Shift-Invariant Protocol Sequences for the Collision Channel Without Feedback

Kenneth W. Shum, *Member, IEEE*, Chung Shue Chen, *Member, IEEE*, Chi Wan Sung, *Member, IEEE*, and Wing Shing Wong, *Fellow, IEEE*

***Abstract*—We consider collision channel without feedback in which collided packets are considered unrecoverable. For each user, the transmission of packets follows a specific periodical pattern, called the protocol sequence. Due to the lack of feedback, the beginning of the protocol sequences cannot be synchronized and nonzero relative offsets are inevitable. It results in variation of throughput. In this paper, we investigate optimal protocol sequence sets, in the sense that the throughput variance is zero. Such protocol sequences are said to be shift-invariant (SI). The characterizing properties of SI protocol sequences are presented. We also prove that SI sequences are identifiable, meaning that the receiver is able to determine the sender of each successfully received packet without any packet header. A general construction of SI sequences that meets the lower bound on sequence length is given. Besides, we study the least periods of SI sequences, and show that the least periods must be distinct in some cases. The throughput performance is compared numerically with other protocol sequences.**

***Index Terms*—Collision channel without feedback, protocol sequences.**

I. Introduction

In the context of multiaccess communication, random accessing has attracted many research activities due to its simplicity and effectiveness in different systems and applications [1]–[6]. In a shared channel, when two or more users transmit without coordination, collisions will occur generally. For example, in slotted ALOHA, where each user sends out a packet independent of the others, packet collisions cannot be avoided. To have a collision-free transmission, one may use a rigid protocol such as time division multiple access (TDMA). However, this may not be practical sometimes due to stringent time synchronization requirement. Contention based random access protocols such as IEEE 802.11 CSMA/CA [7] can provide a more flexible transmission scheme. However, they require some backoff algorithms and a feedback link to provide a reliable and stable communication channel.

For system simplicity, it is desirable to have a simple multiple access protocol which does not require stringent time synchronization, frequent channel monitoring, and complicated processing such as backoff algorithm or random number generation [6]. The result will be particularly useful in emerging communication systems such as impulse radio [8] and wireless sensor networks [9] in which well-coordinated transmissions and time offsets may be too costly to devices with constrained resource. The idea of using deterministic coding sequences, namely *protocol sequence*, to define random accessing in a *collision channel without feedback* [2] is worth a revisit. Therein, senders cannot synchronize transmissions between one another as their relative time offsets are unknown to each other due to a lack of feedback link. Besides, packet retransmission and backoff mechanisms are not employed. Each sender will just transmit packets at the times governed by his own protocol sequence.

Generally speaking, the idea of using protocol sequences can be described as a derandomization of the probabilistic ALOHA scheme. The advantages of employing deterministic protocol sequences instead of probabilistic random accessing are twofold. Theoretically, we can derive the zero-error capacity region for the collision channel without feedback when deterministic protocol sequences are employed. Provided that the protocol sequences are properly designed, it can be guaranteed that, with probability one, the throughput of each user is greater than a positive constant regardless of their relative delay offsets. On the other hand, practically, the sequences may have some structures that allow the receiver to determine from whom a packet is sent, even without header information. In other words, the sender of a packet can be identified without overhead.

Under the model of collision channel without feedback, Massey and Mathys have shown that a reliable multiaccess communication is indeed achievable and a corresponding scheme with carefully designed protocol sequences was presented in [2]. More general sequence constructions using constant-weight cyclically permutable codes are reported in [10], [11] afterwards. See also [12] for a recent survey on coding for multiple access channel without feedback. In the context of optical communications, protocol sequences are studied in the name of optical orthogonal codes [13]. They are related but have quite different design criteria. Another class of periodic deterministic sequences, called linear congruence sequences [14], is originally designed for time-frequency hopping signals but can also be regarded as protocol sequences. Independently,

Manuscript received October 11, 2007; revised January 28, 2009. Current version published June 24, 2009. The work of C. S. Chen was supported by an ERCIM "Alain Bensoussan" Fellowship Programme. This work was supported in part by a Grant from the Research Grants Council of the Hong Kong Special Administrative Region under Project 416906, and by a Grant from City University of Hong Kong under Project 7002386.

K. W. Shum and W. S. Wong are with the Department of Information Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong (e-mail: kshum2009@gmail.com; wswong@ie.cuhk.edu.hk).

C. S. Chen was with the Department of Electronics and Telecommunications, Norwegian University of Science and Technology, Norway. He is now with PNA2 Centrum voor Wiskunde en Informatica, 1098 XG Amsterdam, The Netherlands (e-mail: cschen@ieee.org).

C. W. Sung is with the Department of Electronic Engineering, City University of Hong Kong, Kowloon Tong, Hong Kong (e-mail: albert.sung@cityu.edu.hk).

Communicated by G. Gong, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2009.2021335

0018-9448/$25.00 © 2009 IEEE

prime sequences [15], a subset of linear congruence sequences, are proposed and employed in optical spread spectrum systems. Built on the concept of prime sequences, a family of protocol sequences, called wobbling sequences [6], is designed to support multi-rate service and a large number of active users. They are suitable to serve as random access protocols, in particular for applications in some wireless ad hoc or sensor networks.

In the design of protocol sequence, some common concerns include the maximum number of sequences supported for active users, their correlation properties and resulting throughput, the sequence length, overheads required for sender identification, and service rate flexibility. In all the constructions mentioned above, the protocol sequences in [2] have sequence length exponential in the number of users, while all the other have polynomial lengths. However, the former enjoys a special property that the throughput of each user is constant and independent of any relative delay offsets. This zero-variance or *shift-invariant* (SI) property is favorable and also reported in a recent design in [16]. However, both constructions suffer from the same drawback that the sequence length grows exponentially with the number of users.

In this paper, we investigate the protocol sequences whose throughput performance is shift-invariant in general, and discuss several implications. After setting up the channel model and required notations in Section II, we prove several important properties of SI protocol sequences in Section III. In Section IV, we first derive a lower bound on the period of SI protocol sequences and then describe a construction method that can achieve this lower bound. In Section V, it is shown that in some special cases, the least periods of SI sequences must be distinct. Section VI gives some numerical studies. Finally, we close in Section VII with some concluding remarks.

II. Channel Model and Notations

Following the model of collision channel without feedback [2], we consider a communication channel in which time is divided into time slots of equal duration and shared by K active users. Each user i follows a binary sequence, $s_i(t), t = 0, 1, 2, \dots$, and will transmit a packet at time slot t if $s_i(t) = 1$. Otherwise, it keeps silent. Here, for simplicity, we restrict our attention to the slot-synchronized model in which users transmit packets aligned to the slot boundaries. It is assumed that users know the slot boundaries. However, they do not know the time offsets between one another and cannot coordinate their transmission schedules. Generally, there are time delay offsets between users. It should be noted in fact it is possible to remove the assumption that users are slot synchronized. Some approaches and discussions are presented in [2], [17], and [18] with coding, interleaving, and error correction techniques. However, this more general scenario will not be addressed in this paper.

At any time slot, a packet collision occurs if more than one user transmits at the same time. All transmitted packets in this duration are considered lost. Otherwise, the receiver can receive the packet correctly and decode the content. The effective throughput of a user is defined as the fraction of packets it can send without suffering any collision. For practical considerations, forward error-correcting code can be applied across packets to recover data lost or correct erasures due to potential collisions [18]–[20].

Some notations and definitions are as follows. We consider K binary sequences of period L. For $i = 1, \dots, K$, the ith sequence is specified by a row vector

$$\mathbf{s}_i := (s_i(0), s_i(1), \dots, s_i(L-1)) \tag{1}$$

whose components are the first L bits of the sequence. The cyclic shift of a sequence $\mathbf{s}$ by τ is denoted by

$$\mathbf{s}^{(\tau)} := (s(0 \oplus \tau), s(1 \oplus \tau), \dots, s((L-1) \oplus \tau)) \tag{2}$$

where $\oplus$ represents addition modulo L. The tth bit of $\mathbf{s}^{(\tau)}$ is denoted by $s^{(\tau)}(t)$. The *Hamming weight* of a sequence is the number of ones in a period.

In this paper, we study the following generalized notion of Hamming cross correlation. We denote the set of users by $\mathcal{K} := \{1, 2, \dots, K\}$. Let $\mathcal{O}_K$ be the collection of all ordered tuples of length $1, 2, \dots, K$, whose components are distinct elements in $\mathcal{K}$ and sorted in ascending order. It consists of n-tuples in the form $(i_1, i_2, \dots, i_n)$ for some n between 1 and K, and $i_1 < i_2 < \dots < i_n$. An element in $\mathcal{O}_K$ corresponds to an ordered tuple of users.

For $\mathsf{A} = (i_1, i_2, \dots, i_n) \in \mathcal{O}_K$ with $i_1 < \dots < i_n$, we define the Hamming cross correlation associated with A as

$$H(\tau_1, \dots, \tau_n; \mathsf{A}) := \sum_{t=0}^{L-1} \prod_{j=1}^{n} s_{i_j}^{(\tau_j)}(t). \tag{3}$$

In other words, it counts the number of slots in a period where all users in A transmit simultaneously. When A consists of only one user, it reduces to the Hamming weight. When A consists of two users, it is the usual Hamming cross correlation defined for a pair of users.

