DS-SS with de Bruijn Sequences for Secure Inter Satellite Links

Susanna Spinsante
Department of Information Engineering
Marche Polytechnic University
Ancona, Italy I-60131
s.spinsante@univpm.it

Chirag Warty
IEEE Associate Member
Ahilya Technologies
Los Angeles, CA
chiragwarty@ieee.org

Ennio Gambi
Department of Information Engineering
Marche Polytechnic University
Ancona, Italy I-60131
e.gambi@univpm.it

Abstract—Today, both the military and commercial sectors are placing an increased emphasis on global communications. This has prompted the development of several Low Earth Orbit satellite systems that promise a worldwide connectivity and real-time voice, data and video communications. Constellations that avoid repeated uplink and downlink work by exploiting Inter Satellite Links have proved to be very economical in space routing. However, traditionally Inter Satellite Links were considered to be out of reach for any malicious activity and thus little, or no security was employed. This paper proposes a secured Inter Satellite Links based network, built upon the adoption of the Direct Sequence Spread Spectrum technique, with binary de Bruijn sequences used as spreading codes. Selected sequences from the de Bruijn family may be used over directional spot beams. The main intent of the paper is to propose a secure and robust communication link for the next generation of satellite communications, relying on a classical spread spectrum approach employing innovative sequences.

TABLE OF CONTENTS
1 INTRODUCTION .................................................. 1
2 constellation design ............................................ 1
3 satellite link .................................................... 3
4 de bruijn sequences ............................................ 3
5 system design .................................................... 6
6 preliminary evaluation ........................................ 6
7 conclusion ....................................................... 7
REFERENCES ...................................................... 7
BIOGRAPHY .......................................................... 8

1. Introduction
Message routing on ground may be efficiently managed through several strategies available for optimizing the path between source and destination; but routing in space needs a very precise calculation of path length and resource allocation. Future space network architecture is envisioned to be widely distributed, independent and to some degree intelligent in its operation. The development of a satellite cluster system that supports an inter-satellite communication makes possible the execution of a complex communication environment designed to minimize space-ground-space communication jumps, and enables Geosynchronous Earth Orbit (GEO) to Low Earth Orbit (LEO), and GEO to Unmanned Aerial Vehicles (UAV) space links. The economic benefits of such a network in space far outweigh the technological challenges. Inter Satellite Link (ISL) enhances system reliability, capacity and reduces the number of gateways required. By eliminating the dependency on ground infrastucture for traffic links, ISL-based systems can become more autonomous. Moreover, ISL can make communications virtually unaffected by terrestrial service disruptions that may be caused by earthquakes, hurricanes, floods and other natural and man-made causes. Here we study the performance of the satellite cross link using de Bruijn sequences for spread spectrum transmission, which can be further enhanced by deploying directional spot beam antennas on board the space nodes.

Two basic designs are considered, the former consisting of a network of similar constellation satellites with predictable in-space trajectories and pre-determined orbits (static constellation). The second model will consist of satellite networks combined with other heterogeneous space platforms like commercial and military planes, UAVs, etc. Like a handshake in space, crosslinks provide rapid, ultra-secure communications by enabling the satellites to pass signals to one another, while requiring only one ground station on friendly soil. Some of the current satellite constellations use L-band to communicate between the space and ground terminals based on a hybrid Frequency Division Multiple Access (FDMA/TDMA) scheme, using a 90 millisecond Time Division Duplex (TDD) frame. Each frame is composed by 2250 symbols of channel bursts at a modulation rate of 25 kilo/symbols per second (kps). However, Ka-Band and V-band are used as the operating frequency bands for in-space communications, with modulation techniques as basic as Binary Phase Shift Keying (BPSK) and Quadrature Phase Shift Keying (QPSK). These elementary communication techniques make the space segment very vulnerable to eavesdropping and jamming by malicious entities. The simulation model considers the link to operate at the currently used Ka-band (23 GHz) and V-band (60 GHz). Consequently, the theoretical model is developed to analyze characteristics and performance of Inter-satellite links using de Bruijn sequences for spread spectrum links in satellite networks.

The remainder of the paper is organized as follows: constellation design for the predictable and dynamic network topology is presented in Section 2. In space inter-satellite links are described in Section 3. The characteristics of de Bruijn sequences and their cardinality and correlation properties are presented in Section 4. An overall integrated system design is proposed in Section 5, and in Section 6 the simulated performance of the link are discussed.

