Generation and Evaluation of BDS Navigation Data for Spoofing Applications

A dissertation submitted in partial fulfilment of the academic requirements for the award of

Master of Engineering

in

Electronics and Communication Engineering

(Communication Engineering)

by

D.Rajnarayana

1601-19-744-005

Department of Electronics and Communication Engineering

Chaitanya Bharathi Institute of Technology (A)

Affiliated to Osmania University

Accredited by NAAC-UGC and NBA-AICTE

ISO 9001:2015 Certified Institution

Gandipet, Hyderabad, 500075

Telangana State, INDIA

July, 2021

Generation and Evaluation of BDS Navigation Data for Spoofing Applications

A dissertation submitted in partial fulfilment of the

academic requirements for the award of

Master of Engineering
in
Electronics and Communication Engineering
(Communication Engineering)

by

D.Rajnarayana

1601-19-744-005

Under the esteemed guidance of

Dr. A. D. Sarma

Professor, Dept. of ECE

Director R & D, CBIT

Department of Electronics and Communication Engineering

Chaitanya Bharathi Institute of Technology (A)

Affiliated to Osmania University

Accredited by NAAC-UGC and NBA-AICTE

ISO 9001:2015 Certified Institution

Gandipet, Hyderabad, 500075

Telangana State, INDIA

July, 2021

Department of Electronics and Communication Engineering

Chaitanya Bharathi Institute of Technology (Autonomous)

Hyderabad – 500075

Certificate

This is to certify that the project work titled **"Generation and Evaluation of BDS Navigation Data for Spoofing Applications"** submitted by **Dasari Rajnarayana** bearing **Roll No.1601-19-744-005**, a student of **Department of ECE, Chaitanya Bharathi Institute of Technology,** in partial fulfillment of the requirements for award of the degree **Master of Engineering** with **Communication Engineering** as specialization is a record of the bonafide work carried out by him during the academic year 2020-2021.

Guide	**Co-Guide**	**Head of the Department**
Dr. A.D Sarma	**Dr. A. Supraja Reddy**	**Dr. D. Krishna Reddy**
Professor	**Associate Professor**	**Professor**
Director R&D	**Dept. of ECE**	**Dept. of ECE**
Dept. of ECE	**CBIT, Hyderabad**	**CBIT, Hyderabad**
CBIT, Hyderabad		

Declaration

This is to certify that the work reported in the present thesis titled "Generation and Evaluation of BDS Navigation Data for Spoofing Applications" is a record work done by me in the Department of Electronics and Communication Engineering (ECE), Chaitanya Bharathi Institute of Technology, Hyderabad. No part of the thesis is copied from books/journals/internet and wherever the portion is taken the same has been duly referred in the text. The reported results are based on the project work done entirely by me and not copied from any other source.

Place: Hyderabad D.Rajnarayana

Date:

Acknowledgement

I would like to express sincere gratitude to my supervisor, **Dr. A. D. Sarma, Professor,** Department of ECE, Chaitanya Bharathi Institute of Technology, Hyderabad for his valuable guidance, co-operation, encouragement and endless patience, without whose inspiring guidance, this project would be a dream to me. I am very grateful for his generous support throughout the course of this work.

I wish to express my deepest gratitude to my Co-guide, **Dr. A. Supraja Reddy, Assoc. Prof.,** Department of ECE, CBIT, for her valuable guidance, co-operation, encouragement and constant monitoring during the project.

I am highly grateful to **Dr. D. Krishna Reddy, Head of the Department, ECE**, **Professor,** CBIT, Hyderabad, for providing permission to use the facilities available in the institute and for providing his seamless support and knowledge throughout the project.

I am very grateful to our project coordinators, **Dr. A. Supraja Reddy, Assoc. Prof.,** Department of ECE, CBIT, **Sri M. V. Nagabhushanam, Assistant Prof.,** Department of ECE,CBIT, **Dr. A. D. Sarma, Professor, Director R & D,** Department of ECE, CBIT for their constant monitoring and cooperation during the project.

I express a wholehearted gratitude to **Dr. P. Ravinder Reddy, Professor, Principal,** CBIT, for providing the best environment for carrying throughout academic schedules and project with ease.

Finally I convey my heartfelt thanks to my parents, friends and all those who helped me directly or indirectly in carrying out this project work, for their constant support in the successful completion of the project.

Abstract

Beidou Navigation Satellite System (BDS) is China's own satellite navigation system. BDS is designed for providing better positioning and navigation service to users globally like any other GNSS. When GNSS signals are weak in reception, receivers are vulnerable to interferences like jamming and spoofing. Thus, GNSS receivers experience challenges in civilian and defence applications. Spoofing is the intelligent type of interference to GNSS receivers by sending false signals intentionally by the attacker. Most of the receivers are unable to detect the spoofing interference and differentiate between genuine signal and false signal. GNSS false signals can be easily generated by making modifications in navigation data. The main aim of this project is to generate navigation data for a newly developed Beidou navigation satellite system (BDS-3) for spoofing applications. To carry out the aim, initially beidou RINEX navigation file of one day is read to extract navigation data. The BDS-3 system of PRN C20, 23, 27, 28, 32, 37, 41, 46 MEO and C38, 39, 40 IGSO satellites position, velocity and time are computed and validated using ephemeris parameters from extracted navigation data. These ephemeris parameters are used in construction of navigation message. B2a signal transmits B-CNAV2 navigation message by performing 64-ary non-binary LDPC (96, 48) error correction encoding. The navigation data is generated and evaluated for spoofing operation. BDS-3 satellite positions and desired/spoofing position are used to compute pseudoranges. The pseudoranges and satellite positions are used to estimate the desired/spoofed position by Least squares position estimation algorithm. This algorithm gives an estimated static spoofed location i.e., false position is compared with the true position. The navigation data is generated by relevant algorithms can be used to implement a low-cost software simulator for spoofing application. Future work can also be extended to spoofing a dynamic location by transmitting RF signals using SDR devices.

Contents

List of Figures

List of Tables

List of Abbreviations

AIF	Accuracy Integrity Flag
BDS	Beidou Navigation Satellite System
BDT	Beidou Time
BPSK	Binary Phase Shift Keying
CGCS	Chinese Geodetic Coordinate System
C/N	Carrier to Noise
CRC	Cyclic Redundancy Check
DRONE	Dynamic Remotely Operated Navigation Equipment
DIF	Data Integrity flag
GEO	Geo Stationary Orbit
GF	Galois Field
GLONASS	Global Navigation Satellite System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HS	Satellite Health status
ICD	Interface Control Document
IERS	International Earth Rotation and Reference System Service
IGSO	Inclined Geo Synchronous Orbit
IODE	Issue of Data Ephemeris
ITRF	International earth Reference Framework
LDPC	Low Density Parity Check
MATLAB	Matrix Laboratory
MEO	Medium Earth Orbit
PRN	Pseudo Random Number
PVT	Position, Velocity, Time
RF	Radio Frequency

RDSS	Radio Determination Satellite Service
RINEX	Receiver Independent Navigation Exchange
SBAS	Satellite Based Augmentation Service
SDR	Software Defined Radio
SIF	Satellite Integrity Flags
SISMAI	Signal In Space Monitoring Accuracy Index
SOW	Seconds Of Week
UHF	Ultra-High Frequency
UTC	Universal Coordinated Time
WN	Week Number

Chapter 1

Introduction

1.1 Introduction

China developed its navigation system (BDS) from a regional navigation system capability to global system coverage through the BDS-3 system. BDS-3 systems are the only satellite systems among four GNSS's that mixes geostationary (GEO), inclined geosynchronous satellite orbits(IGSO), medium earth orbits(MEO) satellites, radio determination satellite service (RDSS) and satellite-based augmentation system (SBAS) services into a single constellation (Kaplan et al., 2017). Beidou satellites systems have an attribute of inter-satellite links are better compatible with other GNSS's like GPS, GLONASS. BDS-3 system provides open service signals and also offer search and rescue operations. As satellite systems providing signals from space transmitting positioning and timing data as open service to users globally became more vulnerable to interferences like jamming and spoofing. Jamming is an intrusion interference to GNSS receivers and spoofing is intentionally interference by broadcasting false navigation signals to receivers. Spoofing is achieved by providing false position to receivers so that they are unable to detect the threat from transmitters. With the viability, false signals can be generated by making changes in navigation data. The BDS navigation data is extracted from RINEX navigation file of one day's data with ephemeris parameters. From this ephemeris parameters, BDS satellite PVT is computed and validated for each PRN. In BDS-3 system's B2a is an open service signal of 1176.45 MHz frequency navigation message is constructed and evaluated from extracted navigation data. The spoofed navigation data is generated for all acquired PRN's for achieving a spoofing attack. The spoofed navigation data is evaluated for a static desired/spoofed location by using least squares position estimation algorithm for spoofing application using MATLAB.

1.2 Aim and Objectives

The main aim of this project is to generate and evaluate of BDS navigation data for Spoofing Applications.

To achieve the aim, following objectives are fulfilled:

i. Reading a Beidou's RINEX navigation file.

ii. Computation of BDS-3 satellites PVT.
iii. Generation of B2a Navigation message and computing subframe.
iv. Generation and Evaluation of Spoofed BDS Navigation Data.

1.3 Motivation

BDS is the newly added GNSS providing significant positioning, navigation, and timing services in daily life (Lu et. al., 2020). The development BDS-3 system that extended to provide open services globally faces many interferences. GNSS's with secure navigation is the future demand. Since GNSS receivers are not integrated fully to detect such interferences. Interference signals cause controlling of the receiver position, navigation in time. Jamming and spoofing are the two main interferences among many attacks of GNSS signals. Spoofing is a more menacing attack than jamming because the receiver cannot detect the attack or warn the users. It is achieved by sending false GNSS signals to desired location through navigation data. In this thesis, the BDS-3 satellites navigation data is extracted from RINEX navigation file and constructed their navigation message frames by non-binary LDPC encoding. BDS-3 satellite PVT is computed for all possible PRN's for position estimation of desired/spoofed location.

1.4 Literature Survey

To carry out the objectives of the project, concepts related to GNSS systems, signal structure, characteristics and navigation data are referred from standard books (Grewal, 2020; Borre, 2007; Kaplan, 2006). To understand basic performance of BDS system (Yang et. al.,2020) and the concept of B2a signal structure, characteristics, ranging codes and B-CNAV2 navigation message frame are referred from ICD of B2a signal (version 1.0, 2017). The development of Beidou navigation satellite system for providing open services globally, signal plans and services are referred from (Development of the Beidou navigation satellite system, version 4.0, 2019).

For BDS-3 system signal acquisition, tracking, baseband signal processing and implementation of real-time software receiver and referred in (Gao Y et. al., 2019) and challenges of the Beidou receiver in (Bhuiyan et. al.,2014).With increase in availability, interoperability of GNSS systems SDR receivers are designed and implemented on

B1C/B2a signals (Li et. al., 2019). B2a signal navigation is constructed by broadcasting ephemeris parameters in navigation message. The broadcasting ephemeris parameters of BDS in navigation messages according to BDCS used for computation of PVT (Xiaogang et. al., 2017; Truong et. al., 2013). For non-binary LDPC error correction coding of B-CNAV2 and mapping relation of binary bits to navigation message symbols are defined in Galois field GF (2^6) is studied in (Jorge et. al.,2006)

Different types of GNSS spoofing attacks and techniques are referred for implementation of a simplest attack was proposed in the paper (Humphreys et. al., 2008; Psiaki et. al., 2016). Spoofing techniques to generate baseband signals as input to SDR hardware devices to transmit RF signals and implementing new method position spoofing with low cost SDR devices is considered in (Wang et. al., 2015; Riddhi et. al., 2020) .For generating spoofed navigation data and navigation data in bits decoding, computing pseudoranges and evaluating of static desired/spoofed position by least squares position estimation studied in (Borre et. al., 2007).

1.4 Methodology

The BDS open service signals, ranging codes of spread spectrum are available and their liable for spoofing attacks. The navigation information is utilized to generate false signals. The methodology involves navigation data is extracted for one day by reading Beidou navigation file using Matlab tool. It contains PRN, year, month, day, hour and broadcasting ephemeris parameters which are used for the computation of satellite's position, velocity and time by series of algorithms. The Bediou time (BDT) is computed from UTC time from the navigation file by year, month, day, minute, seconds. The broadcasting ephemeris parameters and BDT are the inputs for the estimation of satellite positions and plotted their footprints to identify MEO/IGSO satellites. From the extraction of navigation data, B2a signal navigation message is constructed. The non-binary 64-ary LDPC (96, 48) encoding operation is used to construct B2a navigation message frames. For non-binary encoding, mapping navigation data in binary is mapped to message symbols which are defined in Galois Fields GF (2^6) with a primitive polynomial. The spoofed navigation data is generated by the navigation data in bits for transmission as input and decoding is done for validation. By, the generation of spoofed navigation data of navigation message which is intended to spoof the desired

location. The desired/spoofed location is evaluated by the pseudoranges and computed satellite positions as input to the least squares position estimation method.

1.5 National and International Status

Several research approaches are implemented GNSS signal interferences on jamming and spoofing. In view of this, nationally, Stealthy GPS Spoofing proposed four novel spoofing techniques persistent false target, persistent walking target, persistent pull-off target, and persistent walking pull-off target models and also proposed efficient spoofing strategies are static pull-off, dynamic pull-off, walking position, and stationary position for various civilian and military applications by the author (Bethi et. al., *2020).*

Internationally, the protection effect and scheme implementation complexity of various anti-spoofing techniques against spoofing attacks are analyzed from the perspective of signal-level and data-level by the author (Wu et. al., 2020; Wang et. al., 2020).

An asynchronous lift-off spoofing for GNSS receivers in the signal tracking stage is proposed by the author (Gao et. al., 2020) on Doppler frequency variations, short fluctuations in carrier-to-noise ratio (C/N) and signal lock time, and gentle changes to the receiver's 3D Earth-Centered Earth Fixed (ECEF) coordinates, when the target's position and velocity were approximately known during the attack.

1.6 Organization of the report

This report organized to 5 chapters and the draft of forthcoming sections is as follows. Chapter 2 is the introduction to Beidou navigation satellite system, architecture, principle of operation, Beidou signals and services. B2a signal structure, ranging codes, navigation message frames, and ephemeris parameters are concentrated. Chapter 3 discusses about various spoofing types of GNSS and generation and evaluation of spoofed navigation data. Chapter 4 includes results and discussion of carried work in detail to achieve aim and objectives. Conclusions and future scope of work based on overall project are reviewed in Chapter 5.

Chapter 2

Introduction to Beidou Navigation Satellite System

2.1 Introduction

China constructed own satellite navigation system and developed a GNSS to provide more services across the world compared to other GNSS's. The construction of BDS has divided into three stages namely BDS-1 which is used in china and neighboring regions. BDS-2 referred as Compass provides services to customers in Asia-Pacific regions (Yang et. al., 2011). BDS-3 systems are built to provide global services from 2020 (Yang et. al., 2020). BDS signal structure, generation of ranging codes and navigation message frame parameters are studied in this Chapter.

2.2 Beidou Architecture

The BDS architecture is mainly divided into three segments: a space segment, ground segment and user segment.

2.2.1 Space Segment

The space segment of BDS contains number of satellites located in Geostationary Earth Orbit (GEO), Inclined Geo-Synchronous Orbit (IGSO) and Medium Earth Orbit (MEO).

2.2.2 Ground Segment

In BDS ground segment contains various ground stations, master control stations, time synchronization/uplink stations, monitoring stations, operation and management facilities of the inter-satellite link.

2.2.3 User Segment

The user segment contains various BDS products, systems, and services with compatible other navigation satellite systems and chips, modules, antenna, terminals, application systems & services.

2.3 Principle of operation

Initially BDS systems are developed for regional services and extended to global services by the development of BDS-3 systems (Montenbruck et. al., 2013). The space constellation of BDS-3 consists 3 GEO satellites operate at an altitude of 35,786 kilometers. The IGSO satellites operated in orbit at an altitude of 35,786 kilometers and an inclination of the orbital planes of 55 degrees with reference to the equatorial plane. The MEO satellites operate in orbits at an altitude of 21,528 kilometers and an inclination same as IGSO satellites. The coordinate system of BDS is in accordance with the specifications of International Earth Rotation and Reference System (IERS) and China Geodetic Coordinate System 2000 (CGCS 2000). The ellipsoid parameters such as Semi major axis, Earth's rotation rate etc., are same and aligned with the latest International Earth Reference Framework (ITRF), and is updated annually according to development of BDS. The time system of BDS is called Beidou Navigation satellite system Time (BDT) with seconds as the base unit which is broadcast in the navigation message as per ICD of B2a signal (version 1.0, 2017).

2.4 Beidou signals and services

Beidou transmits navigation signals in three frequency bands: B1, B2, and B3, which are in the same area of L-band are shown in Fig 2.1. From 2020, BDS goal to improve service performance, expand service functions, and guarantee continuous and stable operation. Further improvement in global positioning, navigation and timing, regional short message communication, and ground augmentation service capabilities are included. To provide the satellite-based augmentation, point positioning service, global short message communication, and international search and rescue services, etc. are extended as shown in Table 2.1(Lu et. al., 2020). B2a open service signal's B-CNAV2 navigation message frame is generated and studied in this Chapter.

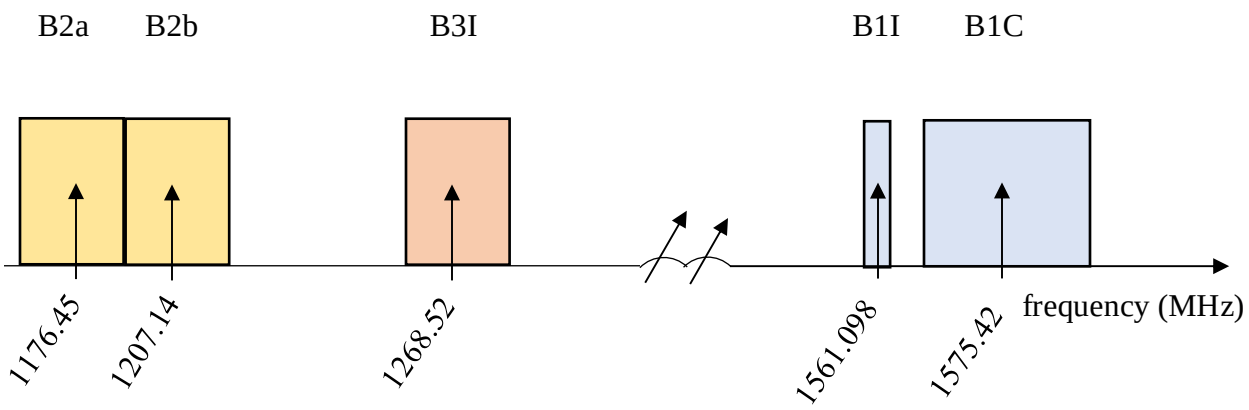


Fig 2.1 Beidou Signals

Table 2.1 Beidou Signal Services

Services		Signals	Broadcasting satellites
Open Service		B1I, B1C, B2a, B2b, B3I	3IGSO+24MEO
		B1I,B3I	3GEO
Satellite-Based Augmentation service		BDSBAS-B1C	3GEO
		BDSBAS-B2a	
Short Message Communication Service	Regional	L (Uplink), S (downlink)	3 GEO
	Global	L (Uplink)	14 MEO
		B2b (downlink)	3IGSO+24MEO
International Search and Rescue Service		UHF (Uplink)	6 MEO
		B2b (downlink)	3IGSO+24MEO
Point Positioning Service		B2b	3 GEO

2.5 Status of Beidou satellites in constellation

There are 49 beidou satellites in constellation of which 44 are included in operational as shown in Table 2.2 (Test and Assessment Research Center of China Satellite Navigation office) transmits B1I, B1C, B2a, B2b and B3I signals accordingly. The satellites information and ephemeris parameters which are included in RINEX navigational file are used to compute the satellite PVT.