A function $F : \{0, 1, \dots, L-1\}^n \to \mathbb{R}$ is said to be *shift-invariant* if $F(\tau_1, \dots, \tau_n)$ equals identically to a constant for every choice of $\tau_1, \dots, \tau_n$. We say that a sequence set is shift-invariant if the Hamming cross correlation in (3) is shift-invariant as a function of $\tau_1, \dots, \tau_n$, for every A in $\mathcal{O}_K$.

When only the users in the ordered tuple $\mathsf{A} = (i_1, \dots, i_n) \in \mathcal{O}_K$ are active and the offset of user i_j is τ_j, for $j = 1, 2, \dots, n$, the *throughput* of user i_j is defined as

$$\theta_j(\tau_1, \tau_2, \dots, \tau_n; \mathsf{A}) := \frac{1}{L} \sum_{t=0}^{L-1} s_{i_j}^{(\tau_j)}(t) \prod_{\ell \neq j} \left(1 - s_{i_\ell}^{(\tau_\ell)}(t)\right) \tag{4}$$

where the product is over all $\ell = 1, \dots, n$ except $\ell = j$. This is the fraction of time slots in which user i_j transmits and users $i_1, \dots, i_{j-1}, i_{j+1}, \dots, i_n$ keep silent.

The fraction of time in which a user is transmitting is called the *duty factor*, which equals the Hamming weight of the corresponding sequence divided by the period. We will denote the duty factor of user i by

$$f_i := \frac{1}{L} \sum_{t=0}^{L-1} s_i(t). \tag{5}$$

Note that for all $i, \theta_1(\tau; (i))$ is identically equal to f_i.

Example 1: The following is a set of three shift-invariant protocol sequences with duty factors $1/2, 1/2$ and $1/3$

$$\begin{aligned}\mathbf{s}_1 &= (1,0,1,0,1,0,1,0,1,0,1,0)\\ \mathbf{s}_2 &= (1,1,0,0,1,1,0,0,1,1,0,0)\\ \mathbf{s}_3 &= (1,1,1,1,0,0,0,0,0,0,0,0).\end{aligned}$$

We have $H(\tau_1,\tau_2;(1,2)) = 3, H(\tau_2,\tau_3;(2,3)) = 2$, $H(\tau_1,\tau_3;(1,3)) = 2$ and $H(\tau_1,\tau_2,\tau_3;(1,2,3)) = 1$, for all τ_1,τ_2 and τ_3.

III. Properties of Shift-Invariant Protocol Sequences

We will use the following notation. Given K binary sequences $\mathbf{s}_1,\ldots,\mathbf{s}_K$ of length L, and $b_i \in \{0,1\}$ for all i, let $N(b_1,\ldots,b_K|\mathbf{s}_1,\ldots,\mathbf{s}_K)$ be the number of time indices $t, 0 \le t < L$, such that $s_i(t) = b_i$ for all $i, 1 \le i \le K$.

A. Characterization

The next theorem gives a few properties of SI sequences, which are equivalent to each other.

Theorem 1: Let $\mathbf{s}_1,\ldots,\mathbf{s}_K$ be binary sequences of period L. The following conditions are equivalent.

1) The sequence set $\{\mathbf{s}_1,\ldots,\mathbf{s}_K\}$ is shift-invariant.

2) For each choice of $b_1,\ldots,b_K$, the number of times that the column vector $[b_1,\ldots,b_K]^T$ appears in the $K \times L$ matrix

$$\mathbf{M}(\tau_1,\ldots,\tau_K) := \begin{bmatrix}\mathbf{s}_1^{(\tau_1)}\\ \mathbf{s}_2^{(\tau_2)}\\ \vdots\\ \mathbf{s}_K^{(\tau_K)}\end{bmatrix} \tag{6}$$

is independent of the offsets $\tau_1,\ldots,\tau_K$. In other words, $N(b_1,\ldots,b_K|\mathbf{s}_1^{(\tau_1)},\ldots,\mathbf{s}_K^{(\tau_K)})$ is a shift-invariant function of $\tau_1,\ldots,\tau_K$.

3) The throughput function $\theta_j(\tau_1,\tau_2,\ldots,\tau_n;\mathsf{A})$ is shift-invariant for every $\mathsf{A} \in \mathcal{O}_K$ and $j = 1,2,\ldots,n$.

In the second property, the matrix in (6) is obtained by cyclically shifting row i in the *sequence matrix*

$$\begin{bmatrix}\mathbf{s}_1\\ \mathbf{s}_2\\ \vdots\\ \mathbf{s}_K\end{bmatrix}.$$

by τ_i. Hence it can be rephrased in the following equivalent form.

2') For each choice of delay offsets $\tau_1,\ldots,\tau_K$, the matrix $\mathbf{M}(\tau_1,\ldots,\tau_K)$ can be obtained by permuting the columns in $\mathbf{M}(0,\ldots,0)$.

In the next section, we will present a construction for SI sequences, and use Property 2' to show that the constructed sequences are indeed SI.

Proof: 1) $\Rightarrow$ 2). By permuting the rows of $\mathbf{M}(\tau_1,\ldots,\tau_K)$, we may assume without loss of generality that $b_i = 1$ for $i = 1,2,\ldots,n$, and $b_i = 0$ for $i = n+1,\ldots,K$. Suppose that the relative offsets are $\tau_1,\ldots,\tau_K$. Let $\mathcal{B}$ be the set of columns in $\mathbf{M}(\tau_1,\ldots,\tau_K)$ such that the top n components are all one. For $j = n+1, n+2,\ldots,K$, let $\mathcal{B}_j$ be the set of columns in $\mathcal{B}$ whose jth component is also equal to 1. By the principle of inclusion-and-exclusion, what we want to count is equal to

$$|\mathcal{B}| - \sum_{n<j<K} |\mathcal{B}_j| + \sum_{n<j_1<j_2\le K} |\mathcal{B}_{j_1} \cap \mathcal{B}_{j_2}| - \ldots + (-1)^{K-n}|\mathcal{B}_{n+1} \cap \ldots \cap \mathcal{B}_K|. \tag{7}$$

The first term $|\mathcal{B}|$ equals $H(\tau_1,\ldots,\tau_n;(1,\ldots,n))$. Each summand in the first summation equals

$$H(\tau_1,\ldots,\tau_n,\tau_j;(1,\ldots,n,j)).$$

Similarly, all summands in (7) can be written in terms of Hamming cross correlations, which are assumed to be SI. Therefore, the whole expression in (7) is SI.

$N(b_1,\ldots,b_K|\mathbf{s}^{(\tau_1)},\ldots,\mathbf{s}^{(\tau_K)})$ is the number of columns in $\mathbf{M}(\tau_1,\ldots,\tau_K)$ that equals $[b_1 b_2 \ldots b_K]^T$, and hence is shift-invariant by the first statement in condition 2.

2) $\Rightarrow$ 3). Set $\tau_{n+1},\ldots,\tau_K$ to any arbitrary values. Suppose that A consists of the first n users, i.e., $\mathsf{A} = (1,2,\ldots,n), n \le K$. We sum $N(b_1,\ldots,b_K|\mathbf{s}_1^{(\tau_1)},\ldots,\mathbf{s}_K^{(\tau_K)})$ over all combinations of $b_{n+1},\ldots,b_K$ and obtain

$$N\left(b_1,\ldots,b_n|\mathbf{s}_1^{(\tau_1)},\ldots,\mathbf{s}_n^{(\tau_n)}\right) = \sum_{b_{n+1}=0}^{1} \cdots \sum_{b_K=0}^{1} N\left(b_1,\ldots,b_K|\mathbf{s}_1^{(\tau_1)},\ldots,\mathbf{s}_K^{(\tau_K)}\right).$$

As each summand in the right-hand side (RHS) is SI by assumption, so is the left-hand side (LHS). By setting $b_j = 1$ and $b_\ell = 0$ for $\ell \in \{1,2,\ldots,n\} \setminus \{j\}$, we conclude that, when users in A are active, the throughput of user j is SI.

We have thus proved Property (3) for the case $\mathsf{A} = (1,2,\ldots,n)$. The proof for other choices of A is similar.

3) $\Rightarrow$ 1). Suppose the throughput is SI. We will show that the Hamming cross correlation is SI by induction on the length of A.

When the length of A is one, i.e., $\mathsf{A} = (i)$ for some $i \in \mathcal{K}, H(\tau;(i))$ equals the Hamming weight of the corresponding sequence and is obviously SI.

Suppose that the Hamming cross correlation of each A consisting of no more than $n-1$ users is SI. Let B be an n-tuple in $\mathcal{O}_K$. Without loss of generality, assume that $\mathsf{B} = (1,2,\ldots,n)$. Suppose that the relative offsets of users $1,\ldots,n$ are $\tau_1,\ldots,\tau_n$, respectively. Let $\mathcal{B} := \{1,2,\ldots,n\}$.

