A Group-theoretic Framework for Rendezvous in Heterogeneous Cognitive Radio Networks

Lin Chen*, Kaigui Bian*, Lin Chen†, Cong Liu‡, Jung-Min Jerry Park♯, and Xiaoming Li*
*Peking University, Beijing, China. †University Paris-Sud, Orsay, France.
‡Sun Yat-Sen University, China. ♯Virginia Tech, Blacksburg, VA, USA.
*{abratchen, bkg, lxm}@pku.edu.cn, †chen@lri.fr, ‡liucong3@mail.sysu.edu.cn, ♯jungmin@vt.edu

ABSTRACT

In cognitive radio (CR) networks, a pair of CR nodes have to "rendezvous" on a common channel for link establishment. Channel hopping (CH) protocols have been proposed for creating rendezvous over multiple channels to reduce the possibility of rendezvous failures caused by the detection of primary user signals. Rendezvous within a minimal bounded time over multiple channels is a challenging problem in heterogeneous CR networks where two CR nodes may have asynchronous clocks, different sensing capabilities, no common universal channel set, and heterogeneous channel index systems. In this paper, we present a systematic approach using group theory for designing CH protocols that guarantee the maximum number of rendezvous channels and the minimal time-to-rendezvous (TTR) in heterogeneous environments. We derive the minimum upper bound of TTR, and propose two types of rendezvous protocols that are independent of environmental heterogeneity. Analytical and simulation results show that these protocols are resistant to rendezvous failures under various network conditions.

Categories and Subject Descriptors

C.2.2 [**Computer-Communication Networks**]: Network Protocols

Keywords

Cognitive radio, rendezvous, heterogeneous

1. INTRODUCTION

In *cognitive radio* (CR) networks, "rendezvous" is a bootstrapping primitive for two communicating nodes or secondary users (SUs) to find each other on a *rendezvous/control channel* within a bounded time, prior to data communications [12]. However, *rendezvous failure* occurs between two SUs when the rendezvous channel is unavailable due to the detection of primary user (PU) or interference signals.

MobiHoc'14, August 11–14, 2014, Philadelphia, PA, USA.

http://dx.doi.org/10.1145/2632951.2632988.

Two metrics are usually used for evaluating the performance of a rendezvous protocol.

1. Ideally, we want to maximize the number of rendezvous channels—referred to as *rendezvous diversity*—thereby minimizing the risk of rendezvous failures [4];
2. It is also desired to minimize the *time-to-rendezvous (TTR)* for obtaining a small rendezvous delay between two SUs [3, 8, 10, 15].

Since the *common control channel (CCC)* approach is subject to the rendezvous failure problem, *channel hopping (CH) approaches* have been widely used to create multiple rendezvous channels between two SUs [3, 6, 8, 10, 11, 15]. Specifically, each SU starts a channel hopping process according to its own CH sequence and local clock; two SUs' CH sequences are carefully chosen to spread out rendezvous points over multiple pairwise common channels.

There are four primary challenges for designing a CH-based rendezvous protocol that has a small TTR and a high rendezvous diversity in *heterogeneous environments.*

1. *Lack of clock synchronization.* It is difficult to require two independent nodes to have synchronized clocks without any handshake between them. Existing research efforts address this problem by using quorum-based [3, 5], difference set-based [9], modular-based [2, 12, 15], jump-stay [10], and circle-based channel hopping approaches [7].
2. *Different sensing capabilities.* Two CR nodes may have different spectrum sensing capabilities, and thus their perceptions of channel availability or sensible channel sets can be different. Recent studies show that efficient rendezvous can be achieved for two CR nodes without assuming the same sensible channel set [13, 14].
3. *No universal channel set or common channel index system.* Most existing work assumes that all nodes share a known universal channel set, where N frequency channels are mapped to channel indices using a common channel index system. However, a CH-based protocol may fail to guarantee rendezvous when two nodes have no universal channel set or a common way of mapping channel indices to frequency channels. For example, given three channels with center frequencies a, b, c, two nodes using the same CH sequence $\{0, 1, 2\}$ fail to achieve rendezvous when one node maps indices $\{0, 1, 2\}$ to frequencies $\{a, b, c\}$, while the other maps indices $\{0, 1, 2\}$ to $\{b, c, a\}$.

4. *Independence of consecutive integer channel indices.* In many existing works, every node has a set of *consecutive* integer channel indices in a common channel index system which allows the exploitation of arithmetic modular operations for guaranteeing rendezvous in the constructed CH sequences [2, 10, 13, 14]. For instance, it is assumed in [13, 14] that there exists a universal channel set $U = \{c_0, c_1, \ldots, c_{|U|-1}\}$ and that each node i can sense a range of consecutive channels $V_i = \{c_x, c_{x+1}, \ldots, c_{x+|V_i|-1}\}$. However, it is difficult for every node to sense a range of consecutive channels that come from a universal spectrum in practical scenarios.

We would like to point out that it is the holistic combination of the above four challenges that makes the design of rendezvous protocols far from trivial and requires an original study that cannot draw on any existing result which, to the best of our knowledge, addresses only the first and/or the second challenge. Formally, we coin the term *heterogeneous rendezvous* problem in CR networks to denote the following problem: *How can two channel hopping secondary users, given asynchronous local clocks, different sensing capabilities, no universal channel sets, and heterogeneous channel index systems, achieve the maximum "rendezvous diversity" within a minimum upper-bounded TTR?*

In response to the formulated problem, we present a systematic approach based on *group theory* for analyzing and devising CH-based rendezvous protocols that address above challenges altogether. The contributions of this work are summarized as follows.

1. *Establishment of the group-theoretic framework*: We formulate the heterogeneous rendezvous problem from the group-theoretic perspective, and cast the CH-based rendezvous protocol design into the established framework.

2. *Theoretical performance bound of rendezvous protocols*: We derive that the *minimum upper bound for TTR* to achieve the *maximum rendezvous diversity* in heterogeneous environments is N_iN_j, where N_i and N_j are the sizes of two distinct channel sets available to the two nodes i and j.

3. *Design of optimal rendezvous protocols that achieve the derived performance bound*: We first propose rendezvous protocols that achieve maximum rendezvous diversity within a TTR bounded by N_iN_j, given that N_i and N_j are co-prime. By leveraging the *symmetrization* technique, we further propose an advanced rendezvous protocol that achieves maximum rendezvous diversity within a TTR bounded by $O(N_iN_j)$ without assuming co-prime N_i and N_j.

Note that the follow-on tasks after initial rendezvous—such as neighbor discovery handshake [1], channel contention procedure, and data transfer—are outside the scope of this paper.

The rest of this paper is organized as follows. We provide the system model and formulate the problem in Section 2. In Sections 3 and 4, we describe the elementary and advanced CH-based rendezvous protocols respectively. We evaluate the performance of our proposed rendezvous schemes in Section 5, and conclude the paper in Section 6.

2. PROBLEM FORMULATION

2.1 System Model

2.1.1 Heterogeneous network environments

We assume a CR network where every secondary user/node $i \in \Lambda$ is equipped with a CR operating over a number of orthogonal frequency channels that are licensed to primary users, where Λ is the set of user IDs in the network.

Clock drift. We consider a time-slotted communication system. Local clocks of two nodes may differ from each other by a certain amount of *clock drift*. A network node is assumed to be capable of hopping across different channels according to a channel hopping sequence and its local clock.

Different sensible channel sets. We term the set of frequency channels which a secondary user i can sense and operate over its *sensible channel set* or *channel set*, denoted by C_i. $N_i = |C_i| < \infty$ is called its *sensible channel number* or simply *channel number*.

Different channel labeling functions. We do not assume a universal channel set for all nodes whereby their sensible frequency channels are mapped to a set of channel indices in the same way. Hence, each node i has its own channel labeling function to assign each frequency channel in C_i a channel index chosen from its channel label set $\mathbb{Z}_{N_i} = \{0, 1, 2, \ldots, N_i - 1\}$. We call the elements of the label set $\mathbb{Z}_{N_i}$ *channel labels* or *channel indices*. The labeling function λ_i is a 1-1 correspondence between C_i and $\mathbb{Z}_{N_i}$:

$$\lambda_i : C_i \to \mathbb{Z}_{N_i}.$$

Let $\lambda_i^{-1} : \mathbb{Z}_{N_i} \to C_i$ denote the inverse map of λ_i.

Heterogeneous environments. The CR network environment is *heterogeneous* in the sense that

- Tight synchronization is unavailable for different nodes' local clocks.
- C_i is *not necessarily identical* with C_j for two distinct nodes i and j.
- Each node i has its own channel labeling function λ_i, i.e., given the same channel at frequency a, it is possible that $\lambda_i(a) \neq \lambda_j(a)$.