2. Constellation Design
Routing among satellites and space platforms is accomplished by relaying packets by using intermediate satellites as relays. It has long been realized that the LEO satellite constellations using intersatellite links can provide global coverage,
while offering real-time communication services between end-users. The communication system is affected mainly by the choice of design factors like constellation design, altitude, power, routing method, satellite cross link design, etc. [1, 2]. There are two major types of constellations: polar and Walker. Both constellations are designed to provide the most efficient global coverage by using the minimum number of satellites, and each has its own advantages and disadvantages. A polar constellation provides coverage for the entire globe, including the poles, while a Walker constellation only covers a certain latitude (between $+/- 70^\circ$). With the same number of satellites, a Walker constellation can therefore provide a higher diversity than a polar constellation. The satellite constellation is made up of predetermined number of satellites in prescribed orbits to provide global coverage with minimum time delay. In this paper we examine satellite cross-links with time-dependent Doppler variation, keeping other parameters constant. Space based platforms can be characterized in the two main categories: satellites [3], with fixed orbit and predictable trajectory, non-satellites [4], i.e. platforms with unpredictable path and dynamic trajectory.

Routing in Predictable Network Topology

The choice of relay and cross-links has a determining effect on the performance of space based communication system, affecting the time delay and the quality of service (QoS). In the case of satellites, the orbits and the positions are known to every member in the constellation. This allows the source node to predict the neighboring nodes that can be utilized as relays. Here we consider a polar orbit where all satellites are rotating in the same direction. The movement of the satellites can be broken down into two segments, one going from north to south and the second from south to north.

Among the commercial satellite systems designed or operated in time, only a few were supposed to provide ISLs:

- Iridium: RF ISL, in the band: 22.55 - 23.55 GHz, providing 25 Mbps data rate. There are 4 ISLs per satellite: 2 intra plane, and 2 inter plane;
- Orblink: RF ISL, in the band: 65.0 - 71.0 GHz, providing 15 Gbps data rate, with 2 ISLs per satellite, both intra plane;
- Teledesic: RF ISL at 60 GHz, with 155 Mbps data rate and 8 ISLs per satellite, featuring permanent and dynamics links.

Among the systems cited above, only Iridium was deployed and is currently operational. Each satellite node is assumed to maintain four ISL cross links, with intra plane links maintained constantly and inter plane links managed dynamically, as the satellite transcends its orbital path. In the case of Iridium, constellation nodes located in planes 1 and 6 can maintain only three connections, two of which are intra plane. The nodes in the boundary planes do not establish cross links between each other due to rapid angular velocity changes that occur between satellites in counter rotating planes. The satellites are considered to be in six orbital planes separated by 31.6 degree at an altitude of 780km (LEO) and 86.4 degree inclination. Due to the inherent nature of the cross links they can be modeled as time varying in a deterministic manner, depending on the relative motion of the satellites. Here we consider the time varying free space loss contribution, as one of the significant parameter affecting the link performance. For cross links between two satellites in a LEO orbit it is reasonable to consider a flat Earth model to simulate in space routing, as shown in Fig. 2. From such a model, the position of satellite in Cartesian coordinate system can be given as:

$$\begin{align*}
(x_1(t), y_1(t)) &= (v_1 \cdot \cos \theta_1, v_1 \cdot \sin \theta_1) \quad (1) \\
(x_2(t), y_2(t)) &= (v_2 \cdot (t - t_0) \cos \theta_2, v_2 \cdot (t - t_0) \sin \theta_2) \quad (2)
\end{align*}$$

where $t_0$ is the time taken by the second satellite to cross the track of the first satellite. In the model, $\Delta h$ is assumed to be the vertical (z-axis) separation between the satellites. As a result, the ISL distance is given by:

$$L(t) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2} \quad (3)$$

From previous equations, the above definition can be expressed as:

$$L^2(t) = t^2[v_1^2 + v_2^2 + 2v_1 \cdot v_2 \cdot \cos(\theta_1 - \theta_2)] + 2v_2t_0[v_1 \cdot \cos(\theta_1 - \theta_2) - v_2] + v_2^2t_0^2 + \Delta h^2$$

Since the ISL is time varying, the ISL distance dependency on time can be given as a reduced form of the previous equation:

$$L^2(t) = a_L t^2 + b_L t + c_L \quad (4)$$

Thus, the received signal power on the ISL cross link can be said to be: $P_R(t) = \left( EIRP \cdot G_R / L^2(t) \right) \cdot (\lambda/4\pi)^2$, which can be further generalized for Free Space Path Loss (FSPL) as: $FSPL(t)_{dB} = 32.44 + 20 \log_{10} L(t)_{km} + 20 \log_{10} f_{MHz}$, where, due to the time varying nature of the cross link, even the EIRP could be considered time dependent as well.

