Retrieval of Encrypted PRN Sequences via a Self-calibrating 40-element Low-cost Antenna Array: Demonstration of Proof-of-concept

D. Dötterböck, M. Subhan Hammed, T. Pany, Universität der Bundeswehr München, Neubiberg, Germany
R. Lesjak, T. Prechtl, *Joanneum Research*

BIOGRAPHIES

Dominik Dötterböck received his diploma in Electrical Engineering and Information Technology from the Technical University Munich. Since 2007, he is a senior research associate at the Universität der Bundeswehr München at the Institute of Space Technology and Space Applications. His current research interests include signal design, signal-processing algorithms for GNSS receivers and software receivers.

Muhammad Subhan Hameed studied Electrical Engineering at National University of Sciences and Technology (NUST) in Pakistan and has a master degree in space science and technology from Technical University Munich (TUM). He is currently working as a research assistant at Universität der Bundeswehr München. His research interests focus on satellite navigation and GNSS receiver technology.

Thomas Pany is with the Universität der Bundeswehr München at the faculty of aerospace engineering and leads the navigation group within Institute of Space Technology and Space Applications (ISTA). He is working with GNSS since 1997 and with software radio technology since 2002. He has around 200 publications including one book and five patents.

Roman Lesjak received his bachelor and master degree in Geomatics Science from Graz University of Technology. From 2009 to 2016, he was a researcher at the Institute of Geodesy at Graz University of Technology. Since 2017, he is leading the localization and navigation group at JOANNEUM RESEARCH. His current research areas are interference detection and mitigation as well as multi-sensor localization.

Thomas Prechtl studied Mechanical Engineering and Business Economics at Graz University of Technology and received his master degree in Automation Technology/Economics at Campus02 University of Applied Sciences Graz. His research interests focus on radiowave interference detection.

ABSTRACT

In this paper we present the proof-of-concept of simultaneous chip extraction of all satellite's encrypted signals in view based on an asynchronous COTS antenna/frontend platform and open signal synchronization.

INTRODUCTION

Fully encrypted PRN sequences are used by almost every GNSS to restrict access to certain navigation services. After the signals leave the satellite broadcast antenna, they can be accessed openly by any user, so they can be analyzed using e.g. high gain dish antennas raising the signal amplitude above the noise floor. The spectrum (=modulation scheme), spreading code sequence, chip shapes, transmit power or phase relationship are often monitored parameters using this method. After extraction of the spreading code sequences those signals can in principle also be used for navigation purposes by other devices. This is well known, but as

operation of a number of high gain dish antennas to monitor a constellation of GNSS satellites represent a high effort, this has – at least to our knowledge – never been done on an operational basis.
The required gain to estimate chip sequences with a low chip error rate is about 13-20 dB pending the transmit power and the chip duration. This gain can also be realized using a phased array antenna with e.g. 40 elements. As calibration and operation of such an antenna with the corresponding receiver can potentially also result in an equally high effort, a solution was sought and found to realize this system with lower cost. It is based on the fact, that Open Service signals transmitted from the same satellites can be used to online calibrate the array and thus totally uncalibrated antenna elements plus unsynchronized frontends (which could even be located on different parts of the Earth) can be used. In the following sections we will first describe and derive the theory of retrieving encrypted PRN sequences and analyze the required gain for our approach. After that the designed hardware and the software with its modifications are described. Finally some first results for retrieving the signals Beidou B1A and GPS M Code are presented based on a setup with only four geodetic antennas.

THEORY

Considering a generic signals model for a GNSS signals consisting of an open signal and an encrypted component, this signal can be written as:

$$s(t) = \sqrt{2C_{OS}}\exp(-2\pi j f_D t + j\hat{\varphi}_{OS}) \sum_{n=-\infty}^{\infty} c_{OS,n} m_{OS}\left(t - nT_{c;OS}\right) + \sqrt{2C_{ENC}}\exp\left(-2\pi j\left(f_D + f_{off}\right) f_D t + j\hat{\varphi}_{OS}\hat{\varphi}_{Off}\right) \sum_{n=-\infty}^{\infty} c_{ENC,n} m_{ENC}\left(t - nT_{c;ENC}\right) \quad (1)$$

Where:

$C_{OS},\ C_{ENC}$	power (open/encrypted)
$\hat{\varphi}$	carrier phase
f_D	frequency
m	modulation
f_D	Doppler
T_c	chip duration
$c_{OS,n}\,, c_{ENC,n}$	code chips (open, encrypted)
n	chip index
$\hat{\varphi}_{OS}\hat{\varphi}_{Off}$	open signal phase and phase offset of encrypted signal
f_{off}	frequency offset (open/encrypted)
t	satellite time scale

Considering that the open signal is tracked, the parameters $t,\ \hat{\varphi}_{OS}$ and f_D can be known quite accurate because both signals OS and the encrypted are coming from the same transmitter and the transmitter generates the signals coherently (as it is the case for GNSS satellites). So knowing already the chip rate of the encrypted signal, the signal $c_s(t)$ can be estimated in a kind of side channel attack through applying a carrier removal and synchronizing to the same send time so that the signal c_s can be estimated as:

$$c_s(t) = \sqrt{2C_{ENC}} \sum_{\mathrm{n}=-\infty}^{\infty} c_{ENC,n} m_{ENC}\left(t - nT_{c;ENC}\right) \quad (2)$$

Having N antennas/receivers tracking the same satellite, their samples are coherently summed in order to reach a good chip estimate for c_{ENC}:

$$c_{sum}(t) = \sum_{a=1}^{N} c_{s;a}(t) \quad (3)$$

If $m(t)$ and T_c is known (which is usually the case), an optimal matched filter can be applied to demodulate the code values c_n from $c_{sum}(t)$. With the help of the open signal tracking a synchronization of the signal sources is not necessary and the antennas can be located in practice anywhere with line-of-sight to the same satellite. Assuming that the noise in c_{sum} is AWGN, the noise in c_{sum} scales with $\sqrt{N}$ and the chip error rate P_c is given by:

$$P_c = \frac{1}{2}\operatorname{erfc}\left({}^{C}/_{N_0}\, NT_{c;ENC}\right), \tag{4}$$

where ${}^{C}/_{N_0}$ is the carrier-to-noise ratio of a single antenna source and we assume that the signal has binary chip values, e.g. +1,-1. For our validation with only four antennas, but also in general depending on real transmit powers and chip durations, there can be a significant correlation loss through wrong estimated chips, when those estimated chip sequences are fed in to a test user receiver to acquire and track the encrypted signal. The power loss L calculated as:

$$L = 20\log_{10}(1 - 2P_c). \tag{5}$$

As an example a chip error rate of 25% yields a correlation loss of 6dB compared to a receiver having the true PRN code.

We conclude that the use of the Open Service signals to obtain synchronisation and coherency avoids the use of a complex, cost-intensive coherent phased array system and allows even the use of unsynchronized frontends. Furthermore, there is no need for a calibration of the system. The Open Service signals perform an online calibration and therefore ensure an optimal performance.