2.1.2 CH sequence

A CH sequence determines the order in which a node visits all available channels. We represent node i's CH sequence u_i with period T as a sequence of channel indices:

$$u_i = \{u_i^0, u_i^1, ..., u_i^t, ..., u_i^{T-1}\},$$

where $u_i^t \in \mathbb{Z}_{N_i}$ denotes the channel index of sequence u_i in the t-th timeslot of a CH period, and $|u_i| = T$.

Given two CH sequences with period T, u_i and u_j, if $\exists t \in [0, T-1]$ s.t.

$$\lambda_i^{-1}(u_i^t) = \lambda_j^{-1}(u_j^t) = a$$

with $a \in C_i \cap C_j$, we say that u_i and u_j *rendezvous* in the t-th timeslot on frequency channel a. The t-th timeslot is called a *rendezvous slot*; frequency channel a is called a *rendezvous channel* between u_i and u_j; u_i^t and u_j^t are called a *pair of rendezvous channel indices.*

Let $\mathcal{C}(u_i, u_j)$ denote the *set of rendezvous channels* between two CH sequences u_i and u_j, and $\mathcal{T}(u_i, u_j)$ denote the *set of rendezvous slots.* Obviously, $\mathcal{C}(u_i, u_j) \subseteq C_i \cap C_j$ and $\mathcal{T}(u_i, u_j) \subseteq [0, T-1]$.

2.1.3 Common period of two CH sequences

Given two CH sequences with different periods, u_i and u_j whose periods are T_i and T_j respectively, we extend them to a CH sequence with period $T = \mathrm{lcm}(T_i, T_j)$[1], such as $u'_i = \prod_{k=1}^{T/T_j} u_i$ and $u'_j = \prod_{k=1}^{T/T_i} u_j$, where $\prod_{k=1}^{K} s_k$ denotes the concatenated sequence $s_1 \parallel s_2 \parallel s_3 \parallel \cdots \parallel s_K$.

$T = \mathrm{lcm}(T_i, T_j)$ is termed the *common period* of u_i and u_j. We define $\mathcal{C}(u_i, u_j) \triangleq \mathcal{C}(u'_i, u'_j) \subseteq C_i \cap C_j$, and $\mathcal{T}(u_i, u_j) \triangleq \mathcal{T}(u'_i, u'_j) \subseteq [0, T-1]$.

2.2 CH Protocol

A CH protocol is a rule of creating a CH sequence for each node and can be represented as a map r

$$\begin{aligned} r : \Lambda \times \mathbb{N} &\rightarrow \bigcup_{T=1}^{\infty} \mathbb{N}^T \\ (i, N_i) &\mapsto r(i, N_i) \end{aligned}$$

where $\mathbb{N}^T$ is the set of natural number sequences with length T and $\bigcup_{T=1}^{\infty} \mathbb{N}^T$ denotes the set of all CH sequences. Node i's CH sequence will be $r(i, N_i)$.

In heterogeneous environments, two nodes may have no knowledge about the clock time, the channel set, and the channel labeling function of each other. A node knows its ID i and the number of sensible channels, i.e., N_i. Our definition of a CH protocol r only relies on a node's ID i and channel number N_i. Note that r is independent of the clock time, the channel set (we are not interested in which channels are available to a node but the total number of available channels) and the channel labeling function, and that node i's CH sequence only relies on its own information and requires no knowledge about other nodes.

2.3 Heterogeneous CH (HCH) System

Given a CH sequence u_i, we use $rotate(u_i, k)$ to denote the *cyclic rotation* of CH sequence u_i by k timeslots, i.e.,

$$rotate(u_i, k) = \{v_i^0, ..., v_i^t, ..., v_i^{T-1}\},$$

where $v_i^t = u_i^{(t+k) \bmod T}$, $t \in [0, T-1]$ and k is an integer. For example, given $u_i = \{0, 1, 2\}$, $rotate(u_i, 2) = \{2, 0, 1\}$.

DEFINITION 1. *A* Heterogeneous CH (HCH) system *for a CR network is a pair $H = (\Lambda, r)$. $\forall i, j \in \Lambda, i \neq j$ and $\forall k, l \in \mathbb{Z}$, H satisfies the following property: if $C_i \cap C_j \neq \varnothing$, then $|\mathcal{T}(rotate(r(i, N_i), k), rotate(r(j, N_j), l))| \geq 1$, where Λ is the set of node IDs in the network, and r is the CH protocol to be designed.*

In Definition 1, the required property states that two nodes' CH sequences should have at least one rendezvous timeslot per common period given any amount of clock drifts k and l, provided that they share at least one common channel. Obviously, it is impossible to rendezvous with no channel in common.

2.4 Group-based Interpretation of Rendezvous

Nodes i and j rendezvous on a frequency channel a in timeslot t, which implies that they simultaneously hop onto the same frequency regardless of their assigned channel indices, $\lambda_i(a) \in \mathbb{Z}_{N_i}$ and $\lambda_j(a) \in \mathbb{Z}_{N_j}$, to a. I.e., frequency a can be mapped to any channel index in $\mathbb{Z}_{N_i}$ and $\mathbb{Z}_{N_j}$. Hence the pair of rendezvous channel indices $(\lambda_i(a), \lambda_j(a))$ can be any element in the group $\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$. We intuit that a feasible protocol has to enumerate/generate all elements in $\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$. As a result, we transform the concept of rendezvous between two CH sequences to an element in $\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$; the maximum rendezvous diversity independent of channel labeling functions corresponds to enumerating/generating all elements in $\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$.

Min TTR Bound for Max Rendezvous Diversity. Theorem 1 substantiates the aforementioned intuition, whence additionally we obtain the minimum period, i.e., the minimum TTR bound for the maximum rendezvous diversity ($|C_i \cap C_j|$).

THEOREM 1. *Given CH sequences $r(i, N_i)$ and $r(j, N_j)$, let*

$$u = \prod_{n=1}^{T/|r(j,N_j)|} r(i, N_i); \qquad v = \prod_{n=1}^{T/|r(i,N_i)|} r(j, N_j),$$

where $T = \mathrm{lcm}(|r(i, N_i)|, |r(j, N_j)|)$. The set of channel index pairs in all timeslots equals $\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$, i.e. $\forall k, l \in \mathbb{Z}$,

$$\{(rotate(u, k)^t, rotate(v, l)^t | t \in [0, T-1]\} = \mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}.$$

As a corollary, their common period T must be $N_i N_j$ or greater; $r(i, N_i)$ and $r(j, N_j)$ can rendezvous on every channel in $C_i \cap C_j$ within T timeslots.

PROOF. It is obvious that $\{(rotate(u, k)^t, rotate(v, l)^t | t \in [0, T-1]\} \subseteq \mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$. It suffices to prove $\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j} \subseteq \{(rotate(u, k)^t, rotate(v, l)^t | t \in [0, T-1]\}$.

Suppose $C_i \cap C_j = \{a\}$ and $\exists (n, m) \in \mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$ but $(n, m) \notin \{(rotate(u, k)^t, rotate(v, l)^t | t \in [0, T-1]\}$. We construct two channel labeling functions $\tilde{\lambda}_i : C_i \rightarrow \mathbb{Z}_{N_i}$ and $\tilde{\lambda}_j : C_j \rightarrow \mathbb{Z}_{N_j}$, such as

$$\tilde{\lambda}_i(x) \triangleq \begin{cases} \lambda_i(x) & \text{if } x \neq a, \lambda_i^{-1}(n) \\ n & \text{if } x = a \\ \lambda_i(a) & \text{if } x = \lambda_i^{-1}(n), \end{cases}$$

$$\tilde{\lambda}_j(x) \triangleq \begin{cases} \lambda_j(x) & \text{if } x \neq a, \lambda_j^{-1}(m) \\ m & \text{if } x = a \\ \lambda_j(a) & \text{if } x = \lambda_j^{-1}(m). \end{cases}$$

We need to prove that i and j cannot rendezvous with channel labeling functions $\tilde{\lambda}_i$ and $\tilde{\lambda}_j$. Suppose $\exists t \in [0, T-1]$ s.t. $\tilde{\lambda}_i^{-1}(rotate(u, k)^t) = \tilde{\lambda}_j^{-1}(rotate(v, l)^t)$. Since $C_i \cap C_j = \{a\}$, $\tilde{\lambda}_i^{-1}(rotate(u, k)^t) = \tilde{\lambda}_j^{-1}(rotate(v, l)^t) = a$, therefore $n = \tilde{\lambda}_i(a) = rotate(u, k)^t$ and $m = \tilde{\lambda}_j(a) = rotate(v, l)^t$. Hence, $(n, m) \in \{(rotate(u, k)^t, rotate(v, l)^t | t \in [0, T-1]\}$, and this is a contradiction.

