On the Theoretical Gap of Channel Hopping Sequences With Maximum Rendezvous Diversity in the Multichannel Rendezvous Problem

Cheng-Shang Chang, *Fellow, IEEE*, Jang-Ping Sheu, *Fellow, IEEE*, and Yi-Jheng Lin

***Abstract*— In the literature, there are several well-known periodic channel hopping (CH) sequences that can achieve maximum rendezvous diversity in a cognitive radio network (CRN). For a CRN with N channels, it is known that the period of such a CH sequence is at least N^2. The asymptotic approximation ratio, defined as the ratio of the period of a CH sequence to the lower bound N^2 when $N \to \infty$, is still 2.5 for the best known CH sequence in the literature. An open question in the multichannel rendezvous problem is whether it is possible to construct a periodic CH sequence that has the asymptotic approximation ratio of 1. In this paper, we tighten the theoretical gap by proposing CH sequences, called IDEAL-CH, that have the asymptotic approximation ratio of 2. For a weaker requirement that only needs the two users to rendezvous on *one* commonly available channel in a period, we propose channel hopping sequences, called ORTHO-CH, with period $(2p+1)p$, where p is the smallest prime not less than N.**

***Index Terms*— Multichannel rendezvous, worst case analysis.**

I. Introduction

THE multichannel rendezvous problem that asks two users to find each other by hopping over their available channels is a fundamental problem in cognitive radio networks (CRNs) and has received a lot of attention lately (see, e.g., the excellent book [1] and references therein). Such a problem is also found to be relevant and useful to new networking trends, such as the Internet-of-Things (see, e.g., [2], [3], [4]). In this paper, we tighten a theoretical gap on the minimum period of the periodic channel hopping (CH) sequences that achieve maximum rendezvous diversity. A channel is called a *rendezvous* channel of a periodic CH sequence if two asynchronous users (with any arbitrary starting times of their CH sequences) rendezvous on that channel within the period of the sequence. A periodic CH sequence is said to achieve maximum rendezvous diversity for a CRN with N channels if all the N channels are rendezvous channels. In the asymmetric setting, it was shown in Theorem 1 of [5] that there do not exist deterministic periodic CH sequences that can achieve maximum rendezvous diversity with periods less than or equal to N^2. For the symmetric setting, the negative result of Theorem 1 of [5] is further extended in Theorem 3 of [6]. It was shown that the length of the period p satisfies the following lower bound:

$$p \geq \begin{cases} N^2+N & \text{if } N \leq 2 \\ N^2+N+1 & \text{if } N \geq 3 \text{ and } N \text{ is a prime power} \\ N^2+2N & \text{otherwise.} \end{cases}$$

The lower bound is not always tight. Via extensive computer enumeration, it was shown in [6] that the lower bound is tight when $N = 1, 2, 5, 6$. It is also tight for $N = 8$ by an explicit CH sequence in [7]. In the literature, there are various periodic CH sequences that can achieve maximum rendezvous diversity, see, e.g., CRSEQ [8], JS [9], DRDS [6], T-CH [10], and DSCR [11]. In particular, T-CH [10] and DSCR [11] have the shortest period $2N^2 + N\lfloor N/2 \rfloor$ when N is a prime. These CH sequences are called *nearly optimal* CH sequences as their periods are $O(N^2)$, which is comparable to the lower bound N^2. However, the asymptotic approximation ratio, defined as the ratio of the period to the lower bound N^2 when $N \to \infty$, is still 2.5 for T-CH and DSCR, 3 for CRSEQ and DRDS. One of the open questions in the multichannel rendezvous problem is whether it is possible to construct a periodic CH sequence that has the asymptotic approximation ratio of 1. The main objective of this paper is to further tighten the theoretical gap by proposing CH sequences, called IDEAL-CH, that have the asymptotic approximation ratio of 2. To the best of our knowledge, this is the best asymptotic approximation ratio in the literature.

The mathematical tools for the construction of IDEAL-CH are (i) perfect difference sets [12] and (ii) ideal matrices [13]. Using difference sets for constructing CH sequences is not new (see, e.g., [6], [7]). However, it seems that researchers in the field may not be familiar with the concept of ideal matrices. To our surprise, we find out that the constructions of CRSEQ [8], T-CH [10], and DSCR [11], are all based on ideal matrices and they are "equivalent" in that sense. In particular, CRSEQ, T-CH, and DSCR all add a "stay" matrix in front of a "jump" matrix constructed from an ideal matrix. The added "stay" matrix increases the length of a CH sequence. To push the asymptotic approximation ratio further down, our idea is to embed difference sets into an ideal matrix. By doing so,

Manuscript received September 11, 2019; revised April 16, 2020 and October 14, 2020; accepted March 17, 2021; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor J. Shin. This work was supported by the Ministry of Science and Technology, Taiwan, under Grant 106-2221-E-007-023-MY3, Grant 109-2221-E-007-091-MY2, and Grant 106-2221-E-007-019-MY3. Date of publication March 26, 2021; date of current version August 18, 2021. *(Corresponding author: Cheng-Shang Chang.)*

The authors are with the Institute of Communications Engineering, National Tsing Hua University, Hsinchu 300044, Taiwan (e-mail: cschang@ee.nthu.edu.tw; sheujp@cs.nthu.edu.tw; s107064901@m107.nthu.edu.tw).

Digital Object Identifier 10.1109/TNET.2021.3067643

we are able to eliminate the need for adding a "stay" matrix and thus shorten the length of IDEAL-CH.

CRSEQ, JS, DRDS, T-CH and DSCR, and IDEAL-CH are sequences that can achieve maximum rendezvous diversity within their periods. A weaker requirement is to ask the two users to rendezvous on *one* commonly available channel and measure the maximum time-to-rendezvous (MTTR). For this, we propose a CH sequence, called ORTHO-CH, which can guarantee the rendezvous of the two users within a period of the ORTHO-CH sequence. When the available channel set of a user is a subset of the N channels, the period of our ORTHO-CH sequence is $(2p+1)p$, where p is the smallest prime not less than N. Thus, ORTHO-CH has the MTTR bound $(2p+1)p$. Such a result is comparable to the best algorithms in the literature, e.g., FRCH [14] with the MTTR bound $(2N+1)N$ for $N \neq ((5+2\alpha)*r-1)/2$ for all integer $\alpha \geq 0$ and odd integer $r \geq 3$, and SRR [15] with the MTTR bound $2p^2+2p$.

The paper is organized as follows: In Section II, we provide a brief review of the multichannel rendezvous problem, including the classification of the problem in Section II-A, the formulation of the problem and summaries of known results in Section III-B. In Section III, we propose the IDEAL-CH sequences that have the asymptotic approximation ratio of 2. By extending the mathematical theories for IDEAL-CH, we propose in Section IV the ORTHO-CH sequences that have the MTTR bound $p(2p+1)$, where p is the smallest prime not less than the total number of channels. The paper is concluded in Section V.

II. The Multichannel Rendezvous Problem

In this section, we provide a brief review of the multichannel rendezvous problem (MRP).

A. Classification of the Problem

As mentioned in the Introduction, the multichannel rendezvous problem asks two *users* to find each other by hopping over a set of possible *channels (discrete locations)* with respect to *time*. In view of this, there are three key elements in the multichannel rendezvous problem: (i) users, (ii) time, and (iii) channels. Based on the assumptions on *users, time, and channels*, CH schemes can be classified into various settings. To compare the level of difficulty between two settings A and B, we use the partial ordering $A \prec B$ when the assumption in setting A is *stronger* than that in B. Thus, the CH sequences constructed by using a *weaker* assumption in setting B are also applicable in setting A.

1) Users: There are three commonly used settings for users: (i) the symmetric setting (*sym* for short), (ii) the ID setting (*ID* for short), and (iii) the asymmetric setting (*asym* for short). In the *symmetric* setting, users are *indistinguishable* and thus follow the same algorithm to generate their CH sequences. On the other hand, users are *distinguishable* by their unique identifiers (ID) in the ID setting. For instance, a device in a CRN may be equipped with a unique 48-bit medium access control (MAC) address. The asymmetric setting is a special case of the unique ID setting when these two users can be distinguished by one bit ID, e.g., user 1 is assigned with ID 0 and user 2 is assigned with ID 1. In the asymmetric setting, the two users can be assigned two different roles so that they can follow two different algorithms to generate their CH sequences. In the literature, these CH algorithms are called *role-based CH algorithms* (see, e.g., [16]–[18], [19]). For instance, a user can be assigned the role of a sender or the role of a receiver. The receiver can stay on the same channel while the sender cycles through all the available channels. Since users follow different algorithms, the time-to-rendezvous can be greatly reduced by using role-based algorithms. In the general ID setting, a common approach is to map an ID into an M-bit binary vector and partition the time into intervals with M time slots. Then, ask each user to play a role in the ℓ^{th} time slot in an interval according to the ℓ^{th} bit in the mapped binary vector. However, using IDs to generate CH sequences might be vulnerable to attacks from adversaries. As such, it is preferable to remain anonymous in practice.

In the symmetric setting, the two users are indistinguishable. The key in the symmetric setting is to *break symmetry*. One way to break symmetry is to select a channel from the available channel set of a user and use that as the ID of a user. One problem for that is when the two users select the same channel and thus have the same ID. In the level of difficulty of the three settings for users,

$$asym \prec ID \prec sym.$$

2) Time: For the multichannel rendezvous problem, we only consider the discrete-time setting, where time is indexed from $t = 0, 1, 2, \ldots$. There are two settings for time: (i) the synchronous setting (*sync* for short) and (ii) the asynchronous setting (*async* for short). In the *synchronous* setting, the clocks (i.e., the indices of time slots) of both users are assumed to be synchronized to the global clock and thus the time indices of these two users are the same. When the clocks of the two users are synchronized, both users can start their CH sequences simultaneously to speed up the rendezvous process. On the other hand, in the *asynchronous* setting, the clocks of both users may not be synchronized to the global clock and thus the time indices of these two users might be different. In a distributed environment, it might not be practical to assume that the clocks of two users are synchronized as they have not rendezvoused yet. Without clock synchronization, guaranteed rendezvous is much more difficult. In the level of difficulty of the two settings for time,

$$sync \prec async.$$

3) Available Channels (Search Space): For the multichannel rendezvous problem, we only consider distinct channels (discrete locations in [20]) as the search space. These N channels are indexed from $0, 1, \ldots, N-1$. The available channel set of a user is a subset of these N channels. There are two settings for available channels: (i) the homogeneous setting (*homo* for short) and (ii) the heterogeneous setting (*hetero* for short). In the *homogeneous* setting, the available channel sets of the two users are assumed to be the same. On the other hand, in the heterogeneous setting, the available channel sets of the two users might be different. In a CRN, two users that are close

to each other are likely to have the same available channel sets. Due to the limitation of the coverage area of a user, two users tend to have different available channel sets if they are far apart. Rendezvous in a homogeneous environment is in general much easier than that in a heterogeneous environment. In the level of difficulty of the two settings for available channels,

$$homo \prec hetero.$$

4) Labels of Channels: There are three widely used settings for the labels of channels: (i) the globally labelled setting (*global* for short), (ii) the locally labelled setting (*local* for short), and (iii) the indistinguishable setting (*ind* for short). In the multichannel rendezvous problem, the N channels are commonly assumed to be *globally labelled*, i.e., the labels of the channels of the two users are the same. On the other hand, the users are only allowed to label their available channels by themselves in the *locally labelled* setting. In the locally labelled setting, the labels of channels could be different. In the book [1], the locally labelled setting is referred to as the *oblivious* setting. The most difficult setting for labels of channels is where users are not allowed to leave any marks for channels (see, e.g., [21]). In such a setting, these N channels are *indistinguishable* and a user even does not know the previous channels on which it hops. Thus, nothing can be learned from a failed attempt to rendezvous in the indistinguishable setting. In the level of difficulty of the three settings for labels of channels,

$$global \prec local \prec ind.$$

Like the notations in queueing theory, a multichannel rendezvous problem (MRP) can be described by a series of abbreviations and slashes such as

$$A/B/C/D,$$

where A is the abbreviation for the setting of *users*, B is the abbreviation for the setting of *time*, C is the abbreviation for the setting of *available channels*, and D is the abbreviation for the setting of *labels of channels*. For instance, the sym/async/hetero/global MRP denotes the problem where (i) the two users are symmetric and thus follow the same algorithm, (ii) the clocks of the two users are not synchronized, (iii) the available channel sets of the two users are different, and (iv) the channels are globally labelled.