Table 2.2 BDS Satellites Status in Constellation

Satellite Number(PRN)	Satellite Name	Type of system	Launch date	Status
C20	MEO-2	BDS-3	05.11.2017	Operational
C23	MEO-5	BDS-3	29.07.2018	Operational
C27	MEO-7	BDS-3	12.01.2018	Operational
C28	MEO-8	BDS-3	12.01.2018	Operational
C32	MEO-13	BDS-3	19.09.2018	Operational
C37	MEO-18	BDS-3	19.11.2018	Operational
C38	IGSO-1	BDS-3	20.04.2019	Operational
C39	IGSO-2	BDS-3	25.06.2019	Operational
C40	IGSO-3	BDS-3	05.11.2019	Operational
C41	MEO-19	BDS-3	16.12.2019	Operational
C46	MEO-24	BDS-3	23.09.2019	Operational
C59	GEO-1	BDS-3	01.11.2018	Operational
C60	GEO-2	BDS-3	09.03.2020	Operational
C61	GEO-3	BDS-3	23.06.2020	Testing

2.6 B2a Signal Structure

BDS-3 system satellites broadcasts the B2a open service signal contains 20.46MHz bandwidth with a center frequency of 1176.45MHz and composed of data components and pilot components. BPSK (10) modulation is used for both data with and pilot channels. The complex envelope of B2a signal is expressed as in equation (2.1). The expressions of $S_{B2a\_data}(t)$ and $S_{B2a\_pilot}(t)$ are referred in ICD of B2a signal (version 1.0, 2017).

$$S_{B2a}(t) = S_{B2a\_data}(t) + j\, S_{B2a\_pilot}(t) \quad -(2.1)$$

where, $S_{B2a\_data}(t)$ is the data component generated from the navigation message data

$$S_{B2a\_data}(t) = \frac{1}{\sqrt{2}} D_{B2a\_data}(t).\, C_{B2a\_data}(t) \quad -(2.2)$$

$D_{B2a\_data}(t)$ is modulated with the ranging code $C_{B2a\_data}(t)$ from equation (2.2).

where, $S_{B2a\_pilot}(t)$ is the pilot component contains only ranging code $C_{B2a\_pilot}(t)$ in equation (2.3)

$$S_{B2a\_pilot}(t) = \frac{1}{\sqrt{2}} C_{B2a\_pilot}(t) \quad -(2.3)$$

2.7 B2a Ranging Code Characteristics

B2a ranging codes are generated by performing XOR logical operation of the primary codes with secondary codes. For one period of primary code has the same length of secondary code chip width. The start of a secondary code chip is aligned strictly with the start of the first chip of a primary code. B2a primary codes of data and pilot components are generated by Gold code sequence of modulo-2 addition on two 13-stage linear feedback shift registers. B2a secondary codes of data components is fixed sequence of code length 5 and pilot components are generated by Truncated Weil sequence of length 100. C37 and C38 satellites ranging codes are generated in this chapter.

2.8 Generation of B2a Ranging Codes

BDS ranging codes are binary sequences that are modulated on the carrier wave while transmitting B2a signal. B2a signal-ranging codes are generated by XORing of primary codes and secondary codes. For every beidou MEO/IGSO satellite a unique pseudo random noise (PRN) sequence is assigned. The primary and secondary codes are validated according to ICD of B2a signal (version 1.0, 2017).

2.8.1 Generation of data component primary code

The primary code is obtained by the Gold code that is generated by modulo-2 addition on two 13-stage linear feedback shift registers (Fig 2.2). It has a length of 10230 chips and a chip rate of 10.23Mcps. The first 24 chips of primary code data component C37 and C38 are shown in Fig 2.3. The generator polynomials of the data component are;

$$g_1(x) = 1 + x + x^5 + x^{11} + x^{13}$$

$$g_2(x) = 1 + x^3 + x^5 + x^9 + x^{11} + x^{12} + x^{13}$$

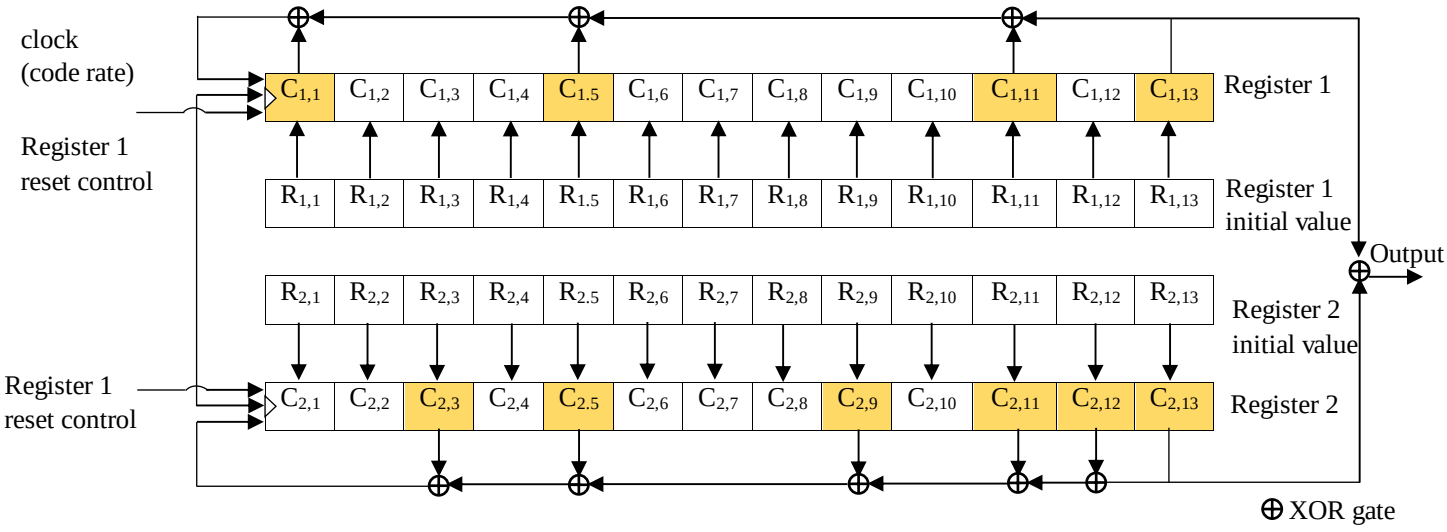


Fig 2.2 Primary code generator for B2a data components

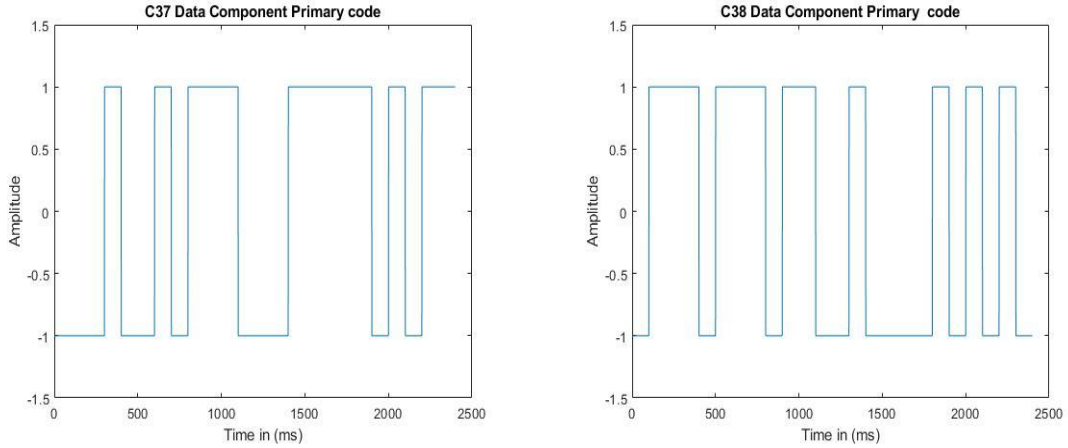


Fig 2.3 Primary code for data components of C37 and C38 satellites

2.8.2 Validation of data component primary code

The obtained first 24 chips of the data component from primary code generator of C37 and C38 satellites are validated by first 24 chips in octal form as shown in Table 2.3

Table 2.3 C37 and C38 satellites data component primary code

S.NO	PRN	The first 24 chips of Data component primary code(binary)	The first 24 chips(octal)
1	37	000100101110001111101011	04561753
2	38	011101110110010000101010	35662052

2.8.3 Generation of data component secondary code

For all Beidou satellites, secondary codes data components are same. The secondary code component is the fixed 5-bit sequences with the 00010 bit values in binary format and its MSB is transmitted first as shown in Fig.2.4

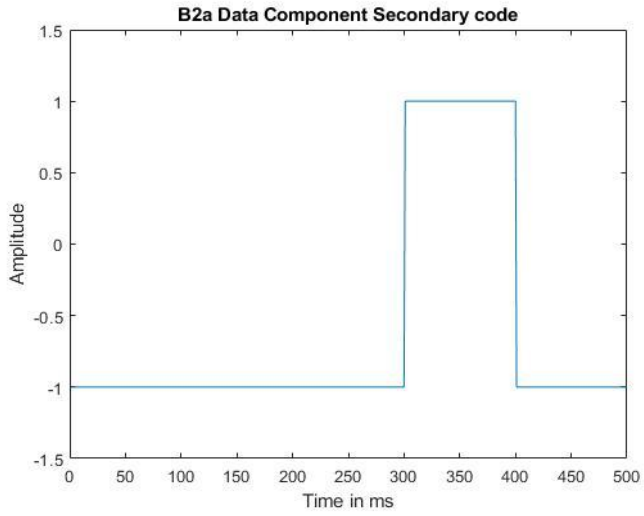


Fig 2.4 Secondary code of B2a Data component for all satellites

2.8.4 Generation of pilot component primary code

The primary code of the B2a pilot component is obtained by the Gold code that is generated by modulo-2 addition on two 13-stage linear feedback shift registers Fig 2.5. It has a length of 10230 chips and a chip rate of 10.23Mcps. The first 24 chips of pilot component primary codes of C37 and C38 results are shown in Fig 2.6.The generator polynomials of the pilot component are;

$$g_1(x) = 1 + x^3 + x^6 + x^7 + x^{13}$$

$$g_2(x) = 1 + x + x^5 + x^7 + x^8 + x^{12} + x^{13}$$

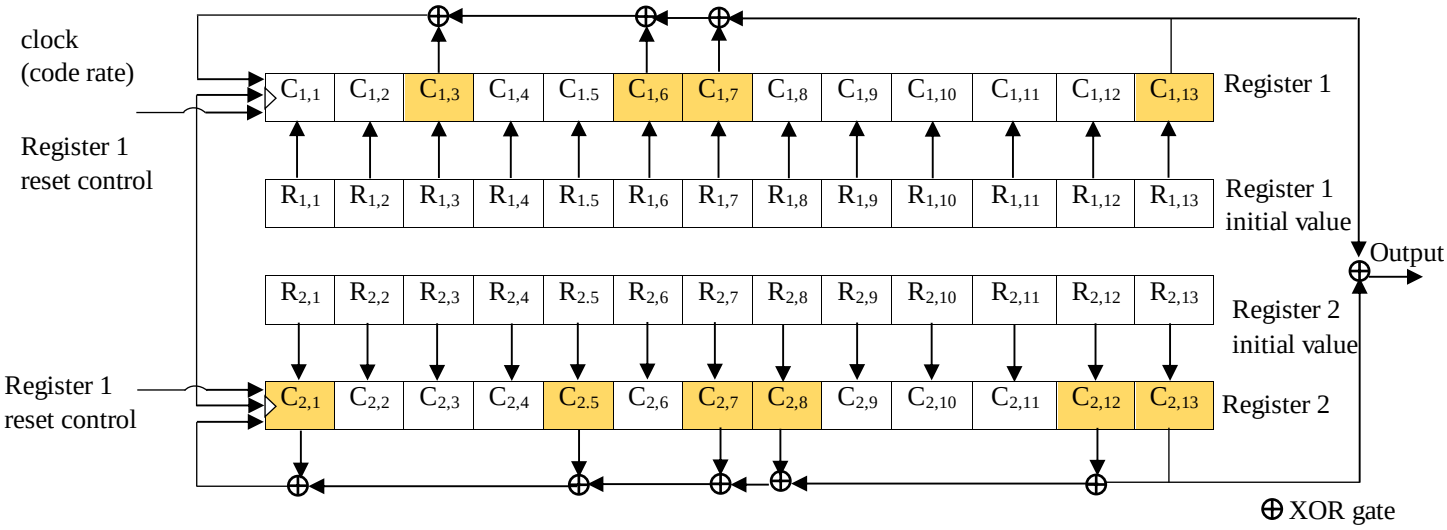


Fig 2.5 Primary code generator for B2a pilot components

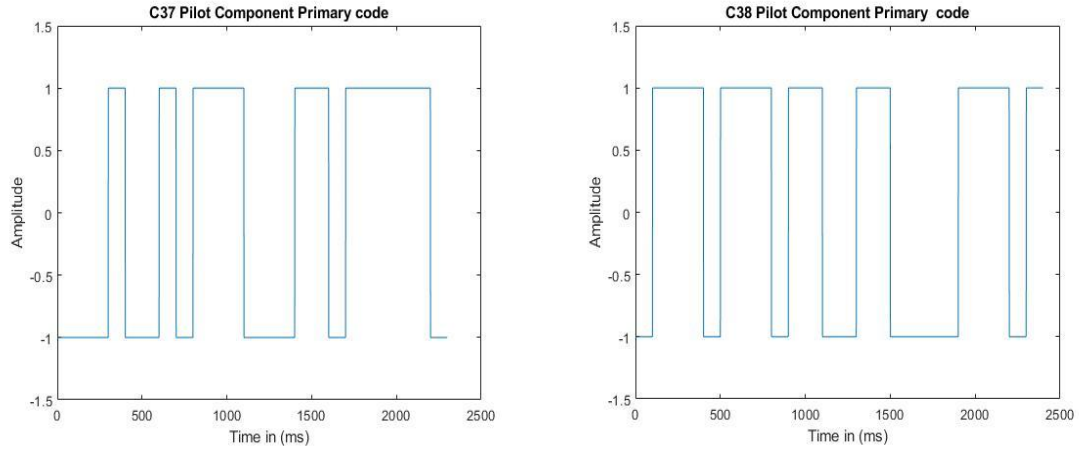


Fig 2.6 Primary code for pilot component of C37 and C38 satellites

2.8.5 Validation of pilot component primary code

The obtained first 24 chips from the pilot component primary code generator of C37 (MEO) and C38 (IGSO) are validated with first 24 chips in octal as shown in Table 2.4.

Table 2.4 C37 and C38 satellites pilot component primary code

S.No	PRN	The first 24 chips of pilot component primary code (binary)	The first 24 chips (octal)
1	37	000100101110001111101011	04561575
2	38	011101110110010000101010	35663035

2.8.6 Generation of pilot component secondary code

The pilot component of secondary codes are obtained by truncation on Weil codes. Its length is first 100 chips generated by Weil code of length of 1021 chips. The first 24 chips of pilot component secondary codes of C37 and C38 satellite results are shown in Fig 2.7

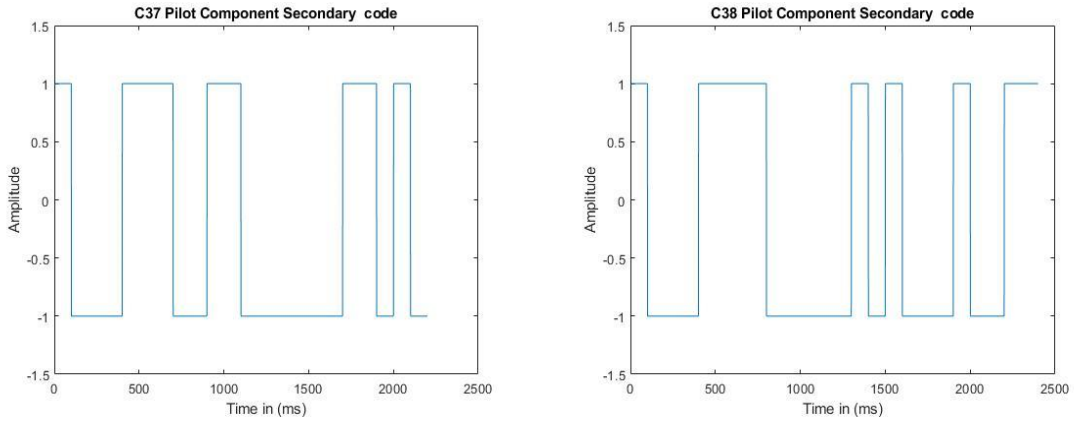


Fig 2.7 Secondary codes for pilot component of C37 and C38 satellites

2.8.7 Validation of pilot component secondary code

The obtained first 24 chips from the pilot component secondary code generator of C37 and C38 are validated with first 24 chips in octal as shown in Table 2.5.

Table 2.5 C37 and C38 satellites pilot component secondary code

S.No	PRN	The first 24 chips of pilot component secondary code (binary)	The first 24 chips (octal)
1	37	100011100110000001101000	10714032
2	38	100011110000010100010011	43602423

The data and pilot component ranging codes are generated by XORring primary code and secondary codes of C37 and C38 satellites are shown in Fig 2.8 and 2.9.

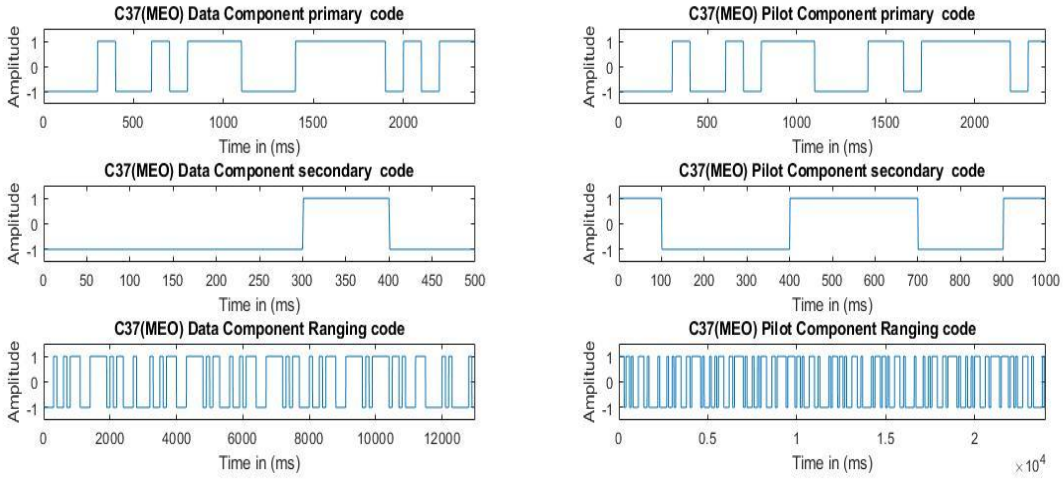


Fig 2.8 C37 Satellite ranging code

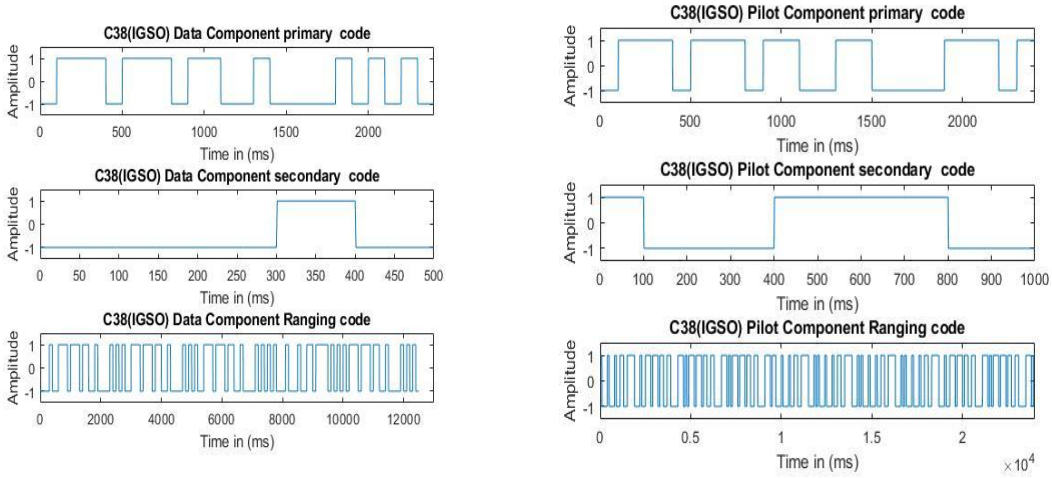


Fig 2.9 C38 Satellite ranging code

2.9 B2a Navigation Message

Any GNSS navigation users determine the navigation satellite broadcasting ephemeris data by receiving navigation message. B2a signal broadcasts the B-CNAV2 navigation message. B-CNAV2 navigation message is important part of B2a signal structure were navigation message data is modulated on B2a data component. Each frame of B-CNAV2 has a length of 600 message symbols obtained by error correction encoding. Its symbol rate is 200sps and transmission of one frame is 3 seconds as per ICD of B2a signal.

2.9.1 LDPC Encoding

The Low Density Parity Check Encoding (LDPC) is the error correction encoding which allows detection and correction of channel including errors at the GNSS receivers (R. Gallager, 1962; Claude Berrou, 2010). B-CNAV2 navigation message frames of B2a signal are encoded with 64-ary LDPC (96, 48) code. The message length of 48 codewords and parity check matrix $\mathbf{H}_{48\times96}$ of 48 rows and 96 columns defined in GF (2^6) are inputs for LDPC encoding. The generator matrix generates first 48×48 part corresponds to the information symbols and remaining 48×48 corresponds to the check symbols (K. Deergha Rao, 2015).