Hence we conclude that

$$\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j} \subseteq \{(rotate(u, k)^t, rotate(v, l)^t | t \in [0, T-1]\},$$

and that $T \geq |\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}| = N_i N_j$.

Elements in group $\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$ enumerate all possible pairs of rendezvous channel indices, whence the two CH sequences achieve maximum rendezvous diversity. □

2.5 Design Requirements

We identify three design requirements for a CH-based rendezvous protocol to be applicable in heterogeneous environments.

[1]The least common multiple of two integers x and y is usually denoted by $\mathrm{lcm}(x, y)$.

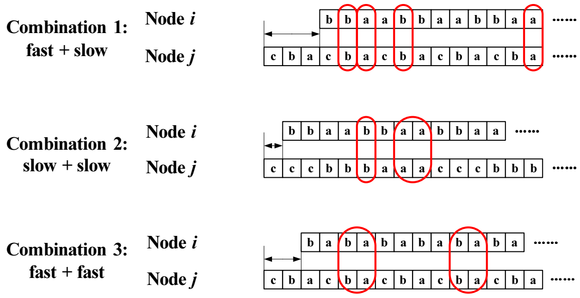

Figure 1: Three combinations of fast and/or slow CH sequences of nodes i and j, with $C_i = \{a, b\}$ and $C_j = \{a, b, c\}$.

1. *Maximum rendezvous diversity.* We have to establish the maximum rendezvous diversity between a pair of rendezvous nodes to minimize the probability of rendezvous failure. As is shown in Theorem 1, it suffices to enumerate all possible pairs of channel indices, i.e., to enumerate all elements in $\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$.

2. *Delay bounded by $O(N_iN_j)$.* According to Theorem 1, the common period of two nodes' CH sequences must be at least N_iN_j; therefore we expect that the maximum rendezvous diversity can be achieved within a delay bounded by $O(N_iN_j)$.

3. *Robustness to cyclic rotation.* To be independent of clock synchronization, rendezvous between two CH sequences has to be robust to cyclic rotation.

Fast/slow CH sequences. We define a pair of CH sequences for each node i with $N_i = |C_i|$ sensible channels: (1) a *fast* CH sequence whereby node i changes its current channel every timeslot to traverse all N_i channels in C_i; and (2) a *slow* CH sequence whereby node i changes its current channel every N_i timeslots to traverse all N_i channels in C_i. For example, suppose $N_i = 3$ and $C_i = \{a, b, c\}$, then $\{a, b, c, a, b, c, a, b, c\}$ is a fast CH sequence and $\{a, a, a, b, b, b, c, c, c\}$ is a slow CH sequence. Note that the relative order of a, b and c does not matter, which means that $\{b, a, c, b, a, c, b, a, c\}$ is also a fast CH sequence and $\{c, c, c, a, a, a, b, b, b\}$ is a slow CH sequence as well. Therefore we can use channel labels to represent a CH sequence alternatively. For instance, $\{0, 2, 1, 0, 2, 1, 0, 2, 1\}$ is a fast sequence and $\{2, 2, 2, 0, 0, 0, 1, 1, 1\}$ is a slow sequence, no matter which channel labeling function is used by node i.

There are three possible combinations/pairs of fast and/or slow CH sequences that can be chosen by two nodes (i.e., *fast+slow*, *slow+slow*, and *fast+fast*), as illustrated in Figure 1. Our research findings indicate that the above design requirements can be satisfied when two nodes happen to choose any of these three combinations, then the maximum rendezvous diversity is established within a bounded delay. This conclusion holds despite any amount of cyclic rotation to either CH sequences.

For Combination 1 in Figure 1, one node employs a slow CH sequence while the other employs a fast one. This is the asymmetric CH protocol[2] *ACH* [3,6], where every node knows its pre-assigned role as a sender to use a fast CH sequence, or a receiver to use a slow one. In group theory, using two elements, such as $(1, 0)$ and $(0, 1)$, can easily generate the group $\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$. In ACH, the sender node uses the generator $(1, 0)$ to obtain its fast CH sequence while the receiver node uses the generator $(0, 1)$ to obtain its slow CH sequence, which collectively generate the group $\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$. The drawback is that two nodes create CH sequences in different/asymmetric ways, which necessitate pre-assigned roles.

For Combination 2 or 3 in Figure 1, both nodes choose a slow (or fast) CH sequence. When N_i and N_j are co-prime, they gaurantee maximum rendezvous diversity with a bounded delay by Chinese Remainder Theorem. We show that such designs with the channel number co-primality constraint meet the above design requirements in Section 3 and term them *elementary HCH systems*. These two designs are called ϵ_1- and ϵ_2-rendezvous in Section 3; ϵ stands for *elementary*.

However, it is impractical to assume that two rendezvous nodes happen to be pre-assigned the sender/receiver role, or meet the co-primality constraint on channel numbers N_i and N_j. In Section 4, we propose an advanced HCH system design, which meets the above design requirements and is independent of all aforementioned assumptions. The advanced design leverages the *symmetrization* technique that enables every node to create a bit string that determines how to interleave its fast and slow CH sequences. Based on Combination 1, this advanced design introduces the notion of *choice sequence* to symmetrize Combination 1 while preserving all its properties.

[2]An *asymmetric* protocol means that two nodes generate their CH sequences in different/asymmetric ways.

3. ELEMENTARY HCH SYSTEMS WITH CHANNEL NUMBER CO-PRIMALITY

In this section, we propose two *elementary* HCH systems, termed ϵ_1- and ϵ_2-rendezvous, both of which require co-primality of channels numbers N_i and N_j. We consider generating the group $\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$ in a symmetric way—using a single group generator. By Chinese Remainder Theorem, group $\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$ is cyclic if and only if N_i and N_j are co-prime; in this case, $\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j} = \mathbb{Z}_{N_iN_j}$.

3.1 CH Sequence Construction

ϵ_1-rendezvous. With N_i and N_j co-prime, $(1, 1)$ is a generator of the cyclic group $\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$. For every node $i \in \Lambda$, let $r(i, N_i)^t$ denote the channel index of its CH sequence in timeslot t, which is determined in ϵ_1-rendezvous as follows

$$r(i, N_i)^t = t \bmod N_i,$$

where $t \in [0, N_i - 1]$.

ϵ_2-rendezvous. Similarly, we propose another HCH system that requires N_i and N_j to be co-prime. For every node $i \in \Lambda$, the channel index of its CH sequence in timeslot t is determined in ϵ_2-rendezvous as follows

$$r(i, N_i)^t = \lfloor \frac{t}{N_i} \rfloor \bmod N_i,$$

where $t \in [0, N_i^2 - 1]$.

3.2 Robustness to Heterogeneous Environments

If nodes i and j employ ϵ_1- or ϵ_2-rendezvous, the common periods of their CH sequences are $T = N_iN_j$ and $N_i^2N_j^2$, re-

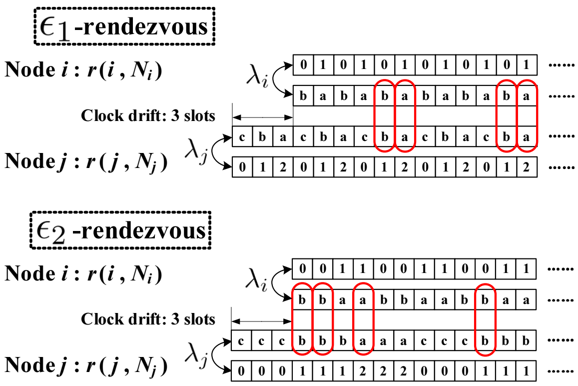

Figure 2: Nodes i and j have different labeling functions: $\lambda_i(b) = 0$, $\lambda_i(a) = 1$; $\lambda_j(c) = 0$, $\lambda_j(b) = 1$, $\lambda_j(a) = 2$. In ϵ_1-rendezvous: node i uses $r(i, 2) = \{0, 1\}$ while node j uses $r(j, 3) = \{0, 1, 2\}$. In ϵ_2-rendezvous: node i uses $r(i, 2) = \{0, 0, 1, 1\}$ while node j uses $r(j, 3) = \{0, 0, 0, 1, 1, 1, 2, 2, 2\}$.

spectively. Figure 2 illustrates examples of elementary HCH systems with $N_i = 2$ and $N_j = 3$. In Figure 2, two nodes rendezvous over all common channels (maximum diversity). The following theorem shows ϵ_1- and ϵ_2-rendezvous protocols' robustness to heterogeneous environments.