We note that there are five categories for the classification of the multichannel rendezvous problem in the book [1]: $<$ Alg, Time, Port, ID, Label $>$. Here we combine the *Alg* (algorithm) category and the *ID* category into our *user* category. Also, the symmetric (resp. asymmetric) port setting in [1] corresponds to the homogeneous (resp. heterogeneous) setting in which the two users have the same (resp. different) available channel sets. Thus, the four categories in our classification are basically the same as the five categories in [1].

B. Mathematical Formulation of the Problem

To formulate the multichannel rendezvous problem (MRP), let us consider a CRN with N channels (with $N \geq 2$), indexed from 0 to $N-1$. There are two (secondary) users who would like to rendezvous on a common unblocked channel by hopping over these channels with respect to time. We assume that time is slotted (the discrete-time setting) and indexed from $t = 0, 1, 2, \ldots$. The length of a time slot, typically in the order of 10ms, should be long enough for the two users to establish their communication link on a common unblocked channel. In the literature, the slot boundaries of these two users are commonly assumed to be aligned. In the case that the slot boundaries of these two users are not aligned, one can double the size of each time slot so that the overlap of two misaligned time slots is not smaller than the original length of a time slot.

The available channel set for user i, $i = 1, 2$,

$$\mathbf{c}_i = \{c_i(0), c_i(1), \ldots, c_i(n_i - 1)\},$$

is a subset of the N channels. Let $n_i = |\mathbf{c}_i|$ be the number of available channels to user i, $i = 1, 2$. In the homogeneous setting, the available channel set for each user is simply the set of the N channels, i.e.,

$$\mathbf{c}_1 = \mathbf{c}_2 = \{0, 1, \ldots, N-1\}.$$

We assume that there is at least one channel that is commonly available to the two users (as otherwise, it is impossible for the two users to rendezvous), i.e.,

$$\mathbf{c}_1 \cap \mathbf{c}_2 \neq \varnothing. \tag{1}$$

Denote by $X_1(t)$ (resp. $X_2(t)$) the channel selected by user 1 (resp. user 2) at time t (of the global clock). Note that $\{X_1(t), t \geq 0\}$ and $\{X_2(t), t \geq 0\}$ are sequences of random variables. Then, the time-to-rendezvous (TTR), denoted by T, is the number of time slots (steps) needed for these two users to select a common available channel, i.e.,

$$T = \inf\{t \geq 0 : X_1(t) = X_2(t)\} + 1, \tag{2}$$

where we add 1 in (2) as we start from $t = 0$. The maximum time-to-rendezvous (MTTR) is defined as the essential supremum of the random variable T, i.e., the least upper bound of T. As such, we say a CH scheme has a maximum time-to-rendezvous (MTTR) bound γ (for some finite constant γ) if $T \leq \gamma$.

In addition to the time-to-rendezvous, we are also interested in the time to achieve maximum rendezvous diversity, denoted by $T^\sharp$, which is defined as the first time that the two users have met each other on every commonly available channel. Specifically, let T_i be the first time that these two users hop on channel i at the same time, i.e.,

$$T_i = \inf\{t \geq 0 : X_1(t) = X_2(t) = i\} + 1. \tag{3}$$

Then

$$T^\sharp = \max_{i \in \mathbf{c}_1 \cap \mathbf{c}_2} T_i. \tag{4}$$

Note that T can also be presented as follows:

$$T = \min_{i \in \mathbf{c}_1 \cap \mathbf{c}_2} T_i. \tag{5}$$

Clearly, $T \leq T^\sharp$. The maximum conditional time-to-rendezvous (MCTTR) is defined as the essential supremum of the random variable $T^\sharp$, i.e., the least upper bound of $T^\sharp$.

TABLE I
KNOWN RESULTS OF VARIOUS RENDEZVOUS ALGORITHMS IN THEIR MOST DIFFICULT SETTINGS

	users	time	channels	labels	MTTR/MCTTR	ETTR
WFM [20], [28]	asym	async	homo	local	N	$\frac{N+1}{2}$
WFM-MRD [28]	asym	async	hetero	local	N^2 (MRD)	
AFCHS [29]	asym	async	hetero	global	N^2 (MRD)	
coprime MC [22], [23]	asym	async	hetero	local	$2(n_1+1)n_2$ (MRD)	
FOCAL [30]	sym	async	homo	global	1	1
SynMAC [31]	sym	sync	hetero	global	N (MRD)	
M-QCH [32]	sym	sync	hetero	global	$3N$ (MRD)	
SSCH [33]	sym	sync	homo	global	$N+1$	$\frac{N+1}{2}+\frac{1}{2}-\frac{1}{2N}$
FPP [34]	sym	sync	homo	global	$N+1$	$\frac{N+1}{2}+\frac{1}{2}-\frac{1}{2N}$
RRICH [28]	sym	sync	hetero	global	$N(N+1)$ (MRD)	
CACH [28]	sym	sync	hetero	global	$N(u+1)$ (MRD)	
SeqR [35]	sym	async	homo	global	$N(N+1)$	
DRSEQ [36]	sym	async	homo	global	$2N+1$	$N-\frac{1}{6}+\frac{2N^2+11N-4}{6N(2N+1)^2}$
JS [9]	sym	async	hetero	global	$3N^3+o(N^3)$ (MRD)	
CRSEQ [8]	sym	async	hetero	global	$P(3P-1)$ (MRD)	
DRDS [6]	sym	async	hetero	global	$3P^2$ (MRD)	
T-CH [10]	sym	async	hetero	global	$P(2P+\lfloor P/2 \rfloor)$ (MRD)	
DSCR [11]	sym	async	hetero	global	$P(2P+\lfloor P/2 \rfloor)$ (MRD)	
IDEAL-CH (ours)	sym	async	hetero	global	$2P'^2$ (MRD)	
EJS [37]	sym	async	hetero	global	$4P(P+1-G)$	
FRCH [14]	sym	async	hetero	global	$N(2N+1)^*$	
SARAH [38]	sym	async	hetero	global	$8N^2+o(N^2)$	
SRR [15]	sym	async	hetero	global	$2P^2+2P$	
ORTHO-CH (ours)	sym	async	hetero	global	$2P^2+P$	
S-ACH [5]	ID	async	hetero	global	$6LN^2$ (MRD)	
E-AHW [39]	ID	async	hetero	global	$(3L+1)NP$ (MRD)	
CBH [24]	ID	async	hetero	local	$O(L(\max[n_1,n_2])^2)$ (MRD)	
Adv. rdv-η_1 [25]	ID	async	hetero	local	$(2L+3)n_1n_2)$ (MRD)	$(2L+3)\frac{n_1n_2}{G}$
Two-prime MC [22]	ID	async	hetero	local	$6(\lceil L/4 \rceil * 5+6)n_1n_2$ (MRD)	$\frac{n_1n_2}{G}+O((1-\frac{n_1n_2}{G})^L)$
QR [40]	sym	async	hetero	global	$9(\lceil \lceil \log_2 N \rceil /4 \rceil * 5+6)n_1n_2$	$\frac{n_1n_2}{G}+O((1-\frac{n_1n_2}{G})^{\log_2 N})$
Catalan [27]	sym	async	hetero	global	$O((\log\log N)n_1n_2)$ (MRD)	
MTP [41]	sym	async	hetero	global	$64(\lceil \log_2 \log_2 N \rceil +1)(\max[n_1,n_2])^2$ (MRD)	
FMR [42]	sym	async	hetero	global	$9(2\lceil \log_2(\lceil \log_2 N \rceil) \rceil +7)n_1n_2$ (MRD)	
QECH [4]	sym	async	hetero	global	$O((\log N)n_1n_2)$	
AW [20]	sym	sync	homo	local		$0.829N$
random	sym	async	hetero	ind		$\frac{n_1n_2}{G}$

Remarks: N is the total number of channels, P is a prime not less than N, P' is a prime with $P'-2\sqrt{P'} \geq N$, n_1 (resp. n_2) is the number of available channels of user 1 (resp. user 2), G is the number of common channels of two users, and L is the length of a user ID (in bits). (MRD) stands for maximum rendezvous diversity. For FRCH, $N \neq ((5+2\alpha)*r-1)/2$ for all integer $\alpha \geq 0$ and odd integer $r \geq 3$. For CACH (resp. FOCAL, SynMAC, M-QCH), the channel load is $1/u$ (resp. 1, 1, 2/3).

As such, we say a CH scheme has a maximum conditional time-to-rendezvous (MCTTR) bound γ if $T^\sharp \leq \gamma$.

In the literature, there are three commonly used metrics for evaluating the performance of a CH sequence:

(i) expected time-to-rendezvous (ETTR),
(ii) maximum time-to-rendezvous (MTTR), and
(iii) maximum conditional time-to-rendezvous (MCTTR).

The simplest way to generate CH sequences is the *random* algorithm that selects a channel uniformly at random in a user's available channel set in every time slot. The random algorithm performs amazingly well in terms of ETTR and its ETTR is quite close to the lower bound in the asym/async/hetero/local MRP (see, e.g., [22]). As such, it outperforms many CH algorithms proposed in the literature in terms of ETTR, including the modified modular clock algorithm [23], FRCH [14], CBH [24], the advanced rendezvous protocol (Adv. rdv) [25], CHGA [26], JS [9]. However, the random algorithm does not have bounded MTTR. Moreover, as pointed out in [27], the deterministic setting is the gold-standard in the theoretical analysis community for cognitive radio networks as it does not require to have an available source of randomness, and provides an absolute guarantee on rendezvous time. Thus, for theoretical analysis, researchers in the field focus mostly on MTTR/MCTTR.

In Table I, we provide a summary of the known results of various rendezvous algorithms in their most difficult settings.

III. IDEAL-CH

In this paper, we focus on the sym/async/hetero/global MRP. As shown in Table I, CRSEQ [8], JS [9], DRDS [6], T-CH [10], and DSCR [11] are known CH sequences that achieve maximum rendezvous diversity. However, the asymptotic approximation ratio, defined as the ratio of the period to the lower bound N^2 when $N \to \infty$, is still 2.5 for T-CH and DSCR, 3 for CRSEQ and DRDS. In this section, we tighten

the theoretical gap by proposing IDEAL-CH that has the asymptotic approximation ratio of 2.

A. MACH Sequences and Matrices

Recall that a periodic CH sequence is said to achieve the maximum rendezvous diversity (MRD) for a CRN with N channels if the two users rendezvous on every channel within the period of the sequence. In the following definition, we formally state the mathematical properties for an Asynchronous Channel Hopping sequence with Maximum rendezvous diversity (MACH sequence).

Definition 1: An (N, p)-MACH sequence $\{c(t), 0 \leq t \leq p-1\}$ satisfies the following one dimensional maximum rendezvous diversity (1D-MRD) property:

> **The 1D-MRD property**: for any time shift $0 \leq d \leq p-1$ and any channel $0 \leq k \leq N-1$, there exists $0 \leq t \leq p-1$ such that
>
> $$c(t) = c(t \oplus d) = k, \tag{6}$$
>
> where $\oplus$ denotes addition modulo p.

We note that an MACH sequence is simply called a *good* sequence in [6], and its connection to the Disjoint Relaxed Difference Set (DRDS) was first made in that paper. Analogous to the definition of an MACH sequence, we define its 2D version as follows:

Definition 2: A $p \times p$ matrix $C = (c_{i,j})$ with $i, j = 0, 1, \ldots, p-1$ is called an (N, p)-MACH *matrix* if it satisfies the following two-dimensional maximum rendezvous diversity (2D-MRD) property:

> **The 2D-MRD property**: for any 2D-shift $0 \leq \delta, \tau \leq p-1$ and any channel $0 \leq k \leq N-1$, there exist $0 \leq i, j \leq p-1$ such that
>
> $$c_{i,j} = c_{i \oplus \delta, j \oplus \tau} = k. \tag{7}$$

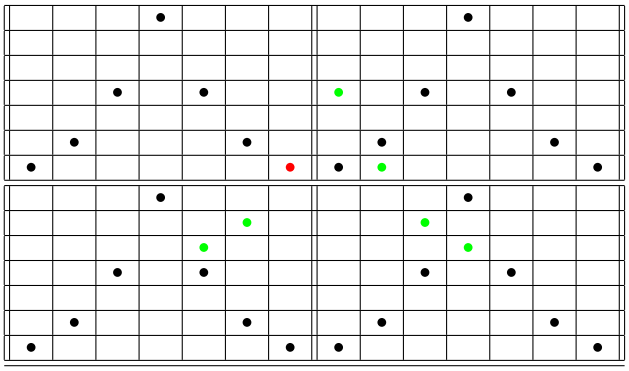
A weaker version of an (N, p)-MACH matrix is called an (N, p)-*semi*-MACH matrix, in which the 2D-MRD property may not be satisfied for $\tau = 0$.

