SYN-MAC: A Distributed Medium Access Control Protocol for Synchronized Wireless Networks*

Hongyi Wu, Anant Utgikar, and Nian-Feng Tzeng
The Center for Advanced Computer Studies
University of Louisiana at Lafayette
P.O. Box 44330, Lafayette, LA 70504-4330
Phone: 337-482-6338; Fax: 337-482-5791
Email: {wu, apu7797, tzeng}@cacs.louisiana.edu

Abstract

In this paper, we propose a novel medium access control (MAC) protocol, called SYN-MAC (for SYNchronized MAC), based on a binary countdown approach tailored for wireless networks. SYN-MAC has several attractive features such as simplicity, robustness, high efficiency, fairness, and quality of service capability. We evaluate SYN-MAC in terms of collision probability, system throughput, and packet delay, via both analysis and simulation. Our results show that, with properly chosen parameters, SYN-MAC can achieve a very low collision probability, packet delay tolerance, and extremely high channel efficiency (of $> 90\%$) under a wide range of traffic load. As a result, SYN-MAC may serve as an alternative to IEEE 802.11 for the wireless stations in synchronized networks.

1 Introduction

With unmatched flexibility to support the communication of mobile users, the wireless local area networks (WLANs) and the mobile ad hoc networks have become increasingly popular over the past few years. Though developed as independent networking technologies, the WLAN and the mobile ad hoc network are envisioned to be integrated into other existing networks, e.g., the cellular system, the satellite system, and/or the Internet, serving as a cost-effective complement to the fixed infrastructure. Several integrated systems involving the cellular and the ad hoc technologies have been proposed in [1, 2, 3], where each mobile station can communicate with both the cellular system and the ad hoc network (or the WLAN). In addition, more and more mobile devices are equipped with the GPS (global positioning system) receivers, giving rise to a loosely integrated ad hoc and satellite system. The infrastructure of the integrated networks can provide effective support (e.g., synchronization, signaling, authentication, etc.) to the mobile stations in the ad hoc

*This work is supported in part by NSF CAREER Award CNS-0347686. Part of this work was presented in the student poster session of IEEE International Conference on Network Protocols (ICNP) 2003, Atlanta, GA.

networks or the WLANs, dramatically enhancing system performance. In particular, the mobile stations can reach system-wide synchronization by detecting the pilot signals in the cellular systems and/or the GPS signals from the satellites, without consuming additional resources (e.g., the bandwidth of cellular/satellite channels). Other synchronization schemes recently proposed for multi-hop wireless networks may also be employed [4]. In this work, we investigate the potential performance improvement of wireless networks with such synchronization. Specifically, we propose and evaluate a novel medium access control (MAC) protocol based on an enhanced binary countdown scheme for synchronized wireless networks.

The MAC protocol resolves contention for accessing to the shared medium. As a key design issue of wireless communication, various MAC protocols have evolved over the years for different networks. In the cellular system, centrally-controlled contention-free schemes, such as FDMA (frequency division multiple access), TDMA (time division multiple access), or CDMA (code division multiple access), are usually adopted for the data channels, while random access is employed in the uplink control channel [5]. When an access point is present, the WLAN may use a polling scheme as defined in IEEE 802.11 PCF (point coordination function) [6] to provide contention-free and QoS (quality of service)-guaranteed service. In a wireless network involving multiple hops (i.e., where two stations may not communicate with each other directly), efficient and distributed multiple access control is especially important. Several asynchronous and distributed MAC protocols have been considered in the last several decades. In particular, the carrier sense multiple access with collision avoidance (CSMA/CA) scheme has been standardized in IEEE 802.11 DCF (distributed coordination function) [6] and widely implemented in WLANs and ad hoc networks. On the other hand, synchronized and distributed approaches able to potentially achieve higher performance, however, have not been adequately studied yet, since the multi-hop wireless network (e.g., the mobile ad hoc network) was originally designed as an independent system with no provision to obtain system-wide synchronization.

In this paper, we propose a SYN-MAC (short for Synchronized MAC) protocol, based on an enhanced binary countdown scheme that solves the unfairness problem and the hidden station problem brought up earlier in [7]. SYN-MAC has several attractive features such as simplicity, robustness, high efficiency, fairness, and QoS capability. We evaluate SYN-MAC in terms of collision probability, system throughput, and packet delay, via both analysis and simulation. Our results show that SYN-MAC achieves significantly better performance compared with existing protocols. With properly chosen system parameters (e.g., the length of the contention intervals as to be discussed in Section 3), SYN-MAC can reach a very low collision probability, packet delay tolerance, and extremely high channel efficiency (of $> 90\%$) under a wide range of traffic load, outperforming ADHOC MAC (a recently proposed MAC protocol for synchronized wireless networks), whose maximum channel efficiency is only 75% [8].

The rest of this paper is organized as follows. In Section 2, we discuss related work. In Section 3, we introduce the proposed SYN-MAC protocol. The analytic and simulation results are presented in Section 4. Finally, Section 5 concludes the paper.

2 Related Work

Various MAC protocols have been proposed for wireless networks. They can be classified into two categories, namely, non-synchronized protocols and synchronized protocols. The former does not need system-wide time synchronization, while the latter does.

Channel contention in the non-synchronized approaches can be resolved by either in-band (i.e., single channel) control handshaking or out-band (i.e., multi-channel) signaling. Several single-channel non-synchronized wireless MAC protocols have been proposed, such as Multiple Access with Collision Avoidance (MACA) [9], MACA for Wireless (MACAW) [10], and Floor Acquisition Multiple Access (FAMA) [11]. The central idea is to use the *Request To Send (RTS)*/*Clear To Send (CTS)* mechanism to solve the hidden station problem in wireless networks. Various approaches have been considered to improve the performance of the *RTS/CTS* scheme by using power control [12, 13], directional antennas [14, 15, 16], etc. The *RTS/CTS* scheme has also been standardized in IEEE 802.11 Distributed Coordination Function (DCF) [6]. On the other hand, several MAC protocols based on out-band signaling have been proposed. For example, [17, 18, 19] use busy tone(s) to avoid collision and eliminate the hidden stations. [20] introduces a multi-channel carrier sense multiple access (CSMA) protocol, which divides the total available bandwidth into N narrow-band sub-channels, and then apply CSMA in each sub-channel. In [21, 22, 23, 24], the total available bandwidth is divided into two or more channels, with one channel used for control and the rest of them for data transmission.

The synchronized approaches can be further classified into two sub-categories, i.e., the centralized protocols and the distributed protocols. The centralized protocols include the FDMA, TDMA, and CDMA approaches for cellular systems and the polling scheme defined in IEEE 802.11 standard [6] and HIPERLAN [25]. While the centralized approaches perform well in a single-hop wireless system, where the base station (or access point) can communicate with all wireless terminals directly, it is technically difficult and inefficient to apply them to a multi-hop wireless network without a central coordinator.