THEOREM 2. *For two nodes i and j with N_i and N_j co-prime, ϵ_1- and ϵ_2-rendezvous can guarantee maximum rendezvous diversity with a TTR bounded by N_iN_j and $N_i^2N_j^2$, respectively, despite any possible channel labeling functions and clock drifts.*

PROOF. ϵ_1**-rendezvous**. Suppose node j's clock is k timeslots behind that of node i. Let k' be k mod $N_j \in \mathbb{Z}_{N_j}$. Since $r(j, N_j)^t = t \bmod N_j$, we have $rotate(r(j, N_j), k) = r(j, N_j) + k'$, where the addition in the right-hand side means $r(j, N_j)$'s component-wise addition by k' in $\mathbb{Z}_{N_j}$ (For example, $\{0, 1, 2\} + 1 = \{1, 2, 0\}$ in $\mathbb{Z}_3$). Therefore, the sequence

$$\begin{aligned} & \{(r(i, N_i)^t, rotate(r(j, N_j), k)^t)\}_{t\in[0,T-1]} \\ = \ & \{t \cdot (1, 1)\}_{t\in[0,T-1]} + (0, k'). \end{aligned}$$

By Chinese Remainder Theorem, the group $\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$ is cyclic if and only if N_i and N_j are co-prime. Since $(1, 1)$ is a generator of the cyclic group $\mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$ and t runs from 0 to $T - 1 = N_iN_j - 1$, we have $\{t(1, 1)\}_{t\in[0,T-1]} = \mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$, thus

$$\begin{aligned} & \{(r(i, \mathbb{Z}_{N_i})^t, rotate(r(j, \mathbb{Z}_{N_j}), k)^t)\}_{t\in[0,T-1]} \\ = \ & \mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j} + (0, k') \\ = \ & \mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}. \end{aligned}$$

Since λ_i/λ_j is a 1-1 correspondence between the channel set C_i/C_j and the label set $\mathbb{Z}_{N_i}/\mathbb{Z}_{N_j}$, we have

$$\lambda_i^{-1}(\mathbb{Z}_{N_i}) \times \lambda_j^{-1}(\mathbb{Z}_{N_j}) = C_i \times C_j.$$

It follows immediately that it guarantees rendezvous with maximum diversity, irrespective of the clock drift and channel labeling functions.

ϵ_2**-rendezvous**. In ϵ_2-rendezvous, the common period of nodes i and j is $T = N_i^2 \cdot N_j^2$. Suppose node j's clock is k timeslots behind that of node i. Fix two integers $a \in [0, N_i - 1]$ and $b \in [0, N_j - 1]$ and consider the following simultaneous congruence equations

$$\begin{cases} \lfloor \frac{t}{N_i} \rfloor \equiv a \pmod{N_i} \\ \lfloor \frac{t+k}{N_j} \rfloor \equiv b \pmod{N_j}, \end{cases} \tag{1}$$

where $t \in [0, N_i^2 \cdot N_j^2 - 1]$. Suppose $t = qN_i^2 + r$, where $0 \le r < N_i^2$. We have $\lfloor \frac{t}{N_i} \rfloor = \lfloor \frac{qN_i^2+r}{N_i} \rfloor = qN_i + \lfloor \frac{r}{N_i} \rfloor$. Thus $\lfloor \frac{r}{N_i} \rfloor \equiv a \pmod{N_i}$. Since $0 \le r < N_i^2$, $0 \le \frac{r}{N_i} < N_i$, $0 \le \lfloor \frac{r}{N_i} \rfloor < N_i$. Note that $a \in [0, N_i - 1]$. We obtain that $\lfloor \frac{r}{N_i} \rfloor = a$ and that $aN_i \le r < (a + 1)N_i$. Hence Equation 1 is equivalent to

$$\begin{cases} t \equiv aN_i, \ldots, aN_i + (N_i - 1) \pmod{N_i^2} \\ t \equiv bN_j - k, \ldots, bN_j + (N_j - 1) - k \pmod{N_j^2}. \end{cases} \tag{2}$$

Since N_i and N_j are coprime, by Chinese Remainder Theorem, Equation 2 (and thus Equation 1) has $N_i \cdot N_j$ solutions up to modulo $N_i^2 \cdot N_j^2$. I.e., for each pair $(a, b) \in \mathbb{Z}_{N_i} \oplus \mathbb{Z}_{N_j}$, it appears in the sequence $\{(r(i, N_i)^t, r(j, N_j)^t)\}_{t\in[0,N_i^2\cdot N_j^2-1]}$ for N_iN_j times. It follows immediately that it guarantees rendezvous with maximum diversity, irrespective of the clock drift and channel labeling functions. □

Discussions. Theorem 2 implies that two nodes adopting ϵ_1- or ϵ_2-rendezvous can achieve rendezvous over all common channels in $C_i \cap C_j$ within a bounded time. The average TTR for both elementary HCH systems is the same, i.e., $\frac{N_iN_j}{|C_i \cap C_j|}$. However, the drawback of such elementary protocols is the requirement of channel number co-primality.

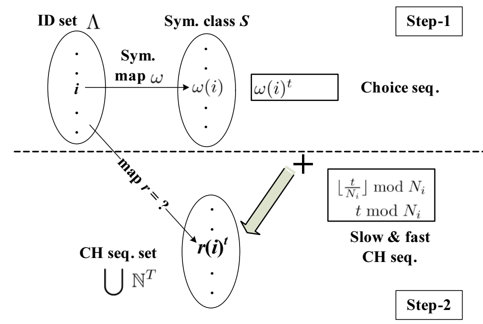

Figure 3: The relationship among ID set, symmetrization map, symmetrization class, and CH sequence, in the advanced HCH system design.

4. ADVANCED HCH SYSTEMS

In this section, we show how to construct the HCH system $H = (\Lambda, r)$ without any assumption on pre-assigned roles, or channel number co-primality. We use a two-step approach and illustrate this procedure in Figure 3.

4.1 A Two-step Approach

The first step is to create a *distinct* equilong bit string for each node i. Let ω be an *injective* map from the ID set Λ to the *bit string* set S that assigns a bit string $\omega(i) \in S$ to each node $i \in \Lambda$. Nodes i and j's bit strings $\omega(i)$ and $\omega(j)$ are said to be *distinct* if they have at least one bit different after any amount of cyclic rotation; in other words, $\omega(i) \neq rotate(\omega(j), k)$, $\forall k \in \mathbb{N}$. If any two bit strings in S are

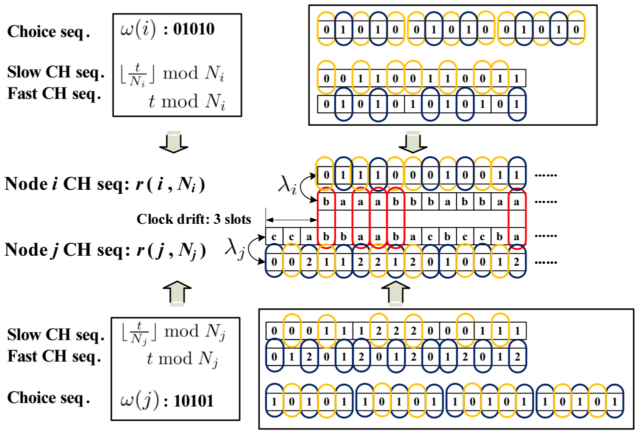

Figure 4: In the advanced HCH design, nodes i and j use $\omega(i) = \{0,1,0,1,0\}$ and $\omega(j) = \{1,0,1,0,1\}$ to construct their CH sequences respectively. For three channels with central frequencies at a, b and c, nodes i and j have different labeling functions: $\lambda_i(b) = 0$, $\lambda_i(a) = 1$; $\lambda_j(c) = 0$, $\lambda_j(b) = 1$, $\lambda_j(a) = 2$.

distinct, we term the *injective* map ω a *symmetrization map* and the bit string set S a *symmetrization class*. Meanwhile, an element (a *bit string*) in S is called a *choice sequence*.

The second step for node i is to use its choice sequence to interleave its slow and fast CH sequences to obtain $r(i, N_i)$—i.e., to choose whether the slow or fast CH sequence should be used in the current timeslot of $r(i, N_i)$. In Figure 4, node i has $N_i = 2$ sensible channels, and it has constructed a slow and a fast CH sequence. The slow CH sequence visits channel ($\lfloor \frac{t}{2} \rfloor$ mod 2) in the t-th timeslot (note that we start from the 0th timeslot)

$$00110011\cdots,$$

and the fast CH sequence visits channel (t mod 2) in the t-th timeslot

$$01010101\cdots.$$

Suppose its choice sequence is $\omega(i) = 01010$. In the t-th slot, node i chooses the channel index in the t-th slot of its corresponding fast (or slow) CH sequence if the t-th bit of its choice sequence is 1 (or 0). For example, since the 0th bit of $\omega(i)$ is 0, node i chooses the channel index of the 0th slot in its slow CH sequence (which is channel index 0). Similarly, since the 1st bit of $\omega(i)$ is 1, node i chooses the channel index of the 1st slot in its fast CH sequence (which is channel index 1).

