Safety-Message Broadcast in Vehicular Ad Hoc Networks Based on Protocol Sequences

Yi Wu, *Member, IEEE*, Kenneth W. Shum, *Member, IEEE*, Wing Shing Wong, *Fellow, IEEE*, and Lianfeng Shen, *Member, IEEE*

***Abstract*—In vehicular collision avoidance systems, safety messages are broadcast by mobile users periodically on the highway to all of their neighbors within hearing range. These safety messages are time sensitive and have stringent delay requirements. Conventional carrier-sense multiple access, where users must content with channel access, is not suitable for this kind of application. In this paper, we propose using protocol sequences to broadcast safety messages. Protocol sequences are deterministic 0–1 sequences. Each user reads out the 0's and 1's of the assigned protocol sequence periodically and transmits a packet in a time slot if and only if the sequence value is equal to 1. It requires no time synchronization among the users. We compare the delay performance with an ALOHA-type random access scheme and show that the delay can, in fact, be reduced by employing protocol sequences instead.**

***Index Terms*—ALOHA, collision channel, IEEE 802.11p, protocol sequences, safety message, vehicular ad hoc networks (VANETs).**

I. Introduction

In a *vehicular ad hoc network* (VANET), maintaining time synchronization among users is a difficult task due to their mobility. Moreover, unlike cellular networks, there are no base stations to facilitate synchronization. There is also no dedicated control agent in a VANET who monitors users at the lower protocol layers. Due to high mobility of the user nodes, it is difficult and undesirable to designate any particular subset of nodes as central access nodes with control authority, even temporarily. This makes the design of a medium-access control (MAC) protocol for low-latency application a very challenging task.

In this paper, we consider the application of safety-message broadcast in a VANET. The goal is to allow all user nodes to simultaneously broadcast safety messages to all their neighbors within transmit range [1]. Safety messages can be divided into two types. The first type is periodic information (also called heartbeat messages) such as the speed and location of an automobile. The second type of messages relates to emergency events such as lane-change warning or precrash warning. These basic safety messages are the core data on which one can build a variety of traffic safety applications such as cooperative collision warning. In the following, we focus on periodic safety-message broadcast.

It is pointed out in [2] that the newly introduced IEEE 802.11p Wireless Access in Vehicular Environment (WAVE) over the dedicated short-range communications (DSRC) band for a VANET is not desirable for the transmission of time-critical safety messages because the delay may be unbounded when the channel is very busy. In American systems, safety messages are generated approximately every 0.1 s, encapsulated using the WAVE short message protocol and sent according to the carrier-sense multiple access with collision avoidance (CSMA/CA)-based enhanced distributed channel access mechanism over the control channel, which is one of the seven channels in the DSRC spectrum [3]. There are several other suggested multiple-access schemes in the literature. For example, in [4], a packet is retransmitted several times within its useful lifetime, with the pattern of retransmissions randomly chosen. In [5], the packet loss rate is reduced by adaptively adjusting the rate of transmitting the safety beacon. By using a hash function to evenly spread the access time to the control channel, excessive contention for channel is alleviated in [6]. In [7], a feedback channel is added in the application layer to avoid the transmission of an unnecessary safety message, and in [8], a scheme based on slot reservation is discussed. Performance evaluation of DSRC for safety-message broadcast can be found in [9].

In principle, the delay experienced by a user in random or contention-based MAC scheme is unbounded; a user may need to wait for a long time until he/she has the opportunity to send some data. On the other hand, by scheduling the data packets according to a certain deterministic pattern, which is called *protocol sequence* by Massey and Mathys in [10], a hard guarantee of delay can be accomplished. The scheduling

Manuscript received April 20, 2012; revised October 31, 2012, March 17, 2013, and July 5, 2013; accepted August 6, 2013. Date of publication August 28, 2013; date of current version March 14, 2014. This work was supported in part by the National Natural Science Foundation of China under Grant 61171081 and Grant 61174060; by the National High Technology Research and Development Program of China (863 Program) under Grant 2008AA01Z205; by the Program for New Century Excellent Talents in University of China under Grant NCET-10-0018; by the Shun Hing Institute of Advanced Engineering, The Chinese University of Hong Kong under Project MMT-8115035; and by the University Grants Committee of the Hong Kong Special Administrative Region of China under Project AoE/E-02/08. The review of this paper was coordinated by Prof. Y. Qian.

Y. Wu is with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China, and also with the College of Photonic and Electronic Engineering, Fujian Normal University, Fuzhou 350007, China (e-mail: wuyi@seu.edu.cn).

K. W. Shum is with the Institute of Network Coding, The Chinese University of Hong Kong, Shatin, Hong Kong (e-mail: wkshum@inc.cuhk.edu.hk).

W. S. Wong is with the Department of Information Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong (e-mail: wswong@ie.cuhk.edu.hk).

L. Shen is with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: lfshen@seu.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2013.2279857

0018-9545 © 2013 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

of packet transmissions in a protocol-sequence-based scheme follows a binary and periodic sequence. A user simply reads out the sequence values once per time slot duration and sends a packet if and only if the sequence value is equal to 1. We note that we do not need any designated coordinator to schedule the packet transmissions. If the protocol sequences are appropriately chosen, one can guarantee that each user can send at least one packet in a sequence period. The sequence period thus provides an upper bound of delay. Applications of different classes of the deterministic MAC scheme in a wireless ad hoc network have been studied by several researchers. For example, Reed–Solomon codes are used to generate the schedules of packet transmissions in [11] and [12], optical orthogonal codes are used in [13] and [14], and Gold sequences are used in [15].

One key property of protocol sequences is that they are designed to accommodate asynchronous users, which is an indispensable feature in the VANET application. There are three different levels of synchronization, namely, asynchronous, slot-synchronous, and frame-synchronous. The asynchronous model is the minimal framework in which slot boundaries of the users are not necessarily aligned, although the slot duration of all users is identical. Hence, packets sent from different users may partially overlap with each other. The relative delay offsets between two protocol sequences in this model may be any real number. In the slot-synchronous model, the slot boundaries of the users are aligned. Two packets from two different users either overlap completely or do not overlap at all. However, the protocol sequences need not start at the same slot. The relative delay offsets of two users are integral multiples of the duration of a time slot. In the frame-synchronous model, all users start their protocol sequences at the same time instance. The relative delay offsets are integral multiples of the sequence period.

The works in [11]–[14] require frame synchronization, which can be accomplished by the Global Positioning System for instance. In the literature of the mobile ad hoc network (MANET), the frame-synchronous code-based approach to multiple access is often reffered to as topology-transparent scheduling or, simply, code-based scheduling. (We refer the readers to [16] and [17] for more information on code-based scheduling in MANETs.) The dynamics of code-based scheduling in MANETs is much slower than in VANETs. Achieving frame synchronization in VANETs is more costly.

On the other hand, the work in [15] is for a slot-synchronous system and is more related to our approach. Methods for decentralized and autonomous clock synchronization can be found in [18] and [19] and the references therein. Any results on the slot-synchronous system can be also extended to practical systems that are asynchronous. For example, we can require that each user only transmits in the first half of an active time slot and leaves the second half idle. Then, the analysis of the slot-asynchronous system is the same as that of the asynchronous system. For ease of presentation, we will focus on slot-synchronous systems. Further discussions on protocol sequences for asynchronous systems can be found in [20] and [21].

Regardless of the synchronization model, we have the code assignment problem or the sequence assignment problem. As the number of users on the highway is virtually unbounded,

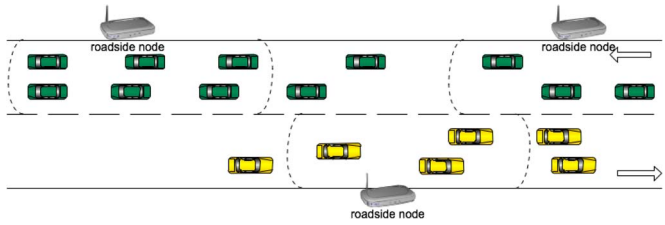

Fig. 1. VANET on a highway.

it is impossible to assign distinct protocol sequences to all users. The protocol sequences must be spatially reused. The assignment should be adaptive to the time-varying topology to assure that no protocol sequence is assigned to two users within hearing range. There are some existing assignment schemes in the literature. In [22], frequency division in the MAC layer is used, and the carrier frequencies are assigned according to the locations of the users. It is supposed in [22] that the users know their locations and the one-to-one mapping between location and bandwidth division. In [14], a distributed assignment method is proposed. A subset of protocol sequences or codes is reserved for this purpose, and a network association phase before the actual data communication phase is required. A protocol sequence allocation scheme in ad hoc networks based on the Global Positioning System can be found in [23]. We can also distribute the protocol sequences to the users via roadside nodes or roadside units near highway entrances or toll booths (see Fig. 1). These roadside units are expected to be sparsely located as they do not serve as base stations. When a user enters the highway or when a user passes through a toll booth, he/she is assigned a protocol sequence from a roadside node via a downlink control channel. The user will use the assigned sequence for message broadcast until entering the range of the next roadside node. At that point, the user will trigger the roadside node to issue a new protocol sequence to be used. If the number of active users increases, for example, in peak hours, the roadside node can switch to a larger pool of protocol sequences, such that every mobile user in a segment of the highway can be assigned a unique protocol sequence. (See [24] and [25] on the application of roadside units for enhancing security and connectivity in VANETs.)

In this paper, we consider slot-synchronous single-hop broadcast and analyze the delay performance of a class of protocol sequences, which are called the generalized prime (GP) sequences. In the majority of the existing works on the protocol sequences, the design objective is to maximize the throughput and support as many users as possible (see, e.g., [26] and [27]). However, in the application of safety-message broadcast, throughput is of secondary importance. The primary concern is the minimization of the time within which a user has to wait until he can receive a packet from his neighbor. The period of a protocol sequence set has a fundamental impact on delay performance. The question of finding protocol sequences with a minimal or near-minimal period has been extensively studied [28]–[30].

The period of protocol sequences is nonetheless not the sole consideration factor. Suppose that there are two users and

they schedule their packets according to the following protocol sequences of period 9:

$$s_1(t): \ 111\,000\,000$$
$$s_2(t): \ 100\,100\,100.$$

For $i = 1, 2$, the sequence $s_i(t)$ is assigned to user i. The first user sends packets in three consecutive time slots in each period of nine slot durations. The second user sends one packet in a period of three slot durations. We can check that no matter what the relative delay offsets are, there is exactly one collided packet in a period of nine slot durations, i.e., each of the two users can send two packets successfully. Both protocol sequences yield the same packet delivery ratio. However, the transmission pattern of the first protocol sequence is very bursty. The first user needs to wait for six slot durations until he can send again. In contrast, the locations of the 1's in the second protocol sequence are very evenly spread. The nonuniform distribution of packet transmissions causes relatively longer delay for the first user. The protocol sequences proposed in this work have the property that the 1's in a sequence period are evenly distributed, while maintaining some nonblocking property. A quantitative measure of the evenness of the distribution of 1's can be found in a separate work [31].