By the principle of inclusion-and-exclusion, the number of time slots in a period where user 1 transmits and users 2 to n are silent, is

$$\begin{aligned}&L\theta_1(\tau_1,\ldots,\tau_n;\mathsf{B})\\ &\quad= H(\tau_1;(1)) - \sum_{\alpha\in\mathcal{B}\setminus\{1\}} H(\tau_1,\tau_\alpha;(1,\alpha))\\ &\qquad+ \sum_{\alpha,\beta\in\mathcal{B}\setminus\{1\}_{\alpha<\beta}} H(\tau_1,\tau_\alpha,\tau_\beta;(1,\alpha,\beta))\\ &\qquad\ldots + (-1)^{n+1}H(\tau_1,\ldots,\tau_n;\mathsf{B}).\end{aligned}$$

By rearranging terms in the above equation, we can express $H(\tau_1,\ldots,\tau_n;\mathsf{B})$ in terms of throughput $\theta_1(\tau_1,\ldots,\tau_n;\mathsf{B})$, and $H(\tau_1,\ldots,\tau_{|\mathsf{A}|};\mathsf{A})$ with the length of A, denoted by $|\mathsf{A}|$, strictly less than n. Therefore, $H(\tau_1,\dots,\tau_n;\mathsf{B})$ can be written in terms of functions, that are all SI by induction, and so $H(\tau_1,\dots,\tau_n;\mathsf{B})$ must be also SI.

By similar argument, we can show that for every n-tuple B in $\mathcal{O}_K$, the Hamming cross correlation associated with B is SI. □

Having proved that the three properties in Theorem 1 are equivalent, we see that we could define SI sequences by each of the three properties, and the result would be the same.

B. Throughput

We see from the previous characterization theorem that when SI sequences are used, the individual throughput is a constant, independent of delay offsets. We determine this constant in this subsection, and show that the throughput is the same as if user i transmits a packet in each slot independently with probability f_i, for all i.

We first prove the following lemma, which is a generalization of the case when $M=2$ in [21].

Lemma 2: Suppose that $\mathbf{s}_1,\mathbf{s}_2,\dots,\mathbf{s}_n$ are n sequences of period L. Let w_i be the Hamming weight of $\mathbf{s}_i$ for $i=1,2,\dots,n$. For $b_1,\dots,b_n\in\{0,1\}$, we have

$$\sum_{\tau_1=0}^{L-1}\cdots\sum_{\tau_n=0}^{L-1} N\left(b_1,\dots,b_n|\mathbf{s}_1^{(\tau_1)},\dots,\mathbf{s}_n^{(\tau_n)}\right)=L\prod_{i=1}^{n}N(b_i|\mathbf{s}_i). \tag{8}$$

In particular, putting $b_1=b_2=\cdots=b_n=1$, and $\mathsf{A}=(i_1,\dots,i_n)$, we have

$$\sum_{\tau_1=0}^{L-1}\cdots\sum_{\tau_n=0}^{L-1} H(\tau_1,\dots,\tau_n;\mathsf{A})=Lw_{i_1}w_{i_2}\cdots w_{i_n}. \tag{9}$$

Proof: Given a time index t, we have $s_i(t\oplus\tau_i)=b_i$ for all i if and only if

$$\left[s_i^{(\tau_i)}(t)\right]^{b_i}\left[1-s_i^{(\tau_i)}(t)\right]^{1-b_i}=1$$

for all i. We can thus express the counting function

$$N\left(b_1,\dots,b_n|\mathbf{s}_1^{(\tau_1)},\dots,\mathbf{s}_n^{(\tau_n)}\right)$$

as

$$\sum_{t=0}^{L-1}\prod_{i=1}^{n}\left[s_i^{(\tau_i)}(t)\right]^{b_i}\left[1-s_i^{(\tau_i)}(t)\right]^{1-b_i}.$$

Summing the above over all possible relative offsets and exchanging the order of summation and multiplication, we obtain

$$\sum_{\tau_1,\dots,\tau_n} N\left(b_1,\dots,b_n|\mathbf{s}_1^{(\tau_1)},\dots,\mathbf{s}_n^{(\tau_n)}\right)$$
$$=\sum_{t=0}^{L-1}\prod_{i=1}^{n}\sum_{\tau_i=0}^{L-1}\left[s_i^{(\tau_i)}(t)\right]^{b_i}\left[1-s_i^{(\tau_i)}(t)\right]^{1-b_i}.$$

Note that the inner summation equals w_i when $b_i=1$, or $L-w_i$ when $b_i=0$. Therefore,

$$\sum_{\tau_1,\dots,\tau_n} N\left(b_1,\dots,b_n|\mathbf{s}_1^{(\tau_1)},\dots,\mathbf{s}_n^{(\tau_n)}\right)$$
$$=\sum_{t=0}^{L-1}\prod_{i=1}^{n}N(b_i|\mathbf{s}_i)$$
$$=L\prod_{i=1}^{n}N(b_i|\mathbf{s}_i).$$

This proves the equality in (8). □

Theorem 3: Let $\mathbf{s}_1,\mathbf{s}_2\dots,\mathbf{s}_K$ be K SI protocol sequences with duty factors $f_1,f_2,\dots,f_K$, respectively. The throughput of user i is equal to

$$f_i\prod_{j\neq i}(1-f_j). \tag{10}$$

Proof: We set $b_i=1$ and $b_j=0$ for $j\neq i$, and divide both sides of (8) by L^{n+1}. The LHS of (8) becomes

$$\frac{1}{L^n}\sum_{\tau_1=0}^{L-1}\cdots\sum_{\tau_n=0}^{L-1}\frac{1}{L}N(b_1,\dots,b_n|\mathbf{s}_1^{(\tau_1)},\dots,\mathbf{s}_n^{(\tau_n)})$$

which equals the average throughput over all possible offsets. The RHS of (8) becomes

$$\prod_{i=1}^{n}\frac{N(b_i|\mathbf{s}_i)}{L}$$

which equals $f_i\prod_{j\neq i}(1-f_j)$. □

Unless some duty factors equal zero or one, we see from the above theorem that the throughput of any user is always nonzero. In other words, the number of successfully received packets in each period is a positive constant no matter what the offsets are. Each user can successfully send out at least one packet in each period. We call this particular property *user-irrepressibility*, which is first investigated in [6].

When all K users have the same duty factor f, the individual throughput is

$$f(1-f)^{K-1}.$$

It is easy to see that the individual throughput (and, hence, the system throughput) is maximized in this symmetric case when $f=1/K$. When K tends to infinity, the system throughput tends to e^{-1}—the same as in slotted ALOHA.

C. Identifiability

It is assumed that a receiver can detect whether no packet, one packet or multiple packets are transmitted in any given time slot. In the case of multiple transmissions in a time slot, all packets are assumed to be lost. We let

$$Y(t):=\begin{cases}0, & \text{if time slot } t \text{ is idle}\\ 1 & \text{if exactly one user transmits at time slot } t\\ *, & \text{if more than one user transmits at time slot } t.\end{cases}$$

We say that a sequence set is *identifiable* if the receiver can determine the sender of each successfully received packet, based on the information represented by $Y(t)$, regardless of the offsets.

Example 1 (Continued): Suppose that the relative delay offsets of users 1, 2, and 3 are, respectively, 0, 1, and 3. The shifted protocol sequences are

$$(1,0,1,0,1,0,1,0,1,0,1,0)$$
$$(0,1,1,0,0,1,1,0,0,1,1,0)$$
$$(0,0,0,1,1,1,1,0,0,0,0,0)$$

The received pattern $Y(t)$ is

$$(1,1,*,1,*,*,*,0,1,1,*,0)$$

The receiver must be able to tell, based on this pattern only, that the packets at $t = 0$ and $t = 8$ originates from user 1, the packets at $t = 1$ and $t = 9$ from user 2, and the packet at $t = 3$ from user 3.

It is noted that the offsets need not be uniquely determined. If the delay offset of user 3 is changed from 3 to 2, then the transmitted protocol sequences are

$$(1,0,1,0,1,0,1,0,1,0,1,0)$$
$$(0,1,1,0,0,1,1,0,0,1,1,0)$$
$$(0,0,1,1,1,1,0,0,0,0,0,0)$$

with the same received pattern. Therefore, it is not possible to tell from the information provided by $Y(t)$ whether the delay offsets of user 3 is 2 or 3. However, in any case, we are sure that the packet at $t = 3$ is transmitted by user 3.

In [2], Massey and Mathys devised an algorithm, called decimation algorithm, to solve the identification problem for the SI sequences they constructed in their paper. In the following theorem, we show that the identification problem can be solved in general for all SI sequences.

Theorem 4: If a set of protocol sequences is shift-invariant, then it is identifiable.