In the following subsections, we will elaborate on how to construct a choice sequence and CH sequence.

4.2 Existence of Symmetrization Class

Let $\mathbb{F}_2$ denote the Galois field of size 2, and $\mathbb{F}_2^l$ denote the set of all bit strings with length l. $G = \{rotate(\cdot, k) | k \in [0, l-1]\}$ is a cyclic group acting on $\mathbb{F}_2^l$. For $rotate(\cdot, k) \in G$ and $\sigma \in \mathbb{F}_2^l$, the group action $\circ$ is defined by $rotate(\cdot, k) \circ \sigma \triangleq rotate(\sigma, k)$. The orbit of $\sigma \in \mathbb{F}_2^l$ is denoted by $G \circ \sigma$

$$G \circ \sigma \triangleq \{g \circ \sigma | g \in G\} \equiv \{rotate(\sigma, k) | k \in [0, l-1]\}.$$

A subset $S \subseteq \mathbb{F}_2^l$ is said to be an l-*symmetrization class* if it contains distinct bit strings with length l—$\forall \sigma, \tau \in S$, $\sigma \neq \tau$ implies $(G \circ \sigma) \cap (G \circ \tau) = \varnothing$, i.e., $\forall k \in [0, l-1]$, $\sigma \neq rotate(\tau, k)$. Elements in S are called *choice sequences*. For example, when $l = 3$, $S = \{000, 001, 011, 111\}$ is a 3-symmetrization class; however, $S = \{000, 001, 010, 011\}$ is not a 3-symmetrization class because $rotate(001, 1) = 010$.

We define the *rotation Hamming distance* δ_H in $\mathbb{F}_2^l$ such as: for $u, v \in \mathbb{F}_2^l$,

$$\delta_H(u, v) \triangleq \min_{k \in \mathbb{Z}} d_H(u, rotate(v, k)),$$

where d_H is the Hamming distance in $\mathbb{F}_2^l$.

The *degree* of a subset $F \subseteq \mathbb{F}_2^l$, $\delta(F)$, is defined such as $\delta(F) \triangleq \min_{u,v \in F, u \neq v} \delta_H(u, v)$. If $S \subseteq \mathbb{F}_2^l$ is a symmetrization class, $\delta(S) \geq 1$. In other words, any two sequences in S are distinct.

The following lemma shows the existence of an l-symmetrization class for $\forall l \in \mathbb{N}$.

Lemma 1. *$\forall l \in \mathbb{N}$, there exists an l-symmetrization class. $\forall M \in \mathbb{N}$, there exists $l \in \mathbb{N}$ and an l-symmetrization class S_l such that $|S_l| \geq M$.*

Proof. Given $l \in \mathbb{N}$, let $\mathbb{F}_2^l/G \triangleq \{G \circ \sigma | \sigma \in \mathbb{F}_2^l\}$ be the set of all orbits in $\mathbb{F}_2^l$ under the action of group G. The number of cycles of group element $g = rotate(\cdot, k) \in G$ as a permutation in $\mathbb{F}_2^l$ is $\gcd(k, l)$. By Polya Enumeration Theorem, $|\mathbb{F}_2^l/G| = \frac{1}{|G|}\sum_{k=0}^{l-1} 2^{\gcd(k,l)} = \frac{1}{l}\sum_{k=0}^{l-1} 2^{\gcd(k,l)} = \frac{1}{l}\sum_{d|l}\varphi(d)2^{l/d} \geq 2^l/l$. Suppose

$$\mathbb{F}_2^l/G = \{\Sigma_1, \Sigma_2, \ldots, \Sigma_{|\mathbb{F}_2^l/G|}\},$$

and let S_l be$\{\sigma_1, \sigma_2, \ldots, \sigma_{|\mathbb{F}_2^l/G|}\}$ with $\sigma_i \in \Sigma_i$. We conclude that S_l is an l-symmetrization class. Given $M \in \mathbb{N}$, $\exists l \in \mathbb{N}$ s.t. $2^l/l \geq M$, and then S_l is an l-symmetrization class and $|S_l| \geq M$. $\square$

4.3 Construction of Symmetrization Classes And Choice Sequences

Suppose S is a sufficiently large l-symmetrization class for some $l \in \mathbb{N}$, we term

$$\omega : \Lambda \to S$$

a symmetrization map if ω is injective. Intuitively, ω assigns a choice sequence to each node $i \in \Lambda$. Note that any two bit strings in S are distinct. Since ω is injective, for two different nodes i and j, $\omega(i)$ and $\omega(j)$ are distinct bit strings.

Next, we show both centralized and distributed algorithms to construct choice sequences based on a few example symmetrization classes.

A centralized algorithm for optimal (minimum) l-symmetrization class. For $l \in \mathbb{N}$, S_l in the proof of Lemma 1 is called an optimal l-symmetrization class. Given an ID set Λ, we need to find a sufficiently large l such that we can construct a symmetrization map ω from Λ to S_l. To be precise, since $|S_l| = \frac{1}{l}\sum_{d|l}\varphi(d)2^{l/d} \geq 2^l/l$, we have $|S_l| \geq |\Lambda|$ if $l - \log_2 l \geq \log_2 |\Lambda|$. In this case, there exists an injective map ω from Λ to S_l. S_l is optimal in the sense that it achieves the minimum l to guarantee the existence of a symmetrization map, where the minimum $l \approx g + \log_2 g$ with $g = \lceil \log_2 |\Lambda| \rceil$.

Suppose we have four nodes whose IDs are 00, 01, 10 and 11, respectively. Since $10 = rotate(01, 1)$, we need to assign each of them a distinct bit string. In

$$\mathbb{F}_2^3 = \{000, 001, 010, 011, 100, 101, 110, 111\},$$

for example, elements 001, 010 and 100 are identical under cyclic rotation, so only one of them, say 001, is preserved in the 3-symmetrization class, while the rest of them, 010 and 100, are eliminated. In this manner, we can obtain the optimal 3-symmetrization class $S_3 = \{000, 001, 011, 111\}$, and thus build a symmetrization map $\omega : \mathbb{F}_2^2 \to S_3$ for the four nodes: $\omega(00) = 000$, $\omega(01) = 001$, $\omega(10) = 011$ and $\omega(11) = 111$.

However, the calculation of the optimal symmetrization class requires a centralized controller or that nodes' choice sequences (i.e., bit strings) be pre-assigned. Next, we present two distributed algorithms that allow each node to generate its choice sequence autonomously. Given an ID set Λ, every node can represent its ID to be a $\lceil \log_2 |\Lambda| \rceil$-bit string, i.e. it can construct an injective map

$$\pi : \Lambda \to \mathbb{F}_2^g,$$

where $g = \lceil \log_2 |\Lambda| \rceil$ is the ID length[3].

A distributed algorithm for η_1 symmetrization class. Each node i can generate a $(2g+3)$-bit string using the symmetrization map ω

$$\omega : \Lambda \to \mathbb{F}_2^{2g+3},$$

where

$$\forall i \in \Lambda, \omega(i) \triangleq \pi(i)10^{g+1}1.$$

For any two nodes i and j, their $(2g+3)$-bit strings are distinct. We term $Z \triangleq \{u10^{g+1}1 | u \in \mathbb{F}_2^g\}$ an η_1 symmetrization class. Note that the η_1 symmetrization map can be efficiently computed by each node in one iteration.

For example, suppose node i's ID is a 6-bit string 110110, i.e. $\pi(i) = 110110$ and we have $g = |\pi(i)| = 6$. Then its choice sequence will be

$$\omega(i) = \pi(i)10^{g+1}1 = \pi(i)10^7 1 = 110110100000001.$$

A distributed algorithm for η_2 symmetrization class. Here we present the η_2 symmetrization class with $l = g + \lceil \sqrt{g} \rceil (2 + \lceil \log_2 g \rceil) + 3$, where $g = \lceil \log_2 \Lambda \rceil$.

Let $\mathbf{b}_h^{(\lceil \log_2 g \rceil)}$ be the $\lceil \log_2 g \rceil$-bit binary representation of natural number h with $h \leq g$. An auxiliary map η_2 is defined on $\bigcup_{h=0}^{g} \{0^h\}$, i.e., the zero strings, such as

$$\eta_2(0^h) = \begin{cases} 0^h & \text{if } h < \lceil \sqrt{g} \rceil; \\ 0^{\lceil \sqrt{g} \rceil} 1 \mathbf{b}_h^{(\lceil \log_2 g \rceil)} & \text{if } h \geq \lceil \sqrt{g} \rceil. \end{cases}$$

For each node $i \in \Lambda$, suppose

$$\pi(i) = \prod_{k=1}^{K} 1^{o_k} 0^{z_k} \triangleq 1^{o_1} 0^{z_1} 1^{o_2} 0^{z_2} \cdots 1^{o_K} 0^{z_K},$$

where $\forall k \in [1, K]$, $o_k, z_k \geq 0$ and $\sum_{k=1}^{K} (o_k + z_k) = g$.

