Constructions of Robust Protocol Sequences for Wireless Sensor and Ad hoc Networks

Chung Shue Chen, Wing Shing Wong, Ye-Qiong Song

Constructions and Analysis of Robust Protocol Sequences for Wireless Sensor and Ad-hoc Networks*

Chung Shue Chen†
LORIA-CNRS (National Center of Scientific Research)
Rue du Jardin Botanique, 54600 Villers Les Nancy, France
E-mail: chungshue.chen@loria.fr

Wing Shing Wong
Department of Information Engineering
The Chinese University of Hong Kong, Shatin, Hong Kong
E-mail: wswong@ie.cuhk.edu.hk

YeQiong Song
LORIA-INPL (National Polytechnic Institute of Lorraine)
Campus Scientifique - BP 239, 54506 Vandoeuvre-les-Nancy Cedex, France
E-mail: song@loria.fr

Abstract

In this paper, a class of periodic unipolar binary sequences are investigated for their potential applications in defining new protocols for distributed wireless multiple access. Based on linear congruence sequences, one can show that for any finite subset of these sequences with total proportional rate not exceeding a specific threshold, there cannot be enough collisions to completely block any particular sequence, no matter how they are shifted with respect to one another. This property can be exploited in certain applications such as wireless sensor and ad hoc networks. A further investigation on how to enhance the allowable rate sum is carried out. New protocol sequences with interesting and useful properties are designed accordingly.

*The work described in this paper was partially supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region (Project no. CUHK416906).
†Corresponding author.

1 Introduction

Digital sequences have found many civilian and military applications over the past semi-century. Pseudo-noise (PN) sequence [1] is one of the well-known examples. Typically, they can be classified into binary and non-binary sequences with a broad usage in various signal processing and communication systems. Applications may require specific correlation properties and structures [2]. For example, in spread spectrum systems, cross-correlation between spreading codes has a significant impact on the system performance since it reflects mutual interference among users. The number of sequences available is also one of the key measures in identifying the importance of a sequence set. Usually, there are tradeoffs between these properties due to different applications.

In wireless sensor networks [3–5], due to computing power limitation and strict energy consumption constraints, it will be favorable to have a simple multiple access protocol which does not require frequent monitoring of the channel for feedback information and does not require complicated processing such as back-off algorithm or random number generation. Besides, when considering an ad-hoc system with dynamic network topology [6] which may be due to user mobility or time-varying propagation delays, sharing a radio channel among a large number of devices with the requirement of well-coordinated transmissions and time offsets could be very complicated. This is particularly hard for thin devices. The above reasons lead to our following explorations.

To have a simple multiple access scheme for wireless sensor and ad-hoc networks, the idea of using deterministic coding sequences to define random accessing in *collision channel without feedback* [7] is worth a revisit and consideration. It is desirable to avoid the need for feedbacks and retransmissions, particularly in a mobile environment [8]. Unipolar periodic binary sequences are employed as *protocol sequences* [9] to address when a user can transmit and when it should be silent. Some related works and discussions can be found in [10–22]. In [10], linear congruence sequences were designed for time-frequency hopping systems. Independently, prime sequences were constructed [11] and applied in spread spectrum optical networks [12]. It was observed that prime sequences were closely

related to the linear congruence sequences despite they were originally constructed for different purposes [13]. In [14], some concatenated prime sequences are used for collision resolution in contention access local area networks and the result has shown their superiority over some back-off algorithms. Using constant-weight cyclically permutable codes for multiple access collision channel is reported in [15, 16]. The performance of these sequences relies on the linear cyclic codes employed and is relatively complicated to analyze. In [17], a new family of protocol sequences built on the concept of prime sequences, namely wobbling sequences, is designed to support multi-rate communication and service guarantee in random access channels. In general, the maximum number of allowable users, their throughput performance, and the length of sequence period are those major concerns. Meanwhile, correlation properties between sequences are often the important indicators [18]. For practical considerations, coding across packets can be applied to recover data lost or correct erasures due to possible collisions following typical algorithms in the literature [19–21]. Discussions on some advanced coding and decoding schemes can be found in [22] and [8] as well. Techniques of convolutional coding, data interleaving, and error correction are addressed in detail.

In this paper, a class of periodic unipolar binary sequences are investigated for the radio channel sharing among multiple users. The reported work offers an approach of distributed wireless access especially with interesting properties of individual performance guarantees. The system model is described in Section 2. Sequence designs are investigated in Section 3. For the enhancement of system's allowable rate sum, new constructions are described and considered in Section 4. Section 5 shows the numerical studies of throughput performance. Finally, some concluding remarks are presented in Section 6.

2 System Model

Following Massey's model of collision channel without feedback [7], a communication channel shared by a number of M active users is divided into time slots of equal durations. Each active user follows a unipolar binary protocol sequence, $W = \{W(0), W(1), W(2), \ldots\}$, and transmits a packet at time slot i if and only if $W(i) = 1$ [23]. A user with the per-

mission to transmit in a given time slot will transmit a data packet. Otherwise, it keeps silent. In this paper, we limit the discussion and assume that users know and align to the slot boundaries. However, users are not required to synchronize to each other. For example, different users may have different transmission starting time. They are allowed to have a relative time shift or delay offset between one another. Some practices of slot-synchronized operation and the corresponding details can be found in [24–26]. It is worth pointing out that for a full flexibility one would consider to eliminate the requirement of synchronized slot boundaries. It is in fact possible to do so and to allow users to be completely unsynchronized [9, 22, 27]. However, for the simplicity, this more general scenario will not be investigated in this paper. Here, we will focus on the slot-synchronized model.

At any time slot, a packet collision occurs if more than one user transmits simultaneously. All transmitted packets in this duration are considered lost. Otherwise, the receiver can receive its packet correctly and decode the content. Discussions on sender and packet identification issues can be found in [9, 17] for practical considerations. However, one may also consider the simple approach of requiring each packet to include a header which contains user identity and data index commonly defined in conventional MAC protocols [6] when necessary. If the payload of a packet is large enough, the cost of this overhead could be quite small comparatively.

To measure throughput performance, the *effective rate* of a user is defined as the fraction of packets it can send without suffering any collision. In a random access system, one is usually most interested in the symmetric case in which all the users are signaling at the same rate [7]. Here, we will focus on the design for symmetric users. In this scenario, it is well known that the system capacity or effective rate sum of a slot-synchronized system will approach $1/e$ as the number of active users, M, tends to infinity. However, in addition to system throughput, it is also important to look at the service reliability for each individual user. Related works in the tradition usually focus on the system throughput. However, it will be favorable to have a design which can support both system and individual performance stability such that one can always ensure the reliability of a com-

munication channel for any of the active users as long as the sum of allowable rates does not exceed a specified level.

In the following, an investigation on the class of *linear congruence sequence* [10] and its deployment for distributed wireless accessing is conducted. The analysis has also motivated our new development and the consequent constructions. The details are given below.

3 Distributed Wireless Accessing

3.1 Linear Congruence Sequence

Let $W = \{W(i), i = 0, 1, 2, \ldots\}$ be a binary sequence. The sequence W can also be represented by indexing the positions at which it has value 1, i.e., by $\{I_W(i), i = 1, 2, \ldots\}$, where $I_W(i)$ denotes the position at which the i-th entry of 1's in W appears. For a periodic binary sequence with period L, its *duty factor* [7] or proportional rate r is defined as

$$r = \frac{1}{L} \sum_{i=0}^{L-1} W(i). \tag{3.1}$$

Let b and l be two relatively prime integers with $0 \leq b < l$. The linear congruence sequence generated by (b, l) is expressible [17] as

$$I_W(i) = il + ib - \left\lfloor \frac{ib}{l} \right\rfloor l \tag{3.2}$$

where b is known as the *key generator* and i starts from 1. It can be shown that the sequence generated by (b, l) has a duty factor of $1/l$. For $b > 0$, it has a period of l^2. The sub-sequence $W = \{W(i), i = 0, 1, \ldots, l^2 - 1\}$ is known as the *core pattern*. Given $b = 0$, by substitution, (3.2) is reducible as

$$I_W(i) = il. \tag{3.3}$$

Its minimum period equals to l.

For example, given $b = 1$ and $l = 3$, following (3.2), I_W is equal to $\{4, 8, 9, \ldots\}$ while the core pattern of W is equivalent to $\{0, 0, 0, 1, 0, 0, 0, 1, 1\}$. It has a duty factor r equal to

1/3 and a period of 9.

Note that, for prime number l, the set of linear congruence sequences is also known as *prime sequences* [11], which can be obtained from a Galois field GF(l) and are representable [2] as

$$\{0, b, 2b, \ldots, (l-1)b\} \text{ modulo } l \tag{3.4}$$

where $0 \leq b \leq l-1$.

