Review on Detection of Spoofing attack on GNSS

Tanvi Rajat*, Tejas Patel**

*Research scholar, Electronics & Communication engineering department (GEC, Surat, India)

**Assistant Professor, Electronics & Communication Engineering Department, (GEC, Surat, India)

*tanvirajat24@gmail.com, ** tspgec@gmail.com

Abstract: **Global Navigation Satellite System (GNSS) which is used to explain the gathering of satellite positioning systems that are at the moment in service or intended. It can be also be provides the Position, Velocity and Time (PVT) solution. Nowadays most of the people depend on the GNSS for the businesses, governments operate and also how we conduct our personal lives. Spoofing is the intentional interference which is the type of satellite interferences. The spoofing degrades the information GNSS signal from the GNSS receiver to the victim's receiver. The spoofer added the spoofing signal and misinterprets the original signal and it can identify itself as the original GNSS signal.**

Spoofing detection is necessary to detect the spoofing signals from the GNSS signal and different types of spoofing detection techniques are researches by the scientist. In this paper will provide a review on methods of spoofing attack detection on GNSS receiver.

I. INTRODUCTION

The GNSS receiver main purpose is that to determined the user position based on the received signals coming from constellation of different satellite view. GNSS is used in collaboration with GPS systems to provide precise location positioning anywhere on earth. Though Global Navigation Satellite Systems (GNSS), like GPS and Galileo, are based on Direct Sequence Spread Spectrum method, which brings an intrinsic robustness, signals broadcast by the constellations arrive at the antenna with an extremely low signal power level, that makes GNSS based civil infrastructures vulnerable to different disturbs[1]. The different types of GPS system vulnerabilities are non-deliberate interference like Radio frequency interference (RFI), Ionospheric; Solar Maximum, Spectrum Congestion and deliberate interference like Spoofing- counterfeit signal, Jamming. Spoofing is a process whereby someone tries to control reported position out of a device [5]. This may take the reporting incorrect Position, Velocity and Time (PVT) solution form to a local user or to a remotely located client. A common misunderstanding is that spoofing is of necessity an RF attack. In day to day life, intentional interference effects which are able to compromise the GNSS receivers correct functioning [1]–[4].

In the literature, we see that there are three types of spoofing attacks are Simplistic, Intermediate, Sophisticated or Meaconing attack (6). A simplistic attack via GPS Signal Simulator, in this attack, the simple spoofer is composed by a GPS signal generator connected to transmitting antenna. It can be easily implemented but can be also detected by the basic countermeasure method. Intermediate Attack via Portable Receiver Spoofer, in this attack intermediate spoofer receive GNSS signals, makes controlled delayed replicas and send them to the victim receiver. It cannot be easily detected and also it can be effective. Sophisticated Spoofing Attack Multiple Phase-locked Portable Receiver-Spoofer, in this attack the receiver-spoofer's receiving and transmitting antennas are situated respectively on the upper and lower faces of the device and are shielded The counter measure techniques of spoofing attack are in two categories i.e. Spoofing Detection and spoofing mitigation. The spoofing detection techniques algorithms concentrate on discriminating spoofing signals notwithstanding this not necessarily execute countermeasures against the spoofing attack. But Spoofing mitigation techniques primarily concentrate on neutralizing the detected spoofing signals and aid the victim receiver to recover its positioning and navigation abilities. Several anti-spoofing techniques based on single-antenna processing have been proposed.

