Performance Analysis of an In-Band Full-Duplex MAC Protocol for Future Wireless Networks

Wardah Sarmad, Syed Maaz Shahid, Ezhan Karasan, *Member, IEEE*, and Sungoh Kwon, *Senior Member, IEEE*

***Abstract*—In this article, we extend IEEE 802.11 from carrier-sense multiple access with collision avoidance to carrier-sense multiple access with collision detection (CSMA/CD) for in-band full-duplex (IBFD) wireless systems by utilizing the capabilities of full-duplex. In IBFD communications, nodes can effectively apply CSMA/CD but this may result in false alarms and missed collision detection due to residual self-interference. To analyze the performance of medium access control (MAC) protocol for an IBFD communications system, first, a Markov chain-based analytical model is designed for a CSMA/CD-based IEEE 802.11 distributed coordination function with IBFD capabilities. Then, the analytical expressions for goodput and packet loss probability are driven to investigate the impact of various parameters, including contention window size, packet length, and the number of nodes, on the performance of the designed model in the presence of sensing errors. The accuracy of the analytical model is validated by comparing the numerical and simulation results for saturated traffic conditions.**

***Index Terms*—Collision detection, goodput, in-band full duplex (IBFD), medium access control (MAC) protocol, Markov chain model, packet loss probability, wireless communications.**

I. Introduction

IN-BAND full-duplex (IBFD) technology is believed to meet the data demands expected from future-generation wireless systems [1], [2], [3]. Limited bandwidth and expensive radio resources are the biggest obstacles that conventional wireless communications technologies must overcome to provide high data rates. Simultaneous data transmission and reception on the same frequency band in IBFD systems [3] overcomes the scarcity of frequency spectrum by enhancing spectral efficiency and maximizing bandwidth utilization [2], [4]. Theoretically, IBFD communications can double the capacity of a wireless network if self-interference [5] due to simultaneous transmission and reception on the same frequency is perfectly eliminated [3], [6].

Manuscript received 3 March 2023; revised 27 July 2023 and 9 November 2023; accepted 20 December 2023. Date of publication 19 January 2024; date of current version 15 March 2024. This work was partly supported by Korea Hydro & Nuclear Power Company (2023) and the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant NRF-2021R1I1A3A04037415. *(Corresponding author: Sungoh Kwon.)*

Wardah Sarmad and Ezhan Karasan are with the Department of Electrical and Electronics Engineering, Bilkent University, 06800 Ankara, Türkiye (e-mail: wardahsarmad@gmail.com; ezhan@ee.bilkent.edu.tr).

Syed Maaz Shahid and Sungoh Kwon are with the Department of Electrical, Electronic and Computer Engineering, University of Ulsan, Ulsan 44610, South Korea (e-mail: maaz.shahid26@gmail.com; sungoh@ulsan.ac.kr).

Digital Object Identifier 10.1109/JSYST.2023.3348531

In order to fully utilize IBFD communications, wireless communications systems (including cellular systems and Wi-Fi) require upgrading of the physical layer along with the medium access control (MAC) layer. With IBFD communications, the carrier-sense multiple access with collision avoidance (CSMA/CA) MAC protocol [7] in IEEE 802.11 can be upgraded to carrier-sense multiple access with collision detection (CSMA/CD) [8] to increase the network capacity and sense the collisions earlier. The upgraded protocol in IBFD systems allows a node to detect the successful reception of a packet by sensing its own transmission. However, there exists imperfect self-interference in IBFD communications even after applying self-interference cancellation techniques called residual self-interference (RSI). RSI results in sensing errors (i.e., imperfect collision detection) including false collision detection and miss collision detection [9]. False collision detection (i.e., false alarm) reduces channel utilization, and missed collision detection ensures a lost packet, consequently reducing system output [10].

In the literature, many full-duplex MAC (FD-MAC) protocols have been designed and investigated to realize the full potential of IBFD systems. Authors have designed CSMA/CA-based MAC protocols for full-duplex communications and provided performance analyzes of the protocols [4]. However, a fixed contention window in the protocol does not follow the IEEE 802.11 Binary Exponential Backoff in case of a collision. An FD-MAC protocol for wireless networks was designed, and its performance was evaluated with a real-time implementation in [11]. A MAC layer scheme for full-duplex wireless networks was proposed [12]. The protocols in [11] and [12] deviate from the IEEE 802.11 distributed coordination function (DCF) mechanism. A distributed FD-MAC design based on the IEEE 802.11 DCF was proposed [13]. The authors did not provide an analysis of the protocol and neglected the effects of imperfect sensing in IBFD communications. Performance analysis of a MAC protocol for IBFD communications was provided in [14] but the impact of sensing errors (i.e., miss collision detection) on the designed protocol was not incorporated.

FD-MAC protocols were designed in [9], [15], and [16] based on a CSMA/CA mechanism. Markov chain models were used to carry out an analysis of the designed protocols, but some mechanisms of the IEEE 802.11 MAC protocol, such as the maximum retry, were not considered in the analytical models. In [16], the effect of sensing errors on the proposed mechanism was not discussed. The authors in [17] presented a MAC protocol based on CSMA/CD for wireless networks. Work

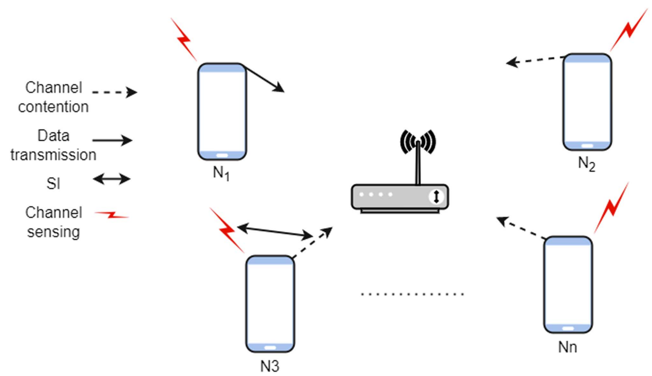

Fig. 1. Network architecture for the IBFD CSMA/CD protocol with n-contending nodes.

done in [9], [15], [16], and [17] only considered channel usage as the throughput in order to evaluate protocol performance, which does not accurately depict the successfully transmitted packets. Furthermore, the authors in [9], [15], and [17] did not treat collisions accurately and overlooked a possible miss collision detection due to imperfect sensing. It is feasible to extend IEEE 802.11 from CSMA/CA to CSMA/CD for IBFD wireless systems since nodes continuously sense the channel to detect collisions after transmission due to FD capabilities. Consequently, it becomes important to analyze the impact of sensing errors on the performance of the IBFD-MAC protocol.

In this article, we design a Markov chain-based analytical model for the IBFD MAC protocol using a CSMA/CD mechanism. To improve the model compared to [9], we introduce a maximum retry limit and backoff freezing mechanisms into the Markov chain model under the IEEE 802.11 MAC protocol. The maximum retry limit ensures a finite number of retransmission attempts by a node, while backoff freezing allows a node to freeze its backoff counter during the backoff process when sensing that the channel is busy. We derive analytical expressions for goodput and packet loss probability using the designed model to assess the performance of the CSMA/CD-based IBFD MAC protocol. Furthermore, we investigate the impact of various parameters, including packet length, contention window size, and the number of nodes, on the performance of the IBFD MAC protocol using simulation and numerical results.

The rest of this article is organized as follows. The system model and the IBFD MAC protocol design are explained in Sections II and III, respectively. Section IV discusses the analytical model of a CSMA/CD-based IBFD-MAC protocol using Markov chain model. Detailed numerical and simulation results are presented in Section V. Finally, Section VI concludes this article.

