IP–MAC: A Distributed MAC for Spatial Reuse in Wireless Networks

Md. Mustafizur RAHMAN†, Nonmember, Choong Seon HONG†, Member, Sungwon LEE†, JangYeon LEE††, and Jin Woong CHO††, Nonmembers

SUMMARY The CSMA/CA driven MAC protocols withhold packet transmissions from exposed stations when they detect carrier signal above a certain threshold. This is to avoid collisions at other receiving stations. However, this conservative scheme often exposes many stations unnecessarily, and thus minimizes the utilization of the spatial spectral resource. In this paper, we demonstrate that remote estimation of the status at the active receivers is more effective at avoiding collisions in wireless networks than the carrier sensing. We apply a new concept of the interference range, named as n-tolerant interference range, to guarantee reliable communications in the presence of n (n ≥ 0) concurrent transmissions from outside the range. We design a distributed interference preventive MAC (IP–MAC) using the n-tolerant interference range that enables parallel accesses from the noninterfering stations for an active communication. In IP–MAC, an exposed station goes through an Interference Potentiality Check (IPC) to resolve whether it is potentially interfering or noninterfering to the active communication. During the resolve operation, IPC takes the capture effect at an active receiver into account with interfering signals from a number of possible concurrent transmissions near that receiver. The performance enhancement offered by IP–MAC is studied via simulations in different environments. Results reveal that IP–MAC significantly improves network performance in terms of throughput and delay.

key words: wireless network, spatial reuse, concurrent transmissions, CSMA/CA, channel access, wireless MAC

1. Introduction

Over the last decade, we have been observed a tremendous growth in the popularity of the Wireless Ad hoc and Local Area Networks (WLAN) emerging in environments like industries, enterprises, apartments, shopping malls, and public access networks. Usually, many wireless devices overlap in the same space and share the same set of available frequencies due to the limited number of available channels. Therefore, the medium access control (MAC) protocols for these devices are required to endeavor scheduling as many concurrent transmissions as possible in a geographical region to maximize the spatial reuse of the available channels.

Millions of wireless devices are already deployed and the Distributed Coordination Function (DCF) of the IEEE 802.11 [1] becomes as the de facto standard for them. This is due to its efficiency in contention coordination, simplicity, and low implementation cost. DCF coordinates the channel access through a clear channel assessment (CCA), an exponential random backoff, and a set of inter-frame spaces. The CCA at a station signals with a busy channel when it detects energy above a constant threshold, named as CCA Sensitivity (CCA₀), to indicate the presence of other active transmission(s) in the vicinity. However, DCF is known to have many design flaws as it was primarily engineered to the mainstream WiFi networks: single cell infrastructure-based WiFi networks. For example, when a station gets a busy indication from the CCA, it respects to the ongoing communication and keeps silence (exposed) until the ongoing communication ends. This conservative scheme in DCF often exposes many stations unnecessarily, thus making it difficult to maximize the utilization of the spatial spectral resource.

The DCF as well as other CSMA/CA driven MAC protocols are designed on the basic principle that a signal of any strength from any concurrent transmitter always corrupts an ongoing communication. However, according to the well known capture effect model (also known as the SINR model) for wireless networks, it is evident that the intended signal power, combined interfering signal power and the receiver capture threshold (or, the minimum required SINR) together determine the success or failure of packet receptions, rather than the energy level, such as CCA₀ at the nearby stations. The channel assessment in DCF exposes a station even when its signal strength is not strong enough to cause a collision at other active receiver(s). Therefore, an efficient node exposure scheme is required that estimates the receive condition at other active receivers and exposes a station only when it is suspected to be an interferer for them.

There exists a number of research works addressing the problem of spatial reuse in wireless networks. They can be classified into four categories: use of directional antenna to alleviate interference [2], [3], scheduling mutually non-interfering communication locally, [4]–[8], transmit power control (TPC) to shorten the interference range [9], [10], and reducing the number of exposed stations using a tunable CCA₀ [11]–[13]. The directional antenna based solutions can be applied only when the location of the receiver is known and they are unscalable. They also incur huge increases in cost. Other schemes consider the capture effect at an active receiver, and thereby, schedule noninterfering concurrent transmissions either by collecting 2-hop channel requests or by reducing the number of exposed stations by adjusting CCA₀ or TPC. The scheduling based on 2-hop
information incurs huge overhead in information exchange and the protocols become unscalable. In TPC or CCA₀ adjustment based schemes, a communication converts an exposed station into a hidden station according to its so-called interference range. A node from inside the range senses carrier and refrains from transmitting until the initial one (hereinafter referred to as master communication or, simply as “the master”) ends. A node from outside the interference range gets a clear channel and proceeds for a concurrent transmission. This node alone does not corrupt the master communication. However, when several nodes, from outside the interference range, distributively get the channel clear, they create a pandemonium and may jointly corrupt the master communication (the concurrent communications as well). Thus, to improve the level of spatial reuse, the concept of interference range should describe not only a prohibited area but also the upper bound of the number of concurrent communications from outside the area. This paper applies, for the first time, the concept of such an ineffective value for n that safeguards the master communication as well as improves the level of spatial reuse in the network.

The important challenge, here, is that, how can an exposed station (by the CCA) identify whether its location is inside the n-tolerant interference range of the master or not. Hence, we design a function module, called as Interference Potentiality Checking (IPC), which can be used to resolve a station as non-interfering or potentially interfering to the master communication in the context of its n-tolerant interference range. A station overhears parameters from the master and its IPC module estimates the SINR status at the master receiver with interfering signals from n number of concurrent transmissions and decides accordingly. We also propose a distributed and DCF-like interference preventive MAC (IP–MAC) to enable parallel accesses from the noninterfering stations. An IP–MAC station is equipped with an IPC module to locate its position with respect to the master communication and attempts for a parallel transmission when it resolves itself as non-interfering to the master. It should be noted that with a properly chosen value of n, IPC also helps in limiting the number of concurrent attempts during the master communication. Further, the use of n-tolerant interference range also combat with the channel asymmetry and estimation errors in IPC. We use simulations to evaluate how IP–MAC scales and how well IP–MAC works under various network topologies. Our evaluation shows that IP–MAC supports concurrent transmissions from spatially separated locations, and improves aggregate network throughput.

