Congruential Recursive Codes for Time Hopping Access in UltraWide Band Impulse Radio Systems

Enzo Baccarelli, Mauro Biagi, Cristian Pelizzoni, Nicola Cordeschi, Fabio Garzia
{enzobac, biagi, pelcris, cordeschi}@infocom.uniroma1.it, fabio.garzia@uniroma1.it *

ABSTRACT

In this contribution Time-Hopping (TH) codes are developed based upon the theory of congruences. These codes can be used for coherent multiuser asynchronous spread spectrum communication systems. They represent a compromise between Costas codes, which have nearly ideal auto-ambiguity properties, and congruential codes presenting nearly ideal cross-properties. The presented code applied not in ranging applications but communications system presents good performance in terms of Bit Error Rate (BER) for UltraWide Band Impulse Radio (UWB-IR) systems. Examples of typical auto- and cross-ambiguity functions are given to illustrate the performance of the presented codes jointly with BER evaluation.

Categories and Subject Descriptors

H.1 [**Models and Principles**]: Systems and Information Theory

General Terms

Algorithms, Theory.

Keywords

Access Codes, CDMA, UWB-IR, Theory of Congruences.

1. ADDRESSED PROBLEM

UltraWide Band Impulse Radio (UWB-IR) networks, often use time-hopping access codes. Since distance ranging or high target resolution is virtually always desired specially in signals of very short duration and these signals must be chosen in such a way that their auto-correlation functions exhibit a narrow mainlobe and adequately small sidelobes; these pulses compression features are necessary to determine precisely the time of arrival of the received signal. When either or all of the transmitter, target, or receiver is in motion, these properties should extend to the ambiguity function for the signal set considered. In particular, one would like the auto-ambiguity function to assume the ideal "thumb tack" shape required to perform reliable target and/or channel scattering function measurements [10]. A situation very similar is present in asynchronous spread spectrum communications when interference occurs between two or more of the signals (codewords) considered. These interference problems are typical of such multiuser environments. To achieve jamming resistance or low probability of intercept, it is necessary to use a sequence of time-hop codes with small cross-correlation functions between any two elements of the sequence: as the exact time of arrival of the received signal is unknown a priori, this property is required to minimize the output of the matched filter for the correct signal in cases where spurious codes are present within the received signal. Simultaneously good auto-ambiguity functions and small mutual cross-ambiguity functions is therefore well motivated. Unfortunately, there seems to be qualitative evidence in the literature that a tradeoff is involved between these two entities. On the one hand, time hop pulse trains based upon Costas arrays [3], such as Welch-Costas codes [3,4], are known to have nearly ideal auto-ambiguity functions but, even in the best cases, not very good cross-ambiguity properties [12]. Furthermore, for any given Costas set, the behavior of the cross-ambiguity function between two elements is heavily dependent on the pair of codes considered, which makes it necessary to find a "good" pair of codes if one is to use the class of Costas codes in practical multiuser situations. Here we consider the application form a communication point of view and in particular an approach suitable for multi user scenario.

*Mauro Biagi, Enzo Baccarelli, Cristian Pelizzoni, Nicola Cordeschi and Fabio Garzia are with INFO-COM Dept., University of Rome "La Sapienza", via Eudossiana 18, 00184 Rome, Italy. Ph. no. +39 06 44585471 FAX no. +39 06 4873330. This work is partially supported by Italian National project Wireless 8O2.16 Multi-antenna mEsh Networks (WOMEN) under grant number 2005093248.

IWCMC'06, July 3–6, 2006, Vancouver, British Columbia, Canada.