2.9.2 B-CNAV2 Data formats

B-CNAV2 navigation messages can be defined in 63 message types. But only, eight message types are defined, i.e., Message Type 10, 11, 30, 31, 32, 33, 34 and 40. In B-CNAV2 broadcasting order of message types are dynamically adjusted and Message Type 10, Message Type 11 broadcast continuously together. The receiver recognize its Message Type length of 6 bits every time when a navigation message is received. In this thesis, B-CNAV2 Message type 10 and 11 data formats are used for generating navigation message frame in Chapter 4. B-CNAV2 Message Type 10 contains ephemeris-I (203 bits), week no (13 bits), IODE (8 bits) and in Message Type 11 ephemeris-II (222 bits), Satellite Health status (2 bits) along with satellite integrity flags of B1C and B2a, SISMAI and CRC check sequence (24 bits) each.

2.10 B-CNAV2 Navigation Message Parameters

2.10.1 Preamble

Preamble (Pre) is the first 24 symbols of each message frame with the value of 0xE24DE8 in hexadecimal i.e., '111000100100110111101000' in binary format.

2.10.2 Ranging Code Number

B-CNAV2 navigation message ranging code number is PRN broadcasted in message frame. It is the unsigned integer with a length of 6 bits. Its effective value is in the range of 1 to 63.

2.10.3 B-CNAV2 Message Types

Message Types is an unsigned integer used to identify the message types of B-CNAV2 navigation message frames with a length of 6 bits Table 2.6.

Table 2.6 B-CNAV2 Message Types

MesType (Binary)	Message Type
001010	Message Type 10
001011	Message Type 11

2.10.4 BDS Time Parameters

The navigation system time parameters broadcasted in message frames contains Seconds of Week (SOW). It is broadcast in all message types of B-CNAV2. Week Number (WN). It is the week number of BDT (s) as shown in Table 2.7.

Table 2.7 BDS Time Parameters

Parameter	Representation(bits)	Scaling factor	Effective range value	Unit
SOW	18	3	0~604797	s
WN	13	1	0~8191	week

2.10.5 Beidou Satellite Integrity Status Flag

The data integrity status flag (DIF), signal integrity flag (SIF) and accuracy integrity flag (AIF) of each 1 bit length. The B2a and B1C signal flags are transmitted in B-CNAV2 both message types of 10 and 11.

2.10.6 Signal In Space Monitoring Accuracy Index

The signal in space monitoring accuracy index (SISMAI) of length 4 bits. It indicates variance of the Gaussian distribution.

2.10.7 Issue of Data, Ephemeris

Issue of Data, Ephemeris (IODE) of 8 bit length extracted from navigation data. It indicates issue number of a set of ephemeris parameters and the range of the ephemeris data age.

2.10.8 Beidou Satellite Health Status

Satellite Health Status (HS) is transmitted in B-CNAV2 Message Type 11 are shown in Table 2.8.It is an unsigned integer of length 2 bits.

Table 2.8 Beidou Satellite Health Status Parameter

Satellite Health Status value	Indication	Operation
0	The satellite is healthy	Provides services
1	The satellite is unhealthy or in test	Does not provides service
2	Reserved	Reserved
3	Reserved	Reserved

2.10.9 Ephemeris Parameters

B-CNAV2 navigation message contains a set of broadcasting ephemeris parameters which are unique for each satellite system are extracted from RINEX navigation file are shown in Table 2.9. There are two types ephemeris parameters are in Message Type 10 and 11 broadcast in navigation message.

Table 2.9 B-CNAV2 Ephemeris Parameters

No.	**Parameter**	**Definition**
1	t_{oe}	Ephemeris reference time
2	SatType	Satellite orbit type
3	ΔA	Semi-major axis difference at reference time
4	$\dot{A}$	Change rate in semi-major axis
5	Δn_0	Mean motion difference from computed value at reference time
6	$\Delta \dot{n}_0$	Rate of mean motion difference from computed value at reference time
7	M_0	Mean anomaly at reference time
8	e	Eccentricity

9	ω	Argument of perigee
10	Ω_0	Longitude of ascending node of orbital plane at weekly epoch
11	i_0	Inclination angle at reference time
12	Ω	Rate of right ascension
13	i_0	Rate of inclination angle
14	C_{is}	Amplitude of sine harmonic correction term to the angle of inclination
15	C_{ic}	Amplitude of cosine harmonic correction term to the angle of inclination
16	C_{rs}	Amplitude of sine harmonic correction term to the orbit radius
17	C_{rc}	Amplitude of cosine harmonic correction term to the orbit radius
18	C_{us}	Amplitude of sine harmonic correction to the argument of latitude
19	C_{uc}	Amplitude of cosine harmonic correction to the argument of latitude

2.10.10 Beidou Satellite Type

In B-CNAV2 navigation message SatType in binary of length 2 bits broadcasts in Message Type 10. It indicates type of satellite information is transmitted as shown in Table 2.10.

Table 2.10 B-CNAV2 SatType Parameter

Beidou Satellite PRN	Orbit Constellation	Sat Type (2bits)
C20	MEO	11
C23	MEO	11
C27	MEO	11
C28	MEO	11
C32	MEO	11
C37	MEO	11
C38	IGSO	10
C39	IGSO	10
C40	IGSO	10
C41	MEO	11
C46	MEO	11
C59	GEO	01
C60	GEO	01

2.11 Conclusion

From 2020, beidou navigation satellite system is constructed GNSS for providing global coverage like GPS, GLONASS. It possess interoperability and compatible for integration to other satellite based navigation systems. BDS-3 satellite system signal plans, services B2a signal structure and characteristics are studied. The data and pilot component ranging codes of B2a open service signal are generated and validated in this chapter. Navigation message's ephemeris parameters which are used to compute of satellite PVT algorithm is referred. The non-binary LDPC (96, 48) encoding operation concepts are used for generation of B-CNAV2 navigation message frames of two Message types simulated and validated in Chapter 4.

Chapter 3

Overview of GNSS Spoofing

3.1 Introduction

With the advancement of the Global Navigation Satellite System (GNSS) providing open services to users became more vulnerable to interferences like jamming and spoofing. Spoofing is the type of attack intentionally broadcasting false signals to receivers interpreting that received satellite signals are real. It is the intelligent form of interference by fooling the receiver and difficult to detect a successful attack (Humphreys et. al., 2008). The main aim of spoofing attack is to provide false position to the GNSS receiver by transmitting counterfeit as GNSS signals. An overview spoofing and types of spoofing attacks of GNSS systems, generation of spoofed navigation data for spoofing a static location and evaluation are discussed in this chapter.

3.2 GNSS Spoofing

The modern GNSS systems procure attention to provide safe and secure signals in civilian and military applications. Spoofing is an interference which counterfeits the GNSS signals to deceive the target receiver by providing false position. The PVT can be controlled and changed by this intentional interference. The spoofing attack is effectively implemented, when receiving GNSS signals are weak and tried disrupt the receiver it's PVT. Spoofing attack can be easily implemented for open service signals and they are free to use. But, for military or authentic signals are encrypted and secure. They are difficult to achieve for this type of interference.

As shown in Fig 3.1 open service GNSS signals which are weak in reception with low signal power, are received by the GNSS receiver in the drone. The attacker tries to send false signals to navigate the drone into false positioning i.e. desired/spoofed location. The false signals are strong enough, so that the receiver of a drone locks to these false signals and navigates to desired location set up by the attacker.

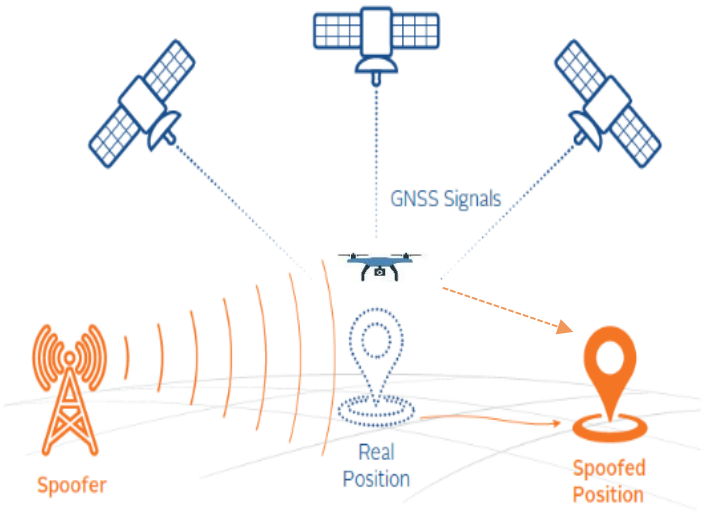


Fig 3.1 Demonstration of GNSS Spoofing

Spoofing shows greater impact in drone technology because it is an unmanned aerial vehicle and automated navigation using real GNSS signals for navigation purpose. This leads to dreadful impact to spoofing. Many spoofing and anti-spoofing techniques were developed and worked for safe and secure navigation from these type interferences (Alexandre et. a., 2017; Bhatti et. al., 2017; Gaspar et. al., 2018; Jahromi et. al., 2012; Kerns et. al., 2014; Shijith et. al., 2017).

3.2 Types of Spoofing Attacks

Mainly, spoofing attacks are divided into three types: simplistic, intermediate and sophisticated.

3.2.1 Simplistic attack using GNSS Signal Simulator

Most of the commercial civilian GNSS receivers are available today are insignificant to spoofing. A simple amplifier and an antenna to a GNSS signal simulator hardware is used to transmit the spoofed signal towards the target receiver which is used in a simplistic spoofing attack. In this type of attack, the simulators broadcast the GNSS signals to desired target receiver for spoofing. The simulator type of attack are cost, size difficulty in synchronization of output with real GNSS signals and ease to detect. GNSS Signal Simulator as shown in Fig 3.1

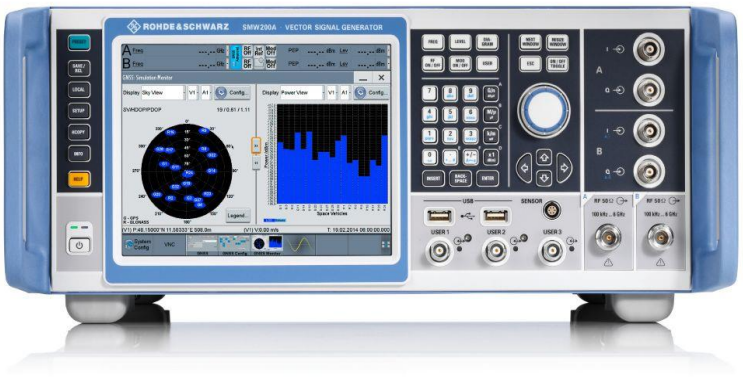


Fig 3.2 GNSS Signal Simulator (Rohde & Schwarz GPS, Glonass, Galileo, BeiDou Receiver)

3.2.2 Intermediate attack using Portable Receiver-Spoofer

In intermediate attack the receiver based spoofer is used to accumulate original GNSS signals for estimation of its own position, velocity and time. Based on these estimations, receiver spoofer generates the GNSS spoofing signals to desired target receiver. The portable receiver spoofer can be placed at distance from the target receiver if the receiving antenna at a static position in performing the attack. Unlike GNSS signal simulators, receiver-spoofer is difficult to detect and able to synchronize the GNSS time to the target antenna as shown in Fig 3.2

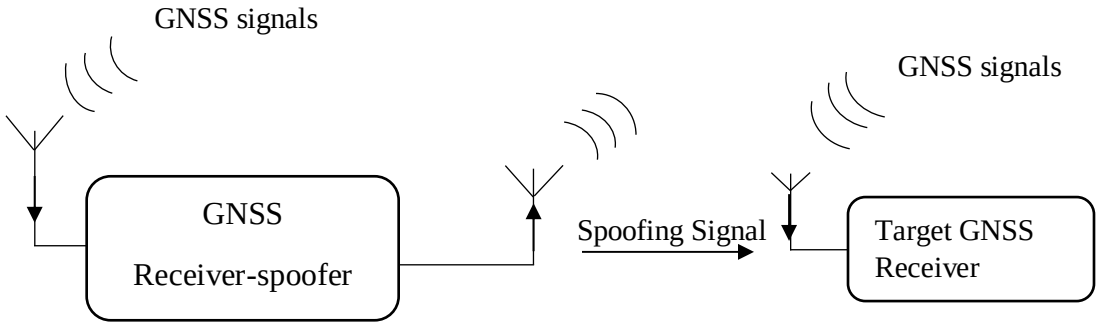


Fig 3.3 Portable Receiver-Based Spoofer (Humphreys, 2008)

3.2.3 Sophisticated attack using Multiple Phase-locked Portable Receiver-Spoofers

The sophisticated attack is the most complex technique among the three attacks and it is an effective type of spoofing attack. This attack overcomes all of the challenges of mounting a single receiver-spoofer attack. This type of technique is expected to know position of antenna of the target receiver to synchronize perfectly with the spoofing signal carrier phase and code phase elements with the original incoming signal. The only defensive technique against this attack is crypto-graphic authentication because it impossible to detect with receiver-based spoofing defenses.

3.4 Generation of Spoofed navigation data

The ephemeris parameters in navigation message are used for generation of spoofed navigation data. To implement a spoofing attack receiver positon and pseuodranges are required. The knowledge of GNSS receiver data processing is important for performing a spoofing attack (Tippenhauer et. al., 2011; Warner et. al., 2012). After the incoming signal with high frequency acquisition gives rough estimates of signal parameters (Sharawi et. al., 2007). The acquisition purpose is to identify all satellites visible to the user. If satellite is visible, the acquisition must determine the frequency and code phase. The code phase refers to the current navigation data block where ranging code begins in which navigation data is included. These parameters are refined into Code tracking and Carrier tracking. After tracking the signal properties in time carrier, ranging codes are refined for navigation data extraction (Kai Borre et. al., 2007). The extracted navigation data in bits is used as input to generate spoofed navigation data and decoding the ephemeris parameters in navigation message for validation by computing satellite positions whether signal is matched as real signal.

3.5 Evaluation of Spoofed navigation data

The Beidou satellites broadcasting ephemeris data in navigation message is transmitted to desired target location for achieving position spoofing (Kang Wang et. al., 2005). The static spoofed position is evaluated by computing pseuodranges from previously computed

satellite positions. The pseuodranges and four satellite positions are input for least squares position estimation method gives target position and satellites azimuthal and elevation angles as output (Borre et. al., 2007).

3.6 Conclusion

Various types spoofing attacks are discussed in this chapter. The generation techniques of spoofing signals using GNSS simulators, portable receiver-based spoofer and multiphase locked receiver-based spoofing devices. Among these simulator based simplest attack using GNSS signal simulator can be easily implemented. With feasibility, the ephemeris parameters of B-CNAV2 navigation message frame is constructed. The spoofed navigation data is generated for a static desired/spoofing location and evaluated by least squares position estimation method using relevant algorithms in Matlab tool.

Chapter 4

Results and Discussion

4.1 Introduction

For generating navigation data, beidou navigation system's RINEX navigation file is used to extract navigation data and ephemeris parameters of each PRN. The set of ephemeris parameters of BDS-3 satellites C20, C23, C27, C28, C32, C37, C38, C39, C40, C41 and C46 is acquired. In this chapter, all beidou satellites of acquired PRN's PVT is computed and plotted their footprints. Also, the BDS-3 system's open service B2a signal navigation message is constructed using ephemeris parameters. For C37 and C38 PRN's navigation message frames are generated and validated. The generated navigation data is evaluated for spoofing application by satellite positions and pseudoranges. The satellites positions of C20, C23, C37, C38 and desired/spoofed location are used to compute pseudoranges. The acquired satellites positions and pseudoranges are given input to least squares position estimation algorithm to estimate desired position.

4.2 Beidou RINEX Navigation file

RINEX navigation file contains the ephemeris data and satellite information. The Beidou navigation satellite system (BDS) navigation data is included in RINEX version 3.04.

IISC00IND_R_20211090000_01D_CN.rnx

```
     3.04           N: GNSS NAV DATA    C: BEIDOU           RINEX VERSION / TYPE
sbf2rin-13.8.0                          20210420 000805 UTC PGM / RUN BY / DATE
IISC                                    MARKER NAME         COMMENT
22306M002                               MARKER NUMBER       COMMENT
  1337936.4550  6070317.1261  1427876.7852                  COMMENT
                                                            END OF HEADER
C02 2021 04 18 23 00 00 7.481523789465E-04-3.086064737090E-11 0.000000000000E+00
     1.000000000000E+00-1.566250000000E+02-2.831903674441E-09-1.597083387654E+00
    -5.232635885477E-06 9.291477035731E-04-2.120155841112E-06 6.493456361771E+03
     8.280000000000E+04-6.984919309616E-08-3.083858556481E+00 3.678724169731E-08
     1.011930103408E-01 5.767187500000E+01-3.797566395998E-01 3.841588589013E-09
     3.375140588153E-10 0.000000000000E+00 7.980000000000E+02 0.000000000000E+00
     2.000000000000E+00 0.000000000000E+00 9.000000000000E-10-1.450000000000E-08
     8.282760000000E+04 0.000000000000E+00
C03 2021 04 18 23 00 00-3.886626800522E-04 3.571543061298E-11 0.000000000000E+00
     1.000000000000E+00-1.335625000000E+02-2.684397530218E-09-2.346349974620E+00
    -4.443340003490E-06 9.271968156099E-04-4.679895937443E-06 6.493345682144E+03
     8.280000000000E+04-1.173466444016E-07 3.103681203249E+00 2.980232238770E-08
     1.057964916943E-01 1.387031250000E+02 9.272711438794E-01 3.791586506226E-09
     2.889406069646E-10 0.000000000000E+00 7.980000000000E+02 0.000000000000E+00
     2.000000000000E+00 0.000000000000E+00 2.300000000000E-09-8.100000000000E-09
     8.282760000000E+04 0.000000000000E+00
```

Fig 4.1 Beidou RINEX Navigation file

IISC00IND_R_20211090000_01D_CN is the RINEX navigation file is used. The file name indicates RINEX Beidou navigation file contains one day's data downloaded from https://cddis.nasa.gov/archive/gnss/data/daily. The header section of this file contains version format, type of navigation data with a satellites system identifier as "C" for BDS and receiver position (Gutner et. al., 2018) as shown in Fig 4.1.