This means that for example all the open signals of satellites of interest can be acquired and tracked by central processor for all antenna/frontend channels of an antenna array platform. This way a synchronisation between the signal streams of all antenna channels is established. The code NCOs deliver the necessary timing information to synchronise the streams regarding the chip edges. The carrier NCOs track the receiver clock and synchronize their carrier to the common open satellite signal individually. This way all the dynamics of the carrier can be wiped of the signal. The last missing step is to account for the phase difference between the open signal and the encrypted signal. This can be done by applying a fixed known phase offset or by estimating the phase offset in an optimization process. Finally, all the synchronized and phase corrected samples can be added up in order to generate the necessary gain for the estimation of the chips or waveforms.
Following this approach, the antenna chains of the antenna platform have no stringent requirement regarding the sample stream synchronisation. Synchronisation errors that occur for our approach are coming from code tracking noise. This is typically very small compared to the chip length, even when the open signal, which is used for the tracking, has a lower bandwidth and code rate then the encrypted signal.
For the proper constructive accumulation of signal streams, the carrier of the open signal has to be wiped off for all signal streams. Having a sufficiently high carrier-to-noise ratio giving only a few degrees of phase error, a PLL bandwidth will allow to constructively add the single signal streams into a combined one.

For the design of an own antenna platform in order to process many encrypted signals in parallel the following assumptions were made according to the data sheets of the receiver antennas and the used frontends:

- Noise figure of 1 dB for the antenna LNA
- 1 dB loss before the LNA
- Gain of 28 dB for the antenna LNA
- Noise figure of 2.5 dB for the frontend
- Antenna temperature of 140°
- Receiver noise temperature of 170°, depending on quantization
- The noise power spectral density finally was set between -203.0 and -203.7 dBW/Hz (2 and 4 Bit Quantization)

As losses were included:

- Atmospheric losses between 0.18 and 1.65dB
- Implementation losses of 0.2 dB (4 Bit) and 0.69 dB (2 Bit)
- Satellite antenna de-pointing loss of 0.25 dB

Further losses due to imperfect code and phase tracking were up to now not considered. Phase errors would lead to amplitude losses because samples are not perfectly rotated in-phase. They grow towards lower elevation with lower carrier to noise ratios and can finally be analyzed with the frontend clock stability when the antenna platform is ready for test. Code errors lead to wrong mapping of samples to neighbor chips, which in case of a different chip sign or in case of BOC modulation leads to losses in both neighboring chips/BOC subchips. This loss is assumed very small, because the code synchronization error of the open signals will be a small fraction of the chip/subchip size. In order to keep the synchronization error small, carrier aided tracking can be applied for the tracking channels. A further unknown loss could be possible coupling effects of the antenna elements, including correlated noise of the antennas.

Figure 1 shows a prediction for the required gain from using more than one antenna in case GPS M Code from IIR-M satellites. Looking at the required gain, it can be seen that in theory with 40 antenna elements for GPS it will be able to hold the given maximum chip error rate of 16% down to an elevation angle of about 35°. The 16% here are assumed to be justifiable and result from the simple example of chip amplitude of 1 and noise σ_n of 1. At elevations to the horizon, the theoretical gain will be not possible due to the satellite and receiver antenna patterns and shadowing of the antenna elements, unless the antennas would be placed at a large enough distance.

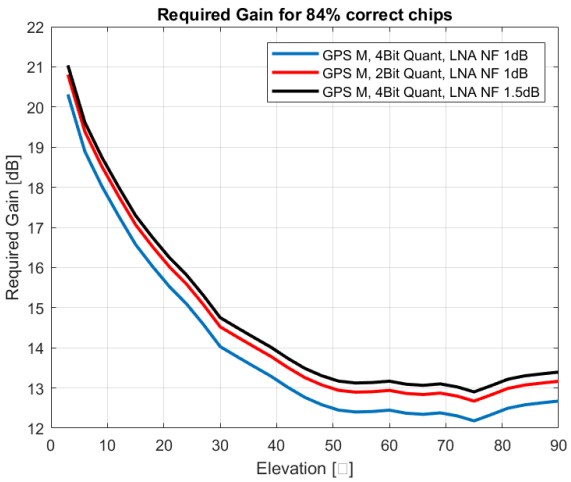


Figure 1: Assumed required minimum gain of antenna platform for GPS IIR-M M Code

Considering that there are at least two signals present, one open and one encrypted, there are different constellations regarding the complexity to retrieve the encrypted chips without interference from the open component or any further one. The more simple cases occur when the encrypted signal is not spectrally overlapping or waveform-orthogonal to the open signal or any other signal component. Here filtering or averaging out through multiplication with e.g. the high rate BOC modulation of the encrypted signal allows to directly apply a matched filter approach. A more tricky case is, if the signal of interest is spectrally overlapping with another signal. One example for this is the Beidou B1 signal, which has an overlap of the legacy B1I with the lower sideband of the B1A BOC(14,2). *Figure 2* shows as an example the power spectral density of Beidou B1 with the left side lobe of B1A with around 3dB more power. The straight forward approach to this is mixing to the upper offset carrier of the signal of interest where there is no overlap of spectra. This is the use of a single sideband of a BOC modulation and leads to 3dB loss of signal power. Apart from the possibility to estimate B1A and B1I together, which was discarded, there is another way to get a better result in theory: through orthogonalization of the signal of interest and the other signals.

Considering the modulation waveforms m and m_{os} as vectors over the duration of one encrypted chip, where m_{os} is one open signal, e.g. B1I and m is B1A. These signal components waveforms can be orthonormalized through a Gram-Schmidt process with the projection from $\boldsymbol{v}$ to $\boldsymbol{u}$ [13]:

$$proj_{\boldsymbol{u}}(\boldsymbol{v}) = \frac{\langle \boldsymbol{v}, \boldsymbol{u} \rangle}{\langle \boldsymbol{u}, \boldsymbol{u} \rangle} \boldsymbol{u} \tag{6}$$

Applying this to our waveform $\boldsymbol{m}$ the modified projection waveform $\boldsymbol{m}'$ then results in:

$$\boldsymbol{m}' = \boldsymbol{m} - proj_{\boldsymbol{mos}}(\boldsymbol{m}) \tag{7}$$

The original and orthonormalized waveforms are plotted in *Figure 3*. The resulting power loss from using the orthonormalized instead of the transmitted waveform of B1A can then be calculated to 2.26dB compared to 3dB for the single sideband processing. A similar approach was already used in [12] to overcome the interference from periodic interferers.