Our construction of CH sequences, called the IDEAL-CH, is to construct an (N, p)-MACH matrix and then use that to construct an $(N, 2p^2)$-MACH sequence. In our construction, there are two elegant mathematical tools for dealing with circular shifts: (i) perfect difference sets [12] and (ii) ideal matrices [13]. Intuitively, a perfect difference set with a period p and k elements can be visualized as a dot pattern that has a dot on the 1D-coordinate of an element. Repeat the dot pattern infinitely often in the line. Then, for any time shift, exactly one pair of dots will overlap in every period of p. On the other hand, an ideal matrix can be viewed as a two-dimensional version of a perfect difference set. A $p \times p$ ideal matrix has exactly one element in each column and can be visualized as a dot pattern that has a dot on the 2D-coordinate of an element in the matrix. Repeat the dot pattern infinitely often in the plane. Then, except for purely vertical shifts, exactly one pair of dots will overlap within a $p \times p$ square box for any other two-dimensional shifts (see Table II for an illustration).

Similarly, an (N, p)-MACH sequence can be repeatedly extended to a periodic sequence in the line. For any time shift, every channel is a rendezvous channel within an interval of length p. On the other hand, an (N, p)-MACH matrix can be repeatedly extended in the plane. Then, for any two-dimensional shift, every channel is a rendezvous channel within a $p \times p$ square box.

TABLE II

A 7×7 IDEAL MATRIX IS REPEATED INFINITELY OFTEN IN THE PLANE. IT OVERLAPS WITH THE DOTS OF THE SHIFTED 7×7 IDEAL MATRIX (MARKED IN GREEN) AT EXACTLY ONE DOT PAIR (THE RED DOT). THE 2D SHIFT IS REPRESENTED BY $\delta = 3$ AND $\tau = 4$



The idea of constructing an (N, p)-MACH matrix is to *first construct a $p \times p$ ideal matrix, replace each column of the ideal matrix by a permutation to form a semi-MACH matrix, and then embed a perfect difference set in each column of that semi-MACH matrix* so that the overlaps between the constructed matrix and any two-dimensional circular shift of that matrix contain all the rendezvous channels. Specifically, we show if p is a prime and is equal to $L^2 + L + 1$ for some prime power L, our IDEAL-CH can guarantee L^2 rendezvous channels within the period $2p^2$. For IDEAL-CH, the asymptotic approximation ratio is $\frac{2(L^2+L+1)^2}{(L^2)^2}$ and it approaches 2 when $L \to \infty$.

B. Difference Sets

In this section, we briefly review the notion of difference sets.

Definition 3 (Relaxed Difference Sets (RDS)): Let $Z_p = \{0, 1, \ldots, p-1\}$. A set $D = \{a_0, a_1, \ldots, a_{k-1}\} \subset Z_p$ is called a (p, k, λ)-relaxed difference set (RDS) if for every $(\ell \bmod p) \neq 0$, there exist at least λ ordered pairs (a_i, a_j) such that $a_i - a_j = (\ell \bmod p)$, where $a_i, a_j \in D$. A $(p, k, 1)$-relaxed difference set is said to be *perfect* if there exists exactly one ordered pair (a_i, a_j) such that $a_i - a_j = (\ell \bmod p)$ for every $(\ell \bmod p) \neq 0$. In this paper, we are only interested in the case $\lambda = 1$ and we simply say a set D is an RDS (or a perfect difference set) in Z_p when $\lambda = 1$.

Clearly, if $D = \{a_0, a_1, \ldots, a_{k-1}\}$ is a perfect difference set in Z_p, then $D_\ell = \{(a_0 + \ell) \bmod p, (a_1 + \ell) \bmod p, \ldots, (a_{k-1} + \ell) \bmod p\}$, $\ell = 0, 1, 2, \ldots, p-1$, are all perfect difference sets in Z_p. Such a rotation property will be used in our embedding of perfect difference sets. An explicit construction of $(p^2+p+1, p+1, 1)$-perfect difference set was shown in [12] for any p that is a prime power. For instance, the set $D = \{0, 1, 3\}$ is a perfect difference set in Z_7. Singer's

construction [12] of $(p^2+p+1, p+1, 1)$-perfect difference set is linear in p once a *primitive polynomial of degree 3* in a Galois field $GF(p)$ is found. It is known that there exists (at least) one primitive polynomial of any degree in $GF(p)$. Since there are at most p^3 monic polynomials of degree 3 in $GF(p)$ and testing a monic polynomial of degree 3 requires at most $O(p^3)$ steps (of $GF(p)$ arithmetic operations), the time complexity of finding a primitive polynomial of degree 3 in $GF(p)$ is at most $O(p^6)$. In the literature, there are faster randomized algorithms that randomly generated a polynomial to test.

In view of the mathematical property of an RDS, a periodic CH with N rendezvous channels is equivalent to that there are N *disjoint* RDS in that periodic sequence. Such an equivalent statement was previously made in [6]. Furthermore, the Disjoint Relaxed Difference Set (DRDS) algorithm in [6] can be used for constructing a CH sequence with maximum rendezvous diversity that has a period of $3N^2$ when the number of channels N is a prime. In [43], [44], efficient algorithms were proposed to find *disjoint* $(p^2+p+1, p+1, 1)$-perfect difference sets for a prime power p. If the number of disjoint perfect difference sets that can be found for a prime power p is not less than the total number of channel N, then they can be used to construct CH sequences with maximum rendezvous diversity. However, there is no lower bound on the number of disjoint perfect difference sets that can be found for a prime power p in [43], [44].

C. Ideal Matrices

In this section, we introduce the notion of an ideal matrix in [13]. As discussed before, an ideal matrix can be viewed as a two-dimensional version of a perfect difference set.

Definition 4 (Ideal Matrix [13]): A binary $(0,1)$ $p \times p$ matrix $M = (m_{i,j})$ is called an *ideal* matrix if it satisfies the following two constraints:

(i) Each column of M contains exactly one 1, i.e., for all $j = 0, 1, 2, \ldots, p-1$,

$$\sum_{i=0}^{p-1} m_{i,j} = 1. \tag{8}$$

(ii) The doubly periodic correlation function $\rho(\cdot,\cdot)$, defined by

$$\rho(\delta, \tau) = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} m_{i\oplus\delta, j\oplus\tau} m_{i,j} \tag{9}$$

where δ, τ are integers between 0 and $p-1$ satisfies the condition

$$\rho(\delta, \tau) \le 1 \tag{10}$$

whenever either δ or τ is nonzero.

Since an ideal matrix M contains exactly p 1's, we have

$$\rho(0,0) = p. \tag{11}$$

On the other hand, we have from (8) that

$$\begin{aligned}\sum_{\delta=0}^{p-1}\sum_{\tau=0}^{p-1} \rho(\delta,\tau) &= \sum_{i=0}^{p-1}\sum_{j=0}^{p-1}\sum_{\delta=0}^{p-1}\sum_{\tau=0}^{p-1} m_{i\oplus\delta, j\oplus\tau} m_{i,j} \\ &= \sum_{j=0}^{p-1}\sum_{i=0}^{p-1} m_{i,j} \sum_{\tau=0}^{p-1}\sum_{\delta=0}^{p-1} m_{i\oplus\delta, j\oplus\tau} \\ &= p^2. \end{aligned} \tag{12}$$

Also, as each column of M contains exactly one 1, we have for $\delta = 1, 2, \ldots, p-1$,

$$\rho(\delta, 0) = 0. \tag{13}$$

It then follows from (10), (11), (12) and (13) that for $\tau \neq 0$

$$\rho(\delta, \tau) = 1. \tag{14}$$

In view of (13) and (14), one way to visualize an ideal matrix M as a dot pattern is to put a dot on the 2D-coordinate of a 1 in M. Now repeat the pattern of the matrix infinitely often in the plane. Then, the ideal matrix has the following three important properties:

(P1) (No shift) If $(\delta \mod p) = (\tau \mod p) = 0$, all dots overlap.

(P2) (Purely vertical shifts) For all the purely vertical shifts (along the columns) with $(\tau \mod p) = 0$ and $(\delta \mod p) \neq 0$, no dot will overlap.

(P3) (The other shifts) For any the other shifts, i.e., $(\tau \mod p) \neq 0$, exactly one pair of dots will overlap.

As each column of an ideal matrix contains exactly one dot, one can view the dot pattern from an ideal matrix as a "graph" of a function $f(\cdot)$ with both its domain and range being the set of integers $\{0, 1, \ldots, p-1\}$. The function $f(\cdot)$ can be characterized as follows:

$$f(j) = p - 1 - i, \tag{15}$$

where i is uniquely determined by the condition $m_{i,j} = 1$. With such a functional characterization, a $p \times p$ ideal matrix M can be constructed when p is a prime.

Theorem 5 (The Elliot-Butson Construction [45]): If p is a prime and

$$f(j) = ((c_2 j^2 + c_1 j + c_0) \mod p), \tag{16}$$

with $c_2 \neq 0$, then the $p \times p$ matrix $M = (m_{i,j})$ with

$$m_{i,j} = \begin{cases} 1, & \text{if } p-1-i = f(j), \\ 0, & \text{otherwise}, \end{cases} \tag{17}$$

is an ideal matrix.

To see the insight of the Elliot-Butson construction, we note that i is uniquely determined by j from (17). Thus, there is exactly one 1 in each column and (8) is satisfied. To show (14), it suffices to show that for any $\tau \neq 0$ and δ there exists a unique j such that $m_{i,j} = m_{i\oplus\delta, j\oplus\tau} = 1$. It follows from (16) and (17) that

$$((c_2\ j^2 + c_1\ j + c_0) \mod p) = p - 1 - i$$

and

$$((c_2(j+\tau)^2 + c_1(j+\tau) + c_0) \mod p) = ((p-1-i-\delta) \mod p).$$

Solving from these two equations yields

$$(2c_2\tau j \mod p) = ((-c_2\tau^2 - c_1\tau - \delta) \mod p). \quad (18)$$

Since $c_2 \neq 0$, $\tau \neq 0$ and p is a prime, there is a unique j satisfying (18).

One special case of the Elliot-Butson construction is to choose

$$f(j) = \frac{j(j+1)}{2} \quad (19)$$

and this construction is exactly the set of the triangular numbers used in the constructions of the jump columns in CRSEQ [8] and T-CH [10]. Another example is to choose

$$f(j) = \frac{j(3j-1)}{2} \quad (20)$$

and this construction is exactly the set of the Euler pentagonal numbers used in the constructions of the jump columns in DSCR [11].

D. From an Ideal Matrix to a Semi-MACH Matrix

To construct a semi-MACH matrix from an ideal matrix, the idea is to replace each column of an ideal matrix by a permutation of $(0, 1, 2 \ldots, p-1)$. Specifically, define the i^{th}-rotation to be the permutation $(i, i \oplus 1, \ldots, i \oplus (p-1))$. Construct a $p \times p$ matrix $\tilde{M} = (\tilde{m}_{i,j})$ by replacing the j^{th} column of a $p \times p$ ideal matrix $M = (m_{i,j})$ by the $(p-i)^{th}$-rotation if $m_{i,j} = 1$. By doing so, every dot in the ideal matrix is mapped to channel 0 (that serves as an anchor) and every other channel simply rotates around channel 0 in a column. In the following, we show the conversion for the 7×7 ideal matrix:

$$\begin{bmatrix} 0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&1&0&1&0&0\\ 0&0&0&0&0&0&0\\ 0&1&0&0&0&1&0\\ 1&0&0&0&0&0&1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1&2&4&0&4&2&1\\ 2&3&5&1&5&3&2\\ 3&4&6&2&6&4&3\\ 4&5&0&3&0&5&4\\ 5&6&1&4&1&6&5\\ 6&0&2&5&2&0&6\\ 0&1&3&6&3&1&0 \end{bmatrix}$$

One immediate consequence of such a conversion is when one pair of dots overlap, the p channels in that column also overlap. In view of the three properties of an ideal matrix, the matrix $\tilde{M}$ is a (p,p)-semi-MACH matrix that satisfies the 2D-MRD property except for purely vertical shifts, i.e., $\tau = 0$ in (7).