4.2.1 Extraction of Navigation Data

The navigation data is extracted by reading Beidou Rinex Navigation file of one Day data using Matlab tool. The navigation data of Fig 4.2 (a) contains the Satellite number (PRN), Year, Month, Day, Hour, Second. The broadcasting ephemeris data contains C_{rs}, Δn, M_o, C_{us}, eccentricity, $\sqrt{A}$, t_{oe}, C_{ic}, Ω_o, C_{is}, i_o, C_{rc}, ω, $\dot{\Omega}o$, week no, Satellite Health Status and Transmission time of satellite(sec of BDT week) show in Fig 4.2 (b). This data is used in the estimation of satellite position and construction of desired B2a signal navigation message frames for each Beidou satellite.

navdata

1x585 struct with 40 fields

...	prn	year	month	day	hour	minute	second	af0	af1	af2	aode	crs	deltan
27	32	2021	4	19	0	0	0	-9.4490e-04	-1.2414e-11	0	[]	-39.4531	3.7330e-09
28	37	2021	4	19	0	0	0	-8.9973e-04	-9.3650e-12	0	[]	42.3750	3.8016e-09
29	46	2021	4	19	0	0	0	3.0989e-04	-1.7403e-11	0	[]	54.6406	3.7544e-09
30	20	2021	4	19	0	0	0	-9.5713e-04	1.9861e-11	0	[]	-31.8281	3.7784e-09
31	41	2021	4	19	0	0	0	-9.4657e-04	-6.6489e-12	0	[]	-43.5781	3.8352e-09
32	23	2021	4	19	0	0	0	-8.9013e-04	-5.9854e-12	0	[]	39.1094	3.8912e-09
33	10	2021	4	19	0	0	0	-5.4540e-05	5.5831e-12	0	[]	384.3750	1.2804e-09
34	40	2021	4	19	0	0	0	1.5253e-04	3.7845e-12	0	[]	377.0938	7.9646e-10
35	7	2021	4	19	0	0	0	-1.3448e-04	-3.8704e-11	0	[]	373.6250	1.2672e-09
36	9	2021	4	19	0	0	0	5.8581e-04	-2.7454e-11	0	[]	2.0469	1.4483e-09
37	39	2021	4	19	0	0	0	3.0471e-05	3.5172e-13	0	[]	-25.5781	1.3511e-09
38	6	2021	4	19	0	0	0	2.9282e-04	3.9897e-11	0	[]	0.2188	1.4747e-09
39	16	2021	4	19	0	0	0	-7.9089e-04	-1.9941e-11	0	[]	-10.4844	1.3740e-09
40	13	2021	4	19	0	0	0	2.2710e-04	1.5372e-11	0	[]	-405.2031	8.5325e-10
41	2	2021	4	19	0	0	0	7.4804e-04	-3.0927e-11	0	[]	-179.6250	-1.8386e-09
42	60	2021	4	19	0	0	0	3.6100e-07	4.0501e-13	0	[]	-100.0156	-2.1033e-09
43	5	2021	4	19	0	0	0	8.3469e-05	1.9522e-11	0	[]	-163.6094	-2.3712e-09
44	3	2021	4	19	0	0	0	-3.8853e-04	3.5789e-11	0	[]	-147.2031	-1.9369e-09

(a) Navigation data of each PRN

M0	cuc	ecc	cus	art	toe	cic	Omega	cis	i0	crc	omega	Omegadot	idot	cflg12	weekno
-2.2807	-2.1285e-06	6.6815e-04	8.0559e-06	5.2826e+03	86400	-1.0245e-08	-1.4083	-1.9092e-08	0.9640	199.4531	-1.1917	-6.6453e-09	1.4751e-10	[]	798
1.6181	2.1588e-06	5.2644e-04	8.6459e-06	5.2826e+03	86400	-1.9558e-08	0.7007	7.2177e-08	0.9515	181.6563	-0.8749	-6.6978e-09	-1.8501e-10	[]	798
0.0425	2.8242e-06	6.7611e-04	8.3637e-06	5.2826e+03	86400	2.4214e-08	0.7019	2.4680e-08	0.9554	188.7969	-0.1152	-6.7246e-09	-1.7929e-10	[]	798
2.7916	-1.6140e-06	9.0829e-04	8.3214e-06	5.2826e+03	86400	-2.9337e-08	-1.4024	3.2596e-09	0.9654	194.6250	-0.7904	-6.6438e-09	1.9572e-10	[]	798
-1.0761	-2.2030e-06	0.0016	7.8501e-06	5.2826e+03	86400	-4.6566e-10	-1.4042	-2.8871e-08	0.9629	200.7031	-1.6030	-6.7071e-09	1.3608e-10	[]	798
2.6390	1.9693e-06	2.6830e-05	8.3717e-06	5.2826e+03	86400	-8.4750e-08	0.7034	-5.4948e-08	0.9501	187.0156	-1.1234	-6.7192e-09	-2.6644e-10	[]	798
2.7217	1.3047e-05	0.0070	9.5707e-06	6.4936e+03	86400	5.1688e-08	1.5358	4.1444e-08	0.8908	-73.1875	-2.5722	-2.1044e-09	-7.3217e-11	[]	798
3.1330	1.2894e-05	0.0018	9.7654e-06	6.4930e+03	86400	3.3062e-08	1.6485	7.5437e-08	1.0106	-36.0625	-2.9274	-1.8904e-09	3.8216e-11	[]	798
3.1061	1.2351e-05	0.0082	9.8380e-06	6.4934e+03	86400	-1.6764e-08	1.5425	1.6997e-07	0.8890	-75.7656	-2.5401	-2.0262e-09	-1.0000e-10	[]	798
-1.8285	-1.2247e-07	0.0081	1.0733e-05	6.4933e+03	86400	-9.3132e-08	-0.4141	2.0489e-08	0.9510	-85.7188	-2.3529	-1.9419e-09	-1.0358e-11	[]	798
-0.9844	-1.0929e-06	0.0017	1.0953e-05	6.4939e+03	86400	-1.6065e-07	-0.5371	-8.2888e-08	0.9617	-88.8281	-2.9277	-1.8840e-09	7.5717e-11	[]	798
-1.5465	-3.3109e-07	0.0110	1.0479e-05	6.4932e+03	86400	-6.9384e-08	-0.4566	-8.5216e-08	0.9459	-85.3438	-2.1860	-1.9426e-09	3.7144e-11	[]	798
-1.3902	-6.4494e-07	0.0037	1.0725e-05	6.4931e+03	86400	-1.2666e-07	-0.4680	-1.1222e-07	0.9613	-84.5000	-2.4426	-1.8804e-09	3.7859e-11	[]	798
0.5643	-1.3470e-05	0.0038	5.2997e-06	6.4933e+03	86400	1.7509e-07	-2.6018	-1.3411e-07	1.0034	85.3594	-2.5400	-1.9719e-09	9.1075e-11	[]	798
-1.3374	-6.0531e-06	9.2812e-04	-6.3377e-07	6.4934e+03	86400	-4.5635e-08	-2.8729	4.9826e-08	0.1075	16.0313	-0.5880	2.8926e-09	4.0180e-10	[]	798
-2.3887	-3.2499e-06	3.0239e-04	-5.6997e-06	6.4934e+03	86400	-6.7521e-08	2.8622	-3.1199e-08	0.1191	167.3750	0.9392	3.1180e-09	8.9289e-12	[]	798
-2.0078	-5.5097e-06	8.9315e-04	-1.0426e-06	6.4934e+03	86400	-3.4925e-08	-2.9800	8.5682e-08	0.1075	27.2500	-0.2532	3.3798e-09	3.5073e-10	[]	798
-2.0885	-4.9965e-06	9.2900e-04	-3.7430e-06	6.4933e+03	86400	-1.3318e-07	-2.9708	7.9162e-08	0.1099	113.3281	0.7231	3.1187e-09	3.7894e-10	[]	798

(b) Broadcasting Ephemeris data of each PRN

Fig 4.2 Extracted Navigation Data from RINEX navigation file

4.3 Estimation of Beidou satellite positions

The main objective of spoofing operation is to transmit an original like beidou signal to the targeted spoofed location (Riddhi et. al., 2020). It is important to know the spoofed position to transmit the beidou signal. The desired target position is calculated by BDS-3 satellite position with the help of pseudoranges. The satellites position and pseudo ranges can be used to compute the desired/spoofed position to send as real signals. For each beidou satellite, ephemeris parameters are unique and used to estimate the satellite positions for first epoch time (Fig 4.3). The satellite coordinates are calculated according to user algorithm given in the ICD of B2a signal (version 1.0, 2017).

Ephemeris

1x11 struct with 18 fields

Fields	prn	weekno	iode	toe	deltan	Mo	ecc	omega	Omega	io	Omegadot	idot	cis	cic	crs	crc
1	37	798	1	86400	-3.6490e-09	1.6181	5.2644e-04	-0.8749	0.7007	0.9515	-6.6978e-09	-6.6978e-09	7.2643e-08	-1.9558e-08	0.3047	181.6563
2	38	798	1	86400	1.0379e-09	1.8949	0.0015	-2.8168	-2.5967	0.9765	-2.0437e-09	-2.0437e-09	3.7253e-08	2.2911e-07	0.1563	164.5313
3	20	798	1	86400	-3.6722e-09	2.7916	9.0829e-04	-0.7904	-1.4024	0.9654	-6.6438e-09	-6.6438e-09	2.7940e-09	-2.9802e-08	0.0117	194.6250
4	23	798	1	86400	-3.5594e-09	2.6390	2.6830e-05	-1.1234	0.7034	0.9501	-6.7192e-09	-6.7192e-09	-5.4948e-08	-8.4750e-08	-0.2305	187.0156
5	27	798	1	86400	-3.6158e-09	-2.3177	7.1580e-04	0.9309	2.8074	0.9668	-6.9971e-09	-6.9971e-09	3.8184e-08	4.4703e-08	0.1602	300.0313
6	32	798	1	86400	-3.7176e-09	-2.2807	6.6815e-04	-1.1917	-1.4083	0.9640	-6.6453e-09	-6.6453e-09	-1.9558e-08	-1.0245e-08	-0.0820	199.4531
7	39	798	1	86400	1.3511e-09	-0.9844	0.0017	-2.9277	-0.5371	0.9617	-1.8840e-09	-1.8840e-09	-8.2888e-08	-1.6112e-07	-0.3477	-88.8281
8	40	798	1	86400	7.9649e-10	3.1330	0.0018	-2.9274	1.6485	1.0106	-1.8904e-09	-1.8904e-09	7.5437e-08	3.3528e-08	0.3164	-36.0625
9	41	798	1	86400	-3.6154e-09	-1.0761	0.0016	-1.6030	-1.4042	0.9629	-6.7071e-09	-6.7071e-09	-2.8871e-08	0	-0.1211	200.7031
10	46	798	1	86400	-3.6961e-09	0.0425	6.7611e-04	-0.1152	0.7019	0.9554	-6.7246e-09	-6.7246e-09	2.4214e-08	2.4214e-08	0.1016	188.7969
11	28	798	1	86400	-3.5386e-09	1.6999	4.0344e-05	-2.2983	2.8072	0.9667	-6.9892e-09	-6.9892e-09	2.7940e-08	-6.5193e-09	0.1172	302.4063

Fig 4.3 BDS-3 satellites ephemeris data

4.3.1 Computation of BDS PVT

Beidou satellite positions are calculated by the ephemeris parameters obtained from the navigation file and time as inputs. Beidou time of first epoch is calculated by the Year, Month, Day and Hour by conversion of Julian Day Number to BDS week and BDS seconds of week i.e., BDT. The first epoch is computed from the navigation file as 86400 seconds. To estimate satellite position of a particular PRN important steps are followed in flow chart (Fig 4.4).

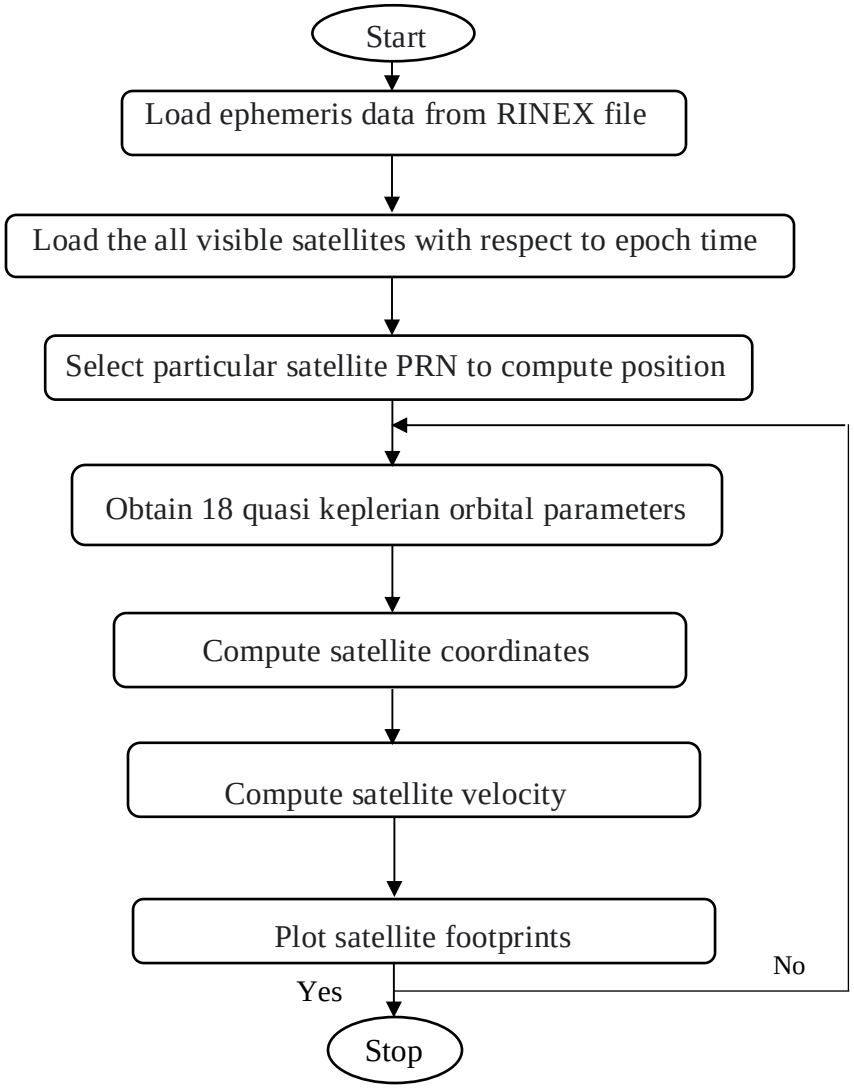


Fig 4.4 Flow chart for computing BDS PVT

In BDS-3 system, only 24 Medium Earth Orbit (MEO) and 3 Inclined Geosynchronous Orbit (IGSO) satellites transmits B2a signal for providing open services. BDS MEO satellites provide global services to users and IGSO satellites are used for regional operation. The Beidou satellite data available in navigation file correspond to 5(GEO), 9(IGSO), 8(MEO) satellites. For first epoch time, BDS-3 system 8 MEO coordinates are presented in Table 4.1. Their location in Latitude, Longitude altitude results are given in Table 4.2. Their respective velocities are given in Table 4.3. Similarly, the corresponding data of 3 IGSO's are given in Tables 4.4, 4.5 and 4.6.

Table 4.1 8 MEO satellite positions in X, Y, Z coordinates

S.No	PRN	X (m)	Y (m)	Z (m)
1	C20	12519452.50275711	13711128.82354881	20864901.24946760
2	C23	-9077380.653944692	13512433.04054209	22666951.91924152
3	C27	599705.7364316145	16387003.62339532	-22596443.48382129
4	C28	-18574613.94014776	16322606.49835052	-12935179.04357799
5	C32	1310576.297104838	26868010.96782424	7472168.360410886
6	C37	8986365.756745795	21472094.78151535	15394325.16450250
7	C41	-10706901.03729400	23659857.80055539	-10156799.56812944
8	C46	22284208.82331291	16685021.32694515	-1654579.712976414

Table 4.2 8 MEO satellites location in Latitude, Longitude, Altitude

S.No	PRN	Latitude(deg)	Longitude(deg)	Altitude(m)
1	C20	48.378794762039830	47.601204550034960	21563634.53291024
2	C23	54.357457709568130	123.8924114836181	21542518.20646717
3	C27	-54.07377313703261	87.904114684370190	21555268.26690472
4	C28	-27.65064179998908	138.6923242767796	21532775.70753201
5	C32	15.546660815271915	87.207421842608380	21541863.84930847
6	C37	33.519515105492490	67.290022091796600	21535194.48571924
7	C41	-21.39035141191960	114.3483908099773	21509949.89064952
8	C46	-3.406587165005087	36.823572161087460	21509453.99539085

Table 4.3 8 MEO satellite velocities

S.No	PRN	X velocity(m/s)	Y velocity (m/s)	Z velocity(m/s)
1	C20	-1403.687801982382	3256.955307608218	-1296.409776783368
2	C23	-2996.093115233361	-2297.160569522892	169.6332978989946
3	C27	-3621.817872224122	911.1215776628521	567.0453149583060
4	C28	-2609.354698752896	-932.1636745341820	2570.213755459915
5	C32	-2193.291876540801	921.1824970065085	-2934.711179412077
6	C37	-3003.388682037486	-364.3208020425277	2264.909221587871
7	C41	-1662.414825141581	-1952.186795584970	-2780.447623434341
8	C46	-1164.058295698583	1860.362014746953	3080.190229771266

Table 4.4 3 IGSO satellites position in X, Y, Z coordinates

S.No	PRN	X (m)	Y (m)	Z (m)
1	C38	-6840639.544919043	23072628.11400838	-34593840.63921975
2	C39	-16766741.80720797	30183472.74907443	24140233.25355726
3	C40	-7074098.614605847	40993181.85646164	7303868.961442960

Table 4.5 3 IGSO satellites location in Latitude, Longitude, Altitude

S.No	PRN	Latitude (deg)	Longitude (deg)	Altitude (deg)
1	C38	-55.202712462787970	106.5141892682318	35777394.62955345
2	C39	34.986803480082300	119.0519144713851	35758639.13660149
3	C40	9.968231271750260	99.790969788698490	35857917.71819416

Table 4.6 3 IGSO satellite velocities

S.No	PRN	X velocity(m/s)	Y velocity (m/s)	Z velocity(m/s)
1	C38	-2751.618806936871	-1331.107966007891	-348.5305721985451
2	C39	-2489.267137175293	57.371150934923660	-1808.500268587749
3	C40	-1555.754392990820	-721.8903736941380	2545.425637209501

Both MEO/IGSO beidou satellites of BDS-3 system provide open services to users which transmit B2a signal frequency. The footprints of B2a signal of C59 and C60 GEO satellites are shown in Fig 4.5. Footprints of C38, C39 and C40 are IGSO satellite footprints are shown in Fig 4.6. BDS-3 system has 24 MEO's, but navigation data of only 8 MEO satellite are available in navigation file and their footprints are shown in Fig 4.7.