2. TIME HOPPING ACCESS SCHEMES FOR UWB-IR

Time-hopping coding is mandatory when a wireless service allowing access to multiple user is offered and privacy of contents must be assured. In UWB-IR systems each user emits pulse signals based on Pulse Position Modulation (PPM) format since this approach allow the user to exploit all the potentials of this technology for detection end positioning. Let us consider a pulse $s(t)$ with a pulse duration

equal to T_s and we consider Gaussian pulse according to the approach pursued in [3]. At this stage we are only interested in considering collision events so considerations about performance and pulse shaping are made in the following sections. Obviously, not only the UWB pulse shape choice is critical but also other system parameters as, in example, the pulse duration T_s that reduces (or increases) the user rate [2]. So, we have that the pulse $s_j(t)$ transmitted by user j is defined over a single time frame T_f as in

$$s_j(t) \doteq w(t - c_j T_h - b^{(j)}\Delta) \quad 0 \le t \le T_f, \quad 0 \le j \le N-1, \quad (1)$$

where T_h is the time slot dedicated to each user (for transmission/reception) and $b^{(j)}\Delta$ is the 2-PPM time shift carrying modulated bit information. The term c_j dictates the slot position in the frame and it falls in one slot's interval [0,N-1] and the value assumed by c_j is generated according to the random Time Hopping code. In order to explain better, we have to specify that the employed time-hopping codes belong to a set of families of codes that assure random access. In particular a lot of study are devoted to avoid periodicity effects in these codes in order to guarantee pure random access so to assure security in communications. At the receiver, the signal transmitted in the 0-th transmission slot has to be received in the 0-th receiving slot so we have for the analog received signal $r(t)$ the following expression

$$r(t) = \sqrt{\varepsilon_0} w(t - c_0 T_h - b^{(0)}\Delta - \tau_{p0}) +$$

$$+ \sum_{m=-M}^{0} \sum_{j=1}^{N} \sqrt{\varepsilon_j} w(t - c_j T_h - b^{(j)}\Delta - \tau_{pj} - mT_f) + n(t), \quad (2)$$

where $\sqrt{\varepsilon_j}$ takes into account for the received energy by j-th transmitter (different from the transmitted due to possible fading effects), $\tau_{pj} = d_j/c$ takes into account for the propagation delay given by the ratio between the distance from the transmitter to the receiver and the light speed c. Finally the parameter m in (2) accounts for the chance that a pulse may collide more than one frame after its transmission (from M frames before to the actual one), so M that is the maximum number of previous frames allowing possible collisions and it may be evaluated as [2]

$$\mathrm{M} \triangleq \left\lceil \frac{d_{\max}}{c} \bmod T_f \right\rceil = \left\lceil \frac{d_{\max}}{c} \bmod (N+1)T_h \right\rceil . \quad (3)$$

3. CONGRUENTIAL CODING FOR IMPULSE RADIO UWB SYSTEMS

Although congruential coding is known in literature, its application to communication problems is limited to very few works, in fact the main application deals with radio detection and raging problems. According to [10], let us consider a frame of length T_f seconds, divided into N equal segments of length T_h seconds. For sake of simplicity N is restricted to be an odd prime; from a practical point of view, this condition induces little loss of generality. The slot assigned within the frame to user k is given by the following expression

$$y_k = \left[a\frac{k(k+1)}{2} \right]_N . \quad (4)$$

The class of extended quadratic congruence placement operators should be read, "y is congruent to x, modulo N". Since N is assumed to be an odd prime, J_N forms an Abelian group under multiplication modulo N; hence, $\underline{J}_N = J_N + \{0\} = \{0, 1, ..., N-1\}$ forms a finite field of order N. The parameter a use useful to change the configuration of slot assignments (possibly after N frames). This parameter will be present also in the proposed scheme and its importance become more clear. At this stage we can affirm that it can be used to change configuration (this does not avoid collision). It is important to note the symmetry with respect to the center of the arrays, which demonstrates that the placement operator of [11] induces a many-to-one correspondence over J_N .
In fact in Fig.1 the diagram describing the slots assigned by congruential code for each user is reported. This diagram has to be described in the following way.

