The Design and Analysis of Protocol Sequences for Robust Wireless Accessing

Chung Shue Chen
LORIA-CNRS
Villers Les Nancy, France
Email: chungshue.chen@loria.fr

Wing Shing Wong
Dept of Information Engineering
The Chinese Univ. of Hong Kong, Hong Kong
Email: wswong@ie.cuhk.edu.hk

Ye-Qiong Song
LORIA-INPL
Villers Les Nancy, France
Email: song@loria.fr

***Abstract*—In this paper, a family of linear congruence sequences with interesting cross-correlation properties is investigated for potential applications in defining new multiple access protocols for distributed wireless systems. One can show that for any finite subset of the sequences with rate sum not exceeding a certain level, there cannot have enough collisions to completely block any particular user no matter how they are shifted with respect to one another. The user un-suppressibility and service guarantee can be exploited in many applications such as wireless sensor or impulse radio systems. To enhance the system's allowable rate sum while possessing the non-blocking property, new protocol sequences are designed. Besides, the throughput shift-invariant property is obtained.**

I. Introduction

In a wireless communication system, the most fundamental question of a multiple access control is how to accommodate users in the shared channel. To avoid transmission conflict, one may employ a rigid protocol such as time division multiple access (TDMA). However, it may not be practical due to the difficulties in synchronizing transmissions from different senders [1]. Contention-based random access protocols such as IEEE 802.11 CSMA/CA can provide a more flexible transmission scheme. However, usually they require some backoff algorithms and a feedback link to ensure successful delivery.

For system simplicity, it is desirable to have a simple multiple access protocol which does not require stringent time synchronization and complicated processing such as backoff algorithm or random number generator. The model of *collision channel without feedback* [2] is worth of a revisit. Senders are assumed cannot synchronize transmissions between one another due to a lack of feedback link and their relative time offsets are unknown. Thus, each user will make packet transmissions simply at times governed by its *protocol sequence* in a distributed way. It can be shown that a simple and reliable multiple access scheme under these constraints is still possible even without a requirement of packet retransmission. The result can provide a helpful alternative for wireless accessing.

Potential applications include wireless sensor networks in which computing power and communication capability are often very limited [5]. Meanwhile, frequent monitoring of the channel for feedback information and complicated backoff processing can be eliminated. Besides, when considering an ad-hoc system with dynamic topology [6], sharing a radio channel with the requirement of well-coordinated transmissions and time offsets could be hard for thin devices.

This work is also supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region (Project no. CUHK416906).

In this paper, a class of periodic binary sequences with interesting properties is investigated for defining new multiple access protocols in a shared radio channel. The idea of using deterministic binary sequences to define medium accessing can be traced back to [2]–[4]. Some related works in the collision channel can be found in [7]–[10]. Besides, packet recovery from collisions with multiuser detectors was discussed in [1]. In protocol sequence designs, major concerns include the number of sequences available, user throughput performance and the length of sequences. Cross-correlation between sequences is one of the important performance indicators.

II. Channel Model

Following the model of collision channel without feedback [2], a communication channel is divided into time slots of equal durations. Each user follows a binary sequence, $W = \{W(t), t = 0, 1, 2, \cdots\}$, and will transmit a data packet at time slot t if $W(t) = 1$. Otherwise, it keeps silent. Here, we restrict our attention to the slot-synchronized model in which users transmit packets aligned to the common slot boundaries. However, users do not know the time offsets between one another and cannot synchronize their transmissions. They may have different transmission starting time.

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. For system simplicity, each packet will include a header which contains sender identity like those commonly defined in conventional MAC protocols [6]. If the packet payload is large, the cost of overhead is relatively small. For advanced packet identification or coding schemes, discussions can be found in [2], [8].

For a periodic binary sequence with period L, its *duty factor* or proportional transmission rate, r, is defined as

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

The effective throughput 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 users are signaling at the same rate [2]. Here, we will focus on the design for symmetric users. It is known that in this case the system capacity tends to $1/e$ 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. Without loss of generality, it is favorable to have a design which can support both system and individual performance stability. Thus, one can always ensure the availability of a reliable communication channel for any of the active users as long as the allowable rate sum does not exceed a given level.