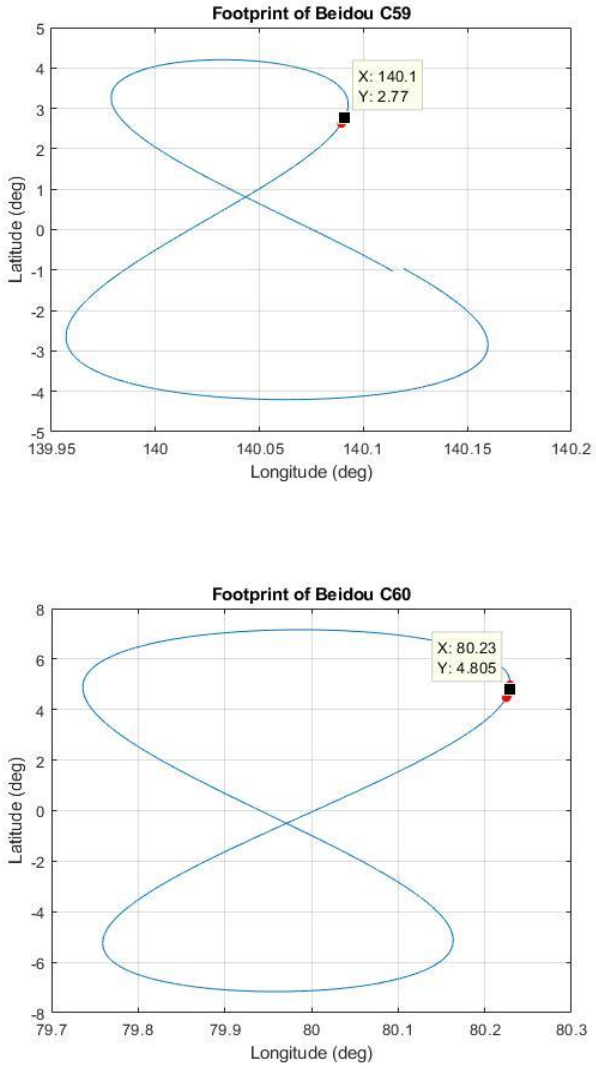


Fig 4.5 Footprints of C59 and C60 GEO satellites

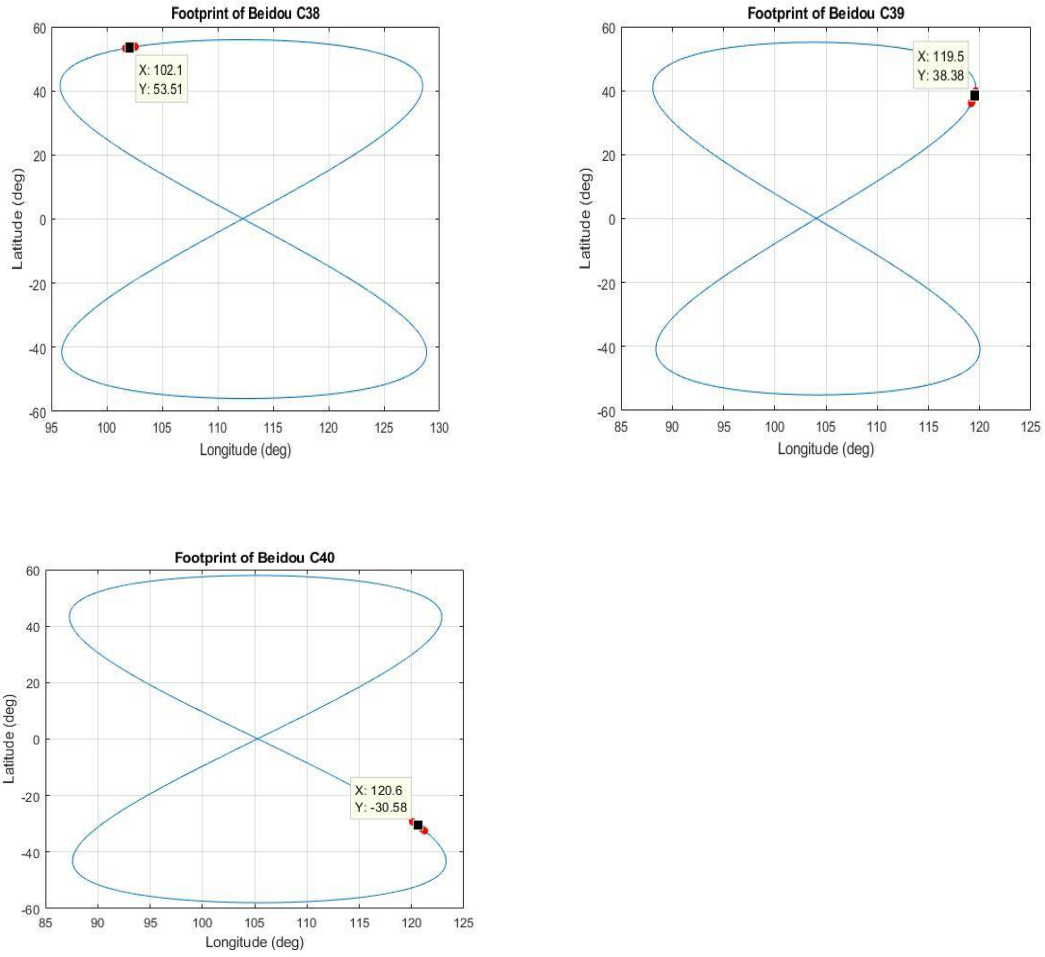


Fig 4.6 Footprints of IGSO C38, C39 and C40 satellites

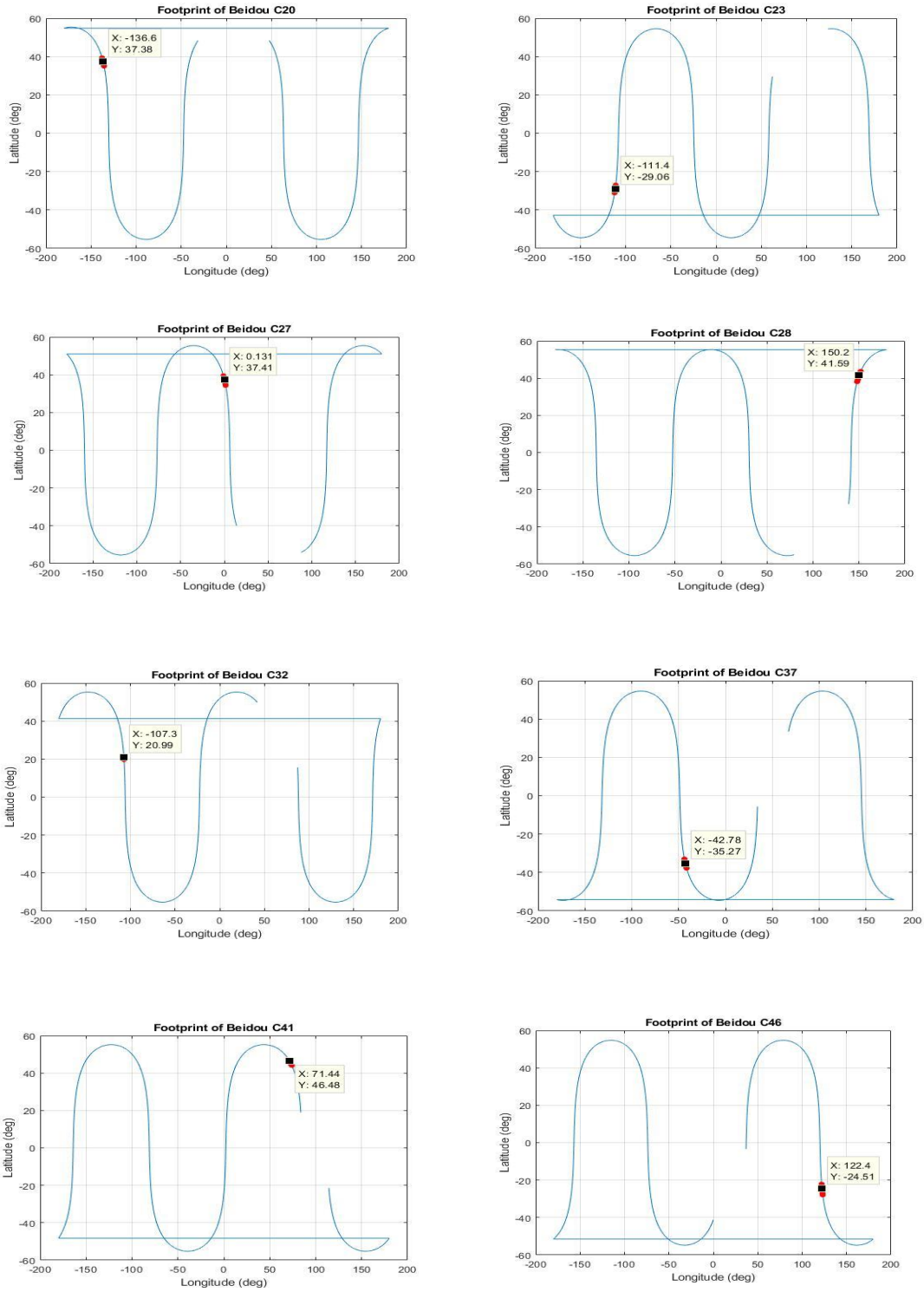


Fig 4.7 Footprints of B2a signal MEO satellites

IGSO satellite positions are validated by crosschecking with the results on altitude and figure of eight shaped footprints (Zaho et. al., 2005). Similarly, MEO satellites are validated by cross checking with altitude (Chen et. al., 2013; He et. al., 2013; Xiaolong et. al., 2018).

4.4 Generation of B2a Navigation Message

B2a signal broadcasts B-CNAV2 navigation message. B-CNAV2 navigation message data provides all the necessary satellite information to the users. The data component of the B2a signal contains modulated B-CNAV2 navigation message data. B-CNAV2 which is generated by satellite ephemeris parameters undergoes non-binary LDPC encoding as shown in Fig 4.8.

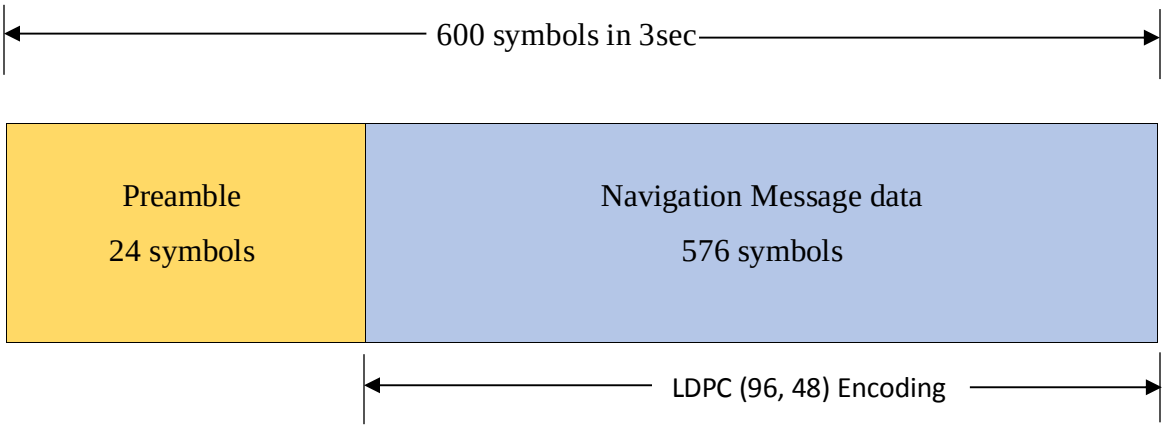


Fig 4.8 B-CNAV2 Navigation Frame

4.4.1 Extraction of B-CNAV2 Navigation Message Data

The first 24 symbols of the B-CNAV2 navigation message frame is preamble (pre). Each frame before LDPC encoding has a length of 288 bits of message data, contains satellite PRN, Message Type which is used to identify what type of message is received, Seconds of week, Cyclic Redundancy check sequence, Week number, Satellite health status, Satellite integrity status flag values of B1C and B2a signals, Signal in space monitoring

accuracy index (SISMAI), Issue of data ephemeris, Satellite Health status, Ephemeris-I of Message Type 10 and Ephemeris-II parameters in Message Type 11 as shown in Fig 4.9.

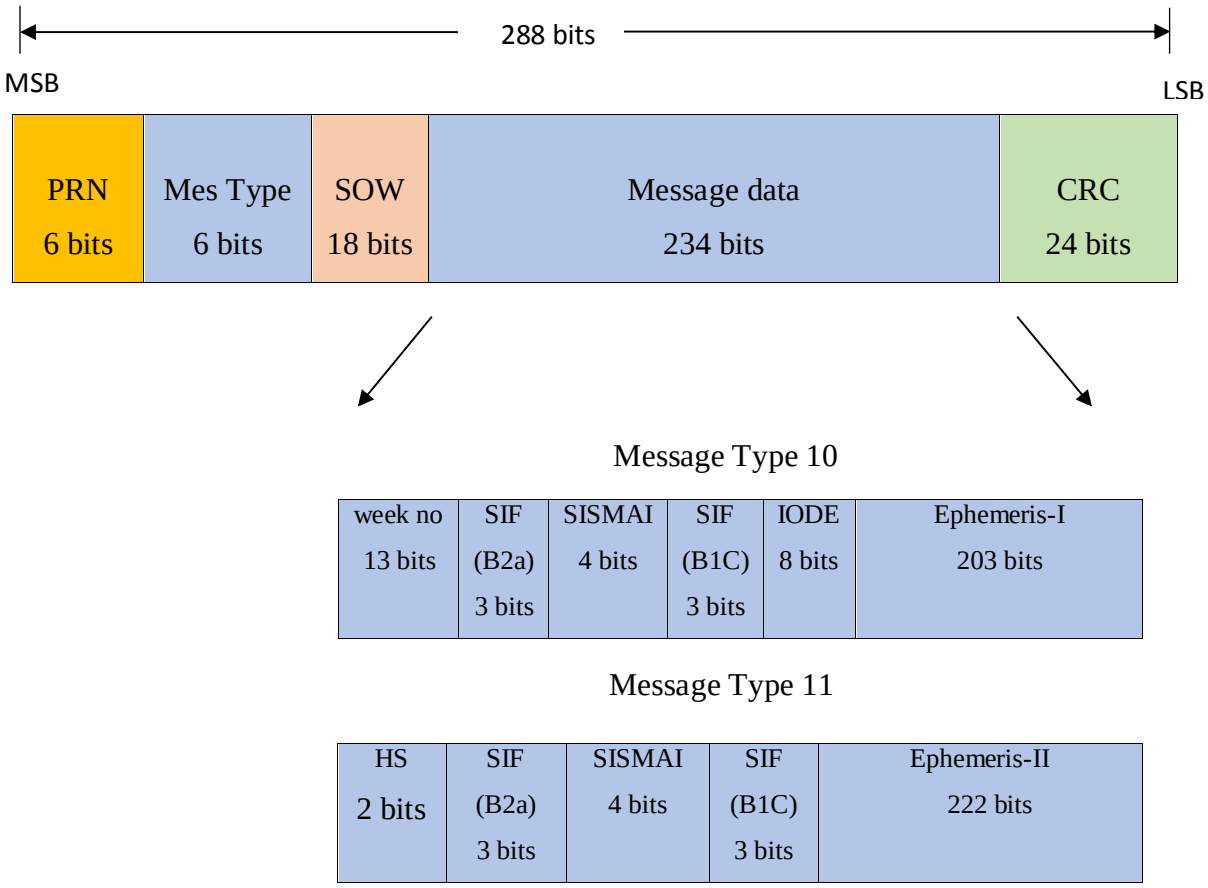


Fig 4.9 B-CNAV2 Navigation Message Frame Structure

While transmission of the B-CNAV2 navigation message, the ephemeris parameters should be transmitted without any error and loss of information. The ephemeris data of each beidou satellite is used to estimate the satellite position. The satellite information and ephemeris data of C37 (MEO) and C38 (IGSO) in Fig 4.3 are the inputs to extraction of navigation message data for encoding. Initially, ephemeris data in decimal values with a sign bit are converted with the help of the Scaling factor. Message type 10 and 11

parameters of C37 (MEO) satellite are shown in Table 4.7 and 4.8. Similarly, message types of 10 and 11 of C38 (IGSO) satellite are shown in Table 4.9 and 4.10.

Table 4.7 Message Type 10 parameters of C37 satellite

Frame parameters	Representation in Binary
PRN (6 bits)	100101
MesType 10 (6 bits)	001010
SOW (18 bits)	101000110000000000
Week Number (13 bits)	0001100011110
IODE (8 bits)	00000010
t_{oe} (11 bits)	00100100000
Sat Type C37(MEO) (2bits)	11
ΔA (26 bits)	11111111111011101101001101
$\dot{A}$ (25 bits)	00101101101010100000000000
Δn_o (17 bits)	01110000111111010
$\Delta \dot{n}_o$ (23 bits)	10110100000111110100001
M_o (33 bits)	010000011110110100101010000000000
e (33 bits)	000000000100010100000000001111010
ω (33 bits)	110111000101101010101011101001010

Table 4.8 Message Type 11 parameters of C37 satellite

Frame Parameters	Representation in Binary
PRN (6 bits)	100101
MesType 11 (6 bits)	001011
SOW (18 bits)	101000110000000000
Health Status (2 bits)	00
Ω_o (33 bits)	000111001000110011111001011010000

i_o (33 bits)	001001101100010011011100000110100
$\dot{\Omega}_o$ (19 bits)	1110110110101111110
$\dot{\iota}_0$ (15 bits)	111101111110100
C_{is} (16 bits)	0000000001001110
C_{ic} (16 bits)	1111111111101011
C_{rs} (24 bits)	000000000010101001100000
C_{rc} (24 bits)	000000001011010110101000
C_{us}(21 bits)	000000010010001000100
C_{uc}(21 bits)	000000000100100001110

Table 4.9 Message Type 10 parameters of C38 satellite

Frame parameters	Representation in Binary
PRN (6 bits)	100110
MesType 10 (6 bits)	001010
SOW (18 bits)	000111111010010000
Week Number (13 bits)	0001100011110
IODE (8 bits)	00000001
t_{oe} (11 bits)	00101000100
Sat Type C38(IGSO) (2bits)	10
ΔA(26 bits)	000011010011110100110010 01
$\dot{A}$(25 bits)	1001110001000001011000111
Δn_o(17 bits)	11010101100111011
$\Delta \dot{n}_o$(23 bits)	10111010111010001110001
M_o(33 bits)	010011010011010011111101111101010
e(33 bits)	000000001100000001001110100110110
ω(33 bits)	100011010011101101110111010100000

Table 4.10 Message Type 11 parameters of C38 satellite

Frame Parameters	Representation in Binary
PRN (6 bits)	100110
MesType 11 (6 bits)	001011
SOW (18 bits)	000111111010010000
Health Status (2 bits)	00
Ω_o (33 bits)	100101100011001101000000100111100
i_o (33 bits)	001001111100100100111010111101010
$\dot{\Omega}_o$(19 bits)	1111101001101001100
$\dot{\iota}_0$ (15 bits)	000001010000010
C_{is} (16 bits)	0000000000101000
C_{ic} (16 bits)	0000000011110110
C_{rs} (24 bits)	111111100101110100110000
C_{rc} (24 bits)	000000001010010010001000
C_{us} (21 bits)	000000000101001100111
C_{uc} (21 bits)	111111100011100100011

4.4.2 Generation of CRC check sequence

In B-CNAV2 navigation message frame, a cyclic redundancy check (CRC) sequence is used to add parity check bits along with message data. PRN (6 bits), MesType (6 bits), SOW (18 bits), Message data (234 bits) of a frame participate in CRC before LDPC encoding. CRC check sequence of 24 bits is generated by generator polynomial of CRC-24 Q i.e., g(*x*) and 264 bits of data as shown in the flow chart (Fig 4.10). The results of C37 (MEO) CRC of Message Type 10 and 11 are shown in Fig 4.11. Similarly, C38 (IGSO) check sequence in Fig 4.12.

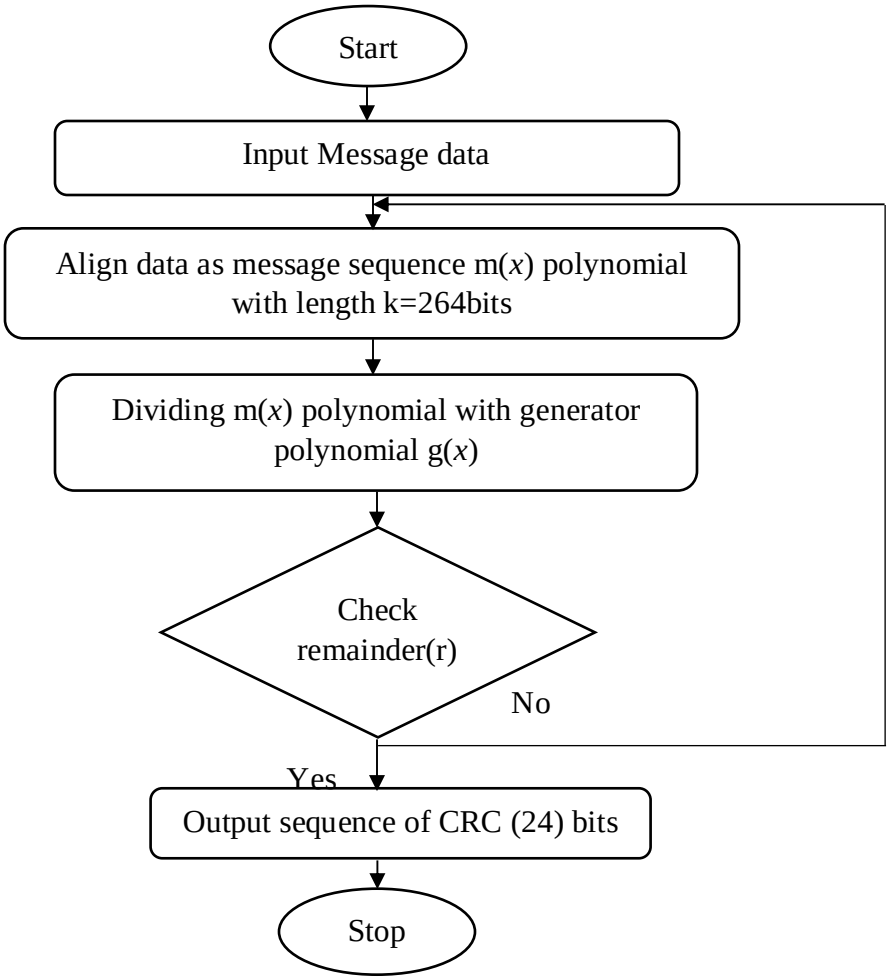


Fig 4.10 Flow chart for CRC sequence

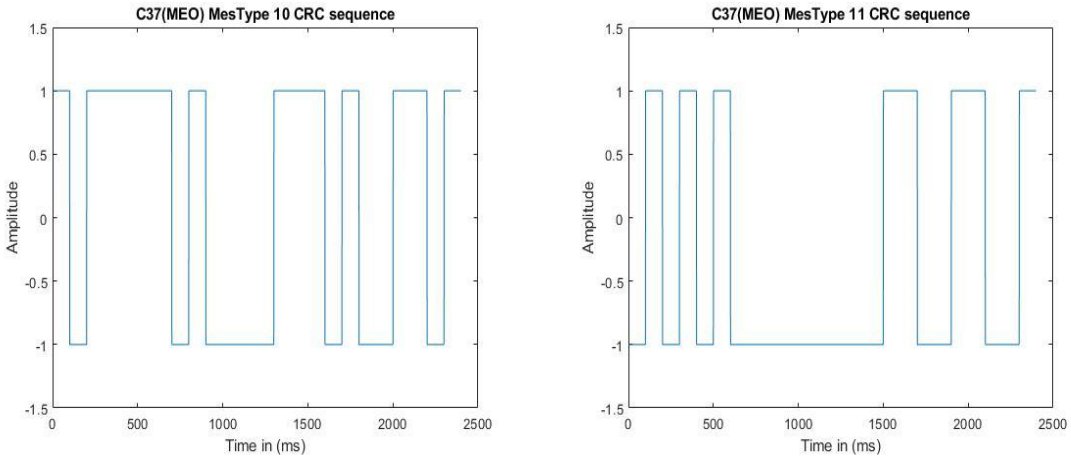


Fig 4.11 CRC check sequence of C37 MesType 10 and 11

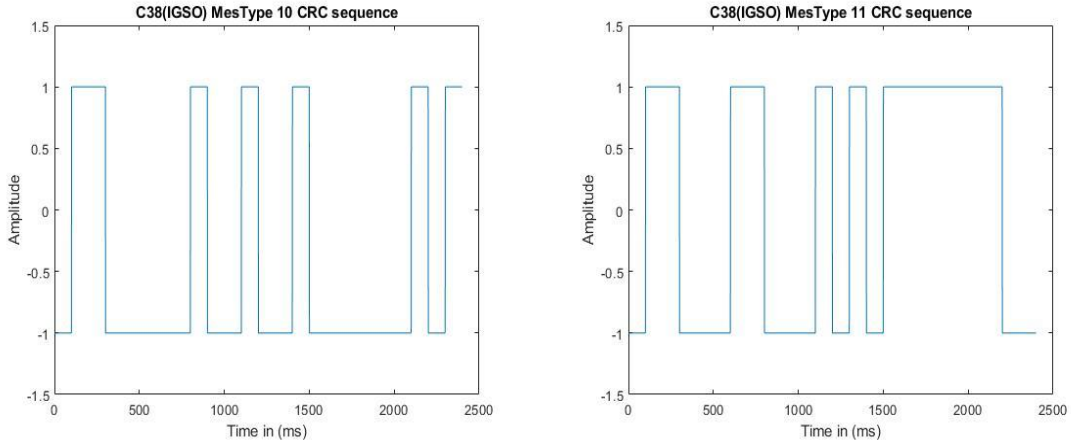


Fig 4.12 CRC check sequence of C38 MesType 10 and 11

The B-CNAV2 navigation messages are encoded with non-binary LDPC encoding. In non-binary LDPC encoding, every 6 bits in binary form of message data composed of one codeword which is defined in Galois Fields GF (2^6) with primitive polynomial $p(x) = 1+x+x^6$ (Jorge et. al., 2006). Each element in Galois field is described by vector and power representation. The vector representation is used for mapping relation between non-binary symbols to binary bits are represented (Appendix A). The input message information of 48 codewords i.e., 288 bits including CRC check sequence 24 bits is input to LDPC encoding.