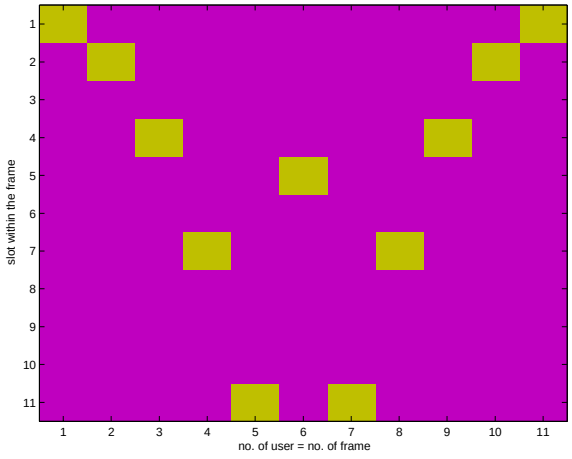

Figure 1: Access codes partitioning according to [10] with N=11 a=1

First, the user k *mod* N from the algorithm receive the number of the slot it has to transmit in and, at the next frame, it has to considered itself as the user number $(k+1)$ *mod* N so the diagram can be interpreted as the slot assigned at each user when the number of frame, in the abscissa, increases. Second it can be interpreted as the slots assigned at each user in the current frame. By observing Fig.1 we can appreciate (a=1, N=11) that users labelled as 1, 2, 3, 4, 5 encounter collisions with 11, 10, 9, 8, 7 so the only user free from collision is the number 6.

In Fig.2 a new diagram for (a=4, N=11) is reported and also in this case hits occur.

The user involved in collisions are the same of the above example, in fact users 1, 2, 3, 4, 5 collide with users 11, 10, 9, 8, 7. This can be interpreted in the following way. Each user encounter collision during the transmission except the user number 6, this means that the user labelled as 1 suffer from collisions till it will be the 6th and the collision restart. This lead to the conclusion that, from a collision point of view the scheme in [10] is inefficient and some slots remain unassigned.

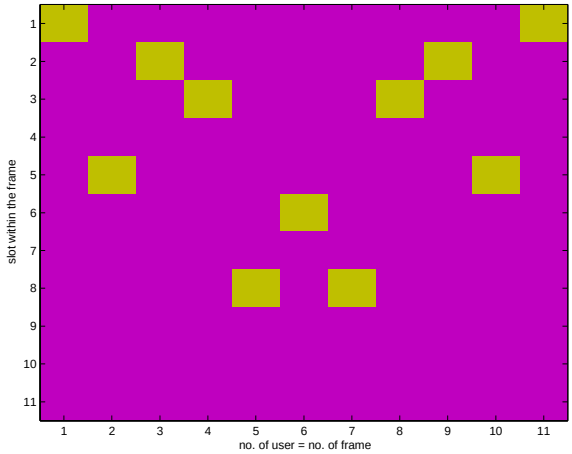

Figure 2: Access codes partitioning according to [10] with N=11 a=4

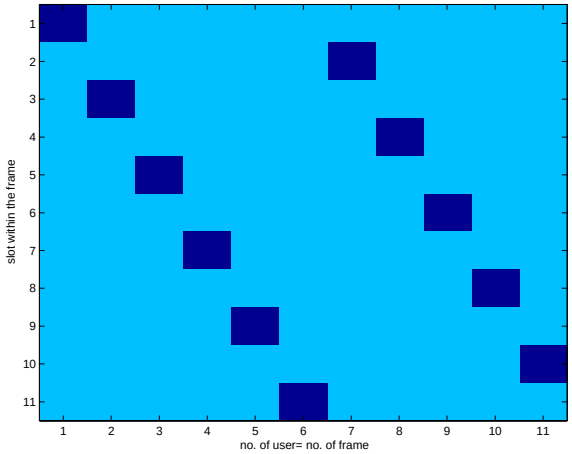

Figure 3: Access codes partitioning according to the proposed scheme with N=11 a=1

3.1 Proposed Recursive Congruential TH scheme

The proposed scheme is based on congruence property and in particular by starting form the following definition

$$y_k = \left((ak^{(N-1)} + 1)k \ mod \ N\right). \tag{5}$$

where "a" as previously mentioned is an integer number able to change the slot allocation as for the codes in [10]. Now, we have that the computational cost is higher than the previous one, but it is bounded under that of pseudo-noise usually adopted. Now, by considering the diagram of Fig.3 (a=1, N=11) it is possible to appreciate that the time slots assigned according to the above congruential relationship, do not incur in collision and this is the optimal behavior for such a code because it efficiently occupies all the time slot so each column and row presents only one occupied slot. This property is fundamental because by avoiding multi-access interference, it is possible, for the receiver, to proceed with standard reception techniques (i.e., matched filtering) without take care of multi-user interference suppression issues [1]. Obviously in the presence of InterSymbol Interference (ISI) or delay spread the matched filter results to be no more optimal. When we consider a different values for a (e.g. $a = 4$), we hold the property that no collisions occur (see Fig.4) so the diagram presents, as in the previous case, one-to-one correspondence between users (or frame) and assigned slot. As additional consideration to be carried out, we note that a possible way for hold the wireless channel secure from undesired detection, after a frame $T_f = N^2 T_h$ the parameter a can be changed according to a congruential relationship so