III. Distributed Wireless Accessing

In the following, an investigation on the class of *linear congruence sequence* [3] and its deployment for robust wireless accessing with user *un-suppressibility* [9] is reported. The result and analysis has also motivated our design for a system enhancement. The details are given below.

A. Linear Congruence Sequence

Let $W = \{W(t), t = 0, 1, 2, \cdots\}$ be a binary sequence. It can also be represented by indexing the positions of '1's. $I_W(i)$ is used to denote the position at which the i-th entry of 1's in W appears. Let b and l be two integers such that $0 \leq b < l$. The linear congruence sequence generated by (b, l) is expressible as

$$I_W(i) = il + ib - \lfloor ib/l \rfloor l \tag{2}$$

where b is known as the *key generator*. The duty factor of a sequence generated by (b, l) is equal to $1/l$. For $b > 0$, the minimum period is equal to l^2. For $b = 0$, $I_W(i) = il$.

For example, given $b = 1$ and $l = 3$, following (2), $I_W = \{4, 8, 9, \cdots\}$. The core pattern of W is $\{0, 0, 0, 1, 0, 0, 0, 1, 1\}$. The sequence has a duty factor $r = 1/3$ and period of 9.

Note that, for prime l, the set of linear congruence sequences is also known as *prime sequences* [4].

B. Correlation Properties

Let W_1 and W_2 be two binary sequences with common period L. For any relative time shift s, we define the Hamming cross-correlation function between W_1 and W_2 as

$$H_{W_1,W_2}(s) = \sum_{t=0}^{L-1} W_1(t) W_2(t+s) \tag{3}$$

while the normalized cross-correlation is given by

$$\bar{H}_{W_1,W_2}(s) = H_{W_1,W_2}(s)/L. \tag{4}$$

Let l, b_1 and b_2 be integers satisfying $0 \leq b_1, b_2 < l$, $b_1 \neq b_2$ and $\gcd(|b_2 - b_1|, l) = 1$, where gcd denotes the greatest common divisor. For linear congruence sequences W_1 and W_2 generated by (b_1, l) and (b_2, l) respectively,

$$\bar{H}_{W_1,W_2}(s) \leq 2/l^2 = 2r^2 \tag{5}$$

for any $0 \leq s < l^2$, where r, the duty factor, is equal to $1/l$. For $b_1, b_2 > 0$, this upper bound is tight [9].

If $b_1 = 0$ or $b_2 = 0$,

$$\bar{H}_{W_1,W_2}(s) = 1/l^2 = r^2. \tag{6}$$

For example, given $l = 5$, let W_i be the set of sequences generated by (i, l), where $0 \leq i < 5$. Following (2),

$$\begin{bmatrix} W_0 \\ W_1 \\ W_2 \\ W_3 \\ W_4 \end{bmatrix} = \begin{bmatrix} 0000100001000010000100001 \\ 0000010000010000010000011 \\ 0000001000000101000000101 \\ 0000000100100000001001001 \\ 0000000010001000100010001 \end{bmatrix}. \tag{7}$$

The number of *coincidences*, or hits, between two distinct sequences in (7) is given by

$$\begin{bmatrix} H_{W_0,W_{i\neq 0}}(s) \\ H_{W_1,W_2}(s) \\ H_{W_1,W_3}(s) \\ H_{W_1,W_4}(s) \\ H_{W_2,W_3}(s) \\ H_{W_2,W_4}(s) \\ H_{W_3,W_4}(s) \end{bmatrix} = \begin{bmatrix} 1111111111111111111111111 \\ 1210110220110121120111021 \\ 1210110211111201101211111 \\ 1202010202110211111111201 \\ 1111111021121101011211201 \\ 1121011102120111012111111 \\ 1121012002101211120111021 \end{bmatrix} \tag{8}$$

for the relative time shift $0 \leq s \leq 24$. It demonstrates that

$$0 \leq H_{W_i,W_{j\neq i}}(s) \leq 2 \tag{9}$$

where $H_{W_i,W_{j\neq i}}(s)$ indicates the number of packets collided between senders by W_i and W_j with relative time offset s. The number of hits is counted in the common period, $l^2 = 25$.

C. Protocol Sequences and Un-suppressibility

Following the definition of (2), a family of protocol sequences can be formulated below. To satisfy the condition for the performance of (5) and (6), and have a greater flexibility of b, here l is restricted to *prime* number, denoted by p.