3.2 Correlation Properties

Let W_1 and W_2 be two binary sequences with common period L and duty factors r_1 and r_2 respectively. For any relative time shift s, the Hamming cross-correlation function between W_1 and W_2 is defined as

$$H_{W_1,W_2}(s) = \sum_{i=0}^{L-1} W_1(i)W_2(i+s) \tag{3.5}$$

while the normalized Hamming cross-correlation function between W_1 and W_2 is defined as

$$\bar{H}_{W_1,W_2}(s) = \frac{1}{L}\sum_{i=0}^{L-1} W_1(i)W_2(i+s). \tag{3.6}$$

Let l, b_1, and b_2 be integers satisfying $0 \leq b_1 < l$, $0 \leq b_2 < l$, $b_1 \neq b_2$, and HCF $(|b_2 - b_1|, l) = 1$; let W_1 and W_2 be the linear congruence sequences generated by (b_1, l) and (b_2, l) respectively. It is shown [17] that

$$\bar{H}_{W_1,W_2}(s) \leq 2/l^2 = 2r^2 \tag{3.7}$$

for any $0 \leq s < l^2$, where $r_1 = r_2 = r = 1/l$. For $b_1, b_2 > 0$, the equality of (3.7) holds at least once and the given upper bound is tight.

In the special case when $b_1 = 0$ or $b_2 = 0$,

$$\bar{H}_{W_1,W_2}(s) = 1/l^2 = r^2. \tag{3.8}$$

For example, given $l = 5$, let W_i be the set of sequences generated by (b_i, l), where $b_i = i$. Here, HCF$(|b_i - b_j|, 5) = 1$, for any $i \neq j$. Following (3.2),

$$\begin{bmatrix} W_1 \\ W_2 \\ W_3 \\ W_4 \end{bmatrix} = \begin{bmatrix} 000001000001000001000011 \\ 000000100000101000000101 \\ 000000010010000000100100 1 \\ 000000001000100010001 0001 \end{bmatrix}. \tag{3.9}$$

The number of coincidences or *hits* between any two distinct sequences or rows in (3.9) is given by

$$\begin{bmatrix} H_{W_1,W_2}(s) \\ H_{W_1,W_3}(s) \\ H_{W_1,W_4}(s) \\ H_{W_2,W_3}(s) \\ H_{W_2,W_4}(s) \\ H_{W_3,W_4}(s) \end{bmatrix} = \begin{bmatrix} 121011022011012112011102 1 \\ 121011021111120110121111 1 \\ 120201020211021111111201 \\ 111111102112110101121120 1 \\ 112101110212011012111111 \\ 112101200210121112011102 1 \end{bmatrix} \tag{3.10}$$

for all the relative time shifts, $s = 0, 1, 2, \ldots, l^2 - 1$. The result shown in (3.10) demonstrates that

$$0 \leq H_{W_i,W_j}(s) \leq 2. \tag{3.11}$$

Given $i = 0$, $W_0 = \{0, 0, 0, 0, 1, \ldots\}$. Comparing W_0 with each of the sequences in (3.9), one can find that

$$H_{W_0,W_j}(s) = 1 \tag{3.12}$$

for any $0 < j < l$. Fig. 1 illustrates the number of hits between any two distinct sequences in each of the relative time shifts, $s = 0, 1, 2, \ldots, 24$, when $l = 5$.

3.3 A Family of Protocol Sequences

Following the definition of (3.2), a family of periodic protocol sequences can be formulated below. To satisfy the condition for the performance of (3.7) and (3.8), and have a full flexibility in choosing the key generator b, we simply employ prime l. In the following, p is used to denote prime l. Consequently, the considered protocol sequences may also refer to prime sequences.

Definition 3.1 *For any prime p, a family of periodic binary sequences, $\mathbf{F}_p$, is defined as the set of linear congruence sequences generated by (b, p), where $0 \leq b < p$.*

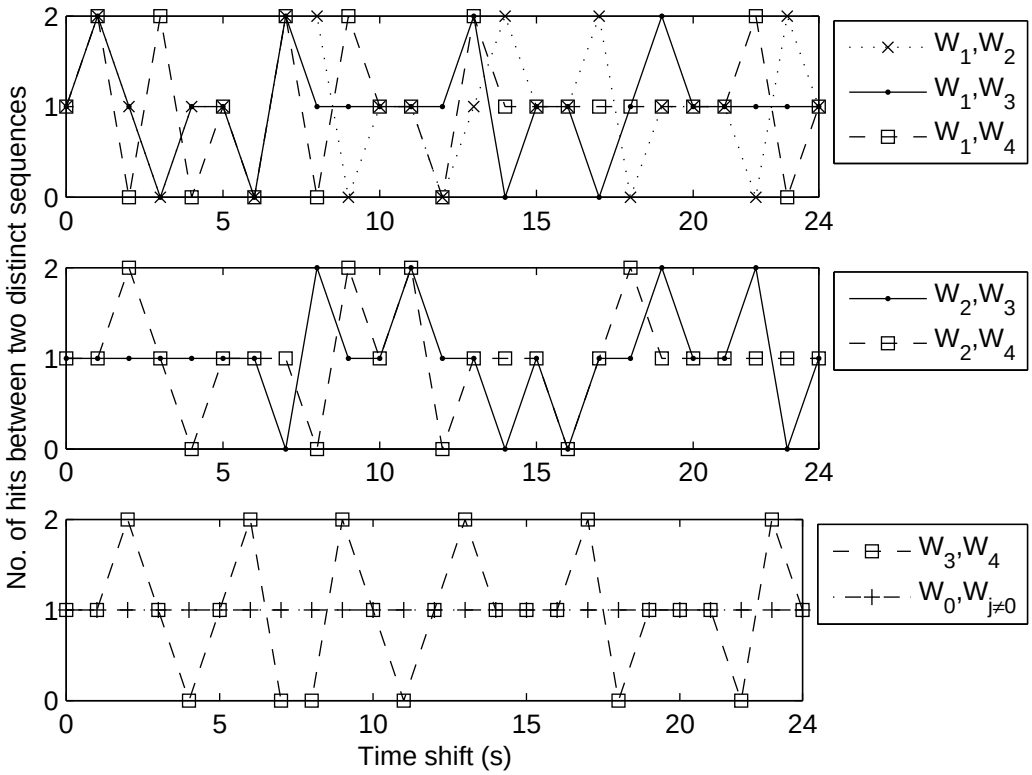

Figure 1: The number of hits between any two distinct linear congruence sequences with a relative time shift s from 0 to 24, when $l = 5$.

Note that all the sequences in $\mathbf{F}_p$ have a minimum common period $L = p^2$ and each of them has a duty factor $r_i = 1/p$. Here, we focus on the scenario of symmetric users. Following Definition 3.1, by (3.7) and (3.8),

$$\max_s \left\{ H_{W_i,W_j}(s) \right\} = 2 \tag{3.13}$$

for any $i \neq j$. Furthermore, a *non-totally-blockage* property of a set of the above sequences can be established accordingly. The details are given below.

Consider a collision channel without feedback in which multiple active users need to be supported in a distributed manner and, over a long time horizon, occasional data loss is not a serious problem or can be recovered by some channel coding [8, 22], the set $\mathbf{F}_p$ could be used to define protocol sequences for data transmissions. For any finite subset of $\mathbf{F}_p$ denoted by $\mathbf{W} = \{W_i, i = 0, \ldots, N-1\}$, where N denotes the cardinality of $\mathbf{W}$, provided that

$$\sum_{j=0, j\neq i}^{N-1} r_j \equiv \left(\sum_{j=0}^{N-1} r_j \right) - r_i < \frac{1}{2}, \tag{3.14}$$

which refers to the sum of duty factors of active users excluding r_i, by (3.5), (3.13), and (3.14), one can find that the total number of collisions to W_i is expressible as

$$\begin{aligned} \sum_{j=0, j\neq i}^{N-1} \sum_{t=0}^{L-1} W_i(t) W_j(t + s_j) &\equiv \sum_{j=0, j\neq i}^{N-1} H_{W_i,W_j}(s_j) \\ &\leq \sum_{j=0, j\neq i}^{N-1} 2 \\ &< \frac{1/2}{1/p} \times 2 \\ &= p \end{aligned} \tag{3.15}$$

or here equivalently $r_i L$, for any combination of various relative time shifts s_j of W_j with reference to W_i. (3.15) means that the number of collisions to W_i in any period L, i.e. p^2, is always less than p. Thus, there cannot have enough collisions to completely block any particular user i in any cycle as long as the sum of duty factors of active users $\{r_{j\neq i}\}$ does not exceed 1/2, even when the relative time shifts among users may change from time to time due to different reasons, for example, user mobility or time varying propagation

delay. Similarly, one can also show that as long as

$$\sum_{j=0}^{N-1} r_j \leq \frac{1}{2}, \tag{3.16}$$

for each user in the above set, at least 2 transmission packets within the common period encountered, i.e. p^2 slots, will not be blocked. This *un-suppressibility* [17] property is helpful to ensure that even in the worst case all the users can successfully transmit information to a guaranteed amount in every time period in a distributed random access manner even without the requirements of user synchronization and packet retransmissions.