Routing in Dynamic Network Topology

The cross link works well if the receiver is in the 3dB cone width of the transmitted beam, but as the node travels towards

![Figure 1. Inter Satellite Link network in space](image1)

![Figure 2. Geometrical model for the LEO ISL](image2)
Figure 3. Spot beam coverage and overlapping region for handoff

the edge of the cone there is significant signal deterioration due to delay and Doppler phenomenon. To enable a connection between nodes with dynamic path and irregular trajectory, a search needs to be done for periods during which the variation in azimuth over time is small. To find these periods of small variations derivatives of azimuth angles are computed [5]. These are the optimal time periods for establishing a cross-link between the satellite and an independent node. Since the direction of travel of the node relative to satellite plays a significant role in affecting the link quality, a soft handoff scheme should be in place to ensure a seamless end-to-end data transfer, as shown in Fig. 3. The geometry of such network will need to have overlapping coverage regions. GEO or MEO backbone architecture would be more suitable than LEO network. A system with backbone can be expressed as a function of coverage and number of apertures available for cross-link:

\[ a_j = \frac{u}{v} \left( \int_{c_j} \frac{1}{i} dV \right) \]  

where \( a_j \) is the number of apertures that backbone satellite \( j \) must carry, \( c_j \) is \( j \)'s coverage region, \( i \) is the level of coverage experienced by \( dV \), \( u \) is the total number of user nodes, and \( v \) is the total volume of space of possible user locations. The technical details of this type of topology are beyond the scope of this paper, however the de Bruijn sequences proposed in the next section can be implemented on any cross-links, irrespective of the topology.

3. INTER SATELLITE LINK

Inter-satellite link is the network architecture that was first successfully employed by Motorola in the form of Iridium satellite network. In the network with ISL capability the satellites can talk not only to the ground station and gateways, but also to each other, forming a network in space. When a signal is up-linked to a satellite the information is passed through the network of satellites to the one that is immediately over the destination gateway. This scheme allows nodes to talk to each other without ever referencing to any ground stations at all, thereby reducing signal latency that can adversely affect time-sensitive protocols such as TCP/IP. In this paper the model assumes that satellites in the constellation travel in straight lines, with a given height difference and trajectories, as illustrated in Fig. 1. The first satellite crosses the track of the second satellite at time \( t = 0 \), which results in the local coordinate system shown in Fig. 2.

ISLs are links established between satellites in the same plane (intra-plane) and between satellites in adjacent planes (inter-plane). Intra-plane links are maintained permanently, with each satellite having forward and backward connectivity with the satellites directly in front and behind. Inter-plane links are dynamically established and terminated as the satellite transends its orbital path. Except for the satellites in counter-rotating planes one and six, each satellite has four ISLs. The satellites located within planes one and six maintain only three ISLs each, two of which are intra-plane [6]. The horizontal pointing angle between two satellites in adjacent orbital planes, using a reference of zero degrees parallel to the equator, varies by approximately ±65 degrees over one orbital period. This angle varies most slowly over the equator where satellites in adjacent orbits are the most separated, and it varies most rapidly over the poles where the orbits cross. A nominal horizontal azimuth of ±45 to 50 degrees with an antenna steerable over a 30 to 45 degree range is sufficient to maintain inter-orbital links between latitudes of 50 to 60 degrees north and south. Efficient link assignment and routing algorithms can optimize network delay and decrease overhead [6].

4. DE BRUIJN SEQUENCES

Binary de Bruijn sequences [7] are a special class of nonlinear shift register sequences with maximal period \( N = 2^n \): \( n \) is called the span of the sequence, i.e. the sequence may be generated by an \( n \)-stage shift register. In the binary case, the total number of distinct sequences of span \( n \) is \( 2^{2^n-n} \), in the more general case of span \( n \) sequences over an alphabet of cardinality \( \alpha \), the number of distinct sequences is \( \alpha!\alpha^{(n-1)}/\alpha^n \). In this paper we refer to binary de Bruijn sequences. The states \( \{S_0, S_1, \ldots, S_{N-1}\} \) of a span \( n \) de Bruijn sequence are exactly all the possible \( 2^n \) different binary \( n \)-tuples; when viewed cyclically, a de Bruijn sequence of length \( 2^n \) contains each binary \( n \)-tuple exactly once over a period, even the all-zero \( n \)-tuple. This is the reason why de Bruijn binary sequences may not be generated by means of classical and well-known Linear Feedback Shift Registers (LFSR).