Proof: Suppose that for $k = 1, \dots, K$, the delay offset of user k is τ_k. Also, suppose that, starting from time t_0, the receiver observes the channel for a full period, and the received pattern is $Y(t)$, for $t \in \{t_0, t_0+1, \dots, t_0+L-1\} =: \mathcal{U}$. We will show how to identify the successfully transmitted packets from user i.

Let $\mathcal{T}_i$ be the collection of delay offsets $\delta \in \{0, \dots, L-1\}$ so that the following two conditions are satisfied:

1) For all $t \in \mathcal{U}$ such that $\mathbf{s}_i^{(\delta)}(t) = 1$, we have $Y(t)$ equals 1 or $*$.
2) $|\{t \in \mathcal{U} : \mathbf{s}_i^{(\delta)}(t) = 1, Y(t) = 1\}| = Lf_i \prod_{j \neq i}(1 - f_j)$ = number of successful packets from user i within one period.

The actual delay offset of user i, τ_i, which is assumed to be unknown to the receiver, certainly satisfies the above conditions. Hence $\mathcal{T}_i$ is nonempty. We set $\mathcal{S}_i(\delta) := \{t \in \mathcal{U} : \mathbf{s}^{(\delta)}(t) = 1, Y(t) = 1\}$.

We claim that for each $\delta \in \mathcal{T}_i$, the packets with time indices in $\mathcal{S}_i(\delta)$ are indeed from user i. The claim is obviously true for $\delta = \tau_i$. For $\delta \in \mathcal{T}_i \setminus \{\tau_i\}$, we will prove the claim by contradiction.

Suppose $\delta_0 \in \mathcal{T}_i, \delta_0 \neq \tau_i$ and $\mathcal{S}_i(\delta_0) \neq \mathcal{S}_i(\tau_i)$. Since $\mathcal{S}_i(\delta_0)$ and $\mathcal{S}_i(\tau_i)$ have the same cardinality, we can find a temporal index in $\mathcal{S}_i(\delta_0)$ but not in $\mathcal{S}_i(\tau_i)$, and a temporal index in $\mathcal{S}_i(\tau_i)$ but not in $\mathcal{S}_i(\delta_0)$. Hence $\mathcal{S}_i(\delta_0) \setminus \mathcal{S}_i(\tau_i)$ and $\mathcal{S}_i(\tau_i) \setminus \mathcal{S}_i(\delta_0)$ are nonempty and have the same cardinality. As $Y(t)$ is equal to 1 for all $t \in \mathcal{S}_i(\delta_0) \setminus \mathcal{S}_i(\tau_i)$, the packets corresponding $t \in \mathcal{S}_i(\delta_0) \setminus \mathcal{S}_i(\tau_i)$ are successfully received. However, these packets are not from user i. Now, suppose that the delay offset of user i were changed from τ_i to δ_0, we would have collisions for $t \in \mathcal{S}_i(\delta_0) \setminus \mathcal{S}_i(\tau_i)$, and empty slots for $t \in \mathcal{S}_i(\tau_i) \setminus \mathcal{S}_i(\delta_0)$. Let $Y'(t)$ be the resulting received pattern. We would have

$$Y'(t) = \begin{cases} 0, & \text{if } t \in \mathcal{S}_i(\tau_i) \setminus \mathcal{S}_i(\delta_0) \\ 1, & \text{if } t \in \mathcal{S}_i(\tau_i) \cap \mathcal{S}_i(\delta_0) \\ *, & \text{if } t \in \mathcal{S}_i(\delta_0) \setminus \mathcal{S}_i(\tau_i) \\ Y(t), & \text{otherwise.} \end{cases}$$

For $t \in \mathcal{S}_i(\delta_0) \setminus \mathcal{S}_i(\tau_i)$, the time slots at time t change from $Y(t) = 1$ to $Y'(t) = *$, while for $t \in \mathcal{S}_i(\tau_i) \setminus \mathcal{S}_i(\delta_0)$, the time slots at time t change from $Y(t) = 1$ to $Y'(t) = 0$. Therefore, the number of "1" in $Y'(t)$ is strictly less than that in $Y(t)$. This contradicts the shift invariance of throughput, and thus proves the claim that $\mathcal{S}_i(\delta) = \mathcal{S}_i(\tau_i)$ for all $\delta \in \mathcal{T}_i$.

In order to identify the successful packets from user i at the receiver, we search for a δ that satisfies the two conditions above. For any such δ, the packets with temporal indices in $\mathcal{S}_i(\delta)$ are the packets from user i. □

IV. An Optimal Construction

We will first derive a lower bound on the period of SI protocol sequences in this section. Next, a construction method that achieves this lower bound is presented.

Lemma 5: Suppose that $(\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_K)$ is a sequence set of period L. Let n_i/d_i be the duty factor of $\mathbf{s}_i$ for $i = 1, \dots, K$. If the sequences are shift-invariant, then the period L must be divisible by

$$\frac{\prod_{i \in \mathcal{A}} d_i}{\gcd(\prod_{i \in \mathcal{A}} d_i, \prod_{i \in \mathcal{A}} n_i)} \tag{11}$$

for any subset $\mathcal{A}$ of $\mathcal{K}$. Here $\gcd(x, y)$ denotes the greatest common divisor of x and y.

Proof: Suppose that $\mathcal{A}$ contains n elements. By definition, $H(\tau_1, \dots, \tau_n; \mathcal{A})$ is equal to a constant, say h, for all $\tau_1, \dots, \tau_n$. Summing $H(\tau_1, \dots, \tau_n; \mathcal{A})$ over all $\tau_1, \dots, \tau_n$, we obtain from (9)

$$L^n h = L \prod_{i \in \mathcal{A}} (L n_i / d_i)$$

which can be simplified to

$$h \prod_{i \in \mathcal{A}} d_i = L \prod_{i \in \mathcal{A}} n_i.$$

Let g be the gcd of $\prod_{i \in \mathcal{A}} d_i$ and $\prod_{i \in \mathcal{A}} n_i$. We have

$$h \left(\frac{1}{g} \prod_{i \in \mathcal{A}} d_i \right) = L \left(\frac{1}{g} \prod_{i \in \mathcal{A}} n_i \right).$$

Since $(\prod_{i \in \mathcal{A}} d_i)/g$ and $(\prod_{i \in \mathcal{A}} n_i)/g$ are relatively prime, we conclude that L is divisible by $(\prod_{i \in \mathcal{A}} d_i)/g$. □

Theorem 6: For any set of K shift-invariant sequences with duty factors $n_1/d_1, n_2/d_2, \ldots, n_K/d_K$, such that $\gcd(n_i, d_i) = 1$ for all i, the period is divisible by $d_1 d_2 \cdots d_K$. In particular, the period is larger than or equal to $d_1 d_2 \cdots d_K$.

Proof: Suppose that p is a prime factor of $d_1 d_2 \cdots d_K$, and p^m is the largest power of p that divides $d_1 d_2 \cdots d_K$. Let $\mathcal{A}$ be the set of all indices i so that p divides d_i. Since n_i/d_i is a reduced fraction for all i, p cannot divide both n_i and d_i. Therefore $\prod_{i \in \mathcal{A}} n_i$ is not divisible by p, and $\gcd(\prod_{i\in\mathcal{A}} d_i, \prod_{i\in\mathcal{A}} n_i) = 1$. By Lemma 5, the period is divisible by p^m. Since this is true for any prime power factor of $d_1 d_2 \cdots d_K$, we conclude that the period must be divisible by $d_1 d_2 \cdots d_K$. □

In the symmetric case where all K users have the same duty factor n/d, the period must be at least d^K, which increases exponentially with the number of users.

We now describe an algorithm for the construction of SI sequences with common period achieving the lower bound in Theorem 6. Suppose that $n_i/d_i, i = 1, \ldots, K$, are the duty factors of K sequences. We will assume that the duty factor is neither 0 nor 1. In our construction, the ith sequence has period

$$P_i := \prod_{j=1}^{i} d_j \tag{12}$$

and $P_K = d_1 \cdots d_K$ is a common period of the whole sequence set. The *least period* of a sequence $\mathbf{s}$ is the smallest positive integer τ such that $\mathbf{s}^{(\tau)} = \mathbf{s}$. In general, the least period of the ith sequence in our construction may be smaller than P_i.

Construction: For $i = 1, 2, \ldots, K$, the ith sequence is constructed as follows. Select P_{i-1} vectors of length d_i, say $\boldsymbol{\sigma}_{i1}, \boldsymbol{\sigma}_{i2}, \ldots, \boldsymbol{\sigma}_{iP_{i-1}}$, such that the Hamming weights of them are all equal to n_i, and interleave these P_{i-1} vectors in the manner defined in (13). (P_0 is defined as 1, as the empty product is equal to 1 by convention.) A period of P_i bits in $\mathbf{s}_i$ is defined as

$$\begin{aligned}&(\boldsymbol{\sigma}_{i1}(0), \boldsymbol{\sigma}_{i2}(0), \ldots, \boldsymbol{\sigma}_{iP_{i-1}}(0)\\ &\boldsymbol{\sigma}_{i1}(1), \boldsymbol{\sigma}_{i2}(1), \ldots, \boldsymbol{\sigma}_{iP_{i-1}}(1)\\ &\ldots, \boldsymbol{\sigma}_{i1}(d_i - 1), \boldsymbol{\sigma}_{i2}(d_i - 1), \ldots, \boldsymbol{\sigma}_{iP_{i-1}}(d_i - 1)).\end{aligned} \tag{13}$$

The construction can be described as the following interleaving operation. Write down a $P_{i-1} \times d_i$ array of zeros and ones, such that there are n_i ones in each row. The ith sequence is obtained by reading out the columns of this array. The ith sequence has the property that, for each j between 0 and $P_{i-1} - 1$, there are precisely n_i ones at time $j, j + P_{i-1}, j + 2P_{i-1}, \ldots, j + (d_i - 1)P_{i-1}$.