E. From a Semi-MACH Matrix to an MACH Matrix

To deal with the problem of purely vertical shifts, the idea of T-CH in [10] is to concatenate a $p \times p$ "stay" matrix (with all the p elements in the k^{th} column being k, $k = 0, 1, 2, \ldots, p-1$) and a $p \times (p + \lfloor p/2 \rfloor)$ "jump" matrix with the j^{th} column taken from the $(j \mod p)^{th}$ column of a semi-MACH matrix. This results in a $p \times (2p + \lfloor p/2 \rfloor)$ matrix and thus has a period of $p(2p + \lfloor p/2 \rfloor)$. The construction of T-CH shortens the number of "jump" columns in CRSEQ [8] from $2p-1$ to $p + \lfloor p/2 \rfloor$. It seems that DSCR [11] is somehow equivalent to T-CH. They both are constructed by concatenating a $p \times p$ "stay" matrix and a $p \times (p + \lfloor p/2 \rfloor)$ "jump" matrix with the j^{th} column taken from the $(j \mod p)^{th}$ column of a semi-MACH matrix. The only difference is that they use different quadratic functions in the Elliot-Butson construction for ideal matrices.

Our idea to tackle the problem of purely vertical shifts is to *reserve some channels of the p channels for embedding relaxed difference sets (RDS)* that can guarantee the needed overlaps for purely vertical shifts.

Now we show how to construct an (L^2, p)-MACH matrix from a (p,p)-semi-MACH matrix when p is a prime and p is equal to $L^2 + L + 1$ for some prime power L. The detailed steps are outlined in Algorithm 1. Let $D = \{a_0, a_1, \ldots, a_L\}$ be an $(L^2 + L + 1, L + 1, 1)$-perfect difference set and $\tilde{M} = (\tilde{m}_{i,j})$ be a (p,p)-semi-MACH matrix. Let $D^c = Z_p \backslash D = \{b_0, b_1, \ldots, b_{L^2-1}\}$. The idea is to reserve the $L+1$ channels in D for the perfect difference sets and only use the L^2 channels in D^c. The $L+1$ channels in D in the j^{th} column of $\tilde{M}$ are replaced by channel $(j \mod L^2)$ and the other L^2 channels are re-mapped to the L^2 channels in $\{0, 1, 2, \ldots, L^2 - 1\}$. Specifically, we construct a $p \times p$ matrix $C = (c_{i,j})$ by the following rule:

$$c_{i,j} = \begin{cases} (j \mod L^2) & \text{if } \tilde{m}_{i,j} \in D \\ \ell & \text{if } \tilde{m}_{i,j} = b_\ell. \end{cases} \quad (21)$$

For example, the matrix C mapped from the $(7,7)$-semi-MACH matrix and the perfect difference set $D = \{0, 1, 3\}$ is shown as follows:

$$\begin{bmatrix} 1&2&4&0&4&2&1\\ 2&3&5&1&5&3&2\\ 3&4&6&2&6&4&3\\ 4&5&0&3&0&5&4\\ 5&6&1&4&1&6&5\\ 6&0&2&5&2&0&6\\ 0&1&3&6&3&1&0 \end{bmatrix} \Rightarrow \begin{bmatrix} \mathbf{0}&0&1&\underline{\mathbf{3}}&1&0&\mathbf{2}\\ 0&\mathbf{1}&2&\mathbf{3}&2&\mathbf{1}&0\\ \mathbf{0}&1&3&0&3&1&\mathbf{2}\\ 1&2&\underline{\mathbf{2}}&\mathbf{3}&\underline{\mathbf{0}}&2&1\\ 2&3&\mathbf{2}&1&\mathbf{0}&3&2\\ 3&\underline{\mathbf{1}}&0&2&0&\underline{\mathbf{1}}&3\\ \underline{\mathbf{0}}&\mathbf{1}&\mathbf{2}&3&\mathbf{0}&\mathbf{1}&\underline{\mathbf{2}} \end{bmatrix} \quad (22)$$

In this example, the three numbers $0, 1, 3$ in D of the j^{th} column are mapped to $(j \mod 4)$ for $j = 0, 1, \ldots, 6$. Moreover, $D^c = \{2, 4, 5, 6\}$ and these four numbers in the $(7,7)$-semi-MACH matrix are re-mapped to $\{0, 1, 2, 3\}$, i.e.,

$$2 \mapsto 0,\ 4 \mapsto 1,\ 5 \mapsto 2,\ 6 \mapsto 3.$$

In (22), we mark the channels that are used for the perfect difference sets in boldface. From the (rotation) property of the perfect difference set, we know for any purely vertical shift, there is an overlap of channel j in column j, $j = 0, 1, \ldots, L^2 - 1$. Also, those *underlined* numbers are the dots of the $p \times p$ ideal matrix. These are used as "anchors" for any other shifts.

Algorithm 1 Construction of an (L^2, p)-MACH Matrix

Input A set of L^2 channels $\{0, 1, 2, \ldots, L^2-1\}$ with L being a prime power and L^2+L+1 being a prime.
Output An (L^2, p)-MACH matrix $C = (c_{i,j})$ with $p = L^2 + L + 1$.
1: Let $p = L^2 + L + 1$ and construct a $p \times p$ ideal matrix $M = (m_{i,j})$.
2: Construct a (p, p)-semi-MACH matrix $\tilde{M} = (\tilde{m}_{i,j})$ by replacing the j^{th} column of M by the $(p-i)^{th}$-rotation of $(0, 1, \ldots, p-1)$ (for all $j = 0, 1, \ldots, p-1$) if $m_{i,j} = 1$.
3: Construct a perfect difference set $D = \{a_0, a_1, \ldots, a_L\}$ in Z_p.
4: Let $D^c = Z_p \backslash D = \{b_0, b_1, \ldots, b_{L^2-1}\}$.
5: Construct an (L^2, p)-MACH matrix $C = (c_{i,j})$ by the channel mapping rule in (21).

Theorem 6: If L is a prime power and L^2+L+1 is a prime, then Algorithm 1 constructs an (L^2, p)-MACH matrix with $p = L^2 + L + 1$.

Proof: It suffices to prove the 2D-MRD property. Consider the matrix C from Algorithm 1 and the matrix $C' = (c'_{i,j})$ with $c'_{i,j} = c_{i\oplus\delta, j\oplus\tau}$. When $\delta = \tau = 0$, the two matrices overlap with each other. For $\delta \neq 0$, we consider the following two cases:

Case 1($\tau = 0$): This corresponds to a purely vertical shift. Since we embed a perfect difference set D in the j^{th} column of C, the 2D-MRD property is satisfied for channel j in the j^{th} columns of these two matrices, $j = 0, 1, \ldots, L^2-1$.

Case 2 ($\tau \neq 0$): This corresponds to a shift that is not a purely vertical shift. From (P3) of an ideal matrix, there is a column j_1 of matrix C that overlaps with a column j_2 of matrix C'. From the deterministic re-mapping in (21), the 2D-MRD property is satisfied for all the L^2 channels in the overlapped column. ■

F. From an MACH Matrix to an MACH Sequence

In this section, we show that one can construct an $(N, 2p^2)$-MACH sequence from an (N, p)-MACH matrix. The idea to take an (N, p)-MACH matrix $C = (c_{i,j})$ and concatenate two of them to form a $p \times 2p$ matrix

$$\tilde{C} = (\tilde{c}_{i,j}) = (C|C).$$

By doing so, we have $\tilde{c}_{i,j} = c_{i,(j \mod p)}$ for all $i = 0, 1, \ldots, p-1$ and $j = 0, 1, \ldots, 2p-1$. As the matrix-based construction of CH sequences for T-CH in [10], we then map the matrix $\tilde{C} = (\tilde{c}_{i,j})$ to the CH sequence $\{c(t), t = 0, 1, \ldots, 2p^2-1\}$ by letting $c(t) = \tilde{c}_{i,j}$ with $i = \lfloor t/(2p) \rfloor$ and $j = (t \mod (2p))$. Since $\tilde{c}_{i,j} = c_{i,(j \mod p)}$, this is equivalent to letting $c(t) = c_{i,j}$ with $i = \lfloor t/(2p) \rfloor$ and $j = (t \mod p)$.

For example, concatenating two of the $(4, 7)$-MACH matrix in (22) yields the following 7×14 matrix:

$$\left[\begin{array}{ccccccc|ccccccc}
\mathbf{0} & 0 & 1 & \underline{\mathbf{3}} & 1 & 0 & \mathbf{2} & \mathbf{0} & 0 & 1 & \underline{\mathbf{3}} & 1 & 0 & \mathbf{2} \\
0 & \mathbf{1} & 2 & \mathbf{3} & 2 & \mathbf{1} & 0 & 0 & \mathbf{1} & 2 & \mathbf{3} & 2 & \mathbf{1} & 0 \\
\mathbf{0} & 1 & 3 & 0 & 3 & 1 & \mathbf{2} & \mathbf{0} & 1 & 3 & 0 & 3 & 1 & \mathbf{2} \\
1 & 2 & \underline{\mathbf{2}} & \mathbf{3} & \underline{\mathbf{0}} & 2 & 1 & 1 & 2 & \underline{\mathbf{2}} & \mathbf{3} & \underline{\mathbf{0}} & 2 & 1 \\
2 & 3 & \mathbf{2} & 1 & \mathbf{0} & 3 & 2 & 2 & 3 & \mathbf{2} & 1 & \mathbf{0} & 3 & 2 \\
3 & \underline{\mathbf{1}} & 0 & 2 & 0 & \underline{\mathbf{1}} & 3 & 3 & \underline{\mathbf{1}} & 0 & 2 & 0 & \underline{\mathbf{1}} & 3 \\
\underline{\mathbf{0}} & \mathbf{1} & \mathbf{2} & 3 & \mathbf{0} & \mathbf{1} & \underline{\mathbf{2}} & \underline{\mathbf{0}} & \mathbf{1} & \mathbf{2} & 3 & \mathbf{0} & \mathbf{1} & \underline{\mathbf{2}}
\end{array}\right]. \tag{23}$$

Now the constructed CH sequence with length 98 is then

$$0, 0, 1, 3, 1, 0, 2, 0, 0, 1, 3, 1, 0, 2, 0, 1, 2, 3, 2, 1, 0,$$
$$0, 1, 2, 3, 2, 1, 0, 0, 1, 3, 0, 3, 1, 2, 0, 1, 3, 0, 3, 1, 2,$$
$$\ldots$$
$$3, 1, 0, 2, 0, 1, 3, 0, 1, 2, 3, 0, 1, 2, 0, 1, 2, 3, 0, 1, 2.$$

Theorem 7: Suppose that the matrix $C = (c_{i,j})$ with $i, j = 0, 1, \ldots, p-1$ is an (N, p)-MACH matrix. Construct the sequence $\{c(t), 0 \leq t \leq 2p^2-1\}$ by letting $c(t) = c_{i,j}$ with $i = \lfloor t/(2p) \rfloor$ and $j = (t \mod p)$. Then, the sequence $\{c(t), 0 \leq t \leq 2p^2-1\}$ is an $(N, 2p^2)$-MACH sequence.