A family of periodic binary sequences, $\mathbf{F}_p$, is defined as the set of linear congruence sequences generated by (b, p), where $0 \leq b < p$. The sequences in $\mathbf{F}_p$ have a minimum common period $L = p^2$ and each has a duty factor $1/p$. By (5) and (6),

$$\max_s \left\{ H_{W_i,W_j}(s) \right\} = 2 \tag{10}$$

for any $i \neq j$. A user un-suppressibility [9] property of a set of above protocol sequences can be established accordingly.

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], the set $\mathbf{F}_p$ can be used to define protocol sequences for packet transmissions. Note that a packet retransmission mechanism can be embedded if preferred and feedback channel is available. However, the detail is out of the scope here.

For any finite subset of $\mathbf{F}_p$, $\{W_i, i = 0, 1, \cdots, (M-1)\}$, provided that

$$\sum_{i=0, i\neq j}^{M-1} r_i \equiv \left(\sum_{i=0}^{M-1} r_i \right) - r_j < \frac{1}{2} \tag{11}$$

which refers to the sum of duty factors of active users excluding user j, following the definition of (3), by (10) and (11), the total number of collisions to W_j is equal to

$$\sum_{i=0,i\neq j}^{M-1}\sum_{t=0}^{L-1} W_j(t)W_i(t+s_{i,j}) \equiv \sum_{i=0,i\neq j}^{M-1} H_{W_i,W_j}(s_{i,j}) \leq \sum_{i=0,i\neq j}^{M-1} 2 < \frac{1/2}{1/p}\times 2 = p \quad (12)$$

for any combinations of relative time shifts $s_{i,j}$ in W_i with reference to W_j. The number of collisions in any period p^2 is strictly less than p. Thus, there cannot have enough collisions to completely block any particular user j in any cycles as long as the sum of other duty factors $\{r_{i\neq j}\}$ does not exceed $1/2$, even if the relative time shifts between one another may change from time to time due to different reasons.

Similarly, as long as $\sum_{i=0}^{M-1} r_i \leq 1/2$, we have

$$\sum_{i=0,i\neq j}^{M-1}\sum_{t=0}^{L-1} W_j(t)W_i(t+s_{i,j}) \leq \frac{1/2-1/p}{1/p}\times 2 = p-2. \quad (13)$$

That is, for each user in the above set, in any cycle, at least 2 transmitted packets have no collision. User un-suppressibility is ensured such that, even in the worst case, all the users can successfully transmit information to a guaranteed amount in every time period in a distributed multiple access. A reliable communication is possible even without the requirement of user synchronization or a feedback link.

Note that the bound of allowable rate sum in (11) is not tight. One can find examples in which the un-suppressibility holds while the inequality is violated. A natural follow-up is to enhance the maximum allowable rate sum and construct a set of corresponding periodic sequences which possess the un-suppressibility guarantee. Designs are presented below.

IV. New Protocol Sequences

In this section, new constructions of protocol sequences which have smaller normalized cross-correlations are described. The result can significantly enhance the allowable rate sum of active users in the system.

A. General Idea

Recall (5) and (6), one can find that

$$H_{W_i,W_j}(s) = \{0,1,2\} \quad (14)$$

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 sequences with $\bar{H}_{W_i,W_j}(s) = r^2$ based on an observation of the following property [11] that

$$\lambda_{avg}(W_i,W_j) \triangleq \sum_{s=0}^{L-1} \bar{H}_{W_i,W_j}(s) = r_i r_j L. \quad (15)$$

Generally, the average number of coincidences between any two sequences W_i and W_j, with duty factors r_i and r_j respectively, over their common period L is equal to $r_i r_j L$ since 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 $1, 2, \cdots$, up to $L-1$, stepwise.

Take (8) as an example, where $L = 25$ and $r = 1/5$,

$$\lambda_{avg}(W_i,W_j) = \frac{1}{L}\sum_{s=0}^{L-1} H_{W_i,W_j}(s) = 25/25 = 1. \quad (16)$$

That is, the average number of hits between two sequences is in fact equal to 1 after averaging out over all the relative time shifts $0 \leq s < L$. 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.