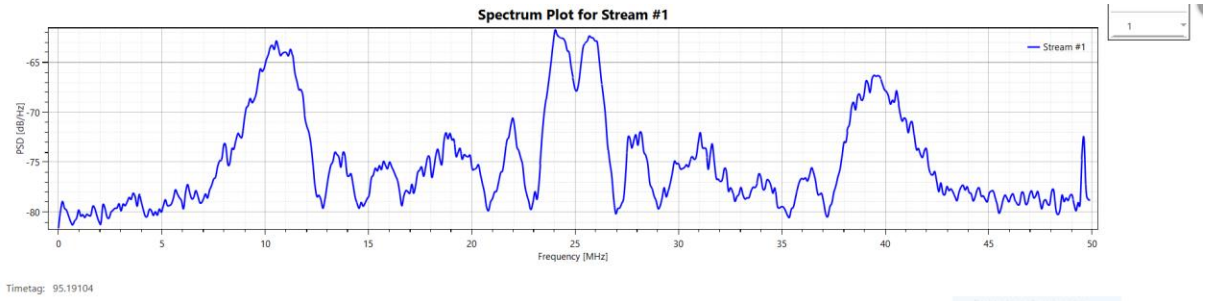


Figure 2: Power spectral density of Beidou B1 signal as calculated within MuSNAT

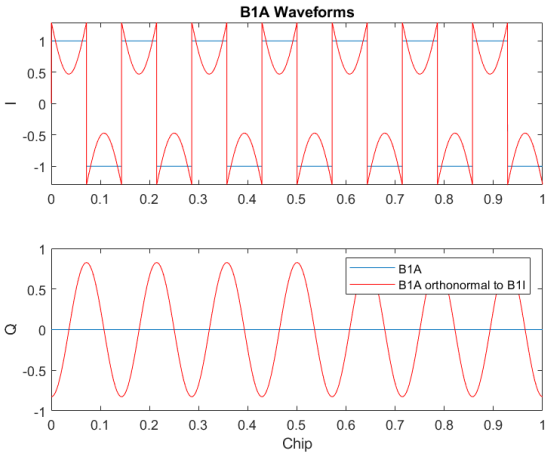


Figure 3: Original and orthonormalized waveform of Beidou B1A

HARDWARE SETUP

For the estimation of the chip sequences of ideally all visible satellites, a hardware platform is required consisting of a high gain antenna, software-defined radio (SDR) components and recording PCs. For the purpose of this activity, low to medium-cost commercial off-the-shelf (COTS) components should be used. In the context of this activity, an antenna array consisting of 40 antenna elements was designed to build the high gain antenna. Before selecting a specific antenna model, different antennas were investigated with respect to their antenna gain pattern. Special focus was put on the gain at low elevations to be able to estimate also the chip sequences of low satellites. In the end, the best model was the Tallysman VSE6137, which is the PCB version of the VSP601 L1/E1 antenna with a bandwidth of 1575 ± 20 MHz.

Although, the antenna has quite a high gain for low elevations, the gain is not high enough to reliably estimate the chip sequences down to 5° elevation. Hence, a simple tilting mechanism was designed to tilt the whole antenna array (cfg. *Figure 4*).
The full systems consists of a construction holding the antenna array with the 20 SDR platforms below and two control cabinets with the PCs and network switches as well as power supply (cfg. *Figure 6*). The whole system is designed for outdoor conditions. Therefore, a stable construction was designed and the control cabinets are temperature controlled to guarantee a maximum inside temperature of 50° C, which is tolerated by the hardware.

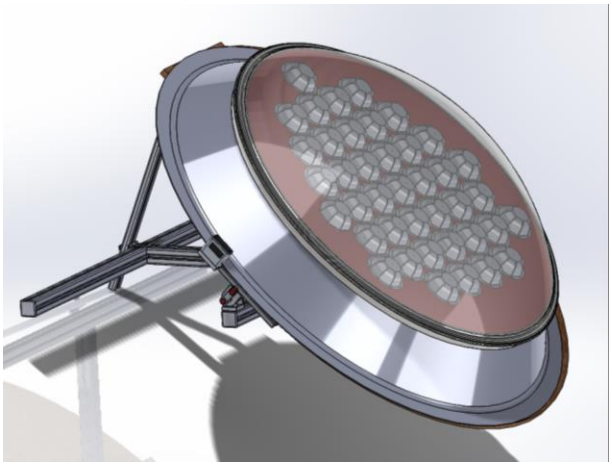


Figure 4: Design of the antenna array

The 40 antenna elements are connected to 20 dual-channel SDR platforms (BladeRF 2.0 micro xA4) to sample the spectrum with a bandwidth up to 40 MHz. Each SDR platform is connected to a NUC PC where the data is stored and forwarded to the central processing unit. The BladeRF 2.0 samples the data with 12 bit resolution, which is decimated to 4 bit on the NUC in real-time. All SDR platforms are using a common 10 MHz signal coming from a GPS-DO to guarantee a stable sampling. The PCs are synchronized via a GNSS based NTP server to have a quite accurate time information of the sampling start. Nevertheless, the exact synchronization of the data is done in software using open GNSS signals.

A detailed view on the inside of a cabinet is shown in *Figure 5*. From the antenna array with the SDR platforms, USB cables get into the cabinet to reach the NUC recording PCs (one PC for one SDR). The PCs are connected to 10 GBit/s network switches, which are connected to the central recording PC holding the required data storage (called database). Due to the real-time data decimation on the PCs, the data can be transferred to the central processing unit in real-time. In the database, all sampling data are stored according to the ION GNSS Software Defined Receiver Metadata Standard [16].

On the central processing unit, the data of the 40 antenna elements are combined to estimate the chip sequences.