4.4.3 LDPC (96, 48) encoding of B-CNAV2

B-CNAV2 navigation message data is encoded with Low density parity check (LDPC) code. The input to encoding are information of length k equal to 48 codeword symbols, i.e., 288 bits and check matrix H_{48X96}. LDPC (96, 48) encoding gives a total of 96 codewords i.e., 576 message bits as shown in Fig 4.13. In LDPC (96, 48) encoding, the output contains 48 codewords of information symbols and the other 48 codewords are check symbols. The preamble (pre) of 24 bits are joined with 576 bits gives the one B-CNAV2 navigation message frame which is used to modulate on data component ranging

codes for a unique PRN. C37 (MEO) and C38 (IGSO) satellites' B-CNAV2 navigation message frames of Message Type 10 are shown in Fig 4.14 and 4.15.

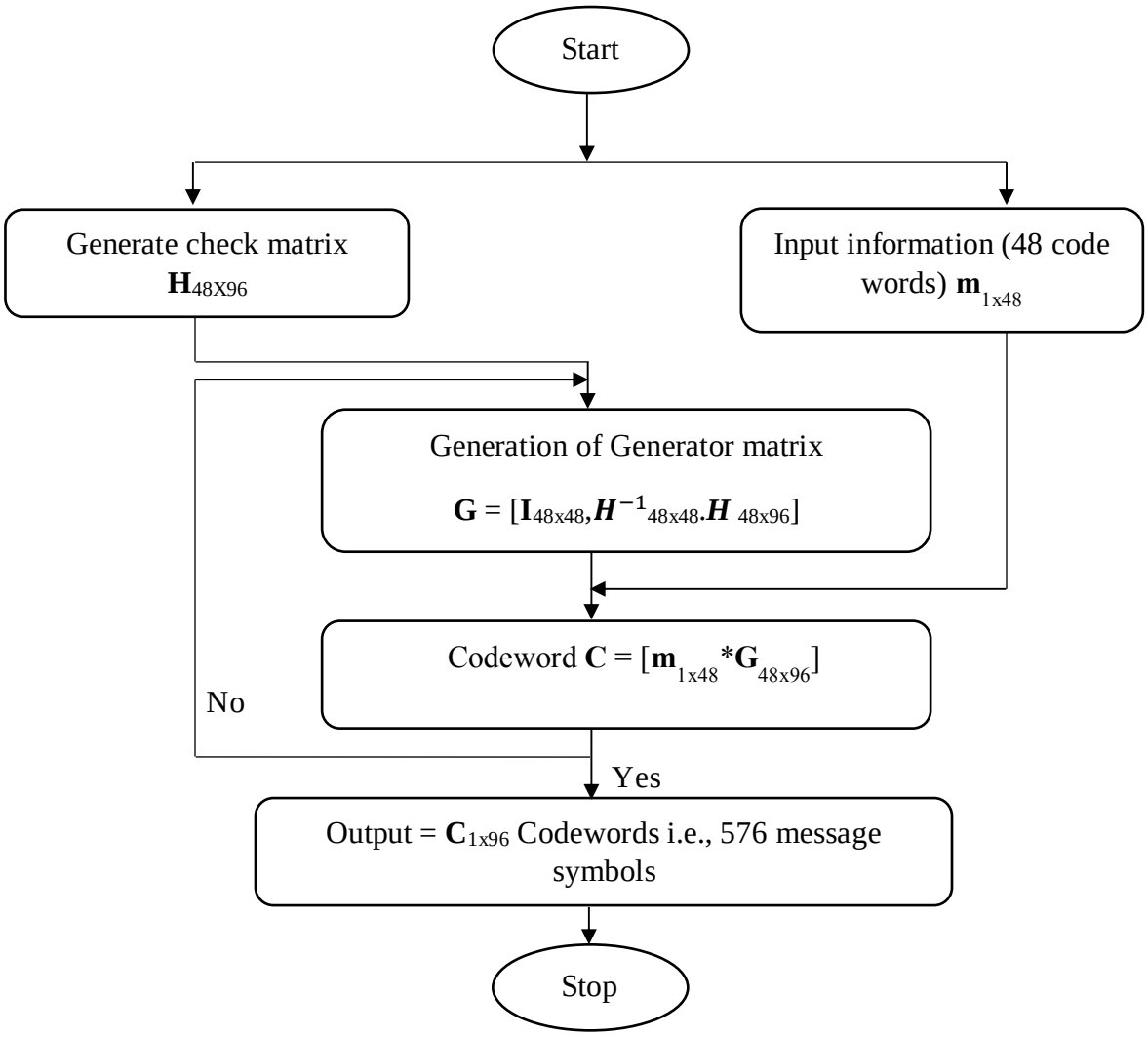


Fig 4.13 Flow chart of LDPC (96, 48) encoding

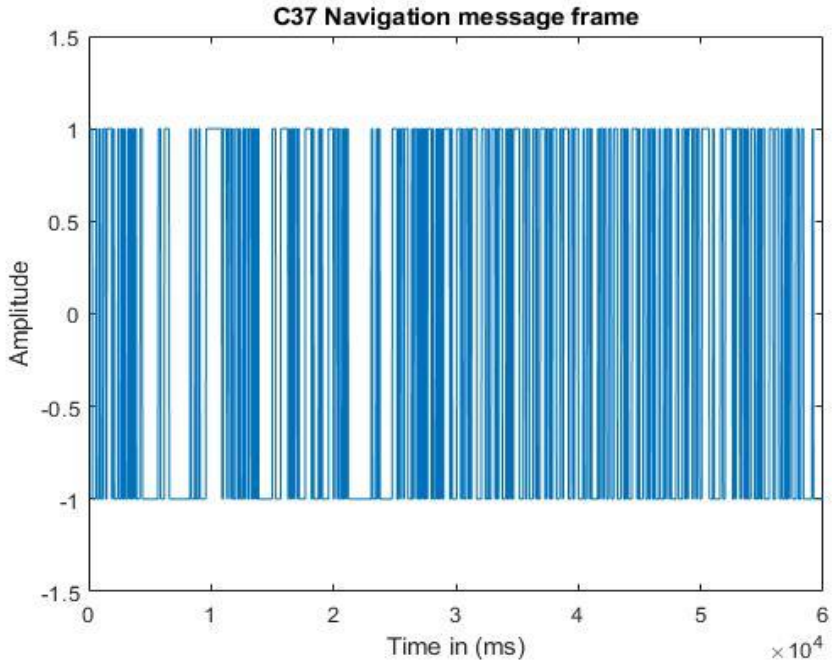


Fig 4.14 C37 satellite B-CNAV2 Navigation message frame

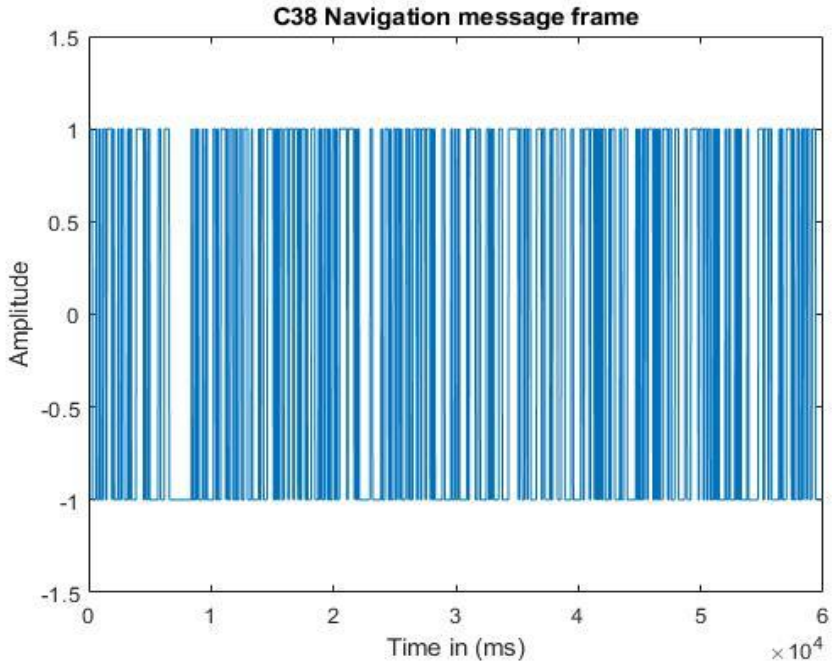


Fig 4.15 C38 satellite B-CNAV2 Navigation message frame

4.5 Generation of spoofed navigation data

The spoofed navigation data is generated by satellite ephemeris parameters in the B-CNAV2 frame. If the navigation message frame is transmitted correctly to the desired target location then spoofing is fully achieved. The spoofed navigation data of a signal is to match the original BDS signal on the spoofing location side. So, all the message data is carefully generated and decoded. The satellite information and ephemeris data is all need to generate spoofed data for first epoch time (Fig 4.16).

Ephemeris

1x11 struct with 18 fields

...	prn	weekno	iode	toe	deltan	Mo	ecc	omega	Omega	io	Omegadot	idot	cis	cic	crs
1	37	798	1	86400	-3.6490e-09	1.6181	5.2644e-04	-0.8749	0.7007	0.9515	-6.6978e-09	-6.6978e-09	7.2643e-08	-1.9558e-08	0.3047
2	38	798	1	97200	1.0379e-09	1.8949	0.0015	-2.8168	-2.5967	0.9765	-2.0437e-09	-2.0437e-09	3.7253e-08	2.2911e-07	0.1563
3	20	798	1	86400	-3.6722e-09	2.7916	9.0829e-04	-0.7904	-1.4024	0.9654	-6.6438e-09	-6.6438e-09	2.7940e-09	-2.9802e-08	0.0117
4	23	798	1	86400	-3.5594e-09	2.6390	2.6830e-05	-1.1234	0.7034	0.9501	-6.7192e-09	-6.7192e-09	-5.4948e-08	-8.4750e-08	-0.2305
5	27	798	1	86400	-3.6158e-09	-2.3177	7.1580e-04	0.9309	2.8074	0.9668	-6.9971e-09	-6.9971e-09	3.8184e-08	4.4703e-08	0.1602
6	32	798	1	86400	-3.7176e-09	-2.2807	6.6815e-04	-1.1917	-1.4083	0.9640	-6.6453e-09	-6.6453e-09	-1.9558e-08	-1.0245e-08	-0.0820
7	39	798	1	86400	1.3511e-09	-0.9844	0.0017	-2.9277	-0.5371	0.9617	-1.8840e-09	-1.8840e-09	-8.2888e-08	-1.6112e-07	-0.3477
8	40	798	1	86400	7.9649e-10	3.1330	0.0018	-2.9274	1.6485	1.0106	-1.8904e-09	-1.8904e-09	7.5437e-08	3.3528e-08	0.3164
9	41	798	1	86400	-3.6154e-09	-1.0761	0.0016	-1.6030	-1.4042	0.9629	-6.7071e-09	-6.7071e-09	-2.8871e-08	0	-0.1211
10	46	798	1	86400	-3.6961e-09	0.0425	6.7611e-04	-0.1152	0.7019	0.9554	-6.7246e-09	-6.7246e-09	2.4214e-08	2.4214e-08	0.1016
11	28	798	1	86400	-3.5386e-09	1.6999	4.0344e-05	-2.2983	2.8072	0.9667	-6.9892e-09	-6.9892e-09	2.7940e-08	-6.5193e-09	0.1172

Fig 4.16 Input for spoofed navigation data

The spoofed navigation data bits in binary are transmitted to desired target location for spoofing attack through navigation messages. The output of generating spoofed navigation data is the navigation bits that are generated by the scaling factor and quantized for every parameter including two's compliment parameters of B-CNAV2 frame. The output of spoofed navigation message data in binary form for all satellites are shown in Fig 4.17.

Navbits

1x11 struct with 18 fields

	prn	weekno	iode	toe	deltan	Mo	ecc	omega	Omega	io	Omegadot	idot	cis	cic	crs
1	'100101'	'0001100011...	'00000001'	'00100100000'	'1000001010...	'0100000111...	'0000000001...	'1101110001...	'0001110010...	'0010011011...	'1110110110...	'1111011111...	'0000000001...	'1111111111...	'0000000001...
2	'100110'	'0001100011...	'00000001'	'00101000100'	'0010001110...	'0100110100...	'0000000011...	'1000110100...	'1001011000...	'0010011111...	'1111101011...	'1111101001...	'0000000000...	'0000000011...	'0000000000...
3	'010100'	'0001100011...	'00000001'	'00100100000'	'1000000111...	'0111000110...	'0000000001...	'1101111111...	'1100011011...	'0010011101...	'1110110111...	'1110110111...	'0000000000...	'1111111111...	'0000000000...
4	'010111'	'0001100011...	'00000001'	'00100100000'	'1000010110...	'0110101110...	'0000000000...	'1101001000...	'0001110010...	'0010011010...	'1110110110...	'1110110111...	'0000000000...	'1111111110...	'1111111111...
5	'011011'	'0001100011...	'00000001'	'00100100000'	'1000001111...	'1010000110...	'0000000001...	'0010010111...	'0111001001...	'0010011101...	'1110110111...	'1110110011...	'0000000000...	'0000000000...	'0000000000...
6	'100000'	'0001100011...	'00000001'	'00100100000'	'1000000001...	'1010001100...	'0000000001...	'1100111101...	'1100011010...	'0010011101...	'1110110111...	'1110110111...	'1111111111...	'1111111111...	'1111111111...
7	'100111'	'0001100011...	'00000001'	'00100100000'	'0010111001...	'1101011111...	'0000000011...	'1000100010...	'1110101000...	'0010011100...	'1111101011...	'1111101011...	'1111111110...	'1111111101...	'1111111110...
8	'101000'	'0001100011...	'00000001'	'00100100000'	'0001101101...	'0111111110...	'0000000011...	'1000100010...	'0100001100...	'0010100100...	'1111101011...	'1111101011...	'0000000001...	'0000000000...	'0000000001...
9	'101001'	'0001100011...	'00000001'	'00100100000'	'1000001111...	'1101010000...	'0000000011...	'1011111010...	'1100011011...	'0010011100...	'1110110111...	'1110110110...	'1111111111...	'0000000000...	'1111111111...
10	'101110'	'0001100011...	'00000001'	'00100100000'	'1000000100...	'0000000110...	'0000000001...	'1111101101...	'0001110010...	'0010011011...	'1110110111...	'1110110110...	'0000000000...	'0000000000...	'0000000000...
11	'011100'	'0001100011...	'00000001'	'00100100000'	'1000011001...	'0100010101...	'0000000000...	'1010001001...	'0111001001...	'0010011101...	'1110110011...	'1110110011...	'0000000000...	'1111111111...	'0000000000...

Fig 4.17 Output of spoofed navigation data

4.5.1 Navigation data decoding

The navigation message data contains of ephemeris parameters of 2's compliment values. The 2's compliment ephemeris parameters as per ICD of B2a signal are to be decoded at receiving side to match original beidou signal (Humphreys et.al., 2008). The ephemeris parameters in binary form are rearranged and converted into decimal value. The true values of ephemeris parameters are obtained by decoded decimal values which are multiplied by respective scaling factor and units. The input for navigation data decoding is generated spoofed navigation data in bits as shown in Fig 4.18.

navbits

11x40 cell

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	'100101'	'0001100011...	'00000001'	'00100100000'	'1000001010...	'0100000111...	'0000000001...	'1101110001...	'0001110010...	'0010011011...	'1110110110...	'1111011111...	'0000000001...	'1111111111...	'0000000000...
2	'100110'	'0001100011...	'00000001'	'00101000100'	'0010001110...	'0100110100...	'0000000011...	'1000110100...	'1001011000...	'0010011111...	'1111101001...	'0000010100...	'0000000000...	'0000000011...	'1111111001...
3	'010100'	'0001100011...	'00000001'	'00100100000'	'1000000111...	'0111000110...	'0000000001...	'1101111111...	'1100011011...	'0010011101...	'1110110111...	'0000100010...	'0000000000...	'1111111111...	'1111111111...
4	'010111'	'0001100011...	'00000001'	'00100100000'	'1000010110...	'0110101110...	'0000000000...	'1101001000...	'0001110010...	'0010011010...	'1110110110...	'1111010001...	'1111111111...	'1111111110...	'0000000000...
5	'011011'	'0001100011...	'00000001'	'00100100000'	'1000001111...	'1010000110...	'0000000001...	'0010010111...	'0111001001...	'0010011101...	'1110110011...	'0000001100...	'0000000000...	'0000000000...	'1111111111...
6	'100000'	'0001100011...	'00000001'	'00100100000'	'1000000001...	'1010001100...	'0000000001...	'1100111101...	'1100011010...	'0010011101...	'1110110111...	'0000011001...	'1111111111...	'1111111111...	'1111111111...
7	'100111'	'0001100011...	'00000001'	'00100100000'	'0010111001...	'1101011111...	'0000000011...	'1000100010...	'1110101000...	'0010011100...	'1111101011...	'0000001101...	'1111111110...	'1111111101...	'1111111111...
8	'101000'	'0001100011...	'00000001'	'00100100000'	'0001101101...	'0111111110...	'0000000011...	'1000100010...	'0100001100...	'0010100100...	'1111101011...	'0000000110...	'0000000001...	'0000000000...	'0000000101...
9	'101001'	'0001100011...	'00000001'	'00100100000'	'1000001111...	'1101010000...	'0000000011...	'1011111010...	'1100011011...	'0010011100...	'1110110110...	'0000010111...	'1111111111...	'0000000000...	'1111111111...
10	'101110'	'0001100011...	'00000001'	'00100100000'	'1000000100...	'0000000110...	'0000000001...	'1111101101...	'0001110010...	'0010011011...	'1110110110...	'1111100000...	'0000000000...	'0000000000...	'0000000000...
11	'011100'	'0001100011...	'00000001'	'00100100000'	'1000011001...	'0100010101...	'0000000000...	'1010001001...	'0111001001...	'0010011101...	'1110110011...	'0000001101...	'0000000000...	'1111111111...	'1111111111...

Fig 4.18 Input of Navigation data decoding

The extracted navigation message data parameters after data decoding are shown in Fig 4.19. These are used to compute satellite position for validation for all acquired PRN's.

decode

11x18 cell

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	37	798	1	86400	-3.6490e-09	1.6181	5.2644e-04	-0.8749	0.7007	0.9515	-6.6978e-09	-6.6978e-09	7.2643e-08	-1.9558e-08	0.3047
2	38	798	1	97200	1.0379e-09	1.8949	0.0015	-2.8168	-2.5967	0.9765	-2.0437e-09	-2.0437e-09	3.7253e-08	2.2911e-07	0.1563
3	20	798	1	86400	-3.6722e-09	2.7916	9.0829e-04	-0.7904	-1.4024	0.9654	-6.6438e-09	-6.6438e-09	2.7940e-09	-2.9802e-08	0.0117
4	23	798	1	86400	-3.5594e-09	2.6390	2.6830e-05	-1.1234	0.7034	0.9501	-6.7192e-09	-6.7192e-09	-5.4948e-08	-8.4750e-08	-0.2305
5	27	798	1	86400	-3.6158e-09	-2.3177	7.1580e-04	0.9309	2.8074	0.9668	-6.9971e-09	-6.9971e-09	3.8184e-08	4.4703e-08	0.1602
6	32	798	1	86400	-3.7176e-09	-2.2807	6.6815e-04	-1.1917	-1.4083	0.9640	-6.6453e-09	-6.6453e-09	-1.9558e-08	-1.0245e-08	-0.0820
7	39	798	1	86400	1.3511e-09	-0.9844	0.0017	-2.9277	-0.5371	0.9617	-1.8840e-09	-1.8840e-09	-8.2888e-08	-1.6112e-07	-0.3477
8	40	798	1	86400	7.9649e-10	3.1330	0.0018	-2.9274	1.6485	1.0106	-1.8904e-09	-1.8904e-09	7.5437e-08	3.3528e-08	0.3164
9	41	798	1	86400	-3.6154e-09	-1.0761	0.0016	-1.6030	-1.4042	0.9629	-6.7071e-09	-6.7071e-09	-2.8871e-08	0	-0.1211
10	46	798	1	86400	-3.6961e-09	0.0425	6.7611e-04	-0.1152	0.7019	0.9554	-6.7246e-09	-6.7246e-09	2.4214e-08	2.4214e-08	0.1016
11	28	798	1	86400	-3.5386e-09	1.6999	4.0344e-05	-2.2983	2.8072	0.9667	-6.9892e-09	-6.9892e-09	2.7940e-08	-6.5193e-09	0.1172

Fig 4.19 Output of navigation data decoding

4.5.2 Validation of Spoofed Navigation data

The spoofed navigation message data is validated by computing satellite position from decoded data. The ephemeris decoded navigation data of four satellites is used to compute the satellite's position for validation. Satellite position values in X, Y, Z coordinates for four beidou satellites are validated by comparing previously calculated satellite position values (Table 4.11).