So, one way to obtain a set of periodic binary sequences with $\bar{H}_{W_i,W_j}(s) = r_i r_j$ can be done by concatenating the original sequences from (2) with their shifted versions so as to combine all the effects due to the time shifts. Thus, in the new sequences, for any relative time shift, one can get the average performance, "$H_{W_i,W_j}(s) = 1$", i.e. on average one collision with another sequence per p packets transmitted. In other words, $\bar{H}_{W_i,W_j}(s) = 1/p^2$. The cross-correlation between two sequences will be shift invariant.

Thus, as long as $\sum_{i=0}^{M-1} r_i \leq 1$, similarly to (13),

$$\sum_{i=0,i\neq j}^{M-1}\sum_{t=0}^{L-1} W_j(t)W_i(t+s_{i,j}) \equiv \sum_{i=0,i\neq j}^{M-1} H_{W_i,W_j}(s_{i,j}) = \sum_{i=0,i\neq j}^{M-1}\left(\frac{L}{p}\cdot\frac{1}{p}\right) \leq \frac{1-(1/p)}{1/p}\cdot\frac{L}{p^2} = \frac{L}{p} - \frac{L}{p^2} \quad (17)$$

which shows that, in any common period L, the number of collisions is strictly less than the number of packets one transmits, L/p. There cannot have enough collisions to completely block any particular user. Even when the system is saturated and rate sum equals to 1, each user has a throughput not less than $1/p^2$. In fact, the actual throughput could be much higher since in general the upper bound on the number of collisions given by (17) is not tight. Section V will show the performance.

B. Construction 1

Let us start with $p = 3$ to elaborate the details. By (6), 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 (otherwise, W_0 and W_1) as the basic codewords. By (5), $\max_s \bar{H}_{W_1,W_2}(s) = 2/9$. Thus, 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 worst case.

To make all sequence pairs with $\bar{H}(s) = 1/9$, by following the idea of "averaging out", the construction is expressible as

$$\begin{bmatrix} W_1^{(1)} \\ W_2^{(1)} \\ W_0^{(1)} \end{bmatrix} = \begin{bmatrix} W_{1,\theta=0} & W_{1,\theta=1} & \cdots & W_{1,\theta=8} \\ W_{2,\theta=0} & W_{2,\theta=0} & \cdots & W_{2,\theta=0} \\ W_{0,\theta=0} & W_{0,\theta=0} & \cdots & W_{0,\theta=0} \end{bmatrix} \quad (18)$$

where $W_{i,\theta=n}$ refers to a cyclic shift of W_i by n bits toward the left while the superscript on $W_i^{(1)}$ is to label Construction 1. For example, here, $W_{1,\theta=0} \equiv W_1 = \{000100011\}$ and $W_{1,\theta=1} = \{001000110\}$. New sequences need to be longer.

Following (18), for any relative shift s, the normalized cross-correlation between $W_1^{(1)}$ and $W_2^{(1)}$ is given by:

$$\begin{aligned}
&\bar{H}_{W_1^{(1)},W_2^{(1)}}(s) \equiv \frac{1}{p^4}\sum_{t=0}^{p^4-1} W_1^{(1)}(t)W_2^{(1)}(t+s)\\
&= \frac{1}{p^4}\sum_{n=0}^{p^2-1}\sum_{t=0}^{p^2-1} W_{1,\theta=n}(t)W_{2,\theta=0}(t+s)\\
&= \frac{1}{p^4}\sum_{n=0}^{p^2-1}\sum_{t=0}^{p^2-1} W_1(t)W_2(t+s-n)\\
&= \frac{1}{p^4}\sum_{n=0}^{p^2-1} p^2 \cdot \bar{H}_{W_1,W_2}(s-n) = \frac{p^2}{p^4}\times 1 = \frac{1}{p^2} = \frac{1}{9}
\end{aligned} \tag{19}$$

since by (15), $\sum_{n=0}^{p^2-1}\bar{H}_{W_1,W_2}(s-n) = 1$, where $L = p^2$ and $r_i = r_j = 1/p$. For $W_0^{(1)}$ and the other, since $\bar{H}_{W_0,W_1}(s) = \bar{H}_{W_0,W_2}(s) = 1/p^2$, it is straightforward that

$$\bar{H}_{W_0^{(1)},W_1^{(1)}}(s) = \bar{H}_{W_0^{(1)},W_2^{(1)}}(s) = 1/p^2. \tag{20}$$

Hence, $\{W_0^{(1)}, W_1^{(1)}, W_2^{(1)}\}$ is a set of sequences with normalized Hamming cross-correlation equal to r^2. The result is independent of s. Even when all of them are used simultaneously and rate sum equals to 1, the un-suppressibility holds.