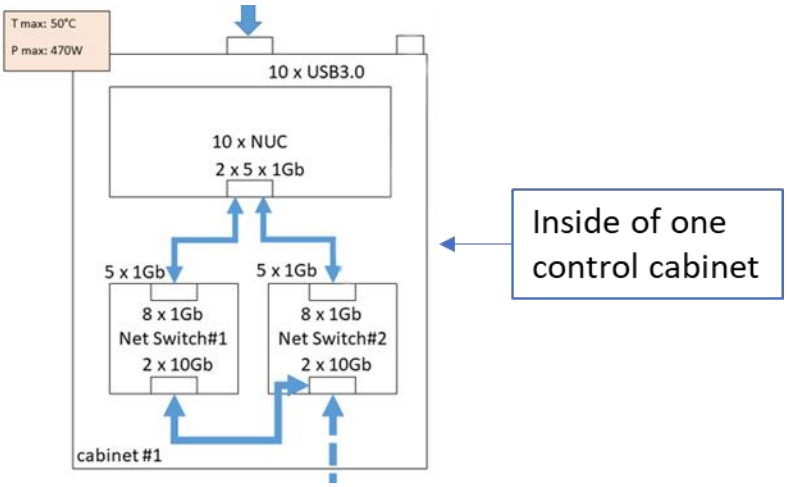


Figure 5: System architecture of one cabinet

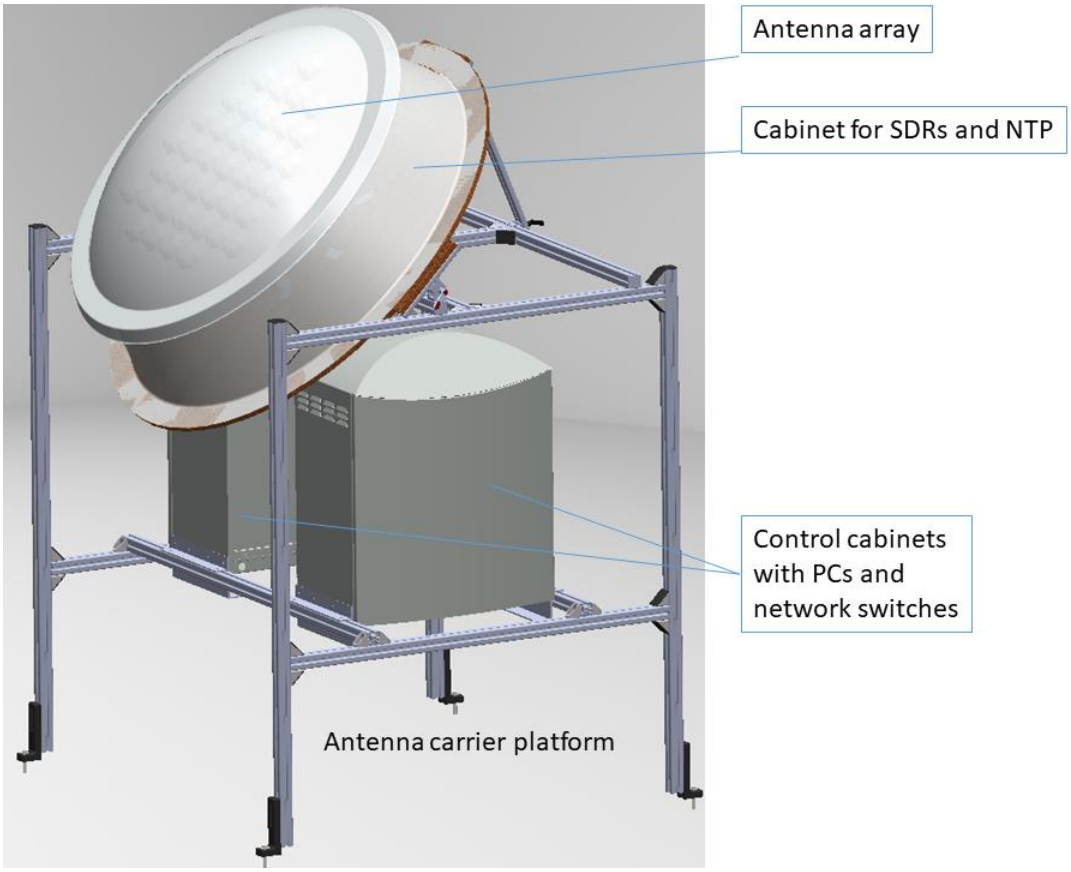


Figure 6: Design of the full system

SOFTWARE IMPLEMENTATION

In order to realize an all-in-view chip estimator within UniBwM's MuSNAT [14] software receiver, two main adaptations were made in the software, namely the capability to process the Beidou B1C signal including navigation message decoding for send time

synchronization and the parallel chip estimation from an antenna array itself. The chip estimation implementation will be explained in the following, the Beidou processing can be found in the Appendix.

Chip Estimation

In *Figure 7* the chip estimation algorithm and data flow are sketched. According to their synchronisation points (e.g. NCO based code phase) the streams are added to one final chip stream, which together with a proper time stamp (e.g. send time) can be sent to the data base and the GNSS SDRs. In case of chip estimation, the stream is further compressed into one bit per chip through correlation along each chip with the known BOC or any other modulation. The synchronisation and chip estimation works as follows:

1. All antennas streams are tracked with DLL and PLL individually per each satellite
2. During the replica generation for the known signal also replicas for the unknown signal are generated. Based on the known signals code NCO this is a chip index (per signal sample) of the encrypted signal, as well as a replica (per sample) of the known or detected modulation waveform. The carrier replica of the known signal tracking can be reused.
3. In the correlation process of the known signal tracking the carrier replica is applied including a constant phase shift in order to wipe off the carrier and to rotate to the encrypted signal phase.
4. Additionally the unknown or detected modulation of the encrypted signal is multiplied.
5. For every sample this resulting chip estimate of the sample is added to the chip stream of the specific antenna at the chip index calculated in step 2.
6. After all receivers channels have indicated a correlation dump of the known signal tracking all antennas chip streams are summed up per sample and written to the output file.

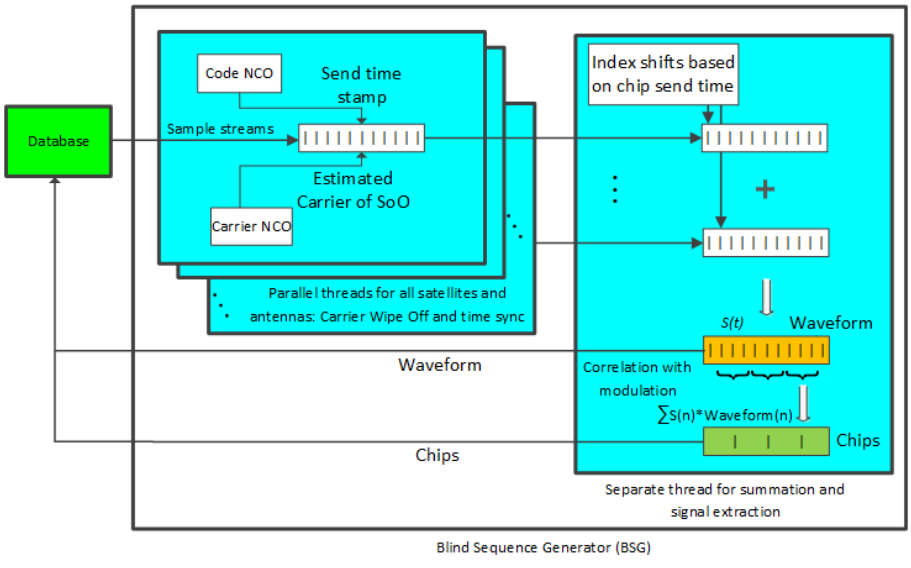


Figure 7: Chip estimation algorithm and data flow in the MuSNAT

RESULTS

First experiments for extracting the chips of navigation signals have been made using UniBwM's dish antenna, shown in *Figure 8* with a diameter of 2.4 meter. In this scenario, the signal source is a single satellite's signal with a carrier to noise ratio of normally above 70 dBHz. Knowing that chip estimation from a simulated signal with a carrier-to-noise ratio similar to the one achievable with the dish antenna results a negligible chip error rate of less than 0.1% using the current chip estimator, the estimation of the chips from a real satellite signal received with the dish antenna can be used as "error free" reference chip sequence.

Figure 9 shows to the left the complex chip scatter cloud, a 2-D histogram, of B1A PRN 36 resulting from upper sideband processing of the dish antenna signal with our MuSNAT chip estimation. To the right there is in analogy the scatter cloud of the same signal when using just four geodetic antennas. The two prominent states are only visible for the dish result, but also for the small array setup the I-component is little more expanded than the Q-component. When comparing the I-components as both chip sequences, inequalities between the sequences are evaluated as chip errors of the array setup sequence. Calculating the chip error rate this way,

Figure 10 shows batch-wise over time the chip error rate for this scenario. About 70% correct chips seem to be a good result for this setup with four antennas and a carrier-to-noise ratio of around 52 dBHz per single antenna element. The discriminator outputs of one array antenna element tracking Beidou B1C is shown in *Figure 10* to the right.

Figure 8: Antenna installations at UniBwM: Dish antenna and geodetic antennas on rooftops.