Example 1 (Continued): If we pick $\boldsymbol{\sigma}_{11} := (1, 0)$, $\boldsymbol{\sigma}_{21} := \boldsymbol{\sigma}_{22} := (1, 0)$, and $\boldsymbol{\sigma}_{3j} := (1, 0, 0)$ for $j = 1, 2, 3, 4$, we then obtain the three sequences in Example 1.

Example 2: $K = 2$ and the duty factors are $1/4$ and $1/3$. We pick $\boldsymbol{\sigma}_{11} := (1, 0, 0, 0), \boldsymbol{\sigma}_{21} := (1, 0, 0)$, $\boldsymbol{\sigma}_{22} := (0, 1, 0)$ and $\boldsymbol{\sigma}_{23} := \boldsymbol{\sigma}_{24} := (0, 0, 1)$. The two constructed sequences are

$$\begin{gathered}(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)\\ (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1).\end{gathered}$$

The first sequence is obtained by repeating $(1, 0, 0, 0)$ periodically. For the second sequence, we write down $\boldsymbol{\sigma}_{2j}, j = 1, \ldots, 4$ in an array

1	0	0
0	1	0
0	0	1
0	0	1

and read out the columns from left to right.

In order to verify the SI property, we define a $K \times P_K$ matrix $\mathbf{M}$ as follows. Let $d_1, d_2, \ldots, d_K$ be given positive integers. For each $i = 1, 2, \ldots, K$, pick P_{i-1} vectors of length $d_i, \boldsymbol{\pi}_{i1}, \boldsymbol{\pi}_{i2}, \ldots \boldsymbol{\pi}_{iP_{i-1}}$, such that each $\boldsymbol{\pi}_{ij}$ is a permutation of $(0, 1, \ldots, d_i - 1)$. The ith row of $\mathbf{M}$ is obtained by periodically repeating the row vector

$$\begin{aligned}\mathbf{b}_i := (&\boldsymbol{\pi}_{i1}(0), \boldsymbol{\pi}_{i2}(0), \ldots, \boldsymbol{\pi}_{iP_{i-1}}(0)\\ &\boldsymbol{\pi}_{i1}(1), \boldsymbol{\pi}_{i2}(1), \ldots, \boldsymbol{\pi}_{iP_{i-1}}(1), \ldots\\ &\boldsymbol{\pi}_{i1}(d_i - 1), \boldsymbol{\pi}_{i2}(d_i - 1), \ldots, \boldsymbol{\pi}_{iP_{i-1}}(d_i - 1)).\end{aligned} \tag{14}$$

As an example, when $K = 3$ and $d_i = 3$ for all i, we pick $(2, 1, 0)$ as $\boldsymbol{\pi}_{ij}$ for all i and $j, i = 1, \ldots, K, j = 1, \ldots, P_{i-1}$. The resulting matrix $\mathbf{M}$ is

$$\begin{bmatrix} 210\,210\,210\,210\,210\,210\,210\,210\,210\\ 222\,111\,000\,222\,111\,000\,222\,111\,000\\ 222\,222\,222\,111\,111\,111\,000\,000\,000\end{bmatrix}. \tag{15}$$

Lemma 7: Let $\mathbf{M}'$ be the matrix obtained by cyclically rotating the ith row of $\mathbf{M}$ by τ_i, for some integers $\tau_1, \tau_2, \ldots, \tau_K$. Then columns of $\mathbf{M}'$ are the columns of $\mathbf{M}$ in some permuted order.

Proof: We arbitrarily choose the offsets $\tau_1, \ldots, \tau_K$ and fix them. Without loss of generality, we assume that $\tau_1 = 0$. We will show that for $0 \le c_i < d_i, i = 1, \ldots, K$, the column vector $[c_1\ c_2\ \ldots\ c_K]^T$ appears in the columns of $\mathbf{M}'$ exactly once. It is equivalent to saying that the columns of $\mathbf{M}'$ are distinct.

We can alternatively construct $\mathbf{M}'$ in a recursive manner. Let $\mathbf{A}_1$ be the $1 \times d_1$ matrix

$$\mathbf{A}_1 := [\boldsymbol{\pi}_{11}(0) \quad \boldsymbol{\pi}_{11}(1) \quad \ldots \quad \boldsymbol{\pi}_{11}(d_1 - 1)].$$

The entries in $\mathbf{A}_1$ are distinct by definition.

After constructing an $(i - 1) \times P_{i-1}$ matrix $\mathbf{A}_{i-1}$, we define an $i \times P_i$ matrix

$$\mathbf{A}_i := \begin{bmatrix}\mathbf{A}_{i-1} & \mathbf{A}_{i-1} \cdots & \mathbf{A}_{i-1}\\ & \mathbf{b}_i^{(\tau_i)} & \end{bmatrix}.$$

The first $i - 1$ rows of $\mathbf{A}_i$ is a repetition of $\mathbf{A}_{i-1}$ d_i times. The ith row of $\mathbf{A}_i$ is a cyclically rotated version of $\mathbf{b}_i$ in (14).

For any choice of $c_1, c_2, \ldots, c_i$, with $0 \le c_j < d_j, j = 1, \ldots, i$, the column vector $\boldsymbol{v} := [c_1\ c_2\ \ldots\ c_{i-1}]^T$ appears once and only once in $\mathbf{A}_{i-1}$ by induction hypothesis. Suppose that the ℓth column of $\mathbf{A}_{i-1}$ is $[c_1\ c_2\ \ldots\ c_{i-1}]^T$. Consider columns $\ell, \ell + P_{i-1}, \ell + 2P_{i-1} \ldots \ell + (d_i - 1)P_{i-1}$ in matrix $\mathbf{A}_i$. By construction, the first $i - 1$ components in these columns are precisely $c_1, c_2, \ldots, c_{i-1}$. No matter how we cyclically rotate the last row in $\mathbf{A}_i$, the last components in these columns are

$0, 1, \ldots, d_i - 1$ in some order. This proves that the columns of $\mathbf{A}_i$ are all distinct.

We have shown by mathematical induction that $\mathbf{A}_i$ have distinct columns for $i = 1, 2, \ldots, K$. The proof is complete by noting that $\mathbf{M}'$ equals $\mathbf{A}_K$. □

Theorem 8: Using notation in the previous lemma, we map entries in the ith row of $\mathbf{M}$ with values $d_i - 1, d_i - 2, \ldots, d_i - n_i$ to 1 and those with values $d_i - n_i - 1, d_i - n_i - 2, \ldots, 0$ to 0. Let the ith row of the resulting matrix be the ith sequence $\mathbf{s}_i$. The sequences $\mathbf{s}_1, \ldots, \mathbf{s}_K$ are SI sequences of length $d_1 d_2 \cdots d_K$ with duty factors $n_1/d_1, \ldots, n_K/d_K$, respectively.

Proof: The SI property of the constructed sequences follows from Lemma 7 and condition (2') after Theorem 1. □

Example 3: Apply the map in Theorem 8 to the matrix in (15), and mapping $0 \mapsto 0, 1 \mapsto 0, 2 \mapsto 1$, we obtain the following three protocol sequences

$$\begin{aligned}\mathbf{s}_1 &: 100100100100100100100100100\\ \mathbf{s}_2 &: 111000000111000000111000000\\ \mathbf{s}_3 &: 111111111000000000000000000.\end{aligned}$$

These form a set of three SI protocol sequences, with duty factor $1/3$ and common period 27.

This construction generalizes previously known constructions in the literature. If $\boldsymbol{\sigma}_{ij}$ is chosen as

$$(1, 1, \ldots, 1, 0, 0, \ldots, 0)$$

i.e., we put appropriate number of "1" in the leftmost components, for all i and j, we then obtain the construction by da Rocha [19] and Massey and Mathys [2]. The construction in this paper also includes the construction in [16] as a special case. However, the construction presented in this section is by no mean exhaustive. There are examples which cannot be constructed using our construction. The following is an example.

Example 4: The two sequences

$$\begin{aligned}&111000\,111111\,000111\,000000\,000000\,000000\\ &110110\,110000\,100100\,110010\,110100\,100000\end{aligned}$$

are SI with duty factor $1/3$ and $5/12$. The least periods of them are both 36. We can check that the Hamming cross correlation equals 5 for every relative offset. However, they cannot be generated by the construction in Theorem 8.