Proof: It suffices to prove the 1D-MRD property for the sequence $\{c(t), 0 \leq t \leq 2p^2-1\}$, i.e., for any time shift $0 \leq d \leq 2p^2-1$ and any channel $0 \leq k \leq N-1$, there exists $0 \leq t \leq 2p^2-1$ such that

$$c(t) = c((t+d) \mod (2p^2)) = k. \tag{24}$$

Let $\delta = \lfloor d/(2p) \rfloor$ be the vertical shift and $\tau = (d \mod (2p))$ and be the horizontal shift. From the matrix-based construction of the CH sequence $\{c(t), 0 \leq t \leq 2p^2-1\}$, we can represent such a sequence by the $p \times 2p$ matrix $\tilde{C} = (C|C)$. Similarly, we can also represent the sequence $\{c((t+d) \mod (2p^2)), 0 \leq t \leq 2p^2-1\}$ by a $p \times 2p$ matrix $(C_1|C_2)$ for some $p \times p$ matrices C_1 and C_2. In view of the 2D-MRD property of the matrix $C = (c_{i,j})$, it suffices to show that either C_1 or C_2 is a $p \times p$ square box in the plane repeated from C.

Consider the following two cases:

Case 1 ($0 \leq \tau \leq p$): In this case, the horizontal shift τ is not greater than p. Thus, the first matrix C_1 is a $p \times p$ square box in the plane repeated from the matrix C. The 2D-MRD property of the matrix $C = (c_{i,j})$ then guarantees the 1D-MRD property of the sequence $\{c((t+d) \mod (2p^2)), 0 \leq t \leq 2p^2-1\}$. For example, for the CH sequence in (23), the sequence $\{c((t+d) \mod 98), 0 \leq t \leq 97\}$ in this case can be represented by the matrix C_1 marked in *red* and the matrix

C_2 marked in *blue*.

$$\left[\begin{array}{ccccccc|ccccccc}
\mathbf{0} & 0 & 1 & \underline{\mathbf{3}} & 1 & 0 & \mathbf{2} & \mathbf{0} & 0 & 1 & \underline{\mathbf{3}} & 1 & 0 & \mathbf{2} \\
0 & \mathbf{1} & 2 & \mathbf{3} & 2 & \mathbf{1} & 0 & 0 & \mathbf{1} & 2 & \mathbf{3} & 2 & \mathbf{1} & 0 \\
\mathbf{0} & 1 & 3 & 0 & 3 & 1 & \mathbf{2} & \mathbf{0} & 1 & 3 & 0 & 3 & 1 & \mathbf{2} \\
1 & 2 & \underline{\mathbf{2}} & \mathbf{3} & \underline{\mathbf{0}} & 2 & 1 & 1 & 2 & \underline{\mathbf{2}} & \mathbf{3} & \underline{\mathbf{0}} & 2 & 1 \\
2 & 3 & \mathbf{2} & 1 & \mathbf{0} & 3 & 2 & 2 & 3 & \mathbf{2} & 1 & \mathbf{0} & 3 & 2 \\
3 & \underline{\mathbf{1}} & 0 & 2 & 0 & \underline{\mathbf{1}} & 3 & 3 & \underline{\mathbf{1}} & 0 & 2 & 0 & \underline{\mathbf{1}} & 3 \\
\underline{\mathbf{0}} & \mathbf{1} & \mathbf{2} & 3 & \mathbf{0} & \mathbf{1} & \underline{\mathbf{2}} & \underline{\mathbf{0}} & \mathbf{1} & \mathbf{2} & 3 & \mathbf{0} & \mathbf{1} & \underline{\mathbf{2}} \\
\mathbf{0} & 0 & 1 & \underline{\mathbf{3}} & 1 & 0 & \mathbf{2} & \mathbf{0} & 0 & 1 & \underline{\mathbf{3}} & 1 & 0 & \mathbf{2} \\
0 & \mathbf{1} & 2 & \mathbf{3} & 2 & \mathbf{1} & 0 & 0 & \mathbf{1} & 2 & \mathbf{3} & 2 & \mathbf{1} & 0 \\
\mathbf{0} & 1 & 3 & 0 & 3 & 1 & \mathbf{2} & \mathbf{0} & 1 & 3 & 0 & 3 & 1 & \mathbf{2} \\
1 & 2 & \underline{\mathbf{2}} & \mathbf{3} & \underline{\mathbf{0}} & 2 & 1 & 1 & 2 & \underline{\mathbf{2}} & \mathbf{3} & \underline{\mathbf{0}} & 2 & 1 \\
2 & 3 & \mathbf{2} & 1 & \mathbf{0} & 3 & 2 & 2 & 3 & \mathbf{2} & 1 & \mathbf{0} & 3 & 2 \\
3 & \underline{\mathbf{1}} & 0 & 2 & 0 & \underline{\mathbf{1}} & 3 & 3 & \underline{\mathbf{1}} & 0 & 2 & 0 & \underline{\mathbf{1}} & 3 \\
\underline{\mathbf{0}} & \mathbf{1} & \mathbf{2} & 3 & \mathbf{0} & \mathbf{1} & \underline{\mathbf{2}} & \underline{\mathbf{0}} & \mathbf{1} & \mathbf{2} & 3 & \mathbf{0} & \mathbf{1} & \underline{\mathbf{2}}
\end{array}\right]$$

Case 2 ($p < \tau \leq 2p-1$): In this case, the horizontal shift τ is larger than p. Thus, the second matrix C_2 is a $p \times p$ square box in the plane repeated from the matrix C. The 2D-MRD property of the matrix $C = (c_{i,j})$ then guarantees the 1D-MRD property of the sequence $\{c((t+d) \mod (2p^2)), 0 \leq t \leq 2p^2-1\}$. For example, for the CH sequence in (23), the sequence $\{c((t+d) \mod 98), 0 \leq t \leq 97\}$ in this case can be represented by the matrix C_1 marked in *red* and the matrix C_2 marked in *blue*.

$$\left[\begin{array}{ccccccc|ccccccc}
\mathbf{0} & 0 & 1 & \underline{\mathbf{3}} & 1 & 0 & \mathbf{2} & \mathbf{0} & 0 & 1 & \underline{\mathbf{3}} & 1 & 0 & \mathbf{2} \\
0 & \mathbf{1} & 2 & \mathbf{3} & 2 & \mathbf{1} & 0 & 0 & \mathbf{1} & 2 & \mathbf{3} & 2 & \mathbf{1} & 0 \\
\mathbf{0} & 1 & 3 & 0 & 3 & 1 & \mathbf{2} & \mathbf{0} & 1 & 3 & 0 & 3 & 1 & \mathbf{2} \\
1 & 2 & \underline{\mathbf{2}} & \mathbf{3} & \underline{\mathbf{0}} & 2 & 1 & 1 & 2 & \underline{\mathbf{2}} & \mathbf{3} & \underline{\mathbf{0}} & 2 & 1 \\
2 & 3 & \mathbf{2} & 1 & \mathbf{0} & 3 & 2 & 2 & 3 & \mathbf{2} & 1 & \mathbf{0} & 3 & 2 \\
3 & \underline{\mathbf{1}} & 0 & 2 & 0 & \underline{\mathbf{1}} & 3 & 3 & \underline{\mathbf{1}} & 0 & 2 & 0 & \underline{\mathbf{1}} & 3 \\
\underline{\mathbf{0}} & \mathbf{1} & \mathbf{2} & 3 & \mathbf{0} & \mathbf{1} & \underline{\mathbf{2}} & \underline{\mathbf{0}} & \mathbf{1} & \mathbf{2} & 3 & \mathbf{0} & \mathbf{1} & \underline{\mathbf{2}} \\
\mathbf{0} & 0 & 1 & \underline{\mathbf{3}} & 1 & 0 & \mathbf{2} & \mathbf{0} & 0 & 1 & \underline{\mathbf{3}} & 1 & 0 & \mathbf{2} \\
0 & \mathbf{1} & 2 & \mathbf{3} & 2 & \mathbf{1} & 0 & 0 & \mathbf{1} & 2 & \mathbf{3} & 2 & \mathbf{1} & 0 \\
\mathbf{0} & 1 & 3 & 0 & 3 & 1 & \mathbf{2} & \mathbf{0} & 1 & 3 & 0 & 3 & 1 & \mathbf{2} \\
1 & 2 & \underline{\mathbf{2}} & \mathbf{3} & \underline{\mathbf{0}} & 2 & 1 & 1 & 2 & \underline{\mathbf{2}} & \mathbf{3} & \underline{\mathbf{0}} & 2 & 1 \\
2 & 3 & \mathbf{2} & 1 & \mathbf{0} & 3 & 2 & 2 & 3 & \mathbf{2} & 1 & \mathbf{0} & 3 & 2 \\
3 & \underline{\mathbf{1}} & 0 & 2 & 0 & \underline{\mathbf{1}} & 3 & 3 & \underline{\mathbf{1}} & 0 & 2 & 0 & \underline{\mathbf{1}} & 3 \\
\underline{\mathbf{0}} & \mathbf{1} & \mathbf{2} & 3 & \mathbf{0} & \mathbf{1} & \underline{\mathbf{2}} & \underline{\mathbf{0}} & \mathbf{1} & \mathbf{2} & 3 & \mathbf{0} & \mathbf{1} & \underline{\mathbf{2}}
\end{array}\right]$$

■

With Theorem 7, we propose the construction of the IDEAL-CH in Algorithm 2.

Algorithm 2 The IDEAL-CH

Input A set of L^2 channels $\{0, 1, 2, \ldots, L^2-1\}$ with L being a prime power and L^2+L+1 being a prime.
Output A CH sequence $\{c(t), t = 0, 1, 2 \ldots, 2(L^2+L+1)^2-1\}$ with $c(t) \in \{0, 1, 2, \ldots, L^2-1\}$.
1: Use Algorithm 1 to construct an (L^2, p)-MACH matrix with $p = L^2+L+1$.
2: For $t = 0, 1, 2 \ldots, 2(L^2+L+1)^2-1$, let $c(t) = c_{i,j}$ with $i = \lfloor t/(2p) \rfloor$ and $j = (t \mod p)$.

As a direct consequence of Theorem 6 and Theorem 7, we have the following corollary.

Corollary 8: If L is a prime power and L^2+L+1 is a prime, then Algorithm 2 constructs a CH sequence with period $2(L^2+L+1)^2$ that achieves maximum rendezvous diversity for the L^2 channels $\{0, 1, 2, \ldots, L^2-1\}$.

G. The General Construction of an (N, p)-MACH Matrix

By using a computer search for the set of numbers L with L being a prime power and L^2+L+1 being a prime, we find $\{2, 3, 5, 8, 17, 27, 41, 59, 71, 89\}$ for $L \leq 100$. There are 4,688 positive integers with such properties under 100,000. For the integers that do not possess such properties, we have to resort to less efficient constructions. Instead of using a perfect difference set in Step 3 of Algorithm 1, we can use an RDS. It was shown in [46] that the size of an RDS in Z_p is bounded below by $\sqrt{p}$. Here we show how to construct an RDS D in Z_p with the size smaller than $2\sqrt{p}$.

To construct an RDS in Z_p for any period p, the idea is first to place a periodic dot pattern with the period Δ in the interval $[0, p-1]$, and then add Δ dots in the interval $[0, \Delta-1]$ as the "delimiter." As there is at least one dot within an interval of length Δ, the Δ dots that serve as the delimiter will overlap with at least one dot in any time-shifted dot pattern. This is stated in the following proposition.

Proposition 9: For any $\Delta \geq 2$ and $p \geq \Delta$, the set $D = \{0, 1, \ldots, \Delta-1\} \cup \{2\Delta-1, 3\Delta-1, \ldots, \lfloor p/\Delta \rfloor \Delta - 1\}$ is an RDS in Z_p.

Such a construction of an RDS can be characterized with two parameters: the period p and the spacing Δ. For example, if we choose $\Delta = 5$ for $p = 23$, then $D = \{0, 1, 2, 3, 4, 9, 14, 19\}$ is an RDS in Z_{23} with 8 elements. Note that the number of elements in D in Proposition 9 is $\Delta + \lfloor p/\Delta \rfloor - 1$. To minimize the number of elements in D in Proposition 9, one may choose the spacing $\Delta = \lceil \sqrt{p} \rceil$. Since $x \leq \lceil x \rceil < x+1$ and $\lfloor x \rfloor \leq x$, we have

$$\lceil \sqrt{p} \rceil + \lfloor p/\lceil \sqrt{p} \rceil \rfloor - 1 < 2\sqrt{p}. \tag{25}$$

Thus, one can construct an RDS in Z_p with the size smaller than $2\sqrt{p}$.

Instead of using a perfect difference set in Step 3 in Algorithm 1, now we can replace it by using an RDS in Z_p with the spacing $\Delta = \lceil \sqrt{p} \rceil$ in Proposition 9. This leads to the general construction of an (N, p)-MACH matrix in Algorithm 3.