In Section II, we describe the system model and a general protocol for channel access. This general protocol provides a unifying framework of analysis and includes a deterministic access scheme with protocol sequences and an ALOHA-like random access scheme as special cases. In Section III, the family of a GP sequence is given. In Section IV, we analyze the delay performance of a protocol-sequence-based scheme, under the assumption that the users in the vicinity are using distinct GP sequences. In Section V, we describe an application of protocol sequences in VANETs, without assuming that the assigned protocol sequences are distinct, and compare the delay performance with some baseline schemes. Some of the longer proofs are given in the appendices.

II. System Model and Notations

Consider a particular user in a VANET and the surrounding users whose transmission ranges include this user. We call this particular user "user 0" and suppose that there are K users in the vicinity of user 0 who can transmit packets to user 0. User 0 wants to receive information from the K surrounding users and broadcast packets to them.

The communication channel is modeled as a time-slotted collision channel [10]. In this paper, we assume, for the sake of notational simplicity, that the system is slot-synchronous. The results in this paper can be extended to the slot-asynchronous case. If two or more users transmit packets in a time slot, then there is a collision, and the collided packets cannot be recovered. On the other hand, if only one user among the K users transmits at a time slot, then the packet can be received by user 0 without any error. We assume that the system is limited by interference, so that all packet erasures are due to packet collisions. If there are errors due to thermal noise for instance, we can employ a forward error-correcting code. In the rest of this paper, we will assume that successfully received packets are error-free.

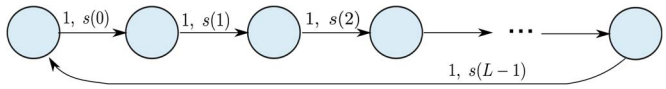

Fig. 2. Markov chain of the deterministic channel access scheme based on protocol sequence $s(t)$.

We assume that the transmission is half-duplex. When a user is transmitting a packet, he/she cannot receive anything from the channel. Otherwise, if a user is not transmitting, he/she listens to the channel and receives data from the others. We also assume that a user always has some data to send, so that there is no queue underflow problem. This assumption is applicable to the broadcast of periodic messages such as location or speed update.

We describe a general protocol for the time-slotted collision channel without feedback. This includes the deterministic channel access scheme using protocol sequences and several random channel access schemes. In the general protocol, each user decides whether he/she transmits or not by a finite Markov chain. The Markov chain of user i is represented by a directed graph. The vertices are also known as the states. Each directed edge has two labels. The first label is a probability between 0 and 1. The second label is either 0 or 1. It is required that for each state, the sum of the probabilities of the outgoing edges is equal to 1. The initial state is chosen according to a distribution function, and each user chooses the initial state independently. At the beginning of each time slot, user i picks one of the outgoing edges from the current state randomly according to the probability distribution specified by the first labels of the outgoing edges and transmits a packet if and only if the second label of the chosen edge is 1. Then, user i jumps to the state that is incident to the chosen edge.

For the protocol-sequence-based scheme, the number of states in the Markov chain is the same as the sequence period. There is only one outgoing edge from each node, and the graph is a cycle. The second labels of the edges are the bits in the protocol sequence (see Fig. 2). The users may not start their transmissions of packets at the same time. Suppose that for $k = 0, 1, 2, \ldots, K$, user k starts transmitting at τ_k, which is called *relative delay offset*. User k transmits a packet at time slot $t + \tau_k$ if and only if $s_k(t) = 1$. The relative delay offsets τ_k is a parameter that cannot be controlled. It is a parameter that is randomly drawn at the beginning and remains constant during the communication session. When the common period of the binary sequences is L, we model the relative delay offsets as discrete random variables uniformly and independently distributed between 0 and $L - 1$. It is equivalent to picking the initial state of the associated Markov chain uniformly at random.

We will compare with two random access schemes. The first one is called *π-persistent random access*. In this scheme, a user simply sends independently in a time slot with probability π. This is a special case of the general Markov chain framework with only one state (see Fig. 3). There are two self-loops, i.e., one with labels π and 1 and one with labels $1 - \pi$ and 0. The π-persistent random access is called *synchronous*

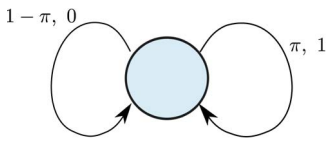

Fig. 3. Markov chain of the π-persistent random access scheme.

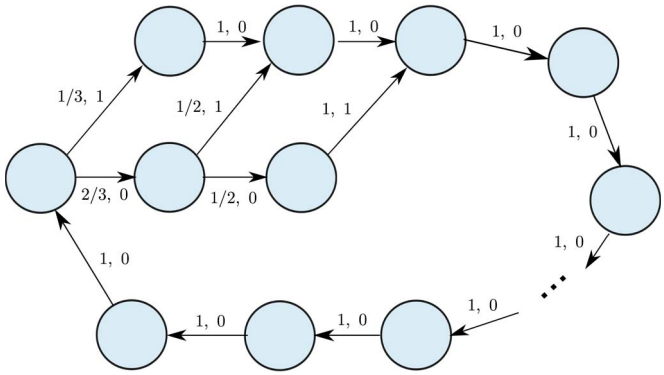

Fig. 4. Markov chain of the nonpersistent random access scheme.

p-persistent repetition in [4]. The second random scheme is called *nonpersistent random access*. User k transmits packets in slots

$$\tau_k + qm + U_{k,m}(W) \tag{1}$$

for $m \geq 0$, where τ_k is the relative delay offsets of mobile user k, q is a positive integer, $U_{k,m}(W)$'s are independent random variables uniformly drawn from $\{0, 1, \ldots, W-1\}$, and W is an integer that represents the window size. This scheme is the analog of nonpersistent CSMA for a time-slotted system. The random variable $U_{k,m}(W)$ models a random waiting time. An example of the Markov chain for $W = 3$ is shown in Fig. 4. We pick the nodes in the outer cycle in Fig. 4 randomly as the initial state. As in the deterministic scheme based on protocol sequences, we model the delay offset τ_k as a random variable uniformly distributed between 0 and $q-1$.

We consider four performance metrics.

The *duty factor* is defined as the fraction of time a user is transmitting [10]. It measures the rate of energy consumption. If the Hamming weight of a protocol sequence is w, the duty factor is given by $f \triangleq w/L$. For π-persistent random access, the duty factor is equal to π, and for nonpersistent random access, the duty factor is equal to $1/q$.

For $k = 1, 2, \ldots, K$, the *individual delay* of user k with respect to user 0 is defined by, starting at a randomly chosen time instance, the waiting time until user 0 can receive a packet from user k without collision. We denote the individual delay of user k with respect to user 0 by random variable X_k. For notational convenience, we will simply say "individual delay of user k" if it is understood that the delay is relative to user 0. For π-persistent random access, the individual delay is geometrically distributed, i.e., $\Pr(X_j \leq t) = 1 - \phi^{t+1}$, for $t = 0, 1, 2, \ldots$, where $\phi \triangleq 1 - \pi(1-\pi)^K$ is the probability that user j either remains silent in a time slot or transmits a packet with collision.

The *group delay* with respect to user 0 is defined by, starting at a randomly chosen time instance, the waiting time until users 1 to K have transmitted at least one uncollided packet to user 0. We will use Y to denote the group delay with respect to user 0. In addition, we will write "group delay" instead of "group delay with respect to user 0" if user 0 is understood. Alternately, we can define the group delay as the maximum of the individual delays

$$Y \triangleq \max_{1 \leq k \leq K} X_k.$$

The probability $\Pr(Y \leq t)$ is equal to the probability of the event $\bigcap_{k=1}^{K} \{X_k \leq t\}$.

For a given integer T, a user is said to be blocked by the others in T slot durations if all of his transmitted packets in this period of time are in collision, i.e., $X_k > T$. The *blocking probability* of a user is the probability that the user is blocked by the others.

We use the following notations in this paper. For a positive integer n, let $\mathbb{Z}_n \triangleq \{0, 1, \ldots, n-1\}$ be the set of residues of integers modulo n, with the modulo-n addition and subtraction denoted by $\oplus_n$ and $\ominus_n$, respectively.

Let L be the common period of a set of binary and periodic sequences. We define the *Hamming weight* of a protocol sequence $s(t)$ in this set as

$$w_s \triangleq \sum_{t=0}^{L-1} s(t)$$

which equals the number of 1's in $s(t)$ within a period. A cyclic shift of protocol sequence $s(t)$ by τ is denoted by $s^{(\tau)}(t) \triangleq s(t \ominus_L \tau)$. Given a pair of protocol sequences, i.e., $a(t)$ and $b(t)$, their *Hamming cross correlation* is defined by

$$H_{ab}(\tau) \triangleq \sum_{t=0}^{L-1} a(t) b^{(\tau)}(t).$$

It counts the number of overlapping 1's after cyclically shifting the second sequence $b(t)$ by τ. The *Hamming autocorrelation* of a sequence $a(t)$ is defined by

$$H_{aa}(\tau) \triangleq \sum_{t=0}^{L-1} a(t) a^{(\tau)}(t).$$

We define the *characteristic set* of $s(t)$ as the set of time indexes where $s(t)$ is equal to 1. For a characteristic set $\mathcal{I} \subseteq \mathbb{Z}_L$, we let $\mathcal{I} \oplus_L x$ be the translation $\{i \oplus_L x : i \in \mathcal{I}\}$. If the characteristic sets of sequences $a(t)$ and $b(t)$ are $\mathcal{I}_1$ and $\mathcal{I}_2$, respectively, we can easily check that $H_{ab}(\tau)$ is equal to the size of $\mathcal{I}_1 \cap (\mathcal{I}_2 \oplus_L \tau)$.

For example, the characteristic sets of the sequences $s_1(t)$ and $s_2(t)$ in the previous section are, respectively $\{0, 1, 2\}$ and $\{0, 3, 6\}$. It can be checked that, for all choices of delay τ, the set $\{0, 1, 2\}$ and the translated set $\{0, 3, 6\} \oplus_9 \tau$ contain exactly one common element. This verifies that $H_{s_1 s_2}(\tau) = 1$ for all τ.