II. System Model

The network architecture considered for IBFD Wi-Fi networks includes an access point (AP) and n nodes that participate in channel contention by sensing its status (busy or idle), denoted as $(N_1, N_2, N_3, \ldots, N_n)$, as shown in Fig. 1. Nodes are randomly distributed in the coverage area of the AP. We assume there are two antennas on each node: one for data transmission and one for reception (sensing). Two separate antennas are used to achieve isolation between the transmitter and receiver by physical separation to avoid the effect of transmitter leakage [3]. All IBFD nodes sense the channel continuously, regardless of their actions, and only one node can access the channel at a time. In order to detect channel conditions, each node performs carrier sensing before transmission and contends for access using a backoff procedure. Nodes continuously sense the channel after transmissions to detect collision following the CSMA/CD mechanism. We assume that RSI exists between two antennas, even after suppressing the self-interference shown in Fig. 1.

A saturated traffic model (i.e., nodes always have packets to transmit to the AP) and an ideal channel (no errors or hidden terminals) are considered as described in [18] and [19]. When there is a collision between the transmissions of more than two nodes, collision detection is assumed to be perfect, since the collision signal is much stronger than the RSI. Detection errors occur only in two cases: when a single node transmits but a false collision is detected, or when two nodes start transmission at the same time, and the collision is not detected by at least one node.

III. IBFD MAC Protocol

The CSMA/CD-based IBFD MAC protocol is assumed to be time-slotted. The time slot is set to an opportune time in which a node can sense transmission from another node, and contending nodes determine which one will transmit at the end of each time slot. A node monitors the channel before initiating transmission. If the channel is sensed as free for the distributed interframe spacing (DIFS) period, the node attempts transmission [20]. Each node utilizes a binary exponential backoff and selects a random backoff time. The backoff time is uniformly distributed in the range $[0, \mathrm{CW}_i - 1]$, where CW_i is the contention window size and i is the number of failed transmissions for a specific packet (i.e., the collision count).

Each node has a maximum number of retransmission attempts, $W_{\max}$ after which the packet is dropped. When a node attempts the first transmission, the contention window size, CW_i, is set to $\mathrm{CW}_{\min}$, where $\mathrm{CW}_{\min}$ is the minimum contention window or initial contention window [21]. Whenever a collision occurs, the contention window of the node, CW_i, doubles in size until it reaches its capacity, which is the maximum contention window such that $\mathrm{CW}_{\max} = 2^{W_{\max}}\mathrm{CW}_{\min}$. The backoff counter decreases per slot when the channel remains idle; it stops when another transmission is sensed on the channel, and starts again when the channel is sensed as idle for more than the DIFS period. The node starts its transmission when the backoff counter reaches zero. When a packet is successfully delivered, the contention window size is set to $\mathrm{CW}_{\min}$.

There is the possibility of false alarms or missed collision detection due to sensing errors, or collisions, or successful transmissions when nodes send their packets under the CSMA/CD-based FD-MAC protocol. A scenario with three nodes $(N_1, N_2,$ and $N_3)$ that are contending for a channel to transmit their packets, is used to discuss different cases. A packet is transmitted successfully when a node (e.g., N_1) wins contention and sends its packet, as depicted with Case 1 in Fig. 2. The effect of a false

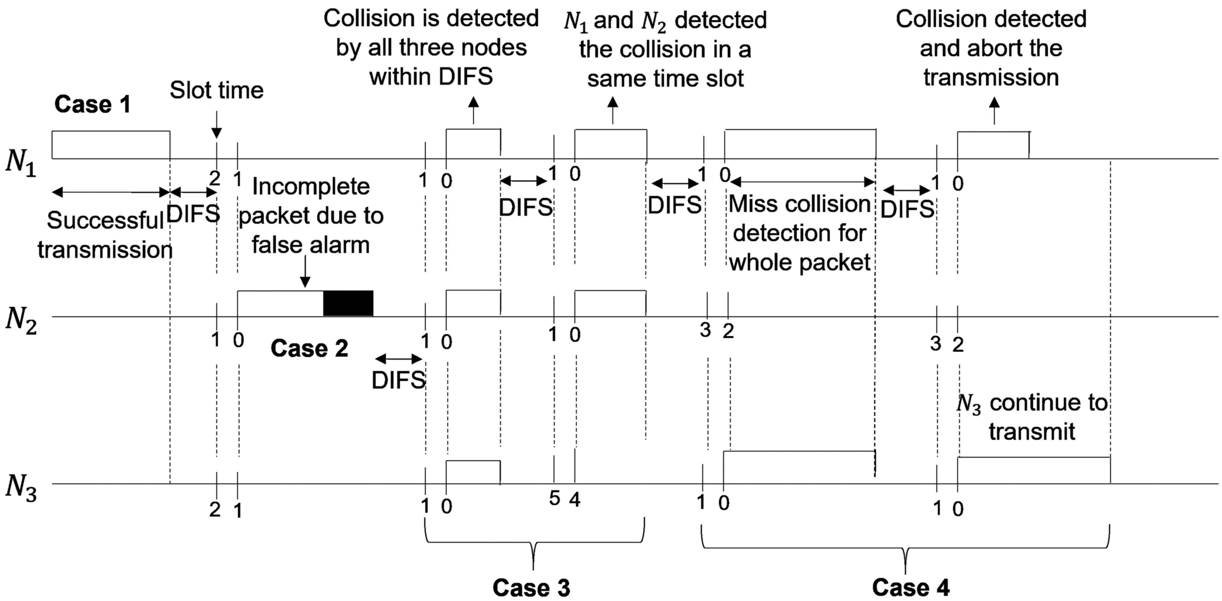

Fig. 2. Example scenarios under the IBFD-MAC protocol.

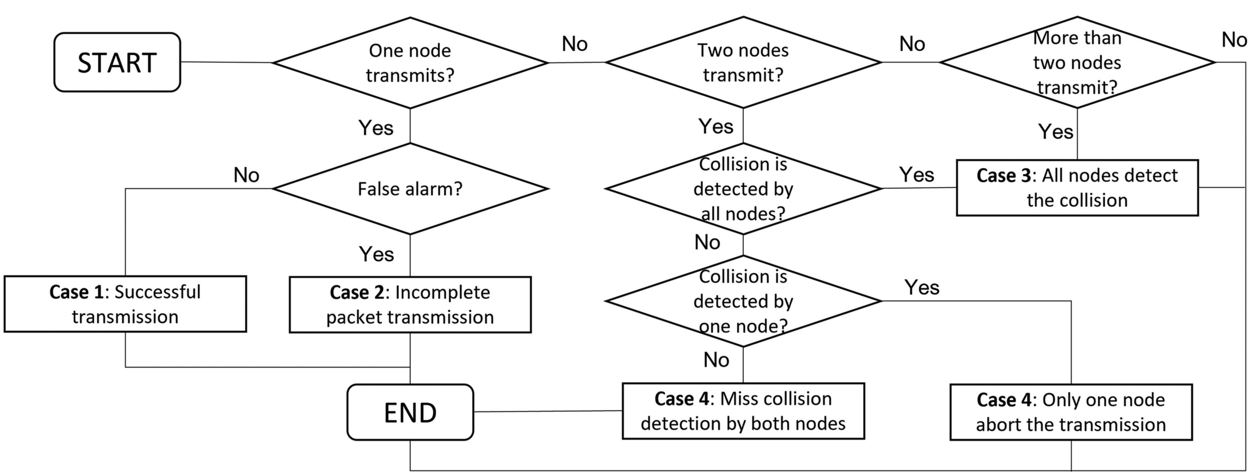

Fig. 3. Conditions for four cases happening due to contending for a channel by IBFD nodes.

alarm is shown in Case 2, where node N_2 starts transmission after the DIFS period while sensing the channel, incorrectly sensing a collision due to a sensing error, and immediately aborts transmission.

When two nodes start transmissions after contending for a channel, (let us say nodes N_1 and N_3 start transmitting after the backoff process), both nodes detect a collision and abort their transmissions at the same time. Similarly, when three nodes start transmitting in the same slot after the backoff process, they detect collisions within the DIFS period and terminate their transmissions all at once. Collision detection is labeled as Case 3 in Fig. 2.