Even though there is a constraint for $p - (\lceil \sqrt{p} \rceil + \lfloor p/\lceil \sqrt{p} \rceil \rfloor - 1) \geq N$ in Algorithm 3, such a constraint does not affect the asymptotic ratio (in the limiting regime). This is shown in the following corollary.

Corollary 10: The $(N, 2p^2)$-MACH sequence constructed by the general construction of an (N, p)-MACH matrix in Algorithm 3 and Theorem 7 has the asymptotic ratio of 2.

Proof: Let D be the RDS constructed in Proposition 9 with the spacing $\Delta = \lceil \sqrt{p} \rceil$. Since $|D| \leq 2\sqrt{p}$, the number of rendezvous channels $|D^c| = p - |D| \geq p - 2\sqrt{p}$. Thus, the asymptotic approximation ratio is

$$\frac{2p^2}{|D^c|^2} = \frac{2p^2}{(p-|D|)^2} \to 2, \tag{26}$$

when $p \to \infty$.

Now, we show the constraint $p - (\lceil \sqrt{p} \rceil + \lfloor p/\lceil \sqrt{p} \rceil \rfloor - 1) \geq N$ does not affect the asymptotic ratio. Note that Theorem 1

Algorithm 3 The General Construction of an (N,p)-MACH Matrix

Input: A set of N channels $\{0,1,2,\ldots,N-1\}$.
Output: An (N,p)-MACH matrix with p being the smallest prime such that $p-(\lceil\sqrt{p}\rceil+\lfloor p/\lceil\sqrt{p}\rceil\rfloor-1)\geq N$.
1: Find the smallest prime p such that $p-(\lceil\sqrt{p}\rceil+\lfloor p/\lceil\sqrt{p}\rceil\rfloor-1)\geq N$ and construct a $p\times p$ ideal matrix $M=(m_{i,j})$.
2: Construct a (p,p)-semi-MACH matrix $\tilde{M}=(\tilde{m}_{i,j})$ by replacing the j^{th} column of M by the $(p-i)^{th}$-rotation of $(0,1,\ldots,p-1)$ (for all $j=0,1,\ldots,p-1$) if $m_{i,j}=1$.
3: Let $\Delta=\lceil\sqrt{p}\rceil$. Construct an RDS $D=\{0,1,\ldots,\Delta-1\}\cup\{2\Delta-1,3\Delta-1,\ldots,\lfloor p/\Delta\rfloor\Delta-1\}$ in Z_p.
4: Let $D^c=Z_p\backslash D=\{b_0,b_1,\ldots,b_{p-1-|D|}\}$.
5: Construct a $p\times p$ matrix $C=(c_{i,j})$ by the following channel mapping rule:

$$c_{i,j}=\begin{cases}(j \mod N) & \text{if } \tilde{m}_{i,j}\in D\\ (\ell \mod N) & \text{if } \tilde{m}_{i,j}=b_\ell.\end{cases}$$

of [47] states that there exists a prime number p in the interval $[N,N+N^{0.525}]$ for sufficiently large N's. This theorem implies for any arbitrary $\epsilon\in(0,1)$ and for all $N>N_0$ (a sufficiently large integer), there exists a prime p_N with

$$(1+\epsilon)N\leq p_N\leq(1+2\epsilon)N. \tag{27}$$

Let $N_0'=12/\epsilon^2$. From (25) and (27), we have for all $N>\max\{N_0,N_0'\}$,

$$\begin{aligned}&p_N-(\lceil\sqrt{p_N}\rceil+\lfloor p_N/\lceil\sqrt{p_N}\rceil\rfloor-1)\\&\quad\geq p_N-2\sqrt{p_N}\\&\quad\geq(1+\epsilon)N-2\sqrt{(1+2\epsilon)N}\\&\quad=N+(\epsilon N-2\sqrt{(1+2\epsilon)N})\\&\quad\geq N+(\epsilon N-2\sqrt{3N})\geq N.\end{aligned} \tag{28}$$

Letting $N\to\infty$, we have from (27) that

$$1+\epsilon\leq\lim_{N\to\infty}\frac{p_N}{N}\leq 1+2\epsilon.$$

Since ϵ is arbitrary, letting $\epsilon\to 0$ completes the argument. ■

Regarding the computational complexity of Algorithm 3, it is clear that Step 2 to Step 5 is $O(p^2)$. Since the smallest prime p with $p-(\lceil\sqrt{p}\rceil+\lfloor p/\lceil\sqrt{p}\rceil\rfloor-1)\geq N$ is smaller than $N+N^{0.525}$ for N sufficiently large, the time complexity of Algorithm 3 is still $O(N^2)$.

The asymptotic ratio of 2 guarantees that one can construct a CH sequence with a period $2[(1+2\epsilon)N]^2$ for any arbitrarily small ϵ and any sufficiently large N, and the MCTTR is bounded by that period. As such, our result has the best MCTTR bound among all the existing CH sequences when N is sufficiently large. However, for a small number N, there is no guarantee that our CH sequence outperforms other existing CH sequences in terms of MCTTR.

IV. ORTHO-CH

To use the IDEAL-CH in the sym/async/hetero/global MRP, each user can simply replace at random those channels not in its available channel set by some channels in its available channel set. By doing so, the two users are still guaranteed to rendezvous on *every* commonly available channel in the period of the IDEAL-CH sequence. Thus, the MCTTR is bounded by the period of the IDEAL-CH sequence.

In this section, we consider a weaker requirement that only needs the two users to rendezvous on *one* commonly available channel in a period. For this, we propose a channel hopping sequence, called ORTHO-CH, that can guarantee the rendezvous of the two users within a period of the ORTHO-CH sequence. When the available channel set of a user is a subset of $\{0,1,\ldots,N-1\}$, the period of our ORTHO-CH sequence is $(2p+1)p$, where p is the smallest prime not less than N. Thus, ORTHO-CH has the MTTR bound $(2p+1)p$.

A. Orthogonal MACH Matrices

For the construction of the ORTHO-CH sequence, we introduce a new notion of *orthogonal MACH matrices*.

Definition 11: A set of $p\times p$ matrices $\{C^{(r)}=(c_{i,j}^{(r)}),r=1,2,\ldots,K\}$ is called a set of *orthogonal* (N,p)-MACH *matrices* if it satisfies the following two properties:

(i) **The cover property**: for any channel $0\leq k\leq N-1$, it appears at least once in every column of every matrix in the set of matrices.

(ii) **The 2D-MRD property**: for any two different matrices r_1 and r_2, any 2D-shift $0\leq\delta,\tau\leq p-1$, and any channel $0\leq k\leq N-1$, there exist $0\leq i,j\leq p-1$ such that

$$c_{i,j}^{(r_1)}=c_{i\oplus\delta,j\oplus\tau}^{(r_2)}=k. \tag{29}$$

We note that the cover property is not needed in Definition 2 for an (N,p)-MACH matrix even though such a property is satisfied in our constructions of the (N,p)-MACH matrices in Algorithm 1 and Algorithm 3. Intuitively, one can view an (N,p)-MACH matrix as a matrix that is "orthogonal" to itself in the sense of the 2D-MRD property.

We choose the phrase "orthogonal" from the notion of orthogonal Latin squares [48]. In a $p\times p$ Latin square, every row and every column is a permutation of $\{0,1,\ldots,p-1\}$. Two $p\times p$ Latin squares $C^{(r_1)}=(c_{i,j}^{(r_1)})$ and $C^{(r_2)}=(c_{i,j}^{(r_2)})$ are said to be orthogonal if the p^2 ordered pairs $(c_{i,j}^{(r_1)},c_{i,j}^{(r_2)})$, $i,j=0,1,\ldots,p-1$ are all different. The number of mutually orthogonal $p\times p$ Latin squares is bounded by $p-1$ and it is achieved when p is a prime power. In particular, when p is a prime, the $p-1$ orthogonal Latin squares can be constructed by letting $c_{i,j}^{(r)}=(r\cdot i+j) \mod p$, $r=1,2,\ldots,p-1$. In the following theorem, we show such a construction also leads to a set of $p-1$ orthogonal (p,p)-MACH matrices.

Theorem 12: Suppose that p is a prime. For $r=1,2,\ldots,p-1$, $0\leq i,j\leq p-1$, let

$$c_{i,j}^{(r)}=(r\cdot i+j) \mod p. \tag{30}$$

Then, the set of matrices $\{C^{(r)}=(c_{i,j}^{(r)}),r=1,2,\ldots,p-1\}$ is a set of orthogonal (p,p)-MACH matrices.

Proof: As $r\neq 0$, we have from (30), every channel $0\leq k\leq p-1$ appears exactly once in every column of every matrix

in the set, and thus the cover property is satisfied. To show the 2D-MRD property, for $r_1 \neq r_2$, any 2D-shift $0 \leq \delta, \tau \leq p-1$ and any channel $0 \leq k \leq N-1$, we let i^* be the unique solution of the following equation:

$$((r_1 - r_2) \cdot i \mod p) = ((r_2 \cdot \delta + \tau) \mod p), \quad (31)$$

and

$$j^* = ((k - r_1 \cdot i^*) \mod p). \quad (32)$$

Then, we have from (32) and (30) that

$$c^{(r_1)}_{i^*,j^*} = k.$$

Also, it is easy to see from (30) and (31) that

$$\begin{aligned} c^{(r_2)}_{i^* \oplus \delta, j^* \oplus \tau} &= c^{(r_2)}_{(i^*+\delta) \mod p, (j^*+\tau) \mod p} \\ &= (r_2 \cdot (i^* + \delta) + (j^* + \tau)) \mod p \\ &= (r_2 \cdot i^* + (r_2 \cdot \delta + \tau) + j^*) \mod p \\ &= (r_1 \cdot i^* + j^*) \mod p \\ &= c^{(r_1)}_{i^*,j^*}. \end{aligned}$$

■

For $p = 5$, the four $(5,5)$-MACH matrices are as follows:

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{bmatrix}, \quad (33)$$

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{bmatrix}. \quad (34)$$

These four matrices are also mutually orthogonal Latin squares.

B. From Orthogonal MACH Matrices to Asynchronous CH Sequences

In this section, we show that one can construct the ORTHO-CH sequence from a set of orthogonal (p,p)-MACH matrices, $\{C^{(r)}, r = 1, 2, \ldots, p-1\}$. The idea is quite similar to the quasi-random algorithm in [40]. Each user selects a nonzero channel r from its available channel set as its ID channel. Then, construct the $p \times (2p+1)$ matrix $\tilde{C}^{(r)}$ by concatenating the ID column $\mathbf{r}$ (that stays on channel r) and two identical matrices of $C^{(r)}$, i.e.,

$$\tilde{C}^{(r)} = (\tilde{c}^{(r)}_{i,j}) = (\mathbf{r}|C^{(r)}|C^{(r)}). \quad (35)$$

As in the matrix-based construction for IDEAL-CH, we then map the $p \times (2p+1)$ matrix $\tilde{C}^{(r)}$ to the periodic ORTHO-CH sequence with period $(2p+1)p$. Channels that are not in the available channel set are randomly replaced by channels in the available channel set. If the two users select the same ID channel, then both users are guaranteed to rendezvous from the cover property of a set of orthogonal MACH matrices. On the other hand, if the two users select two different ID channels, then both users are guaranteed to rendezvous on every commonly available channel from the 2D-MRD property of a set of orthogonal MACH matrices. As such, the two users are guaranteed to rendezvous within the period $(2p+1)p$. The detailed construction is shown in Algorithm 4.

Algorithm 4 The ORTHO-CH

Input A set of available channels $\mathbf{c}$ that is a subset of $\{0, 1, \ldots, N-1\}$.

Output A CH sequence $\{c(t), t = 0, 1, 2 \ldots, p(2p+1)-1\}$ with $c(t) \in \mathbf{c}$, where p is the smallest prime not less than N.

1: If channel 0 is the only channel in $\mathbf{c}$, output $c(t) = 0$ for all $t = 0, 1, 2 \ldots, p(2p+1)-1$.

2: Randomly select a nonzero channel r from $\mathbf{c}$ as the ID channel.