Given two subsets $\mathcal{A}$ and $\mathcal{B}$ of $\mathbb{Z}_L$, we define their *difference set* by

$$\mathcal{A} \ominus_L \mathcal{B} \triangleq \{(a \ominus_L b) \in \mathbb{Z}_L : a \in \mathcal{A}, b \in \mathcal{B}\}$$

$$s(t) = \overbrace{\underbrace{100}_{3}\underbrace{1000}_{4}\underbrace{100}_{3}}^{7}$$
$$\Updownarrow$$
$$L = 10,\ \mathcal{I} = \{0, 3, 7\},\ d^*(\mathcal{I}) = \{3, 4, 6, 7\}.$$

Fig. 5. Difference set of a characteristic set of a sequence contains the intervals between 1's.

and their *sum set* by

$$\mathcal{A} \oplus_L \mathcal{B} \triangleq \{(a \oplus_L b) \in \mathbb{Z}_L : a \in \mathcal{A}, b \in \mathcal{B}\}.$$

If $\mathcal{B} = \{x\}$ is a singleton, then we write $\mathcal{A} \oplus_L \{x\}$ as $\mathcal{A} \oplus_L x$. The self-difference set $\mathcal{A} \ominus_L \mathcal{A}$ is denoted by $d(\mathcal{A})$. We note that the zero element in $\mathbb{Z}_L$ belongs to $d(\mathcal{A})$ for any nonempty set $\mathcal{A}$. In addition, if $y \in d(\mathcal{A})$, then $-y \in d(\mathcal{A})$. We let $d^*(\mathcal{A})$ be the set of nonzero elements in $d(\mathcal{A})$, i.e., $d^*(\mathcal{A}) \triangleq d(\mathcal{A}) \setminus \{0\}$. For a protocol sequence $s(t)$ with characteristic set $\mathcal{I}$, the elements in $d^*(\mathcal{I})$ are the time differences between pairs of "1" in the protocol sequence. An illustration is given in Fig. 5.

III. Generalized Prime Sequences

The GP sequences can be considered as a class of protocol sequences obtained by derandomizing the nonpersistent random scheme. Let p be a prime number and $rem(x, p)$ denote the remainder of x after division by p, which is an integer between 0 and $p-1$. For a given prime number p and an integer q, which is greater than or equal to p, we derandomize the nonpersistent random scheme by replacing the random numbers $U_{k,m}(W)$ in (1) by $rem(km, p)$. User k, for $k = 0, 1, \ldots, p-1$, transmits packets at time indexes

$$\tau_k + qm + rem(km, p) \tag{2}$$

for $m = 0, 1, 2, \ldots$. We note that in (2), only the relative delay offset τ_k is a random variable; the other terms are a deterministic function. The value of τ_k is fixed at the beginning of a communication session. Then, the sequence is a deterministic and periodic sequence with period $L = pq$. The characteristic set of sequence $s_k(t)$ is

$$\mathcal{I}_k = \{rem(k\ell, p) + \ell q : \ell = 0, 1, 2, \ldots, p-1\}. \tag{3}$$

The sequence associated with $\mathcal{I}_k$ is called *the sequence generated by* k. We will also say that k is the *generator* of sequence $s_k(t)$.

The p cyclically distinct sequences defined in (2) for $k = 0, 1, 2 \ldots, p-1$ are called the *GP sequences*. We use the symbol $\mathsf{GP}(p, q)$ to denote the resulting set of protocol sequences. This construction is an extension of two existing classes of protocol sequences in the literature of optical communication [32]. If $q = p$, the resulting protocol sequences are the *prime sequences* [33], and if $q = 2p-1$, we have the *extended prime sequences* [34]. As we will see in Appendix A, the GP sequences are closely related to the Chinese remainder theorem (CRT) sequences [29] when p and q are relatively prime. Anyway, in GP sequences, the choice of parameter q is flexible, and the value of q may be a multiple of p.

Example 1: Let $p = 5$ and $q = 7$. The protocol sequences in $\mathsf{GP}(5, 7)$ are

$s_0(t)$: 1000000 1000000 1000000 1000000 1000000

$s_1(t)$: 1000000 0100000 0010000 0001000 0000100

$s_2(t)$: 1000000 0010000 0000100 0100000 0001000

$s_3(t)$: 1000000 0001000 0100000 0000100 0010000

$s_4(t)$: 1000000 0000100 0001000 0010000 0100000

and the five corresponding characteristic sets are

$$\mathcal{I}_0 = \{0, 7, 14, 21, 28\},\ \mathcal{I}_1 = \{0, 8, 16, 24, 32\}$$
$$\mathcal{I}_2 = \{0, 9, 18, 22, 31\},\ \mathcal{I}_3 = \{0, 10, 15, 25, 30\}$$
$$\mathcal{I}_4 = \{0, 11, 17, 23, 29\}.$$

The Hamming cross correlation of a GP sequence is upper bounded by 2 in general and is upper bounded by 1 if q is sufficiently large. We summarize the Hamming cross correlation and autocorrelation properties in the following theorem.

Theorem 1: Let p be a prime number, and let $q \geq p$. For $g = 0, 1, 2, \ldots, p-1$, let $s_g(t)$ be the GP sequence generated by g.

1) $H_{s_0 s_h}(\tau) \in \{0, 1\}$ for $h = 1, 2, \ldots, p-1$.
2) If $q \geq 2p-1$, then $H_{s_g s_h}(\tau) \in \{0, 1\}$, for distinct g and h in $\{1, 2, \ldots, p-1\}$.
3) If $q \leq 2p-2$, then $H_{s_g s_h}(\tau) \in \{0, 1, 2\}$, for distinct g and h in $\{1, 2, \ldots, p-1\}$.
4) Suppose that q is not a multiple of p. For $g = 0, 1, \ldots, p-1$, let τ_g be the unique integer between 0 and pq, which satisfies $rem(\tau_g, p) = g$ and $rem(\tau_g, q) = 1$. (The integer τ_g is well defined by Chinese remainder theorem [35].) For $g = 1, 2, \ldots, p-1$, the Hamming autocorrelation $H_{s_g s_g}(\tau)$ of s_g is

$$H_{s_g s_g}(\tau) = \begin{cases} p-i, & \text{if } \tau = \pm rem(i\tau_g, pq), 0 \leq i < p \\ 0, & \text{otherwise.} \end{cases}$$

For $g = 0$, the Hamming autocorrelation $H_{s_0 s_0}(\tau)$ is given by

$$H_{s_0 s_0}(\tau) = \begin{cases} p, & \text{if } \tau \text{ is an integral multiple of } q \\ 0, & \text{otherwise.} \end{cases}$$

As a numerical example, consider sequences $s_1(t)$ and $s_4(t)$ in Example 2. The Hamming cross correlation of $s_1(t)$ and $s_4(t)$, i.e., $H_{s_1 s_4}(\tau)$, is equal to

$$\begin{cases} 0, & \text{if } rem(\tau, 35) \in \{2, 4, 6, 8, 10, 12, 16, 18, 24, 25, 31, 33\} \\ 2, & \text{if } rem(\tau, 35) \in \{3, 11\} \\ 1, & \text{otherwise.} \end{cases}$$

The Hamming autocorrelation of $s_4(t)$ is equal to

$$H_{s_4 s_4}(\tau) = \begin{cases} 5, & \text{if } rem(\tau, 35) = 0 \\ 4, & \text{if } rem(\tau, 35) = 6, 29 \\ 3, & \text{if } rem(\tau, 35) = 12, 23 \\ 2, & \text{if } rem(\tau, 35) = 17, 18 \\ 1, & \text{if } rem(\tau, 35) = 11, 24 \\ 0, & \text{otherwise.} \end{cases}$$

The proof of Theorem 1 is given in Appendix A.

Theorem 2: Suppose $p > K$, $q \geq 2p-1$, and users 0, 1, $\ldots, K$ are assigned distinct GP sequences from $\mathsf{GP}(p,q)$. Then, it is guaranteed with probability 1 that, for $i = 1, 2, \ldots, K$, user i can send at least one packet to user 0 successfully within a sequence period.

Proof: Consider a particular sequence, for example, $s(t)$, in $\mathsf{GP}(p,q)$. Since $q \geq 2p-1$, there is at most one overlapping "1" between $s(t)$ and the other K sequences assigned to the other users, regardless of the relative delay offsets. As the number of packets sent by a user in a sequence period is strictly larger than K, there is at least one packet that is not in collision. Hence, the user who is using $s(t)$ can send at least one packet to user 0 successfully within a period. ■

Remark 1: GP sequences can be regarded as optical orthogonal codes (OOCs) with unequal Hamming cross correlation and autocorrelation properties [36]. The Hamming autocorrelation of an OOC is usually required to be a small value for the purpose of code synchronization. In the context of protocol sequences, there is no such requirement for Hamming autocorrelation. An OOC, in general, is not suitable for the application in broadcasting safety messages, because the 1's in general OOCs do not spread evenly. If the 1's are bursty as in the example in Section 1, then the delay may be very long.

Remark 2: From part 4 of Theorem 1, we note that for $g = 1, 2, \ldots, p-1$, the Hamming autocorrelation of s_g can be any integer from 0 to p. Nevertheless, $H_{s_g s_g}(\tau)$ is nonzero for only $2p-1$ values of τ and is zero for the other values of τ. If $q \gg 3$, the Hamming autocorrelation is zero for a large fraction of the values of delay offset τ.

IV. Delays of Protocol-Sequence-Based Scheme

For a random-access scheme, there is no hard guarantee on delay; the maximal individual delay and group delay are unbounded. In contrast, for the protocol-sequence-based scheme, the maximal individual delay and group delay are upper bounded by the sequence period, provided that the protocol sequences are appropriately designed. Bounded delay is a desirable property for the safety-message broadcast application. Here, we first investigate the individual delay for a general protocol-sequence-based scheme, then we derive the distribution of individual delay when we use GP sequences as the protocol sequences.

A. Individual Delays in General

We show in this section that the individual delay in a protocol-sequence-based system can be expressed as a deterministic function of the characteristic sets and the delay offsets. For $k = 0, 1, 2, \ldots, K$, let $\mathcal{I}_k$ be the characteristic set of the protocol sequence assigned to user k.

Suppose that the relative delay offset of user k, which is denoted by τ_k, is given and fixed. User k transmits packets in the time slots indexed by $\mathcal{I}_k \oplus_L \tau_k$. Since a packet transmitted by user k is received by user 0 successfully if and only if there is no other user transmitting in the same time slot and user 0 is in the listening mode, the successful packets sent by user k have time indexes in

$$(\mathcal{I}_k \oplus_L \tau_k) \setminus \bigcup_{\substack{j=0 \\ j \neq k}}^{K} (\mathcal{I}_j \oplus_L \tau_j) \tag{4}$$

where "$\mathcal{A} \setminus \mathcal{B}$" denotes the set of elements in $\mathcal{A}$ but not in $\mathcal{B}$. We note that if the set of time indexes in (4) is empty, then user k cannot send any packet to user 0. The individual delay of user k with respect to user 0, for given relative delay offsets, can be computed by

$$X_k = \min \left((\mathcal{I}_k \oplus_L \tau_k) \setminus \bigcup_{\substack{j=0 \\ j \neq k}}^{K} (\mathcal{I}_j \oplus_L \tau_j) \right).$$

We adopt the convention that $\min \emptyset = \infty$.

