Multi-channel Medium Access Without Control Channels: A Full Duplex MAC Design

Yan Zhang, Loukas Lazos, Kai Chen, Bocan Hu, and Swetha Shivaramaiah
Dept. of Electrical and Computer Engineering, University of Arizona
Email: {yanzhang, llazos, chenkai, bocanhu, sshivaramaiah}@email.arizona.edu

APPENDIX

1 FD-MMAC Operational Examples

To ease the understanding of the FD-MMAC protocol, we present three operational examples. These examples demonstrate the fairness of the global backoff process, the destination discovery process performed by senders, the channel switching operation of destinations, and the operation of exposed terminals.

1.1 Fairness of the Global Backoff Operation

As outlined in Section 6.2, we adapt the CSMA backoff mechanism to the multi-channel environment. A sender retains his selected backoff value when switching channels and continues the countdown once it reaches an idle channel. When the backoff counter reaches zero, the sender maintains this value until it discovers the destination. This implements a global contention mechanism that extends to all channels.

In the example of Fig. **??**, we demonstrate the fairness of the global backoff process. Assume that three channels f_1, f_2, and f_3 are available. Three senders S_1, S_2, and S_3 have backoff counters b_1, b_2, and b_3 respectively with $b_1 < b_2 < b_3$. Ideally, we would like that the three senders occupy a channel in the order S_1, S_2, S_3, since $b_1 < b_2 < b_3$. Initially, S_1 and S_2 reside on f_1 while S_3 resides on f_2. Since $b_1 < b_2$, the backoff counter of S_1 will be the first one to expire and S_1 will occupy f_1. Once f_1 becomes busy, sender S_2 switches to f_2 while his counter is at $b_2 - b_1$. When the backoff counter of S_2 reaches zero, S_2 will occupy f_2, forcing S_3 to switch to f_3. S_3's backoff counter will be the last one to expire, thus maintaining the original order of transmission according to the selected backoff values b_1, b_2, and b_3.

1.2 Sender/Destination Operation

In the example of Fig. 1(a), we demonstrate the destination discovery performed by a sender. Initially, terminals A, B, C, and D reside on channel f_1. Terminal A initiates a data frame transmission to terminal B, which replies with BCN_B. Terminal D detects that f_1 is busy and switches to f_2, in order to be available for reception. Terminal C, who resides on f_1, has a frame P_C for D. Operating according to the sender state diagram of Fig. 6(c), terminal C transitions to the "Sense" state. Since f_1 is idle from C's perspective, C transitions to the "Backoff" state and uniformly selects a β from $[0, cw_0 - 1]$. When $\beta = 0$, terminal C transitions to the "Transmit" state and initiates the transmission of P_C. Because D resides on f_2, C does not receive BCN_D. Terminal C aborts further transmission of P_C and transitions to the "Switch" state. In this state, it updates the idle time for f_1 to $t_{curr} + T_{MTU}$ in the CST and switches to f_2, which has the lowest index among the idle channels. Once in f_2, terminal C transitions to the "Sense" state and senses f_2 to be idle. It then transitions to the "Backoff" state for a second time and retains $\beta = 0$. Terminal C retransmits P_C and completes the communication with D.

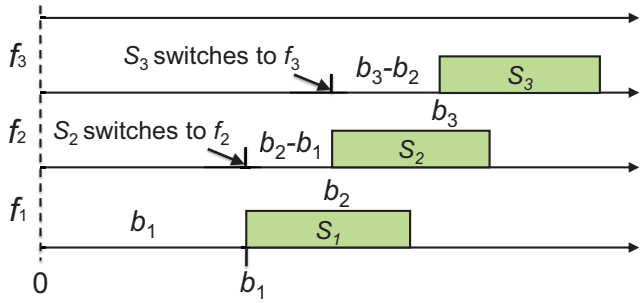
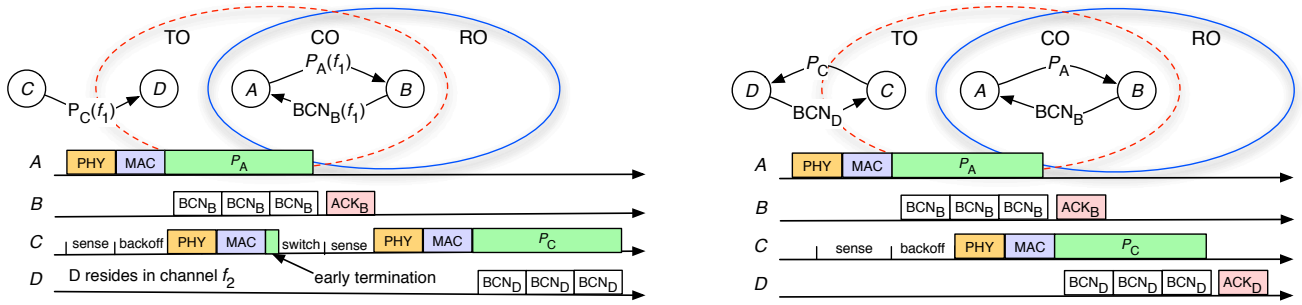


Fig. 1: The backoff process for three terminals S_1, S_2, and S_3 with backoff counters b_1, b_2, and b_3 respectively, and $b_1 < b_2 < b_3$.