In the next section, we will discuss the background and some related works. Then we present the proposed IP–MAC protocol in Sect. 3. In describing the proposed protocol, we first introduce the basic design components of IP–MAC including the IPC and then describe the protocol operation and how it meets the challenges. In Sect. 4, the simulation results are presented and analyzed. Finally, the paper concludes in Sect. 5.

2. Background and Related Works

This section introduces the concept of the tolerance of a communication and reviews some of the related works.

2.1 System Model

2.1.1 Channel Model

We consider that the wireless physical channel is flat or frequency-independent and an electromagnetic signal may be diffracted, reflected, and scattered when it propagates through the channel. These effects have two important consequences on the signal strength. First, the signal strength decays exponentially with respect to distance, and second, for a given distance d, the signal strength is random and log-normally distributed about the mean distance-dependent value. One of the most common radio propagation models that describes the unique characteristics of such environment is the log-normal path loss model [14]. According to this model, the received power (Pᵣ) in dB at a distance d (from the source) is given by

\[ P_r(d) = P_t - 10\gamma \log_{10} \left( \frac{d}{d_0} \right) + N(0, \sigma_n), \]  

(1)

where \( P_t \) is the radiated signal power from the transmitting station, \( \gamma \) is the attenuation factor, i.e., the rate at which the signal decays with respect to distance, \( N(0, \sigma_n) \) is a Gaussian random variable with mean 0 and variance \( \sigma_n \) (standard deviation due to multipath effects), and \( PL(d_0) \) is the power decay for the reference distance \( d_0 \). The value of \( \gamma \) is different in different environments depending on the channel conditions. Empirical results show that the value of \( \gamma \) remains in between 1.6 and 6.0. In a very short distance (≤ 1 m), the radio signal is likely to follow the free space path loss model. Thus, \( PL(d_0) \approx 20 \log_{10} \left( \frac{4\pi d_0 f}{c} \right) \), when \( d_0 \leq 1 \text{ m} \). Here, \( f \) is the carrier frequency and \( c \) denotes the speed of light and we assume unit antenna gains. Therefore, for a specific carrier frequency, \( PL(d_0) \) value is pseudo-constant (approximately 20 dB with \( f = 2.4 \text{ GHz} \) and \( d_0 = 1 \text{ m} \)). This model can be used for both large and small coverage systems [15], and empirical studies have shown that the log-normal model provides more accurate multipath channel models than the well-known Nakagami and Rayleigh models for indoor environments [16].

Let, \( P(d_0) = P_t - PL(d_0) \) is the signal power measured at distance \( d_0 \) from the transmitter, and mean \( N(0, \sigma_n)^{\dagger} = 0 \), then without loss of generality, we can simplify Eq. (1) as:

\[ P_r(d) = P(d_0) - 10\gamma \log_{10} \left( \frac{d}{d_0} \right). \]  

(2)

\(^\dagger\)We discuss on the multipath fading later in Sect. 3.3.2.
In the Watt unit, Eq. (2) is represented by:

\[ p(d) = p(d_0) \times \left( \frac{d}{d_0} \right)^{-\gamma} \]  

where \( p(\cdot) \) is the power in Watt for a power \( P_r(\cdot) \) in dBm.

The path-loss model for radio propagation is useful in determining the signal strength at a certain distance, or in determining the propagation distance for a certain receive signal power such as the communication (or transmission), interference and carrier sensing ranges of a station. In this paper, we use the notation \( P_r(P)^{-1} \) to represent the propagation distance \( d \) for a received signal power of \( P \); i.e., \( P_r(P)^{-1} = d \) when \( P_r(d) = P \).

2.1.2 Radio Receiver Model

In modeling the function of a radio receiver, we consider a region of a network with \( n + 2 \) active wireless stations where a station \( T \) transmit a packet to a receiver \( R \) and \( n \) other stations \( \{t_i| 1 \leq i \leq n\} \) transmit packets to some other stations as shown in Fig. 1. The receiver \( R \) located at a distance of \( d \) and \( d_i \) from stations \( T \) and \( t_i \), respectively. All stations use omni-directional antennas that radiate the signal equally in all directions. We also assume that every node transmits with the same power and the channel is symmetric.

The signals from \( T \) and each interferer \( t_i \), superpose with each other at \( R \). \( R \) receives a signal power of \( p(d) \) (Watt) for the packet transmitted from \( T \), and it receives signal power \( p(d_i) \) (Watt) for the interferer \( t_i \). Then, according to the capture effect model, \( R \) receives the packet from \( T \) with a certain packet error probability when:

\[ \frac{p(d)}{\sum_{i=1}^{n} p(d_i) + \omega_0} \geq \beta \]  

where \( \beta \) is the required minimum SINR or capture threshold (CPT) for the Modulation and Coding Scheme (MCS) used by \( T \) in transmitting the packet, and \( \omega_0 \) is the Gaussian distributed ambient noise. Unless otherwise the interfering station is far away from the receiver, the noise level \( \omega_0 \) contributes much less than the interfering signal \( p(d_i) \). Therefore, we exclude noise levels in formulas afterward.

The capture effect in Eq. (4) shows when an intended packet collides at a receiver due to the interfering signals and it is often used to theoretically describe the interference range of a given communication. A CSMA/CA based protocol assumes that a receiver can receive a packet successfully when \( p(d_i) < CCA_0 \); i.e., an interferer \( t_i \) does not corrupt a reception at a receiver \( R \) when \( p(d_i) < CCA_0 \). In other words, it assumes that \( t_i \) is located outside the interference range, \( \varphi (\varphi = P_r(CCA_0)^{-1}) \), of \( R \) (i.e., \( d_i > \varphi \)), and hence, it does not corrupt the reception at \( R \). Note that, such an assumption makes a protocol fragile because it considers interfering signals from only one interfering node. This is why a CSMA/CA based protocol usually use a very low \( CCA_0 \) (and resulting in exposing many stations unnecessarily).

2.2 The Tolerance of a Communication

When a MAC protocol allows concurrent communications near a master communication, the master must tolerate interference from the nearby concurrent transmitters. The capture effect in Eq. (4) describes the tolerance of such a communication. Note that, though we mention about the tolerance of the master only, it is true for each of the concurrent communications as well. However, in this paper, we focus on the tolerance of the master only because if the master tolerates interference from other concurrent communications then the network performance would be at least equal to that of the single transmission schemes (like CSMA/CA).