Case 4 depicts two instances of missed collision detection. When both nodes do not sense a collision due to RSI, they continue to transmit and consider their packets to have been transmitted successfully. In another case, only one node (N_1) senses the collision, aborts transmission, and doubles its contention window size, whereas the other node (N_3) continues to transmit because now there is no way to detect a collision, and it sets its contention window to the initial length after completing the transmission. This is the main benefit of the CSMA/CD-based FD-MAC protocol over the conventional HD-MAC protocol when a collision does not last for the full-packet length under the CSMA/CD-based FD-MAC protocol. The conditions for four possible cases, which are shown in Fig. 2, are summarized in Fig. 3.

Based on the above-mentioned cases, we can say that when only one node is transmitting, all other nodes detect the transmission, i.e., a collision-free transmission is either successful or aborted due to a false alarm. When two nodes transmit, the collision can be detected or missed due to a sensing error, and when at least three nodes simultaneously start transmission, a collision is always detected by all the nodes within the DIFS period.

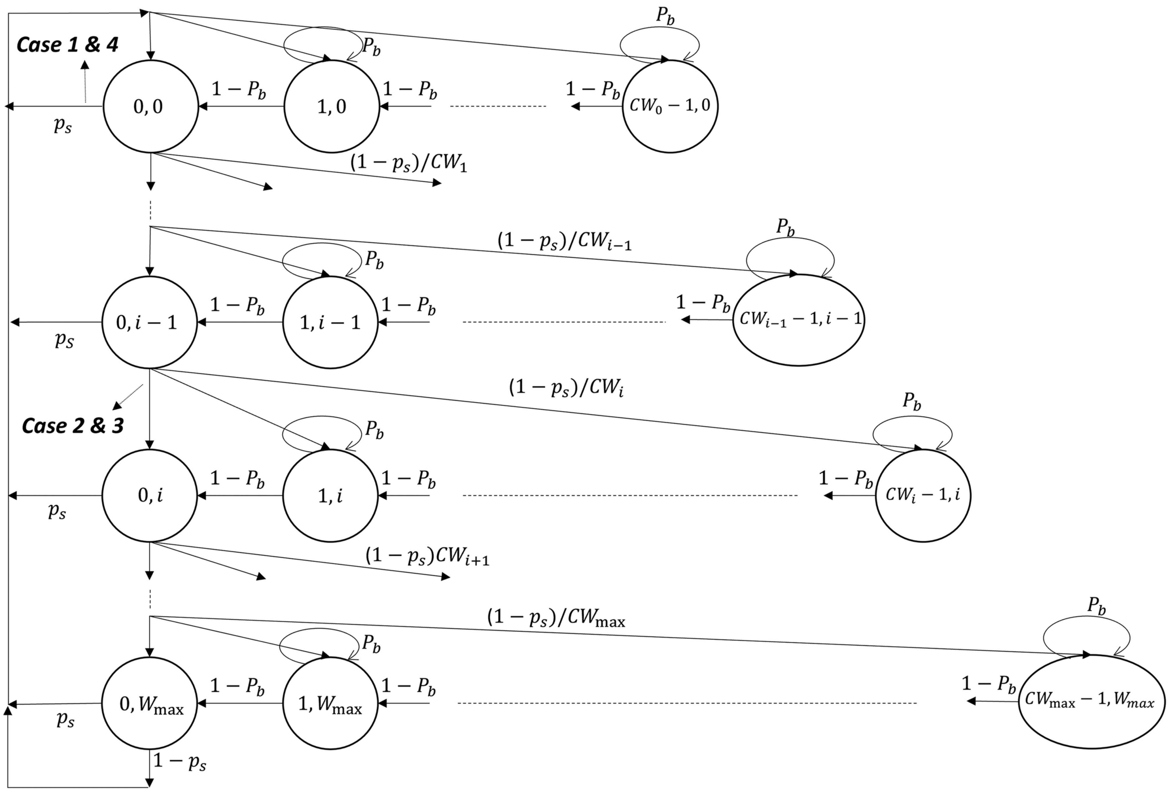

Fig. 4. Discrete-time Markov chain model.

IV. Performance Analysis

In this section, we analyze the performance of the proposed IBFD MAC protocol based on a modified bidimensional discrete-time Markov chain model [9], and we derive its goodput and its packet loss probability. Unlike throughput, which considers channel utilization as system output, goodput only considers the time intervals used for successful transmissions to be network output. We first derive the probability of packet transmission using the Markov chain model, and then (based on the probability of packet transmission) we derive the goodput and the packet loss probability to evaluate the performance of the IBFD MAC protocol.

A. Packet Transmission Probability

The bidimensional discrete-time Markov chain model [9] is modified to depict the actions of a single node, and the modified model is illustrated in Fig. 4. The Markov chain model is based on a critical approximation that includes a constant probability of a successful transmission without collision awareness, p_s, and a constant probability of a busy channel, P_b. We introduce the probability of a busy channel to account for the channel condition in the backoff procedure, which means the channel is busy with a probability of P_b. It is expressed as

$$P_b = 1 - (1 - p)^{n-1} \tag{1}$$

where p is the probability that a certain node begins transmission in the next slot and n represents the total number of nodes contending for the channel. The state of a node is represented by $\{w_i, W_i\}$, where W_i is the number of transmission attempts so far and w_i is the backoff time selected randomly from interval $[0, \mathrm{CW}_i - 1]$. Here, CW_i represents the contention window size. The relation between W_i and CW_i is

$$\mathrm{CW}_i = 2^{W_i}\mathrm{CW}_{\min}$$

where $\mathrm{CW}_{\min}$ represents the initial contention window size.

The packet starts its transmission from state $\{0, 0\}$. In the event of a collision, the node will transition to the next state with probability $(1 - p_s)/\mathrm{CW}_i$, whereas a successful transmission will cause the node to return to the state $W_i = 0$ with probability p_s/CW_0. When the channel is detected as busy, the node freezes its backoff counter and stays in the same state with probability P_b, indicating self-transitions. When the channel is free, with probability $1 - P_b$, the node will transition to the next state. Note that nodes perceive the state of the channel independently, and hence, their backoff counters decrement asynchronously unlike [20], e.g., while one node detects a collision, other nodes involved in the collision misdetects. If a node continuously experiences collisions, and the state reaches $W_{\max}$ (the maximum contention window size), the packet will be lost if the next retransmission attempt fails, and the Markov chain will transition back to the state $W_i = 0$ to transmit the next packet. The state transition of a node according to different cases including successful transmission (Case 1), false collision detection (Case 2), miss collision detection (Case 3), and collision detection (Case 4), can be seen in Fig. 4.

The one-step state transition probabilities are

$$P(k,i|k+1,i) = 1 - P_b, k \in [0, \mathrm{CW}_i - 2], i \in [0, W_{\max}] \tag{2}$$

$$P(k,i|k,i) = P_b, k \in [1, \mathrm{CW}_i - 1], i \in [0, W_{\max}] \tag{3}$$

$$P(k,0|0,i) = \frac{p_s}{\mathrm{CW}_0}, k \in [0, \mathrm{CW}_0 - 1], i \in [0, W_{\max}] \tag{4}$$

$$P(k,0|0,W_{\max}) = 1/\mathrm{CW}_0, k \in [0, \mathrm{CW}_0 - 1] \tag{5}$$

$$P(k,i|0,i-1) = \frac{1-p_s}{\mathrm{CW}_i}, k \in [0, \mathrm{CW}_i - 1], i \in [1, W_{\max}]. \tag{6}$$

State transition probability in (2) shows when a channel is idle, and the backoff time is decremented. The probability in (3) depicts a self-transition when the channel is busy, whereas (4) accounts for the fact that a successful transmission has occurred, and transmission now takes place with the backoff counter at 0. State transition probability in (6) takes care of the retry limit, and (5) describes an unsuccessful transmission. The probabilities in (2), (3), and (6) highlight the main modifications to create a more realistic Markov chain model.