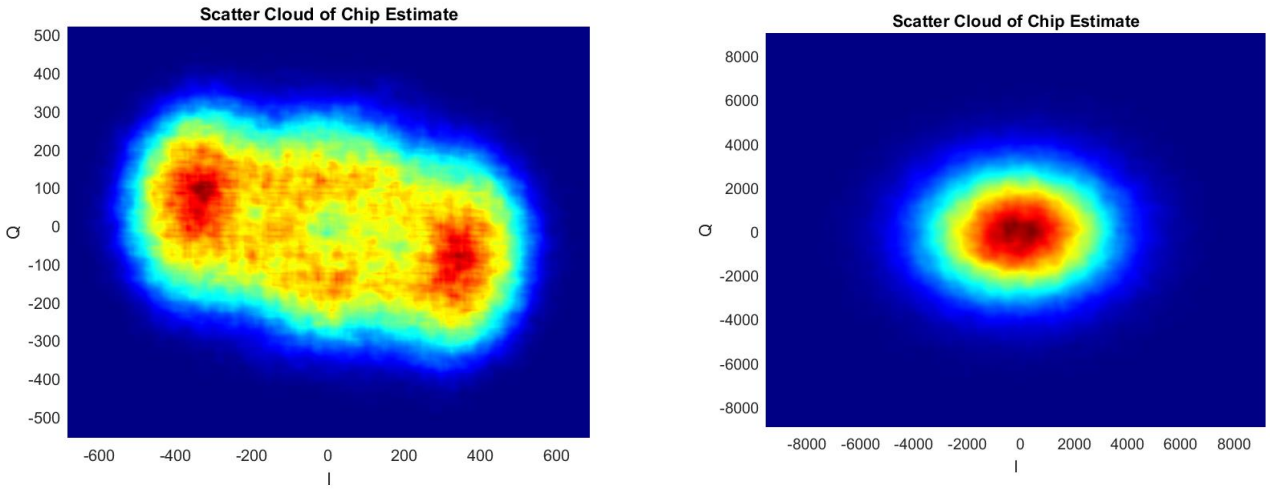


Figure 9: Left: Chip scatter cloud of dish antenna signal from BDS B1A PRN36 upper sideband, right: Chip scatter cloud of four-antenna estimation from BDS B1A PRN36 upper sideband

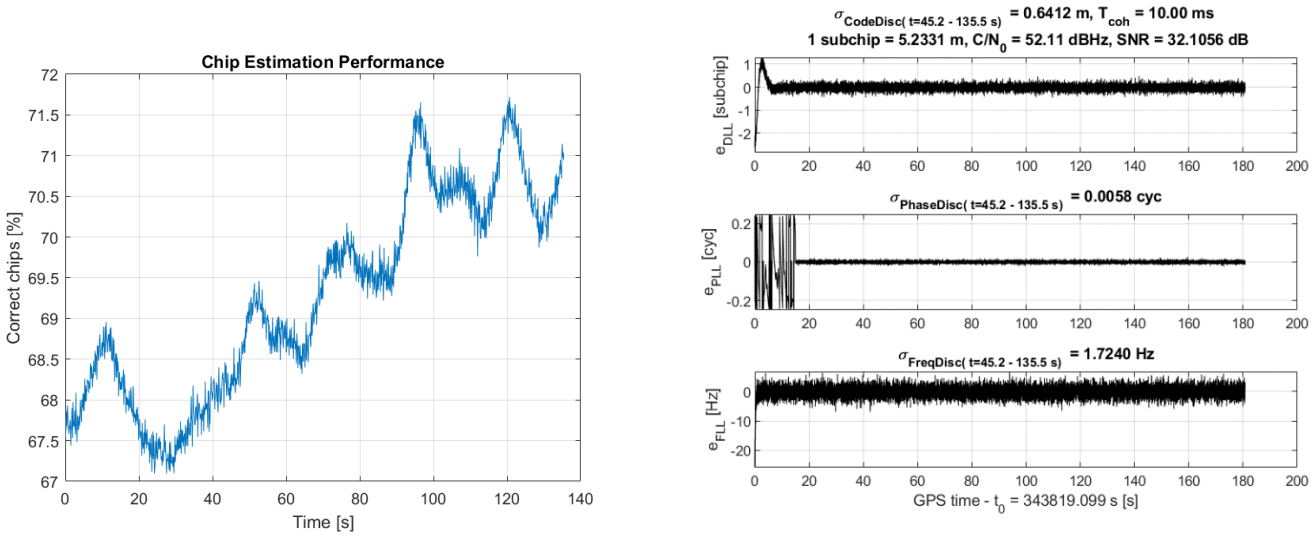


Figure 10: Left: Chip error rate for four-antenna estimation from BDS B1A PRN36 upper sideband based on dish signal as reference, right: B1C tracking discriminator values for single antenna

Our next test scenario was the demodulation of the GPS M Code. In order to get insight to the signal we first made a couple of test recordings. Doing this we discovered what was also reported in [15], namely that GPS IIRM and IIF satellites activate a flex power mode to boost P(Y) signal powers. At the same time, the M Code power seems to be largely reduced. One recording was by chance at the time when the flex power mode started. *Figure 11* shows to the left two power spectral densities from the dish signal, in blue from the beginning of the record when the M Code was present and in red after the P(Y) got a power boost. Another observation is that during the change of the transmitting mode for a period of a good part of a second the C/A code signal power is getting a little bit higher. So having problems in recording M Code signals from GPS IIRM and IIF satellite generations, we switched to GPS III satellites, where no flex power mode seemed to be used. Processing a GPS PRN 18 data set with our chip estimator, we got the results for the dish antenna and the small antenna array plotted in *Figure 12*. To the left the chips of the dish antenna look very good. The visible circles and the grid come from the two bit quantization sample record and only a few samples per chip accumulated. From the scatter plot for the antenna array (right figure), a stretching in the I-component is hardly visible, but the calculated chip estimation performance is around 58% correct chips in this scenario, as can be seen in *Figure 13*.

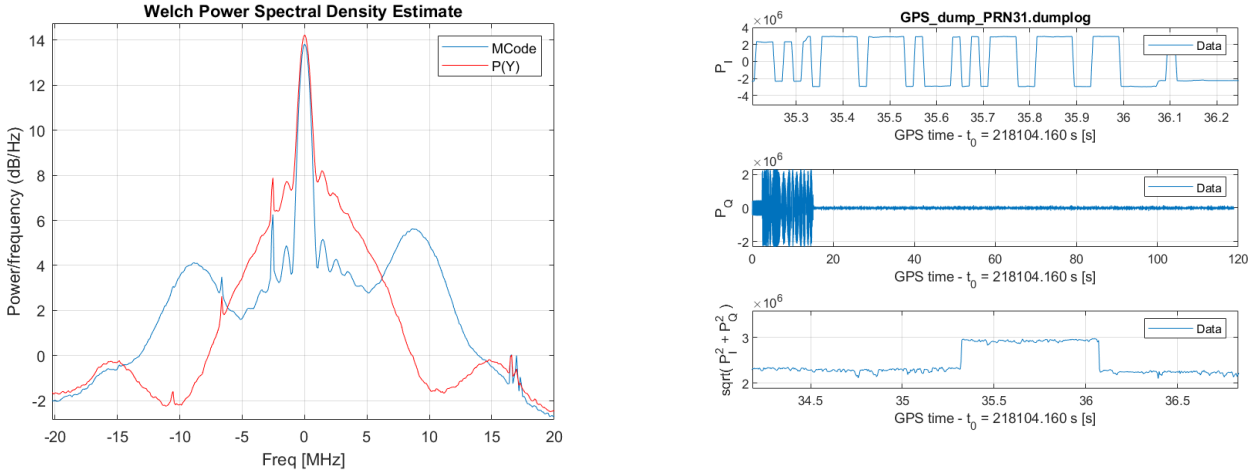


Figure 11: Left: PSD of dish antenna signal from GPS M Code PRN31; right; Correlation values of dish antenna signal from GPS M Code PRN31