With the help of Eq. (3), we can express Eq. (4) in the distance form as:

\[ \frac{\sum_{i=1}^{n} p(d_i) + \omega_0}{\sum_{i=1}^{n} d_i^{-\gamma}} \geq \beta. \]  

We reach to the following observation from (5) that defines the tolerance of an active communication.

**Lemma 1:** The reception at a receiver \( R \), which is distance away from its sender \( T \), can tolerate transmissions from \( n \) other active transmitters (or interferers), where all of them are at least \( D \) distance away from \( R \), and the following condition is satisfied:

\[ n \leq \left[ \frac{1}{\beta} \left( \frac{D}{d} \right)^{\gamma} \right]. \]  

**Proof:** Suppose, the nearest interfering station(s) is \( D \) distance away from the receiver \( R \). Therefore, a station individually interferes at \( R \) with a maximum strength of \( p(D) \). If we consider that all the stations interfere with strength of \( p(D) \), then according to Eq. (5), \( R \) can tolerate \( n \) transmissions from distance \( D \) (or, further) when:

\[ \frac{1}{n} \left( \frac{d}{D} \right)^{-\gamma} \geq \beta. \]  

After rearranging, we reach to the Eq. (6). 

Now, we can define the interference range of \( R \) with its tolerance.

**Definition 1:** The \( n \)-tolerant Interference Range (\( \varphi_n \)) is the distance from an active receiver, beyond which \( n \) active
transmitters do not corrupt the reception at the receiver. In mathematical form,

\[ \varphi_n \simeq d \left( (n + 1) \times \beta \right)^{t} \]  

(8)

where, each active interferer interferes with a power of:

\[ p(d) \leq \frac{p(d)}{(n + 1) \times \beta}. \]  

(9)

The value of \( n \) plays significant roles in Eq. (8) and Eq. (9). The range \( \varphi_n \) extends or shrinks with the value of \( n \). Thus, if a protocol allows parallel communications with a small value of \( n \), it enables parallel transmissions from many stations and when the number of such parallel transmissions exceeds \( n \), they jointly collide at the master. On the other hand, with a large value of \( n \), the range \( \varphi_n \) might become larger than the \( P_r(CCA_0)^{-1} \). So, it will reduce the level of spatial reuse than that in DCF. We discuss on the impact of \( n \) on a protocol in Sect. 3.1.4 in detail. Further, the value of \( n \) determines the maximum allowable interfering signal power from an interfering station. Therefore, a station can use that in estimating the interfering signal strength at the master from that station. In Sect. 3.3.2, we will see that it also helps a channel access scheme in handling the channel asymmetry.

From the above discussions, it is clear that the concept of \( \varphi_n \) is an essential part in improving the level of spatial reuse. In the following subsection, we discuss some related works with this concept.

2.3 Related Works

Scheduling based methods, like [4]–[6], schedule noninterfering parallel transmissions from channel access requests. All intended transmitters request for channel access before data transmissions. Hence, they know about other channel access requests and \( P_r \) from each of them. Then they determine mutually noninterfering concurrent communications using these information and the transmitters for these communications access the channel for data transfers. Although these protocols can determine the number of interfering stations and signal strength for each of them, they require enhancement in the channel access protocol by introducing new frames, and altering the control sequence. Further, finding the noninterfering communications at a given time is a NP-hard problem. The Mesh Network Alliance (MNA) [7] and Mesh Deterministic Access (MDA) in IEEE 802.11s [8] protocols use TDMA like periodic contention free slots for parallel transmissions. Both protocols require multihop information to distribute the periodic noninterfering slots.

MAC protocols with transmit power control (for example, in [9],[10]) are efficient in energy conserving and seem to offer improved spatial diversity. However, the low power transmissions traverse shorter distances; hence, distant stations find the channel free and access the channel. Transmissions with high power from such stations corrupt the low power receptions.

Zhu et al. [11] demonstrates that a tunable \( CCA_0 \) is effective at avoiding interference instead of virtual carrier sensing. They provide a distributed adaptive scheme to adjust the \( CCA_0 \) dynamically, based on the periodic estimation of channel conditions. Periodic estimations at each node need to be disseminated throughout the network, and therefore, incurs huge overhead. In another work [12], they propose an adaptive CCA, where the \( CCA_0 \) is adjusted using the packet error rate (PER). The adaptation scheme is effective when it is coordinated centrally. Independent adaptation at stations aggravates the performance because they cannot determine the PER at neighbors and hidden stations. The Collision-Aware DCF [13] utilizes the available channel along both the spatial and time dimensions. It passes the spatial and time reservation requirements to the neighbors through the PHY header, and the neighbors defer based on the communication distance and channel status. However, it requires a neighbor database at every station and cannot limit the number of parallel transmissions within 6 (because more than 6 stations might identify themselves as non-interfering).

3. Interference Preventive MAC (IP–MAC)

In this Section, we describe the proposed interference preventive MAC (IP–MAC) protocol that uses the concept of \( n \)-tolerant interference range \( \varphi_n \) to start parallel transmissions from the noninterfering exposed stations. IP–MAC follows the basic IEEE 802.11 DCF (or, EDCA) to access the channel and it uses the 4-way cycle (RTS-CTS-DATA-ACK) for the communications. We consider that an IP–MAC station is capable of aggregating several small sized data packets into a superframe or aggregated frame [17]. The receiving station decouples the aggregated frame into several subframes. Channel accesses in IP–MAC are classified into two categories: clear and busy channel accesses. A station accesses in a clear channel using the DCF sequence, and a exposed station accesses in a busy channel when it is outside the \( n \)-tolerant interference range of a communication. In the rest of the paper, a master communication refers to the clear channel access, and a parallel communication refers to the busy channel access. IP–MAC maintains conventional Inter-frame Spaces (IFS) and backoff schemes for the clear channel access, and bypasses the DIFS for busy channel accesses. Unless otherwise specified, an IP–MAC station transmits a control frame (e.g., RTS, CTS and ACK) at the maximum power level, \( p_{max} \), to cover its transmission range, \( \Theta \).

3.1 Design Components

The major objective of IP–MAC is to allow parallel transmissions, wherever applicable, without disrupting the active (master) one. Hence, the design must address the following questions to achieve the goal. 1) How does the protocol incorporate the concept of \( n \)-tolerant interference range? 2) How can an exposed station get the status at the master (i.e.,
p(d) at the master receiver)? 3) How does a potential interferer resolve whether it can transmit in parallel or not? 4) Which stations can actually start parallel transmissions? Although these questions are related to each other, we address them in separate design modules, as described in the following subsections.