Remarks: We have shown in Section III-C that the sender of a successfully received packet can be uniquely identified for SI protocol sequences in general. For the protocol sequences constructed by the method in this section, the *generalized decimation decoding* described in [19] is applicable and can recognize the sender in a more efficient way.

V. Structural Theorems

This section investigates some structures in protocol sequence set when the denominators of the duty factors are all equal to a prime number p. Recall that the least period of a sequence $\mathbf{s}$ is the smallest integer τ such that $\mathbf{s}^{(\tau)} = \mathbf{s}$. We will show in this section that the least periods must be distinct whenever the least common period is a power of prime.

The proof is based on analysis of SI sequences in the Fourier transform domain. Let ω denote the complex Lth root of unity $e^{2\pi i/L}$. The Fourier transform of a sequence $\mathbf{s}$ is defined as

$$\hat{s}(\lambda) := \sum_{t=0}^{L-1} s(t)\omega^{-\lambda t}$$

for $\lambda = 0, 1, \ldots, L-1$. The *support* of the Fourier transform, denoted by $\operatorname{supp}(\hat{s})$, is the set of frequencies λ such that $\hat{s}(\lambda)$ is nonzero. We say that a set of protocol sequences are *pairwise shift-invariant* if $H(\tau_1, \tau_2; \mathsf{A})$ are SI for every 2-tuple A. For pairwise shift-invarance, there is no restriction on $H(\tau_1, \tau_2, \ldots, \tau_{|\mathsf{B}|}; \mathsf{B})$ for B of length 3 or higher. The results are based on the following key property of pairwise shift invariance in the frequency domain, which can be interpreted as follows: The protocol sequences in a pairwise shift-invariant sequence set are "mutually orthogonal" and occupy disjoint bandwidth, if we neglect the "DC component."

Theorem 9: For every pair of nonzero sequences in a pairwise shift-invariant sequence set, the intersection of the supports of their Fourier transforms equals $\{0\}$.

Proof: It suffices to prove the following: If the Hamming cross correlation between $\mathbf{s}_1$ and $\mathbf{s}_2$ is SI, then for $\lambda = 1, 2, \ldots, L-1$, either $\hat{s}_1(\lambda)$ or $\hat{s}_2(\lambda)$, or both, is equal to zero.

Since Hamming cross correlations of $\mathbf{s}_1$ and $\mathbf{s}_2$ are SI, the function $h(\tau) := \sum_{t=0}^{L-1} s_1(t)s_2(t \oplus \tau)$ identically equals a constant h_0 for all τ. The Fourier transform of $h(\tau)$ is

$$\sum_{\tau=0}^{L-1} h_0 \omega^{-\lambda t} = \begin{cases} h_0 L & \text{for } \lambda = 0, \\ 0 & \text{for } \lambda \neq 0. \end{cases}$$

On the other hand

$$\begin{aligned}\sum_{\tau=0}^{L-1} h(\tau)\omega^{-\lambda\tau} &= \sum_{\tau=0}^{L-1}\sum_{t=0}^{L-1} s_1(t)s_2(t \oplus \tau)\omega^{-\lambda\tau}\\ &= \sum_{t=0}^{L-1} s_1(t)\omega^{\lambda t} \sum_{\tau=0}^{L-1} s_2(t \oplus \tau)\omega^{-\lambda(t+\tau)}\\ &= \hat{s}_1(-\lambda)\hat{s}_2(\lambda).\end{aligned}$$

Therefore, $\hat{s}_1(-\lambda)\hat{s}_2(\lambda) = 0$ for $\lambda \neq 0$. The proof is finished by noting that $\hat{s}_1(-\lambda) = 0$ if and only if $\hat{s}_1(\lambda) = 0$. □

Example 3 (Continued): For the three protocol sequences in Example 3, the supports of their Fourier transforms are $\operatorname{supp}(\hat{s}_1) = \{0, 9, 18\}, \operatorname{supp}(\hat{s}_2) = \{0, 3, 6, 12, 15, 21, 24\}$ and $\operatorname{supp}(\hat{s}_3) = \{0, 1, \ldots, 26\} \setminus \{3, 6, 9, \ldots, 24\}$. We see that, if 0 is disregarded, they are mutually disjoint.

Theorem 10: If the least common period of a SI sequence set, in which there is neither all-zero nor all-one sequence, is a power of a prime number p, then the least periods of all sequences in the set are distinct.

If the lower bound on sequence period in Theorem 6 is achieved, we have the following stronger statement.

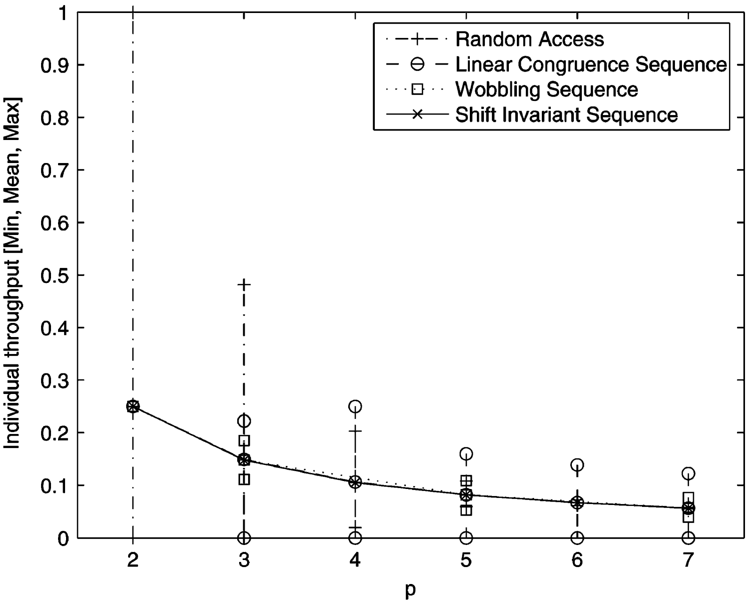

Fig. 1. The minimum, mean, and maximum individual throughputs from simulation are plotted. The number of users is denoted by p, and the duty factor of each user is equal to $1/p$. The result investigates the scenario when the system sum rate equals one.

Theorem 11: Suppose that the duty factors of a set of K shift-invariant sequences are n_i/p, for $i = 1, \dots, K, 0 < n_i < p$, and p is a prime number. If the least common period of the protocol sequences is p^K, then the least periods of the sequences are p, $p^2, \dots, p^K$. Moreover, they can be constructed by the method described in Section IV.

The proofs of Theorem 10 and 11 are contained in the Appendix. As an illustration, consider a set of three SI sequences, each with duty factor $1/3$. The minimum period is 27 by Theorem 6. For all set of three SI sequences with duty factor $1/3$, achieving the minimum period 27, the least periods of the sequences must be 3, 9, and 27. Furthermore, we can construct all such sequence sets by the construction in Section IV. An example is shown in Example 3.

Corollary 12: When the duty factors are n_i/p for $i = 1, 2, \dots, K$, the number of distinct sets of SI sequences of period p^K, up to relabeling and cyclically shifting of the sequences, is

$$\frac{1}{p^{K(K+1)/2}} \prod_{i=1}^{K} \binom{p}{n_i}^{p^{i-1}}.$$

The proof is relegated to the Appendix.

For the case when there are p sequences of length p^p, with duty factor $1/p$ for each sequence, the sum of duty factor equals 1 and the system is fully saturated. The total number of distinct sets of SI sequences for this case is

$$p^{1+p+p^2+\dots+p^{p-1}-p(p+1)/2}.$$

VI. Numerical Studies

A numerical evaluation of the throughput performance of SI protocol sequences is presented below. The result is compared with those achieved by linear congruence sequences [14], wobbling sequences [6], and a random access scheme. Nevertheless, it is noted that originally these sequences may have different design favors or criteria for different applications.

We study the symmetric, fully saturated system in which there are p active user, each of which has a duty factor equal to $1/p$. Since the system is symmetric, it suffices to consider the throughput of one particular user. In general, given a set of protocol sequences, the throughput of a user depends on his time offsets relative to the other users. To obtain an average performance, we conduct 10^5 simulation runs, assuming that the time offsets of the p users are uniformly distributed within the period of a given sequence set. Note that the periods of linear congruence sequences, wobbling sequences, and SI sequences are p^2, p^4, and p^p, respectively. For comparison purpose, we also consider the following simple random access scheme: in each time slot, each user transmits a packet independently with probability $1/p$; the throughput of a user is averaged over a period of p^p.

The throughput performance of different schemes are compared in Fig. 1, for $p = 2, 3, \dots, 7$. For each p, the maximum, mean and minimum individual throughputs of the schemes are plotted. The mean individual throughput of each scheme coincides with each other. We connect the mean individual throughputs by a piece-wise linear curve. The symbols above and below this curve indicate the maximum and minimum throughput of the corresponding scheme, among the 10^5 simulation runs.