For sequences of duty factor equal to $1/5$, to make $\bar{H}_{W_i^{(1)},W_{j\neq i}^{(1)}}(s) = 1/25$, following the same idea,

$$\begin{bmatrix} W_1^{(1)}\\ W_2^{(1)}\\ W_3^{(1)}\\ W_4^{(1)}\\ W_0^{(1)} \end{bmatrix} = \begin{bmatrix} [W_{1,\theta=0}\ \cdots\ W_{1,\theta=24}]_{25\times 25}\\ \big[[W_{2,\theta=0}]_{25}\ \cdots\ [W_{2,\theta=24}]_{25}\big]_{25}\\ [W_{3,\theta=0}]_{25\times 25}\ \cdots\ [W_{3,\theta=24}]_{25\times 25}\\ [W_{4,\theta=0}]_{25\times 25\times 25}\\ [W_{0,\theta=0}]_{25\times 25\times 25} \end{bmatrix} \tag{21}$$

where $[W_i]_k$ refers to a concatenation of k copies of W_i consecutively. The aim is to extend the original sequences such that for any pair of them all their shifted combinations are contained. Consequently, no matter how they shift, the resultant cross-correlation is always equal to the desired average. That is, $\bar{H}_{W_i^{(1)},W_{j\neq i}^{(1)}}(s) = 1/p^2$. The proof is very similar to that in (19) and because of limited space, it is omitted here.

Similarly, for each p, a set of shift invariant sequences with $\bar{H}_{W_i,W_{j\neq i}}(s) = 1/p^2$ can be constructed in an iterative way. Even when all the protocol sequences are used simultaneously, the un-suppressibility still holds. It is worth pointing out that the idea of "averaging out" with (15) is generally applicable to many codewords. Similar results are achievable.

However, the new sequence needs to be much longer than the original one for the allowable rate sum enhancement. Let $L_p^{(1)}$ be the sequence length of Construction 1 for the set of p. Since $W_0^{(1)}$ requires only a simple concatenation, we have

$$L_p^{(1)} = \left(p^2\right)^{p-1} = p^{2(p-1)}. \tag{22}$$

For example, $L_3^{(1)} = 3^4 = 81$, while $L_5^{(1)} = 25^4$. It should be noted that $L_p^{(1)}$ could be very large. As a demonstration, when $p = 7$, $L_7^{(1)} = 7^{12}$. In a channel of 1 Mb/s, it takes about 13.84×10^3 seconds to complete one sequence cycle. This could be a problem for some applications. It is desirable to have a shorter required sequence length.

C. Construction 2

In Construction 1, we may have excessively collected too many copies of the variants or shifted versions of the original sequences to average out all the cross-correlation combinations. However, some concatenations may not be necessary.

By an investigation of the cross-correlations between linear congruence sequences, it is found [9] that, for $i \neq j$,

$$\sum_{n=0}^{p-1} \bar{H}_{W_i,W_j}(n\cdot p + t) = 1/p \tag{23}$$

for any integer $0 \le t < p$. Thus, a design that contains concatenations with cyclic shifts over $\{0, p, 2p, \cdots, p(p-1)\}$ suffices to characterize the average performance and represent all the combinations. For $p = 3$, (18) can be simplified as

$$\begin{bmatrix} W_1^{(2)}\\ W_2^{(2)}\\ W_0^{(2)} \end{bmatrix} = \begin{bmatrix} W_{1,\theta=0} & W_{1,\theta=3} & W_{1,\theta=6}\\ W_{2,\theta=0} & W_{2,\theta=0} & W_{2,\theta=0}\\ W_{0,\theta=0} & W_{0,\theta=0} & W_{0,\theta=0} \end{bmatrix}. \tag{24}$$