On the other hand, several synchronized but distributed approaches [7, 8] have been proposed recently. [8] introduces an MAC architecture, called ADHOC MAC, for mobile ad hoc networks. It deploys a reliable reservation ALOHA (RR-ALOHA) protocol to establish slotted/framed wireless channels. Each station can transmit in one or several slots in a frame. In a slot, the station sends not only data but also Frame Information (FI) that reports the frame status as perceived by the terminal (i.e., which station transmits in which slot). Upon collecting FIs from its neighbors, a new station has the frame status within two hops and thus can choose an appropriate slot to transmit. ADHOC MAC is a distributed approach, providing flexible and reliable medium access. As discussed in [8], however, the overhead of this protocol is very high, because each station has to send the FIs. In fact, the maximum channel efficiency of ADHOC MAC is only 75% as reported in [8].

A CSMA/CP (Carrier Sense Multiple Access with Collision Prevention) protocol is proposed in [7]. The authors considered the use of binary countdown to resolve medium access contention. The basic idea of binary countdown lies in selecting the winner based on a k-bit binary number. One gives up contention as soon seeing a higher number. Given four numbers 0010, 0100, 1001, and 1010 for instance, the first two competitors will give up after comparing the first (highest) bit, and the third competitor gives up after the third bit. Finally, 1010 wins the contention. Binary countdown is a well known approach that has many applications. For example, it has been discussed in [26] as a MAC protocol, where the unique station addresses are used for contention, leading to a collision-free medium access. At the same time, however, it results in unfairness among the stations because the station with a larger address always has higher priority. In [7], the basic binary countdown scheme is used on a control channel. After winning the channel

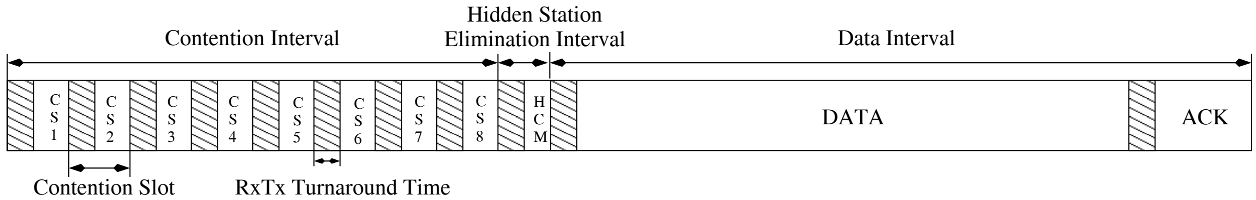

Figure 1: Frame format of the proposed MAC protocol, where CS stands for Contention Signal, HCM stands for Hidden station Clear Message, and ACK stands for Acknowledgement.

access, the RTS/CTS scheme is used to deal with the hidden station problem. Further improvement and QoS support can be achieved using better binary number assignment approaches. However, the following problem in binary countdown itself needs to be considered in order to attain higher efficiency in a multi-hop wireless network. Let's consider a special case, where two nodes A and C are trying to send data to another node, B. Assume nodes A and C are not within the transmission range of each other (and there are no other competitors), then no matter which binary numbers are chosen for contention, both A and C will win the channel access. Consequently, nodes A and C will simultaneously send out RTS to B, which, however, cannot receive the RTS correctly because of collision. As a result, no one may transmit during this slot, and bandwidth is completely wasted. In fact, there is a very high probability for such a problem to happen in ad hoc networks. In a wireless LAN with an access point, the probability is even higher (e.g., let B be the access point). One solution for this problem is to employ a random back-off scheme before sending out RTS. This, however, results in lower channel efficiency. In the next section, we propose a novel approach in order to avoid such collision at the receiver without sacrificing bandwidth utilization.

3 Proposed SYN-MAC Protocol

In this section, we introduce the proposed SYN-MAC protocol for synchronized mobile ad hoc networks or wireless LANs. We first describe the proposed protocol, then present a correctness proof, followed by the worst case analysis and further discussion.

3.1 Protocol Description

As discussed earlier in Sec. 1, time synchronization can be obtained from the cellular infrastructure or from the satellite when a GPS receiver is available. In the proposed SYN-MAC protocol, the network-wide synchronized frames are used by the mobile stations. As depicted in Fig. 1, a frame consists of three intervals: the contention interval, the hidden station elimination interval, and the data interval. The contention interval is used to resolve contention. It consists of k contention slots. Each contention slot, say contention slot i, includes the turnaround time between the transmitting and receiving modes and the time to send a very short message, called the contention signal (and denoted as CS_i). The hidden station elimination interval is for solving the hidden station problem. A Hidden station Clear Message (HCM) is transmitted by the receiver during this interval. Finally, data and acknowledgment are sent in the data interval. The parameters, such as interval length and slot length, are to be discussed later in Sec. 4.1.

The proposed medium access control scheme includes three major steps: contention resolution, hidden station elimination, and data transmission, as described next.

3.1.1 Step 1: Contention Resolution

A binary countdown approach is adopted to resolve contention. A station (say, X) that has data to send generates a random number with k bits, i.e., $\{b_i \mid 1 \leq i \leq k\}$, where k is the number of contention slots in a contention interval. If $b_i = 1$, station X sends a short message CS_i in contention slot i, which contains the destination's MAC address. Otherwise, if $b_i = 0$, station X listens to the channel. If the channel is busy (i.e., one or several other stations are transmitting), station X stops further transmission and gives up its attempt of gaining access to the channel in this frame. If each station in a collision domain (i.e., an area where all stations can hear from each other) generates a distinct random number, only one station that survives at the end of the contention interval moves to Step 2 and continues to transmit. If two or more stations generate an identical random number that is the largest among all numbers generated, collision may happen. As to be discussed later in Sec. 4.1, however, we can choose k large enough to keep the collision probability satisfactorily low.

A station Y that is not a sender determines whether it is an intended receiver by checking the first received contention signal. If multiple stations are transmitting simultaneously in a contention slot, Y cannot receive a valid contention signal and thus wait for the next contention slot. When there is exactly one station transmitting in a contention slot, say slot i, station Y can receive a valid CS_i and marks itself as a receiver if CS_i carries its MAC address. At the same time, station Y generates a *random number mask*,

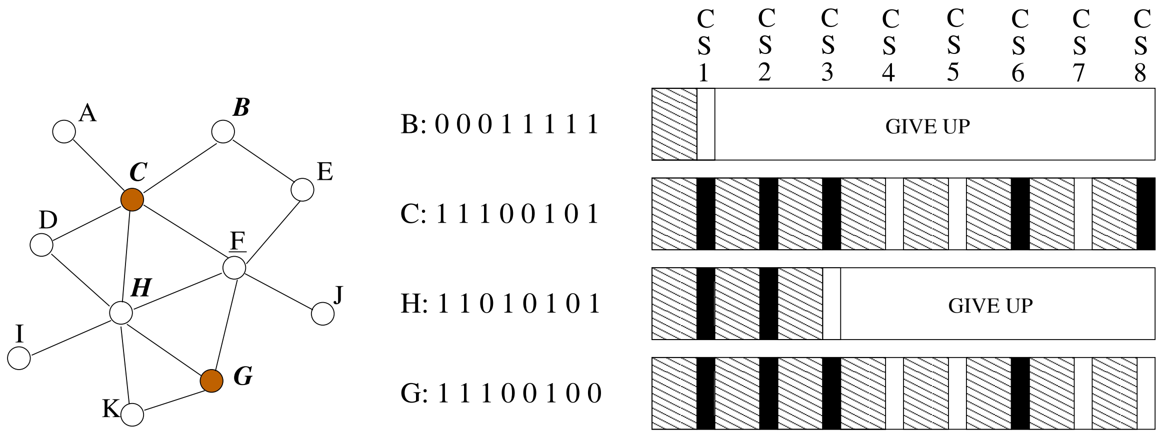

Figure 2: An example of contention resolution. The shaded nodes are the winner after Step 1. The nodes with underlines mark themselves as receivers.

which is a k-bit string with the i-th bit being 1 and all other bits being 0. After marking itself as a receiver, station Y ignores the following contention slots in this contention interval. Otherwise, if station Y receives a contention signal that contains another station's address, Y gives up its attempt to be a potential receiver and ignores the remaining contention slots in this contention interval.