Example 2: Suppose that user 0 employs protocol sequence

$$s_0(t): \ 100001000010000$$

and that there are $K = 2$ users in the vicinity of user 0. Users 1 and 2 employ protocol sequences

$$s_1(t): \ 100010001000000$$

$$s_2(t): \ 100100100000000.$$

All of the given protocol sequences have period $L = 15$. Let the delay offsets of the three users be $\tau_0 = 0$, $\tau_1 = 0$, and $\tau_2 = 4$, respectively. Hence, user 2 is transmitting packets according to the following schedule:

$$s_2(t \ominus_{15} 4): \ 000010010010000.$$

The characteristic sets of the three protocol sequences after shifting are, respectively, $\{0, 5, 10\}$, $\{0, 4, 8\}$, and $\{4, 7, 10\}$. The packet sent by user 1 at time slot 0 cannot be received by user 0 because user 0 transmits at time slot 0. The packet sent by user 1 at time slot 4 is in collision because user 2 transmits at time slot 4. The transmission by user 1 at time slot 8 is successful. Similarly, user 2 can send a packet to user 0 at time slot 7. Hence, the individual delays of users 1 and 2 with respect to user 0 are

$$\min\left(\{0, 4, 8\} \setminus \{0, 4, 5, 7, 10\}\right) = 8$$

$$\min\left(\{4, 7, 10\} \setminus \{0, 4, 5, 8, 10\}\right) = 7.$$

The group delay with respect to user 0 is $\max\{8, 7\} = 8$.

As there are L^K different combinations of relative delay offsets, we may regard the individual delay as function mapping from $\{0, 1, \ldots, L-1\}^K$ to the set of nonnegative integers. To characterize the delay performance, we want to count, for a given nonnegative integer x, the number of combinations of relative delay offsets that render the individual delay of user k with respect to user 0 less than or equal to x. As the relative delay offsets are modeled as random variables uniformly distributed between 0 and $L-1$, this can be expressed as in the form of cumulative distribution function (cdf), i.e.,

$$F_{X_k}(x) \triangleq \Pr(X_k \leq x).$$

If the protocol sequences are not properly designed, a user may be blocked for an indefinite period of time. This happens when

$$\mathcal{I}_k \subseteq \bigcup_{j\neq k} (\mathcal{I}_j \oplus_L \tau_j)$$

for some combinations of relative delay offsets. In this case, $F_{X_k}(x)$ is strictly less than 1 for all x. We can compute the blocking probability of user k by

$$\frac{1}{L^{K-1}} \left| \left\{ (\tau_1, \ldots, \tau_{k-1}, \tau_{k+1}, \ldots, \tau_K) : \mathcal{I}_k \subseteq \bigcup_{\substack{j=0 \\ j\neq k}}^{K} (\mathcal{I}_j \oplus_L \tau_j) \right\} \right| \tag{5}$$

where $|\mathcal{A}|$ denotes the cardinality of set $\mathcal{A}$.

B. Delay Analysis of GP Sequences

Here, we will give an analytic expression for the cdf of individual delay, under the assumption that the GP sequences assigned to the users are distinct. A few lemmas are required before we prove the main theorem in this section.

Lemma 3: Let $a(t)$ and $b(t)$ be binary sequences with common period L specified by characteristic sets $\mathcal{A}$ and $\mathcal{B}$, respectively. Then

$$\mathcal{A} \ominus_L \mathcal{B} = \{\tau \in \mathbb{Z}_L : H_{ab}(\tau) > 0\}.$$

Proof: It follows directly from the definition that:

$$\begin{aligned} \mathcal{A} \ominus_L \mathcal{B} &= \{a - b : a \in \mathcal{A},\ b \in \mathcal{B}\} \\ &= \{\tau \in \mathbb{Z}_L : \exists a \in \mathcal{A}, b \in \mathcal{B}, \text{such that } a = b + \tau\} \\ &= \{\tau \in \mathbb{Z}_L : \mathcal{A} \cap (\mathcal{B} + \tau) \neq \emptyset\} \\ &= \{\tau \in \mathbb{Z}_L : H_{ab}(\tau) > 0\}. \end{aligned}$$

This finishes the proof of Lemma 3. ■

We recall that there are, at most, two collided packets between two distinct users in a sequence period if $q \leq 2p-1$ and, at most, one if $q \geq 2p-2$. Let $\mathcal{I}$ and $\mathcal{I}'$ be the characteristic sets of two distinct GP sequences. If the Hamming cross correlation is either 0 or 1, then $d^*(\mathcal{I})$ and $d^*(\mathcal{I}')$ are disjoint. Otherwise, if the Hamming cross correlation takes value in $\{0, 1, 2\}$, then $d^*(\mathcal{I})$ and $d^*(\mathcal{I}')$ have two common elements x and $-x$, for some integer x between 1 and $L-1$.

The previous discussion motivates the following notations. For two subsets $\mathcal{A}$ and $\mathcal{B}$ in $\mathbb{Z}_L$ such that $d^*(\mathcal{A}) \cap d^*(\mathcal{B}) = \{\pm x\}$, let $f_1(\mathcal{A}, \mathcal{B})$ be the number of pairs $(a_1, a_2) \in \mathcal{A} \times \mathcal{A}$ such that $a_1 \ominus_L a_2 = x$ and $f_2(\mathcal{A}, \mathcal{B})$ be the number of pairs $(b_1, b_2) \in \mathcal{B} \times \mathcal{B}$ such that $b_1 \ominus_L b_2 = x$. We use $e(\mathcal{A}, \mathcal{B})$ as a short-hand notation for

$$e(\mathcal{A}, \mathcal{B}) \triangleq \begin{cases} 0, & \text{if } d^*(\mathcal{A}) \cap d^*(\mathcal{B}) = \emptyset \\ f_1(\mathcal{A}, \mathcal{B}) f_2(\mathcal{A}, \mathcal{B}), & \text{if } d^*(\mathcal{A}) \cap d^*(\mathcal{B}) = \{\pm x\}. \end{cases}$$

We need the following technical lemma.

Lemma 4: Let $a(t)$ and $b(t)$ be two protocol sequences of period L, with Hamming cross correlation value of, at most, 2. Let $\mathcal{A}$ and $\mathcal{B}$ be the corresponding characteristic sets of $a(t)$ and $b(t)$. Suppose that $d^*(\mathcal{A}) \cap d^*(\mathcal{B})$ is either empty or equal to $\{\pm x\}$ for some $x \in \mathbb{Z}_L \setminus \{0\}$, and x is not equal to $L/2$ when L is even. Then

$$|\mathcal{A} \ominus_L \mathcal{B}| = |\tau \in \mathbb{Z}_L : H_{ab}(\tau) > 0\}| = |\mathcal{A}||\mathcal{B}| - e(\mathcal{A}, \mathcal{B}).$$

The proof of Lemma 4 is given in Appendix B.

We can check that the condition in Lemma 4 is indeed satisfied by the GP sequences.

Lemma 5: Let $\mathcal{I}$ and $\mathcal{I}'$ be the characteristic sets of two distinct sequences in $\mathsf{GP}(p, q)$. Then

$$d^*(\mathcal{I}) \cap d^*(\mathcal{I}') = \begin{cases} \emptyset, & \text{for } q \geq 2p-1 \\ \emptyset \text{ or } \{\pm x\}, & \text{for } p < q \leq 2p-2. \end{cases}$$

In the second case, x is not equal to $L/2$ if L is even.

The proof of Lemma 5 is relegated to Appendix C.

Given a subset of time indexes $\mathcal{T}$ in $\{0, 1, \ldots, L-1\}$ with cardinality w, we let $x_{[1]}, x_{[2]}, \ldots, x_{[w]}$ be the elements in $\mathcal{T}$ in ascending order, i.e., $\mathcal{T} = \{x_{[1]}, x_{[2]}, \ldots, x_{[w]}\}$ and $x_{[1]} < x_{[2]} < \ldots < x_{[w]}$. We will use square brackets in subscripts to emphasize that the numbers are sorted in ascending order.

Given the delay offset of a user, the cdf of the individual delay is given in the following theorem.

Theorem 6: Consider $K+1$ active users, labeled from 0 to K. For $k = 0, 1, \ldots, K$, suppose that user k is assigned a GP sequence with period L and Hamming weight w and that these $K+1$ GP sequences are distinct. Denote the characteristic set of the protocol sequence assigned to user k by $\mathcal{J}_k$. Let ℓ be a fixed integer between 1 to K, and let the relative delay offset of user ℓ be fixed at τ_ℓ^*. Let the time indexes in $\mathcal{J}_\ell \oplus_L \tau_\ell^*$ be $x_{[1]} < x_{[2]} < \ldots < x_{[w]}$. For each nonempty subset $\mathcal{S}$ of $\{1, 2, \ldots, w\}$, let $\mathcal{J}_\ell(\tau_\ell^*, \mathcal{S})$ be the set $\{x_{[\ell]} : \ell \in \mathcal{S}\}$. If the relative delay offsets of users $0, 1, 2, \ldots, \ell-1, \ell+1, \ell+2, \ldots, K$ are distributed uniformly and independently between 0 and $L-1$, then the conditional cdf $F_{X_\ell}(x|\tau_\ell^*)$ of individual delay X_ℓ is equal to 0 for $0 \leq x < x_{[1]}$, and

$$\sum_{\substack{\mathcal{S} \subseteq \{1,\ldots,n\} \\ \mathcal{S} \neq \emptyset}} (-1)^{|\mathcal{S}|+1} \prod_{\substack{i=0 \\ i\neq \ell}}^{K} \left(1 - \frac{|\mathcal{S}|w - e\left(\mathcal{J}_\ell\left(\tau_\ell^*, \mathcal{S}\right), \mathcal{J}_i\right)}{L}\right)$$

for $x_{[n]} \leq x < x_{[n+1]}$, $n = 1, 2, \ldots, w$. The given summation is extended over all nonempty subsets of $\{1, 2, \ldots, n\}$, and the product is over all $i \in \{0, 1, 2, \ldots, K\} \setminus \{\ell\}$. (We let $x_{[w+1]} \triangleq \infty$ by convention.)