Table 4.11 Beidou Satellites position in X, Y, Z coordinates

Beidou satellites	X (m)	Y (m)	Z (m)
C20	12519452.50275711	13711128.82354881	20864901.24946760
C23	-9077380.653944692	13512433.04054209	22666951.91924152
C27	599705.7364316145	16387003.62339532	-22596443.48382129
C28	-18574613.94014776	16322606.49835052	-12935179.04357799

4.6 Evaluation of spoofed navigation data

Each beidou satellite transmits its unique ephemeris data. The broadcasted ephemeris data provides the exact location of each satellites, so that receivers can get prior information in order to calculate position (Wang et. al., 2015). The ephemeris data of spoofed navigation data provides intended spoofing location which is evaluated by the four satellite positions and pseudorange measurements by the least-squares position estimation method.

4.6.1 Computation of pseudoranges

The pseudorange is the measured distance between satellites to target spoofing location. For a given set of satellites positions, the broadcasted data is used to compute the spoofed position through trilateration (Kai Borre et. al., 2007). Based on the satellite positions pseudoranges and spoofing position are computed.

Let coordinates of spoofing position are x_r, y_r, z_r in Table 4.12 and x_i, y_i, z_i are the coordinates of beidou satellite positions of C20, C23, C27, C28 are in Table 4.11 gives the four pseudoranges P_1,P_2,P_3,P_4 by substituting in equation 4.1,4.2,4.3 and 4.4(Table 4.13).

Table 4.12 Desired/spoofed position in X, Y, Z coordinates

Desired/spoofed position	Xr(m)	Yr(m)	Zr(m)
	1232875.001502013	5962767.857316440	1894440.540073380

$$P_i = \sqrt{(x_i - x_R)^2 + (y_i - y_R)^2 + (z_i - z_R)^2} \quad \text{where i = 1,2,3,4} \quad \text{- (4.1)}$$

$$P_1 = \sqrt{(x_1 - x_R)^2 + (y_1 - y_R)^2 + (z_1 - z_R)^2} \quad \text{- (4.2)}$$

$$P_2 = \sqrt{(x_2 - x_R)^2 + (y_2 - y_R)^2 + (z_2 - z_R)^2} \quad \text{- (4.3)}$$

$$P_3 = \sqrt{(x_3 - x_R)^2 + (y_3 - y_R)^2 + (z_3 - z_R)^2} \quad \text{- (4.4)}$$

$$P_4 = \sqrt{(x_4 - x_R)^2 + (y_4 - y_R)^2 + (z_4 - z_R)^2} \quad \text{- (4.5)}$$

Table 4.13 Pseudoranges of C20, 23, 27 and 28 satellites

Beidou satellites	Pseudoranges(m)
C20	23394493.13153720
C23	24388440.80824255
C27	26624593.79778191
C28	26824997.51794317

These pseudoranges and satellite positions are given as input to least squares position estimation algorithm to find the spoofed position coordinates for evaluation. The estimated pseudoranges and beidou satellite positions are used for estimating the static spoofing location. From the beidou RINEX navigation file approximate true position of the receiver antenna is used to compare with the desired spoofed position (Table 4.14 and 4.15). The positioning is affected by the estimated desired/spoofing location from ephemeris data from the real location as shown in Fig 4.20 (Wang et. al., 2015).

Table 4.14 Receiver True Position

Receiver	X coordinate (m)	Y coordinate (m)	Z coordinate (m)
True Position	1337936.4550	6070317.1261	1427876.7852

Table 4.15 True Location and Desired Location in Latitude and Longitude

Receiver	Latitude (deg)	Longitude (deg)
True Location	13.021165851928470	77.570375935724870
Desired Location	17.391984300000000	78.318012810000000

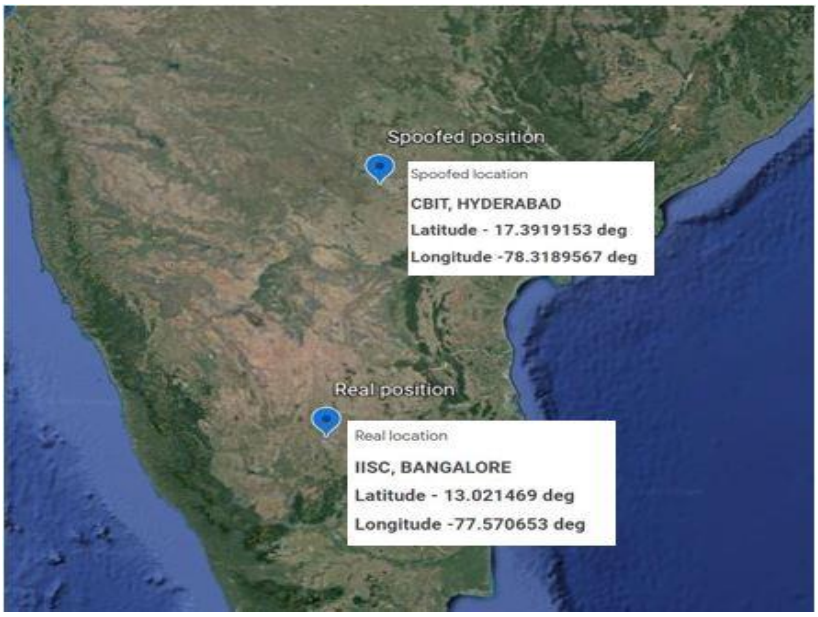


Fig 4.20 True position and Spoofed position in Google Earth view

4.6.2 Estimation of desired/spoofed location using least squares method

The spoofed position is estimated by using least squares position method for evaluation. Least squares method gives target spoofed position for a set of satellite azimuthal and elevation angles (Table 4.16). This method uses pseuodranges and from all calculated satellite position coordinates to estimate desired position.

Table 4.16 Desired Location and Satellite Azimuthal and Elevation angles

Desired Location	Latitude (deg)	Longitude (deg)
	17.392255272702656	78.317428680117940
Beidou satellites	Azimuthal angle(deg)	Elevation angle(deg)
C20	327.9568298744690	40.175110871907790
C23	32.516155778967175	27.529044780323020
C27	174.0908500007334	4.953023132466505
C28	126.6374639783936	3.037524803822290

4.7 Conclusions

The spoofed navigation data for beidou's B2a signal is generated by extracting navigation data from reading beidou navigation file. The necessary ephemeris parameters for each satellite PRN are extracted successfully. The beidou satellite positions, velocities with respect to time of PRN C20,23,27,28,32,37,38,39,40,41 and 46 is computed for one-day data and plotted their footprints. From the shape of the satellite footprints, the MEO or IGSO satellites are determined and crosschecking with altitudes in ICD document. The B2a signal (B-CNAV2) navigation message frames are generated for C37 (MEO) and C38 (IGSO) satellites. The non-binary LDPC error correction encoding is performed to construct navigation message. For non-binary LDPC encoding, the mapping relation between non-binary message symbols to binary bits of message data are defined in Galois field (2^6) is carried out. The spoofed navigation data of the B2a signal generated by the ephemeris parameters of B-CNAV2 navigation message frame. The ephemeris data, of a message frame is decoded for validation. For evaluation of spoofed location, least squares position estimation method is used. With the feasibility of generated navigation data for a static location can be extended to dynamic conditions to counterfeit the original GNSS signal using Hack RF one or Blade RF SDR devices.

Chapter 5
Conclusion and Future work

5.1 Conclusions

Spoofing is an intentional interference on GNSS receivers and is a threat to open service and authorized signal applications. China's new BDS-3 satellite system is respected to take part in global coverage with better functionality like any other GNSS. The GNSS satellites transmit navigation signals to receivers for positioning, navigation services. In view of the recent technological developments in this field of spoofing and anti-spoofing techniques have several applications both in civilian and defence services. A simplistic attack, intermediate attack and sophisticated attack are the main techniques for spoofing operation. Generally, GNSS receivers are not protected and difficult to detect such type of interferences. In this thesis, a navigation data for the spoofing applications is generated and evaluated. BDS-3 system's open service B2a signal of 1176.45 MHz frequency navigation message is constructed using extracted navigation data. This objective is accomplished by reading the beidou RINEX navigation file for ephemeris parameters. The satellite information for one day is extracted from this file. The extracted ephemeris parameters are utilized for generating spoofed navigation data and successfully estimated for a static location. For spoofing a location, BDS-3 satellites position and velocity are computed for individual epoch time. From satellite positions, footprints are plotted to identify the MEO/IGSO satellite types. From the shape and altitudes of footprints, C59, C60 as GEO satellites. C38, C39, C40 as IGSO satellites and similarly for C20, 23,27,28,32,37,41,46, as MEO satellites are identified and validated. B2a signal is transmitted by MEO and IGSO satellites, for signal modulation the data and pilot components of ranging codes are generated and validated to counterfeit as a real signal to GNSS receivers. B-CNAV2 navigation message frame of B2a signal is generated for C37 (MEO) and C38 (IGSO) satellites by non-binary LDPC (96, 48) error correction encoding. For encoding, the navigation message data in binary format is mapped to non-binary symbols which are defined in Galois fields GF (2^6) is performed. The spoofed navigation data is generated by of ephemeris parameters of navigation message frame and validated by navigation data

decoding and satellite position. To evaluate input static desired/spoofed location least squares position estimation algorithm is used. Therefore, from results it can be concluded that the true location in latitude and longitude (13.021469 deg, 77.570653 deg) of a receiver is spoofed to a false position (17.3919153 deg, 78.3189567 deg).

5.2 Future work

In this thesis, the generated navigation data is used for spoofing applications is presented. For estimation of desired/spoofed static location the ephemeris parameters of navigation message frame is used. Further work will include a development of software simulator by integration of applicable algorithms developed in this thesis. The main objectives could be reading the RINEX navigation file of version 3.04, B2a signal ranging code generators for signal modulation and LDPC (96, 48) encoding algorithm for generation of B-CNAV2 navigation message frame. Future work can also focus on spoofing a dynamic location in concurrent by transmitting RF signals using Hack RF or Blade RF SDR hardware devices.

Appendix A

Galois Fields GF (2^6)

Galois field contains not only the binary elements '0' and '1' but also the element α and its powers. For non-binary LDPC encoding, each codeword of 6 bits are defined in GF (2^6) with the primitive polynomial of $p(x) = 1+x+x^6$ (Jorge et. al., 2006). Each element in Galois field can be described by the mapping vector representation and power representation as per ICD of B2a signal.

The Galois filed of GF (2^6) generated by $p(x) = 1+x+x^6$.

Expression representation	Polynomial representation	Vector representation
α^{∞}	0	0 0 0 0 0 0
α^0	1	1 0 0 0 0 0
α^1	α	0 1 0 0 0 0
α^2	α^2	0 0 1 0 0 0
α^3	α^3	0 0 0 1 0 0
α^4	α^4	0 0 0 0 1 0
α^5	α^5	0 0 0 0 0 1
α^6	$1 + \alpha$	1 1 0 0 0 0
α^7	$\alpha + \alpha^2$	0 1 1 0 0 0
α^8	$\alpha^2 + \alpha^3$	0 0 1 1 0 0
α^9	$\alpha^3 + \alpha^4$	0 0 0 1 1 0
α^{10}	$\alpha^4 + \alpha^5$	0 0 0 0 1 1
α^{11}	$1 + \alpha + \alpha^5$	1 1 0 0 0 1
α^{12}	$1 + \alpha^2$	1 0 1 0 0 0
α^{13}	$\alpha + \alpha^3$	0 1 0 1 0 0
α^{14}	$\alpha^2 + \alpha^4$	0 0 1 0 1 0
α^{15}	$\alpha^3 + \alpha^5$	0 0 0 1 0 1
α^{16}	$1 + \alpha + \alpha^4$	1 1 0 0 1 0

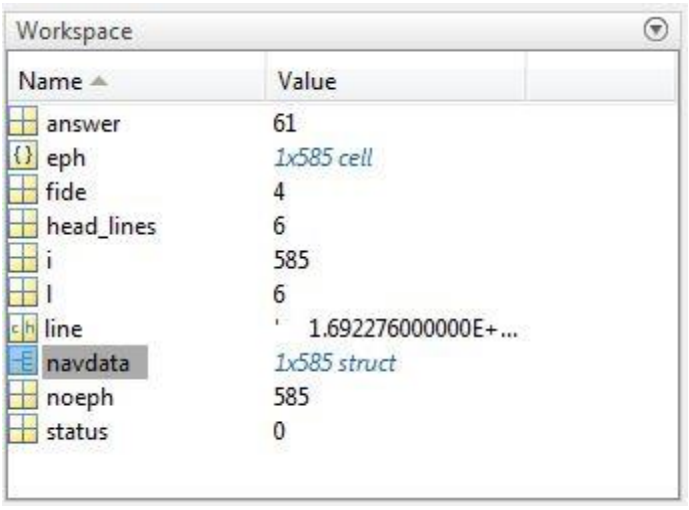
α^{17}	$\alpha + \alpha^2 + \alpha^5$	0 1 1 0 0 1
α^{18}	$1 + \alpha + \alpha^2 + \alpha^3$	1 1 1 1 0 0
α^{19}	$\alpha + \alpha^2 + \alpha^3 + \alpha^4$	0 1 1 1 1 0
α^{20}	$\alpha^2 + \alpha^3 + \alpha^4 + \alpha^5$	0 0 1 1 1 1
α^{21}	$1 + \alpha + \alpha^3 + \alpha^4 + \alpha^5$	1 1 0 1 1 1
α^{22}	$1 + \alpha^2 + \alpha^4 + \alpha^5$	1 0 1 0 1 1
α^{23}	$1 + \alpha^3 + \alpha^5$	1 0 0 1 0 1
α^{24}	$1 + \alpha^4$	1 0 0 0 1 0
α^{25}	$\alpha + \alpha^5$	0 1 0 0 0 1
α^{26}	$1 + \alpha + \alpha^2$	1 1 1 0 0 0
α^{27}	$\alpha + \alpha^2 + \alpha^3$	0 1 1 1 0 0
α^{28}	$\alpha^2 + \alpha^3 + \alpha^4$	0 0 1 1 1 0
α^{29}	$\alpha^3 + \alpha^4 + \alpha^5$	0 0 0 1 1 1
α^{30}	$1 + \alpha + \alpha^4 + \alpha^5$	1 1 0 0 1 1
α^{31}	$1 + \alpha^2 + \alpha^5$	1 0 1 0 0 1
α^{32}	$1 + \alpha^3$	1 0 0 1 0 0
α^{33}	$\alpha + \alpha^4$	0 1 0 0 1 0
α^{34}	$\alpha^2 + \alpha^5$	0 0 1 0 0 1
α^{35}	$1 + \alpha + \alpha^3$	1 1 0 1 0 0
α^{36}	$\alpha + \alpha^2 + \alpha^4$	0 1 1 0 1 0
α^{37}	$\alpha^2 + \alpha^3 + \alpha^5$	0 0 1 1 0 1
α^{38}	$1 + \alpha + \alpha^3 + \alpha^4$	1 1 0 1 1 0
α^{39}	$\alpha + \alpha^2 + \alpha^4 + \alpha^5$	0 1 1 0 1 1
α^{40}	$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^5$	1 1 1 1 0 1
α^{41}	$1 + \alpha^2 + \alpha^3 + \alpha^4$	1 0 1 1 1 0
α^{42}	$\alpha + \alpha^3 + \alpha^4 + \alpha^5$	0 1 0 1 1 1
α^{43}	$1 + \alpha + \alpha^2 + \alpha^4 + \alpha^5$	1 1 1 0 1 1
α^{44}	$1 + \alpha^2 + \alpha^3 + \alpha^5$	1 0 1 1 0 1
α^{45}	$1 + \alpha^3 + \alpha^4$	1 0 0 1 1 0
α^{46}	$\alpha + \alpha^4 + \alpha^5$	0 1 0 0 1 1

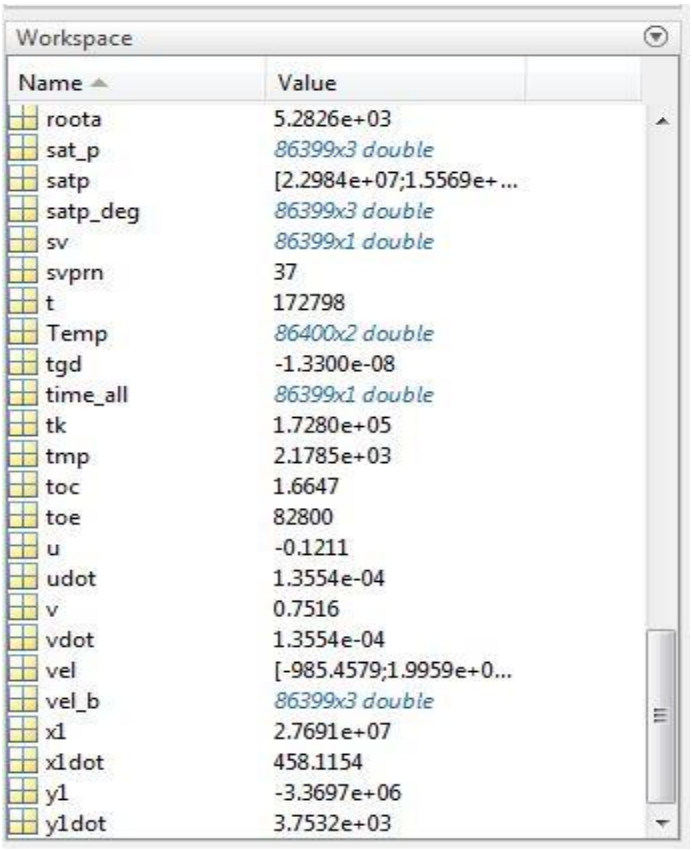
α^{47}	$1 + \alpha + \alpha^2 + \alpha^5$	1 1 1 0 0 1
α^{48}	$1 + \alpha^2 + \alpha^3$	1 0 1 1 0 0
α^{49}	$\alpha + \alpha^3 + \alpha^4$	0 1 0 1 1 0
α^{50}	$\alpha^2 + \alpha^4 + \alpha^5$	0 0 1 0 1 1
α^{51}	$1 + \alpha + \alpha^3 + \alpha^5$	1 1 0 1 0 1
α^{52}	$1 + \alpha^2 + \alpha^4$	1 0 1 0 1 0
α^{53}	$\alpha + \alpha^3 + \alpha^5$	0 1 0 1 0 1
α^{54}	$1 + \alpha + \alpha^2 + \alpha^4$	1 1 1 0 1 0
α^{55}	$\alpha + \alpha^2 + \alpha^3 + \alpha^5$	0 1 1 1 0 1
α^{56}	$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$	1 1 1 1 1 0
α^{57}	$\alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5$	0 1 1 1 1 1
α^{58}	$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5$	1 1 1 1 1 1
α^{59}	$1 + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5$	1 0 1 1 1 1
α^{60}	$1 + \alpha^3 + \alpha^4 + \alpha^5$	1 0 0 1 1 1
α^{61}	$1 + \alpha^4 + \alpha^5$	1 0 0 0 1 1
α^{62}	$1 + \alpha^5$	1 0 0 0 0 1

Appendix B

User Manual

To fulfill the objectives following programs are developed and simulated using MATLAB tool.