An example of contention resolution is illustrated in Fig. 2. Consider a network that includes eleven stations, labelled from A to K. Two stations are connected by a link in the graph if they are within the transmission range of each other. Assume stations B, C, H, and G have data to send to stations E, F, G, and F, respectively. Note that due to the limited transmission range of wireless interfaces, not all of the four stations are competing with each other. For example, station B only competes with station C; station C competes with stations B and H; station H competes with stations C and G; station G competes with station H only. Each of the four stations generates a random number as shown in Fig. 2 (starting from the highest bit). After the first contention slot, station B gives up because it detects the transmission from station C. Similarly, station H gives up after the third contention slot. By the end of the contention interval, stations C and G survive and are ready to enter Step 2. At the same time, node F marks itself as a receiver, as it receives the contention signal from station C in the last contention slot. Note that, although stations E and G are the intended destinations of stations B and H, they do not mark themselves as receivers because they cannot receive valid contention signals from B (that has given up its transmission since the first contention slot) and H (that always transmits contention signals when node G is also in transmission mode), respectively.

3.1.2 Step 2: Hidden Station Elimination

After Step 1, only one station in a collision domain (i.e., no more than one adjacent stations) can survive, unless identical random numbers are generated. However, the hidden station problem in multi-hop wireless networks has not been addressed yet. For instance, since stations C and G cannot receive the contention signals from each other, both of them consider themselves as the winner after Step 1, and thus collision might occur during the data transmission interval. Note that, however, since station F receives the contention signals from both stations C and G, it can recognize the real winner (i.e., the one with a higher random number). In fact, in the above example, F has generated a random number mask 00000001 in Step 1, upon receiving the contention signal from station C in the last contention slot. In order to eliminate potential hidden stations, a station that has marked itself as a receiver in Step 1 sends a Hidden station Clear Message (HCM), which contains its random number mask. If a sender receives the HCM correctly, it computes the bitwise AND of the random number mask and the random number generated by itself. If the result is nonzero, it can proceed to Step 3. Otherwise, the station considers itself as a hidden station and gives up its attempt to access the channel in this frame.

3.1.3 Step 3: Data Transmission

In the last step, the sender transmits data, while the receiver responds with an acknowledgement if the received data is correct, in the data interval. All other nodes (including some nodes marked as receivers in Step 1) cannot send or receive data in this frame.

The protocol flow diagrams for the sender and the receiver are depicted in Fig. 3, which is self-explanatory.

3.2 Protocol Correctness

In this subsection, we deal with the correctness of the proposed protocol. More specifically, we prove that (1) there is no hidden station problem in the proposed protocol, and (2) if no duplicated random numbers are generated, at least one station can transmit successfully. The proof is outlined by discussing the following three cases.

Case 1: a receiver, say R, is in the transmission range of only one sender S. In this case, R will mark itself as a receiver when receiving the first contention signal from S, and send back the HCM message.

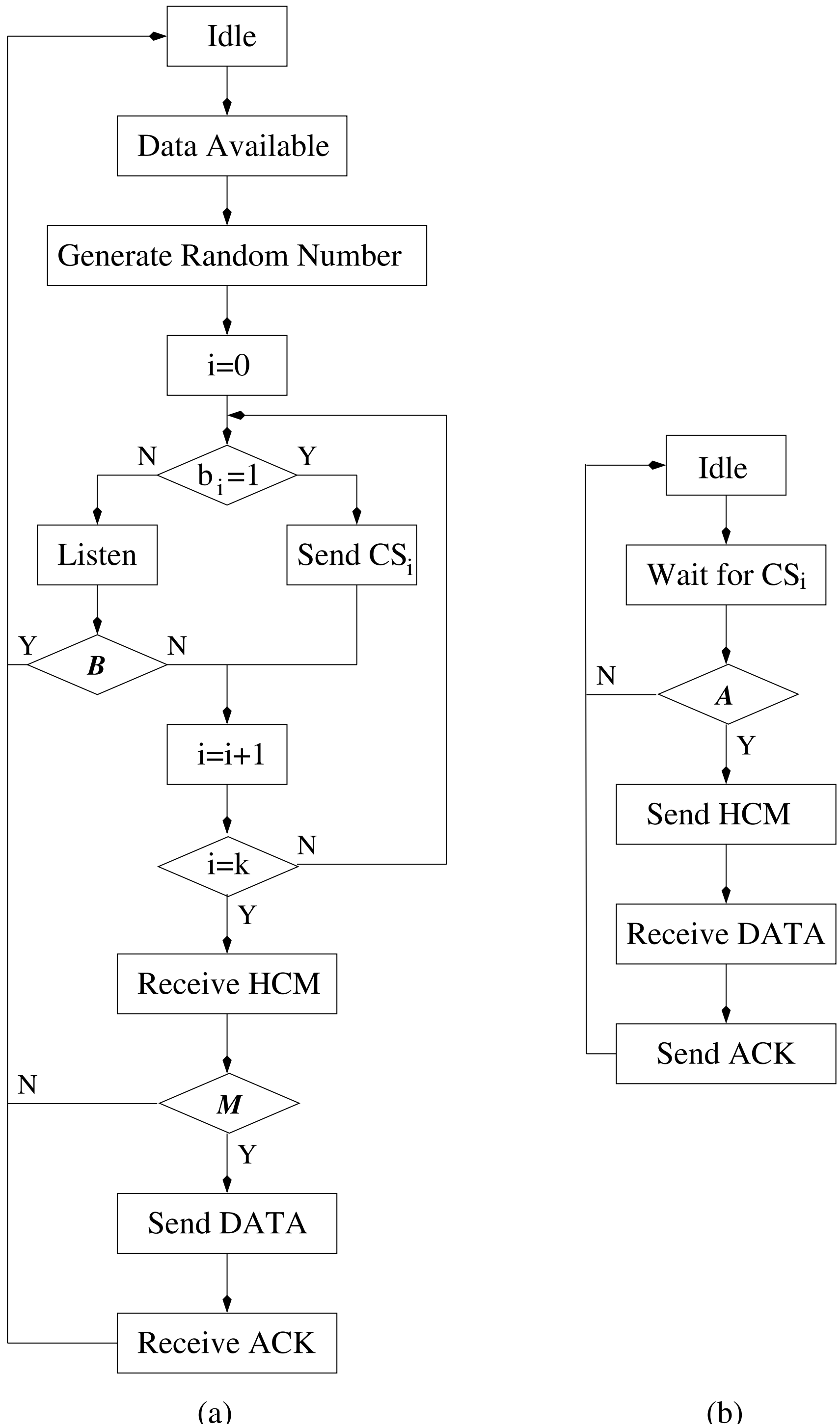

Figure 3: (a) Flow diagram for the sender. B: channel is busy; M: random number mask matches the random number generated by the sender. (b) Flow diagram for the receiver. A: destination MAC address matches the receiver's MAC address.