3.1.1 Parallel Transmission Threshold \((PxT)\)

The prime concern of IP–MAC design is to enable concurrent communications without colliding the active (master) communications. More specifically, the protocol should apply the \(\varphi_n\) for a certain value of \(n\) to keep the master safe from other concurrent transmissions. In IP–MAC, we define the chosen value of \(n\) as the parallel transmission threshold or \(PxT\). Thus, if \(n\) is the number of concurrent accesses from outside the range \(\varphi_n\) of a master, then the master is safe from them when \(n \leq PxT\). We assume that the value of \(PxT\) is imprinted in all IP–MAC supported devices. Since the \(PxT\) determines the size of the \(\varphi_n\) of a master, it takes significant role in IP–MAC protocol operation and we discuss on the impact of different \(PxT\) values on the protocol performance in Sect. 3.1.4.

3.1.2 The Interference Factor Frame (IF-Frame)

In CSMA/CA based protocols, the interference avoiding decision is taken by the potential interferers. More specifically, when a station finds that its own transmission might corrupt other active transmissions, it refrains from transmitting. So, according to Eq. (9), an IP–MAC station, \(I_s\), must know the \(p(d)\), \(p(d_t)\) and \(\beta\) for the master to resolve whether its (own) transmission will corrupt the master or not. The station gets the \(p(d_t)\) using signal strengths of prior received frames from the master\(^†\) (i.e., from the signal strength of overheard RTS and CTS frames from the master sender and receiver). It receives the rest two elements \((p(d)\) and \(\beta\)) from the master through the following three parameters: \(\text{SenderReceiverDistance (SRD)}, \text{Data Frame Transmit-Power Level (DPL)}\) and the required \(\text{capture threshold (CPT)}\) (i.e., \(\beta\)). The station estimates the \(p(d)\) from SRD and DPL pair. We use the SRD–DPL pair here to enable transmit power control during data frame transmissions. A master station estimates\(^††\) SRD using the signal power of control frames (RTS/CTS/ACK) from its partner. The rest two parameters DPL and CPT are selected by the station before transmitting the packet. We name these three parameters together as Interference Factors (IF).

A master station can deliver the IF to its neighbors in several ways, such as: (a) extending the MAC header using additional fields, (b) broadcasting a separate frame before data transmission, or (c) sending as a sub-frame along with other data frame(s) in a superframe or aggregated frame. All options are equally viable for IP–MAC. If the master receiver sends the IF, it can use options (a) and (b). On the other hand, the master sender can use any of the options. Since the options (a) and (b) require changes in the MAC header or in the frame exchange sequence, we select the option (c) for IP–MAC; i.e., the master sender sends the IF as a sub-frame in the data frame.

Before transmitting data packets, the stations create a sub-frame for the IF and place it as the very first sub-frame in an aggregated frame. We name this sub-frame as Interference Factor Frame (IF-Frame). The data packet(s) are appended as sub-frame(s) in the aggregated frame. The address field of the IF-Frame is set to the broadcast address; hence all receiving (overhearing) stations extract the IF. Note that, according to the standard [17], a sub-frame in an aggregated frame carries its own header and frame control sequence (FCS). So, a station can extract the contents of the sub-frame when it receives a sub-frame. Hence, an exposed station can extract the SRD, DPL and CPT just after receiving the last bit of the first sub-frame (i.e., the IF-Frame).

3.1.3 Interference Potentiality Checking (IPC)

The core component of the IP–MAC design is the Interference Potentiality Checking (IPC) that enables self-resolving by a station as non-interfering or potentially interfering for a master communication. Since the carrier sensing mechanism cannot help in accessing a busy channel, an IP–MAC station uses IPC for a concurrent transmission instead. Figure 2 shows the functional block diagram of the IPC. The RTSS and CTSS are, respectively, the strengths at a station of the RTS and CTS frames received (i.e., overheard) from the master. The IF-Frame from the master supplies the SRD, DPL and CPT; and \(\gamma\) is the estimated or calibrated path loss exponent at the host station.

The Master Signal Estimator (MSE) in IPC estimates the master signal strength \(p(d)\) at the master receiver (or, sender) using Eq. (3) with \(d = \text{SRD} \) and \(p(d) = \text{DPL} − \text{PL}(d_0)\). The stronger among the RTSS and CTSS is taken as the interfering signal strength \(p(d)\) at the master from the reference (“this”) station. Finally, the comparator checks condition in Eq. (9) to resolve whether the reference station is outside the range \(\varphi_{d_{ref}}\) of the master or not. IPC returns a \(\text{False}\) when the host station is outside the range \(\varphi_{d_{ref}}\) of the master, a \(\text{True}\) otherwise.

At some stations, the inputs for IPC may not be available due to the condition at the station. For example, some stations may not receive (overhear) the CTS from the master receiver, or the RTS and IFFrame from the master sender. In such cases, IPC selects its inputs according to Table 1. When a station does not receive CTS from the master, its IPC uses the receiver sensitivity \(P_s\) as CTSS; i.e., the IPC considers that the station is at the transmission boundary of

\(^†\)We assume the link between two stations to be symmetric for energy detection. We describe the effect of channel asymmetry and estimation errors later in Section 3.3.2.

\(^††\)The estimated distance might vary from the actual due to multipath fading. However, the equivalent single path distance is used to reproduce the \(p(d)\) only, and estimating the actual distance is not our intention.
the master receiver. When a station does not receive RTS or IF–Frame from the master, its IPC forces the station to remain silent using RTSS = $CC_A0$, CTSS = $p_{max}$ and SRD = $\Theta$.