Similar to (19), the normalized cross-correlation is equal to

$$\begin{aligned}
&\bar{H}_{W_1^{(2)},W_2^{(2)}}(s) \equiv \frac{1}{p^3}\sum_{n=0}^{p-1}\sum_{t=0}^{p^2-1} W_{1,\theta=np}(t)W_{2,\theta=0}(t+s)\\
&= \frac{1}{p^3}\sum_{n=0}^{p-1}\sum_{t=0}^{p^2-1} W_1(t)W_2(t+s-np)\\
&= \frac{1}{p^3}\sum_{n=0}^{p-1} p^2 \bar{H}_{W_1,W_2}(s-np) = \frac{p^2}{p^3}\times\frac{1}{p} = \frac{1}{p^2}
\end{aligned} \tag{25}$$

while $\bar{H}_{W_0^{(2)},W_1^{(2)}}(s) = \bar{H}_{W_0^{(2)},W_2^{(2)}}(s) = 1/p^2$. Thus, even when $W_0^{(2)}, W_1^{(2)}$ and $W_2^{(2)}$ are used simultaneously and the rate sum is equal to 1, the un-suppressibility holds.

Generally, the construction can be formulated iteratively as:

$$\begin{bmatrix} W_1^{(2)}\\ W_2^{(2)}\\ W_3^{(2)}\\ \vdots\\ W_{p-2}^{(2)}\\ \\ W_{p-1}^{(2)}\\ W_0^{(2)} \end{bmatrix} = \begin{bmatrix} \big[W_{1,\theta=0}\ W_{1,\theta=p}\cdots W_{1,\theta=(p-1)p}\big]_{p^{(p-3)}}\\ \big[\,[W_{2,\theta=0}]_p\,[W_{2,\theta=p}]_p\cdots\big[W_{2,\theta=(p-1)p}\big]_p\,\big]_{p^{(p-4)}}\\ \big[\,[W_{3,\theta=0}]_{p^2}\cdots\big[W_{3,\theta=(p-1)p}\big]_{p^2}\,\big]_{p^{(p-5)}}\\ \vdots\\ \big[\,[W_{p-2,\theta=0}]_{p^{(p-3)}}\,[W_{p-2,\theta=p}]_{p^{(p-3)}}\cdots\\ \cdots\big[W_{p-2,\theta=(p-1)p}\big]_{p^{(p-3)}}\,\big]_{p^0}\\ [W_{p-1,\theta=0}]_{p^{(p-2)}}\\ [W_{0,\theta=0}]_{p^{(p-2)}} \end{bmatrix}. \tag{26}$$

Let $L_p^{(2)}$ be the sequence length by Construction 2. From (26), we have

$$L_p^{(2)} = p^2 \times p^{p-2} = p^p. \tag{27}$$

For example, $L_3^{(2)} = 3^3 = 27$, while $L_5^{(2)} = 5^5 = 3125$. Comparing (27) with (22), $L_p^{(2)}/L_p^{(1)} = p^p/p^{2(p-1)} = 1/p^{p-2}$, which indicates a big reduction in the sequence length by

Construction 2. For demonstration, when $p = 7$, $L_7^{(2)} = 7^7$. In a channel of 1 Mb/s, it takes about 0.82s to complete one cycle. This is much smaller than that of 13.84×10^3 seconds in Construction 1 and could be acceptable.

However, note that $L_p^{(2)}$ is still exponentially increasing, although 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 protocol sequences are not allowed. A further improvement is favorable and left open. There is a tradeoff between the sequence length and throughput variance.

V. Performance Evaluation

Investigations on the effective throughput of users with the protocol sequences from Construction 1 and 2 in slot-synchronized collision channel are conducted. Since users are unsynchronized to each other, we assume the time offset between two users is uniformly distributed in their encountered minimum period. In the simulation, we consider there are p active users with symmetric duty factor $1/p$. Both individual and system throughputs are measured when the system is saturated, i.e., $\sum_i r_i = 1$. Data are obtained after 10^5 runs with random time offsets. Since simulation results of Construction 1 and 2 are exactly the same, only one set of the data are plotted and labeled by "New". However, the plots can represent both.

Fig. 1 shows the individual throughput of users taken over sequence periods. The minimum, mean and maximum throughputs obtained from the new protocol sequences are compared with those obtained from prime sequences of (2) and a random access scheme. In the random access scheme, it is assumed that at each time slot a user will transmit a packet randomly by a probability of its duty factor $1/p$. The throughput of a user in the random access scheme is taken over periods same as that of prime sequences for reference.