Proof: User ℓ transmits packets in time slots with time indexes $x_{[1]}, \ldots, x_{[w]}$. For $u = 1, 2, \ldots, w$, let E_u be the event that there is no collision at time slot $x_{[u]}$. For $1 \leq n \leq w$, consider the probability that the individual delay of user ℓ is strictly larger than $x_{[n]}$, i.e.,

$$\begin{aligned} \Pr\left(X_\ell > x_{[n]} | \tau_\ell^*\right) &= 1 - \Pr\left(E_1 \cup E_2 \cup \cdots \cup E_n | \tau_\ell^*\right) \\ &= 1 + \sum_{\substack{\mathcal{S} \subseteq \{1,\ldots,n\} \\ \mathcal{S} \neq \emptyset}} (-1)^{|\mathcal{S}|} \Pr\left(\bigcap_{u \in \mathcal{S}} E_u | \tau_\ell^*\right). \end{aligned} \tag{6}$$

The last equality follows from the principle of inclusion and exclusion. Conditioned on relative delay offset τ_ℓ^*, the event $\bigcap_{u\in\mathcal{S}} E_u$ happens when none of the users $0, 1, \ldots, \ell-1, \ell+1, \ldots, K$ transmits at time slot $x_{[u]}$ for all $u \in \mathcal{S}$.

For each $i \in \{0, 1, \ldots, K\} \setminus \{\ell\}$, user i does not transmit at the time slots indexed by $\mathcal{J}_\ell(\tau_\ell^*, \mathcal{S})$ with probability

$$\begin{aligned}\frac{1}{L}\left|\{\tau : \mathcal{J}_\ell(\tau_\ell^*, \mathcal{S}) \cap (\mathcal{J}_i \oplus_L \tau) = \emptyset\}\right| \\ = 1 - \frac{1}{L}\left|\{\tau : \mathcal{J}_\ell(\tau_\ell^*, \mathcal{S}) \cap (\mathcal{J}_i \oplus_L \tau) \neq \emptyset\}\right| \\ = 1 - \frac{1}{L}\left|\mathcal{J}_\ell(\tau_\ell^*, \mathcal{S}) - \mathcal{J}_i\right|. \end{aligned} \tag{7}$$

The last equality follows from the proof of Lemma 3. Since Lemma 4 also holds for subsets of the characteristic sets of GP sequences, the probability in (7) can be written as

$$1 - \frac{|\mathcal{S}|w - e\left(\mathcal{J}_\ell(\tau_\ell^*, \mathcal{S}), \mathcal{I}_\ell\right)}{L}.$$

Hence

$$\Pr\left(\bigcap_{u\in\mathcal{S}} E_u | \tau_\ell^*\right) = \prod_{\substack{i=0 \\ i\neq\ell}}^{K} \left(1 - \frac{|\mathcal{S}|w - e\left(\mathcal{J}_\ell(\tau_\ell^*, \mathcal{S}), \mathcal{J}_i\right)}{L}\right). \tag{8}$$

We obtain the conditional cdf in the theorem by putting (8) into (6).

Once the conditional cdf of individual delay X_j is explicitly given, the cdf of X_ℓ can be obtained by

$$\Pr(X_\ell \leq x) = \frac{1}{L}\sum_{\tau=0}^{L-1} \Pr(X_\ell \leq x | \tau_\ell = \tau). \tag{9}$$

To compute the cdf of group delay Y, we take the simplifying assumption that the individual delay X_j's are independent and approximate the distribution of Y by

$$\Pr(Y \leq t) = \prod_{j=1}^{K} \Pr(X_j \leq t). \tag{10}$$

The simplifying assumption will be justified by simulation.

We illustrate the given analytic results by an explicit example. Suppose that user 0 is surrounded by 22 other users, and suppose that these 23 active users are assigned distinct GP sequences of length 1035 and weight 23. The sequences are constructed with parameters $p = 23$ and $q = 45$. The cdfs of the individual and group delay of the 22 users with respect to user 0 are plotted in Fig. 6. By Theorem 2, we know that the blocking probability is 0. Thus, the probabilities in (9) is equal to 1 after one sequence period. The cdfs of the individual delays are very close to each other. We can infer that, although the protocol sequences assigned to the 23 users are distinct, the performance in terms of individual delays is virtually the same.

In Fig. 6, we also plot the approximation of the group delay as in (10) and the cdf obtained by simulation. We can see that the two cdfs match each other very well. The expected value of the group delay is roughly equal to 173 by simulation.

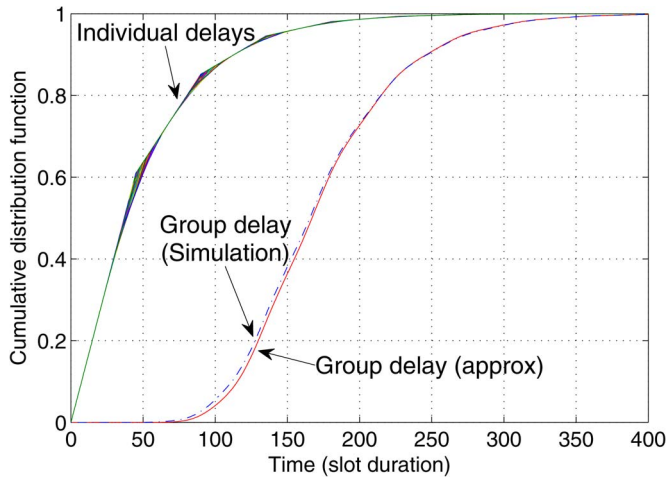

Fig. 6. Individual and group delays of GP sequences ($p = K = 23,\ q = 45,\ L = 1035$).

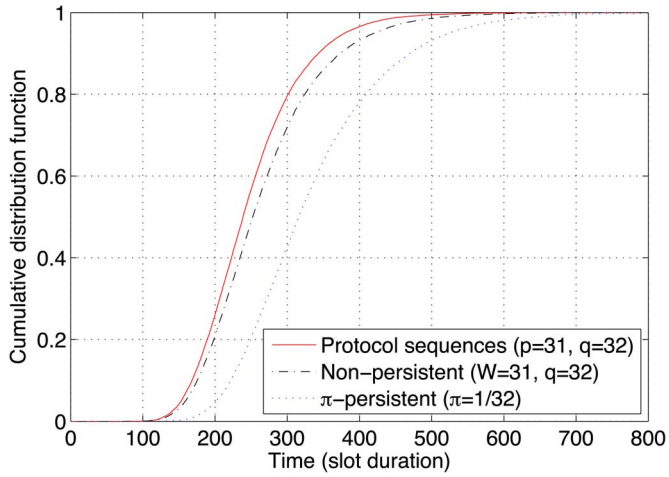

Fig. 7. CDFs of the group delays of the protocol-sequence-based scheme and random access schemes ($K = 31,$ duty factor $= 1/32$).

The approximation in (10) yields 174.2. This justifies that the independence assumption used in (10).

Next, we compare the deterministic protocol-sequence-based channel access schemes with the π-persistent and nonpersistent random access schemes. We use the GP sequences $\mathsf{GP}(31, 32)$. Each user is assigned a distinct GP sequence, and all users are active. The cdfs of the individual and group delay are shown in Fig. 7. The duty factor is $31/992 = 1/32$. For fair comparison, in the π-persistent random access scheme, each user transmits a packet independently with probability $\pi = 1/32$, and in the nonpersistent random access, we pick parameter q in (1) to be $q = 32$. The random and deterministic schemes thus share the same duty factor. The group delay of the protocol-sequence-based scheme is smaller than the two random schemes. If we focus on the 99th percentile, the delays are approximately 470, 520, and 650, respectively. The ratio between the 99th percentile of protocol sequences and the 99th percentile of nonpersistent random access is $470/520 \doteq 0.9$. There is roughly a 10% improvement.

We note that the only difference between the nonpersistent random scheme and the scheme based on GP sequences is

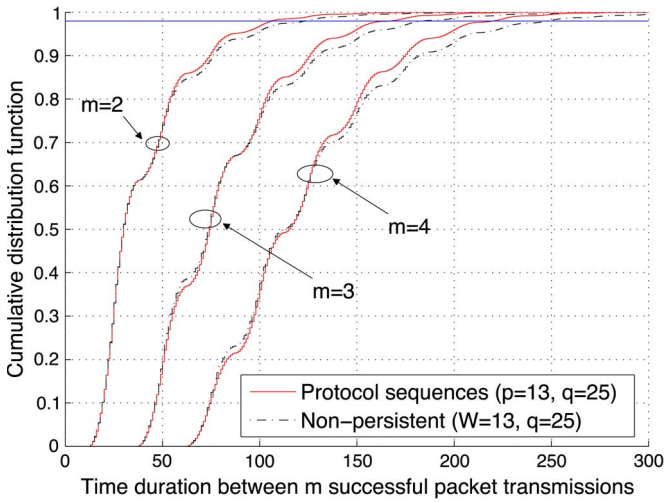

Fig. 8. Comparison of the time duration between consecutive successful packet transmissions for the protocol-sequence-based scheme and nonpersistent random access schemes ($K = 13,$ duty factor $= 1/25$).

that the uniform random variable $U_{k,m}(W)$ is replaced by the deterministic function $rem(km, p)$. The algebraic structure of modulo-p multiplication assures that two users collide, at most, once in a sequence period, and this induces reduction in delay.

The time required to send two or more packets successfully is also of interest. In Fig. 8, we compare the time duration between m consecutive successful packet transmission for the scheme based on GP sequences and the random nonpersistent scheme. In both cases, there are 13 active users, and the duty factor is 1/25. For the protocol-sequence-based scheme, the GP sequences $\mathsf{GP}(13, 25)$ are assigned to the users such that no two users have the same sequence. A sample point in the Monte Carlo simulation is obtained by randomly choosing a user, randomly picking the relative delay offsets of all users, and taking the time difference between the first and the mth successful packets of the chosen user, for $m = 2$, 3 and 4. For the nonpersistent random access, we generate the transmission schedule according to (1) with parameters $W = 13$ and $q = 25$. The cdfs of the intersuccessful-packet time for $m = 2, 3, 4$ are plotted in Fig. 8.

The top part of the figure, where the value of the cdf is close to 1, is pertinent to delay-sensitive applications. The gap between the cdfs pertaining to the protocol-sequence-based scheme and nonpersistent random scheme can be observed. For example, we can look at the horizontal line at probability 0.98 in Fig. 8. The protocol-sequence-based scheme can send four successful packets in roughly 220 packet durations; however, the nonpersistent scheme requires 250 packet durations. The difference can be intuitively explained by the property that the Hamming cross correlation of any two distinct sequences in $\mathsf{GP}(13, 25)$ is at most 1. If user j has a packet collision with user i (for some $j \neq i$), user j is guaranteed not to collide with user i, again within a sequence period. Hence, when user j attempts to send a packet again, there are fewer users who may collide with user j, and it is more likely that the packet sent by user j will be successful. In contrast, with the nonpersistent random scheme, there is no such reduction in the probability of collision.