### 3.1.4 Parallel Transmitters

We proceed with an example to find an answer for the final question stated previously. Suppose, a station $S$ starts a master communication (i.e., $S$ accesses in a clear channel) with station $R$. The master fails when $R$ (or, $S$) experiences a collision during the data (or, ACK) frame transmission. Let, $R$ receives the data frame at a strength of $p(SRD)$. Since the ACK frame is transmitted at $p_{max}$, $S$ receives the frame at a strength of $\geq p(SRD)$. The IPC at a nearby station, $I_l$, uses $p(SRD)$ and $\text{max}(RTSS, CTSS)$ as $(d_l)$, and therefore, $\varphi_{SRD}$ is equal for the both $R$ and $S$. The IPC at $I_l$ outputs a False only when $d_l > \varphi_{SRD}$ for the both $R$ and $S$. Further, a station can never start a parallel transmission when it is unable to receive the IF–Frame from $S$; hence, a station that starts a parallel transmission must be located within the coverage of $S$. Thus, based on the IPC decisions at different locations, we can split the carrier sensing range of $S$ ($p_{c}(CC_A0)^{-1}$) into three regions namely forbidden, green, and yellow zones as shown in Fig. 3. A station in the yellow zone is located outside the coverage ($\Theta$) of $S$, and therefore, it is unable to receive the IF-Frame from $S$. So, its IPC uses the default values from the third row in Table 1 and outputs a True. Thus, a station, which is located in the yellow zone of a master sender, is not allowed to start a parallel transmission.

A station in the forbidden zone is likely to corrupt the reception at $S$ because it is within the range $\varphi_{SRD}(SRD)$ from $S$. The IPC in the station would eventually return a True after receiving the IF–Frame from $S$ and the station will not access in parallel. The size of the forbidden area varies with $p(SRD)$ (or, the SRD according to (5)) and might span up to the sensing range. The ring shaped region between the yellow and forbidden zones is referred to as green zone. A station in the green zone (green station) receives the IF-Frame and the station will not start a parallel transmission; 1) when it is outside the range $\varphi_{SRD}$ of $R$ as well. Hence, IP–MAC allows parallel transmissions only from the green zone of $S$.

The size of a green zone (i.e., the area in the green zone) around a master sender depends on the value of $PxT$. When the $PxT$ is too small, the size of the green zone becomes very large and a large number of stations may attempt for parallel communications. If the number of such concurrent transmissions exceeds the $PxT$ during the master communication, then the master fails too often and results in bandwidth waste. On the other hand, if it is too large, parallel transmissions would rarely occur due to a reduced green zone size. In order to observe the relation between the green zone size and $PxT$, we normalize the SRD and green zone size with respect to the transmission range $\Theta$ of the master. Let, $SRD = k\Theta$, (where, $0 \leq k \leq 1$) and the corresponding green zone area is $A(\Theta) = A(\varphi_{SRD}(k\Theta))$. Further, let $A(\Theta) = A(\varphi_{SRD}(k\Theta)) = lA(\Theta)$, where, $l (0 \leq l \leq 1)$ is the green zone area with respect to the transmission coverage of the master sender, and thus, $\varphi_{SRD}(k\Theta) = (\sqrt{1-l})\Theta$. Hence, according to the condition in Eq. (6), we can write:

$$PxT \leq \left| \frac{1}{\beta} \left( \frac{\sqrt{1-l}}{k} \right)^{\gamma} \right|$$

(10)

Figure 4 shows the relationship between $PxT$, $l$ and $k$ in (10) for typical shadowing environment ($\gamma = 4$ and $\beta = 25$), and we can choose a feasible $PxT$ from the plot. For example, if the protocol requires to enable half of the coverage as green zone (i.e., $l = 0.5$) when $SRD = 0.15\Theta$ (i.e., $k = 0.15$), it should choose $PxT = 23$. In that case, the protocol cannot support parallel transmissions if $k \geq 0.2$; because $k = 0.2$ pushes the $\varphi_{SRD}$ beyond the transmission range (i.e., $l = 0$ when $k \geq 0.2$). We explain these axioms, by an example with $\Theta = 50$ m and $PxT = 23$, as follows: 1) IP–MAC allows parallel transmissions when $SRD \leq 10$ m ($0.2 \times 50$ m) at the master; 2) when $SRD \leq 7.5$ m ($k = 0.15$), the master sender releases control over at least $50\%$ of its coverage for parallel transmissions; 3) IPC generates a False only when the station is outside the range $\varphi_{SRD}(SRD)$; and 4) IP–MAC guarantees safe master communications with at
From the discussions above, we observe that a proper $P_x T$ value can allow parallel transmissions from stations outside the $\varphi_{P_x T}$ of the master. However, a $P_x T$ value is said to be safe when it guarantees that no more than $P_x T$ number of parallel transmissions occur during a master communication; i.e., when $\nu \leq P_x T$. The number of parallel accesses, $\nu$, will depend on the parallel access mechanism at the green stations. We, therefore, investigate the choice of a failsafe $P_x T$ for IP–MAC later in Sect. 3.3.1 after describing the protocol operation.

3.2 IP–MAC Operation

We describe the IP–MAC operation in steps according to its frame exchange sequence shown in Fig. 5. The top sequence in the figure sketches the master communication (both master sender and receiver), and rest sequences show how other stations behave during the master and how they attempt parallel communications.

3.2.1 Master Communication

When a station detects a clear channel for the DIFS period, it contends for medium access with a random backoff number chosen from the range $[0, CW]$ following the exact DCF sequence. The station with the smallest backoff number wins the contention and it (master sender) initiates a master communication by sending a RTS frame to the intended receiver.

All stations, excepting intended receiver (master receiver), update their own Network Allocation Vector (NAV) when they overhear the RTS, and store RTSS for future use. The master receiver replies with a CTS after an SIFS, if it receives the RTS successfully and its NAV is not already set by any other communication. The CTSS is also stored by the stations when they overhear the CTS. During this RTS-CTS handshaking at the master, all stations use the conventional carrier sensing and their IPC selects the default values from the third row in Table 1. Therefore, the master is safe during this period from the stations in all zones.

After receiving the CTS from the partner, the master sender estimates SRD from CTSS and prepares the IF-Frame with the desired CPT and DPL for the data frame(s). Then it aggregates the IF-Frame with the data frame(s), and starts to transmit the aggregated frame. The master ends when the receiver acknowledges by sending the ACK frame.

3.2.2 Parallel Attempts

Soon as a station receives the IF–Frame from the master (in the partly received data frame), it extracts the SRD, CPT and DPL components and performs the IPC along with the previously stored RTSS and CTSS for the overheard† RTS and CTS at the master. A station at the green zone of the master sender get a Parallel Transmission Opportunity (PXOP) if it is located outside the range $\varphi_{P_x T}$ of both master stations. We define the PXOP as the duration in slots, from receiving the IF-Frame to the end of the master communication. Note that, when a station gets the PXOP, it ignores the CCA output for the remaining period of the PXOP and self-discipline according to its IPC decision. For simplicity, a green station hereinafter refers to the station that obtains the PXOP for a master.