However, without loss of generality, the bound on the allowable rate sum stated in (3.14) is not tight enough. One can construct examples of sequence sets in which the previously described non-totally-blockage property holds while inequality (3.14) does not hold. A natural follow-up is to enhance the maximum allowable rate sum and construct a set of corresponding sequences in terms of periodic binary sequences which possess the desirable un-suppressibility. The designs are presented below.

4 New Constructions

In this section, new constructions of periodic binary sequence sets which can have a smaller average number of collisions or the normalized cross-correlation are described. They can significantly enhance the allowable rate sum of active users in the aforementioned model.

4.1 Enhancement of Allowable Rate Sum

Recall (3.7) and (3.13), one can find that

$$H_{W_i,W_j}(s) = \{0, 1, 2\} \tag{4.1}$$

while $\bar{H}_{W_i,W_j}(s) \leq 2r^2$ for $i \neq j$. This could be a hint to construct a new set of codewords with $\bar{H}_{W_i,W_j}(s) = r^2$ based on an inspection of the following property [28] that

$$\lambda_{avg}(W_i, W_j) \triangleq \sum_{s=0}^{L-1} \bar{H}_{W_i,W_j}(s) = r_i r_j L. \tag{4.2}$$

(4.2) indicates that the average number of hits between any two sequences W_i and W_j with respective duty factors r_i and r_j over their common period L is equal to $r_i r_j L$. This is due to the fact that each of the $r_i L$ 1's in W_i will meet $r_j L$ 1's in W_j when s shifts from 0 to $1, 2, \ldots$, up to $L-1$, stepwise.

Following the definitions of (3.5) and (3.6), by (4.2), one can have the following fact that

$$\begin{aligned} \sum_{s=0}^{L-1} H_{W_i,W_j}(s) &\equiv L \cdot \sum_{s=0}^{L-1} \bar{H}_{W_i,W_j}(s) \\ &= r_i L \cdot r_j L. \end{aligned} \tag{4.3}$$

The result of (3.10) demonstrates that $\sum_{s=0}^{L-1} H_{W_i,W_j}(s) = 25$, while $\lambda_{avg}(W_i, W_j) = 1$. Here, $r_i = 1/p = 1/5$ for all i and $L = p^2 = 25$.

The average number of hits between two sequences is in fact equal to 1 after averaging out over all the relative time shifts $0 \leq s \leq L-1$. By (4.2), it is clear that the frequency of "$H_{W_i,W_j}(s) = 2$" is just the same as that of "$H_{W_i,W_j}(s) = 0$". There is no bias. $\lambda_{avg}(W_i, W_j)$ is not dominated by "$H_{W_i,W_j}(s) = 2$". The scenario is sometimes "bad", i.e. equal to 2, but sometimes "good", i.e. equal to 0. Otherwise, it is "fair" and just in between, i.e. equal to 1.

By the above observation, one way to obtain a set of periodic binary sequences with $\bar{H}_{W_i,W_j}(s) = r_i r_j$ for any relative shift s can be conducted by techniques of averaging out all the scenarios. More explicitly, we can concatenate the original prime sequences with their shifted versions so as to take and combine all the effects due to the relative time shifts. As a result, one can get the average performance, i.e. on average one collision with another sequence per p packets transmitted over their encountered common period, and maintain at this cross-correlation for any shift s. Thus, as long as

$$\sum_{j=0}^{N-1} r_j \leq 1, \tag{4.4}$$

there cannot have enough collisions to completely block any particular sequence no matter how the protocol sequences are shifted with respect to one another. This can be shown

by the following upper bound in which the number of collisions to sequence i due to all the other sequences j ($\neq i$) is strictly less than the number of packets it transmits, L/p, in the common period L. By (3.5) and (4.4),

$$\begin{aligned}
\sum_{j=0,j\neq i}^{N-1}\sum_{t=0}^{L-1} W_i(t)W_j(t+s_j) &\equiv \sum_{j=0,j\neq i}^{N-1} H_{W_i,W_j}(s_j) \\
&= \sum_{j=0,j\neq i}^{N-1}\left(\frac{L}{p}\times\frac{1}{p}\right) \\
&\leq \frac{1-(1/p)}{1/p}\left(\frac{L}{p}\times\frac{1}{p}\right) \\
&= \frac{L}{p}-\frac{L}{p^2} \\
&< L/p \qquad (4.5)
\end{aligned}$$

or equivalently r_iL, while $\sum_{j\neq i} r_j \leq 1-1/p$.

Consequently, by (4.5), the effective rate of a user with duty factor $1/p$ has a lower bound of $1/p^2$. However, it should be noted that the actual throughput could be much higher since (4.5) is just an upper bound on the number of collisions. Numerical studies in Section 5 can show more details of the throughput performance.

4.2 Construction 1

For the above properties of (4.4) and (4.5), a new design is necessary. The details are given below. Let us start with $p = 3$ to elaborate the construction. Following (3.8), since $\bar{H}_{W_0,W_1}(s) = \bar{H}_{W_0,W_2}(s) = r^2 = 1/9$, first we take W_0 and W_2 as codewords in our sequence set. Otherwise, one may choose the pair W_0 and W_1 instead. The result is equivalent.

By (3.7), $\max_s \bar{H}_{W_1,W_2}(s) = 2/9$. So, if one employs W_0, W_1, and W_2 simultaneously, W_1 (or W_2) will be completely blocked by W_2 and W_0 (respectively, W_1 and W_0) in the worst case. This can be observed in many examples and has also been verified in experiments [29]. Fig. 3 in Section 5 can show the phenomenon in general as well. A detailed discussion will be given later in Section 5.

To keep all the codewords with $\bar{H}_{W_i,W_{j\neq i}}(s) = 1/9$, one can base on (4.3) and follow the idea of "averaging out" to have the following sequence set:

$$\begin{bmatrix} W_1^{(1)} \\ W_2^{(1)} \\ W_0^{(1)} \end{bmatrix} = \begin{bmatrix} W_{1,\theta=0} & W_{1,\theta=1} & \cdots & W_{1,\theta=8} \\ W_{2,\theta=0} & W_{2,\theta=0} & \cdots & W_{2,\theta=0} \\ W_{0,\theta=0} & W_{0,\theta=0} & \cdots & W_{0,\theta=0} \end{bmatrix} \tag{4.6}$$

where $W_{i,\theta=n}$ refers to a shifted version of W_i by n bits toward the left while the superscript on $W_i^{(1)}$ is used to label the new codeword by Construction 1. For example, since $W_{1,\theta=0} \equiv W_1 = \{000100011\}$, $W_{1,\theta=1} = \{001000110\}$. Note that the new codewords need to be much longer.

Based on (4.6), one can find that, for any relative shift s,

$$\begin{aligned} \bar{H}_{W_1^{(1)},W_2^{(1)}}(s) &\equiv \frac{1}{p^4}\sum_{i=0}^{p^4-1} W_1^{(1)}(i)W_2^{(1)}(i+s) \\ &= \frac{1}{p^4}\sum_{n=0}^{p^2-1}\sum_{i=0}^{p^2-1} W_{1,\theta=n}(i)W_{2,\theta=0}(i+s) \\ &= \frac{1}{p^4}\sum_{n=0}^{p^2-1}\sum_{i=0}^{p^2-1} W_1(i)W_2(i+s-n) \\ &= \frac{1}{p^4}\sum_{n=0}^{p^2-1}\left(p^2\cdot\bar{H}_{W_1,W_2}(s-n)\right) \\ &= \frac{1}{p^4}\times p^2\times 1 \\ &= \frac{1}{p^2} \end{aligned} \tag{4.7}$$

since, by (4.2), $\sum_{n=0}^{p^2-1}\bar{H}_{W_1,W_2}(s-n) = 1$ while $r_i = 1/p$ and $L = p^2$. It is observable that the result is independent of s.

By (3.8), similarly one can also find that

$$\bar{H}_{W_0^{(1)},W_1^{(1)}}(s) = \bar{H}_{W_0^{(1)},W_2^{(1)}}(s) = 1/p^2. \tag{4.8}$$

Hence, it can be claimed that $\{W_0^{(1)}, W_1^{(1)}, W_2^{(1)}\}$ is a set of sequences with normalized Hamming cross-correlation equal to r^2 for any relative time shift s. Even when all the

codewords are used simultaneously and thus the rate sum is equal to 1, the non-totally-blockage property holds.