Cardinality and generation issues

The length of a de Bruijn sequence (i.e. a maximal length sequence) is always an even number. To compare the total number of de Bruijn sequences of length \( N \), and the total number of available m-sequences, or Gold sequences, at a parity of \( n \), similar but not identical length values shall be considered. As an example, for a value of the span \( n \) equal to 7 (i.e. binary sequences of length 128), there are \( 2^{57} \) different sequences; if \( n \) increases up to 10, the number of sequences grows up to \( 2^{502} \). The huge cardinality of the de Bruijn sequences set makes the task of identifying a specific sequence extremely complex to execute, also depending on the specific application.

Pseudorandom numbers and generators are used in a wide set of applications, such as the generation of spreading codes for Code Division Multiple Access schemes (CDMA), and cryptography. One of the most adopted technique for generating pseudorandom numbers relies on LFSRs, as they permit an efficient implementation of a deterministic random behavior. A single LFSR allows one to generate m-sequences; two LFSRs may be adopted to generate Gold and Kasami sequences, also useful in CDMA. However, the main drawback in LFSRs is the predictability of the output.
sequence, and the relatively small number of sequences that may be generated. Non linear FSR (NFSR) are derived from LFSRs, where the linear feedback part is generalized to a nonlinear behavior. NFSRs may generate maximum length sequences (as de Bruijn ones), that can even be used to design binary sequences with negative autocorrelation values, for asynchronous Direct Sequence (DS) CDMA, as discussed in [8]. Binary NFSR sequences may be generated by 2-value nonlinear feedback shift register with \( n \) memory cells, as shown in Fig. 4.

The register may be in a given state at a time \( t = 0, 1, \ldots \) described by: \( \mathbf{a}(t) = (a_1(t), a_2(t), \ldots, a_n(t)) \) where \( a_i(t) \in A = \{0, 1\} \), for \( i = 1, 2, \ldots, n \). At each clock transition, the content of each memory cell is shifted one position to the right, and the leftmost cell \( a_n(t) \) is updated by the output of the nonlinear feedback function \( g(\cdot) \), that defines a mapping of \( A^n \rightarrow A \). At instant \( (t+1) \), the state of each register cell is derived as:

\[
a_i(t+1) = \begin{cases} a_{i+1}(t) & \text{for } i = 1, 2, \ldots, n-1, \\ g(\mathbf{a}(t)) & \text{for } i = n \\
\end{cases}
\]

NFSRs can generate binary sequences with maximum length \( 2^n \) states, including all-zero state of \( n \) memory cells, as de Bruijn sequences.

**Correlation properties**

Auto- and cross-correlation properties of the sequences affect the selection of the spreading codes to use. The former affects the effectiveness of the single-user information extraction process, whereas the latter influences the global performance of the multiuser communication system, in terms of Multiple User Interference (MUI). The autocorrelation \( \theta(k) \) of a binary de Bruijn sequence \( \mathbf{c} = (c_0, c_1, \ldots, c_{N-1}) \) of length \( N = 2^n \), that is defined as \( \theta(k) = \sum_{i=0}^{N-1} c_i c_{i+k} \), for a given shift \( k \), may assume only a set of given values:

\[
\theta(k) = \begin{cases} 2^n & \text{for } k = 0, \\ 0 & \text{for } 1 \leq |k| \leq n - 1 \\
\end{cases}
\]

and \( \theta(k) \neq 0 \), for \( |k| = n \).

As long as the span of the sequence increases, the amount of values \( k \) for which the autocorrelation sidelobes (i.e. the values assumed by \( \theta(k) \) for \( k \neq 0 \)) are zero also increases. It is also known that \( \theta(k) \equiv 0 \) mod 4, for all \( k \), for any binary sequence of period \( N = 2^n \), with \( n \geq 2 \). In a binary de Bruijn sequence the number of 1’s equals the number of 0’s:

\[
\begin{array}{cccccccccc}
1 & 4 & 7 & 10 & 13 & 16 & 19 & 22 & 25 & 28 & 31 \\
\end{array}
\]

Fig. 4. 2-valued NFSR of \( n \) memory blocks and feedback function

As a consequence, any binary de Bruijn sequence in a bipolar form has a null average autocorrelation.

Fig. 5 shows the average normalized autocorrelation profile computed over all the 2048 binary de Bruijn sequences of length 32. With the exception of the peak value at \( k = 0 \), the autocorrelation profile is symmetric with respect to the central value of the shift, \( k = 16 \). A general property states that \( \theta(k) = \theta(N-k) \), for \( 0 \leq k \leq N-1 \). As \( n \) increases, the autocorrelation profiles of the de Bruijn sequences will show many samples equal to 0, a symmetric distribution of the samples, and a reduced number of different positive and negative samples, as to give an average autocorrelation equal to 0.