$$a = \left((bk^{(N-1)} + 1)k \ mod \ L\right) \tag{6}$$

where b is an integer and L integer. This suggests that this kind of approach can be adopted recursively because it can be organized in frame, super-frame and so on.

Remark - about secureness about secureness of the recursive policy

This scheme can be employed in order to guarantee secureness to the access and privacy in data transmission/reception. The Access Point (or Base Station) can decide the degree of privacy P by adding additional congruencial relationships (in the previous case the level is $P = 2$) so, from a the point of view of a user that wants to violate other user communications, the number of parameters to be estimated are $2P$ because for each relationship the parameter of modulo operation (i.e., N) and multiplicative factor (i.e., a), should be cracked. ■

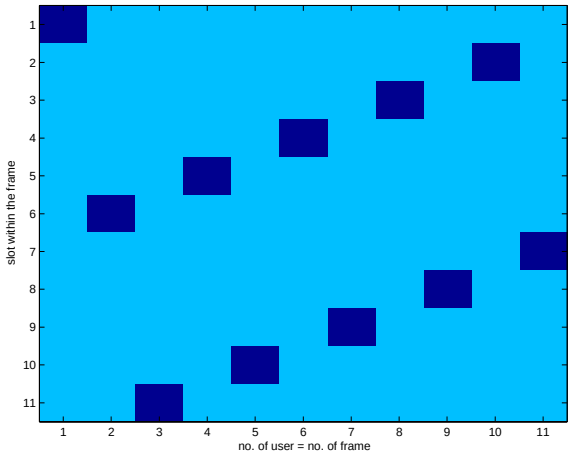

Figure 4: Access codes partitioning according to the proposed scheme with N=11 a=4

Before to proceed, some points should be carried out.

First the proposed approach is computationally not expensive if compared with algorithms for random number generators (i.e., Box-Muller method), second the proposed algorithm (as for the one proposed in [10]) present very low computational cost because only power of integer number are present jointly with modulo ones.

4. PERFORMANCE AND CONCLUSIONS

Usually, access coding performances are compared by considering computational cost of the algorithm generating codewords as previously mentioned and detailed, the number of collisions that induce multi-access interference and Bit Error Rate (BER) degradations and last, the auto- and cross-ambiguity properties of the considered codewords. By considering the ambiguity function defined as

$$A(\tau;k) = \int_{-\infty}^{\infty} \sum_{m=0}^{N-1} \sum_{l=0}^{N-1} s_m(t+\tau) s_l(t) e^{-jkt} \qquad (7)$$

where the term s_m is the generic UWB-IR signals given by eq. (1) we have that it depends jointly on the the number that identifies the user in the frame and on the delay[1] τ. By observing the cross-ambiguity function shown in Fig.5 for the scheme of [10] and the scheme proposed here, it is possible to see that the scheme in [10] presents better performances (for sake simplicity represented as a function of sample time) with respect to the proposed scheme. In fact, the dashed plot presents more peaks than the continuous one and in particular it assumes a triangular shape so ambiguity is heavily sensible to delays τ. This is the drawback of the proposed approach but this does not represent severe limitations because the problem of ambiguity is not so heavy in UWB-IR systems, as in systems devoted *only* to detection and ranging. In fact, although we show the performance for ambiguity features, our main interest is focused on error rate. Furthermore, we recall that modulation format is based on pulse position so when a synchronization error incurs not only access is compromised but also detection within the correct slot. In detail, the correct timing procedure is mandatory for an orthogonal pulse position modulation because if synchronization is not assured we can decide for a bad symbol in place of the correct one. So without considering any access procedure, attention should be paid to synchronization and this means that the proposed scheme does not require additional feature or requirements for a correct timing acquisition technique.