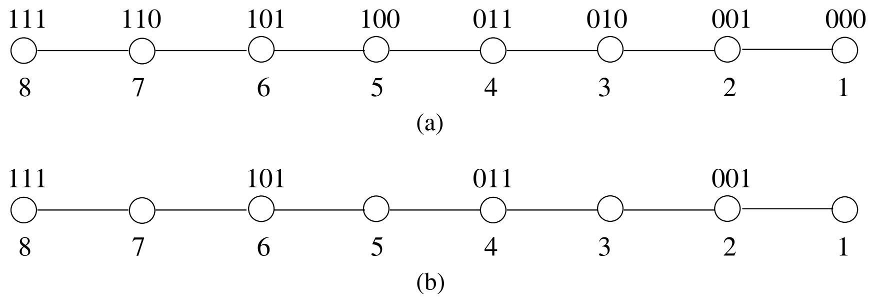

Figure 4: Worst case analysis, where (a) all stations are sender; (b) stations 2, 4, 6, and 8 are senders, and stations 1, 3, 5, and 7 are receivers.

Clearly, there is no hidden station problem for R (because there are no other senders nearby). If S generates a higher random number than its neighbors, it wins the right of transmission and sends the data to R. Otherwise, R will not receive any data (but another sender that has generated the largest random number will transmit).

Case 2: the receiver R is in the transmission range of more than one senders, but R is the intended receiver of only one sender S. In this case, (1) if S generates a larger random number than those of all other senders, R marks itself as the receiver upon getting a valid contention signal from S and sends the HCM message. Upon receiving HCM, S will send the data to R. At the same time, the HCM message blocks other nearby senders from transmitting data. Thus, there is no hidden station problem for R. (2) Otherwise, if the random number generated by S is equal to or smaller than any other sender's random number, R neither marks itself as a receiver nor sends the HCM message. As a result, S will not send data. But another sender which generates the largest random number will succeed.

Case 3: the receiver R is in the transmission range of more than one sender, and R is the intended receiver of more than one sender. Similar to Case 2.

3.3 Further Discussions

In this subsection, we analyze the worst case performance and discuss several unique features of the proposed SYN-MAC protocol.

3.3.1 Worst Case Analysis

Clearly, if all senders generate the same random number, no station can transmit data successfully. But as to be discussed in Sec. 4.1, one may choose proper k to keep the collision probability sufficiently low. In the following discussion, we assume all senders generate different random numbers, and investigate the inherent worst case when applying SYN-MAC to multi-hop wireless networks.

Intuitively, the performance bottleneck of SYN-MAC seems to be at Step 1, where the senders compete for channel access. In particular, the worst case *might* occur if the stations generate the random numbers with a non-increasing order from left to right (or vice versa), e.g., as shown in Fig. 4 (a), where the station identification (ID) numbers are at bottom and the random numbers generated by the stations are at top. In contrast to our intuition, however, Step 1 of SYN-MAC performs very well in this case. More specifically, after the first contention slot, only station 4 gives up (assuming to start from the highest bit); after the second contention slot, stations 2 and 6 give up; after the third contention slot, station 7 gives up. As a result, stations 1, 3, 5, and 8 survive after Step 1[*]. Since the adjacent stations cannot transmit simultaneously, the best scenario is to have four survival stations, as achieved in this case.

In fact, the real bottleneck is at Step 2, due to the receivers. For example, in a network illustrated in Fig. 4 (b), let stations 1, 3, 5, and 7 be the intended receivers of stations 2, 4, 6, and 8, respectively. After Step 1, all senders (i.e., stations 2, 4, 6, and 8) survive, and all receivers (i.e., stations 1, 3, 5, and 7) mark themselves as receivers. But when the receivers send HCM messages to the senders, a collision occurs at each sender except station 8. Consequently, only station 8 can send data[†]. This worst case results from the use of a distributed approach. Similar situations also appear in distributed schemes like HIPERLAN or IEEE 802.11.

3.3.2 Main features of SYN-MAC

The proposed SYN-MAC protocol has several unique features discussed as follows.

[*]This only shows that Step 1 is not the bottleneck. It does not imply that all senders (i.e., stations 1, 3, 5, and 8) can finish the data transmission successfully.

[†]Note that station 8 can finish a successful transmission even in a network with a circular topology, where station 8 has two neighbors, stations 1 and 7.

a) **Simplicity.** The implementation of SYN-MAC is simple. Compared with IEEE 802.11, SYN-MAC needs neither carrier sensing before transmission nor Network Allocation Vector (NAV) maintenance/updates. Since contention can be effectively relieved in Step 1, the back-off mechanism is unnecessary. This simple design results in significantly reduced computational complexity, memory requirement, and energy consumption.

b) **High Efficiency.** High throughput is achieved by choosing an appropriate k value as will be discussed in Sec. 4.1, so that the collision probability (due to two or more stations choosing the same largest random number) is sufficiently low, while the overhead of the contention interval is small. In addition, SYN-MAC exhibits no bandwidth waste during back-off (unlike that in IEEE 802.11), further improving its efficiency.

c) **Fairness.** Since every node generates a random number for each channel access attempt, no stations have *unwanted* priority over other stations. More over, the unfairness problem reported in [27] due to the back-off scheme of IEEE 802.11 DCF (which favors the sender of last successful transmission) does not exist in SYN-MAC.

d) **Robustness.** The protocol is highly robust as long as the synchronization can be maintained. Since channel contention starts all over again after each frame, any problem (e.g., the collisions), if arising, is temporarily for one frame only.

e) **Decentralization.** SYN-MAC is a distributed approach. Each station generates the random number by itself for channel contention. No central controller or infrastructure support is needed.

f) **QoS support.** The QoS support of our protocol can be efficiently achieved by dividing the random numbers into several blocks (see Fig. 5), one for each QoS class. When a station has data in class i to be sent, it generates a random number within block i to compete for the channel. The data with a higher QoS class has higher priority and will eliminate those channel access attempts with lower priority. In the same QoS class, the stations have an equal probability of access to the channel.

Class 4	0 0 0 0 0 0 0 0 ...... 0 0 1 1 1 1 1 1
Class 3	0 1 0 0 0 0 0 0 ...... 0 1 1 1 1 1 1 1
Class 2	1 0 0 0 0 0 0 0 ...... 1 0 1 1 1 1 1 1
Class 1	1 1 0 0 0 0 0 0 ...... 1 1 1 1 1 1 1 1

Figure 5: Random number blocks for different QoS classes.