Aim	Reading a RINEX navigation file of version 3.04.
Purpose	To extract navigation data and storing ephemeris parameters of each PRN in matrix.
Syntax	navdata=struct('prn','year','month','day','hour','minute','second' 'af0','af1','af2','aode','crs','deltan','M0','cuc','ecc', 'cus','art','toe','cic','Omega','cis','i0','crc','omega', 'Omegadot', 'idot','cflg12','weekno','pflg12', 'svaccuracy','svhealth','tgd','aodc','transmit'); Input: Beidou's RINEX navigation file (IISC00IND_R_20211090000_01D_CN.rnx) Output: 1.Extracted Navigation data for one day in workspace. 2. Ephemeris parameters for each PRN.  Fig 1. Extracted Navigation data in matrix

Aim	Computation of BDS satellite PVT
Purpose	To compute pseudoranges and identify SatType which is used in constructing B-CNAV2 navigation message parameter for each PRN.
Syntax	bdssatpos=satpos(time, ephemeris); Input: 1.BDT(Beidou Time) for first epoch 2.Ephemeris parameters of each PRN Output: 1.Satellite Position in X,Y,Z coordinates 2. Satellite Location in Lat(deg), Lon(deg), Alt(m) 3.Satellite Velocity in m/s  Fig 2. Beidou satellite PVT
Subroutine	juldayeas.m, bds_time.m, bdscheck_t.m, ecef2lla.m

Subroutine 1: juldayeas.m

Purpose	Conversion of given date in RINEX navigation file to Julian day.
Syntax	jd= juldayeas(y,m,d,h); Input : y=Year m=Month d=Day h=hour Output: jd = Julian Day Number

Subroutine 2: bds_time.m

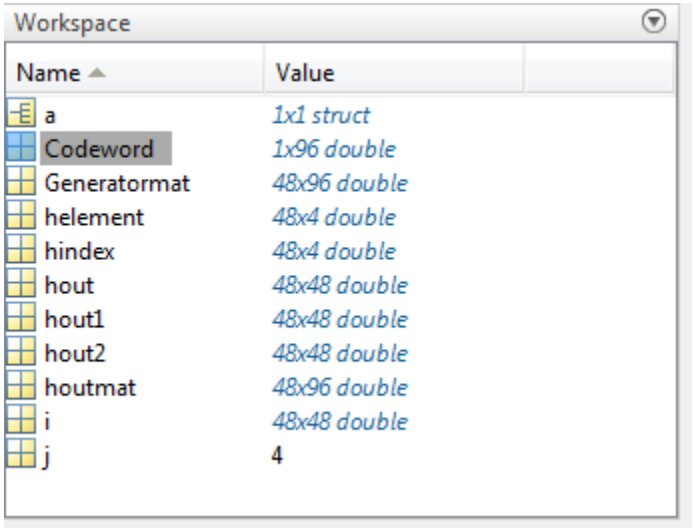
Purpose	Conversion of Julian Day Number to BDS week and Seconds of week (SOW) i.e. BDT (Beidou Time).
Syntax	[week,sec_of_week] = bds_time(jd); Input: jd= Julian Day Number Output: 1. BDS week 2. Seconds of week (SOW) i.e. BDT

Subroutine 3: bdscheck_t.m

Purpose	To avoid week crossovers because BDT week reported in RINEX navigation files are continuous numbers without roll over. BDT week roll over after week 8191.
Syntax	t= bdscheck_t (t); Input: t = BDT time of signal transmission toe = ephemeris reference time Output: tk = total time difference between t and toe

Subroutine 4: ecef2lla.m

Purpose	To plot the footprint of PRN's and crosscheck the satellite location values with altitudes of MEO/IGSO.
Syntax	satp_deg=ecef2lla(satpos); Input: satellite position values in X, Y, Z coordinates Output: Satellite location in Latitude(deg), Longitude (deg), Altitude(m)

Aim	Generation of a B-CNAV2 navigation message
Purpose	To counterfeit as GNSS navigation message signal to target receivers.
Syntax	encode=ldpcenc(codeoutput); Input: 1. Parity check matrix ($H_{48\times96}$) 2. CRC check sequence 3. Non-binary message information matrix ($m_{1\times48}$) 4. Generator matrix ($G_{48\times96}$) Output: 1.Codeword matrix ($C_{1\times96}$) = $m_{1\times48}$.*$G_{48\times96}$  Fig 3. Codeword matrix

Subroutine	check_matrix.m, factor.m, crc24q.m

Subroutine 1: check_matrix.m

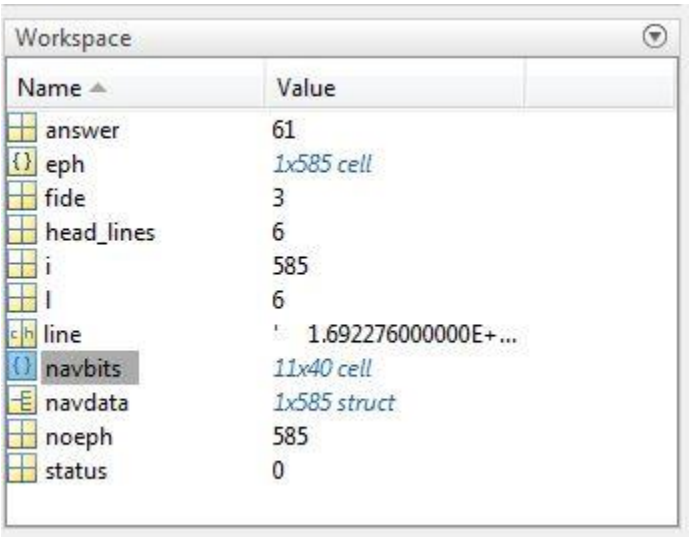
Purpose	To generate LDPC sparse matrix.
Syntax	houtmat (i, hindex(i, j))=helement (i, j); Input : 1. hindex matrix (hindex $_{48\times4}$) 2. helement matrix (helement $_{48\times4}$) Output: houtmatrix = hout ($_{48\times96}$)

Subroutine 2: factor.m

Purpose	Conversion of ephemeris data in decimal values with a sign bit to binary format
Syntax	bin=factor(org, factor, i); Input : org = ephemeris parameter factor = scaling factor of the parameter i= no of bits in representation output: binary bits

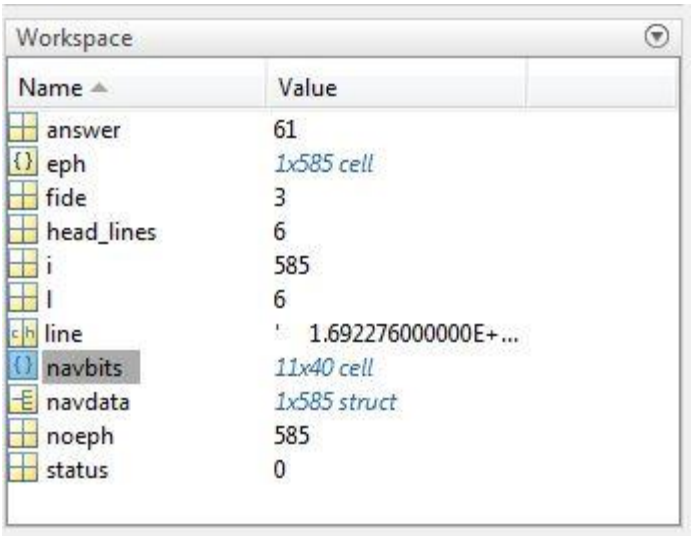
Subroutine 3: crc24q.m

Purpose	To generate parity check sequence for every message frame.
Syntax	msg=('NavMesdata in bits'); Input : 1. PRN (6 bits) 2. MesType (6 bits) 3. SOW (18bits) 4. Messagedata (234 bits) Output: Parity check sequence (24 bits)

Aim	Generation of spoofed navigation data
Purpose	To generate navigation data in binary bits
Syntax	navbits{i, j}=factor(eph, scaling, nobits); Input : 1.Ephemeris parameters 2. Scaling factor 3. no of bits in representation Output: Navigation bits  Fig 4. Navigation data in bits
Subroutine	factor.m

Aim	Validation of spoofed navigation data
Purpose	To validate navigation data by data decoding

Syntax	decode(i).eph = bin2dec(navbits{i,1});
	decode(i).eph= twosComp2dec(navbits{i, 1})*2^(-j);
	
	Inputs: 1.Ephemeris parameters
	2. navbits
	3. j= no of bits representation
	
	output: Navigation decoded data

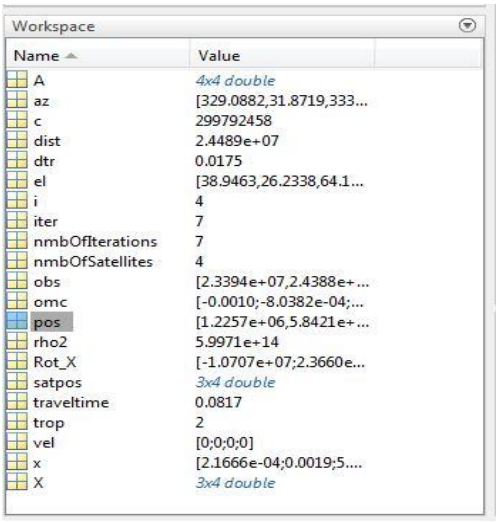
	 Fig 5. Navigation data in bits
Subroutine	bin2dec.m, twosComp2dec.m

Subroutine 1: bin2dec

Purpose	convert text representation of binary number into decimal number
Syntax	bin2dec('binarystring'); Input: binary string Output: decimal number

Subroutine 2: twosComp2dec

Purpose	convert binary number of two's complement with a sign bit number to decimal number
Syntax	intNumber = twosComp2dec(binaryNumber) Input: binary number Output: Decimal number

Aim	To estimate the desired location by Least Squares Position Algorithm
Purpose	To estimate the desired/spoofed location.
Syntax	[pos, el, az,] = leastSquarePos(satpos, pseudoranges); Input: 1.Satellite position in X, Y, Z coordinate 2. Pseudoranges of each satellite (P_1,P_2,P_3,P_4) Output: 1. Desired/Spoofed position 2. Satellites azimuth angles (deg) 3. Satellites elevation angles (deg)  Fig 6. Estimation of Desired/spoofed position
Subroutine	e_r_corr.m, topcent.m, togeod.m

Subroutine 1: e_r_corr.m

Purpose	To return rotated satellite ECEF coordinates due to Earth rotation during signal travel time.
Syntax	X_sat_rot = e_r_corr(travel time, X_sat) Input: 1. Travel time 2. Satellite Positions Output: Corrected satellite positions (do to earth rotation)

Subroutine 2: topocent.m

Purpose	To find Azimuthal and Elevation angels of the satellites
Syntax	[Az, El, D] = topocent(X,dx) Input: Satellite positions Satellite corrected positions Output: D vector length in units like the input Az azimuth from north positive clockwise, degrees El elevation angle, degrees

Subroutine 3: togeod.m

Purpose	To calculate geodetic coordinates latitude, longitude, height given cartesian coordinates X,Y,Z, and reference ellipsoid values semi-major axis and the inverse flattening
Syntax	[dphi,dlambda,h] = togeod(a,finv,X,Y,Z) Input: 1. Semi-major axis 2. satellite positions in X, Y, Z 3. finv = inverse flattening Output: Geodetic coordinates in latitude, longitude, height

References

[1] Alexandre V, Samama N, Thierry T,(2017) "Influence of GNSS spoofing on drone inautomatic flight mode" *ITSNT , 4th International Symposium of Navigation and Timing* , November, Toulouse, France. pp.1 - 9.

[2] Bhatti, J.; Humphreys, T.E. (2017) Hostile control of ships via false GPS signals: Demonstration and detection. Navigation, 64, 51–66.

[3] Bhuiyan M. Z. H., S. Söderholm, S. Thombre, L. Ruotsalainen, H.Kuusniemi, (2014)"Overcoming the Challenges of Beidou Receiver" Implementation, Computer Science, Basel, Switzerland Sensors November.

[4] Chinese Satellite Navigation Office. Beidou navigation satellite system signal in space interface control document open service signal B2a (version 1.0); December 2017.

[5] Chinese Satellite Navigation Office. Development of the Beidou navigation satellite system (version 4.0); December 2019.

[6] ChengJun Li, Yi Qian, Mingquan Lu and Zhengming Feng,(2008). "The design and implement of GPS software simulation platform," Asia Simulation Conference -7th International Conference on System Simulation and Scientific Computing, pp. 186-191, doi: 10.1109/ASC-ICSC.2008.4675353.

[7] Claude Berrou "Codes and Turbo Codes" Springer-Verlag Paris (2010) https://doi.org/10.1007/978-2-8178-0039-4

[8] Deergha Rao .k, Channel Coding Techniques for Wireless Communications, Springer India (2015) https://doi.org/10.1007/978-81-322-2292-7

[9] Duc Minh Truong, Trung Thanh Tran, Thuan Dinh Nguyen and Tung Hai Ta(2013), "Recent results in receiving and decoding signals from the Beidou system," *2013* International Conference on Localization and GNSS (ICL-GNSS), 2013, pp. 1-4, doi: 10.1109/ICL-GNSS.2013.6577255.

[10] Gao Y, Yao Z, Lu M. Design and 'Implementation of a real-time software receiver for BDS-3 signals'' (2019). Wiley Online Library, Navigation ;15. https://doi.org/10.1002/navi.29

[11] Gaspar J., Ferreira R., Sebastião P. and Souto N.,(2018) "Capture of UAVs Through GPS Spoofing," *Global Wireless Summit (GWS)*, Chiang Rai, Thailand, pp. 21-26,

doi: 10.1109/GWS.2018.8686727

[12] Grewal, M.S., Andrews, A.P. and Bartone, C.G. (2020). GNSS Signal Structure, Characteristics, and Information Utilization. In Global Navigation Satellite Systems, Inertial Navigation, and Integration2020 John Wiley & Sons, Inc https://doi.org/10.1002/9781119547860.ch4

[13] Gallager .R, "Low-density parity-check codes," in *IRE Transactions on Information Theory*, vol. 8, no. 1, pp. 21-28, January 1962, doi: 10.1109/TIT.1962.1057683.

[14] Gurtner, W., L. Estey (2007): "RINEX: The Receiver Independent Exchange Format Version 3.04". https://files.igs.org/pub/data/format/rinex304.pdf

[15] Jafarnia-Jahromi A., Broumandan A., Nielsen J. and Lachapelle G.,(2012) "GPS vulnerability to spoofing threats and a review of anti-spoofing techniques", *Int. J. Navig. Observation*, vol. 2012, May.

[16] Jorge Castineria Moreira, Patrick Guy Farrell- Essentials in Error-Control coding: (2006).Appendix B: Galois Fields GF (q), John Wiley & Sons Ltd Publications.

[17] Kai Borre, Dennis Akos, Nicolaj Bertelsen, Peter Rinder,Soren Holdt Jensen- A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach, Birkhauser Publications- 2007.

[18] Kaplan, E.D., and C.J. Hegarty (2006) Understanding GPS Principles and applications 2nd edition, Artech House, Boston, London.

[19] Kang Wang, Shuhua Chen, and Aimin Pan (2015). "Time and Positioning spoofing with open source projects'', Black Hat Europe.

[20] Kerns.A.J, Shepard D.P., Bhatti J.A., Humphreys T.E.,(2014) "Unmanned Aircraft Capture and Control via GPS Spoofing," Journal of Field Robotics, 31(4): 617–636, 2014.

[21] Larcom J. A. and H. Liu, (2013)"Modeling and characterization of GPS spoofing," IEEE International Conference on Technologies for Homeland Security (HST), *2013*, pp. 729-734, doi: 10.1109/THS.2013.6699094.

[22] Li, Y., Shivaramaiah, N.C. & Akos, D.M. (2019) "Design and implementation of an open- source BDS-3 B1C/B2a SDR receiver". *GPS Solut* **23,** 60,

[23] Lina He , Maorong Ge , Jiexian Wang , Jens Wickert and Harald Schuh (2013) "Experimental Study on the Precise Orbit Determination of the BeiDou Navigation Satellite System" *Sensors 13*, 2911-2928; doi:10.3390/s130302911

[24] Liang Chen, Wenhai Jiao, Xiaorui Huang, Changjiang Geng, Lun Ai, Lu Lu, Zhigang Hu (2013) "Study on Signal-In-Space Errors Calculation Method and Statistical Characterization of BeiDou Navigation Satellite System" China Satellite Navigation Conference (CSNC) 2013 Proceedings,Springer, Berlin, Heidelberg. https://doi.org/10.1007/978- 3-642-37398-5_39

[25] Lu X., X. Guo, S. Guo, X. Li, K. Jiang and J. Morton, (2020)"Update on BeiDou Navigation Satellite System and PNT System," *2020* IEEE/ION Position, Location and Navigation Symposium (PLANS), pp. 392-398, doi:10.1109/PLANS46316.2020.9109887.

[26] Magiera J.,(2012)"Design and implementation of GPS signal simulator," International Conference on Localization and GNSS.

[27] Meng, Qian, L. Hsu, Bing Xu, Xiapu Luo and A. el-Mowafy.(2019) "A GPS Spoofing Generator Using an Open Sourced Vector Tracking-Based Receiver." *Sensors (Basel, Switzerland)* 19: n. pag.

[28] Montgomery, P.Y., T.E. Humphreys, and B.M. Ledvina (2009) "Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-antenna Receiver Defense Against a Portable Civil GPS Spoofer" in Proceedings of ION ITM 2009, Jan 26-28, Anaheim, CA, pp. 124-130

[29] Montenbruck, O., Hauschild, A., Steigenberger, P. *et al.* (2013) Initial assessment of the COMPASS/BeiDou-2 regional navigation satellite system. *GPS Solut* **17,** 211–222. https://doi.org/10.1007/s10291-012-0272-x

[30] Ma X., K. Yu, X. He, J. -P. Montillet and Q. Li, (2020)"Positioning Performance Comparison Between GPS and BDS With Data Recorded at Four MGEX Stations," in *IEEE Access*, vol. 8, pp. 147422-147438, doi: 10.1109/ACCESS.2020.3015490.

[31] Psiaki M. L. and T. E. Humphreys (2016), "GNSS Spoofing and Detection," in *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258-1270, June.

[32] Riddhi V. Karpe, Dr. Sukanya Kulkarni(2020), "Software Defined Radio based Global Positioning System Jamming and Spoofing for Vulnerability Analysis" in

International Conference on Electronics and Sustainable Communication Systems (ICESC), July.

[33] Sharawi M. S. and O. V. Korniyenko (2007), "Software Defined Radios: A Software GPS Receiver Example," *IEEE/ACS* International Conference on Computer Systems and Applications, pp. 562-565, doi: 10.1109/AICCSA.2007.370937.

[34] Shijith, N., Poornachandran, P., Sujadevi, V. G., & Dharmana, M. M. (2017) "Spoofing technique to counterfeit the GPS receiver on a drone"International Conference on Technological Advancements in Power and Energy (TAP Energy). IEEE.

[35] Todd E. Humphreys, Brent M. Ledvina, Mark L. Psiaki, Brady W. O' Hanlon and Paul M. Kintner,Jr., (2008) "Assessing the spoofing threat: Development of a Portable GPS Civilian Spoofer'' .Proceedings of the 21st International Technical Meeting of the satellite Division of the Institute of Navigation,September.

[36] Tippenhauer, Nils Ole, C. Pöpper, Kasper Bonne Rasmussen and S. Capkun.(2011) "On the requirements for successful GPS spoofing attacks." *CCS '11*.

[37] Warner, J. S., R. Johnston and Cpp Los Alamos.(2012) "A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing."

[38] Wang J., \. Xi and J. Liu (2010), "The design of GPS IF signal software simulator, International Symposium on Signals, Systems and Electronics, pp. 1- 3, doi: 10.1109/ISSSE.2010.5607059.

[39] Wang, F., Hu, C., Wu, S. *et al.* (2020) Research on BeiDou anti-spoofing technology based on comprehensive radio determination satellite service. *Satell Navig* **1,** 5 https://doi.org/10.1186/s43020-019-0004-2

[40] Wei X. and B. Sikdar,(2019) "Impact of GPS Time Spoofing Attacks on Cyber Physical Systems," IEEE International Conference on Industrial Technology (ICIT),pp. 1155-1160, doi: 10.1109/ICIT.2019.8755016.

[41] Wu Z., Y. Zhang, Y. Yang, C. Liang and R. Liu, (2020) "Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey," in *IEEE Access*, vol. 8, pp. 165444-165496, doi: 10.1109/ACCESS.2020.3022294

[42] Xiao-gang, Xie and Lu Mingquan. (2017) “Broadcast Ephemeris Model of the BeiDou Navigation Satellite System.” Journal of Engineering Science and Technology Review 10: 65-71.

[43] Xu, Xiaolong**,** Min Li , Wenwen Li and Jingnan Liu (2018) “Performance Analysis of Beidou-2/Beidou-3e Combined Solution with Emphasis on Precise Orbit Determination and Precise Point Positioning.” Sensors (Basel, Switzerland).

[44] Yang Y X, Li J L, Xu J Y, et al. (2011). “Contribution of the Compass satellite navigation system to global PNT users”. Chinese Science Bulletin , 2011, 56: 2813–2819, doi:10.1007/s11434-011-4627-4

[45] Yang, Y., Mao, Y. & Sun, B (2020). “ Basic performance and future developments of BeiDou”.global navigation satellite system. *Satellite Navigation* **1,** 1 https://doi.org/10.1186/s43020-019-0006-0

[46] Zeng, K., Liu, S., Shu, Y., Wang, D., Li, H., Dou, Y., Wang, G., & Yang, Y. (2018). All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems. *USENIX Security Symposium (2018).*