Let $b_{k,i}$ be the stationary distribution of the chain, which is defined as

$$b_{k,i} = \lim_{t\to\infty} P\{b(t) = k, s(t) = i\}$$

where $b(t)$ is the backoff time counter and $s(t)$ represents the number of transmission attempts. By solving the global balance equation for the Markov chain model, we can get the probability of transmission by a node in the next slot, referred to as packet transmission probability p, (see Appendix A). It is expressed as

$$p = \frac{2(1-p)^{n-1}(2p_s - 1)(1-\omega)}{(2p_s - 1)(1-\omega) + \mathrm{CW}_{\min}(1 - (2-2p_s)^{W_{\max}+1})p_s} \tag{7}$$

where ω is equal to $(1-p_s)^{W_{\max+1}}$ and p_s is the probability of transmission for an entire packet by at least one node, which can be a successful transmission or a collision between transmissions. p_s is defined as follows [9]:

$$p_s = (1-p)^{n-1}(1-P_f)^L + (n-1)p(1-p)^{n-2} P_m \frac{(1-P_f)^L - P_m^{2L}}{1 - P_f - P_m^2} \tag{8}$$

where L is the length of a packet in a slot, P_f is the probability of a false alarm per slot, and P_m is the probability of a missed detection per slot. Equations (7) and (8) are nonlinear equations with the number of contending nodes. A fixed-point iteration method is applied to get the probabilities of p and p_s, as shown in Fig. 5. Two performance matrices (goodput and packet loss probability) are used to analyze the modified Markov chain model, which are discussed in the following subsections.

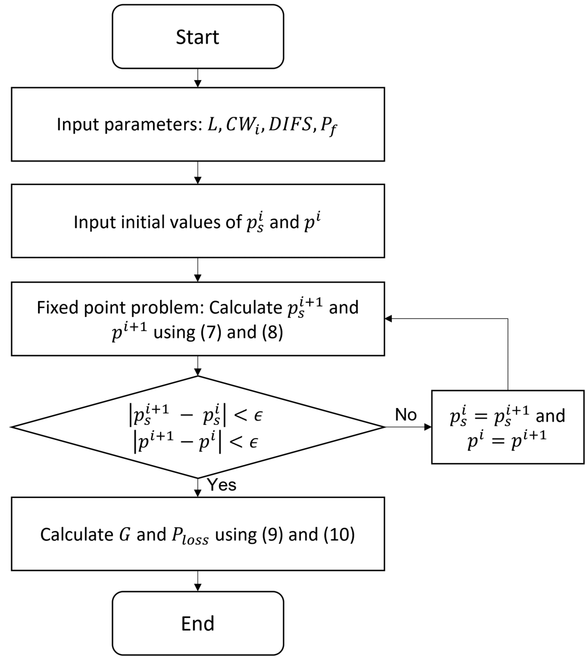

Fig. 5. Fixed-point iterative method for calculating goodput and the packet loss probability.

B. Goodput

Goodput is defined as the proportion of time the channel is occupied for successful transmissions and is expressed as

$$G = \frac{E[\text{Successful transmission length}]}{E[\text{Time consumed for a successful transmission}]} = \frac{P_S L}{P_E + P_S(L_S + \mathrm{DIFS}) + P_C(L_C + \mathrm{DIFS})} \tag{9}$$

where P_E is the probability of an empty channel, P_C denotes the collision probability, and P_S represents the probability of a successful transmission. These probabilities can be written as

$$P_S = \mathrm{np}(1-p)^{n-1}(1-P_f)^{L-1}$$
$$P_E = (1-p)^n$$
$$P_C = 1 - P_E - P_S.$$

L_S and L_C denote the average length of a successful transmission and the average length of a collision, respectively, and can be expressed, according to [9], as follows:

$$L_S = \frac{1-(1-P_f)^{L-1}}{P_f} + (1-P_f)^{L-1}$$

$$L_C = 1 + \binom{n}{2} p^2 (1-p)^{n-2} \frac{P_m^2(1-P_m^{2L-2})}{P_C(1-P_m^2)}.$$

Goodput in (9) is calculated by solving (7) and (8) for P_C, P_E, P_S, L_S, and L_C. The goodput in this work differs from throughput in that goodput only counts the packets that are successfully received, whereas throughput includes all packets that are transmitted, regardless of whether they are successfully received or not.

C. Packet Loss Probability

The packet loss probability P_{loss} indicates how frequently packets are not received correctly within the maximum number of transmission attempts, $W_{\max}+1$. To get the packet loss probability, we define P_{mrl}, which corresponds to the probability that a packet will not be transmitted successfully within the maximum number of retransmission attempts ($W_{\max}$), and P_{miss}, which is the probability of miss detection. P_{mrl} is expressed as (see Appendix B)

$$P_{\text{mrl}} = \omega = (1-p_s)^{W_{\max}+1}$$

where $W_{\max}$ is the maximum number of retransmission attempts. For P_{miss}, we considered missed detection scenarios where a collision by any one of two nodes is not detected. For example, a missed detection occurs when a collision is undetected by at least one node after two nodes start their transmissions in the same time slot. In the case of two simultaneously transmitting nodes (N_1 and N_2), a missed detection takes place when N_1 senses the collision and aborts transmission while N_2 continues to transmit, when N_2 senses the collision and terminates transmission while N_1 continues or when both nodes do not detect the collision. Hence, P_{miss} can be written as (see Appendix C)

$$P_{\text{miss}} = (n-1)p(1-p)^{n-2}\left[P_m^{2\,L} + \frac{P_m^2 - P_m^{2\,L}}{P_m^2 + P_m}\right].$$

Based on P_{mrl} and P_{miss}, P_{loss} becomes

$$P_{\text{loss}} = \omega + (n-1)p(1-p)^{n-2}\left[P_m^{2\,L} + \frac{P_m^2 - P_m^{2\,L}}{P_m^2 + P_m}\right]. \tag{10}$$

Packet loss probability is an important performance metric for a MAC protocol because the missed collisions cannot account for channel utilization. The analysis of the modified Markov chain for IBFD MAC protocol is verified by evaluating the performance in terms of goodput and the packet loss probability by using numerical and simulation results.

V. Numerical Results

In this section, we provide numerical results from the modified Markov chain model and compare them with simulation results to verify the correctness of our analysis. To that end, goodput and the packet loss probability of the IBFD MAC protocol are calculated using MATLAB.

A Monte Carlo simulation that ran for the duration of the simulation was set to 10^7 time slots. The parameters for a discrete-event simulation that follows the 802.11 DCF mechanism, are summarized in Table I based on [9]. In the case when only one node transmits, we calculate the goodput for this successful transmission. However, when two nodes simultaneously start transmissions in the same slot, collisions may occur, and collision detection might be affected by imperfect sensing in one of the nodes. If both nodes detect the collision, they will follow the backoff procedure; otherwise, the packet loss probability must be determined considering the multiple cases of missed collision detection.

TABLE I
Common Simulation Parameters

Parameter	Value
CW_{max}	2^{15}
n	100
P_f	10^{-3}
P_m	10^{-2}
DIFS	2 time slots
ϵ	10^{-7}

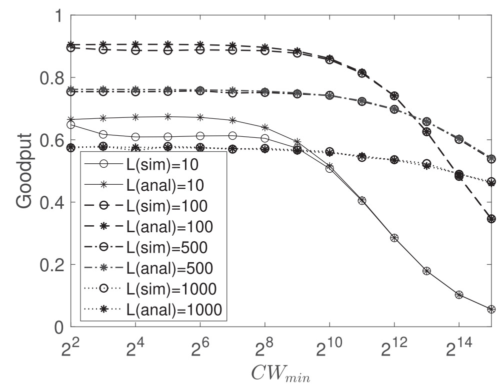

Fig. 6. Goodput with respect to $\text{CW}_{\min}$ for different packet lengths.