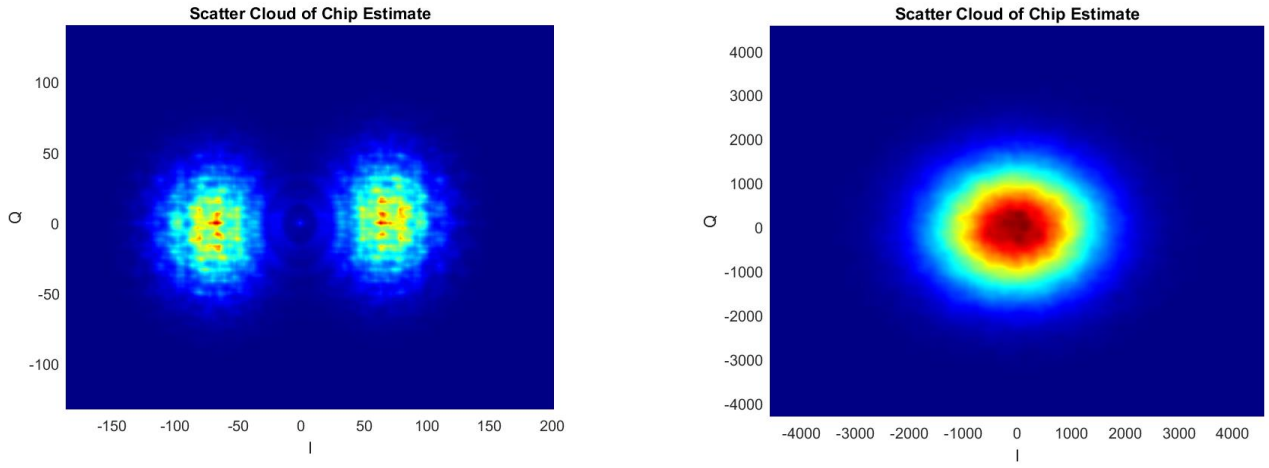


Figure 12: Left: chip scatter cloud of dish antenna signal from GPS M Code PRN18; right: chip scatter cloud of four-antenna combined signal from GPS M Code PRN18

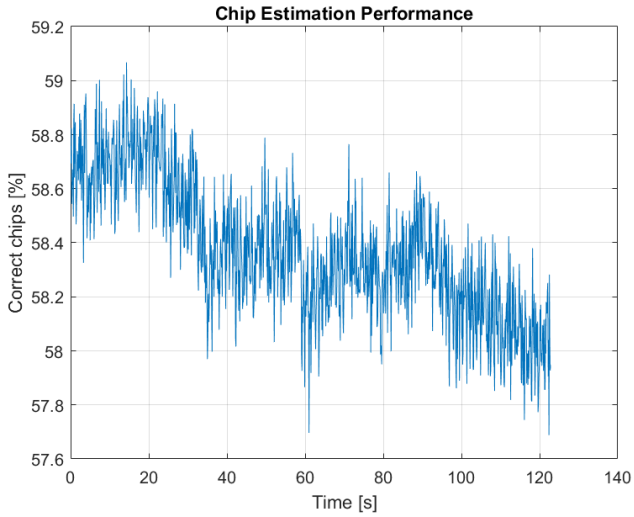


Figure 13: chip scatter cloud of four-antenna combined signal from GPS M Code PRN18

CONCLUSIONS

First testing of real data suggest that with the gain of the full antenna/frontend platform with 40 elements a reduction the chip error rate down to around 2 % can be expected for the presented M Code scenario when having further 10dB gain from 40 instead of four antennas, no further implementation loss occurs and applying to the chip error rate function P_c. So the Proof of concept that our system allows retrieval of encrypted GNSS chips of All-in-view with increased chip error rate at lower elevations has been achieved. Having finally first data sets of the full antenna platform further optimization of the MuSNAT performance and speed on a Ryzen PC (32 cores) and parallel processing of signals from different satellites and constellations will follow. Also further analysis on the transmitted signals and their processing options such as the orthogonalization will be done.

For future design of restricted signals, the results of this paper rose the question if there should be a better protection from side channel attacks through decoupling open and encrypted signals with the use of different timing or even different satellites.

Furthermore, we clearly emphasize the known fact that higher chipping rates of encrypted signals make the estimation of their spreading code sequences more difficult.

APPENDIX

Beidou B1C processing

The Beidou B1C is a new generation civil signal broadcasted by the BDS-III satellites. It is transmitted at the L1 frequency and has a code length of 10230 chips. It comprises of data and pilot components with the data modulated by BOC(1,1) and the pilot modulated by QMBOC(6,1,4/33) [1].

The B1C navigation frame is 1800 symbols in length and is transmitted at a symbol rate of 100 Sym/sec. The frame is divided into three sub frames. Subframe 1 is further divided into two blocks. The first block, containing the satellite PRN number, is 21 symbols long and is encoded with BCH(21,6,3). The second block, containing the Beidou Time (BDT) Second of Hour (SOH) parameter, is 51 symbols long and is encoded with BCH(51,8,11). Both subframe 2 and 3 are encoded with 64-ary NBLDPC codes and are block interleaved.

The B1C navigation message decoder has been developed for MuSNAT in an object-oriented style to maintain modularity. Overall, the following core modules formulate the B1C decoder:

FrameSynchronizer: This class takes the first 21 symbols and last 21 symbols of the 1821 symbols long frame buffer as inputs and sets a frame synchronization flag if a frame synchronization is detected. Unlike other GNSS signals such as the L1 C/A code, the B1C does not have a pre-defined 'preamble' bit sequence which can be used for synchronization, however, it is known that the first message parameter of subframe 1 is the satellite PRN number. The PRN number is already known as a prior to the receiver from the acquisition and tracking stages. Hence, the decoder gets the PRN number from the MuSNAT engine and encodes it with BCH(21,6,3). It then correlates it with the first 21 and last 21 symbols of the frame buffer with zero-lag. If the absolute value of both the correlations is equal to 21, then it is said that the first 1800 symbols in the buffer correspond to a complete synchronized frame and that last the 21 symbols correspond to subframe 1 of the next message frame and with this the frame synchronization flag is set.