1.3 Exposed Terminal Operation

In the example of Fig. 1(b), we demonstrate the operation of an exposed terminal. Terminal C has a data frame for terminal D while being in the TO region of the $A \rightarrow B$ transmission. While in the "Sense" state, terminal C determines that it is in the TO region by measuring a low EVM value and a low RSS value. Terminal C can therefore operate as an exposed terminal. Terminal C transitions to the "Backoff" state, selects β uniformly from $[0, cw_0 - 1]$, and initiates the backoff countdown. When $\beta = 0$, terminal C transitions to the "Transmit" state, and transmits data frame P_C. Because D is currently idle, it replies with BCN_D. Terminal C detects BCN_D using the signal correlation method and continues with the transmission of P_C. For the $A \rightarrow B$ communication, upon termination of the P_A transmission, terminal B transmits ACK_B. The acknowledgment ACK_B is detected at A using the signal correlation technique. Note that ACK_B is not decodable due to the concurrent transmission of P_C from C. Upon termination of



(a) Sender/Destination operation

(b) Exposed terminal operation

Fig. 2: Two operational examples of FD-MMAC.

the P_C transmission, D replies with ACK_D which is decodable at C, because the transmission of P_A is already completed.

2 Proof of Proposition 1

Proposition 1: The aggregate FD-MMAC throughput for M terminals contending over N channels under saturation is:

$$T = \sum_{u=1}^{N} \frac{p'_S \cdot p_d(f_u) \cdot payload}{E[\tau_{slot}(f_u)]}, \tag{1}$$

$E[\tau_{slot}(f_u)]$ denotes the average slot duration for channel f_u and $payload$ denotes the packet length in bits.

Proof: In a single-hop network with N available channels, the aggregate network throughput can be computed by summing the throughput of individual channels. To obtain the throughput of a channel f_u, we first compute the probabilities for the following events. Let p'_I denote the idle slot probability if no senders attempt to transmit during slot n. Let also p'_S denote the probability of a successful transmission, if exactly one sender transmits during slot n. Finally, let p'_C denote the collision probability if two or more senders attempt to transmit during slot n. The probability for each event is given by:

$$\begin{aligned} p'_I &= (1-p_{tr})^{\frac{M}{N}} \\ p'_S &= (\frac{M}{N}) p_{tr} (1-p_{tr})^{\frac{M}{N}-1} \\ p'_C &= 1 - p'_I - p'_S, \end{aligned} \tag{2}$$

where p_{tr} is sender's transmission probability at a time slot, and $\frac{M}{N}$ approximates the number of senders contending on one channel. Based on the Markov model described in Section 7, the transmission probability p_{tr} can be computed by summing over the probabilities of all states with a backoff counter value equal to zero on any of the N channels. This is because a saturated sender will initiate transmission on any channel, once its backoff counter reaches zero. Therefore, we have:

$$p_{tr} = \sum_{k=0}^{m} \pi_{\langle u,k,0 \rangle}, \quad 1 \le u \le N. \tag{3}$$

From (3), p_{tr} is also dependent on p_I given $p_d(f_u)$ and $p(f_u)$. Therefore, p_{tr} can be uniquely determined by finding a value satisfying the following equations:

$$\begin{cases} p_I = (1-p_{tr})^{\frac{M}{N}-1} \\ p_{tr} = \sum_{k=0}^{m} \pi_{\langle u,k,0 \rangle}, \quad 1 \le u \le N. \end{cases} \tag{4}$$

Based on (p'_I, p'_S, p'_C), the throughput of channel f_u can be computed by [**?**]:

$$T_{f_u} = \frac{p'_S \cdot p_d(f_u) \cdot payload}{E[\tau_{slot}(f_u)]}. \tag{5}$$