Then we define the map $\tilde{\eta_2} : \Lambda \to \bigcup_{n=g}^{\infty} \mathbb{F}_2^n$ such as

$$\forall i \in \Lambda, \tilde{\eta_2}(i) \triangleq \prod_{k=1}^{K} 1^{o_k} \eta_2(0^{z_k}).$$

We compute the ratio of lengths of $\eta_2(0^h)$ to 0^h such as

$$\frac{|\eta_2(0^h)|}{|0^h|} = \frac{\lceil \sqrt{g} \rceil + 1 + \lceil \log_2 g \rceil}{h} \leq \frac{\lceil \sqrt{g} \rceil + 1 + \lceil \log_2 g \rceil}{\lceil \sqrt{g} \rceil},$$

[3]Network nodes' IDs are usually equilong. Map π can be perceived as assigning an ID to each device, so it must be injective. g is the ID length.

and the ratio of lengths of $\tilde{\eta_2}(i)$ to $\pi(i)$ such as

$$\frac{|\tilde{\eta_2}(i)|}{g} = \frac{|\tilde{\eta_2}(i)|}{|\pi(i)|} \leq \frac{\lceil \sqrt{g} \rceil + 1 + \lceil \log_2 g \rceil}{\lceil \sqrt{g} \rceil}.$$

We obtain an upper-bound estimation of the length of $\tilde{\eta_2}(i)$, such as

$$|\tilde{\eta_2}(i)| \leq g \cdot \frac{\lceil \sqrt{g} \rceil + 1 + \lceil \log_2 g \rceil}{\lceil \sqrt{g} \rceil} \leq g + \lceil \sqrt{g} \rceil (1 + \lceil \log_2 g \rceil).$$

On basis of the derived bound for the length of $\tilde{\eta_2}(i)$, we let $l = g + \lceil \sqrt{g} \rceil (2 + \lceil \log_2 g \rceil) + 3$, and construct the symmetrization map $\omega : \Lambda \to \mathbb{F}_2^l$ whereby each node i autonomously generates its choice sequence

$$\omega(i) \triangleq \tilde{\eta_2}(i)10^a 1,$$

with $a = l - |\tilde{\eta_2}(i)| - 2 \geq \left[g + \lceil \sqrt{g} \rceil (2 + \lceil \log_2 g \rceil) + 3\right] - \left[g + \lceil \sqrt{g} \rceil (1 + \lceil \log_2 g \rceil)\right] - 2 = \lceil \sqrt{g} \rceil + 1$.

For any two nodes i and j, their choice sequences are distinct bit strings. We term the set of such bit strings an η_2 symmetrization class.

For instance, suppose node i's ID is an 8-bit string $\pi(i) = 00001001$, with $g = |\pi(i)| = 8$ and $\lceil \sqrt{g} \rceil = 3$. The length of its choice sequence is $l = g + \lceil \sqrt{g} \rceil (2 + \lceil \log_2 g \rceil) + 3 = 8 + 3 \times (2 + 3) + 3 = 26$. $\pi(i)$ can be represented as $\pi(i) = 00001001 = 0^4 10^2 1$. Since $4 \geq \lceil \sqrt{g} \rceil = 3$, $\eta_2(0^4) = 0^3 1100 = 0001100$, where the last three digits 100 is the 3-bit binary representation of 4. Since $2 < \lceil \sqrt{g} \rceil = 3$, $\eta_2(0^2) = 0^2 = 00$. Then we have

$$\tilde{\eta_2}(i) = \eta_2(0^4) 1 \eta_2(0^2) 1 = 00011001001.$$

$|\tilde{\eta_2}(i)| = 11$, then $a = l - |\tilde{\eta_2}(i)| - 2 = 26 - 11 - 2 = 13$. Thus node i's choice sequence is

$$\omega(i) = \tilde{\eta_2}(i) 10^{13} 1 = 00011001001100000000000001.$$

4.4 Interleaving Slow and Fast CH Sequences

In this subsection, we present the approach to constructing a CH sequence $r(i, N_i)$ for each node i. As aforementioned, node i constructs its choice sequence via a chosen symmetrization map $\omega : \Lambda \to S$.

Initially, we need to make sure that node i's channel number N_i is a prime number and coprime to the length of the choice sequence l, i.e., $\gcd(N_i, l) = 1$. Through a remapping scheme [12, 13], we can increase N_i to the smallest prime number greater than or equal to N_i and co-prime to l, i.e., $N_i \leftarrow \min\{p \in \mathbb{N} | \text{ prime } p \geq N_i, \gcd(p, l) = 1\}$.

Now we demonstrate how to combine *slow/fast* CH sequences using the choice sequence $\omega(i)$. In timeslot t (t starts from 0), the channel index of its CH sequence, $r(i, N_i)^t$, is calculated in accordance with the choice sequence $\omega(i)$:

- If the ($t \bmod l$)-th bit of $\omega(i)$ is 0, then the node visits channel ($\lfloor \frac{t}{N_i} \rfloor \bmod N_i$) in timeslot t (i.e., uses the t-th element in the slow sequence). In other words, if $\omega(i)^{t \bmod l} = 0$, let $r(i, N_i)^t = \lfloor \frac{t}{N_i} \rfloor \bmod N_i$;

- If the ($t \bmod l$)-th bit of $\omega(i)$ is 1, then the node visits channel ($t \bmod N_i$) in timeslot t (i.e., uses the t-th element in the fast sequence). In other words, if $\omega(i)^{t \bmod l} = 1$, let $r(i, N_i)^t = t \bmod N_i$.

The channel index in this advanced HCH system design is jointly determined by the choice sequence, the current time slot t, and N_i, which is independent of which channels are available to node i (i.e., the set C_i), or the way of assigning channel indices.

Robustness to heterogeneous environments. Figure 4 illustrates an example of the advanced HCH system when $N_i = 2$ and $N_j = 3$. The following theorem proves its rendezvous robustness to various network conditions.

THEOREM 3. *For two nodes i and j, the advanced HCH protocol using an l-symmetrization class can guarantee the maximum rendezvous diversity within a TTR bounded by lN_iN_j, irrespective of all possible channel labeling functions and clock drifts.*

PROOF. Given two nodes i and j, suppose node j's is k timeslots behind that of node i. According to node i's clock, group every $l = |\omega(i)| = |\omega(j)|$ timeslots into a frame, i.e., timeslots $0, 1, 2, \ldots, l-1$ form the first frame, timeslots $l, l+1, l+2, \ldots, 2l-1$ form the second frame, etc. Timeslot t is contained in the $\lfloor t/l \rfloor$-th frame.

By the definition of symmetrization class, there exists $c \in [0, l-1]$ such that $\omega(i)^c \neq rotate(\omega(j), k)^c$. Without loss of generality, assume $\omega(i)^c = 0$ and $rotate(\omega(j), k)^c = 1$. Now we focus on timeslots $c + Fl$ with $F = 0, 1, 2, 3, \ldots$. The resulting subsequence of $\{(r(i, N_i)^t, r(j, N_j)^{t+k})\}_{t\geq 0}$ is $\{(r(i, N_i)^{c+Fl}, r(j, N_j)^{c+Fl+k})\}_{F\geq 0}$. By the definition of r, $\{(r(i, N_i)^{c+Fl}, r(j, N_j)^{c+Fl})\}_{F\geq 0}$ equals

$$\{(\lfloor \frac{c+Fl}{N_i} \rfloor \bmod N_i, (c+Fl+k) \bmod N_j)\}_{F\geq 0},$$

Fix two integers $a \in [0, N_i - 1]$ and $b \in [0, N_j - 1]$ and consider the following simultaneous congruence equations with respect to F

$$\begin{cases} \lfloor \frac{c+Fl}{N_i} \rfloor \equiv a \pmod{N_i} \\ c + Fl + k \equiv b \pmod{N_j}, \end{cases} \tag{3}$$

Suppose $c + Fl = qN_i^2 + r$ with $0 \leq r < N_i^2$. We have $\lfloor \frac{c+Fl}{N_i} \rfloor = \lfloor \frac{qN_i^2+r}{N_i} \rfloor = qN_i + \lfloor \frac{r}{N_i} \rfloor$. Thus $\lfloor \frac{r}{N_i} \rfloor \equiv a \pmod{N_i}$. Since $0 \leq r < N_i^2$, $0 \leq \frac{r}{N_i} < N_i$, $0 \leq \lfloor \frac{r}{N_i} \rfloor < N_i$. Note that $a \in [0, N_i - 1]$. We obtain that $\lfloor \frac{r}{N_i} \rfloor = a$ and that $aN_i \leq r < (a+1)N_i$. Hence Equation 3 is equivalent to

$$\begin{cases} c + Fl \equiv aN_i, \ldots, aN_i + N_i - 1 \pmod{N_i^2} \\ c + Fl + k \equiv b \pmod{N_j}. \end{cases}$$