The first two sequences for overhearing stations in Fig. 5 show the parallel accesses by the green stations. Upon obtaining the PXOP, a green station bypasses the carrier sensing and resumes the backoff countdown. The station transmits a parallel RTS to the intended receiver if its backoff counter expires in the current PXOP. Otherwise, it freezes the backoff counter again and switch back to the carrier sensing as soon as the PXOP expires. It should be noted here that, the success of a parallel access depends on the receive condition at the intended parallel receiver. If the intended parallel receiver captures the parallel RTS in presence of the master (and other parallel transmissions as well)

†Some stations may not receive both RTS and CTS from the master. Default values in Table 1 make IPC to receive corresponding RTS or CTS hypothetically. When the station is beyond the master sender coverage, it virtually receives the IFFrame with $SRD = \text{Transmission Range.}$
and if its IPC allows, then the intended receiver replies with a parallel CTS. So, a receiver does not respond to a parallel RTS when it is within the forbidden zone of any other communication. The backoff process at the green stations keeps the number of parallel attempts in a slot to the minimum and reduces the probability of collision at the parallel receivers. It also reduces the number of contending green stations for the master, because every parallel access exposes some other nearby green stations during their backoff process. Thus, it helps in keeping the total number of parallel accesses during a PXOP below $P \times T$.

The rest three sequences in Fig. 5 show how forbidden stations keep them away from parallel accesses. Legacy or non-IPMAC IEEE 802.11 stations also follow these sequences according to DCF protocol.

3.3 Challenges in IP–MAC

3.3.1 Failsafe value of $P \times T$

According the parallel access mechanism in IP–MAC, we observe that the number of parallel accesses during a PXOP (i.e., $\nu$) depends on the backoff counter values at the green stations. Hence, we adopt Bianchi’s [18] well known probabilistic model in order to determine whether a chosen $P \times T$ is failsafe or not. The analysis uses a Markov Chain model for the backoff window states to find the probability $\tau$ that a station transmits in a randomly chosen slot time. For DCF, $\tau$ is given by:

$$\tau = \frac{1}{N \sqrt{T_c^*}}$$

where, $T_c^*$ is the period of time in slots during which the channel is sensed busy by the non-colliding stations, and $N$ is the number of stations within the carrier sensing range. Before starting the master communication, all stations follow basic DCF that senses for a carrier just before transmitting. Thus, with propagation delay $\delta$, we find $T_c^* = t_{RTS} + DIFS + \delta$; where, $t_{RTS}$ is the transmission time to send an RTS frame. Noninterfering stations contend for parallel accesses with the last backoff counter value frozen by the master. Therefore, the transmission probability in a slot remains unchanged for the PXOP period. For simplicity, let, $N$ represents the number of neighboring stations of the master (ignoring the stations outside the coverage as they do not contend during PXOP). So, a $P \times T = N$ always makes the protocol failsafe because no more than $N$ stations can transmit in a PXOP. The protocol becomes unsafe when $P \times T < N$, because there exists a probability that more than $P \times T$ stations transmit in a PXOP and corrupt the master. If the average number of slots in a PXOP is $\lambda$, then the transmit probability of a station, $\mu$, in any slot in a PXOP is:

$$\mu = 1 - (1 - \tau)^4$$

Thus, the probability of more than $P \times T$ transmissions in a PXOP, $Pr[\nu > P \times T]$, is given by:

$$Pr[\nu > P \times T] = \sum_{i=P \times T+1}^{N} \mu^i (1 - \mu)^{N-1}$$

Figure 6 shows the plot $Pr[\nu > P \times T]$ vs. $P \times T$ for different values of $N$, and we observe that for any value of $N$, $Pr[\nu > P \times T] \approx 0$ when $P \times T \geq 20$. Therefore, in IPMAC a master communication is expected to be safe with $P \times T > 20$.

3.3.2 Dealing with Link Asymmetry and Estimation Errors

In wireless environments, the antenna directivity, multipath fading and spatial channel condition might make the wireless links asymmetric. So, when the master sender receives a stronger $\rho(d)$ than that at the master receiver, it endangers the reception at the master receiver. The same problem occurs when a potential interferer receives weaker RTSS and CTSS from the master than the actual interfering signal power in the opposite direction. The errors in estimating the distance and power also put the master in danger. However, a large $P \times T$ ($P \times T \geq 20$) and the backoff before parallel access in IP–MAC jointly combat with the link asymmetry and estimation errors, and keep the master intact. The large $P \times T$ safeguards the master from such problem in three ways: first, it gives the master a high tolerance, second, it ensures a weaker $\rho(d)$ from a green station, and finally, it reduces the number of green stations (i.e., parallel attempts). The backoff operation minimizes the number of parallel accesses in a slot, and thus, forces different green stations to access in different time slots of a PXOP. Since a parallel transmission continues in the subsequent slots only when it receives a parallel CTS from the intended receiver, the number of active parallel transmissions in a slot is expected to remain far below than the tolerance of the master. The results found in simulations also justify this observation. We also observe that the distance and signal power estimations using the worst channel condition (i.e., the highest possible $y$ for the environment) also minimize the infirmities due to the estimation errors.
4. Performance Analysis

We simulated the proposed IP–MAC protocol in a discrete event simulator to verify its performance and stability compared to the DCF counterpart. We simulated the access schemes with two distinct $CC_{A0}$ values: $-106$ dBm for master communications in IP–MAC and $-90$ dBm for basic DCF operation. The former $CC_{A0}$ value is selected using Eq. (8) and the later one follows the IEEE 802.11 standard (i.e., $CC_{A0} = P_x$). Considering a very low probability of PLCP header corruption at a receiver, both versions use constant $CC_{A0}$ values at the stations (i.e., $20$ dB raise in the carrier sensing level is not used in the simulation). We also ran simulations with TPC scheme to compare the performance of both IP–MAC and TPC. In simulations, $N$ number of stations were deployed in a $100 \times 100$ terrain and they were offered with the same traffic load (same packet size and at same arrival rate). Table 2 lists the basic simulation parameters for the IP–MAC. However, in the TPC simulations, we compute $P_t$ at a station considering the required minimum $p(d)$ at the receiver station with a $10$ dB noise margin.