3: Find the smallest prime p such that $p \geq N$ and construct a $p \times p$ matrix $C^{(r)} = (c^{(r)}_{i,j})$ by letting

$$c^{(r)}_{i,j} = (r \cdot i + j) \mod p.$$

4: Let $\mathbf{r}$ be the $p \times 1$ column vector with all its elements being r. Construct the $p \times (2p+1)$ matrix $\tilde{C}^{(r)}$ by concatenating the column vector $\mathbf{r}$ and two identical matrices of $C^{(r)}$, i.e.,

$$\tilde{C}^{(r)} = (\tilde{c}^{(r)}_{i,j}) = (\mathbf{r}|C^{(r)}|C^{(r)}).$$

5: For $t = 0, 1, 2 \ldots, p(2p+1)-1$, let $c(t) = \tilde{c}^{(r)}_{i,j}$ with $i = \lfloor t/(2p+1) \rfloor$ and $j = (t \mod (2p+1))$.

6: If $c(t)$ is not in $\mathbf{c}$, replace it at random by a channel in $\mathbf{c}$.

For example, if $N = 4$, then $p = 5$. Suppose that the available channel set $\mathbf{c} = \{0, 1, 3\}$ and channel 3 is selected as the ID channel. From (34), the 5×11 matrix $\tilde{C}$ is constructed as follows:

$$\left[\begin{array}{c|ccccc|ccccc} 3 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 \\ 3 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 \\ 3 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 \\ 3 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 \end{array}\right]. \quad (36)$$

Now replace the channels 2 and 4 by randomly selected channels in $\mathbf{c}$ (marked in R) leads to the following CH sequence:

$$\begin{aligned} &3, 0, 1, R, 3, R, 0, 1, R, 3, R, \\ &3, 3, R, 0, 1, R, 3, R, 0, 1, R, \\ &3, 1, R, 3, R, 0, 1, R, 3, R, 0, \\ &3, R, 0, 1, R, 3, R, 0, 1, R, 3, \\ &3, R, 3, R, 0, 1, R, 3, R, 0, 1. \end{aligned}$$

Theorem 13: Suppose that user i, $i = 1$ and 2, have the available channel sets $\mathbf{c}_i$, $i = 1$ and 2, that are subsets of $\{0, 1, 2 \ldots, N-1\}$ and that both users use the ORTHO-CH in Algorithm 4 to generate its CH sequence. If there is at least one commonly available channel, i.e., $\mathbf{c}_1 \cap \mathbf{c}_2 \neq \varnothing$, then both users are guaranteed to rendezvous within $(2p+1)p$ time slots for any clock drift d between these two users, where p is the smallest prime not less than N.

Proof: The case that one of the two users only has channel 0 in its available channel set is trivial as that user will stay on channel 0 all the time. Thus, it suffices to consider the case that both users have at least one channel that is not channel 0. Let r_i be the ID channel selected by user k, $k = 1$ and 2, and $\{c_k(t), t = 0, 1, \ldots\}$ be the CH sequence of user k from the ORTHO-CH in Algorithm 4. Under the assumption that there is at least one commonly available channel, we need to show that there exists $0 \le t \le (2p+1)p-1$ such that for any time shift $0 \le d \le (2p+1)p-1$,

$$c_1(t) = c_2(t+d). \tag{37}$$

Let $\delta = \lfloor d/(2p+1) \rfloor$ be the vertical shift and $\tau = (d \mod (2p+1))$ be the horizontal shift. In view of the matrix-based construction of CH sequences, the condition in (37) holds if and only if for any $0 \le \delta \le p-1$ and $0 \le \tau \le 2p-1$, there exist $0 \le i \le p-1$ and $0 \le j \le 2p-1$ such that

$$\tilde{c}_{i,j}^{(r_1)} = \tilde{c}_{i\oplus\delta, j\oplus\tau}^{(r_2)}, \tag{38}$$

where $\tilde{C}^{(r_k)} = (\tilde{c}_{i,j}^{(r_k)})$, $k = 1$ and 2, are the $p \times (2p+1)$ matrices defined in (35). Now consider the following two cases:

Case 1 ($r_1 = r_2$): In this case, both users select the same ID channel from their available channel sets. As such, r_1 is in the available channel set of user 2. If $\tau = 0$, then both users rendezvous on the same ID channel of column 0, i.e., for all $0 \le i \le p-1$,

$$\tilde{c}_{i,0}^{(r_1)} = \tilde{c}_{i\oplus\delta,0}^{(r_2)} = r_1 = r_2. \tag{39}$$

On the other hand, if $\tau \neq 0$, it then follows from the cover property that column τ of $\tilde{C}^{(r_2)}$ contains at least one r_1. Thus, there exists $0 \le i^* \le p-1$ such that the $(i^* \oplus \delta)^{th}$ element of column τ of $\tilde{C}^{(r_2)}$ is r_1, i.e., $\tilde{c}_{i^*\oplus\delta,\tau}^{(r_2)} = r_1$. Since the p elements in column 0 of $\tilde{C}^{(r_1)}$ are all r_1, we then have

$$\tilde{c}_{i^*,0}^{(r_1)} = \tilde{c}_{i^*\oplus\delta,\tau}^{(r_2)} = r_1. \tag{40}$$

For example, suppose that $\{c_1(t), 0 \le t \le 54\}$ is the CH sequence in (36). Then, the sequence $\{c_2((t+d) \mod 55), 0 \le t \le 54\}$ in this case can be represented by the concatenation of its ID column, the first $C^{(r_2)}$ matrix, and the second $C^{(r_2)}$ matrix. The overlaps of the ID column (resp. the first matrix, the second matrix) with the sequence $\{c_1(t), 0 \le t \le 54\}$ is marked in *green* (resp. *red*, *blue*) in (41). Note that the 5 elements marked in green form a permutation of $\{0, 1, 2, 3, 4\}$.

$$\left[\begin{array}{c|ccccc|ccccc}
3 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 \\
3 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 \\
3 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 \\
3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 \\
3 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 \\
3 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 \\
3 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 \\
3 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 \\
3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 \\
3 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1
\end{array}\right]. \tag{41}$$

Case 2 ($r_1 \neq r_2$): In this case, the two users select two different ID channels. As such, their CH sequences are constructed from two mutually orthogonal MACH matrices. As in the proof of Theorem 7, we consider the following two subcases:

Case 2.1 ($0 \le \tau \le p$): In this subcase, the *first* matrix $C^{(r_2)}$ of $\tilde{C}^{(r_2)}$ overlaps with a $p \times p$ square box in the plane repeated from $C^{(r_1)}$ (see, e.g., the square marked in red in (41). Under the assumption that there is at least one commonly available channel, the condition in (38) follows immediately from the 2D-MRD property of two mutually orthogonal MACH matrices.

Case 2.2 ($p < \tau \le 2p-1$): In this subcase, the *second* matrix $C^{(r_2)}$ of $\tilde{C}^{(r_2)}$ overlaps with a $p \times p$ square box in the plane repeated from $C^{(r_1)}$. Once again, under the assumption that there is at least one commonly available channel, the condition in (38) follows immediately from the 2D-MRD property of two mutually orthogonal MACH matrices. ■

In comparison with FRCH in [14], ORTHO-CH has the same MTTR bound $(2N+1)N$ if N is a prime. Note that $N \neq ((5+2\alpha)*r-1)/2$ is required for FRCH. For instance, if $\alpha = 0$ and $r = 3$, then FRCH does not guarantee the rendezvous of the two users for $N = 7$. To achieve such an MTTR bound, FRCH has to remap the channels that are not in the available channel set according to a specific remapping rule. For ORTHO-CH, such replacements can be chosen randomly. In comparison with the Sequence-Rotating-Rendezvous (SRR) algorithm in [15], our ORTHO-CH sequence reduces the MTTR from $2p^2 + 2p$ to $(2p+1)p$. Both constructions are similar in the sense that they both are based on the two mathematical properties of orthogonal MACH matrices (and thus the proofs are also similar). The key difference is that the ORTHO-CH sequence is periodic while the SRR sequence is not. In practice, there might be a nonzero probability that the two users may not rendezvous even when they both hop on a common channel. In such a setting, there might be a problem for the SRR algorithm when the two users select the same ID channel and they miss their rendezvous on the ID channel. In that sense, ORTHO-CH is more robust than SRR. Similarly, IDEAL-CH is more robust than ORTH-TH as every commonly available channel is a rendezvous channel in IDEAL-CH. However, the period p of the general IDEAL-CH is the smallest prime with $p - (\lceil\sqrt{p}\rceil + \lfloor p/\lceil\sqrt{p}\rceil\rfloor - 1) \ge N$, which is in general larger than the period of ORTHO-CH for the same total number of channels N.

As described in the book [1], both IDEAL-CH and ORTHO-CH sequences are known as *global* sequences as they are constructed from all the N channel and then replace those channels not in the available channel set of a user by some channels in its available channel set. Another approach is to construct CH sequences directly from the available channel sets of users. Such sequences are called *local* sequences, e.g., QR [40], Catalan [27], MTP [41], FMR [42], and QECH [4]. When the numbers of channels of the two users, n_1 and n_2 are $O(N^\alpha)$ for some $0 < \alpha < 1$, then the MTTR bounds from these local sequences are $o(N^2)$ (see Table I) and thus better than those from global sequences. On the other hand, if n_1 and n_2 are linear in N, then the $O(N^2)$ of MTTR

bounds of global sequences are better than those of local sequences.

V. Conclusion

By embedding difference sets into an ideal matrix, we are able to tighten the theoretical gap of the asymptotic approximation ratio for CH sequences with maximum rendezvous diversity from 2.5 to 2. The factor of 2 is very similar to the factor of 2 that incurs from assuming that the slot boundaries are aligned (in this paper) even when the continuous-time clocks of the two users are not synchronized. To see this, suppose that the minimum amount of time needed for the two users to rendezvous (by exchanging information) on the same channel is τ. Then, one has to set the slot size to be at least 2τ so that the overlap in a time slot is at least τ even when the slot boundaries are not aligned. In view of this, it seems difficult to further reduce the ratio by using the 2D-MRD property as one needs a factor of 2 to convert it into the 1D-MRD property.

To conclude the paper, we would like to quote the following comment from the end of the excellent book [1]:

"…, closing the gap between the lower bounds on the maximum time to rendezvous in worst-case situations and the upper bounds by the presented algorithms will likely be a long term project."

References

[1] Z. Gu, Y. Wang, Q.-S. Hua, and F. C. M. Lau, *Rendezvous in Distributed Systems: Theory, Algorithms and Applications*. Singapore: Springer, 2017.

[2] L. Chen, Y. Li, and A. V. Vasilakos, "Oblivious neighbor discovery for wireless devices with directional antennas," in *Proc. 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Apr. 2016, pp. 1–9.

[3] S. A. Pambudi, W. Wang, and C. Wang, "Fast rendezvous for spectrum-agile IoT devices with limited channel hopping capability," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2018, pp. 1385–1393.

[4] Z. Zhang, B. Yang, M. Liu, Z. Li, and X. Guo, "A quaternary-encoding-based channel hopping algorithm for blind rendezvous in distributed IoTs," *IEEE Trans. Commun.*, vol. 67, no. 10, pp. 7316–7330, Oct. 2019.

[5] K. Bian and J.-M. 'J.' Park, "Maximizing rendezvous diversity in rendezvous protocols for decentralized cognitive radio networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 7, pp. 1294–1307, Jul. 2013.

[6] Z. Gu, Q.-S. Hua, Y. Wang, and F. C. M. Lau, "Nearly optimal asynchronous blind rendezvous algorithm for cognitive radio networks," in *Proc. IEEE Int. Conf. Sens., Commun. Netw. (SECON)*, Jun. 2013, pp. 371–379.

[7] F. Hou, L. X. Cai, X. Shen, and J. Huang, "Asynchronous multichannel MAC design with difference-set-based hopping sequences," *IEEE Trans. Veh. Technol.*, vol. 60, no. 4, pp. 1728–1739, May 2011.

[8] J. Shin, D. Yang, and C. Kim, "A channel rendezvous scheme for cognitive radio networks," *IEEE Commun. Lett.*, vol. 14, no. 10, pp. 954–956, Oct. 2010.

[9] Z. Lin, H. Liu, X. Chu, and Y.-W. Leung, "Jump-stay based channel-hopping algorithm with guaranteed rendezvous for cognitive radio networks," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 2444–2452.

