GPS Location using the Earth Gravitational Field

Satellite based positioning technology such as Global Positioning Systems (GPS), GLONASS (Russia), Galileo (EU), Beidou (China), QZSS (Japan) and IRNSS (India) are collectively referred to as Global Navigation Satellite Systems (GNSS) and are ubiquitously embedded across millions of terminals around the world.
GNSS has unlimited public applications, is widely deployed to provide ubiquitous experiences and has touched the lives of millions. Since GNSS is an open platform anyone can build a receiver, integrate with a device and run algorithms to generate and use location data. The public and open source availability of GNSS platforms has increased our dependence and reliance on location technologies as a constant in our daily lives.
GNSS is also available as a service to military and government organisations by means of a secure

connection. Such encrypted and secure connections ensure that the data cannot be intercepted, injected and only be read by intended recipients. This service is not an open platform as the receivers are designed with secure sender-receiver IDs, handshaking processes, time stamped data and encrypted hashes to ensure that they are not susceptible to be compromised.
GNSS is available globally and can be received via the following frequencies:

- **GPS**: 1.57542 GHz and 1.2276 GHz
- **GLONASS**: 1.602 GHz and 1.246 GHz
- **BeiDou**: 1.561098 GHz, 1.589742 GHz. 1.20714 GHz and 1.26852 GHz
- **Galileo**: 1.164–1.215 GHz, 1.260–1.300 GHz and 1.559–1.592 GHz
- **QZSS**: 1176.45 MHz, 1227.6 MHz, 1278.75 Mhz and 1575.42 MHz
- **IRNSS**: 1164.45–1188.45 MHz and 2483.5–2500 MHz

GNSS providers publish their transmission meta data in public domain that include bandwidth, channel information, orbital height, satellite identifier(s), detailed orbit and operational information. This meta data is included in GNSS transmissions along with other information at designated frequencies. The transmissions are binary encoded data that ensure public and military users access appropriate broadcasts which are

separated out of phase by a pre-defined number of degrees. The signals contain data that encode pseudo-ranges, carrier cycle counts, dopplers, atomic time, satellite position and other orbital information to assist in calculation of time the signal takes to travel from the satellite to the receiving chip.

The chips receive the transmissions from the monitoring frequency, synchronise their clock and triangulate their information on the basis of the Doppler, noise values, atomic clock, transmitted ephemeris (position), error correction value(s) to calculate position. To ensure accurate position, a minimum of four satellites signals are required and an application of a series of algorithms that are not covered in this paper. To summarise, GNSS platforms are offered as open source (for public) and closed source (for military/government agencies) on separate radio channels, bandwidth and other dynamic protocols to ensure security. GNSS in all forms however, is insecure, clunky and susceptible to hundreds of hacks, vulnerability and attacks.

GNSS is highly susceptible to replay, injection, jamming and other Denial of Service (DoS) attacks. The insecurities and vulnerabilities are applicable to all forms of satellite based GNSS positioning technologies and other transmissions as they are designed for open access. The details of attacks as

highlighted in GPS Vulnerability *Report*, US DOT *Report* and across the internet. The vulnerabilities are out of purview of this paper and are not discussed in details but provided as a high level overview below:

- **Replay attacks**: It has been empirically proven that GNSS can be recorded and replayed. An interesting but easy attack as explained *here* is showcased by a researchers ability to record a GPS signal from a location A and ability to replay the recorded signal in Location B. This lead to instant spoofing and ensuing confusion of smartphones and other receiver location reading. Advanced replay attacks are possible not only on open but also closed GNSS transmissions.
- **Jamming attacks**: The jamming of GNSS is possible by simply transmitting swaths of data on the applicable frequency and channel(s). This blocks any satellite receiver (public or secure) and results in a classical DoS attack. Advanced jamming attacks, dubbed “black jamming” entails radio replay attacks by re-using accurate headers, channel numbers but injecting corrupt data which are used by chips to calculate their own location. While jamming attacks are easy to identify, black jamming is difficult since (a) it seems to be a legitimate transmission, (b) passes checksums

and handshakes and (c) are short lived which hampers detection efforts from obtaining behavioural and pattern data.

Jamming, interception and injection attacks within radio headers, disorients receiving hardware within seconds and enables a perfect crime as these attacks do not generate logs or carry identity of the transmitter.

Hundreds of vulnerabilities and attacks that have been publicly documented here. However, the intention of this article is not to discuss these vulnerabilities but discuss platforms that can serve as a secure, stable and as a backup to existing positioning technologies.

As researchers, it is part of our job to think about scenarios where new technology disrupts industries and the failure of existing technologies. This has nudged my team and I to implement critical processes and out-of-the-box thinking to innovate next generation alternatives to GNSS.

In this paper, we will present an introduction to a new GNSS (**N-GNSS**) platform that uses earths magnetic field to create an alternative platform to satellite GNSS. N-GNSS (*patent pending vide application 202111049994*) platform can immediately serve as a backup for GNSS in scenarios where it is jammed, spoofed, corrupted, unavailable or has poor to low connectivity. Over a period of time we intend for N-GNSS to grow into a

scalable platform that can assist users to obtain accurate positioning data in air, ground or underwater.

Background of the new GNSS or N-GNSS: Earth is a giant magnet powered by the naturally occurring liquid-iron outer core, materials that bear magnetic properties in the crust and upper mantle and induction of electric currents by the flow of sea water through the magnetic field. Other sources of magnetism superimpose with the earth geomagnetic readings such as magnetic dips, blackout zones, elevation, altitude, artificial sources of magnetic strength and general grid variation across the planet.

However, every point on the planet has a magnetic field that points in a particular direction with a defined magnetic strength. The strength of the magnetic field, **S**, can be represented in geocentric spherical coordinates (longitude L, latitude D, radius R) as the negative spatial gradient of a scalar potential

S = {L, D, R, time) = -∇ Variation (L, D, R, time)

The magnetic field (S) varies as per spatial and temporal frames and can be estimated via any fluxgate or another type of magnetometer. To take a very high level overview of the earth magnetic readings at a point, let us assume the following types of sources at any temporal or spatial frame:

- Earths magnetic strength reading

- Static sources of interference
- Dynamic or screaming sources of interference
- Delta values

Static sources: Interference sources that generate stable interference such as man made equipment (power lines, power stations, labs, etc)

Screaming sources: Dynamic sources of interference that change over time such as small magnets or other generator which exhibit temporary spurts of magnetic emission.

Delta values: Known values of interference such as, but not limited to — time of day, direction of sunlight, magnetosphere, earthquakes, inner core, rotation, crust, declination, inclination, ionosphere, magnetosphere and gyrations that occurs in continuity such as solar storms, elevation, topography, altitude changes, spherical and spherical variations, regional anomalies, earths rotation and the magnetic strength changes due to the pole shift/reversal.

A temporal frame is referred to as a “Magnetic Moment” (**MM**) defines the attitude of the invention (spin, tilt, direction of movement, etc) and its location in spatial and temporal frames.

For N-GNSS to be scalable it needs to enumerate all the points as above, do them independently and accurately.

In next section of this paper we will discuss how N-GNSS has created a new Multiple Input Multiple Output (MIMO) spherical antenna that calculates power profiles and identify magnetic sources. N-GNSS is not simply an new antenna design but it also implements modified sensors that can detect screaming and static sources using advanced Digital Signal Processing (DSP), location techniques and algorithms to identify the actual signal of the earths magnetic fields and interference sources.