For sequences of duty factor equal to 1/5, to keep all the codewords with $\bar{H}_{W_i,W_{j\neq i}}(s) = 1/25$, a new set of protocol sequences can be constructed similarly as the following:

$$\begin{bmatrix} W_1^{(1)} \\ W_2^{(1)} \\ W_3^{(1)} \\ W_4^{(1)} \\ W_0^{(1)} \end{bmatrix} = \begin{bmatrix} [W_{1,\theta=0} \ \cdots \ W_{1,\theta=24}]_{25\times 25} \\ \left[[W_{2,\theta=0}]_{25} \ \cdots \ [W_{2,\theta=24}]_{25}\right]_{25} \\ [W_{3,\theta=0}]_{25\times 25} \ \cdots \ [W_{3,\theta=24}]_{25\times 25} \\ [W_{4,\theta=0}]_{25\times 25\times 25} \\ [W_{0,\theta=0}]_{25\times 25\times 25} \end{bmatrix} \tag{4.9}$$

where $W_{i,\theta=n}$ represents a shifted version of W_i by n bits toward the left and $[W_i]_k$ refers to a concatenation of k copies of W_i consecutively. The incentive is to extend the original sequences such that for any two distinct sequences all the shift combinations are included. Consequently, no matter how the shift is, the resultant cross-correlation always contains all the good, bad, and fair scenarios. So, by (4.2),

$$\bar{H}_{W_i^{(1)},W_j^{(1)}}(s) = 1/p^2. \tag{4.10}$$

The proof is very similar to that in (4.7) and thus omitted. One can conclude that even when all the codewords in (4.9) are used simultaneously in an application with active users of rate sum equal to 1, the non-totally-blockage property still holds.

Following the definition of prime sequence, for each p, a set of corresponding sequences with $\bar{H}_{W_i,W_{j\neq i}}(s) = 1/p^2$ can be constructed in an iterative way. It is worth pointing out that the proposed idea of "averaging out" is generally applicable to any sequence set as long as the property of (4.2) holds. Similar constructions and results are achievable.

On the other hand, as aforementioned, the new sequence needs to be much longer than the original one. Let $L_p^{(1)}$ be the length of codewords in Construction 1 for the set of p. Since $W_0^{(1)}$ requires only a simple concatenation, we have

$$L_p^{(1)} = \left(p^2\right)^{p-1} = p^{2(p-1)}. \tag{4.11}$$

To give a demonstration, let $p = 3$, $L_3^{(1)} = 3^4 = 81$. Respectively, $L_5^{(1)} = 25^4$. It should be noted that $L_p^{(1)}$ could be very large as (4.11) is exponentially increasing. For example, when $p = 7$, $L_7^{(1)} = 7^{12}$. In a channel of 250 kb/s, it will take about 5.54×10^4 seconds to complete one sequence cycle. This could be a problem for applications. A natural follow-up is to look for a shorter required codeword length. Construction 2 is thus proposed below.

4.3 Construction 2

In the previous construction, we may have excessively collected too many copies of the variants or shifted versions of the original sequences to achieve the result of averaging out all the cross-correlations by the observation of (4.2). However, some concatenations may not be necessary.

In an investigation of the cross-correlations between linear congruence sequences generated by (b, l) [17], the following property can be established for prime l such that

$$\sum_{s=0}^{p-1} \bar{H}_{W_i,W_j}(s \cdot p + t) = 1/p \tag{4.12}$$

for any integer $0 \leq t < p$, where $i \neq j$ and p is a prime number. For example, given $p = 5$,

$$\begin{aligned} \sum_{\tau=0,5,10,15,20} \bar{H}_{W_i,W_j}(\tau) &= \sum_{\tau=1,6,11,16,21} \bar{H}_{W_i,W_j}(\tau) \\ &= \cdots = \sum_{\tau=4,9,14,19,24} \bar{H}_{W_i,W_j}(\tau) = 1/5. \end{aligned} \tag{4.13}$$

Thus, a design that contains concatenations with relative time shift combinations over the set $\{0, p, 2p, \ldots, p(p-1)\}$ is sufficient to characterize the overall cross-correlation performance and represent all the good, bad, and fair scenarios. For $p = 3$, the new construction can be expressed as:

$$\begin{bmatrix} W_1^{(2)} \\ W_2^{(2)} \\ W_0^{(2)} \end{bmatrix} = \begin{bmatrix} W_{1,\theta=0} & W_{1,\theta=3} & W_{1,\theta=6} \\ W_{2,\theta=0} & W_{2,\theta=0} & W_{2,\theta=0} \\ W_{0,\theta=0} & W_{0,\theta=0} & W_{0,\theta=0} \end{bmatrix}. \tag{4.14}$$

By (4.14) and (4.12), the normalized cross-correlation is given below:

$$\begin{aligned}
\bar{H}_{W_1^{(2)},W_2^{(2)}}(s) &\equiv \frac{1}{p^3}\sum_{i=0}^{p^3-1} W_1^{(2)}(i)W_2^{(2)}(i+s) \\
&= \frac{1}{p^3}\sum_{n=0}^{p-1}\sum_{i=0}^{p^2-1} W_{1,\theta=np}(i)W_{2,\theta=0}(i+s) \\
&= \frac{1}{p^3}\sum_{n=0}^{p-1}\sum_{i=0}^{p^2-1} W_1(i)W_2(i+s-np) \\
&= \frac{1}{p^3}\sum_{n=0}^{p-1}\left(p^2\cdot\bar{H}_{W_1,W_2}(s-np)\right) \\
&= \frac{1}{p^3}\times p^2\times\frac{1}{p} \\
&= \frac{1}{p^2}. \qquad (4.15)
\end{aligned}$$

Similarly, by (3.8), it can be shown that $\bar{H}_{W_0^{(2)},W_1^{(2)}}(s) = \bar{H}_{W_0^{(2)},W_2^{(2)}}(s) = 1/p^2$. Hence, even when all the codewords, $W_0^{(2)}, W_1^{(2)}$, and $W_2^{(2)}$, are used simultaneously and thus the rate sum of active users is equal to 1, the non-totally-blockage property is still maintained.

For $p = 5$, the construction can be formulated iteratively as

$$\begin{bmatrix} W_1^{(2)} \\ W_2^{(2)} \\ W_3^{(2)} \\ W_4^{(2)} \\ W_0^{(2)} \end{bmatrix} = \begin{bmatrix} [W_{1,\theta=0}\ W_{1,\theta=5}\ \cdots\ W_{1,\theta=20}]_{5\times5} \\ \left[[W_{2,\theta=0}]_5\,[W_{2,\theta=5}]_5\ \cdots\ [W_{2,\theta=20}]_5\right]_5 \\ [W_{3,\theta=0}]_{5\times5}\,[W_{3,\theta=5}]_{5\times5}\ \cdots\ [W_{3,\theta=20}]_{5\times5} \\ [W_{4,\theta=0}]_{5\times5\times5} \\ [W_{0,\theta=0}]_{5\times5\times5} \end{bmatrix}. \qquad (4.16)$$

Consequently, $\bar{H}_{W_i^{(2)},W_j^{(2)}}(s) = 1/p^2$ for any $j \neq i$. Even when $\sum_j r_j = 1$, the non-totally-blockage property holds.

Codewords of different p can be constructed in an iterative way and are given below:

$$\begin{bmatrix} W_1^{(2)} \\ W_2^{(2)} \\ W_3^{(2)} \\ \vdots \\ W_{p-2}^{(2)} \\ W_{p-1}^{(2)} \\ W_0^{(2)} \end{bmatrix} = \begin{bmatrix} \left[W_{1,\theta=0}\ W_{1,\theta=p}\ \cdots\ W_{1,\theta=(p-1)p}\right]_{p^{(p-3)}} \\ \left[\,[W_{2,\theta=0}]_p\,[W_{2,\theta=p}]_p\ \cdots\ \left[W_{2,\theta=(p-1)p}\right]_p\,\right]_{p^{(p-4)}} \\ \left[\,[W_{3,\theta=0}]_{p^2}\,[W_{3,\theta=p}]_{p^2}\ \cdots\ \left[W_{3,\theta=(p-1)p}\right]_{p^2}\,\right]_{p^{(p-5)}} \\ \vdots \\ \left[\,[W_{p-2,\theta=0}]_{p^{(p-3)}}\,[W_{p-2,\theta=p}]_{p^{(p-3)}}\ \cdots\ \left[W_{p-2,\theta=(p-1)p}\right]_{p^{(p-3)}}\,\right]_{p^0} \\ [W_{p-1,\theta=0}]_{p^{(p-2)}} \\ [W_{0,\theta=0}]_{p^{(p-2)}} \end{bmatrix}. \qquad (4.17)$$

Let $L_p^{(2)}$ be the length of codewords in Construction 2. According to (4.17),

$$L_p^{(2)} = p^2 \times p^{p-2} = p^p. \tag{4.18}$$

For example, $L_3^{(2)} = 3^3 = 27$, while $L_5^{(2)} = 5^5 = 3125$. Comparing (4.18) with (4.11), their ratio is given by

$$\frac{L_p^{(2)}}{L_p^{(1)}} = \frac{p^p}{p^{2(p-1)}} = \frac{1}{p^{p-2}} \tag{4.19}$$

which indicates a big reduction in the codeword length by Construction 2 when compared with Construction 1. To have a demonstration, when $p = 7$, $L_7^{(2)} = 7^7$. In a channel of 250 kb/s, it takes about 3.29 seconds to complete one cycle. This is much smaller than that of 5.54×10^4 seconds in Construction 1 and could be acceptable for certain applications. For reference, Fig. 2 shows a comparison between $L_p^{(1)}$ and $L_p^{(2)}$ with respect to different p and measured in channels with data rates: (i) 250 kb/s, (ii) 10 Mb/s, and (iii) 1 Gb/s respectively. The result has indicated a significant improvement by Construction 2 in general.