Since $\gcd(N_i, l) = 1$ and therefore $\gcd(N_i^2, l) = 1$, we have $\exists l^{-1}_{\mathbb{Z}_{N_i^2}} \in \mathbb{Z}$, s.t. $l^{-1}_{\mathbb{Z}_{N_i^2}} l \equiv 1 \pmod{N_i^2}$. Similarly, since $\gcd(N_j, l) = 1$, we have $\exists l^{-1}_{\mathbb{Z}_{N_j}} \in \mathbb{Z}$, s.t. $l^{-1}_{\mathbb{Z}_{N_j}} l \equiv 1 \pmod{N_j}$.

$$\begin{cases} F \equiv l^{-1}_{\mathbb{Z}_{N_i^2}} (aN_i + g - c) \pmod{N_i^2} \qquad g \in [0, N_i - 1] \\ F \equiv l^{-1}_{\mathbb{Z}_{N_j}} (b - c - k) \pmod{N_j}. \end{cases}$$

There are two possible cases to consider.

Case 1: $N_i = N_j$. $\exists g_0 \in [0, N_i - 1]$ s.t. $l^{-1}_{\mathbb{Z}_{N_i^2}} (aN_i + g_0 - c) \equiv l^{-1}_{\mathbb{Z}_{N_j}} (b - c - k) \pmod{N_i}$. Thus $F \equiv l^{-1}_{\mathbb{Z}_{N_i^2}} (aN_i + g_0 - c) \pmod{N_i^2}$.

Case 2: $N_i \neq N_j$. Since N_i and N_j are both primes, we have $\gcd(N_i, N_j) = 1$, and thus $\gcd(N_i^2, N_j) = 1$. By Chinese Remainder Theorem, we obtain that there exists N_i solutions modulo $N_i^2 N_j$.

Table 1: A comparison of CH schemes in heterogeneous environments.

CH protocol	Assumption	Diversity	Avg. TTR
ACH [4]	Sdr/Rvr role; equal/co-prime chan. num.	$\|C_i \cap C_j\|$	$\frac{N_iN_j}{\|C_i \cap C_j\|}$
HH [14] ICH [13]	Univ. set; consec. chan. indices	No max diversity	$O(N_iN_j)$
ϵ_1- or ϵ_2-ele. rdv	Chan. num. co-primality	$\|C_i \cap C_j\|$	$\frac{N_iN_j}{\|C_i \cap C_j\|}$
Adv. rdv		$\|C_i \cap C_j\|$	$\frac{lN_iN_j}{\delta\|C_i \cap C_j\|}$

Table 2: A comparison of different symmetrization classes in the advanced HCH protocol.

Symmetrization class	Degree δ	Choice sequence length l
Optimal	≥ 1	$\approx g + \log_2 g$
η_1	≥ 1	$2g + 3$
η_2	≥ 1	$g + \lceil \sqrt{g} \rceil (2 + \lceil \log_2 g \rceil) + 3$

It follows immediately that it guarantees rendezvous with maximum diversity, despite any amount of clock drift and heterogeneity of channel labeling functions. □

5. PERFORMANCE EVALUATION

5.1 Comparisons of CH-based Rendezvous Protocols in Heterogeneous Environments

A comparison of existing and proposed rendezvous protocols schemes in heterogeneous environments is summarized in Table 1.

Assumptions vs. rendezvous performance. Existing protocols can partially address the rendezvous problem due to dependency on some assumptions. For example, the ACH protocol assumes the pre-assigned role of a node, which limits its application scenarios (e.g., bluetooth pairing). HH and ICH schemes [13,14] assume that each node can sense a set of consecutive channels that come from a universal spectrum; meanwhile, they fail to achieve the maximum rendezvous diversity. The elementary HCH protocols proposed in this paper can achieve the maximum rendezvous diversity $|C_i \cap C_j|$ with an average TTR (ATTR) of $\frac{N_iN_j}{|C_i \cap C_j|}$. However, channel number co-primality is assumed. The advanced HCH protocol is independent of these environmental assumptions, while it can achieve the maximum rendezvous diversity $|C_i \cap C_j|$, with ATTR $\frac{lN_iN_j}{\delta|C_i \cap C_j|}$. Recall that l is the length of the choice sequence and δ is the degree of the symmetrization class. l and δ vary with different symmetrization classes. The advanced HCH protocol incurs a mere performance degradation of a constant factor, l/δ. For a 4-bit ID string, $l/\delta \leq 4 + \log_2 4 = 6$ for the optimal symmetrization class. A comparison of all aforementioned symmetrization classes is summarized in Table 2.

5.2 Simulation Results

In this section, we compare the performance of existing and proposed rendezvous schemes via simulation results.

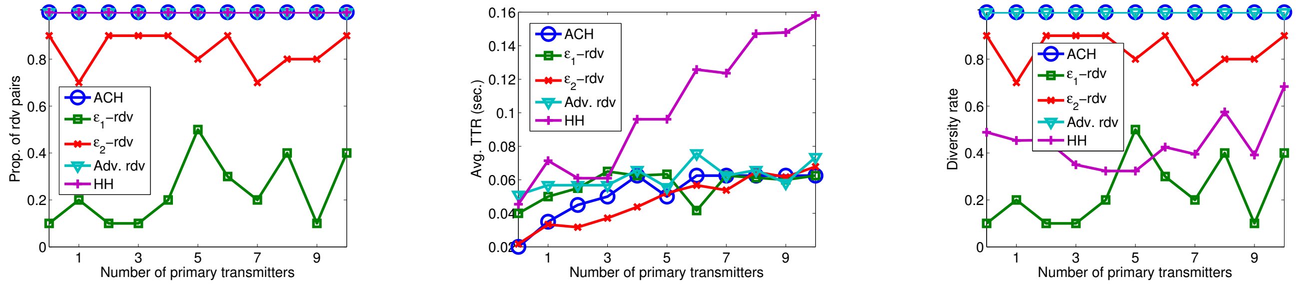

Figure 5: Results in Case 1 with pre-assigned sender/receiver roles, but no channel number co-primality: (a) The proportion of rendezvous pairs; (b) The average rendezvous latency for successful rendezvous pairs; (c) The diversity rate.

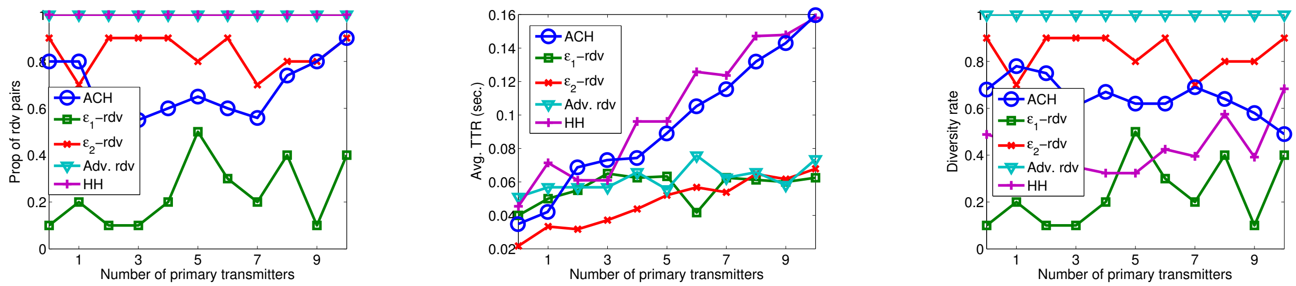

Figure 6: Results in Case 2 with no pre-assigned sender/receiver roles, and no channel number co-primality: (a) The proportion of rendezvous pairs; (b) The average rendezvous latency for successful rendezvous pairs; (c) The diversity rate.

There are a total number of $N = 11$ frequency channels, and 20 pairs of nodes that need to rendezvous via channel hopping. Every node i can only sense and access a number of N_i channels, and its sensible channel set is C_i, where N_i is randomly chosen from $[1, 11]$. The channel labeling function is independently determined by each node. Meanwhile, each node determines its clock time independently, and there is a random clock drift between any two nodes. A node generates its CH sequence using the agreed CH scheme and performs channel hopping in accordance with the CH sequence. The advanced HCH protocol in simulations is based on the η_1 symmetrization class. We simulated $X < N$ primary transmitters operating on X randomly chosen channels. A timeslot has a length of 10 ms. All secondary nodes are within the transmission range of any primary transmitter. A channel is deemed *unavailable* when primary user signals are present on it. Once two nodes hop onto a primary-user free channel in the same timeslot, the rendezvous between them is established.