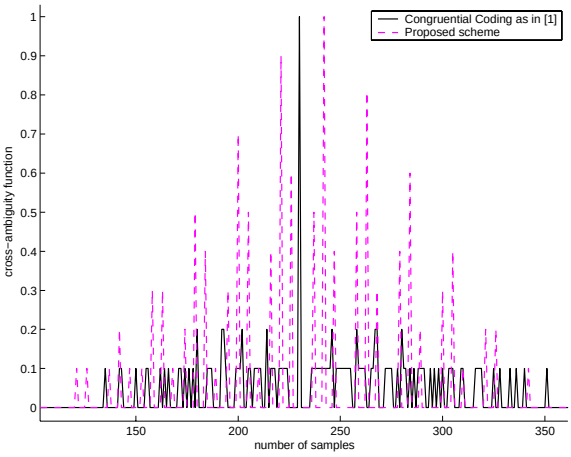

Figure 5: Access codes partitioning according to the proposed scheme with N=11 a=4.

In Fig.6 the auto-ambiguity function is shown and in this case the behavior is the opposite with respect to cross-ambiguity. In fact, in this case the proposed scheme presents ambiguity values (dashed line) lower than those of the above mentioned approach presented also in [10] (continuous line) and once more we recall here that the ambiguity problem can be solved by accurate synchronization phase, required also in the scheme in [10] when applied to signal detection for Orthogonal Pulse Position Modulation as for UltraWide Band Impulse Radio systems.

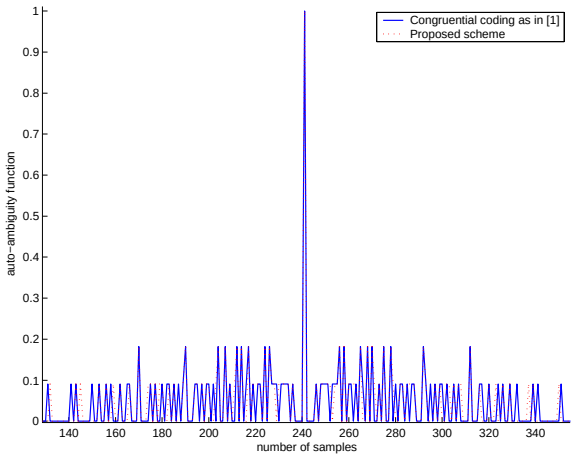

Figure 6: Access codes partitioning according to the proposed scheme with N=11 a=4

From a communication point of view, after evaluating ambiguity and computational cost for system with pulses of the order of nanoseconds, the benchmark is represented by the error rate because error in reception means data retransmission or more complex channel coding techniques. So, the effect of collision avoidance in the slot allocation becomes more evident.

By looking at Fig.7, where performance in terms of error probability are reported for a delay spreaded UWB-IR indoor channel, we proceed with performance comparisons between the proposed scheme and that in [10], by considering an increasing value of emitted power ranging from 0 to $100\mu W$ and channel delay spread values from 0 (ideal channel) to 2.5 times the signalling period. By observing the 3D-plot, it is possible to appreciate that the average error probability is higher when a coding approach as in [10] is considered and this is essentially due to the presence of multi user interference that, in the proposed scheme, is by fact absent. So, in detail when we increase node transmit power the error rate decrease for an assigned value of delay

[1]Note that the parameter τ is not equal the delay spread.

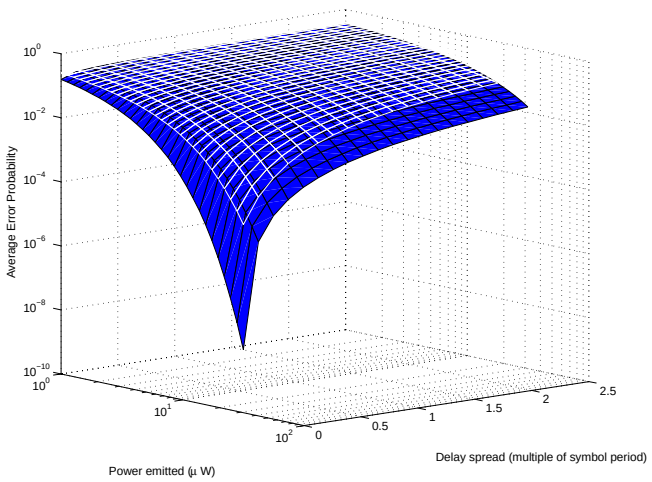

Figure 7: Access codes partitioning according to the proposed scheme with N=11 a=4