At first, we observed IP–MAC behavior and performance in a roseate environment where all stations select the nearest neighbor as the destination. We refer to this topology as Nearest Destination or simply as NearDest. Next, we ran simulations for two realistic environments: Arbitrary and Grid. The arbitrary topology represents the ad hoc peer-to-peer network, where each source station randomly selects a destination among the neighbors. The grid topology has several access points (AP) at regular grid locations in the target area, and $40$ ordinary stations communicate with the nearest AP.

4.1 Channel Access and Packet Delivery

The number of channel accesses characterizes protocol efficiency in spectrum sharing or spatial reuse. Figure 7 shows the normalized gain in channel access by IP–MAC with respect to the DCF. We observe significant increase in channel access by IP–MAC stations than the DCF counterpart in all configurations and it increases linearly with the number of stations. Parallel transmissions rarely occur in lightly loaded networks because packets arrive at distant time instances at the contending stations. So, we observe almost equal performance from both protocols in lightly loaded networks.

In NearDest, the sender and receiver of the flows are very close to each other; hence the receivers get very strong $p(d)$. As a result, about $45\%$ to $78\%$ of the flows allow parallel transmissions from other stations we observe the high access gain in the NearDest. Comparatively a few flows allow parallel transmissions in the arbitrary topology (about $10\%$ to $15\%$). The communications in grid topology are AP bound. Therefore, the number of APs in the area dominates the gain.

The success of a parallel attempt depends on the receive status at the intended parallel receiver. During the simulation runs, we observed that the unsuccessful RTS-CTS handshaking for the parallel transmissions dominates over other failure categories (about $74\%$ to $99\%$ of total failures in arbitrary topology and about $95\%$ to $99.5\%$ in nearest and grid topologies). We also observed that the number of parallel accesses across a PXOP never exceeds $16$ (using $P_xT = 23$). So, we did not observe even single occurrence of master communication failure due to excessive parallel attempts from the green stations or for the link asymmetry.

We identify the following four reasons behind the parallel attempt failures. First, an intended parallel receiver cannot accept RTS request because of a True IPC value. Second, the RTS (or CTS) collides at the intended receiver (transmitter) for the ongoing master and other concurrent transmissions. Third, some other green stations access in parallel near a parallel sender and the CTS from the parallel receiver experiences collision at the parallel sender. And finally, the intended parallel receiver also switches to transmit-mode for another parallel transmission. For the single transmission scheme, the DCF is free from such failures. However, since the $CC_{A0}$ value in the IEEE 802.11 standard neither considers the vulnerability with SRD value nor the impact of transmissions from multiple hidden stations, DCF suffers severe collisions in the ad hoc modes (in the nearest and arbitrary configurations) when the traffic load and/or the number of nodes in the network grows.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_xT$</td>
<td>23</td>
</tr>
<tr>
<td>Transmit Rate (Data/Ctrl)</td>
<td>54 Mbps/1 Mbps</td>
</tr>
<tr>
<td>Transmit Power (Data/Ctrl)</td>
<td>23 dBm/23 dBm</td>
</tr>
<tr>
<td>Receive Threshold (Sensitivity, $P_s$)</td>
<td>$-90$ dBm</td>
</tr>
<tr>
<td>$CC_{A0}$ (IP–MAC/DCF)</td>
<td>$-106$ dBm/$-90$ dBm</td>
</tr>
<tr>
<td>Noise Factor</td>
<td>10 dB</td>
</tr>
<tr>
<td>Link Asymmetry (up/down)</td>
<td>1:1 to 1:3</td>
</tr>
<tr>
<td>Ranges (Theta/$CCA$)</td>
<td>48 m/116 m</td>
</tr>
<tr>
<td>$\beta$</td>
<td>25</td>
</tr>
<tr>
<td>Aggregated Packet Size</td>
<td>1000 bytes</td>
</tr>
<tr>
<td>Offered Load</td>
<td>1–30 KBps</td>
</tr>
</tbody>
</table>

Fig. 7 Gain in channel access in IP–MAC wrt. DCF.
In Fig. 8, we plot the Packet Delivery Ratio (PDR) for the IP–MAC and DCF protocols. The PDR is computed as the ratio of the number of successfully delivered packets to the total number of packets arrived for transmission, we express it in percentile. Overall, PDR in both protocols decreases with the number of contending stations (APs). The rate of decrease increases with offered loads at the stations. The binary exponential backoff scheme in DCF penalizes a station for each transmission failure; hence, the IP–MAC performance is affected by the unsuccessful parallel accesses. Low density networks suffer severely because of the limited scope of parallel access. On the other hand, even though the failure rate is high at high density networks, the successful parallel transmissions compensate the cost and improve overall PDR in the network. Due to the single access policy and unmanaged access by the hidden stations, the service time with DCF increases and the stations experience severe packet dropping. As a result, we observe an worse performance with DCF than that with IP–MAC.

4.2 Impact on Throughput

In Fig. 9, we show the normalized throughput gain for IP–MAC, where the throughput gain is measured as the ratio of throughput obtained by IP-MAC to that obtained by the DCF. The aggregate throughput increases with the number of stations (APs) in the area, and the offered load determines the rate of gain. The increased PDR in IP–MAC improves the average throughput in the nearest and grid topologies. For comparatively large number of unsuccessful attempts in the arbitrary topology, DCF outperforms the IP–MAC.

Table 3, wherein we present the summarized results for the TPC scheme, shows a more aggressive behavior of the TPC in accessing the channel. However, the PDR is comparatively lower than that in IP–MAC in all topologies because of the mutual interference between the master and parallel transmissions. Several parallel transmissions from the hidden (because of reduced transmit power) stations jointly corrupts the master (as well as the parallel transmissions). Therefore, we observe a decreased aggregate throughput in TPC than that of the IP–MAC (most of the time, a worse than DCF as well).

4.3 Impact on Fairness

The comparative fairness (the popular Jains fairness index) of these two protocols is shown in Fig. 10. Since IP–MAC operates on top of the DCF protocol, it inherits the short-term unfairness problem from DCF. The contention resolution and the binary exponential backoff in DCF scheme jointly affect the fairness. The unsuccessful parallel attempts in IP-MAC decrease the fairness further because they force more stations to contend with larger contention window. The situation deteriorates when a station is starved for a longer period due to repeated access from other successful stations (both master and parallel accesses). However, in the grid topology, an increased number of APs in the same area improves overall PDR, and therefore, we observe better fairness with a large number of APs.