However, it should be noted that $L_p^{(2)}$ is still exponentially increasing, despite it is much smaller than $L_p^{(1)}$. As a result, the number of active users to be supported simultaneously will be limited if long codewords are not allowable. A further improvement on the design of codewords will be favorable and left open. Generally speaking, there are tradeoffs between different performance criteria.

5 Throughput Evaluation

Investigations on the effective rates of users following the protocol sequences by Construction 1 and Construction 2 in the slot-synchronized collision channel are conducted respectively. Both individual and system throughputs are measured. In the simulation, we assume there are M active users and each will transmit in a rate $1/p$ of the channel bandwidth. The protocol sequences are used to specify their channel access permission time. Accordingly, a user will transmit a packet at the time slot when its protocol sequence refers to '1'. Otherwise, it is in an idle state.

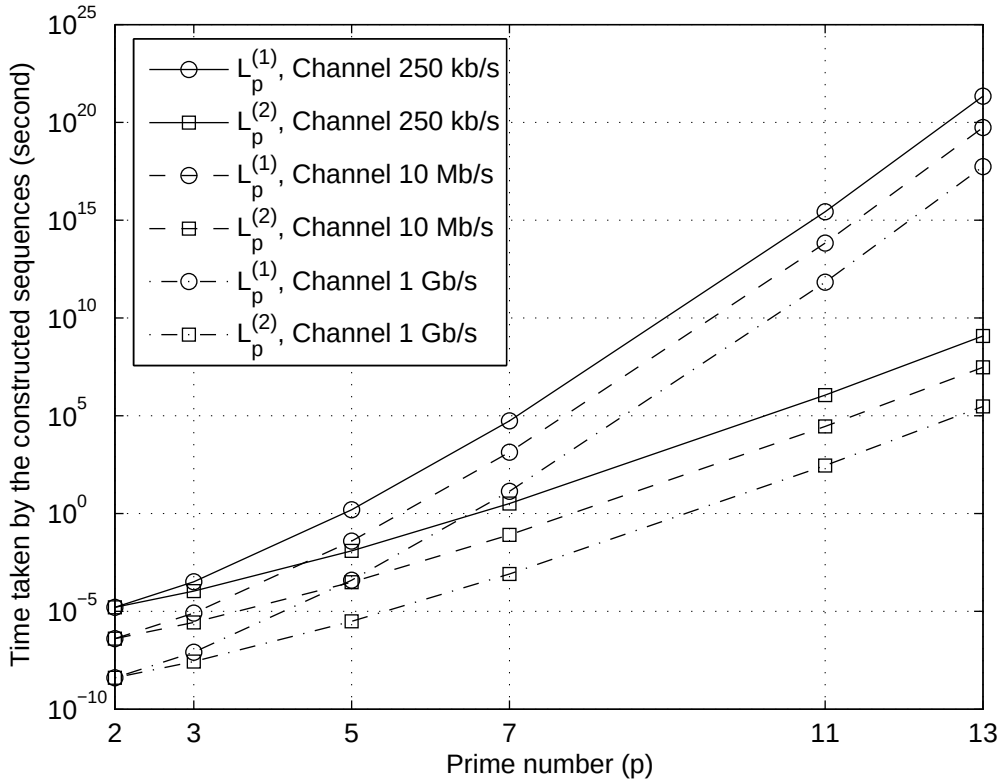

Figure 2: The time taken by the constructed sequences in their encountered periods with respect to different p and measured in channels: (i) 250 kb/s, (ii) 10 Mb/s, and (iii) 1 Gb/s respectively.

A number of p protocol sequences with the key generator

$$b = \{0, 1, 2, \ldots, p-1\} \tag{5.1}$$

are constructed respectively. Each has a duty factor equal to $1/p$. Since users are unsynchronized to each other and may have different transmission starting time, there will be various combinations of relative time shifts among them. In the simulation, we assume that the relative time shift s between two users is uniformly distributed in their encountered minimum period.

User throughputs (individual effective rates) are measured when the system is fully saturated, i.e.,

$$\sum_{i=1}^{M} r_i = 1 \tag{5.2}$$

where $M = p$ and $r_i = 1/p$. Data are evaluated after a simulation of 10^5 runs for various time shift combinations. Results obtained show that the protocol sequences from Construction 1 and Construction 2 have the same performance exactly. Thus, in the following, only one set of the data are plotted. However, the plotted results can represent both Construction 1 and Construction 2, and are simply labeled as "New".

Fig. 3 shows the individual throughputs of users with respect to different p. Each throughput is measured with respect to its encountered minimum period. The minimum, mean, and maximum values of individual throughputs obtained from the new constructions are plotted and compared with those obtained from prime sequences and a random access respectively. In the random access, it is assumed that at each time slot a user will transmit a packet with probability equal to its duty factor $1/p$ and in uniform distribution. The effective rate of a user in the random access scheme is measured in durations same as the periods of prime sequences with respect to different p.

Comparing the performance of the new construction, prime sequences, and random access, the means of their individual throughputs are the same. This is expected as long as the mean is taken by averaging the throughputs of users with uniformly distributed relative time shifts. One can also observe from Fig. 5 that they have the same average system throughput as well. The range of individual throughputs from simulation is indicated by [Min, Max] and shown in Fig. 3, while the standard deviation is plotted in Fig. 4 to indicate the performance fluctuations. As shown in Fig. 3, a user with prime sequence can be completely blocked by other active users in the collision channel and the minimum individual throughput is equal to zero. The random access has the same problem. Meanwhile, the new construction has demonstrated its robustness that there cannot have enough collisions to completely block any particular sequence no matter how they are shifted with respect to one another. It can eliminate the risk of being completely blocked. More importantly, both Fig. 3 and Fig. 4 show that the new construction has a *zero variance* of individual throughputs among all the users and for any relative time shift combination in simulations. In other words, users have the same and *shift invariant*

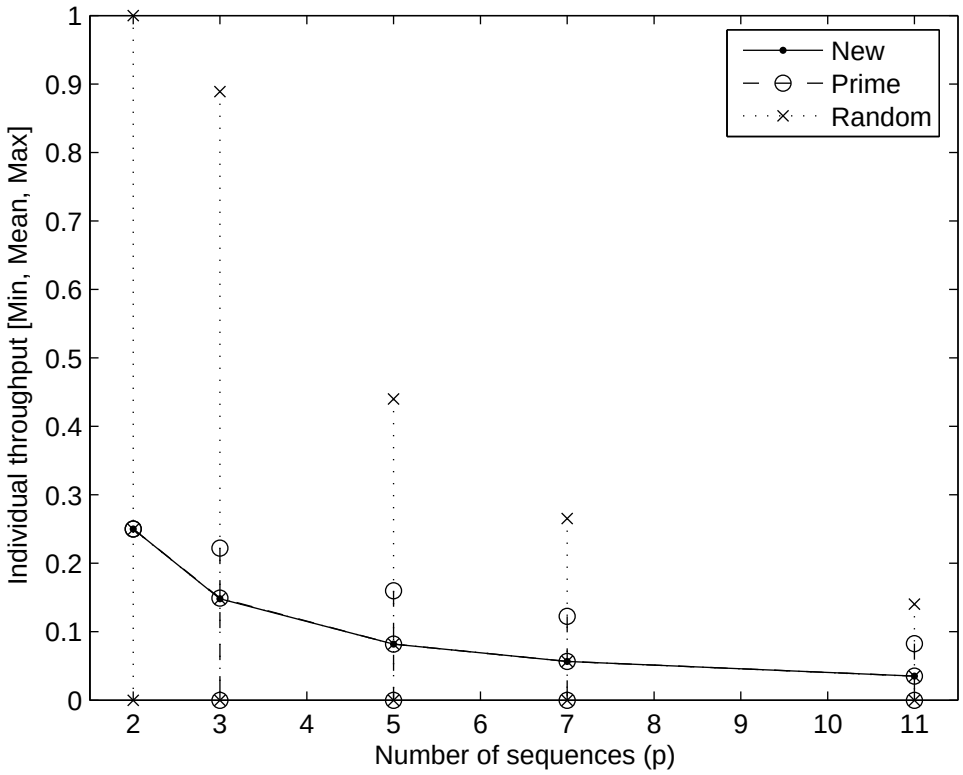

Figure 3: The minimum, mean, and maximum individual throughputs from simulation are shown. The duty factor of a user is equal to $1/p$.

individual throughput. This indicates an extremely stable throughput performance in contrast to the highly fluctuated performance in the prime sequence and random access schemes. The result is helpful to provide a deterministic performance guarantee and could be particularly useful and convenient for channel coding purposes.