The impacts of different parameters (e.g., initial contention window size, packet length) on the designed IBFD-MAC protocols are examined in the presence of false alarms and miss collision detection. To verify the designed analytical model of the CSMA/CD-based IBFD MAC protocol, we compared it with two MAC protocols: CSMA/CA-based FD-MAC protocol [9] and the CSMA/CA-based HD-MAC protocol [20]. Both numerical and simulation results of the CSMA/CA-based FD-MAC protocol are provided for performance comparison. For the sake of simplicity, we denote the CSMA/CA-based HD MAC protocol as HD-MAC, CSMA/CA-based FD MAC protocol as FD-MAC, and the designed CSMA/CD-based MAC protocol as IBFD-MAC.

A. Effects of Different Parameters on Goodput

The goodput of IBFD-MAC protocol with respect to an initial contention window size for different packet lengths is shown in Fig. 6. The goodput was higher for a packet length of 100 when $\text{CW}_{\min}$ was less 2^{13}, compared to other packet lengths, which was the optimal packet length for maximum goodput. For a small packet length, i.e., $L = 10$, there are many more channel accesses to deliver packets, which increases the probability of collisions and leads to the waterfall effect. When the packet length was 500 and 1000, transmissions (and consequently, collisions) were reduced, but the false alarm effect became more prominent. This was the major cause of lower goodput with $L = 500$ or 1000 compared to goodput with $L = 100$.

The goodput for packet lengths of 10 and 100 fell below goodput for large packet lengths after a certain $\text{CW}_{\min}$, which can be seen in Fig. 6. For example, when L was 100, the goodput was more than when L was 500 up to $\text{CW}_{\min}$ at 2^{13}; after that,

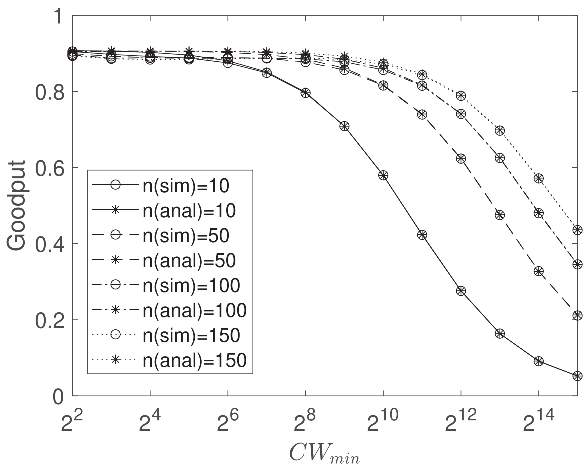

Fig. 7. Goodput versus the initial contention window size for different numbers of nodes.

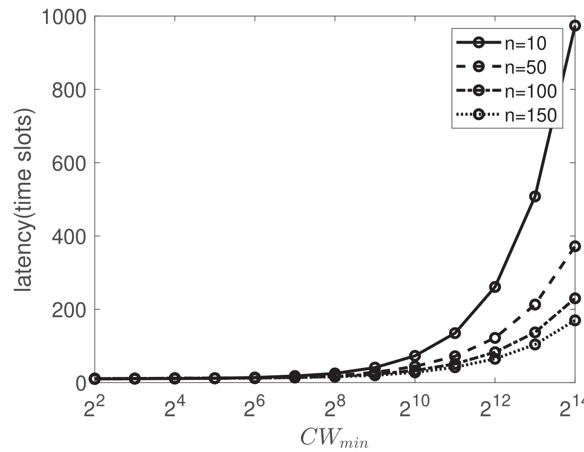

Fig. 8. Latency versus the initial contention window size for different numbers of nodes.

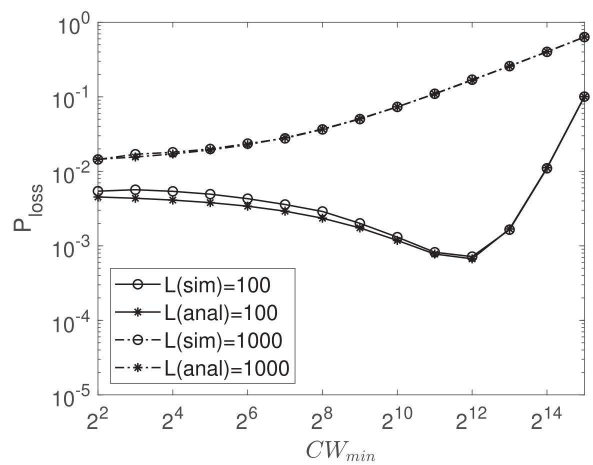

Fig. 9. P_{loss} versus $\mathrm{CW}_{\mathrm{min}}$.

goodput at a packet length of 100 fell below goodput for both larger packets lengths (500 and 1000). The reason is that with an increase in the initial contention window size, a channel remains idle most of the time, since nodes with small packet lengths launch the backoff procedure more frequently. For all packet lengths, goodput decreased as $\mathrm{CW}_{\mathrm{min}}$ increased (i.e., W_{max} decreased due to channel wastage). The goodput for L at 1000 was not affected much by an increase in $\mathrm{CW}_{\mathrm{min}}$, compared to other packet lengths, since the probability of a collision is lower for such a large packet length. Another important conclusion from Fig. 6 is that the error between analytical and simulation results was reduced as the packet length increased. Therefore, the accuracy of the proposed model increased with larger packet lengths.

The effect on goodput from the number of nodes contending for the channel was also explored. Analytical and simulation results with respect to the initial contention window for different numbers of nodes are shown in Fig. 7. A packet length of 100 was chosen because it gave the maximum goodput, compared to other packet lengths, as seen from Fig. 6. In Fig. 7, a waterfall effect is clearly observed when 10 nodes contended for the channel. This is because channel waste was high with an increase in $\mathrm{CW}_{\mathrm{min}}$. On the other hand, as the contention window increased, goodput was higher for a larger n, even with more false alarms and collisions, which means the system has a better performance with more contending nodes.

We also determine the latency of the designed model by conducting simulations with varied initial contention window sizes for different numbers of nodes in the network, as shown in Fig. 8. For lower initial contention window sizes, the latency is approximately the same for different numbers of nodes in the network. When $\mathrm{CW}_{\mathrm{min}}$ is greater than 2^8, a network with ten nodes has high latency, whereas a network with a higher number of nodes ($n = 150$) achieves the lowest latency. Furthermore, when $\mathrm{CW}_{\mathrm{min}}$ is greater than 2^{10} the latency of a network with 10 nodes increases exponentially.

Note that the difference between the latency for different numbers of nodes is getting larger as $\mathrm{CW}_{\mathrm{min}}$ increases. In other words, networks with less number of nodes experience a more significant increase in latency with a larger initial contention window size. The reason is that with fewer nodes in the network and higher initial contention window size, there is a wider range of backoff values for nodes and nodes experience significantly longer backoff periods, resulting in fewer nodes initiating transmissions within a specific time duration. On the other hand, networks with a higher number of nodes had many nodes reaching a backoff value of zero during the same time duration, leading to more frequent packet transmissions and better packet reception at the destination. Therefore, a network with less number of nodes has also lower goodput when $\mathrm{CW}_{\mathrm{min}}$ increases, as depicted in Fig. 7.

B. *Effects of Different Parameters on Packet Loss Probability*

Fig. 9 shows the packet loss probabilities against initial contention window sizes for L at 100 and 1000. For $L = 100$, nodes got a longer backoff more frequently with an increase in $\mathrm{CW}_{\mathrm{min}}$, and the number of transmissions was reduced. As a result, P_{miss} was reduced, and P_{loss} also decreased. However, when $\mathrm{CW}_{\mathrm{min}}$ was greater than 2^{12}, an increase in P_{loss} was

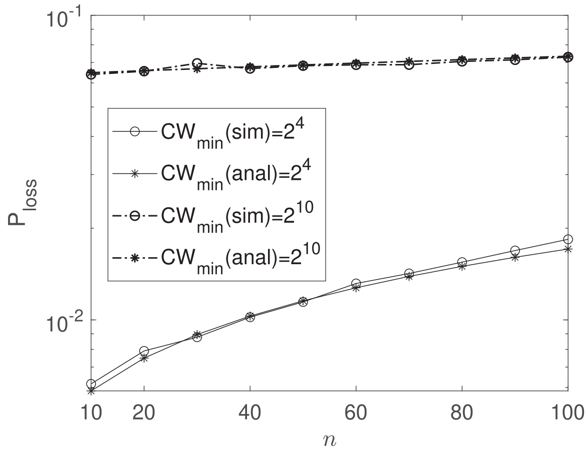

Fig. 10. P_{loss} versus n.