V. Application to Safety-Message Broadcast

In the application of protocol sequences for broadcasting messages in VANETs, because of mobility, two mobile users within their hearing range may use the same protocol sequences. In this case, they may have two or more collided packets within a period. However, if the relative delay offsets are uniformly distributed, the probability that the Hamming autocorrelation is nonzero is $(2p - 1)/(pq)$ by Theorem 1. The chance for having collided packets between two users with the same protocol sequence is not high if q is large enough. As the protocol sequences can be reassigned at roadside nodes, the effect of duplicate sequences can be further mitigated.

If necessary, additional measures may be taken to avoid total blocking. We introduce a hybrid scheme called the *random hopping* scheme. A user makes a random "delay shift" after a certain period of time. The random hopping scheme is between the nonpersistent scheme and the deterministic protocol-sequence-based scheme. There is a design parameter T. If T is set to 1, the random hopping scheme is the same as the nonpersistent scheme, and when $T \to \infty$, the random hopping scheme is the protocol-sequence-based scheme.

We define the random hopping scheme formally as follows. For $i = 1, 2, \ldots, p - 1$, we let $V_{i,0}$, $V_{i,1}$, $V_{i,2}$ ... be independent random variables uniformly distributed over $\{0, 1, \ldots, p - 1\}$. User i transmits a packet at time slots with indexes

$$\tau_i + mq + rem\left(i(m + V_{i,\lfloor m/T \rfloor}), p\right)$$

for $m \geq 0$. The protocol sequence changes "phase" after every group of qT time slots. With the random hopping feature enabled, any two users with the same GP sequence will not be blocked forever. In the random hopping scheme, we do not include the GP sequence generated by p since randomization has no effect on this sequence.

To compare with nonpersistent and π-persistent random scheme in the application of safety-message broadcast, we measure a modified version of group delay. We start with a random time and measure the time until all users have transmitted at least one packet successfully. Let this time instance be x. We then wait until the time after x when every user succeeds in sending at least one more packet. Let the second time instance be y. The difference $y - x$ is interpreted as the time that, after the users have received a packet from each other, they need to wait until every user sends an uncollided packet. We call this the *modified group delay*.

We estimate the cdf of the time difference $y - x$. In Fig. 9, we plot the 95th percentile of the modified group delays for the protocol-sequence-based scheme with random hopping, the nonpersistent random scheme, and the π-persistent random scheme. The horizontal axis is the number of users. The protocol sequence set is $\mathsf{GP}(19, 30)$ with the protocol sequence with least period 30 removed. Parameter T is set to 15. In the simulation, when the number of users is less than or equal to 18, the protocol sequences are randomly chosen in such a way that no two active users use the same sequence. When the number of users is larger than or equal to 19, some sequences are shared by two users. The duty factor of both nonpersistent and π-persistent random schemes in the simulation is 1/30.

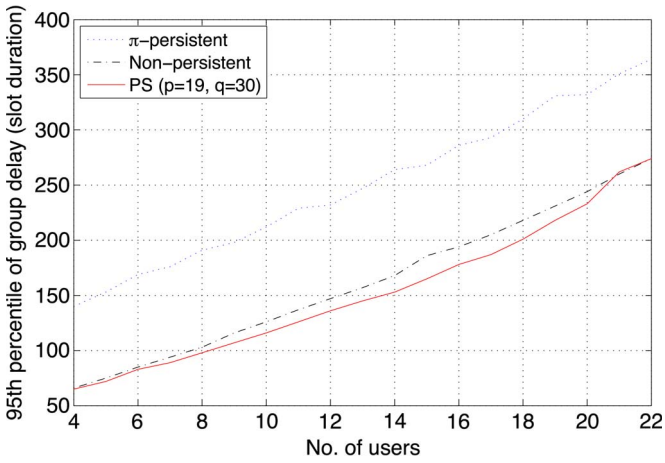

Fig. 9. Ninety fifth percentile of group delay versus number of users.

TABLE I
MODIFIED GROUP DELAY FOR $T = 1, 5, 9, 13, 17$

T	95-th percentile of the modified group delay
1	247
5	241
9	235
13	235
17	234

Parameter W in the nonpersistent scheme is set to p. If we look at the horizontal line where the 95th percentile is 150 slot durations for example, the nonpersistent random scheme can support 12 users, whereas the protocol sequence scheme can support 14 users.

We summarize the observations in Fig. 9 as follows. If the sequence assignment is such that a group of neighboring users have distinct protocol sequences, then for a given 95th percentile of modified group delay, the number of supported users can be increased roughly by 15%. If there are two users with the same assigned protocol sequence, the delay performance is no worse than the nonpersistent slotted ALOHA protocol.

Next, we investigate the effect of parameter T by considering a system with 20 users, sharing the sequences in $\mathsf{GP}(19, 30)$. As in the previous discussion, the GP generated by 19 is not used. Hence, there are two users who are assigned the same protocol sequences. We tabulate the modified group delay for $T = 1, 5, 9, 13, 17$ in Table I.

We note that the 95th percentile of the modified group delay in the row with $T = 1$ is the same as the 95th percentile of the nonpersistent scheme. We observe that by increasing T from 1 to 9, the modified group delay decreases. For T larger than or equal to 9, the performance is dominated by other factors, and the 95th percentile remains constant.

We thus see that by replacing the random numbers in the nonpersistent scheme by some mod-p arithmetics as in the protocol sequence scheme, we can indeed improve the delay performance.

VI. CONCLUSION

In the conventional ALOHA-type transmission scheme, pseudorandom bits are used as an input to the channel access mechanism. In this paper, a family of protocol sequences is constructed. The protocol sequences have a certain structure that can further reduce the individual and group delays. This illustrates the potential advantage of the protocol sequence scheme in the application for broadcasting safety messages in VANETs. The protocol-sequence-based scheme is effective as long as a group of neighboring users are assigned distinct protocol sequences. Maintaining the distinctness of protocol sequences is crucial and is an important direction for future research.

We note that although the system performance analysis is slightly complicated, the construction and regeneration of the protocol sequences are simple, using only modular arithmetic, and do not require random number generators.

APPENDIX A
PROOF OF THEOREM 1

For integer q, which is not divisible by p, there is an alternate description of GP sequences using CRT. Let m and n be two relatively prime positive integers. The function $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, given by $f(x) \triangleq (x \bmod m, x \bmod n)$, is an addition-preserving mapping, i.e., for $x, y \in \mathbb{Z}_{mn}$, we have $f(x \oplus_{mn} y) = f(x) + f(y)$. We note that the addition on the left-hand side is addition mod mn and the addition on the right-hand side is component-wise addition, with the first component reduced mod m and second component reduced mod n. The CRT says that mapping f is a bijection [35]. This function f is called the *CRT correspondence*. As a result, the integers $0, 1, \ldots, mn-1$ can be arranged in an $m \times n$ array. We will apply CRT with $m = p$ and $n = q$, for prime p and integer q, which is not divisible by p. A time index x between 0 and $pq-1$ is mapped to the pair $(x \bmod p, x \bmod q)$.

Consider the image of $\mathcal{I}_0$ under the CRT correspondence. Since $\mathcal{I}_0$ consists of multiples of q, the second coordinate of $(x \bmod p, x \bmod q)$ is zero for all $x \in \mathcal{I}_0$. The image of $\mathcal{I}_0$ under the CRT correspondence is thus

$$\mathcal{I}_0' = \{(j, 0) : j = 0, 1, \ldots, p-1\}. \tag{11}$$

For $g = 1, 2, \ldots, p-1$, the image of the characteristic set of of the sequence generated by g, under the CRT correspondence, is

$$\{(g\ell \oplus_p \ell q \bmod p, rem(g\ell, p) \bmod q) : \text{ for } \ell = 0, 1, \ldots, p-1\}.$$

We make a change of variable $j = rem(g\ell, p)$. When ℓ runs from 0 to $p-1$, the new variable j also runs from 0 to $p-1$. We can rewrite $g\ell \oplus_p \ell q$ as

$$(g \oplus_p q)\ell \equiv (g \oplus_p q)g^{-1}j \equiv (1 \oplus_p g^{-1}q)j \bmod p$$

where g^{-1} is the multiplicative inverse of g mod p. We define g' as a short-hand notation, i.e.,

$$g' \triangleq 1 + rem(g^{-1}q, p).$$

The addition in the given equation is integer addition. When g runs from 1 to $p-1$, $rem(g^{-1}q, p)$ also runs from 1 to $p-1$.

Hence, g' is an integer between 2 and p. The image of $\mathcal{I}_g$ under the CRT correspondence is thus

$$\mathcal{I}'_{g'} \triangleq \{(jg', j) \in \mathbb{Z}_p \times \mathbb{Z}_q : j = 0, 1, \ldots, p-1\}. \quad (12)$$

We can thus present the characteristic set of a GP sequence by (11) and (12) for $g' = 2, 3, 4, \ldots, p$. (We note that $\mathcal{I}'_1$ is not defined.)

1) We use the fact that $H_{s_0 s_h}(\tau) \leq 1$ if and only if $d^*(\mathcal{I}_0) \cap d^*(\mathcal{I}_h) = \emptyset$ and show that $d^*(\mathcal{I}_0) \cap d^*(\mathcal{I}_h) = \emptyset$. First of all, the characteristic set of the sequence generated by 0 is $\mathcal{I}_0 = \{0, q, 2q, \ldots, (p-1)q\}$. Thus, every element in $d^*(\mathcal{I}_0)$ is divisible by q.