The autocorrelation profiles of all the 2048 binary de Bruijn sequences of length 32, shown in Fig. 6 (peaks removed), confirm the symmetric distribution of the null values. The first \((n-1)\) samples adjacent to the peak located at \( k = 0 \), are always equal to 0, as discussed above. This is an important feature to improve the detection capability of the autocorrelation peak, i.e. the matched filtering of the received sequence.

As per the cross-correlation function of a pair of de Bruijn sequences \( \mathbf{a} \) and \( \mathbf{b} \) (\( \mathbf{a} \neq \mathbf{b} \)), of the same span \( n \) and length \( N \), the following bound holds: \(-2^n \leq r_{ab}(k) \leq 2^n - 4 \), for \( 0 \leq k \leq N - 1 \), where \( r_{ab}(k) = \sum_{i=0}^{N-1} a_i b_{i+k} \) denotes the cross-correlation between the two sequences. Complementary de Bruijn sequences \( \mathbf{c} \) and \( \mathbf{\bar{c}} \) provide a null shift cross-correlation \( r_{c,\bar{c}}(0) = -2^n \), that motivates the lower bound on the cross-correlation profile. To avoid this negative peak value, only half of the sequences in the set should be considered, by taking just one sequence in each couple \((c, \bar{c})\). The cross-correlation function of binary de Bruijn sequences shows symmetry properties similar to those exhibited by the autocorrelation function. All the possible cross-correlation values are integer multiples of 4.

If de Bruijn sequences are compared to sequences generated by LFSR, it is well known that \( m \)-sequences generated by using maximal length LFSR, provide an “ideal” two-valued auto-correlation function which is maximal \((N)\) in the dc term, and equal to \(-1/N\) for all the other terms. Gold sequences are obtained by combining two \( m \)-sequences of length \( N = 2^n - 1 \) \((n\) being the span of the register), from a set of so-called “preferred” \( m \)-sequences. Gold sequences
exhibit a three-valued cross-correlation function, with values \([-1, -t(n), t(n) - 2]\), where \(t(n) = 2^n + 1/2\) for odd \(n\), and:  
\[t(n) = 2^{n+2}/2\]  
for even \(n\).

The auto-correlation function of Gold sequences is also a three-valued function, with values \(\{N, -t(n), t(n) - 2\}\). De Bruijn sequences exhibit a satisfactory behavior in terms of correlation properties exploited for code acquisition at the receiver, especially if compared to the Gold ones: for \(k \neq 0\), the normalized auto-correlation values are, on average, smaller than those assumed by the Gold sequences, thus allowing a better detection of the auto-correlation peak.

**Security-related properties**

In the specific case of application discussed in this paper, we are interested in spreading information signals in order to provide physical layer protection of the transmitted information. As a consequence, besides the correlation properties discussed above, it is also necessary to look at the security-related features of de Bruijn sequences selected as spreading codes. First, it is expected that the spreading codes adopted will exhibit a satisfactory degree of randomness, in order to provide the information signals with enough robustness to deter possible jammers or eavesdroppers. In order to design good Pseudo Random Sequence Generators (PRSGs) in cryptographic practice, several randomness criteria have been proposed. Shannon’s basic work [9] demonstrated the one-time-pad scheme is unbreakable by resorting to information theory concepts. However, the ideal one-time-pad scheme is impractical in real systems. Hence, a good PRSG should resemble as much as possible the one-time-pad scheme, and generate pseudorandom sequences with large periods, to guarantee that different messages are encrypted using different key streams. In the mid 1950s, Golomb proposed the well-known three randomness postulates [10], i.e., R-1 (the balance property), R-2 (the run property), and R-3 (the ideal 2-level autocorrelation); the ideal \(n\)-tuple distribution was also introduced as a further criterion. By the end of the 1960s, Berlekamp [11] presented a decoding algorithm to reconstruct an entire codeword from the knowledge of a partial set of its consecutive bits. Later, Massey applied this algorithm in LFSR sequences synthesis [12]: if the length of the shortest LFSR which generates a sequence, known as the linear span or linear complexity of the sequence, is equal to \(n\), then from any known consecutive \(2n\) bits, the full period of the sequence can be reconstructed. This result imposed the application of the large linear span criterion to PRSGs [13]: any pseudorandom sequence used in stream ciphers keystream generators, or pseudorandom number generators, should have large linear spans, in order to minimize their predictability. According to this criterion, de Bruijn sequences are attractive, since their linear complexity \(C\) can be bounded as follows [14]:

\[2^{n-1} + n \leq C \leq 2^n - 1\]  

where both the lower bound and upper bound are achievable. Every de Bruijn sequence of span \(n\) is balanced and exhibits the run property, but it does not provide the 2-level autocorrelation profile. The properties introduced above demonstrate the suitability of selecting binary de Bruijn sequences as spreading codes, even if the 2-level autocorrelation postulate is not satisfied, as the primary intended use of the sequences is not for cryptographic PRSG implementation.