Like other time-frame based approaches, SYN-MAC is less flexible than the non-synchronized schemes (e.g., IEEE 802.11 DCF). In particular, if the data packet size is smaller than the DATA field in the frame, some bandwidth is wasted. This problem can be alleviated by accumulating and aggregating traffic, avoiding to send single small datagrams.

4 Performance Evaluation

In this section, we evaluate the performance of SYN-MAC in terms of system throughput, packet delay, and collision probability. We first discuss an analytic model for a single collision domain. Then, we present the simulation results for general scenarios.

4.1 Analytical Study

As we discussed earlier, a contention slot includes the transmitting/receiving turnaround time and the time to send the contention signal (CS_i). With the Direct Sequence Spread Spectrum (DSSS) physical layer, the transmitting/receiving turnaround time (l_T) is less than 5 μs, and the physical layer convergence protocol (PLCP) header has a length of 48 bits. The contention signal contains a 48-bit receiver's MAC address. Assume the bandwidth is $M\ Mbps$, the total length of a contention slot l_c is no longer than $5 + (48 + 48)/M\ \mu s$. HCM contains the k-bit random number mask only, with a length of $l_{HCM} = (k + 48)/M\ \mu s$. The data and ACK messages have a similar format as the frame defined in IEEE 802.11, but without the "duration" field in the header. More specifically, each ACK message has 12 bytes, or equivalently $l_{ACK} = (12 \times 8 + 48)/M\ \mu s$. Data message is assumed to be 2342 bytes by default, leading to $l_d = (2342 \times 8 +$

48)/M μs.

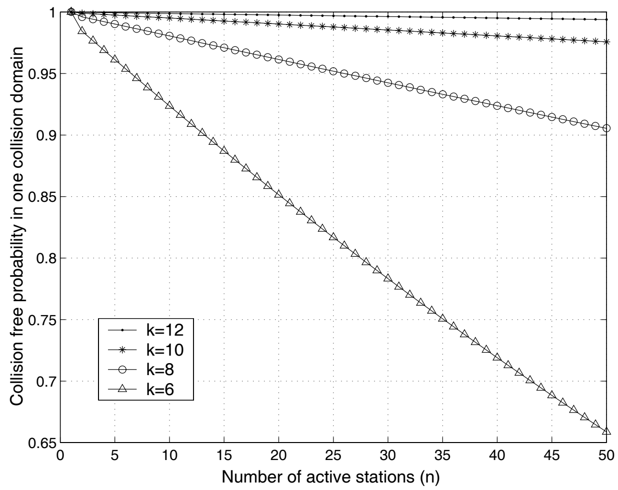

Figure 6: Analyzed collision-free probability.

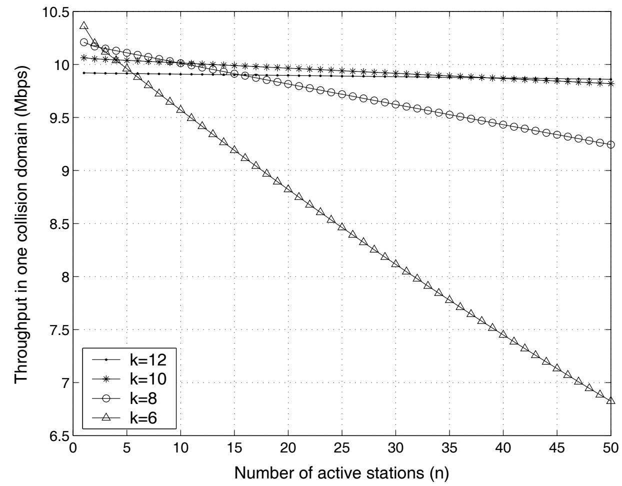

Figure 7: Analyzed throughput.

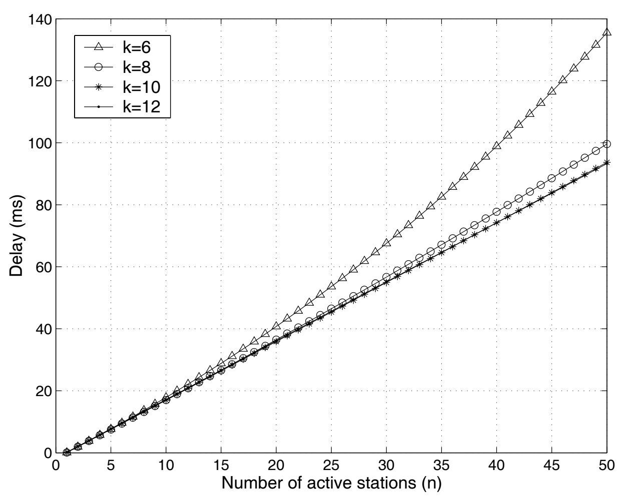

Figure 8: Analyzed delay.

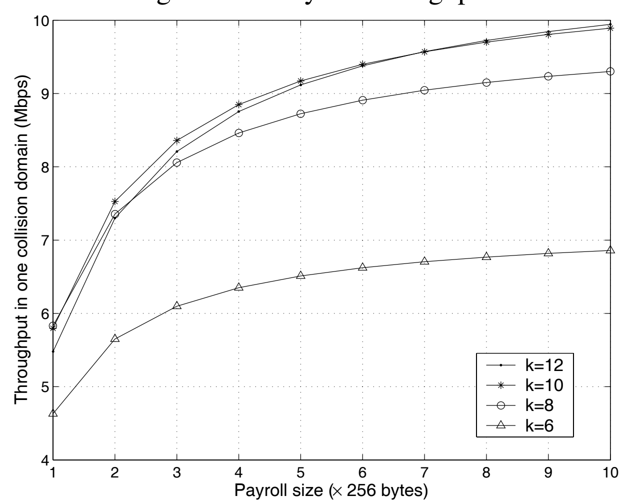

Figure 9: The impact of frame size.

The number of contention slots (k) in the contention interval determines the collision probability. Assume there are n active stations in a collision domain (i.e., n stations within the transmission range of each other have data to send). Each station has a probability of $1/2^k$ to choose a particular random number between 0 and $2^k - 1$. Note that collision occurs only if two or more stations choose the *same largest* random number, which again ranges from 0 to $2^k - 1$. We examine all possible cases as follows. The probability that exactly one station chooses $2^k - 1$ as its random number (i.e., one station chooses $2^k - 1$, while the remaining stations don't choose $2^k - 1$) is

$$n(\frac{1}{2^k})(1 - \frac{1}{2^k})^{n-1}.$$

Similarly, we can derive the probability that exactly one station chooses j ($0 \leq j \leq 2^k - 1$) as its random number and no other stations choose a random number greater than or equal to j,

$$n(\frac{1}{2^k})(1 - \frac{2^k - j}{2^k})^{n-1}.$$

Therefore, the probability that collision does not occur is

$$P_k^n = \sum_{j=0}^{2^k-1} n(\frac{1}{2^k})(1 - \frac{2^k - j}{2^k})^{n-1}. \quad (1)$$

Accordingly, the average throughput in one collision domain equals

$$S_k^n = \frac{l_d}{l} \times P_k^n, \quad (2)$$

where $l = l_C + l_H + l_D$ with $l_C = kl_c$, $l_H = l_{HCM} + l_T$, and $l_D = l_d + l_{ACK} + 2l_T$.