It should be noted that the new construction will have a longer sequence period, p^p, than that of prime sequence, p^2, in general. Besides, in the prime sequence and random access schemes, the probability of obtaining zero individual throughput could be smaller when the throughput is measured over a longer period. With reference to the studies in [29], the random access scheme could obtain a smaller variance of individual throughput, while the difference to prime sequences appears insignificant. However, without loss of generality, a user in these two schemes always has a non-zero probability of being completely blocked. In addition, although the average individual throughputs in these three schemes are the

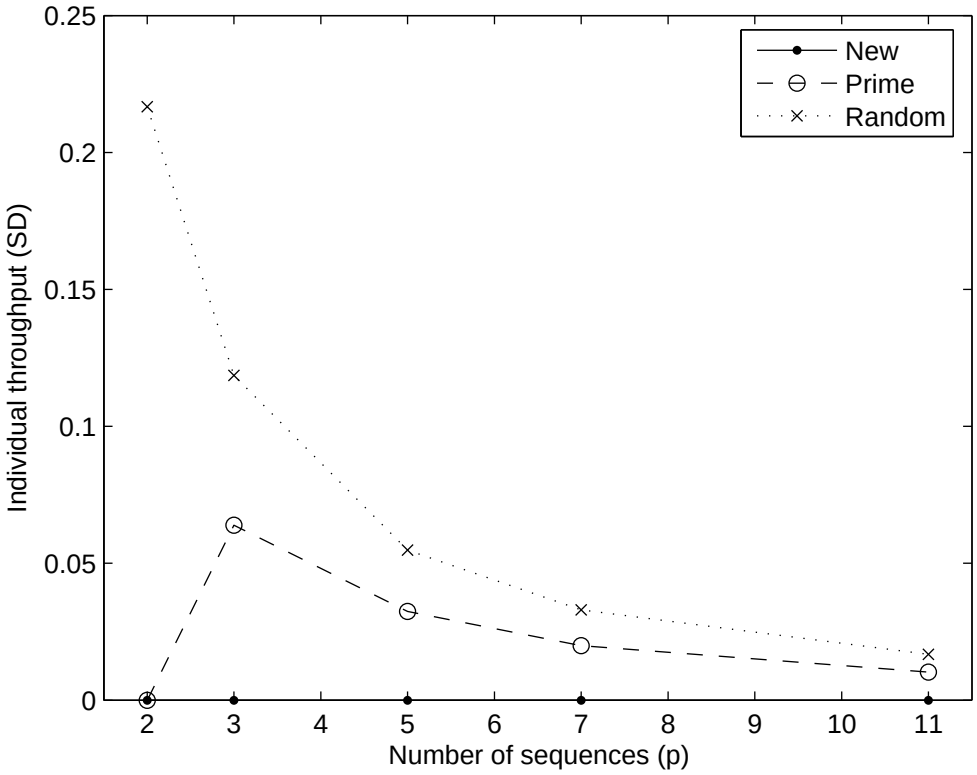

Figure 4: The standard deviations (SD) of individual throughputs are shown for reference. The result is associated with Fig. 3.

same, the new construction guarantees a higher minimum throughput generally as shown in Fig. 3.

Fig. 5 and Fig. 6 show the system throughputs and their standard deviations respectively. It is expected that the average system throughput tends to e^{-1} as p goes to infinity [24]. In addition to the average performance, it is observable that the new construction has a zero variance of system throughput as well. However, as shown in Fig. 5 and Fig. 6, both the prime sequence and random access schemes have high fluctuation in system throughput. It is worth pointing out that the new construction supports a very robust and stable system performance. Meanwhile, it is capable of ensuring the non-totally-blockage of each individual user.

Furthermore, we have conducted a performance comparison between the protocol se-

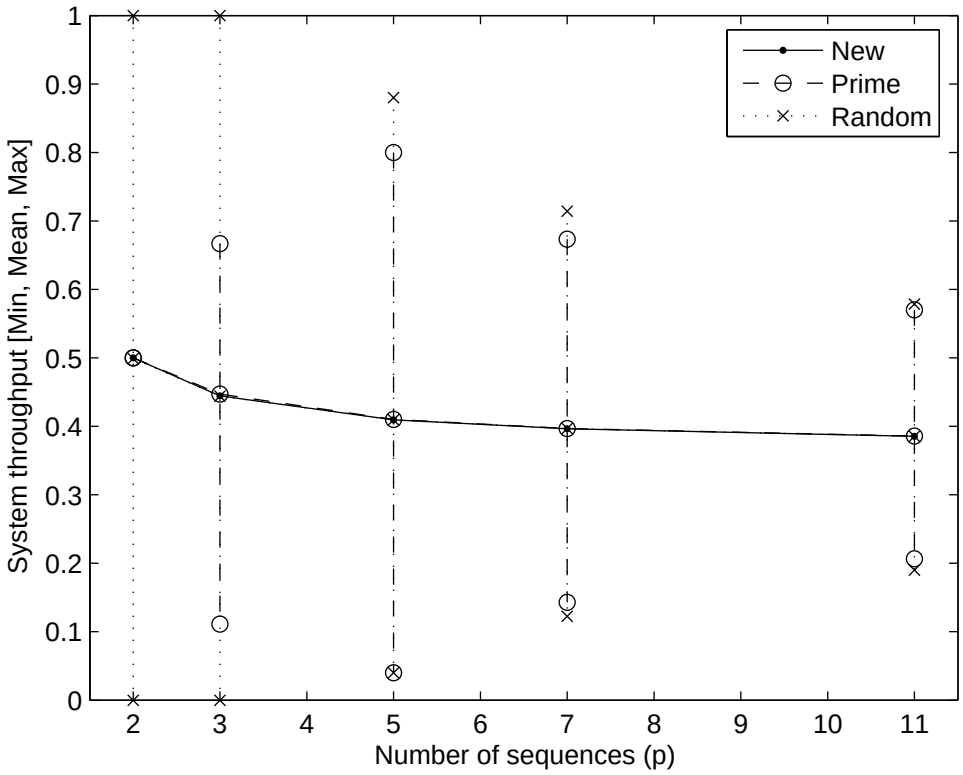

Figure 5: The minimum, mean, and maximum system throughputs from simulation are shown with respect to different prime p.

quences from Construction 2 and Massey's work [9]. Both of them have the same sequence period in this model. Fig. 7 indicates the similarity and difference. Numerical studies show that both of them have the same average individual and system throughputs when the effective rates are measured over complete cycles of their minimum periods. Besides, it is observed that Massey's construction also yields a zero variance on individual and system throughputs as well. However, when effective throughputs are considered in partial periods for practical considerations as the period is exponential, there is a significant difference between the two designs. Fig. 7 shows their standard deviations of individual throughputs measured over 1/8, 1/4, 1/2, and one sequence periods respectively. Result shows that the new construction outperforms and has a much smaller performance fluctuation in partial periods generally. However, it should be noted that [9] is more focused on determining the general capacity regions and also finds out interesting techniques of packet recovery and decimation decoding skills for sender identification.