To derive the average slot duration for a channel, we need to know the actual length of a success, collision, and idle slot. Let them be denoted by τ_S, τ_C, and τ_I respectively. The length of a successful slot is defined as the duration of a successful transmission. FD-MMAC complies with the basic access mechanism of IEEE 802.11 DCF, a successful transmission includes the transmission of a data packet, a SIFS (Short Interframe Space) period, an ACK packet, and a subsequent DIFS (DCF Interframe Space) period before which the backoff process is resumed. Therefore, $\tau_S = \tau_p + \tau_{SIFS} + \tau_{ACK} + \tau_{DIFS}$, where τ_p and τ_{ACK} denote the transmission duration of data packet and ACK packet respectively, and τ_{SIFS} and τ_{DIFS} denote the SIFS and DIFS period respectively. The length of a collision slot in FD-MMAC is defined as the duration of a corrupted transmission or a transmission for which the destination is not detected. Recall that FD-MMAC employs an early collision detection mechanism, in which the sender uses the lack of BCN reply as an indication of a collision or of a failed destination discovery attempt. Thus, we have $\tau_C = \tau_{PHY} + \tau_{MAC} + \tau_{BCN} + \tau_{timeout}$, where τ_{PHY} and τ_{MAC} denote the length of PHY-layer and MAC-layer header, respectively, τ_{BCN} denotes BCN packet transmission duration, and $\tau_{timeout}$ is the time out period. The average slot duration for channel f_u is derived as:

$$\begin{aligned} E[\tau_{slot}(f_u)] &= p'_I \cdot \tau_I + p'_S \cdot p_d(f_u) \cdot \tau_S \\ &+ (1 - p'_I - p'_S \cdot p_d(f_u)) \cdot \tau_C, \end{aligned} \tag{6}$$

Once $E[\tau_{slot}(f_u)]$ is obtained, we are able to compute the throughput of f_u using (5). The aggregate network throughput is then derived as follows:

$$T = \sum_{u=1}^{N} T_{f_u} = \sum_{u=1}^{N} \frac{p'_S \cdot p_d(f_u) \cdot payload}{E[\tau_{slot}(f_u)]}. \tag{7}$$

□

3 Proof of Proposition 2

Proposition 2: For a q-order modulation scheme, the PMF of RV $\mathbf{X}$ is:

$$\Pr[\mathbf{X}=x]=\frac{1}{q}\binom{\log_2 q}{x}. \tag{8}$$

Proof: For random values of $\mathbf{j}$ and $\mathbf{w}$, a transmitted symbol $\mathbf{s}$ is mapped to any of the q symbols of the constellation with equal probability. Therefore, the probability that x out of the $\log_2 q$ bits of $\mathbf{s}$ are flipped is:

$$\begin{aligned}\Pr[\mathbf{X}=x] &= \sum_{\mathbf{s}'}\Pr[\mathbf{r}\rightarrow\mathbf{s}':\mathcal{H}(\mathbf{s},\mathbf{s}')=x]\\ &= \frac{1}{q}\binom{\log_2 q}{x},\end{aligned} \tag{9}$$

where $\mathcal{H}(\mathbf{s},\mathbf{s}')$ is the Hamming distance between the bit pattern (Gray codeword) assigned to $\mathbf{s}$ and $\mathbf{s}'$, respectively. Proposition 2 follows immediately by noting that for any $\mathbf{s}$, there are exactly $\binom{\log_2 q}{x}$ symbols s' with a Hamming distance equal to x and $\mathbf{r}$ is decoded to one of these symbols with probability $\frac{1}{q}$. □

4 Proof of Proposition 3

Proposition 3: Let RV $\mathbf{S_y}=\mathbf{X_1}+\mathbf{X_2}+\ldots+\mathbf{X_y}$ be the number of flipped bits when y symbols are jammed. Here, $\mathbf{X_1}, \mathbf{X_2}, \ldots, \mathbf{X_y}$ are i.i.d.s, following the distribution in (8). The complementary cumulative probability mass function (CCMF) of $\mathbf{S_y}$ is:

$$\Pr[\mathbf{S_y}>e]=1-\left(\frac{1}{q}\right)^y\sum_{i=0}^{e}\binom{y\log_2 q}{i}. \tag{10}$$

Proof: To compute the CCMF of $\mathbf{S_y}$, we first note that $\mathbf{S_y}$ is the sum of y i.i.d.'s following the distribution of Proposition 2. The distribution of the sum of y i.i.d. RVs is given by the discrete convolution formula. We compute this formula for $y=2$ and then extend to the general case by induction. For RV $\mathbf{S_2}=\mathbf{X_1}+\mathbf{X_2}$, it follows that:

$$\begin{aligned}\Pr[\mathbf{S_2}=e] &= \sum_{i=0}^{e}\Pr[\mathbf{X_1}=i]\Pr[\mathbf{X_2}=e-i]\\ &= \sum_{i=0}^{e}\frac{1}{q}\binom{\log_2 q}{i}\frac{1}{q}\binom{\log_2 q}{e-i}\\ &= \left(\frac{1}{q}\right)^2\sum_{i=0}^{e}\binom{\log_2 q}{i}\binom{\log_2 q}{e-i}\\ &= \left(\frac{1}{q}\right)^2\binom{2\log_2 q}{e}.\end{aligned} \tag{11}$$