Remark: From Theorem 3, we can find that the mean individual throughput of each sequence set is equal to

$$\frac{1}{p}\left(1 - \frac{1}{p}\right)^{p-1}.$$

As expected, SI sequences yield constant throughput. Wobbling sequences possess user-irrepressibility, thus guaranteeing a positive minimum throughput. As linear congruence sequences lack this guarantee, a user can be completely blocked and has zero throughput in the worst case. As for the random access scheme, the difference between maximum and minimum throughput becomes smaller and smaller when the averaging period increases. Asymptotically, the individual throughput converges to the mean with probability one, a fact implied by the strong law of large numbers.

VII. Conclusion

There is a tradeoff between the length of protocol sequences and the variance of throughput performance. This paper considers the extreme case where the throughput of each user is not affected by the relative delay offsets of the sequences at all. The cost of such shift-invariant property is that the length of the sequences must be exponential in the number of users. We investigate some properties of SI protocol sequences. A simple construction that achieves the lower bound on period is presented. If a small variance of throughput performance is allowed, the length of the protocol sequences can be reduced. The tradeoff between sequence length and performance deviation caused by offsets variation is an interesting issue for further study.

Appendix

We will continue using the notation as in Section V, and let ω and L be, respectively, $\exp(2\pi i/L)$ and the sequence period. We first show that the least period can be determined from its Fourier transform [22, p. 75].

Lemma 13: Let $\mathbf{s}$ be a sequence of period L. Denote the additive group of residues mod L by $\mathbb{Z}_L$. The least period of $\mathbf{s}$ is the smallest factor m of L such that the support of $\hat{s}$ is contained in the subgroup of $\mathbb{Z}_L$ of order m.

Proof: Suppose that m is a period of $\mathbf{s}$. Then, for $\lambda = 0, \dots, L-1$

$$\hat{s}(\lambda) = \sum_{t=0}^{L-1} s(t \oplus m)\omega^{-\lambda t} = \hat{s}(\lambda)\omega^{-\lambda m}.$$

Hence, $\hat{s}(\lambda)(\omega^{\lambda m} - 1) = 0$. This implies that if $\hat{s}(\lambda)$ is nonzero, λ must be a multiple of L/m, i.e., the support of $\hat{s}$ is contained in the subgroup of $\mathbb{Z}_L$ of order m. Conversely, suppose that the support of $\hat{s}$ is contained in the subgroup of $\mathbb{Z}_L$ of order m. By the inverse Fourier transform

$$s(t) = \frac{1}{L}\sum_{\lambda=0}^{L-1} \hat{s}(\lambda)\omega^{\lambda t} = \frac{1}{L}\sum_{k=0}^{m-1} \hat{s}(Lk/m)\omega^{tLk/m}$$

we verify that $s(t)$ is of period m.

We have shown that any integer m is a period of $\mathbf{s}$ if and only if the support of $\hat{s}$ is contained in a subgroup of order m. The least period of $\mathbf{s}$ is the smallest factor m of L such that the support of $\hat{s}$ is contained in the subgroup of order m in $\mathbb{Z}_L$. □

We denote the Galois group of the cyclotomic field $\mathbb{Q}(\omega)$, generated by ω over $\mathbb{Q}$, by $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$. It consists of $\phi(L)$ automorphisms of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$, where $\phi(\cdot)$ is Euler's totient function. Each automorphism maps ω to ω^a for some integer a which is relatively prime to L [23, p. 255].

For nonzero λ, let $\nu_p(\lambda)$ be the *p-adic valuation function*, which is defined as the largest nonnegative integer i such that p^i divides λ. For $\lambda = 0, \nu_p(0) := \infty$.

Proof of Theorem 10: Assume that $L = p^m$ for some integer m.

Claim: For two $\lambda, \lambda' \in \{1, 2, \dots, p^m - 1\}$, if $\nu_p(\lambda) = \nu_p(\lambda')$, then there is an automorphism $\phi \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ that maps ω^λ to $\omega^{\lambda'}$. To prove the claim, we let $j := \nu_p(\lambda) = \nu_p(\lambda')$. Then the two integers $\bar{\lambda} := \lambda/p^j$ and $\bar{\lambda}' := \bar{\lambda}'/p^j$ are not divisible by p. Hence we can find an integer $\bar{a} \in \{0, 1, \dots, p^{m-j} - 1\}$, relative prime to p^{m-j}, such that

$$\bar{\lambda}' \equiv \bar{a}\bar{\lambda} \bmod p^{m-j}.$$

In other words, there is an automorphism, say $\bar{\phi}$, of $\mathbb{Q}(\bar{\omega})$ over $\mathbb{Q}$, where $\bar{\omega} = \exp(2\pi i/p^{m-j})$, with $\bar{\phi}(\bar{\lambda}) = \bar{\lambda}'$. This automorphism of $\mathbb{Q}(\bar{\omega})$ can be extended to an automorphism of $\mathbb{Q}(\omega)$, meaning that there is a $\phi \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ such that ϕ is equal to $\bar{\phi}$ if we restrict the domain to $\mathbb{Q}(\bar{\omega})$. This is the required automorphism and the claim is proved.

From Lemma 13, the least period of a sequence $\mathbf{s}_i$, for $i = 1, \dots, K$, is equal to p^{m-m_i}, where m_i is the smallest valuation in the support of $\hat{s}_i$,

$$m_i = \min\{\nu_p(\lambda) : \lambda \in \mathrm{supp}(\hat{s}_i), \lambda \neq 0\}.$$

Suppose that there are two sequences, say $\mathbf{s}_i$ and $\mathbf{s}_j$, that share the same least period. Then there are λ and λ' with the same valuation $\nu_p(\lambda) = \nu_p(\lambda')$, such that $\hat{s}_i(\lambda) \neq 0$ and $\hat{s}_j(\lambda') \neq 0$. However, using the claim above, there is an automorphism $\phi \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ which takes ω^λ to $\omega^{\lambda'}$, implying that

$$\begin{aligned}\phi(\hat{s}_i(\lambda)) &= \phi\left(\sum_{t=0}^{L-1} s_i(t)\omega^{-\lambda t}\right)\\ &= \sum_{t=0}^{L-1} \phi(s_i(t))\phi(\omega^{-\lambda t})\\ &= \sum_{t=0}^{L-1} s_i(t)\omega^{-\lambda' t} = \hat{s}_i(\lambda').\end{aligned}$$

Since field automorphism is injective, $\hat{s}_i(\lambda')$ is nonzero. By Theorem 9, $\hat{s}_i(\lambda')$ and $\hat{s}_j(\lambda')$ cannot be nonzero at the same time. This yields a contradiction. □

Proof of Theorem 11: By Theorem 10, the least periods of the K sequences are distinct. However, in a sequence set with common period $L = p^K$, there are only K possible choices of least periods, namely $p, p^2, \dots, p^K$. The least periods of the K sequences must be precisely $p, p^2, \dots, p^K$.

We relabel the sequences so that the least period of the ith sequence is p^i, for $i = 1, 2 \dots, K$. It is certainly true that the first sequence with period p can be constructed by the method in Section IV. In the following, we consider the ith sequence for $i = 2, 3, \dots, K$.

From the proof of Theorem 10, the support of $\hat{s}_i(\lambda)$ is included in

$$\{0\} \cup \{\lambda \in \{1, \dots, L-1\} : \nu_p(\lambda) = K - i\}.$$

Hence $\hat{s}_i(\lambda) = 0$ for all nonzero λ with $\nu_p(\lambda) > K - i$. Let λ_0 be nonnegative integer such that $\nu_p(\lambda_0) > K - i$, i.e., λ_0 is divisible by p^{K-i+1}. We can combine like terms in the definition of $\hat{s}_i(\lambda_0)$ and obtain

$$\hat{s}_i(\lambda_0) = p^{K-i} \sum_{t=0}^{p^i-1} s_i(t)\omega^{-\lambda_0 t}.$$

Here, we have used the fact that $\mathbf{s}_i$ is of period p^i and $\omega^{-\lambda_0(t+p^i)} = \omega^{-\lambda_0 t}$.