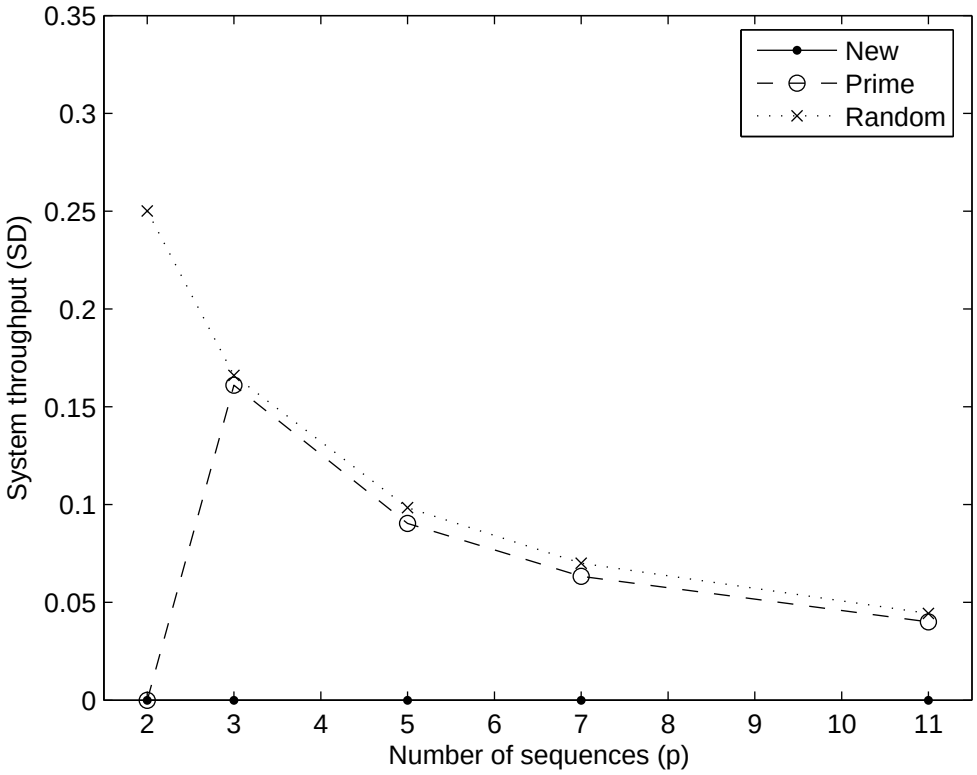

Figure 6: The standard deviations (SD) of system throughputs are shown for reference. The result is associated with Fig. 5.

Note that individual and system throughputs of the new constructions are expressible in closed-form solutions. Appendix I shows the analytical results for reference. One can find that they meet the capacity bound as given in [9] under the slot-synchronized access model as well. Besides, one can find that for the symmetric rate case, the minimum necessary length of the protocol sequences with zero-variance individual and system throughputs is in fact equal to p^p. A proof is given in Appendix II. Generally speaking, there is always a tradeoff between the period length of protocol sequences and the variance of throughput performance. If a higher variance of throughput performance is allowed, the length of the protocol sequences can be reduced.

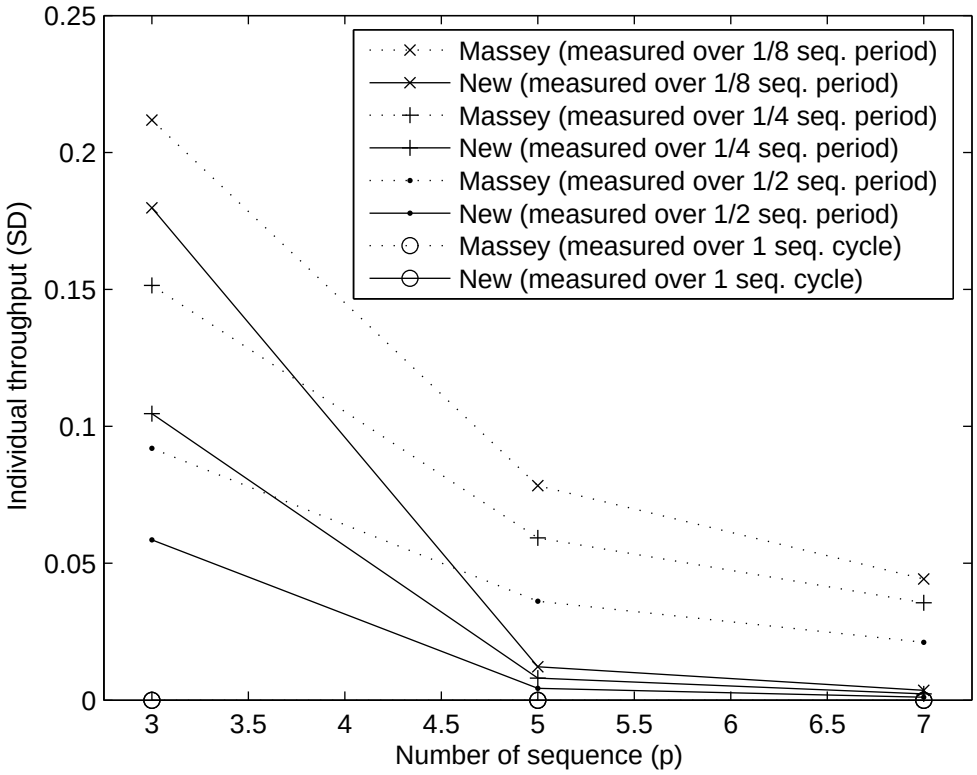

Figure 7: The standard deviations (SD) of individual throughputs measured over 1/8, 1/4, 1/2, and one sequence periods are plotted respectively.

6 Concluding Remarks

In this paper, a class of linear congruence sequences with interesting cross-correlation properties are investigated. Their characteristics reported have led to new designs of protocol sequences which have the following major advantages. While possessing the feature of non-totally-blockage, the enhancement allows a higher rate sum equal to 1. Meanwhile, no matter how the protocol sequences are shifted with respect to one another, no one will be completely blocked. It ensures the reliability of a communication channel for every user. Besides, this robust protocol does not require complicated processing such as back-off algorithm or random number generation. Moreover, it is found that the new design has a zero variance in both individual and system throughputs which corresponds to a very stable service and is capable of providing deterministic performance guarantees in applications. When compared the performance with [9] in partial periods, the new construction is better and has a much smaller throughput fluctuation. The reported work

shows its performance stability, robustness, and especially individual deterministic performance guarantees.

On the other hand, since the protocol sequences are deterministic and periodic, generally speaking a receiver does not require to continuously listen the channel in data reception. Once a packet is successfully received, the corresponding receiver can explicitly address on the incoming ones since the sender's transmission time can be easily determined by the information of (b, p) and packet sequence index in a header. This operation can be more energy efficient. Furthermore, by the periodicity of sequences, one can avoid some collisions in a cooperative approach to have system throughput enhancement when this is a major concern [29]. It should be noted that the current design has a drawback that the period is exponential. A further improvement on the design will be favorable. The study presented here may also lead to other interesting schemes and applications in different communication systems.

Appendix I: Effective Rates of the Sequence Set

In a system of symmetric users with protocol sequences from Construction 1 and each with duty factor $r_j = 1/p$, the individual throughput, $\tilde{r}_j$, is expressible as:

$$\tilde{r}_j = \sum_{i=1}^{p} (1/p)^i (-1)^{i-1} \begin{pmatrix} p-1 \\ i-1 \end{pmatrix} \tag{A.1}$$

for all j, while the system throughput is equal to

$$\begin{aligned} \sum_{j=0}^{p-1} \tilde{r}_j &= p \sum_{i=1}^{p} (1/p)^i (-1)^{i-1} \begin{pmatrix} p-1 \\ i-1 \end{pmatrix} \\ &= \sum_{i=1}^{p} (1/p)^{i-1} (-1)^{i-1} \begin{pmatrix} p-1 \\ i-1 \end{pmatrix} \\ &= \sum_{i=0}^{p-1} (1/p)^i (-1)^i \begin{pmatrix} p-1 \\ i \end{pmatrix} \\ &= \sum_{i=0}^{p-1} (-1/p)^i (1)^{(p-1)-i} \begin{pmatrix} p-1 \\ i \end{pmatrix} \\ &= (1-1/p)^{p-1}. \end{aligned} \tag{A.2}$$

It is found that the result of (A.2) is consistent with the symmetric capacity bound of the

M-user collision channel without feedback [9]:

$$C_{\text{sym}} = \left(1 - \frac{1}{M}\right)^{M-1} \tag{A.3}$$

with corresponding achievable rate point

$$(C_{\text{sym}}/M, C_{\text{sym}}/M, \ldots, C_{\text{sym}}/M) \tag{A.4}$$

expressible as (A.1) for each user.

The proof of (A.1) for Construction 1 can be done similarly to that of Lemma 2 in [9]. The detail is given below. Consider the generated codewords in a binary matrix whose rows correspond to the protocol sequences, due to the sequence concatenation of all the combinations in Construction 1, no matter how the protocol sequences are cyclically shifted, it always results as a permutation of the columns. Thus, the resultant matrix will contain the same number of collisions and successful transmissions regardless of the time offsets. Due to the symmetry, similarly to (4.2), the number of commonly overlapped '1's among a number of k protocol sequences, for any $2 \leq k \leq p$, is equal to:

$$\begin{aligned} &\frac{1}{L^k} \sum_{s_k=0}^{L-1} \cdots \sum_{s_2=0}^{L-1} \sum_{i=0}^{L-1} \left[W_1(i)\, W_2(i+s_2) \;\; \cdots \;\; W_k(i+s_k) \right] \\ &= \frac{(L/p)^k}{L^k} \\ &= \frac{1}{p^k} \end{aligned} \tag{A.5}$$

where s_j is used to denote the relative time shift of W_j with reference to W_1. Besides, the result of (A.5) is independent of j and thus applicable to all the users. This leads to the expression of (A.1). Consequently, one can find that there is a zero variance individual throughput among all. At the same time, the variance of system throughput is equal to zero as well.