Values reported in Table 1 confirm the exponential growth in the number of de Bruijn sequences, with respect to other possible sets. This specific feature of de Bruijn sequences has made them attractive for use in the security field: assuming one adopts a binary de Bruijn sequence of span \(n\) as a spreading code or a cryptographic key, even in the case an opponent is able to understand how long the sequence is, it will be very difficult for him to locate the exact sequence in use, at least for values of \(n\) greater than 6.

Sequences that exhibit a two-valued auto-correlation function, and low cross-correlation values, are usually targeted to spread spectrum for multiple users communications; spreading for the purpose of information hiding and protection may require different properties, such as a remarkable linear span of the sequences, and a huge number of possible sequences to use, in order to avoid brute-force attacks. In this perspective, de Bruijn sequences can represent a valid alternative to classical \(m\)-sequences and Gold codes, that have been historically proposed for the former set of applications. On the other hand, the generation of de Bruijn sequences shows increased complexity, and this feature must be accounted for in the overall system design cost.

### Table 1. Length and total number of \(m\)-sequences, Gold, and de Bruijn sequences, for the same span value \(n\) \((3 \leq n \leq 10)\).

<table>
<thead>
<tr>
<th>(n)</th>
<th>(m)-sequences</th>
<th>Gold</th>
<th>de Bruijn</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>15</td>
<td>2</td>
<td>15</td>
</tr>
<tr>
<td>5</td>
<td>31</td>
<td>6</td>
<td>31</td>
</tr>
<tr>
<td>6</td>
<td>63</td>
<td>6</td>
<td>63</td>
</tr>
<tr>
<td>7</td>
<td>127</td>
<td>18</td>
<td>127</td>
</tr>
<tr>
<td>8</td>
<td>255</td>
<td>16</td>
<td>255</td>
</tr>
<tr>
<td>9</td>
<td>511</td>
<td>48</td>
<td>511</td>
</tr>
<tr>
<td>10</td>
<td>1023</td>
<td>60</td>
<td>1023</td>
</tr>
</tbody>
</table>
In order to model the ISL and obtain some preliminary evaluations about the possible effective adoption of binary de Bruijn sequences as spreading codes for the DS-SS physical layer, some assumptions are made, to simplify the scenario under evaluation. First, it is assumed that the ISL is affected by a random noise contribution, that includes several effects due to sky noise, and possibly by a jamming signal, due to an adversary satellite that is passing near to the ISL and tries to disrupt its transmissions. At this stage of the study, Doppler effects due to the relative movements of the satellites communicating on the ISL are assumed to travel at the same speed along the same trajectory, but at different locations, so their relative velocity is \( \approx 0 \). Doppler effects may become significant when considering inter-satellite ISLs, among satellites traveling along different trajectories, and featuring variable relative velocities. As a second issue, a single channel is supposed to be active on a single ISL. This means the effects due to binary de Bruijn spreading codes are considered, by looking at the way they affect the spreading of the information signal, with respect to other sets of sequences. The auto-correlation features of the spreading codes play the major role in determining how effectively it is possible to recover the useful signal from the noisy channel. When extending the scenario to the case of several channels on the same ISL, the multi user interference effects shall be taken into account, by considering also the cross-correlation properties of the codes. In this sense, the selection criteria applied to a set of spreading codes should also consider the cross-correlation minimization, in order to make the different channels robust against interference due to the other channels active at the same time, on the same ISL. The condition for no inter-user interference is that the binary sequences assigned to the users in the system are orthogonal, i.e. it is verified if and only if:

\[
\langle x^{(i)}, x^{(j)} \rangle = 0, \forall i \neq j
\]