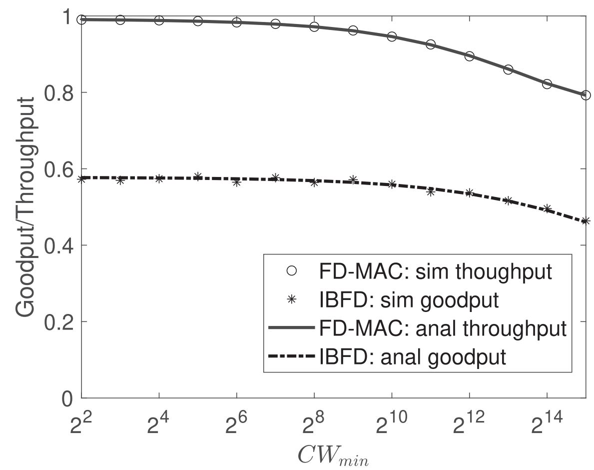

Fig. 11. Throughput and goodput with respect to CW_{min} for $L = 100$.

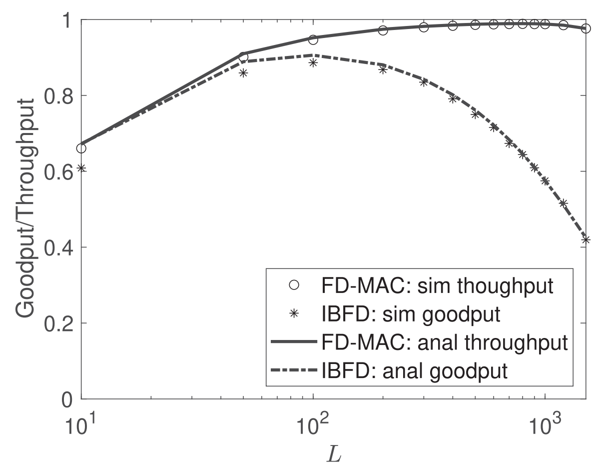

Fig. 12. Throughput and goodput with respect to L for $\text{CW}_{\text{min}} = 2^4$.

observed due to the dominant effect of reducing retransmission attempts for each packet, and the higher contribution of P_{mrl} to P_{loss}. This shows that each packet had a lower chance of being successfully received at the destination as the contention window size exceeded 2^{12}. Therefore, in Fig. 9, we observe a dip in the P_{loss} graph for $L = 100$ when CW_{min} is equal to 2^{12}.

With a larger packet length (i.e., $L = 1000$), the effect of reducing W_{max} on each packet became dominant, and the probability of a false alarm increased. This leads to an increase in the probability that a packet cannot be transmitted successfully within the maximum number of retransmission attempts (P_{mrl}) since there is a direct relationship with the contention window, as seen in (10). Consequently, P_{loss} increased for larger packet lengths with increases in contention window size. Despite the collision reduction, P_{loss} was dominated by false alarms at larger packet lengths.

The packet loss probability was examined against the number of nodes with two different contention window sizes (2^4 and 2^{10}) at a packet length of 1000. P_{loss} increased with an increasing number of nodes compared to contention window size due to the higher number of collisions, as shown in Fig. 10. P_{loss} was higher for larger contention window sizes due to the higher loss contribution by P_{mrl}. As the contention window increased, each packet had fewer chances to be received successfully. Moreover, with more nodes, there were more collisions and undetected collisions. Hence, P_{loss} in a system with more contending nodes having larger contention window sizes increased due to the higher P_{mrl} and P_{miss}.

Based on these results, we can say that the choice of packet length, the number of nodes, and the initial contention window size are crucial to obtaining a higher reliable goodput and the minimum packet loss. The results from this article can aid in determining optimal parameter settings to enhance the performance of the IBFD MAC protocol. These settings are particularly crucial for real-time applications, such as voice and video communication, online gaming, and interactive services, where high data rates and low latency are essentials for delivering a seamless user experience.

C. Comparison of FD-MAC and IBFD-MAC Protocols

The goodput of the IBFD-MAC protocol was compared with the throughput of the FD-MAC protocol [9]. Goodput and throughput from the initial contention window CW_{min} and the length of the packet, L, are shown in Figs. 11 and 12, respectively. Since throughput is channel utilization, and goodput is the real output of the system, the throughput of FD-MAC was higher compared to the goodput of IBFD-MAC.

As the initial contention window size CW_{min} increased, W_{max} decreased, and the nodes got larger backoff numbers and waited longer, on average, before attempting a new transmission (i.e., channel waste increased). As a result, both the throughput of FD-MAC and the goodput of IBFD-MAC decreased, as shown in Fig. 11. In the case of varied packet lengths, throughput increased asymptotically as packet length L increased, whereas goodput increased first and then decreased, as seen in Fig. 12. The chances of a false alarm increased with an increase in packet length, and the effect of false alarms became more prominent. Consequently, the output of the system under IBFD-MAC decreased drastically. Note that higher throughput under FD-MAC does not guarantee a high ratio of packets successfully received

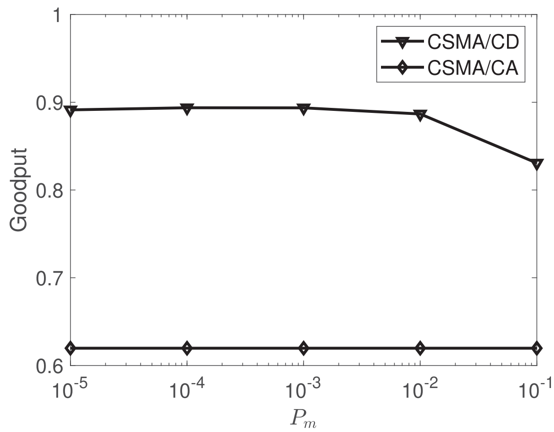

Fig. 13. Goodput comparison of CSMA/CA-based HD-MAC and CSMA/CD-based IBFD-MAC protocols with respect to the probability of missed detection.

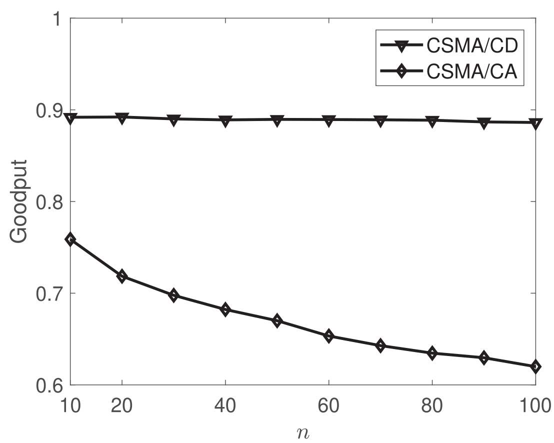

Fig. 14. Goodput versus the number of nodes under CSMA/CA-based HD-MAC and CSMA/CD-based IBFD-MAC protocols.

because throughput shows channel usage as the output of the system.

D. Comparison of CSMA/CD-Based IBFD-MAC and CSMA/CA-Based HD-MAC

The performance comparison between HD-MAC and IBFD-MAC protocols in terms of goodput is presented to show the advantages of IBFD-MAC in wireless communications systems. We set the packet length at 100, with 100 contending nodes, and a contention window size of 2^4 to determine goodput under the different protocols.