We can also derive the average delay for a data packet, which is defined as the duration from the time when the data is ready for transmission to the time when the data is actually sent out. Assume a given station has data to send, the probability that it wins channel access at the m-th attempt (and has failed at the first $m - 1$ attempts) is

$$P_k^n(m) = (\sum_{j=0}^{2^k-1} (\frac{1}{2^k})(1 - \frac{2^k - j}{2^k})^{n-1}) \times (1 - \sum_{j=0}^{2^k-1} (\frac{1}{2^k})(1 - \frac{2^k - j}{2^k})^{n-1})^{m-1}.$$

Thus, the average delay is expressed by

$$D_k^n = l_C + l_H + \sum_{i=1}^{\infty} (i - 1) \times l \times P_k^n(i). \quad (3)$$

Assuming the available bandwidth to be $M = 11$ Mbps and plugging in the typical values discussed earlier, we get the results as shown in Figs. 6–8. When a small number of stations are active, contention is low, and thus the collision probability is low, the throughput is high, and the delay is low. With the increase of n, the collision probability and the delay increase accordingly. As can be observed, there is a tradeoff when choosing an appropriate k. With larger k, a lower collision probability can be achieved. But at the same time, large k also results in higher overhead, possibly leading to lower throughput and longer delay. In the protocol implementation, $k = 10$ can be chosen as the default value, with which the protocol can achieve above 90% channel efficiency and acceptable delay for a wide range of the number of stations (from 1 to 50) in one collision domain. Fig. 9 shows the impact of frame payload size. Clearly, the larger the datagram, the higher the channel efficiency. This indicates that reasonably large frame shall be used in SYN-MAC, and the stations may accumulate outgoing data in order to reduce wasted frame payload space.

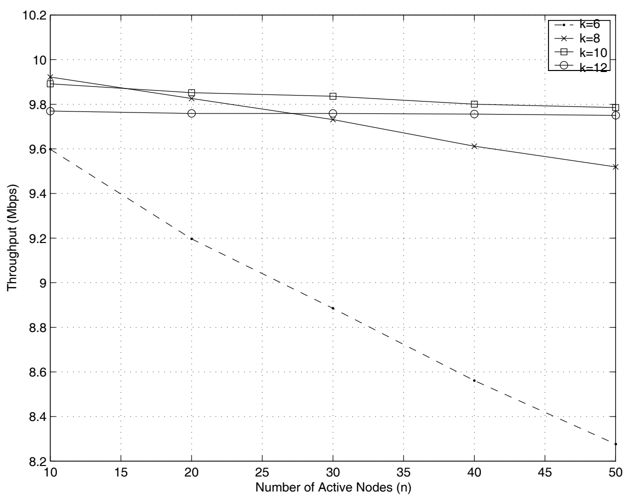

Figure 10: Throughput in a collision domain (simu.).

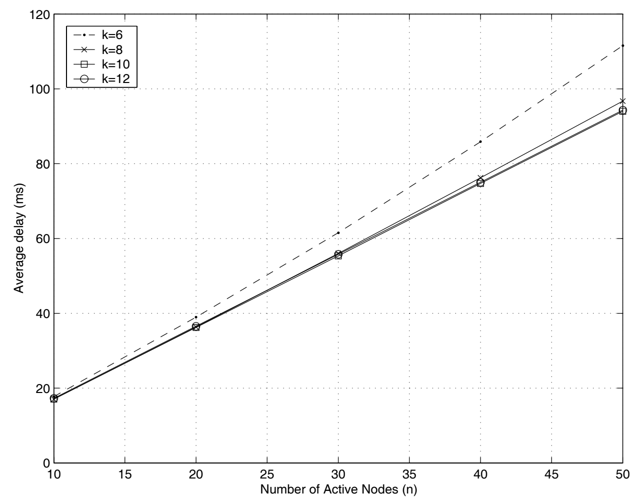

Figure 11: Delay in a collision domain (simulation).

4.2 Simulation Evaluation

To verify our analytic model and obtain results for general multi-hop networks, we have implemented the proposed SYN-MAC protocol by using PARSEC [28]. Similar to those parameters adopted in analysis, the maximum data frame size is 2342 bytes and an ACK frame has 12 bytes. Channel bandwidth is 11 Mbps. DSSS is employed in physical layer, with 8-chip complementary code keying modulation. We assume perfect channel condition, resulting in very low bit error rate. The transmitting/receiving turnaround time equals 5 μs[‡]. 48-bit MAC address is used to identify each node in this simulation. Shorter identifiers (e.g., the lower 16 bits of the MAC address), however, may be employed to reduce overhead and improve system performance. We assume that the stations always have data ready to send. Several scenarios are simulated with variable numbers of nodes (from 10 to 625), different nodal transmission ranges, and a range

[‡]A shorter turnaround time can normally be achieved, resulting in better performance.

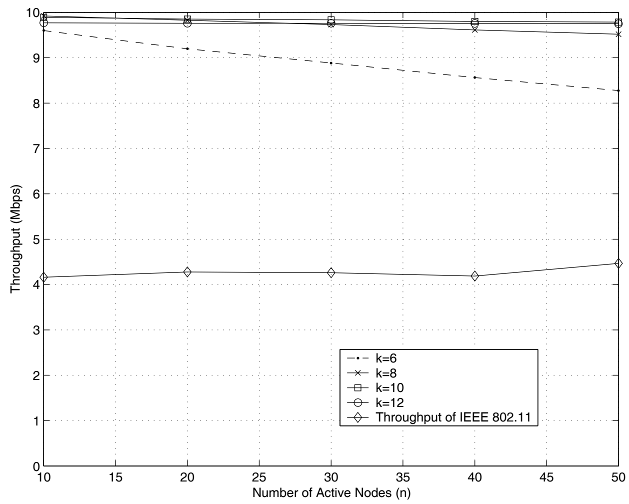

Figure 12: Throughput comparison (simulation).

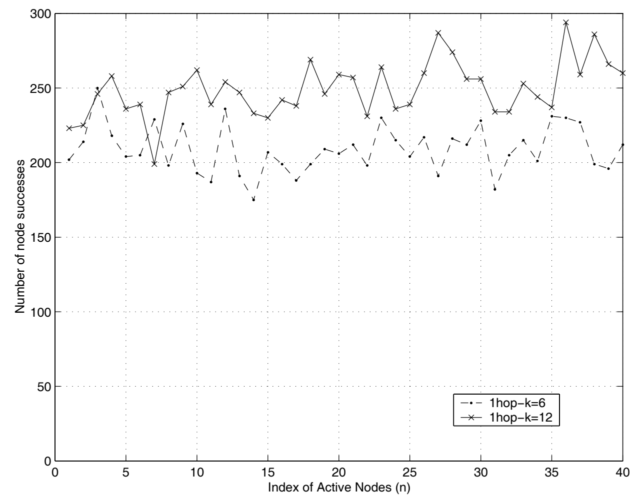

Figure 13: Fairness of SYN-MAC (simulation).

of contention slots ($4 \leq k \leq 12$).

