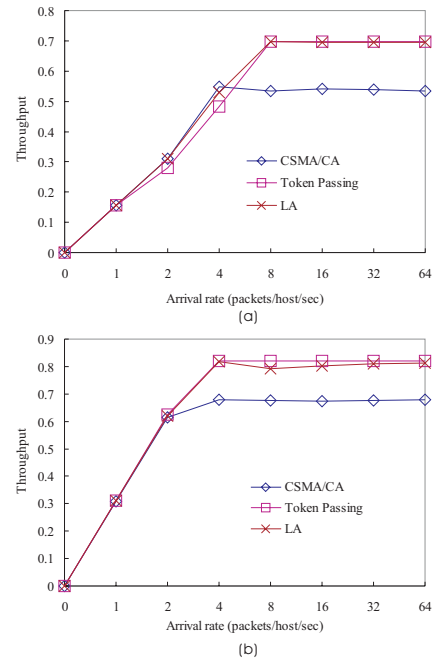

Fig. 6. The comparison of throughput for packet size (a) 512 bytes and (b) 1024 bytes.

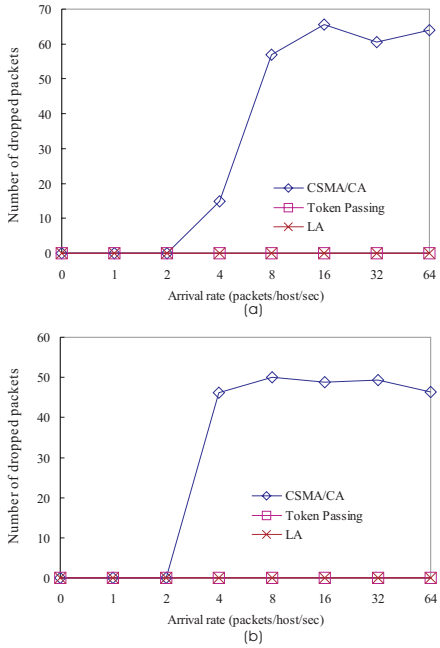

Fig. 7. The comparison of dropped packets for packet size (a) 512 bytes and (b) 1024 bytes.

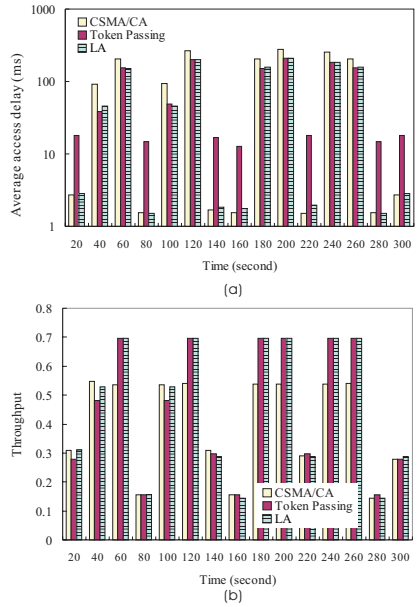

Fig. 8. Effect of irregularly time-varied system loads.

C) Dropped packets: Packets are retransmitted if collisions are incurred. A packet is dropped if the number of retransmission exceeds the retry limit. A protocol that produces dropped packets is unstable because hosts running such a protocol may encounter many collisions before a successful transmission. It is an undesirable feature from the viewpoint of users. In general, a contention-based scheme will suffer from such an unstable feature but a contention-free one will not. In Fig. 7(a) and (b), we see 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 unstable phenomenon as a contention-based protocol does.

D) Effect of time-varied traffic loads: In this experiment, we verify the performance of our protocol in a practical way: the traffic loads are time-varied and are changed irregularly. As shown in Fig. 8, where the packet size is 1024 bytes and the arrival rates are changed every 20 seconds and the values are 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 token passing and IEEE 802.11 DCF schemes according to different arrival rates, takes advantage of the other two protocols that can achieve 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 protocol can switch between two different schemes properly.

IV. 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 loads. 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 ad hoc network are the transmission and maintenance of the token over unreliable wireless links. Our token passing scheme is robust since it can not only handle the station insertions and deletions but also resolve the token lost situation, which are critical issues for a token passing scheme in wireless environment. Simulation results show that the proposed protocol can switch between contention-based and contention-free schemes smoothly, thus takes advantage of both schemes and performs well in all system loads.

References

[1] 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*.

[2] IEEE 802.11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11*, 1999.

[3] G. Bianchi. Performance Analysis of the IEEE 802.11 Distributed Coordination Function. *IEEE Journal on Selected Areas in Communications*, 18(3):535–547, March, 2000.

[4] R. L. Davies, R. M. Watson, A. Munro, and M. H. Barton. Ad-Hoc Wireless Networking: Contention Free Multiple Access Using Token Passing. In *Proceedings of IEEE Vehicular Technology Conference*, pages 361–365, 1995.

[5] C.-S. Hsu and J.-P. Sheu. Performance Evaluation of The Contention-Based Leader Election and Initialization Protocols. *Technical Report of HSCC Lab. http://axp1.csie.ncu.edu.tw/∼cshsu/evaluation.htm*, 2002.

[6] S. Miura, H. Nakamura, M. Kamienoo, and K. Araki. Radio Control Method by Using Radio Token in High Speed Wireless LAN System. In *Proceedings of IEEE Globecom*, pages 1811–1816, 1998.

[7] N. Muriithi and A. G. Burr. A Robust Token Passing Protocol for Peer-to-Peer Radio LANs. In *Proceedings of IEE Colloquium on Radio LANs and MANs*, pages 6/1 –6/6, 1995.

[8] S.-T. Sheu and T.-F. Sheu. DBASE: A Distributed Bandwidth Allocation/Sharing/Extension Protocol for Multimedia over IEEE 802.11 Ad Hoc Wireless LAN. In *Proceedings of IEEE INFOCOM*, pages 1558–1567, 2001.

[9] J. L. Sobrinho and J. M. Brazio. Proposal and Performance Analysis of A Multiple-Access Protocol for High-Speed Wireless LANs. *Computer Networks and ISDN Systems*, 28:283–305, 1996.