<table>
<thead>
<tr>
<th>Nodes/Top</th>
<th>Access</th>
<th>PDR (%)</th>
<th>Throughput Gain</th>
</tr>
</thead>
<tbody>
<tr>
<td>(APs)</td>
<td>Gain</td>
<td></td>
<td>TPC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IP–MAC</td>
</tr>
<tr>
<td>20 (4)</td>
<td>NearDest</td>
<td>1.251</td>
<td>99.61</td>
</tr>
<tr>
<td></td>
<td>Arbitrary</td>
<td>1.253</td>
<td>99.38</td>
</tr>
<tr>
<td></td>
<td>Grid</td>
<td>1.066</td>
<td>98.77</td>
</tr>
<tr>
<td>40 (9)</td>
<td>NearDest</td>
<td>1.895</td>
<td>91.84</td>
</tr>
<tr>
<td></td>
<td>Arbitrary</td>
<td>1.577</td>
<td>76.91</td>
</tr>
<tr>
<td></td>
<td>Grid</td>
<td>1.118</td>
<td>96.46</td>
</tr>
<tr>
<td>60 (16)</td>
<td>NearDest</td>
<td>2.542</td>
<td>76.31</td>
</tr>
<tr>
<td></td>
<td>Arbitrary</td>
<td>2.047</td>
<td>77.28</td>
</tr>
<tr>
<td></td>
<td>Grid</td>
<td>1.391</td>
<td>88.47</td>
</tr>
<tr>
<td>80 (20)</td>
<td>NearDest</td>
<td>3.678</td>
<td>70.14</td>
</tr>
<tr>
<td></td>
<td>Arbitrary</td>
<td>2.341</td>
<td>54.73</td>
</tr>
<tr>
<td></td>
<td>Grid</td>
<td>1.482</td>
<td>89.76</td>
</tr>
<tr>
<td>100 (25)</td>
<td>NearDest</td>
<td>4.295</td>
<td>64.39</td>
</tr>
<tr>
<td></td>
<td>Arbitrary</td>
<td>2.962</td>
<td>42.39</td>
</tr>
<tr>
<td></td>
<td>Grid</td>
<td>1.621</td>
<td>87.58</td>
</tr>
</tbody>
</table>

Fig. 9  Throughput gain in IP–MAC.
4.4 Average Packet Delivery Time

The delivery time of a packet (PDT) is defined as the time from the packet arrival at the MAC layer until the notification of successful transmission. It includes the queuing delay, contention period, and retransmissions due to error or collision. Figure 11 shows the normalized relative PDTs for both protocols. We observe that IP–MAC offers better PDT with more than 10 KB/s load. With lighter loads, the performance improvement is obtained due to the success of the parallel attempts.

4.5 Discussion

We can summarize the results as follows. First, the performance of IP–MAC primarily confides to the underlying network topology. Second, its effectiveness relies on the tradeoff between contributions by the parallel transmission and failure penalty in a particular topology. And finally, its gain in throughput costs fairness. Since the punishments by the exponential backoff mechanism affect the IP–MAC performance, IP–MAC demands for a new failure handling scheme to provide with better performance.

5. Conclusion

Giving a wireless station the ability to identify itself as non-colliding with other transmissions has the potential of fostering MAC protocols to offer enhanced service and improving spatial reuse and overall network performance. The proposed IP–MAC protocol practically supports the identification. In IP–MAC, stations access in clear channels using DCF and cooperate with the neighbors by providing the interference factors. The neighbors of the communication perform an Interference Potentiality Check for the communication and the noninterfering neighbors access the medium in the busy channel. Simulation results show that the IP–MAC performance is severely affected by underlying network topology, and it shows better performance in topologies where the flows are separated spatially. Although the design of IP–MAC is based on the IEEE 802.11 MAC; the core technique can also be extended for other CSMA/CA driven protocols.

There are still more issues to be explored in IP–MAC: impact of multipath fading and multirate data transmission on the performance of IP–MAC. One downside of the protocol is that it might cause to drop network performance in unfriendly environments; hence, it demands for redesigning the retransmission scheme to keep at least the DCF performance.

Acknowledgements

This work was partially supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by MEST (No. 2009-0083838) and by UCN Project, Knowledge and Economy Frontier R&D Program of the Ministry of Knowledge Economy (MKE) in Korea as a result of UCN’s subproject 10C2-C2-21T. Dr. C.S. Hong is the corresponding author.

References

Thus, with a negligible background noise, the left side of Eq. (4) yields:

\[
p_p \sum_{i=1}^{n} P_i = \frac{p(d_0) \times d^{-\gamma}}{\sum_{i=1}^{n} d_i^{-\gamma}}
\]

(A-2)

**Appendix:** Derivation of Eq. (5)

From Eq. (3), we can write,

\[
\sum_{i=1}^{n} p_i(d_i) = \sum_{i=1}^{n} \left( p(d_0) \times \left( \frac{d_i}{d_0} \right)^{-\gamma} \right)
\]

\[
= p(d_0) \times \sum_{i=1}^{n} \left( \frac{d_i}{d_0} \right)^{-\gamma}
\]

\[
= p(d_0) \frac{d_0^{-\gamma} \times d_i^{-\gamma}}{\sum_{i=1}^{n} d_i^{-\gamma}}
\]

Thus, with a negligible background noise, the left side of
JangYeon Lee received the B.S. and M.S. degrees in electronic communication engineering from Hanyang University, Seoul, Korea, in 1996 and 2002, respectively. He joined Korea Electronics Technology Institute (KETI) in 2002, where he has been researching and developing wireless personal area networks (WPAN) system as a senior researcher at the WNRC (Wireless Network Research Center). His current research interests are in the areas of wireless communication system design and implementation, especially, for wireless personal area networks (WPAN) and Binary CDMA technology.

Jin-Woong Cho received the B.S., M.S., and Ph.D. degrees in electronic engineering from Kwangwoon University, Seoul, Korea, in 1986, 1988, and 2001, respectively. He joined Korea Electronics Technology Institute (KETI) in 1992, where he has been researching and developing wireless personal area networks (WPAN) system as a director at the WNRC (Wireless Network Research Center). He worked as STA fellow for Electrotechnical Laboratory in Japan in 1999. His current research interests are in the areas of wireless communication system design and implementation, especially, for wireless personal area networks (WPAN) and Binary CDMA technology.