Since $\omega^{-\lambda_0(t+p^{i-1})} = \omega^{-\lambda_0 t}$, we can further decompose the above summation into a double summation

$$\hat{s}_i(\lambda_0) = p^{K-i} \sum_{t_1=0}^{p^{i-1}-1} \left(\sum_{t_2=0}^{p-1} s_i(t_1 + p^{i-1}t_2) \right) \omega^{-\lambda_0 t_1}.$$

This motivates the definition of the following polynomial

$$g(x) := \sum_{t_1=0}^{p^{i-1}-1} \left(\sum_{t_2=0}^{p-1} s_i(t_1 + p^{i-1}t_2) \right) x^{t_1}. \qquad (16)$$

The above arguments show that $g(\omega^{-\lambda_0}) = 0$ for each $\lambda_0 \in \{1, 2, \dots, p^K - 1\}$ that is divisible by p^{K-i+1}, i.e., all p^{i-1}th roots of unity ζ, except $\zeta = 1$, are roots of $g(x)$. As the degree of $g(x)$ is $p^{i-1} - 1$, we have thus found all roots of $g(x)$. We can write $g(x)$ as

$$g(x) = c \prod_{\zeta \neq 1} (x - \zeta^k)$$

for some constant c, with the product taken over all p^{i-1}th roots of unity except $\zeta = 1$. Hence, we obtain

$$g(x) = c(1 + x + \ldots + x^{p^{i-1}-1}). \qquad (17)$$

The value of c can be determined by considering the number of ones in $s_i(t)$ in a period of p^K, and substituting $\lambda_0 = 0$

$$n_i p^{K-1} = \hat{s}_i(1) = p^{K-i} g(1) = p^{K-i}(cp^{i-1}).$$

Therefore, the constant c must equal n_i. By comparing coefficients of (16) and (17), we have

$$\sum_{t_2=0}^{p-1} s_i(t + p^{i-1}t_2) = n_i$$

for all $t = 0, 1, \dots, p^{i-1} - 1$. We have thus proved that for all $t = 0, 1, \dots, p^{i-1} - 1$, the total number of ones among

$$s_i(t),\ s_i(t + p^{i-1}),\ \dots,\ s_i(t + (p-1)p^{i-1})$$

is equal to n_i. □

Proof of Corollary 12: We relabel the sequences such that the least period of the ith sequence is p^i. For the ith sequence, there are $\binom{p}{n_i}$ choices for $\boldsymbol{\sigma}_{ij}$, for each $j = 1, 2, \dots, P_{i-1}$ in the construction.

The ith sequence so constructed has the property that, for each $t, 0 \le t < p$, there are exactly n_i ones at time $t, t + p^{i-1}, \dots, t + (p-1)p^{i-1}$. (The locations of the n_i ones are different for different t). Since this property is preserved by cyclic shift, we conclude that the $\binom{p}{n_i}^{p^i}$ sequences obtained by exhausting all possible choices of $\boldsymbol{\sigma}_{ij}$'s are closed under cyclic shift. The number of cyclically distinct sequences of least period p^i that can be generated is, therefore

$$\frac{1}{P_i} \binom{p}{n_i}^{P_{i-1}}.$$

The number of distinct sets of SI sequences with duty factors and period specified in the corollary is obtained by multiplying the number of cyclically distinct sequences for user i, for $i = 1, 2, \dots, K$

$$\prod_{i=1}^{K} \frac{1}{P_i} \binom{p}{n_i}^{P_{i-1}}.$$

The corollary is proven by substituting P_{i-1} by p^{i-1}, and $P_1 P_2 \cdots P_K$ by $p^{1+2+\dots+K}$. □

Acknowledgment

Chung Shue Chen would like to thank Prof. Ye-Qiong Song, Prof. Geir E. Øien, and Prof. Rob van der Mei for their valuable comments and discussions.

References

[1] N. Abramson, "Packet switching with satellites," in *AFIPS Conf. Proc., Nat. Comp. Conf.*, June 1973, vol. 42, pp. 695–702.

[2] J. L. Massey and P. Mathys, "The collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. 31, no. 2, pp. 192–204, Mar. 1985.

[3] P. R. Prucnal, M. A. Santoro, and T. R. Fan, "Spread spectrum fiber-optic local area network using optical processing," *J. Lightw. Technol.*, vol. 4, no. 5, pp. 547–554, 1986.

[4] V. Anantharam, "The stability region of the finite-user slotted ALOHA protocol," *IEEE Trans. Inf. Theory*, vol. 37, no. 3, pp. 535–540, May 1991.

[5] A. A. Shaar, M. Gharib, and P. A. Davies, "Collision resolution in contention access local area networks using concatenated prime sequences," in *IEE Proc. Commun.*, Oct. 2002, vol. 149, no. 5, pp. 249–256.

[6] W. S. Wong, "New protocol sequences for random access channels without feedback," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2060–2071, Jun. 2007.

[7] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std 802.11, 1999, IEEE-SA Standards Board.

[8] M. Z. Win and R. A. Scholtz, "Impulse radio: How it works," *IEEE Commun. Lett.*, vol. 2, no. 2, pp. 36–38, Feb. 1998.

[9] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[10] Q. A. Nguyen, L. Györfi, and J. L. Massey, "Constructions of binary constant-weight cyclic codes and cyclically permutable codes," *IEEE Trans. Inform. Theory*, vol. 38, no. 3, pp. 940–949, May 1992.

[11] O. Moreno, Z. Zhang, P. V. Kumar, and V. A. Zinoviev, "New constructions of optimal cyclically permutable constant weight codes," *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 448–455, Mar. 1995.

[12] L. Györfi and S. Győri, "Coding for multiple-access collision channel without feedback," in *Multiple Access Channels—Theory and Practice*, ser. NATO Security Through Science, E. Biglieri and L. Györfi, Eds. Amsterdam, The Netherlands: IOS Press, 2007, pp. 299–326.

[13] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: design, analysis and applications," *IEEE Trans. Inf. Theory*, vol. 35, no. 3, pp. 595–604, May 1989.

[14] E. L. Titlebaum, "Time-frequency hop signals, part I: Coding based upon the theory of linear congruences," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-17, no. 4, pp. 490–493, Jul. 1981.

[15] A. A. Shaar and P. A. Davies, "Prime sequences: Quasi-optimal sequences for OR channel code division multiplexing," *IEE Electron. Lett.*, vol. 19, no. 21, pp. 888–890, 1983.

[16] C. S. Chen, W. S. Wong, and Y. Q. Song, "Constructions of robust protocol sequences for wireless sensor and ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 57, no. 5, pp. 3053–3063, Sep. 2008.

[17] J. Hui, "Multiple accessing for the collision channel without feedback," *IEEE J. Select. Areas Commun.*, vol. 2, no. 4, pp. 575–582, Jul. 1984.

[18] G. Thomas, "Capacity of the wireless packet collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 1141–1144, May 2000.

[19] V. C. da Rocha Jr., "Protocol sequences for collision channel without feedback," *IEE Electron. Lett.*, vol. 36, no. 24, pp. 2010–2012, Nov. 2000.

[20] S. Tinguely, M. Rezaeian, and A. J. Grant, "The collision channel with recovery," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3631–3638, Oct. 2005.

[21] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," in *Proc. IEEE*, 1980, vol. 68, no. 5, pp. 593–619.

[22] V. Čížek, *Discrete Fourier Transforms and Their Applications*. Bristol: Adam Hilger, 1986.

[23] E. Weiss, *Algebraic Number Theory*. New York: Dover, 1998.

Kenneth W. Shum (M'00) received the B.Eng. degree in information engineering from the Chinese University of Hong Kong, Shatin, in 1993, and the M.S. and Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1995 and 2000, respectively.

He is now a Postdoctoral Fellow with the Chinese University of Hong Kong. His research interests include information theory and resource allocation in wireless networks.

Chung Shue Chen (S'02–M'05) received the B.Eng., M.Phil., and Ph.D. degrees in information engineering from the Chinese University of Hong Kong, Shatin, in 1999, 2001, and 2005, respectively.

During 2005–2006, he was an Assistant Professor with the Chinese University of Hong Kong. During 2006–2007, he was a Postdoctoral Researcher with the Centre National de la Recherche Scientifique (CNRS), Lorraine Laboratory of IT Research and Applications (LORIA), France. He was awarded an ERCIM "Alain Bensoussan" Fellowship in 2007, and worked with the Norwegian University of Science and Technology (NTNU), Norway. Under the ERCIM Fellowship programme, he is now with Centrum Wiskunde and Informatica (CWI), the Netherlands. His research interests include radio resource allocation, multiple access control, and QoS management for wireless communication systems.

Chi Wan Sung (M'98) received the B.Eng, M.Phil., and Ph.D. degrees in information engineering from the Chinese University of Hong Kong, Shatin, in 1993, 1995, and 1998, respectively.

Afterward, he became an Assistant Professor with the same university. He joined the faculty of City University of Hong Kong, Kowloon Tong, in 2000, and is now an Associate Professor with the Department of Electronic Engineering. His research interests include multiuser information theory, design and analysis of algorithms, and optimization of wireless networks.

Wing Shing Wong (M'81–SM'90–F'02) received the combined master and bachelor degree (*summa cum laude*), from Yale University, New Haven, CT, in 1976, and the M.S. and Ph.D. degrees from Harvard University, Cambridge, MA, in 1978 and 1980, respectively.

After working with AT&T Bell Laboratories, Holmdel, NJ, for 10 years, in 1992, he joined the Chinese University of Hong Kong, Shatin, where he is now a Professor of Information Engineering. He was the Chairman of the Department of Information Engineering from 1995 to 2003 and is currently serving as the Dean of the Graduate School. He served as the Science Advisor at the Innovation and Technology Commission of the HKSAR Government from 2003 to 2005. He has participated in a variety of research areas including mobile communication systems, nonlinear filtering, search engine, and estimation and control of finite communication bandwidth systems.

Dr. Wong is a Co-Editor-in-Chief of *Communications in Information and Systems*.