spread (see [8-11]) the error probability decreases faster in the proposed approach than in that in [10]. By considering a fixed level of transmit power the error probability increases by increasing the delay spread as obvious since the receiver is simply based on matched filtering technique. It is fundamental to observe that we represent a real case when severe multipath is present so when we increase delay spread, this last induces severe performance degradations. By considering the section obtained for the 3D buy fixing values of delay spread close to 0 it is possible to see the gain offered, with respect to multi-user interference, by the proposed scheme.

4.1 Conclusions

The proposed scheme presents less computational cost than pseudo-noise time hopping codes and, with respect to approaches [10] based on congruences it is not able to outperform it form target detection point of view (e.g. cross-ambiguity function) but it largely outperforms the solution in [10] from an error rate point of view in the presence of delay spread channel and also when ideal channel, with the only presence of multi-user interference, is considered. In addition the proposed technique is suitable for data protection from a privacy point of view with a tunable level of privacy P. Future works will deal with codes based only in part with pseudo-noise schemes by trying to merge them with the ones here presented.

5. REFERENCES

[1] E. Baccarelli and M. Biagi. A simple adaptive coding scheme for multiuser interference suppression in ultra-wideband radio transmissions. *IEEE Trans. on Communications*, 53(8):1283–1287, August 2005.

[2] M. Biagi, C. Pelizzoni, N. Cordeschi, and E.Baccarelli. Performance analysis of impulse-radio uwb networks impaired by multiple access interference. In *Networking with UltraWide Band, NEUWB2 2005*, pages 45–49.

[3] J. Costas. A study of a class of detection waveforms having nearly ideal range-doppler ambiguity properties. *Proceedings of the IEEE*, 72(8):996–1009, August 1984.

[4] R. Fleming, C. Kushner, G. Roberts, and U. Nandiwiada. Rapid acquisition for ultra-wideband localizers. In *IEEE Proc. Conf. UWB Syst. Techn. 2002*, pages 245–250.

[5] J. Foerster. The effects of multipath interference on the performance of uwb systems in an indoor wireless channel. In *Vehicular Technology Conference*, pages 1176–1180.

[6] S. Golomb. Algebraic costructions for costas arrays. *Journal of Combinatorial Theory*, ser A37(1):13–21, January 1984.

[7] A. Saleh and R. Valezuela. A statistical model for indoor multipath propagation. *IEEE Journal of Selected Areas in Communications*, 2(5):128–137, February 1987.

[8] H. T. S.W. Golomb. Constructions and properties of costas arrays. *Proceedings of the IEEE*, 72(9):1143–1163, September 1984.

[9] E. Titlebaum. Time-frequency hop signals part 1:coding based upon the theory of linear congruences. *IEEE Transactions on Aerospace arid Electronic Systems*, aes17(4):490–493, July 1981.

[10] E. Titlebaum, S. Maric, and J. Bellegarda. Ambiguity properties of quadratic congruential coding. *IEEE Transactions on Aerospace and Electronic Systems*, 27(1):18–29, January 1991.

[11] E. Titlebaum and L. Sibul. Time-frequency hop signals part 2:coding based upon the theory of linear congruences. *IEEE Transactions on Aerospace arid Electronic Systems*, aes17(4):494–499, July 1981.

[12] M. Win and R.A.Sholtz. Ultra-wide bandwidth time-hopping spread-spectrum impulse radio for wireless multiple-access communications communications. *IEEE Transactions on Communications*, 48(4):679–689, April 2000.

[13] M. Win and R. Scholtz. Characterization of uwb wireless indoor channels: a communication-theoretic view. *IEEE Journal of Selected Areas in Communications*, 12(12):1613–1627, December 2002.