A mathematical proof of (A.1) for Construction 2 is not available here due to the complexity, despite conceptually Construction 2 is just inherited from Construction 1 with (4.12). However, all the numerical results obtained from Construction 2 agree with (A.1) and (A.2).

Appendix II: The Minimum Necessary Period Length

Consider a set of periodic binary sequences, $\{S_1, S_2, \ldots, S_p\}$, of symmetric rate $1/p$ with common period L. Each of them contains (L/p) 1's.

If the number of coincidences between two sequences, say S_1 and S_2, is shift invariant for any $0 \leq s \leq L-1$,

$$\sum_{s=0}^{L-1} H_{S_1 S_2}(s) = L \times H_{S_1 S_2}(s). \tag{A.6}$$

Similarly to (4.2), since each of the (L/p) 1's in S_1 will meet (L/p) 1's in S_2 when s shifts from 0 to $1, 2, \ldots$, up to $L-1$,

$$\sum_{s=0}^{L-1} H_{S_1 S_2}(s) \equiv \sum_{s=0}^{L-1} \sum_{i=0}^{L-1} S_1(i) S_2(i+s) = \frac{L}{p} \times \frac{L}{p}. \tag{A.7}$$

By (A.6) and (A.7),

$$H_{S_1 S_2}(s) = \frac{(L/p) \times (L/p)}{L} = \frac{L}{p^2}. \tag{A.8}$$

That is, two sequences will meet at L/p^2 times.

Let us consider the number of common coincidences of three sequences, say S_1, S_2, and S_3, which can be expressed as:

$$H_{S_1 S_2 S_3}(\mathbf{s}) \equiv \sum_{i=0}^{L-1} S_1(i) S_2(i+s_2) S_3(i+s_3) \tag{A.9}$$

where $\mathbf{s} = (s_2, s_3)$ represents the relative time shifts of S_2 and S_3 with reference to S_1.

Denote the intersection of sequences $\{S_1(i)\}$ and $\{S_2(i+s_2)\}$ by $\{S_1 \cap S_2(i, s_2)\}$. If the number of coincidences between two sequences is shift invariant, by (A.8),

$$\sum_{i=0}^{L-1} S_1 \cap S_2(i, s_2) = \frac{L}{p^2}. \tag{A.10}$$

Similarly to (A.7), following (A.9) and (A.10),

$$\begin{aligned}\sum_{s_3=0}^{L-1} H_{S_1S_2S_3}(\mathbf{s}) &\equiv \sum_{s_3=0}^{L-1}\sum_{i=0}^{L-1} S_1(i)\, S_2(i+s_2)\, S_3(i+s_3) \\ &= \sum_{s_3=0}^{L-1}\sum_{i=0}^{L-1} (S_1 \cap S_2(i,s_2))\, S_3(i+s_3) \\ &= \frac{L}{p^2} \times \frac{L}{p}. \end{aligned} \tag{A.11}$$

So, if the number of common coincidences of three sequences is also shift invariant, by the result of (A.11),

$$H_{S_1S_2S_3}(\mathbf{s}) = \frac{(L/p^2) \times (L/p)}{L} = \frac{L}{p^3}. \tag{A.12}$$

That is, the three sequences meet commonly at L/p^3 times.

If the number of common coincidences of n sequences is shift invariant for $n = 2, \ldots, k$, where $k \leq p$, i.e., $H_{S_1S_2}, H_{S_1S_2S_3}, \ldots,$ and $H_{S_1S_2S_3\cdots S_k}$ are shift invariant, by induction,

$$H_{S_1S_2S_3\cdots S_k}(\mathbf{s}) = \frac{(L/p^{k-1}) \times (L/p)}{L} = \frac{L}{p^k}. \tag{A.13}$$

That is, k sequences meet commonly at L/p^k times.

Therefore, for p sequences, if $\left\{H_{S_1S_2}, H_{S_1S_2S_3}, \ldots, H_{S_1S_2S_3\cdots S_p}\right\}$ is shift invariant,

$$H_{S_1S_2S_3\cdots S_p}(\mathbf{s}) = \frac{L}{p^p}. \tag{A.14}$$

Since by definition the sequences have positive duty factors, they must meet at least once. So,

$$\frac{L}{p^p} \geq 1 \tag{A.15}$$

which implies

$$L \geq p^p. \tag{A.16}$$

Hence, one can conclude that for the symmetric rate case, the minimum necessary period length of the $\left\{H_{S_1S_2}, H_{S_1S_2S_3}, \ldots, H_{S_1S_2S_3\cdots S_p}\right\}$ shift invariant protocol sequences is equal to p^p.

Note that, if only a number of $2 \leq k \leq p$ protocol sequences with symmetric rate $1/p$ are needed, the minimum sequence period length required for the $\{H_{S_1S_2}, H_{S_1S_2S_3}, \ldots, H_{S_1S_2S_3\cdots S_k}\}$ shift invariant cross-correlation property is equal to p^k as $L/p^k \geq 1$. Besides, this shift invariant cross-correlation property also implies shift invariant individual and system throughputs, Consequently, the individual throughput is given by

$$\sum_{i=1}^{k} \left(\frac{1}{p}\right)^i (-1)^{i-1} \left(\begin{array}{c} k-1 \\ i-1 \end{array} \right) \tag{A.17}$$

while the system throughput is expressible as

$$k \sum_{i=1}^{k} \left(\frac{1}{p}\right)^i (-1)^{i-1} \left(\begin{array}{c} k-1 \\ i-1 \end{array} \right). \tag{A.18}$$

They are consistent with (A.1) and (A.2).

References

[1] S. Haykin, *Communication Systems*, New York: Wiley, 1994, pp. 579–586.

[2] P. Fan and M. Darnell, *Sequence Design for Communications Applications*, England: Research Studies Press; New York: John Wiley, 1996.

[3] 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.

[4] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for networked sensors," *ACM SIGPLAN Notices*, vol. 35, no. 11, pp. 93–104, Nov. 2000.

[5] I. Demirkol, C. Ersoy, and F. Alagoz, "MAC protocols for wireless sensor networks: a survey," *IEEE Commun. Magazine*, vol. 44, no. 4, pp. 115–121, Apr. 2006.

[6] R. Jurdak, C. V. Lopes, and P. Baldi, "A survey, classification and comparative analysis of medium access control protocols for ad hoc networks," *IEEE Commun. Surveys*, vol. 6, no. 1, pp. 2–16, 2004.

[7] J. L. Massey, "The capacity of the collision channel without feedback," *Proc. IEEE Int. Symp. Inform. Theory*, June 1982, pp. 101.

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

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

[10] 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, July 1981.

[11] 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, Oct. 1983.

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

[13] A. A. Shaar and P. A. Davies, "A survey of one-coincidence sequences for frequency-hopped spread-spectrum systems," *IEE Proceedings*, vol. 131, pt. F, no. 7, pp. 719–724, Dec. 1984.

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

[15] 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.

[16] L. Györfi and I. Vajda, "Construction of protocol sequences for multiple-access collision channel without feedback," *IEEE Trans. Inform. Theory*, vol. 39, no. 5, pp. 1762-1765, Sept. 1992.

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

[18] G.-C. Yang and W. C. Kong, *Prime Codes with Applications to Optical and Wireless Networks*, Boston: Artech House, 2002.

[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. Inform. Theory*, vol. 51, no. 10, pp. 3631–3638, Oct. 2005.

[21] R. G. Gallager, "A perspective on multiaccess channels," *IEEE Trans. Inform. Theory*, vol. 31, no. 2, pp. 124–142, Mar. 1985.

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

[23] C. S. Chen and W. S. Wong, "Bandwidth allocation for wireless multimedia systems with most regular sequences," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 635–645, Mar. 2005.

[24] L. G. Roberts, "Dynamic allocation of satellite capacity through packet reservations," *Proc. National Computer Conf.*, 1973, pp. 711–716.

[25] IEEE Std 802.11, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," *IEEE-SA Standards Board*, 1999.

[26] IEEE Std 802.15.4-2006, "Wireless medium access (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs)," *IEEE-SA Standards Board*, Sept. 2006.

[27] S. Csibi and L. Györfi, "Random time and frequency hopping for unslotted asynchronous access," *Proc. IEEE Int. Symp. Spread Spectrum Tech. Appl.*, Mainz, Germany, Sept. 1996, pp. 1123–1127.

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

[29] C. S. Chen and W. S. Wong, "A robust access protocol for wireless sensor networks," *Proc. IEEE Military Commun. Conf.*, Washington D.C., Oct. 2006, pp. 1–6.