[10] G.-Y. Chang, J.-F. Huang, and Y.-S. Wang, "Matrix-based channel hopping algorithms for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2755–2768, May 2015.

[11] B. Yang, M. Zheng, and W. Liang, "A time-efficient rendezvous algorithm with a full rendezvous degree for heterogeneous cognitive radio networks," in *Proc. 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Apr. 2016, pp. 1–9.

[12] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *Trans. Amer. Math. Soc.*, vol. 43, no. 3, pp. 377–385, 1938.

[13] P. V. Kumar, "On the existence of square dot-matrix patterns having a specific three-valued periodic-correlation function," *IEEE Trans. Inf. Theory*, vol. IT-34, no. 2, pp. 271–277, Mar. 1988.

[14] G.-Y. Chang and J.-F. Huang, "A fast rendezvous channel-hopping algorithm for cognitive radio networks," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1475–1478, Jul. 2013.

[15] Y. Fu *et al.*, "How local information improves rendezvous in cognitive radio networks," in *Proc. 15th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON)*, Jun. 2018, pp. 1–9.

[16] C.-F. Shih, T. Y. Wu, and W. Liao, "DH-MAC: A dynamic channel hopping MAC protocol for cognitive radio networks," in *Proc. IEEE Int. Conf. Commun.*, May 2010, pp. 1–5.

[17] J. Li and J. Xie, "Practical fast multiple radio blind rendezvous schemes in ad-hoc cognitive radio networks," in *Proc. Resilience Week (RWS)*, Aug. 2015, pp. 1–6.

[18] R. N. Yadav and R. Misra, "Periodic channel-hopping sequence for rendezvous in cognitive radio networks," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Aug. 2015, pp. 1787–1792.

[19] L. Yu, H. Liu, Y.-W. Leung, X. Chu, and Z. Lin, "Channel-hopping based on available channel set for rendezvous of cognitive radios," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 1573–1579.

[20] E. J. Anderson and R. R. Weber, "The rendezvous problem on discrete locations," *J. Appl. Probab.*, vol. 27, no. 4, pp. 839–851, Dec. 1990.

[21] A. Dessmark, P. Fraigniaud, D. R. Kowalski, and A. Pelc, "Deterministic rendezvous in graphs," *Algorithmica*, vol. 46, no. 1, pp. 69–96, Sep. 2006.

[22] C.-S. Chang, C.-Y. Chen, D.-S. Lee, and W. Liao, "Efficient encoding of user IDs for nearly optimal expected time-to-rendezvous in heterogeneous cognitive radio networks," *IEEE/ACM Trans. Netw.*, vol. 25, no. 6, pp. 3323–3337, Dec. 2017.

[23] N. C. Theis, R. W. Thomas, and L. A. DaSilva, "Rendezvous for cognitive radios," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 216–227, Feb. 2011.

[24] Z. Gu, Q.-S. Hua, and W. Dai, "Fully distributed algorithms for blind rendezvous in cognitive radio networks," in *Proc. ACM MobiHoc*, Aug. 2014, pp. 155–164.

[25] L. Chen, K. Bian, L. Chen, C. Liu, J.-M.-J. Park, and X. Li, "A group-theoretic framework for rendezvous in heterogeneous cognitive radio networks," in *Proc. ACM MobiHoc*, Aug. 2014, pp. 165–174.

[26] L. Chen, S. Shi, K. Bian, and Y. Ji, "Optimizing average-maximum TTR trade-off for cognitive radio rendezvous," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 7707–7712.

[27] S. Chen, A. Russell, A. Samanta, and R. Sundaram, "Deterministic blind rendezvous in cognitive radio networks," in *Proc. IEEE 34th Int. Conf. Distrib. Comput. Syst.*, Jun. 2014, pp. 358–367.

[28] C.-S. Chang, W. Liao, and T.-Y. Wu, "Tight lower bounds for channel hopping schemes in cognitive radio networks," *IEEE/ACM Trans. Netw.*, vol. 24, no. 4, pp. 2343–2356, Aug. 2016.

[29] Y. Zhang, Y.-H. Lo, and W. S. Wong, "On channel hopping sequences with full rendezvous diversity for cognitive radio networks," *IEEE Wireless Commun. Lett.*, vol. 7, no. 4, pp. 574–577, Aug. 2018.

[30] S. Alpern and S. Gal, *The Theory of Search Games and Rendezvous*. Dordrecht, The Netherlands: Kluwer, 2003.

[31] Y. R. Kondareddy and P. Agrawal, "Synchronized MAC protocol for multi-hop cognitive radio networks," in *Proc. IEEE Int. Conf. Commun.*, May 2008, pp. 3198–3202.

[32] K. Bian, J.-M. Park, and R. Chen, "A quorum-based framework for establishing control channels in dynamic spectrum access networks," in *Proc. 15th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Sep. 2009, pp. 25–36.

[33] P. Bahl, R. Chandra, and J. Dunagan, "SSCH: Slotted seeded channel hopping for capacity improvement in IEEE 802.11 ad-hoc wireless networks," in *Proc. 10th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Sep. 2004, pp. 216–230.

[34] C.-S. Chang, W. Liao, and C.-M. Lien, "On the multichannel rendezvous problem: Fundamental limits, optimal hopping sequences, and bounded time-to-rendezvous," *Math. Oper. Res.*, vol. 40, no. 1, pp. 1–23, Feb. 2015.

[35] L. A. DaSilva and I. Guerreiro, "Sequence-based rendezvous for dynamic spectrum access," in *Proc. 3rd IEEE Symp. Frontiers Dyn. Spectr. Access Netw.*, Oct. 2008, pp. 1–7.

[36] D. Yang, J. Shin, and C. Kim, "Deterministic rendezvous scheme in multichannel access networks," *Electron. Lett.*, vol. 46, no. 20, pp. 1402–1404, 2010.

[37] Z. Lin, H. Liu, X. Chu, and Y.-W. Leung, "Enhanced jump-stay rendezvous algorithm for cognitive radio networks," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1742–1745, Sep. 2013.

[38] G.-Y. Chang, W.-H. Teng, H.-Y. Chen, and J.-P. Sheu, "Novel channel-hopping schemes for cognitive radio networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 2, pp. 407–421, Feb. 2014.
[39] I.-H. Chuang, H.-Y. Wu, and Y.-H. Kuo, "A fast blind rendezvous method by alternate hop-and-wait channel hopping in cognitive radio networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 10, pp. 2171–2184, Oct. 2014.
[40] C.-S. Chang, Y.-C. Chang, and J.-P. Sheu, "A quasi-random algorithm for anonymous rendezvous in heterogeneous cognitive radio networks," 2019, *arXiv:1902.06933*. [Online]. Available: https://arxiv.org/abs/1902.06933
[41] Z. Gu, H. Pu, Q.-S. Hua, and F. C. M. Lau, "Improved rendezvous algorithms for heterogeneous cognitive radio networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2015, pp. 154–162.
[42] Y.-C. Chang, C.-S. Chang, and J.-P. Sheu, "An enhanced fast multi-radio rendezvous algorithm in heterogeneous cognitive radio networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 4, no. 4, pp. 847–859, Dec. 2018.
[43] K. Wu, F. Han, F. Han, and D. Kong, "Rendezvous sequence construction in cognitive radio ad-hoc networks based on difference sets," in *Proc. IEEE 24th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2013, pp. 1840–1845.
[44] X. J. Tan, C. Zhou, and J. Chen, "Symmetric channel hopping for blind rendezvous in cognitive radio networks based on union of disjoint difference sets," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10233–10248, Nov. 2017.
[45] J. E. H. Elliott and A. T. Butson, "Relative difference sets," *Illinois J. Math.*, vol. 10, no. 3, pp. 517–531, Sep. 1966.
[46] W.-S. Luk and T.-T. Wong, "Two new quorum based algorithms for distributed mutual exclusion," in *Proc. 17th Int. Conf. Distrib. Comput. Syst.*, May 1997, pp. 100–106.
[47] R. C. Baker, G. Harman, and J. Pintz, "The difference between consecutive primes, II," in *Proceedings of The London Mathematical Society*. London, U.K.: The London Mathematical Society, pp. 532–562, 2001.
[48] L. Euler, "Recherches sur une nouvelle espece de quarres magiques," in *Verhandelingen uitgegeven door het zeeuwsch Genootschap der Wetenschappen te Vlissingen*, vol. 9. Middelburg, The Netherlands: Pieter Gillissen, 1782, pp. 85–239.

Cheng-Shang Chang (Fellow, IEEE) received the B.S. degree from National Taiwan University, Taipei, Taiwan, in 1983, and the M.S. and Ph.D. degrees from Columbia University, New York, NY, USA, in 1986 and 1989, respectively, all in electrical engineering.

From 1989 to 1993, he was employed as a Research Staff Member with the IBM Thomas J. Watson Research Center, Yorktown Heights, NY, USA. Since 1993, he has been with the Department of Electrical Engineering, National Tsing Hua University, Taiwan, where he is currently a Tsing Hua Distinguished Chair Professor. He is also the author of the book *Performance Guarantees in Communication Networks* (Springer, 2000) and a coauthor of the book *Principles, Architectures and Mathematical Theory of High Performance Packet Switches* (Ministry of Education, 2006). His current research interests include network science, big data analytics, mathematical modeling of the Internet, and high-speed switching.

Dr. Chang is also a member of the IFIP Working Group 7.3. He received the IBM Outstanding Innovation Award in 1992, the IBM Faculty Partnership Award in 2001, the Outstanding Research Awards from the National Science Council, Taiwan, in 1998, 2000, and 2002, the Outstanding Teaching Awards from the College of EECS and the university itself in 2003, the Merit NSC Research Fellow Award from the National Science Council in 2011, and the Academic Award in 2011 and the National Chair Professorship in 2017 from the Ministry of Education. He was the recipient of the 2017 IEEE INFOCOM Achievement Award. He was appointed as the first Y. Z. Hsu Scientific Chair Professor in 2002. He served as an Editor for Operations Research from 1992 to 1999, the IEEE/ACM TRANSACTIONS ON NETWORKING from 2007 to 2009, and IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING from 2014 to 2017. He is also serving as an Editor-at-Large for the IEEE/ACM TRANSACTIONS ON NETWORKING.

Jang-Ping Sheu (Fellow, IEEE) received the B.S. degree in computer science from Tamkang University, Taiwan, in 1981, and the M.S. and Ph.D. degrees in computer science from National Tsing Hua University, Taiwan, in 1983 and 1987, respectively.

He was an Associate Dean of the College of Electrical and Computer Science, National Tsing Hua University, from 2016 to 2017. He was the Director of the Department of Computer Science and Information Engineering, National Central University, from 1997 to 1999; the Computer Center, National Central University, from 2003 to 2006; and the Computer and Communication Research Center, National Tsing Hua University, from 2009 to 2015. He is currently the Chair Professor of the Department of Computer Science and the Director of the Joint Research Center, Delta-NTHU, National Tsing Hua University. His current research interests include wireless communications, mobile computing, the Internet of Things, and UAV-assisted communication systems.

Dr. Sheu is also a member of the Phi Tau Phi Society. He received the Distinguished Research Awards from the National Science Council of the Republic of China from 1993 to 1994, from 1995 to 1996, and from to 1998. He received the Distinguished Engineering Professor Award from the Chinese Institute of Engineers in 2003, the K. T. Li Research Breakthrough Award from the Institute of Information and Computing Machinery in 2007, the Y. Z. Hsu Scientific Chair Professor Award in 2009, the Pan Wen Yuan Outstanding Research Award in 2014, the Academic Award in Engineering from the Ministry of Education in 2016, the Medal of Honor in Information Sciences from the Institute of Information and Computing Machinery in 2017, and the TECO Award in 2019. He was an Associate Editor of the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS and the *International Journal of Sensor Networks*. He is also an Advisory Board Member of the *International Journal of Ad Hoc and Ubiquitous Computing* and *International Journal of Vehicle Information and Communication Systems*.

Yi-Jheng Lin received the B.S. degree in electrical engineering from National Tsing Hua University, Hsinchu, Taiwan, in 2018, where he is currently pursuing the Ph.D. degree with the Institute of Communications Engineering. His research interests include wireless communication and cognitive radio networks.