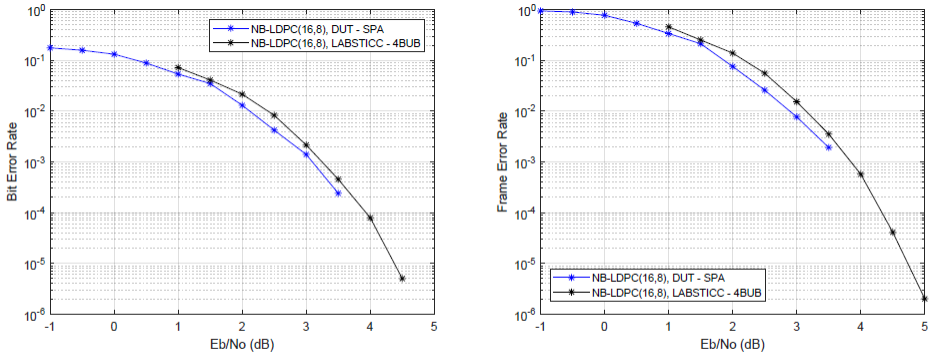
BlockDeinterleaver: This class takes the 1728 symbols long stream of subframe 2 and 3 and performs de-interleaving by implementing a 36 x 48 matrix block de-interleaver. Without any addition or removal, this class only reorders the existing symbols.

BCHDecoder: This class takes the 72 symbols of subframe 1 as input and separately decodes the BCH(21,6,3) encoded PRN number and BCH(51,8,11) encoded SOH parameter using a Maximum Likelihood (ML) BCH decoder. The ML decoder intrinsically corrects error bits by finding the message word which produces a modulated code word that results in the closest match with the received word [2]. Upon instantiation, this class implements the encoder circuits for BCH(21,6,3) and BCH(51,8,11) to initialize the look-up-tables for the ML decoding process. It then compares the received code word with all the entries of the look-up-table and considers the transmitted message word to be that entry of the look-up-table that produces an encoded code word which has the closest match to the received word.

Non-binary LDPC Decoder: This class takes a de-interleaved 1728 symbols long stream of subframe 2 and 3 as input and provides the decoded subframe 2 and 3 as its outputs. The class at first assigns 1200 symbols to a subframe 2 buffer and the remaining 528 symbols to a subframe 3 buffer. Both the buffers are then separately passed to a subroutine that performs the decoding process. Within the decoding subroutine, the first step is to compute the channel log likelihood ratios (LLRs) for the received symbols which are then used as inputs to the non-binary LDPC decoder. As an example, for the 64-ary NB-LDPC(200,100) code implemented for subframe 2, the LLRs are computed in the following manner:

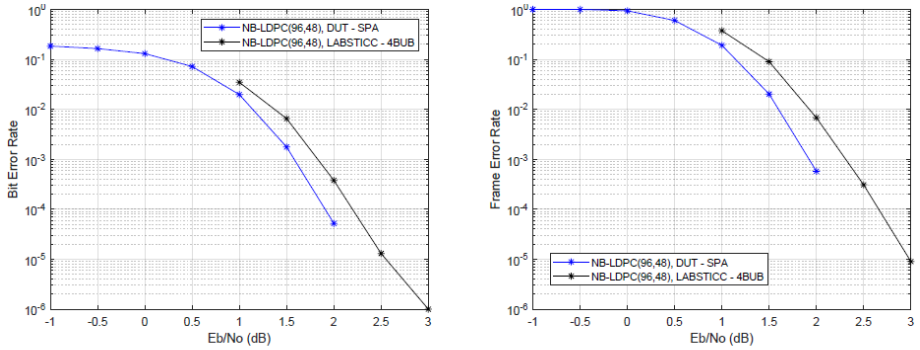
a) Each element in the Galois field of 64-ary is 6 bits long. Hence, the 1200 symbols long stream is divided into 200 groups with each group containing 6 symbols.
b) The 64-ary field contains 64 elements ranging from decimal value 0 to 63. For all the elements, in their binary format, the BPSK modulated word is generated and stored in a 64 x 6 matrix.
c) For a given group of symbols, the difference between it and all the BPSK modulated words is computed.
d) The square of the distances are taken to consider the magnitude. The distances for a given BPSK code word are summed and scaled by the noise variance of the channel.
e) The scaled distances are then made relative to the distance of the first element.

The non-binary LDPC decoder implements a non-binary LDPC decoder based on the NB-LDPC Sum-product Algorithm [3]. The latter was cloned from [4] and was included in the project. For performance evaluation of the NB-LDPC decoder, a comparative analysis was performed by comparing the results of the Accumulative Bubble Check (a-Bub Check) algorithm against the layered Sum-product Algorithm (SPA) used in [1]. The comparison was made by analyzing the BER and FER obtained for different code word lengths for both the algorithms. The results for the BER and FER for a 4-Bubble Check decoder case are maintained as part of the FP7 DaVinci project and were obtained from [2]. The results for the SPA decoder were computed as part of this project. The 4-Bub decoder is denoted by 'LABSTICC - 4BUB' while the SPA decoder is by 'DUT – SPA'.
The analysis was performed for three codes - NB-LDPC(16,8), NB-LDPC(96,48) and NB-LDPC(384,192) having code lengths 16, 96 and 384 respectively. *Figure 14* to *Figure 16* show the BER and FER results for codes for a BPSK modulation and a transmission simulated over an AWGN channel with a maximum of 1e06 transmitted bits. From the plots, it can be observed that the BER improves as the normalized SNR increases. Overall, the SPA decoder performs better than the 4BUB decoder for all code lengths with lower BER and FER values for the same Eb/N0. Also, it can be noted that for increasing code lengths, the difference in BER and FER for both the algorithms also increase indicating that SPA performs even better for increasing code word lengths.



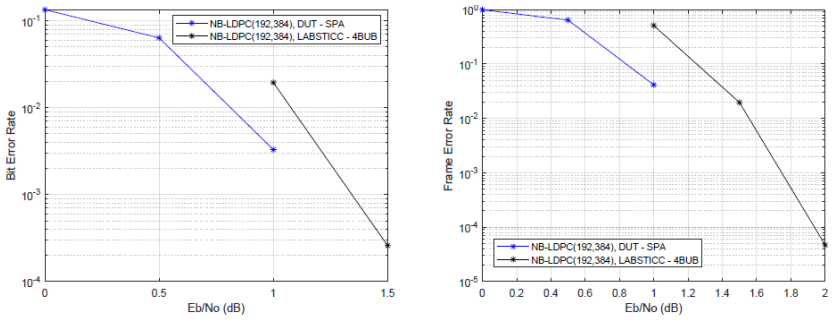
(a) BER (b) FER

Figure 14: BER and FER results for NB-LDPC(16,8) for AWGN channel



(a) BER (b) FER

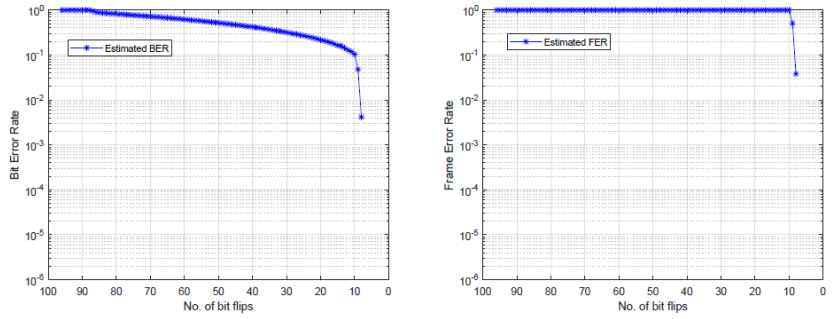
Figure 15: BER and FER results for NB-LDPC(96,48) for AWGN channel