Figs. 10 and 11 demonstrate the throughput and the delay performance of a network in one collision domain. As can be seen, the simulation results closely match our analytic model presented in Sec. 4.1. When k is small (e.g., $k = 6$), the large number of collisions result in low throughput and long delay (due to abundant retransmissions). This effect becomes more evident for the network with more nodes (and thus higher contention). When k is reasonably large (e.g., $k = 10$ or 12), the system with up to 50 active nodes can achieve the throughput about 9.8 Mbps and the average delay lower than 100 ms. As shown in Fig. 12, SYN-MAC achieves significantly higher throughput compared with IEEE 802.11 under similar traffic load. Additionally, SYN-MAC exhibits fairness among all active nodes, as we can see from Fig. 13, where every node has similar throughput with small variation around the average.

We have also simulated a multi-hop wireless network with a grid topology that includes $25 \times 25 = 625$ nodes. The distance between two adjacent nodes is 1 unit. The transmission range of a node is r. To eliminate the edge effect (i.e., nodes at the network edge tend to experience lower contention), we consider merely the core of the network, where all ($16 \times 16 = 256$) nodes in the core have the same number of neighbors. Fig. 14 shows the total throughput of core with 16×16 nodes. For $r = 5$ units, each node has about 80 neighbors, thus experiencing very high contention. The throughput rises with an increase in k (though not obvious from the figure), because larger k helps resolve contention under heavy traffic load.

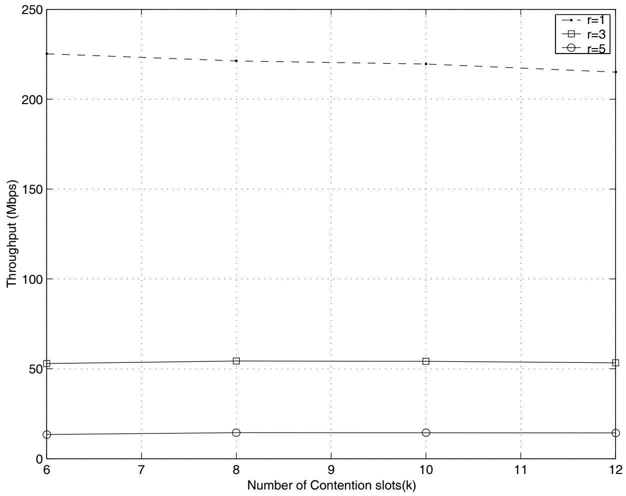

Figure 14: Throughput in a grid network (simulation).

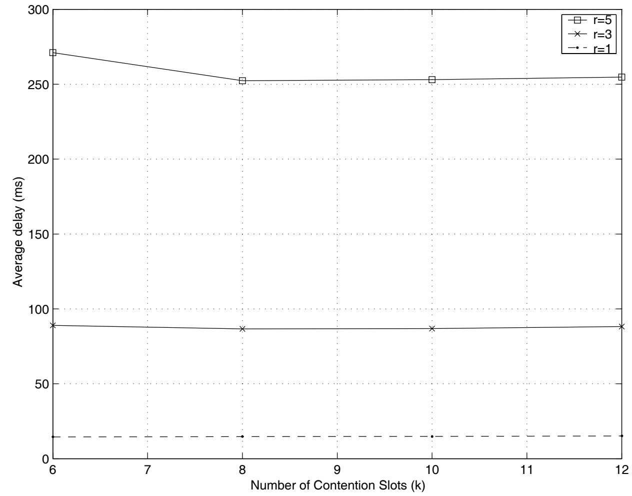

Figure 15: Delay in a grid network (simulation).

Delay performance is illustrated in Fig. 15. When $r = 1$, each node has only four neighbors. Hence, the channel contention is very low, leading to high throughput and low delay. With the increase of r, contention grows, and thus the delay becomes longer. Due to the scale of Fig. 15 (in order to show the results with different r values), the delay change with respect to k becomes not apparent. In fact, the number of contention slots (k) has similar affects on the delay as demonstrated in Fig. 11. More specifically, when contention is low (i.e., $r = 1$), a small k results in low delay because of small overhead. On the other hand, if contention is high (i.e., $r = 5$), a large k is needed to resolve the contention problem.

In addition, we have simulated the networks with randomly distributed nodes in an area of $500m \times 500m$, and each node has a transmission range of $210m$. The throughput as a function of n is depicted in Fig. 16. Note that, although there are 10-40 active stations (similar to the case in Fig. 10), actual contention in the multi-hop network is much lighter because the channel can be spatially reused and not all nodes are competing with each other. Thus, with an increase in the number of stations (i.e., with network size growth), the total network throughput increases monotonically, until it reaches a certain n value (e.g., $n = 30$ for $k = 6$). Similar to what can be found in Fig. 10, $k = 10$ in this figure results in best throughput. The delay in the network with a random topology is similar to that in the grid network as discussed above, according to our simulation outcomes. Thus, the results are omitted here.

SYN-MAC achieves significantly better performance compared with existing protocols according to the results (though not shown here) reported in the literature. For example, the maximum channel efficiency of

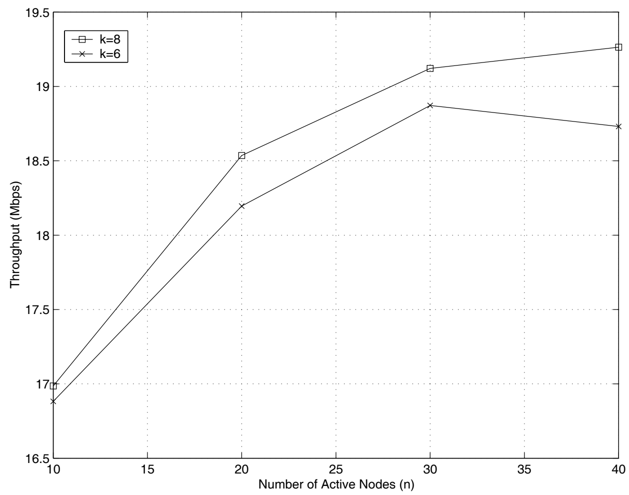

Figure 16: Throughput in a random network (simulation).

ADHOC MAC is only 75% [8], while SYN-MAC can readily exceed 90% channel efficiency with a properly chosen k value. The CSMA/CP protocol [7] may yield zero collision probability, but its serious unfairness is not acceptable in most distributed wireless networks. Other protocols discussed in Sec. 2 are not comparable with SYN-MAC, because they are designed for wireless networks either with centralized controller or without time synchronization, thus inappropriate for synchronized multi-hop wireless networks; if employed, such a protocol performs much worse than SYN-MAC or may even fail altogether.

5 Conclusion

In this paper, we have proposed a novel medium access control (MAC) protocol, called SYN-MAC, for synchronized multi-hop wireless networks. SYN-MAC is a distributed, simple, robust, efficient, fair, and QoS-capable MAC protocol that effectively resolves channel contention and deals with the hidden station problem in wireless networks. We have evaluated SYN-MAC in terms of collision probability, packet delay, and system throughput, via both analysis and simulation. Our results show that a network system using SYN-MAC can achieve a low collision probability, packet delay tolerance, and very high channel efficiency (exceeding 90%) under a wide range of traffic load. In our future work, we shall implement the proposed SYN-MAC protocol in our wireless network testbed, and investigate into the overall system performance under different transport and network layer protocols. SYN-MAC could be standardized and serve as an alternative to IEEE 802.11 for the mobile stations in synchronized networks.