where \( x^{(i)} \) and \( x^{(j)} \) represent two different sequences of the same length, and \( i, j \in \{1, \ldots, M\} \), being \( M \) the number of sequences in the set. This condition is possible only in the case the number of users \( M \leq N \), since there can be at most \( N \) orthogonal non-zero sequences of length \( N \). When \( M = N \), the condition holds if and only if the \( N \times N \) matrix having \( x^{(1)}, x^{(2)}, \ldots, x^{(M)} \) as rows is a Hadamard matrix. Except for trivial cases (\( N=1, N=2 \)), Hadamard matrices exist only when \( N \) is divisible by 4; they are known to exist whenever \( N \) is a power of 2. As a consequence, if \( N = 32 \) (i.e. \( 2^5 \)) is considered for de Bruijn sequences, we could find a Hadamard matrix including those 32 sequences for which the inter-user interference is zero. There is a great number of orthogonal sequences, for each sequence in the binary de Bruijn family of span 5; even still, in order to find an optimal set of sequences for an \( M \)-user system, we should find at least \( M \) sequences that are pairwise orthogonal over the whole set, i.e. if \( c_j \) is orthogonal to \( c_r \), and \( c_j \) is orthogonal to \( c_t \), then it should also be \( c_j \) orthogonal to \( c_r \) and \( c_t \), with \( j \neq r \neq t \). The ISL communication link is assumed to be working in DS-SS and QPSK modulation; for the jammer, it is reasonable to assume a BPSK modulated signal. The binary information sequence is spread by XOR-ing with the specific spreading code chosen, so that \( T_b = N \cdot T_c \), where \( T_b \) is the bit period, \( N \) is the length of the spreading code, and \( T_c \) is the chip time.

### Table 2. BER performance of the ISL for different noise contribution, jamming component, and spreading codes.

<table>
<thead>
<tr>
<th>random noise (var)</th>
<th>jammer (a)</th>
<th>BER ((10^{-\alpha}))</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>0.1</td>
<td>0.241</td>
</tr>
<tr>
<td>0.1</td>
<td>0.5</td>
<td>0.240</td>
</tr>
<tr>
<td>0.3</td>
<td>0.4</td>
<td>0.259</td>
</tr>
<tr>
<td>0.5</td>
<td>0.4</td>
<td>0.282</td>
</tr>
<tr>
<td>1</td>
<td>0.1</td>
<td>0.250</td>
</tr>
<tr>
<td>1</td>
<td>0.4</td>
<td>0.255</td>
</tr>
<tr>
<td>1</td>
<td>0.8</td>
<td>0.257</td>
</tr>
</tbody>
</table>

### 6. Preliminary Evaluation

A DS spread coherent QPSK transmitter-receiver system has been implemented in software, to obtain preliminary evaluations of the proposed DS-SS ISL based on the adoption of de Bruijn sequences as spreading codes. In this work, the focus is on comparing the behavior of the system using de Bruijn sequences to a classical implementation adopting Gold binary sequences as spreading codes (as in CDMA). To this aim, in order to limit the computational burdens due to simulating the real parameters expected on an ISL (like a 23 GHz carrier frequency, or a 1 Mbps data rate), a scaled version of the parameters has been assumed. An information rate of 1 kbps (\( T_b = 1 \text{ ms} \)) is considered, whereas the chip rate amounts to 32 kchip/s (\( T_c = 31.25 \mu s \)) when de Bruijn spreading sequences are applied, and to 31 kchip/s (\( T_c \leq 32.25 \mu s \)) when Gold sequences are selected. The carrier frequency is set equal to \( f_c = 50 \text{ kHz} \), and a BPSK modulated jammer signal is assumed to be located at a frequency offset of 5000 Hz from the carrier frequency. The simulator generates both random noise and a jamming signal. The amplitude of random noise and the jamming signal is set relative to the strength of the transmitted signal (which is set to 1). For example, a value of 2 for the parameter \( a \) related to the jamming signal amplitude means the power of the jamming signal is twice as strong as the desired transmitted signal, at the receiver. For the random noise contribution, it is requested to specify the value assigned to a parameter called \( \text{var} \), to which the random noise samples are related according to: \( \text{rand\_noise} = \sqrt{\text{var} \cdot \text{rand}(S)} \), being \( S \) the number of samples necessary to simulate the QPSK modulation of the signal.

Two conditions are simulated: the former uses binary Gold sequences of length 31 as spreading codes, the latter applies binary de Bruijn sequences of length 32. They are compared at a parity of the random noise contribution (0.1 ≤ \( \text{var} \) ≤ 1) and jamming signal component (0.1 ≤ \( a \) ≤ 8), with respect to the bit error rate evaluated on the despread received signal. The results obtained are shown in Table 2. The difference in the spreading gain due to the different length of the sequences (31 and 32 bits) has been accounted for within the simulation runs.