(a) BER (b) FER

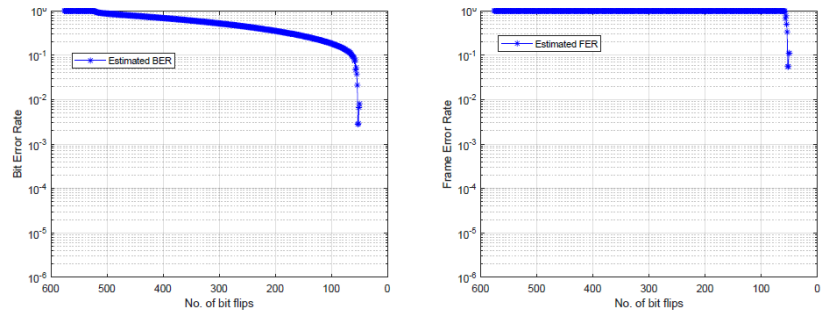
Figure 16: BER and FER results for NB-LDPC(384,192) for AWGN channel

The BER and FER estimations were also performed for the SPA decoder for a simulated bit-flipping channel instead of an AWGN channel in which a known number of bit flips were induced at random locations within the transmitted code word. The number of bit-flip errors were increased from 0 to the code word length. The number of bits transmitted for each run was 1e6. The results of this experiment are shown in Figure 17 to *Figure 19* for different code word lengths. We can observe that there exists a maximum number of bits for each case up to which no error was detected in the decoded code words. We denote this limit as b_{max}. Table 1 lists the ratio of b_{max} to the code word length n for each case. The ratios fall within a range of roughly 10 percent of the code word length. Hence, it can be said that the decoder successfully decodes the received symbols for approximately 10 percent error bits within the code word. However, this a strong generalization due to random location of error bits and does not pertain to burst errors where many error bits may exist consecutively within the received stream.



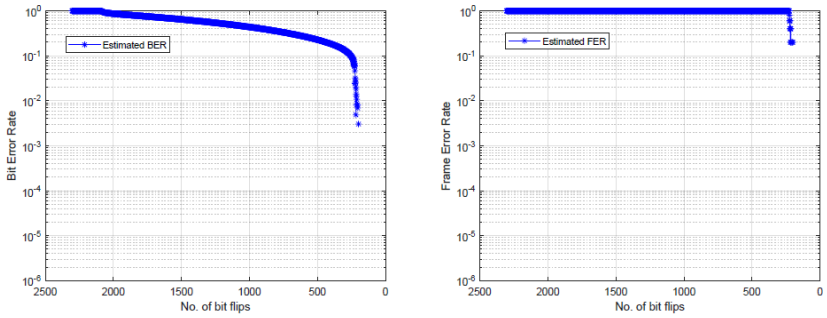
(a) BER (b) FER

Figure 17*: BER and FER results for NB-LDPC(16,8) for randomly positioned bit-flips*



(a) BER (b) FER

Figure 18: BER and FER results for NB-LDPC(96,48) for randomly positioned bit-flips



(a) BER (b) FER

Figure 19: BER and FER results for NB-LDPC(384,192) for randomly positioned bit-flips

REFERENCES

1. P. Steigenberger et al, „GNSS Satellite Transmit Power and Its Impact On Orbit,“ Journal of Geodesy, pp. 609-624, June, Volume 92 2018
2. T. Wang, „Characterization of GPS L1 EIRP: Transmit Power and Antenna Gain Pattern“, ION GNSS+ 2018, Miami, Florida, 2018.
3. T. Wang und et al, „Characterization of the Transmit Power and Antenna Pattern of the GPS Constellation for the CYGNSS Mission“, IGARSS, 2018.
4. China Satellite Navigation Office, "Interface control document, open service signal b1c (version 1.0)", 2017.
5. Sun, Jinhai and Li, Jinhai and Liu, Haiyang and Wang, Feng and Yan, Yuepeng, "Efficient soft-decision maximum likelihood decoding of bch code in the gnss", Journal of Harbin Institute of Technology (New Series), vol. 22, no. 1, pp. 54-58, 2015.
6. Davey, Matthew C and MacKay, David JC, "Low density parity check codes over GF(q)", in 1998 Information Theory Workshop (Cat. No. 98EX131). IEEE, 1998, pp. 70-71.
7. Lcrypto, "Bp decoder for nb ldpc codes", 2019. [Online].Available: https://github.com/Lcrypto/BP-decoder-for-NB_LDPC-codes
8. Arizabaleta, Markel, Gkougkas, Elias, Pany, Thomas, "A Feasibility Study and Risk Assessment of Security Code Estimation and Replay (SCER) Attacks," Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019), Miami, Florida, September 2019, pp. 1039-1050.
9. Allen, David William, Arredondo, Alberto, Barnes, Daniel R., Betz, John W., Cerruti, Alessandro P., Davidson, Benjamin, Kovach, Karl L., Utter, Alexander, "Effect of GPS III Weighted Voting on P(Y) Receiver Processing Performance," Proceedings of the 2019 International Technical Meeting of The Institute of Navigation, Reston, Virginia, January 2019, pp. 936-950.
10. Betz, John W., Cerruti, Alessandro P., "Performance of Dual-Channel Codeless and Semicodeless Processing," Proceedings of the 2019 International Technical Meeting of The Institute of Navigation, Reston, Virginia, January 2019, pp. 583-597.
11. John W. Betz, Alessandro P. Cerruti., "Performance of Dual-Channel Codeless and Semicodeless Processing”, NAVIGATION, Volume 67, Issue 1, March 2020, pp. 109-128.
12. ZHAO, Liang; AMIN, Moeness G.; LINDSEY, Alan R., “Mitigation of periodic interferers in GPS receivers using subspace projection techniques”, Proceedings of the Sixth International Symposium on Signal Processing and its Applications (Cat. No. 01EX467). IEEE, 2001. S. 497-500.
13. Björck, Å., “Numerics of Gram-Schmidt orthogonalization”, Elsevier, Linear Algebra and its Applications, Volumes 197–198, January–February 1994, Pages 297-316
14. Pany, T., Dötterböck, D., Gomez-Martinez, H., Hammed, M. Subhan, Hörkner, F., Kraus, T., Maier, D., Sanchez-Morales, D., Schütz, A., Klima, P., Ebert, D., "The Multi-Sensor Navigation Analysis Tool (MuSNAT) – Architecture, LiDAR, GPU/CPU GNSS Signal Processing," Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019), Miami, Florida, September 2019, pp. 4087-4115.
15. Peter Steigenberger, et al., “The New Flex Power Mode: From GPS IIR-M and IIF Satellites with Extended Coverage Area”, InsideGNSS, May 2020
16. „GNSS Software Defined Receiver MetaData Standard“, [Online]. Available: http://sdr.ion.org.