   For $h = 1, 2, \ldots, p-1$, the difference between any two distinct elements in $\mathcal{I}_h$ is $rem(h\ell_1, p) + \ell_1 q - rem(h\ell_2, p) - \ell_2 q$. The difference between the first and third terms $rem(h\ell_1, p) \ominus_p rem(h\ell_2, p)$ is nonzero mod p because h is nonzero and is between $-(p-1)$ and $p-1$. As $q \geq p$, $rem(h\ell_1, p) \ominus_q rem(h\ell_2, p)$ is not congruent to 0 mod q. This proves that $d^*(\mathcal{I}_0) \cap d^*(\mathcal{I}_h) = \emptyset$.
2) We first prove a uniqueness property. Let $\mathcal{A} = \{0, q, 2q, 3q, \ldots\}$ be the set of multiples of q in $\mathbb{Z}_L$ and $\mathcal{B} = \{0, \pm 1, \pm 2, \ldots, \pm(p-1)\} \subset \mathbb{Z}_L$. By definition, every element c in $\mathcal{A} \oplus_L \mathcal{B}$ can be written as a sum $a \oplus_L b$, with $a \in \mathcal{A}$ and $b \in \mathcal{B}$. For $\mathcal{A}$ and $\mathcal{B}$ as previously defined, there is only one way to decompose c as a sum $a \oplus_L b$. To see this, suppose on the contrary that if $c = a_1 \oplus_L b_1 = a_2 \oplus_L b_2$ for some $a_1, a_2 \in \mathcal{A}$ and $b_1, b_2 \in \mathcal{B}$, then we have

$$a_1 \ominus_L a_2 = b_1 \ominus_L b_2. \quad (13)$$

   The difference $b_1 - b_2$ lies between $-2(p-1)$ and $2(p-1)$. If we reduce $b_1 - b_2$ modulo L (recall that $L = pq$), the residue cannot be a multiple of q, because $q > 2p - 2$ by assumption. However, the left side of (13) is a multiple of q. The equality in (13) cannot hold, and we have a contradiction.

   Suppose that g and h are two distinct nonzero generators, and suppose that

$$rem(g\ell_1, p) +_L \ell_1 q - (rem(g\ell_2, p) + \ell_2 q) \equiv rem(h\ell'_1, p) + \ell'_1 q - (rem(h\ell'_2, p) + \ell'_2 q) \bmod L$$

   for some integers ℓ_1 and ℓ_2 between 0 and $p-1$. After some rearrangements, we get

$$(\ell_1 - \ell_2)q + rem(g\ell_1, p) - rem(g\ell_2, p) \equiv (\ell'_1 - \ell'_2)\, q + rem(g\ell'_1, p) - rem(g\ell'_2, p) \bmod L.$$

   By the uniqueness property previously mentioned, we have

$$\ell_1 - \ell_2 = \ell'_1 - \ell'_2 \quad (14)$$

$$rem(g\ell_1, p) - rem(g\ell_2, p) = rem(h\ell'_1, p) - rem(h\ell'_2, p). \quad (15)$$

   The second equation (15) implies

$$g(\ell_1 - \ell_2) \equiv h(\ell'_1 - \ell'_2) \bmod p.$$

   If we replace $\ell'_1 - \ell'_2$ by $\ell_1 - \ell_2$ in the given equation, we obtain $(g-h)(\ell_1 - \ell_2) \equiv 0 \bmod p$, which contradicts the assumption that $g \neq h$. This proves that $d^*(\mathcal{I}_g)$ and $d^*(\mathcal{I}_h)$ are disjoint for $g \neq h$.
3) When $q = p$, the result follows from the fact that the Hamming cross correlation of two prime sequences is, at most, 2 [33]. We consider q in the range $p < q \leq 2p - 2$. As p and q are relatively prime for $p < q \leq 2p - 2$, we will use the 2-D representations of the sequences via the CRT correspondence.

   For the sake of contradiction, suppose that $H_{s_g s_g}(\tau) \geq 3$ for some τ, i.e., we can find integers i_1, i_2, i_3, j_1, j_2, and j_3, such that

$$(gi_\ell + \tau', i_\ell + \tau'') = (hj_\ell, j_\ell) \quad (16)$$

   for $\ell = 1, 2, 3$, where $\tau'' \in \mathbb{Z}_q$, and $\tau' \in \mathbb{Z}_p$.

   By comparing the second components, we have $j_1 - i_1 \equiv j_2 - i_2 \equiv j_3 - i_3 \equiv \tau'' \bmod q$. Note that $j_1 - i_1$, $j_2 - i_2$, and $j_3 - i_3$ are between $-(p-1)$ and $p-1$. In the following, we suppose that $j_1 - i_1 \geq 0$. The case where $j_1 - i_1 < 0$ can be treated similarly and is omitted. We consider two cases.
   a) $0 \leq j_1 - i_1 \leq q - p$. Because $q \leq 2p - 2$ by hypothesis, we have $q - p \leq p - 2$. There is only one choice for the values of the three differences $j_\ell - i_\ell$, for $\ell = 1, 2, 3$. Indeed, as $j_2 - i_2 \equiv j_1 - i_1 \bmod q$, $j_2 - i_2 = j_1 - i_1 + \alpha q$ for some integer α. If $\alpha \neq 0$, this would render the value of $j_2 - i_2$ out of the permissible range $[-(p-1), p-1]$. Therefore, $j_2 - i_2 = i_1 - i_1$. The same reason shows that $j_3 - i_3 = j_1 - i_1$.
   b) $q - p < j_1 - i_1 \leq p - 1$. For $\ell = 2, 3$, the difference $j_\ell - i_\ell$ may assume two distinct values, namely, either $j_1 - i_1$ or $j_1 - i_1 - q$.

   In any case, by the pigeonhole principle, at least two differences among $j_1 - i_1$, $j_2 - i_2$, and $j_3 - i_3$ are equal. Suppose, without loss of generality, that $j_1 - i_1 = j_2 - i_2 = x$ for some integer x. By comparing the first components on both sides of (16), we obtain $gi_\ell + \tau' \equiv h(i_\ell + x) \bmod p$ for $\ell = 1, 2$. After subtracting, we get $(g-h)(i_1 - i_2) \equiv 0 \bmod p$. Because $i_1 \neq i_2$, we get a contradiction that $g \equiv h \bmod p$.
1) The elements in the characteristic set of a GP sequence can be written as $a + bj$ for some a and b in $\mathbb{Z}_p \times \mathbb{Z}_q$, for $j = 0, 1, 2, \ldots, p-1$. The distribution of the autocorrelation now follows from the fact that:

$$a, a + b, a + 2b, \ldots, a + (p-1)b$$

   form an arithmetic progression in the *Abelian* group $\mathbb{Z}_p \times \mathbb{Z}_q$.

APPENDIX B
PROOF OF LEMMA 4

The first equality is established in Lemma 3. We prove the second equality as follows. Let $\mathbb{I}(P)$ denote the indicator

function defined as 1 if P is true and 0 otherwise. We count the number of elements in $\mathcal{A} \ominus_L \mathcal{B}$ by

$$|\{\tau \in \mathbb{Z}_L : H_{ab}(\tau) > 0\}| = \sum_{\tau=0}^{L-1} \left(H_{ab}(\tau) - \mathbb{I}\left(H_{ab}(\tau) = 2\right)\right).$$

The summation of $H_{ab}(\tau)$ over τ in the last line is equal to $|\mathcal{A}||\mathcal{B}|$ by a change of the order of summations, i.e.,

$$\begin{aligned}\sum_{\tau=0}^{L-1} H_{ab}(\tau) &= \sum_{\tau=0}^{L-1}\sum_{t=0}^{L-1} a(t)b(t \ominus_L \tau) \\ &= \sum_{t=0}^{L-1} a(t) \sum_{\tau=0}^{L-1} b(t \ominus_L \tau) \\ &= |\mathcal{A}||\mathcal{B}|.\end{aligned}$$

If $d^*(\mathcal{A}) \cap d^*(\mathcal{B})$ is the empty set, then the sum of the indicator functions over τ is equal to 0. Otherwise, if $d^*(\mathcal{A}) \cap d^*(\mathcal{B}) = \{\pm x\}$, then $\sum_{\tau=0}^{L-1} \mathbb{I}(H_{ab}(\tau) = 2)$ is equal to

$$\sum_{\tau=0}^{L-1}\sum_{\alpha\in\mathcal{A}}\sum_{\beta\in\mathcal{B}} \mathbb{I}(\beta = \alpha \oplus_L \tau, \alpha \oplus_L x \in \mathcal{A}, \beta \oplus_L x \in \mathcal{B}).$$

The hypothesis that $x \neq L/2$ is required here. After an exchange of the order of summations, we get

$$\begin{aligned}&\sum_{\alpha\in\mathcal{A}}\sum_{\beta\in\mathcal{B}}\sum_{\tau=0}^{L-1} \mathbb{I}(\beta = \alpha \oplus_L \tau, \alpha \oplus_L x \in \mathcal{A}, \beta \oplus_L x \in \mathcal{B}) \\ &= \sum_{\alpha\in\mathcal{A}}\sum_{\beta\in\mathcal{B}} \mathbb{I}(\alpha \oplus_L x \in \mathcal{A})\mathbb{I}(\beta \oplus_L x \in \mathcal{B}) \\ &= f_1(\mathcal{A},\mathcal{B})f_2(\mathcal{A},\mathcal{B}) = e(\mathcal{A},\mathcal{B}).\end{aligned}$$

This proves the second equality $|\{\tau \in \mathbb{Z}_L : H_{ab}(\tau) > 0\}| = |\mathcal{A}||\mathcal{B}| - e(\mathcal{A},\mathcal{B})$ in Lemma 4.

Appendix C
Proof of Lemma 5

Let g and g' be two distinct generators of GP sequences in $\mathbb{Z}_p$, and let $\mathcal{I} = \{(gj, j) : j = 0, 1, \ldots, p-1\}, \mathcal{I}' = \{(g'j, j) : j = 0, 1, \ldots, p-1\}$ be the corresponding characteristic sets.

For $q \geq 2p-1$, it is shown in the second part of Theorem 1 that the Hamming cross correlation of two GP sequences is, at most, 1. Hence, $d^*(\mathcal{I}) \cap d^*(\mathcal{I}') = \emptyset$.

In the remainder of the proof, we suppose that $q \leq 2p-2$. By Theorem 1, the Hamming cross correlation between these two GP sequences is, at most, 2.

Let α be an element of $\mathbb{Z}_L$ belonging to $d^*(\mathcal{I})$ and $d^*(\mathcal{I}')$. Let i_1, i_2, i'_1 and i'_2 be integers such that $i_1 \neq i_2$, $i'_1 \neq i'_2$, and

$$(gi_1, i_1) - (gi_2, i_2) = (\beta, \gamma) \tag{17}$$

$$(g'i'_1, i'_1) - (g'i'_2, i'_2) = (\beta, \gamma) \tag{18}$$

where $\beta \equiv \alpha \bmod p$, and $\gamma \equiv \alpha \bmod q$. Equating the first and second components in (17) and (18), we have

$$g(i_1 - i_2) \equiv g'(i'_1 - i'_2) \equiv \beta \bmod p \tag{19}$$

$$i_1 - i_2 \equiv i'_1 - i'_2 \equiv \gamma \bmod q. \tag{20}$$

By multiplying α by -1 if necessary, we assume $i_1 > i_2$. Because $0 < i_1 - i_2 \leq p-1$, we have $i_1 - i_2 = \gamma$ by (20).