Comparing the performance of the new construction, prime sequences and random access, the means of their individual throughputs are the same. This is natural and expected since the mean is taken by averaging throughputs of users with uniformly distributed time offsets. One can find from Fig. 2 that the means of their system throughputs are the same as well. However, the observed ranges of throughputs as indicated by [Min, Max] are very different.

As shown in Fig. 1, a user with prime sequence can be completely blocked by other users and the minimum individual throughput is equal to zero. The random access has the same problem. On the other hand, the new protocol sequences have shown its robustness and user un-suppressibility. There cannot have enough collisions to completely block any particular user. It has completely eliminated this risk. Furthermore, as shown in Fig. 1 and 2, the new protocol sequences have *zero variance* in both individual and system throughputs. Fig. 3 shows standard deviations in comparison. The new protocol sequences provide an extremely stable and shift invariant throughput performance in contrast to the highly fluctuated performance in the prime sequence and random access schemes. Deterministic performance guarantees are supported.

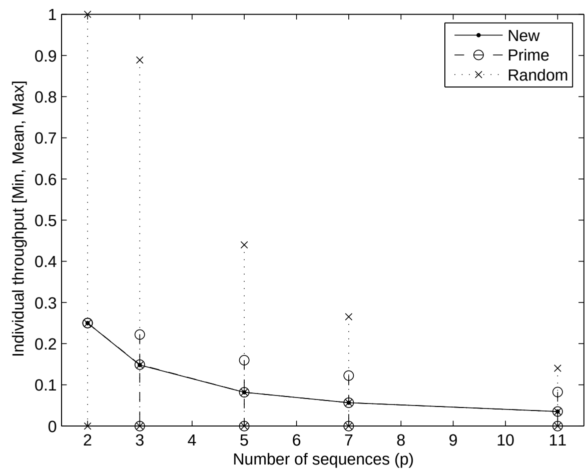

Fig. 1. The minimum, mean and maximum individual throughputs from simulations in which duty factor of users = $1/p$ and system rate sum = 1.

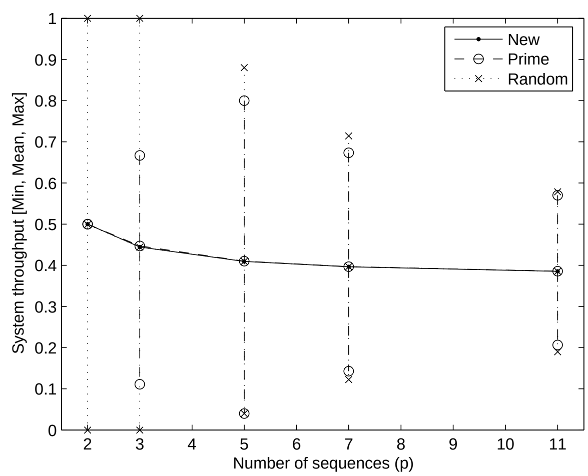

Fig. 2. The minimum, mean and maximum system throughputs from simulation in which duty factor of users = $1/p$ and system rate sum = 1.

It should be noted that in general the new construction has a longer sequence length, p^p, than that of prime sequence, p^2. The probability of zero individual throughput in the prime sequence and random access schemes could be smaller when measured over a longer period. Besides, the random access scheme will obtain a smaller variance in user throughputs [10], while the difference to prime sequences is negligible. However, without loss of generality, a user in these two schemes always has a non-zero probability of being completely blocked. Moreover, although the average throughputs are the same in these three schemes, the new protocol supports a service of higher minimum throughputs generally as shown in Fig. 1 and 2.

Furthermore, we compare the throughput performance between the protocol sequences of Construction 2 and that by Massey and Mathys [2] under this model. Both of them have the same sequence length. Numerical results show that they

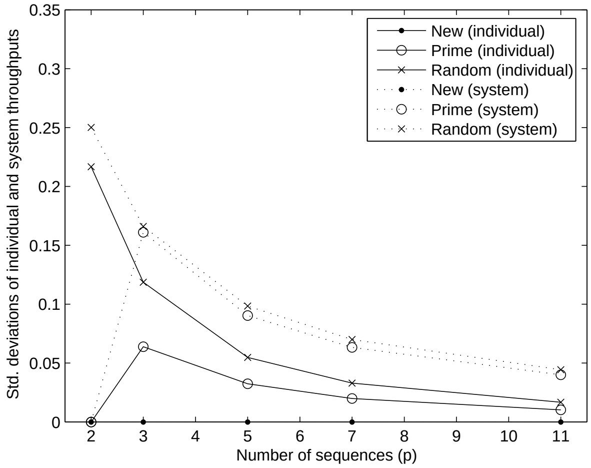

Fig. 3. The standard deviations of individual and system throughputs are shown for comparison. "New" has zero variance for all the cases.