Fig. 13 shows the goodput under HD-MAC and IBFD-MAC compared to the probability of missed detection. Since self-interference was zero, goodput under HD-MAC was constant, and P_m, thus, did not affect the performance of HD-MAC. Under IBFD-MAC, goodput decreased with an increase in P_m due to the increased number of undetected collisions. Nonetheless, goodput under IBFD-MAC was higher compared to goodput under HD-MAC by approximately 30%, even with sensing errors. Goodput versus the number of nodes for HD-MAC and IBFD-MAC were evaluated and are shown in Fig. 14. For IBFD-MAC, the goodput was nearly constant (i.e., 90%) even with sensing

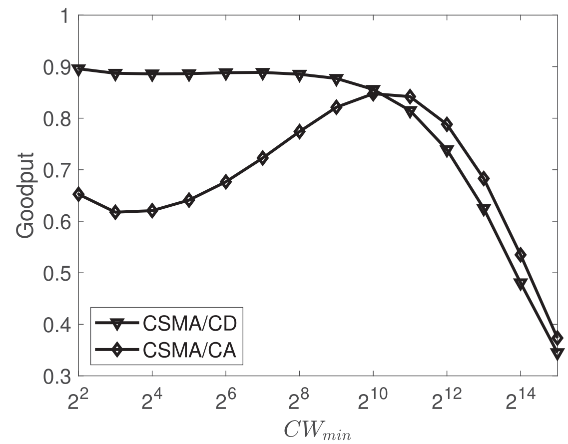

Fig. 15. Goodput versus contention window size under CSMA/CA-based HD-MAC and CSMA/CD-based IBFD-MAC protocols.

errors. Under HD-MAC, goodput decreased with an increase in the number of nodes due to more collisions. A collision lasted for the entire packet under HD-MAC, unlike IBFD-MAC. The main reason for higher goodput from IBFD-MAC is that it detects collisions within two slots (DIFS), which results in better channel utilization.

The effect of initial contention window size $\mathrm{CW_{min}}$ on goodput under both HD-MAC and IBFD-MAC is shown in Fig. 15. Goodput under IBFD-MAC was higher than with HD-MAC up to a contention window size of 2^9. The reason is there was less channel wastage under IBFD-MAC owing to the collision detection mechanism. When $\mathrm{CW_{min}}$ was greater than 2^9, the goodput of IBFD-MAC was reduced and fell below the goodput of HD-MAC due to additional sensing errors. We conclude that IBFD-MAC has higher goodput (even with sensing errors), and accommodates a large number of nodes compared to HD-MAC.

VI. Conclusion

In this article, we extend IEEE 802.11 from CSMA/CA to CSMA/CD for IBFD wireless systems by leveraging full-duplex capabilities. A Markov chain-based model is designed for a CSMA/CD-based IBFD-MAC protocol, which incorporates a maximum retry limit and backoff freezing. The performance is evaluated using two metrics: goodput and packet loss probability. We analytically evaluate the goodput and packet loss probability, considering all possible cases of miss collision detection due to sensing errors. The accuracy of the analytical model is validated by comparing the simulation and numerical results. Results show that the choice of packet length is very important for the IBFD CSMA/CD MAC protocol due to the high probability of false alarms with large packet lengths. Goodput and packet loss probability can be maximized and minimized, respectively, with an appropriate selection of packet length and initial contention window size. In addition, we compare the performance of the designed IBFD MAC protocol to the HD MAC protocol to demonstrate the superiority of IBFD systems over HD systems, even in the presence of sensing errors.

Appendix A

Let $b_{k,i} = \lim_{t\to\infty} P\{b(t) = k, s(t) = i\}$ represents the stationary distribution of the chain where $b(t)$ is backoff counter and $s(t)$ represents the number of transmission attempts. The global balance equation for the Markov chain will be used to obtain a closed-form expression written as

$$(1-p_s)b_{0,i-1} = b_{0,i}$$
$$b_{0,i} = (1-p_s)^i b_{0,0}\ ,\ for \quad 0 \le i \le W_{\max}$$
$$(1-p_s)b_{0,W_{\max}-1} = b_{0,W_{\max}}p_s$$
$$b_{0,W_{\max}} = \frac{(1-p_s)^{W_{\max}} b_{0,0}}{p_s}$$
$$(1-P_b)b_{k,i} = b_{k-1,i}$$
$$b_{k,i} = \frac{1}{(1-P_b)} b_{k-1,i}\ ,\ \text{for} \quad 0 \le i \le W_{\max}\ 1 \le k \le \mathrm{CW}_i - 1. \tag{11}$$

As the chain has regularity, so for all $k \in (1, \mathrm{CW}_i - 1)$, we can write

$$b_{k,i} = \frac{\mathrm{CW}_i - k}{\mathrm{CW}_i} \begin{cases} \sum_{j=0}^{W_{\max}-1} p_s b_{0,j} + b_{0,W_{\max}}, & i = 0 \\ (1-p_s)b_{0,i-1}. & 0 < i \le W_{\max}. \end{cases} \tag{12}$$

By using the set of equations in (11) and the following fact

$$\sum_{j=0}^{W_{\max}-1} p_s b_{0,j} + b_{0,W_{\max}} = b_{0,0}$$

we can write (12) as

$$b_{k,i} = \frac{\mathrm{CW}_i - k}{\mathrm{CW}_i} \frac{1}{1-P_b} b_{0,i} \quad 0 \le i \le W_{\max}, 1 \le k \le \mathrm{CW}_i - 1 \tag{13}$$

where P_b is the probability that the channel is busy. Using (11) and (13), all the values of states can be written in terms of $b_{0,0}$. The sum of all the state probabilities must be equal to 1 and is given by

$$1 = \sum_{i=0}^{W_{\max}} \sum_{k=0}^{\mathrm{CW}_i - 1} b_{k,i}. \tag{14}$$

By solving (14), we can express $b_{0,0}$ as

$$b_{0,0} = \frac{2(1-P_b)(2p_s-1)p_s}{(2p_s-1)(1-\omega) + \mathrm{CW}_{\min}(1-(2-2p_s)^{W_{\max}+1})p_s}$$

where p is the probability that a certain node begins transmission in the next slot and ω is equal to $(1-p_s)^{W_{\max+1}}$. Putting $P_b = 1-(1-p)^{n-1}$, we get

$$b_{0,0} = \frac{2(1-p)^{n-1}(2p_s-1)p_s}{(2p_s-1)(1-\omega) + \mathrm{CW}_{\min}(1-(2-2p_s)^{W_{\max}+1})p_s}. \tag{15}$$

The mathematical expression for p can be written as

$$p = \sum_{i=0}^{W_{\max}} b_{0,i}$$
$$= \sum_{i=0}^{W_{\max}} (1-p_s)^i b_{0,0}$$
$$= \frac{1-(1-p_s)^{W_{\max}+1}}{p_s} b_{0,0}.$$

Using (15), we can get

$$p = \frac{2(1-p)^{n-1}(2p_s-1)(1-\omega)}{(2p_s-1)(1-\omega) + \mathrm{CW}_{\min}(1-(2-2p_s)^{W_{\max}+1})p_s}$$

where p_s is the probability of transmission for an entire packet by at least one node [9], which can be a successful transmission or a collision between transmissions.

Appendix B

P_{mrl} can be derived based on the fact that the packet will be lost when the node has tried to retransmit the packet multiple times, reaching the maximum retry. We can write

$$P_{\mathrm{mrl}} = \frac{(1-p_s)b_{0,W_{\max}}}{b_{0,0}}$$

where

$$b_{0,W_{\max}} = (1-p_s)^{W_{\max}} b_{0,0}.$$

Using $b_{0,W_{\max}}$, P_{mrl} can be written as

$$P_{\mathrm{mrl}} = (1-p_s)^{W_{\max}+1}. \tag{16}$$

Equation (16) shows that a packet is lost when it undergoes $W_{\max}+1$ collisions.