Apart from the numerical values obtained, that may not be related to a practical ISL due to the assumptions detailed above, it is interesting to observe how the application of de Bruijn spreading codes in general gives slightly better performance than Gold codes. When both the random noise contribution and jammer component take the maximum value admitted, the BER obtained by de Bruijn sequences is lower than the one provided by Gold codes. A further comment that may be provided about these results, is related to the limited length of the spreading codes considered in simulations. As shown by previous Table 1, when \( n \) increases, the cardinality
of de Bruijn sequence set almost explodes. It is reasonable to assume that the longer the sequences used, the more the spreading signals will show a noise-like behavior, which makes them more robust against random noise and jammer components. For increasing values of the span $n$, the behavior of de Bruijn sequences, with respect to randomness and correlation properties, becomes more favourable than that of Gold codes, both because of the much greater cardinality of the set, and thanks to the fact that de Bruijn sequences become more and more piecewise orthogonal. It means that when $n$ increases, it is possible to find several values of the shift parameter $k$ for which the cross-correlation between two de Bruijn sequences is zero, thus improving the single code acquisition at the receiver.

In huge sets of sequences it is also possible to apply selection criteria in order to choose only sequences that most exhibit a random-like behavior. From a security perspective, the behavior of the linear complexity bounds of de Bruijn sequences (Eq. 8), for different values of the span $n$, is shown in Fig. 7. The much lower value of the linear span of Gold sequences is also shown for comparison. Any de Bruijn sequence has a large linear span; the normalized linear span of a de Bruijn sequence is always $> 1/2$ (for a sequence of period $r$ and linear span $C$, the normalized linear span is defined by $C/r$); any de Bruijn sequence satisfies the span $n$ property.

The results herein discussed suggest the feasibility of applying de Bruijn sequences as spreading codes, not only thanks to their impressive linear complexity (which is a basic parameter with respect to security), but also because they may provide satisfactory results even under the point of view of error performance. As a final remark, Fig. 8 shows a graphical sketch of the received spread signals affected by random noise and jamming, in the case of de Bruijn and Gold spreading, corresponding to the condition of maximum amplitude of the random noise and jamming interference. It is possible to say that the frequency spectrum profiles of the received signals are almost totally superimposed, and do not provide any insight about the specific code used to spread the information.

### 7. CONCLUSION

In this paper a satellite constellation with inter-satellite links for routing among predictable and dynamic nodes is evaluated, in the presence of malicious nodes in space. Security is provided at the physical layer, through Direct Sequence Spread Spectrum modulation, by using a family of binary de Bruijn sequences as spreading codes. It is shown that binary de Bruijn sequences, a special class of nonlinear shift register sequences, can be optimized to perform similarly as Gold codes, and exhibit a satisfactory degree of randomness in order to provide the information signals with enough robustness against possible jammers or eavesdroppers. Comparison among the two sequence sets shows that the use of de Bruijn sequences makes observation much more computationally exhaustive and time-consuming than Gold codes, for an undesirable receiver. This characteristic of the proposed sequence set is supposed to act as a deterrent for eavesdropping and jamming activity to extract information in real-time. The proposed scheme is presented as an effort to secure information in space networks, and to meet an increasing demand for high reliability and security against malicious activities in space routing.

### REFERENCES


**BIography**

**Susanna Spinsante** (Senior Member, IEEE) received her PhD in Electronic and Telecommunication Engineering in 2005, from Universit Politeneica delle Marche, Ancona (Italy). Since then she has been a research fellow at the Department of Information Engineering of the same University, where she works on spread spectrum systems for communications and radar applications.

**Chirag Warty** (PMP, CSM, MEng) is currently a IEEE Associate Member. He has been the associate editor for the IEEE Interface magazine since January 2009. He currently holds several positions on IEEE Study Groups and IEEE societies. He has been consultant for several projects, in India and in the US. He also leads several research teams across the globe. He has perused several academic degrees in India and United States with a BSEE from University of Mississippi with specialization in RF and wireless, Masters of Engineering from University of Illinois-Chicago, Master of Science in Applied Mathematics from Columbia University. He also has several graduate certificates in communications and signal processing from Cornell, UCLA and Stanford. His research interests include MIMO, software defined radio, OFDM and 4G technologies including game theory for terrestrial wireless and satellite clusters.

**Ennio Gambi** Ennio Gambi was born in Loreto (Ancona, Italy) in 1961. He received the Laurea Degree in Electronic Engineering from the Universit Politeneica delle Marche, Ancona (Italy) in 1986, where he is currently an Associate Professor. His main research interests are on spread spectrum systems, applied both to communication and radar environments. He is co-author of several international papers.