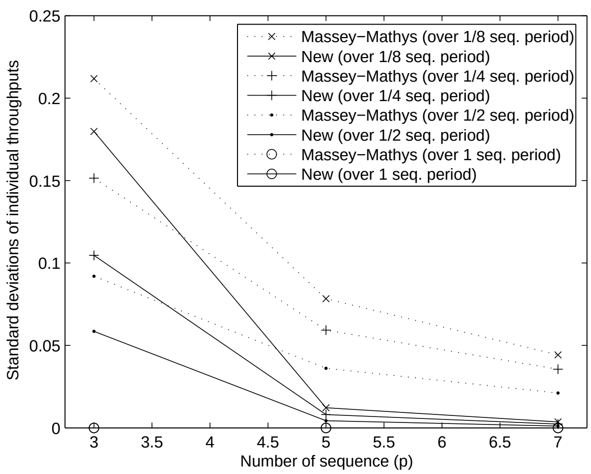

Fig. 4. The standard deviations of individual throughputs measured over 1/8, 1/4, 1/2 and one sequence periods are plotted respectively.

have the same average individual and system throughputs when measured over complete cycles of their minimum sequence periods. It is observed that the construction in [2] also yields zero variance in individual and system throughputs. However, when effective throughputs are considered in partial periods for practical considerations as the sequence length is exponentially increasing, there is a significant difference between the two designs. Fig. 4 shows the standard deviations of individual throughputs measured over 1/8, 1/4, 1/2 and one complete sequence periods respectively. The new construction outperforms and has a much smaller throughput fluctuation in partial periods generally. However, it should be noted that the work in [2] is more focus on the studies of the capacity regions, sender identification techniques and packet recovery.

It is worth pointing out that the achieved throughputs in the new design can be expressed in closed form. For a system of p symmetric users with duty factors $1/p$, the individual throughput for any user j is expressible as:

$$\tilde{r}_j = \sum_{i=1}^{p} (1/p)^i (-1)^{i-1} \binom{p-1}{i-1} \quad (28)$$

while the system throughput equals to $(1-1/p)^{p-1}$. Due to a lack of space, the detail will be addressed elsewhere.

VI. Concluding Remarks

In this paper, a class of linear congruence sequences with interesting cross-correlation properties is investigated for defining robust wireless access protocols. The analysis has also led to new designs with the following major advantages. While holding the feature of user un-suppressibility, the enhancement allows a higher rate sum equal to 1. Meanwhile, no matter how the sequences are shifted relative to one another, no one will be completely blocked. This ensures a reliable communication channel for each user even without backoff mechanisms and a feedback link for user synchronization. It does not require a centralized scheduling. Moreover, it is found that the new design has shift invariant individual and system throughputs. The "zero variance" service is capable of providing deterministic guarantees. When comparing partial period performance with [2], the new design has a much smaller fluctuation.

On the other hand, since the protocol sequences are deterministic, generally a receiver can explicitly address the following packets after a successfully received packet as sender's transmission time can be determined by (b, p) in the header. This is more energy efficient since continuous channel listening for packet reception can be eliminated. Besides, by the sequence periodicity, some collisions can be avoided in a predictive way to have throughput enhancement when concerned [10]. There is also a potential of other interesting designs and applications of the resource sharing.

References

[1] S. Tinguely, M. Rezaeian, and A. J. Grant, "The collision channel with recovery," *IEEE Trans. Inform. Theory*, vol. 51, no. 10, Oct. 2005.

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

[3] 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, pp. 490–493, July 1981.

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

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

[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] 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.

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

[9] 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.

[10] C. S. Chen and W. S. Wong, "A robust access protocol for wireless sensor networks," *Proc. IEEE Milcom*, Washington D.C., Oct. 2006.

[11] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, no. 5, 1980.