In (11), we have used the Vandermonde convolution theorem for the computation of the summation of binomial coefficients. For an arbitrary y, by induction (convolution of $\mathbf{S_{y-1}}$ with $\mathbf{X_y}$) the PDF of $\mathbf{S_y}$ is:

$$\Pr[\mathbf{S_y}=e]=\left(\frac{1}{q}\right)^y\binom{y\log_2 q}{e} \tag{12}$$

It is straightforward to verify that (12) is a valid probability distribution as:

$$\begin{aligned}\sum_{e=0}^{y\log_2 q}\Pr[\mathbf{S_y}=e] &= \left(\frac{1}{q}\right)^y\sum_{e=0}^{y\log_2 q}\binom{y\log_2 q}{e}\\ &= \left(\frac{1}{q}\right)^y 2^{y\log_2 q}\\ &= 1.\end{aligned}$$

From (12), it immediately follows:

$$\Pr[\mathbf{S_y}>e]=1-\left(\frac{1}{q}\right)^y\sum_{i=0}^{e}\binom{y\log_2 q}{i}. \tag{13}$$

□

5 Proof of Proposition 4

Proposition 4: The probability of jamming the first BCN of duration τ_{BCN} when switching to a busy channel is:

$$\Pr[\text{BCN}=jam]=1-\frac{\tau_{PHY}+\tau_{MAC}+\tau_{BCN}-\tau_j}{\tau_p}. \tag{14}$$

where τ_{PHY} and τ_{MAC} denote the lengths of PHY header and MAC header respectively.

Proof: Let the adversary switch to channel f_i during the transmission of P. The jammer's switching time and the transmission start time are independent events. Hence, without loss of generality, we assume that switching time follows a uniform distribution $\mathcal{U}(0,\tau_p)$[1]. To have the opportunity of jamming the first BCN packet, the jammer must switch to f_i before the end of the BCN transmission, which is equal to $\tau_{PHY}+\tau_{MAC}+\tau_{BCN}$. Moreover the jammer must have time to corrupt sufficient number of bits from the BCN. If the jamming period to drop BCN is equal to τ_j, the jammer must switch to f_i before time $\tau_{PHY}+\tau_{MAC}+\tau_{BCN}-\tau_j$ has elapsed from the beginning of the packet transmission. The proof follows by noting that the switching time follows the uniform distribution $\mathcal{U}(0,\tau_p)$. □

6 Proof of Proposition 5

Proposition 5: Let a $\Delta\times\Gamma$ cryptographic interleaver be constructed using random column sub-permutations $\Pi=\{\pi_1,\pi_2,\ldots,\pi_\Gamma\}$. The adversary is guaranteed to jam y consecutive symbols from the same codeword, if he jams $(y-1)\Delta+1$ consecutive symbols.

Proof: We first show that jamming $(y-1)D+1$ consecutive symbols is sufficient to jam y symbols from one codeword and for any permutation Π. Consider the jamming of $(y-1)D$ consecutive symbols, starting from any symbol $s[i]$. The $(y-1)D$ symbols span across at least $(y-1)$ columns of the interleaving block. By construction of Π, every column contains one symbol from each of the D codewords. Therefore, at least $(y-1)$ symbols from each codeword are jammed. Jamming one additional symbol guarantees that y symbols that belong to a single codeword are jammed.

1. In our analysis, we have ignored the case where the jammer switches to channel that is sensed to be busy due to the transmission of an ACK packet.

It can be easily shown by an example that jamming fewer than $(y-1)D+1$ consecutive symbols does not guarantee the jamming of y symbols from one codeword. Consider any Π that maintains a fixed symbol separation of D (symbols of any codeword are separated by $(D-1)$ other symbols). Such a Π can be obtained by simply rearranging the rows of the interleaving block. Because of the fixed symbol separation D, jamming $(y-1)D$ consecutive symbols leads to the jamming of exactly $(y-1)$ symbols from each of the D codewords. Hence, an additional symbol needs to be jammed to guarantee the jamming of y symbols from at least one codeword. □

REFERENCES

[1] C. Hu, H. Kim, and J. Hou. An analysis of the binary exponential backoff algorithm in distributed MAC protocols. Technical report, University of Illinois at Urbana-Champaign, 2005.