Acknowledgment

We would like to thank Yijun Li at the Center for Advanced Computer Studies, University of Louisiana at Lafayette for his help on our simulation.

References

[1] Y.D Lin and Y.C Hsu, "Multihop Cellular: A New Architecture for Wireless Communication," in *Proceedings of IEEE Conference on Computer Communications (INFOCOM'00)*, March 2000, pp. 1273–1282.

[2] X.-X. Wu, B. Mukerjee, and S.-H. Chan, "MACA - An Efficient Channel Allocation Scheme in Cellular Networks," in *Proceedings of IEEE Global Telecommunications Conference (Globecom'00)*, November 2000, vol. 3, pp. 1385–1389.

[3] H. Wu, C. Qiao, S. De, and O. Tonguz, "Integrated Cellular and Ad-hoc Relay Systems: iCAR," *IEEE Journal on Selected Areas in Communications special issue on Mobility and Resource Management in Next Generation Wireless System*, vol. 19, no. 10, October 2001.

[4] Wei Ye, John Heidemann, and Deborah Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," in *Proceedings of IEEE Conference on Computer Communication (INFOCOM'02)*, 2002, pp. 1567–1576.

[5] V.K. Garg and J.E. Wilkes, *Wireless and Personal Communications Systems*, Prentice Hall, 1996.

[6] IEEE, "IEEE std 802.11–Wireless LAN media access control (MAC) and physical layer (PHY) specifications," 1997.

[7] T. You, C.-H. Yeh, and H. Hassanein, "A new class of collision-prevention MAC protocols for ad hoc wireless networks," in *Proceedings of IEEE International Conference on Communications (IEEE ICC'03)*, May 2003.

[8] F. Borgonovo, A. Capone, M. Cesana, and L. Fratta, “ADHOC MAC: a new, flexible and reliable MAC architecture for ad-hoc networks,” in *Proceedings of IEEE Wireless Communications and Networking Conference (IEEE WCNC’03)*, March 2003.

[9] P. Karn, “MACA: A new channel access method for packet radio,” in *Proceedings of ARRL/CRRL Amateur Radio 9th Computer Networking Conference*, September 1990, pp. 134–140.

[10] V. Bharghavan, A. Demers, S. Shenker, , and L. Zhang, “MACAW: A media access protocol for wireless lan’s,” in *Proceedings of ACM SIGCOMM ’94*, 1994, pp. 212–225.

[11] J. J. Garcia-Luna-Aceves and Chane L. Fullmer, “Floor Acquisition Multiple Access (FAMA) in Single-Channel Wireless Networks,” *ACM Mobile Networks & Applications Journal (MONET)*, vol. 4, no. 3, pp. 157–174, 1999.

[12] E. Jung and N. H. Vaidya, “A Power Control MAC Protocol for Ad Hoc Networks,” in *Proceedings of ACM/IEEE the 8th Annual International Conference on Mobile Computing and Networking (MobiCom’02)*, September 2002, pp. 36–47.

[13] J. Monks, V. Bharghavan, and W. Hwu, “A Power Controlled Multiple Access Protocol for Wireless Packet Networks,” in *Proceedings of IEEE Conference on Computer Communication (INFOCOM’01)*, April 2001, pp. 219–228.

[14] L. Bao and J. J. Garcia-Luna-Aceves, “Transmission Scheduling in Ad hoc Networks with Directional Antennas,” in *Proceedings of ACM/IEEE the 8th Annual International Conference on Mobile Computing and Networking (MobiCom’02)*, September 2002, pp. 48–58.

[15] R. Choudhury, X. Yang, R. Ramanathan, and N. H. Vaidya, “Using Directional Antennas for Medium Access Control in Ad hoc Networks,” in *Proceedings of ACM/IEEE the 8th Annual International Conference on Mobile Computing and Networking (MobiCom’02)*, September 2002, pp. 59–70.

[16] Y. Ko, V. Shankarkumar, and N. H. Vaidya, “Medium Access Control Protocols using Directional Antennas in Ad Hoc Networks,” in *Proceedings of IEEE Conference on Computer Communication (INFOCOM’00)*, March 2000, pp. 13–21.

[17] F. Tobagi and L. Klienrock, “Packet Scheduling in Radio Channel: Part II - The Hidden Terminal Problem in Carrier Sense Multiple Access and the Busy Tone Solution,” *IEEE Tranctions on Communications*, vol. 23, pp. 1417–1433, 1975.

[18] J. Deng and Z. Haas, “Dual Busy Tone Multiple Access (DBTMA): A New Medium Access Control for Packet Radio Networks,” in *Proceedings of IEEE Internaltional Conference on Universal Personal Communications (ICUPC’98)*, October 1998, pp. 973–977.

[19] S. Wu and Y. Tseng, “Intelligent Medium Access for Mobile Ad Hoc Networks with Busy Tones and Power Control,” *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 9, pp. 1647–1657, 2000.

[20] A. Nasipuri, J. Zhuang, and S. Das, “A multichannel CSMA MAC protocol for multihop wireless networks,” in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC’99)*, September 1999.

[21] S.L. Wu, C.Y. Lin, Y.C. Tseng, and J.P. Sheu, “A New Multi-Channel MAC Protocol with On-Demand Channel Assignment for Mobile Ad Hoc Networks,” in *Proceedings of International Symposium on Parallel Architectures, Algorithms and Networks*, December 2000, pp. 232–237.

[22] A. Nasipuri and S. Das, “Multichannel CSMA with signal power-based channel selection for multihop wireless networks,” in *Proceedings of IEEE Fall Vehicular Technology Conference (VTC Fall 2000)*, September 2000, pp. 211–218.

[23] A. Nasipuri and S. Das, “Multichannel CSMA with signal power-based channel selection for multihop wireless networks,” in *Proceedings of IEEE Fall Vehicular Technology Conference (VTC Fall 2000)*, September 2000, pp. 211–218.

[24] Y. Li, H. Wu, D. Perkins, N. Tzeng, and M. Bayoumi, “MAC-SCC: Medium Access Control with a Separate Control Channel for Multihop Wireless Networks,” in *Proceedings of Workshop on Mobile and Wireless Networks (MWN 2003)*, May 19-22, 2003.

[25] ETSI, “Hiperlan Functional Specification,” ETSI Draft Standard, 1995.

[26] A. Tanenbaum, *Computer Networks*, Prentice Hall, 2003.

[27] S. Xu and T. Saadawi, “Revealing the Problems with 802.11 MAC Protocol in Multi-hop Wireless Ad Hoc Networks,” *Journal of Computer Networks*, vol. 38, no. 4, pp. 531–548, March 2002.

[28] R. Bagrodia, R. Meyer, M. Takai, Y. Chen, X. Zeng, J. Martin, B. Park, and H. Song, “PARSEC: A Parallel Simulation Environment for complex systems,” *Computer*, pp. 77–85, Oct. 1998.