Appendix C

For P_{miss}, we will consider the cases when collision goes undetected by at least one of the nodes. The probability of miss collision detection for each case can be expressed as

$$P_r\{\text{a node starts transmission during another's transmission}\}$$
$$= (M-1)p(1-p)^{M-2}$$
$$P_r\{\text{collision is not detected by both nodes}\} = P_m^{2L}$$
$$P_r\{\text{one node detects collision and stops transmission}\}$$
$$= \sum_{l=1}^{L-1} P_m^{2l-1}(1-P_m) = \frac{P_m^2 - P_m^{2L}}{P_m^2 + P_m}.$$

By combining the above-mentioned probabilities, we can write P_{miss} as

$$P_{\mathrm{miss}} = (M-1)p(1-p)^{M-2}\left[P_m^{2L} + \frac{P_m^2 - P_m^{2L}}{P_m^2 + P_m}\right].$$

References

[1] K. E. Kolodziej, B. T. Perry, and J. S. Herd, "In-band full-duplex technology: Techniques and systems survey," *IEEE Trans. Microw. Theory Techn.*, vol. 67, no. 7, pp. 3025–3041, Jul. 2019.

[2] D. Kim, H. Lee, and D. Hong, "A survey of in-band full-duplex transmission: From the perspective of PHY and MAC layers," *IEEE Commun. Surv. Tut.*, vol. 17, no. 4, pp. 2017–2046, Fourth Quarter 2015.

[3] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.
[4] R. Doost-Mohammady, M. Y. Naderi, and K. R. Chowdhury, "Performance analysis of CSMA/CA based medium access in full duplex wireless communications," *IEEE Trans. Mobile Comput.*, vol. 15, no. 6, pp. 1457–1470, Jun. 2016.
[5] Z. Zhang, X. Chai, K. Long, A. V. Vasilakos, and L. Hanzo, "Full duplex techniques for 5G networks: Self-interference cancellation, protocol design, and relay selection," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 128–137, May 2015.
[6] K. A. Darabkh, O. M. Amro, H. Bany Salameh, and R. T. Al-Zubi, "A–z overview of the in-band full-duplex cognitive radio networks," *Comput. Commun.*, vol. 145, pp. 66–95, 2019.
[7] G. Bianchi, L. Fratta, and M. Oliveri, "Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless lans," in *Proc. 7th Int. Symp. Pers., Indoor, Mobile Commun.*, 1996, vol. 2, pp. 392–396.
[8] F. A. Tobagi and V. B. Hunt, "Performance analysis of carrier sense multiple access with collision detection," *Comput. Netw. (1976)*, vol. 4, no. 5, pp. 245–259, 1980.
[9] Y. Liao, K. Bian, L. Song, and Z. Han, "Full-duplex MAC protocol design and analysis," *IEEE Commun. Lett.*, vol. 19, no. 7, pp. 1185–1188, Jul. 2015.
[10] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *Proc. Conf. ACM SIGCOMM*, 2013, pp. 375–386.
[11] A. Sahai, G. Patel, and A. Sabharwal, "Pushing the limits of full-duplex: Design and real-time implementation," 2011, *arXiv:1107.0607*.
[12] M. Luvisotto, A. Sadeghi, F. Lahouti, S. Vitturi, and M. Zorzi, "RCFD: A novel channel access scheme for full-duplex wireless networks based on contention in time and frequency domains," *IEEE Trans. Mobile Comput.*, vol. 17, no. 10, pp. 2381–2395, Oct. 2018.
[13] S. Goyal, P. Liu, O. Gurbuz, E. Erkip, and S. Panwar, "A distributed MAC protocol for full duplex radio," in *Proc. Asilomar Conf. Signals, Syst. Comput.*, 2013, pp. 788–792.
[14] M. Murad and A. M. Eltawil, "Performance analysis and enhancements for in-band full-duplex wireless local area networks," *IEEE Access*, vol. 8, pp. 111636–111652, 2020.
[15] Y. Liao, B. Di, K. Bian, L. Song, D. Niyato, and Z. Han, "Cross-layer protocol design for distributed full-duplex network," in *Proc. IEEE Glob. Commun. Conf.*, 2015, pp. 1–6.
[16] H. Zuo et al., "A distributed IBFD MAC mechanism and non-saturation throughput analysis for wireless networks," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf.*, 2017, pp. 1851–1856.
[17] L. Song, Y. Liao, K. Bian, L. Song, and Z. Han, "Cross-layer protocol design for CSMA/CD in full-duplex WiFi networks," *IEEE Commun. Lett.*, vol. 20, no. 4, pp. 792–795, Apr. 2016.
[18] J. Robinson and T. Randhawa, "Saturation throughput analysis of IEEE 802.11e enhanced distributed coordination function," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 5, pp. 917–928, Jun. 2004.
[19] R. Liao, B. Bellalta, and M. Oliver, "Modelling and enhancing full-duplex MAC for single-hop 802.11 wireless networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 4, pp. 349–352, Aug. 2015.
[20] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 535–547, Mar. 2000.
[21] D.-J. Deng, C.-H. Ke, H.-H. Chen, and Y.-M. Huang, "Contention window optimization for IEEE 802.11 DCF access control," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 5129–5135, Dec. 2008.

Wardah Sarmad received the B.E. degree in electrical engineering from the National University of Sciences and Technology (NUST), Islamabad, Pakistan, in 2015 and the M.S. degree in electrical engineering from Bilkent University, Ankara, Turkey, in 2019.

Her research interests are wireless networks, full-duplex communications, and MAC layer protocols.

Syed Maaz Shahid received the B.E. degree in electrical engineering from the National University of Sciences and Technology (NUST), Islamabad, Pakistan, in 2015 and the Ph.D. degree in electrical engineering from the University of Ulsan, Ulsan, South Korea, in 2022.

He is currently a Research Professor with the University of Ulsan. His research interests include cellular network optimization, AI-enabled cellular networks, cognitive sensor networks, and applications of machine learning in signal processing.

Ezhan Karasan (Member, IEEE) received the B.S. degree from Middle East Technical University, Ankara, Turkey, the M.S. degree from Bilkent University, Ankara, Turkey, and the Ph.D. degree from Rutgers University, Piscataway, NJ, USA, in 1987, 1990, and 1995, respectively, all in electrical engineering.

During 1995–1996, he was a Postdoctorate Researcher with Bell Labs, Holmdel, NJ, USA. From 1996 to 1998, he was a Senior Technical Staff Member with the Lightwave Networks Research Department, AT&T Labs Research, Red Bank, NJ, USA. Since 1998, he has been with the Department of Electrical and Electronics Engineering, Bilkent University, where he is currently a Full Professor. He has participated in FP6-IST Network of Excellence (NoE) e-Photon/ONe+ and FP7-IST NoE BONE projects. His current research interests are in the application of optimization and performance analysis tools for the design, engineering, and analysis of optical and wireless networks.

Dr. Karasan is a member of the Editorial Board of Optical Switching and Networking journal. He was a recipient of the 2004 Young Scientist Award from Turkish Scientific and Technical Research Council (TUBITAK), a Career Grant from TUBITAK in 2004, and the 2005 Young Scientist Award from Mustafa Parlar Foundation. He was also a recipient of a fellowship from the North Atlantic Treaty Organization Science Scholarship Program for overseas studies in 1991–1994.

Sungoh Kwon (Senior Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from KAIST, Daejeon, South Korea, in 1994 and 1996, respectively, and the Ph.D. degree in electrical and computer engineering from Purdue University, West Lafayette, IN, USA, in 2007.

From 1996 to 2001, he was a Research Staff Member with Shinsegi Telecomm Inc., Seoul, South Korea. From 2007 to 2010, he was a Principal Engineer with Samsung Electronics Company Ltd., Suwon, South Korea, where he developed LTE schedulers. Since 2010, he has been with the School of Electrical Engineering, University of Ulsan, Ulsan, South Korea, where he is currently a Professor. His research interest includes wireless communication networks, AI for 6G networks, and energy ICT.