We employ the following three metrics to evaluate the performance of rendezvous protocols. (1) We define the *proportion of rendezvous pairs* as the percentage of successful rendezvous pairs in all node pairs that attempt to rendezvous; (2) We use the *average time-to-rendezvous* (ATTR) to measure the average rendezvous latency of successful rendezvous pairs; (3) We define the *diversity rate* of two nodes i and j as $\frac{|\mathcal{C}|}{|(C_i \cap C_j) \setminus C_{PU}|}$, where $|\mathcal{C}|$ is the number of rendezvous channels between nodes i and j, and C_{PU} denotes the set of channels on which PUs appear. The diversity rate quantifies a CH scheme's ability to establish rendezvous in diverse possible channels.

5.2.1 *Case 1: pre-assigned sender/receiver roles; no channel number co-primality*

In this case, every node has a pre-assigned role as a sender or a receiver. For any rendezvous node pairs, the sender node, say node i, uses the sender CH sequence $r_s(i, N_i)$; the receiver node, say node j, uses the receiver CH sequence $r_r(j, N_j)$[4]. The co-primality of channel numbers N_i and N_j is not guaranteed. The results are shown in Figure 5.

Proportion of rendezvous pairs. From Figure 5(a), we can see that ACH, ICH and the proposed advanced rendezvous protocol guarantee that every pair of radios successfully rendezvous while ϵ_1- and ϵ_2-rendezvous protocols cannot guarantee that without assuming channel number co-primality.

Average time-to-rendezvous. From Figure 5(b), we can observe that ACH, ϵ_1-/ϵ_2-rendezvous and the advanced rendezvous protocol come very close in terms of ATTR; however, as the number of primary transmitters increases, the average time-to-rendezvous of the ICH scheme increases rapidly due to its limited rendezvous diversity (see Table 1).

[4]In *symmetric* protocols that are independent of pre-assigned roles (e.g., the advanced HCH protocol), $r_s(i, N_i) = r_r(i, N_i) = r(i, N_i)$. Our definition of HCH protocols (Definition 1) focuses on symmetric protocols only because it is unjustifiable to assume pre-assigned roles in practical systems.

Diversity rate. Figure 5(c) shows that ACH and the proposed advanced rendezvous protocol achieve maximum diversity of rendezvous channels; however, ICH, ϵ_1 and ϵ_2 fail to achieve maximum rendezvous diversity. Specifically, ϵ_1-/ϵ_2-rendezvous fails because we do not assume channel number co-primality in this set of simulations.

5.2.2 *Case 2: no pre-assigned sender/receiver roles, and no channel number co-primality*

In this case, every node has no pre-assigned role as a sender/receiver, and node i in ACH randomly selects $r_s(i, N_i)$ or $r_r(i, N_i)$ as its CH sequence. The results in this case are illustrated in Figure 6.

Proportion of rendezvous pairs. Figure 6(a) shows that without assuming pre-assigned sender/receiver roles, ACH cannot guarantee rendezvous for every node pair when both of them select sender (or receiver) sequences simultaneously. When N_i and N_j are not co-prime, ϵ_1- and ϵ_2-rendezvous protocols fail to guarantee rendezvous for all node pairs. In contrast, ICH and the proposed advanced rendezvous protocols can ensure all node pairs to achieve pairwise rendezvous in such a heterogeneous environment.

Average time-to-rendezvous. In Figure 6(b), we measure ATTR for successful rendezvous pairs. Although the ICH scheme leads to a high proportion of rendezvous pairs, we can observe that as the number of primary transmitters increases, the ATTR of ICH increases rapidly. Moreover, in ϵ_1-/ϵ_2- rendezvous protocols, a few node pairs fail to achieve rendezvous (low proportion of rendezvous pairs), but the rendezvous latency for those successful rendezvous pairs is as small as that of the advanced rendezvous protocol.

Diversity rate. In Figure 6(c), two nodes using ACH (no pre-assigned roles are assumed), ϵ_1/ϵ_2-rendezvous (N_i and N_j may not be co-prime), or ICH protocol fail to achieve the maximum rendezvous diversity; therefore the diversity rate is lower than 1 for these protocols. In contrast, the advanced rendezvous protocol is uniquely able to guarantee the maximum rendezvous diversity.

In sum, without assuming pre-assigned sender/receiver roles or channel number co-primality, the proposed advanced rendezvous protocol is uniquely able to guarantee rendezvous between every pair of nodes with the maximum diversity rate and a small average time-to-rendezvous.

6. CONCLUSIONS

This paper presents a systematic approach using group theory for designing optimal CH protocols that guarantee the maximum rendezvous diversity and the minimal TTR in CR networks. We show the minimum upper bound for TTR is N_iN_j, and propose two types of rendezvous protocols that achieve the maximum rendezvous diversity with a latency of $O(N_iN_j)$. Analytical and simulation results show that these protocols are resistant to rendezvous failures in heterogeneous network conditions.

7. ACKNOWLEDGEMENTS

This work was partially supported by National Natural Science Foundation of China under grant number 61201245, Specialized Research Fund for the Doctoral Program of Higher Education (SRFDP) under grant 20120001120128, and by the National Science Foundation through grants CNS-1314598 and IIP-1265886.

8. REFERENCES

[1] C. Arachchige, S. Venkatesan, and N. Mittal. An Asynchronous Neighbor Discovery Algorithm for Cognitive Radio Networks. Proc. of *IEEE DySPAN*, pp. 1–5, 2008.

[2] P. Bahl, R. Chandra, and J. Dunagan. SSCH: Slotted Seeded Channel Hopping for Capacity Improvement in IEEE 802.11 Ad Hoc Wireless Networks. Proc. of *ACM MobiCom*, pp. 216–230, 2004.

[3] K. Bian and J. Park. Asynchronous Channel Hopping for Establishing Rendezvous in Cognitive Radio Networks. Proc. of *IEEE INFOCOM*, Mini-conference, pp. 236–240, 2011.

[4] K. Bian and J. Park. Maximizing Rendezvous Diversity in Rendezvous Protocols for Decentralized Cognitive Radio Networks. *IEEE Trans. on Mobile Computing*, 12(7):1294–1307, July 2013.

[5] K. Bian, J. Park, and R. Chen. A Quorum-based Framework for Establishing Control Channels in Dynamic Spectrum Access Networks. Proc. of *ACM MobiCom*, pp. 25–36, 2009.

[6] K. Bian, J. Park, and R. Chen. Control Channel Establishment in Cognitive Radio Networks using Channel Hopping. *IEEE Journal on Selected Areas of Communications*, 29(4):689–703, April 2011.

[7] G. Chang, W. Teng, H. Chen, and J. Sheu. Novel Channel-Hopping Schemes for Cognitive Radio Networks. *IEEE Transactions on Mobile Computing*, 13(2):407–421, February 2014.

[8] I.-H. Chuang, H.-Y. Wu, K.-R. Lee, and Y. H. Kuo. Alternate Hop-and-Wait Channel Rendezvous Method for Cognitive Radio Networks. Proc. of *IEEE INFOCOM*, pp. 746–754, 2013.

[9] F. Hou, L. Cai, X. S. Shen, and J. Huang. Asynchronous Multichannel MAC Design With Difference-Set-Based Hopping Sequences. *IEEE Transactions on Vehecular Technology*, 60(4):1728–1739, May 2011.

[10] Z. Lin, H. Liu, X. Chu, and Y.-W. Leung. Jump-Stay Based Channel Hopping Algorithm with Guaranteed Rendezvous for Cognitive Radio Networks. Proc. of *IEEE INFOCOM*, pp. 2444–2452, 2011.

[11] Y. Song and J. Xie. A Distributed Broadcast Protocol in Multi-hop Cognitive Radio Ad Hoc Networks without A Common Control Channel. *Proc. IEEE INFOCOM*, pp. 2273–2281, 2012.

[12] N. Theis, R. Thomas and L. DaSilva. Rendezvous for Cognitive Radios. *IEEE Transactions on Mobile Computing*, 10(2):216–227, 2011.

[13] C.-C. Wu, and S.-H. Wu. On Bidging the Gap between Homogeneous and Heterogeneous Rendezvous Schemes for Cognitive Radios. Proc. of *ACM MobiHoc*, pp. 207–216, 2013.

[14] S.-H. Wu, C.-C. Wu, W.-K. Hon, and K. G. Shin. Rendezvous for Heterogeneous Cognitive Radios: Theoretical Foundations. Technical report, 2013.

[15] Y. Zhang, Q. Li, G. Yu, and B. Wang. ETCH: Efficient Channel Hopping for Communication Rendezvous in Dynamic Spectrum Access Networks. Proc. of *IEEE INFOCOM*, 2011.