We consider the following two cases: 1) $i'_1 - i'_2 = \gamma$; and 2) $q + i'_1 - i'_2 = \gamma$.

In case 1), (19) can be rewritten as $g\gamma \equiv \beta \bmod p$ and $g'\gamma \equiv \beta \bmod p$. In terms of matrix, we get

$$\begin{bmatrix} g & -1 \\ g' & -1 \end{bmatrix} \begin{bmatrix} \gamma \\ \beta \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix} \bmod p.$$

Because $g \neq g'$, the determinant of the system of linear equations is nonzero. The only solution (γ, β) to these two linear congruence equations is $\gamma = \beta = 0$. This contradicts that α is nonzero. Hence, case 1) cannot hold.

In case 2), we have $g\gamma \equiv \beta \bmod p$ and $g'(\gamma - q) \equiv \beta \bmod p$. In matrix form, it can be written as

$$\begin{bmatrix} g & -1 \\ g' & -1 \end{bmatrix} \begin{bmatrix} \gamma \\ \beta \end{bmatrix} \equiv \begin{bmatrix} 0 \\ g'q \end{bmatrix} \bmod p.$$

There is a unique solution to the given system of linear equations Hence, given g and g', β and γ are uniquely determined. From the CRT correspondence, α is uniquely determined. Hence, $d^*(\mathcal{I}) \cap d^*(\mathcal{I}') = \{\pm\alpha\}$.

When L is even, the integer $L/2$ only occurs in the characteristic set generated by $g = 0$ and, thus, cannot be in the intersection of two distinct characteristic sets. This proves that the common difference x is not equal to $L/2$ when L is even.

References

[1] P. Papadimitratos, A. de La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, "Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 84–95, Nov. 2009.

[2] K. Bilstrup, E. Uhlemann, E. G. Strom, and U. Bilstrup, "Evaluation of the IEEE 802.11p MAC method for vehicle-to-vehicle communication," in *Proc. IEEE VTC 2008-Fall*, Calgary, AB, Canada, Sep. 2008, pp. 1–5.

[3] T. ElBatt, S. K. Goel, G. Holland, H. Krishnan, and J. Parikhn, "Cooperative collision warning using dedicated short range wireless communications," in *Proc. 3rd Int. Workshop VANET*, Los Angeles, CA, USA, 2006, pp. 1–9.

[4] Q. Xu, T. Mak, J. Ko, and J. Sengupta, "Medium access control protocol design for vehicle–vehicle safety messages," *IEEE Trans. Veh. Technol.*, vol. 56, no. 2, pp. 499–518, Mar. 2007.

[5] Y. Feng, Y. Du, Z. Ren, Z. Wang, Y. Liu, and L. Zhang, "Adaptive beacon rate adjusting mechanism for safety communication in cooperative IEEE 802.11p-3G vehicle–infrastructure systems," in *Proc. 16th APCC*, Auckland, New Zealand, Oct./Nov. 2010, pp. 441–446.

[6] K.-J. Song, C.-H. Lee, M.-S. Woo, and S.-G. Min, "Distributed periodic access scheme (DPAS) for the periodic safety messages in the IEEE 802.11p WAVE," in *Proc. 3rd Int. Conf. CMC*, Qingdao, China, Apr. 2011, pp. 465–468.

[7] H. Seo, S. Yun, and H. Kim, "Solving the coupon collector's problem for the safety beaconing in the IEEE 802.11p WAVE," in *Proc. IEEE VTC, Fall*, Ottawa, ON, Canada, Sep. 2010, pp. 1–6.

[8] S. Oh, M. Gruteser, and D. Pomili, "Coordination-free safety messages dissemination protocol for vehicular network," *IEEE Tran. Veh. Technol.*, 2013, to be published.

[9] K. A. Hafeez, L. Zhao, B. Ma, and J. W. Mark, "Performance analysis and enhancement of the DSRC for VANET's safety applications," *IEEE Tran. Veh. Technol.*, vol. 62, no. 7, pp. 3069–3083, Sep. 2013.
[10] J. L. Massey and P. Mathys, "The collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 2, pp. 192–204, Mar. 1985.
[11] I. Chlamtac and A. Faragó, "Making transmission schedules immune to topology changes in multi-hop packet radio networks," *IEEE/ACM Trans. Netw.*, vol. 2, no. 1, pp. 23–29, Feb. 1994.
[12] C. H. Rentel and T. Kunz, "MAC coding for QoS guarantees in multihop mobile wireless networks," in *Proc. 1st ACM Int. Workshop Q2SWinet*, 2005, pp. 39–46.
[13] F. Farnoud, B. Hassanabadi, and S. Valaee, "Message broadcast using optical orthogonal codes in vehicular communication systems," in *Proc. First Int. Workshop WiNITS*, 2007, pp. 1–6.
[14] F. Farnoud and S. Valaee, "Reliable broadcast of safety messages in vehicular ad hoc networks," in *Proc. IEEE INFOCOM*, Rio de Janeiro, Brazil, Apr. 2009, pp. 226–234.
[15] D. Kim, D. J. Esteki, Y.-C. Hu, and P. R. Kumar, "A lightweight deterministic MAC protocol using low cross-correlation sequences," in *Proc. IEEE GLOBECOM*, Houston, TX, USA, Dec. 2011, pp. 1–6.
[16] J.-H. Ju and V. O. K. Li, "An optimal topology-transparent scheduling method in multihop packet radio networks," *IEEE/ACM Trans. Networking*, vol. 6, no. 3, pp. 298–306, Jun. 1998.
[17] V. R. Syrotiuk, C. J. Colbourn, and A. C. H. Ling, "Topology-transparent scheduling for MANETs using orthogonal arrays," in *Proc. Joint Workshop Found. Mobile Comput. DIALM-POMC*, San Diego, CA, USA, Sep. 2003, pp. 43–49.
[18] A. Ebner, L. Wischhof, and H. Rohling, "Aspects of decentralized time synchronization in vehicular ad hoc networks," in *Proc. 1st Int. WIT*, Hamburg, Germany, 2004, pp. 67–72.
[19] M. Mustafa, M. Papatriantafilou, E. M. Schiller, and A. Tohidi, "Autonomous TDMA alignment for VANETs," in *Proc. IEEE VTC Fall*, Quebec City, QC, Canada, Sep. 2012, pp. 1–5.
[20] Y. Zhang, K. W. Shum, and W. S. Wong, "Strongly conflict-avoiding codes," *SIAM J. Discr. Math.*, vol. 25, no. 3, pp. 1035–1053, 2011.
[21] Y. Zhang, K. W. Shum, and W. S. Wong, "Completely irrepressible sequences for the asynchronous collision channel without feedback," *IEEE Trans. Vech. Tech.*, vol. 60, no. 4, pp. 1859–1866, May 2011.
[22] S. V. Bana and P. Varaiya, "Space division multiple access (SDMA) for robust ad hoc vehicle communication networks," in *Proc. IEEE Int. Transp. Syst. Conf.*, Oakland, CA, USA, Aug. 2001, pp. 962–967.
[23] W. S. Wong, "Transmission sequence design and allocation for wide area ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 63, no. 2, pp. 869–878, Feb. 2014.
[24] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against Sybil attack in vehicular ad hoc network based on roadside unit support," in *Proc. IEEE MILCOM*, Oct. 2009, pp. 1–7.
[25] S.-I. Sou and O. K. Tonguz, "Enhancing VANET connectivity through roadside units on highways," *IEEE Trans. Veh. Technol.*, vol. 60, no. 8, pp. 3586–3602, Oct. 2011.
[26] P. Mathys, "A class of codes for a T active users out of N multiple-access communication system," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1206–1219, Nov. 1990.
[27] O. Moreno, Z. Zhang, P. V. Kumar, and V. A. Zinoviev, "New constructions of optimal cyclically permutable constant weight codes," *IEEE Trans. Inf. Theory*, vol. 41, no. 2, pp. 448–455, Mar. 1995.
[28] 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.
[29] K. W. Shum and W. S. Wong, "Construction and applications of CRT sequences," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5780–5795, Nov. 2010.
[30] K. W. Shum, Y. Zhang, and W. S. Wong, "User-irrepressible sequences," in *Proc. 6th Int. Conf. SETA*, vol. 6338, *Lecture Notes in Computer Science*, C. Carlet and A. Pott, Eds., Sep. 2010, pp. 88–101.
[31] Y. Wu, K. W. Shum, W. S. Wong, Z. Lin, and L. Shen, "Protocol sequences for mobile ad hoc networks," in *Proc. IEEE INFOCOM*, Budapest, Hungary, Jun. 2013, pp. 323–328.
[32] W. C. Kwong and G.-C. Yang, *Optical Coding Theory With Prime*. Boca Raton, FL, USA: CRC, 2013.
[33] 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.
[34] G.-C. Yang and W. C. Kwong, "Performance analysis of optical CDMA with prime codes," *IEE Electron. Lett.*, vol. 31, no. 7, pp. 569–570, Mar. 1995.
[35] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*. New York, NY, USA: Springer-Verlag, 1990.
[36] G.-C. Yang and T. E. Fuja, "Optical orthogonal codes with unequal auto- and cross-correlation constraints," *IEEE Trans. Inf. Theory*, vol. 41, no. 1, pp. 96–106, Jan. 1995.

Yi Wu (M'07) received the B.Eng. degree in radio technology from Southeast University, Nanjing, China, in 1991; the M.S. degree in communications and information systems from Fuzhou University, Fuzhou, China, in 2004; and the Ph.D. degree in information and communication engineering from Southeast University, in 2013.

She is currently a Professor with the College of Photonic and Electronic Engineering, Fujian Normal University. Her research interests include vehicular ad hoc networks and communication protocols.

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

He is currently a Research Associate Professor with the Institute of Network Coding, The Chinese University of Hong Kong. He has been working on coding theory and its applications, including protocol sequences for multiple-access channels and network coding for distributed storage systems.

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

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

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

Lianfeng Shen (M'12) received the B.S. degree in radio technology and the M.S. degree in radio communications from Southeast University, Nanjing, China, in 1978 and 1982, respectively.

In March 1982, he joined the Department of Radio Engineering, Southeast University. From 1991 to 1993, he was a Visiting Scholar and a Consultant with the Hong Kong Productivity Council, working on wireless communication. In 1998, he was a Senior Consultant with the Telecom Technology Center of Hong Kong. Since 1997, he has been a Professor with the National Mobile Communications Research Laboratory, Southeast University. He has published ten books by Science Press and other presses in China. His current research interest includes broadband mobile communications, including wireless Internet, broadband wireless access systems, home networks, vehicular ad hoc networks, and communication protocols.

Mr. Shen is an Editor of the *Journal on Communication*.