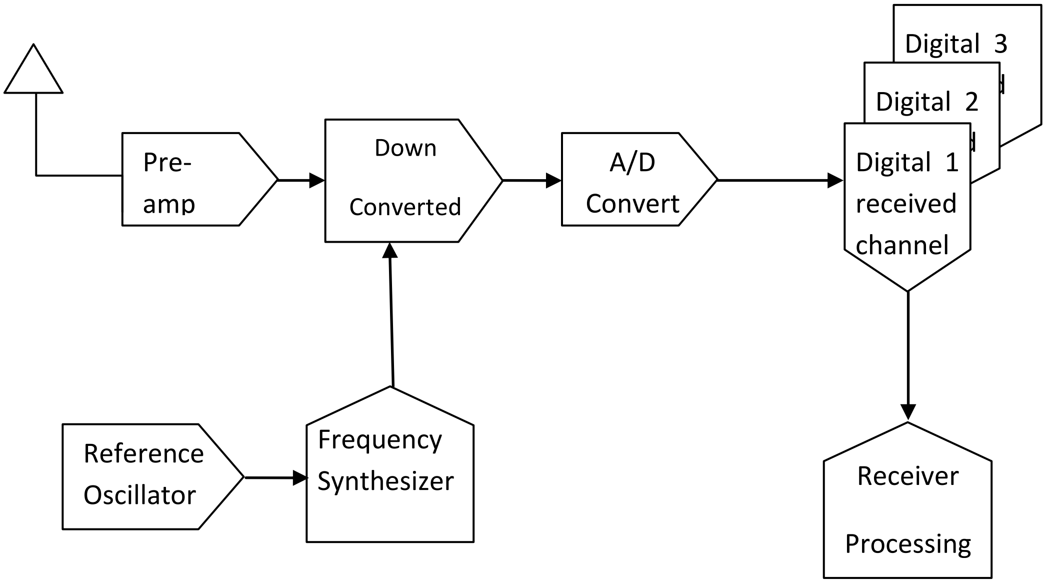

Fig.:1 Ordinary Digital GNSS receiver (adapted from Ward [Kaplan 1996, p.122]

Amplitude discrimination [9]–[11], time-of-arrival (TOA) In this paper, we see that the GNSS receiver, spoofing attack and different type's detection of spoofing attack on GNSS receiver in details and comparisons of different methods based on Spoofing Detection.

II. SPOOFING DETECTION TECHNIQUES

In day to day life the spoofing attack will rapidly increases and it is harmful for or misguides the users which use the GNSS signals for the different application like GPS, navigation maps and etc. That's why the spoofing detection is necessary.

These techniques algorithms which are concentrating on discriminating spoofing signals notwithstanding this not necessarily execute countermeasures against the spoofing attack. This is called as spoofing detection.

There are the different types of spoofing detection as follows: discrimination [12], solution consistency cross-check with inertial measurement units (IMU) [13], polarization discrimination [14], spatial processing based spoofing discrimination [15], position deviation [16], signal quality monitoring [17], and cryptographic authentication [18] are some of the most current spoofing detection techniques. Many single receiver spoofing countermeasure techniques rely on power level monitoring of the received GNSS signals in order to detect spoofing pseudo random number (PRN)s. In [10] the presence of high power spoofing signals is detected based on their abnormally high carrier-to-noise ratio [10] values. [19] Monitors the receiver automatic gain control (AGC) level as a mean of detecting high power spoofing attacks. A pre-despreading spoofing detection method that checks for the excessive structural power content of received GNSS signals is proposed in [21].

The different types of techniques are described in below:

1. Signal Processing based Technique:

Here numerous stages to signal processing by a digital GNSS receiver previous to the navigation and time determination could exist enumerate [Kaplan 1996]. The arrival analog radio frequency (RF) signal commencing the antenna is primary amplified, the down-converted to a lower frequency and its signal potency changed to make better via Automatic Gain Control (AGC). After changing from analog form to digital form, a facsimile Pseudo Random Noise (PRN) code, good thing they figure out Doppler shift caused by relative movement of the receiver and the satellite, is used to separate the entity satellite signals. The individual channels digital data together with their in phase (I) and quadrature (Q) parts are the available for figuring out the driving or flying a vehicle to somewhere and time solutions. At several forum in the processing it's feasible to watch (for changes, unusual things etc.) the acquisition and tracking of signals for anomalies that verisimilitude point toward a spoofing attack is in steps forward. This approach is not amendment in physical existing equipment or signal protocols. Device firmware is always updated. There are different techniques based on signal processing are as follows:

i) RAIM, ii) SINR/SNR, iii) Absolute Power, iv) Doppler shift detection, v) Correlation peak monitoring and vi) Clock bias monitoring.

2. Correlation with other GNSS Sources:

The P(Y) signals would therefore out of phase with the non military personnel signals and this distinction be discernible through reference with another beneficiary while the satirizing assault will be available. This procedures needn't bother with any progressions of flag conventions or the satellite send them [Psiaki et al. 2011; Heng et al. 2013].

Psiaki [Psiaki et al. 2011], O'Hanlon [O'Hanlon et al. 2013] and Lo et al. [Lo et al. 2009; Levin et al. 2011] propose the protected reference recipients use in modest number to check GNSS beneficiaries in the field. Be that as it may, the deals start amount in the signal previews being sent for verification valor pulverizes the references. What's more, arrange based verification valor is helpless against normal digital assault types, for example, man-in-the-center, which could spin the confided in reference collector into a spoofing hotspot for numerous beneficiaries. Heng isolates topic by proposing impromptu verification through friends [Hengetal.2013]. Be that as it may, this would require simultaneousness by collector age on the verification convention. Additionally, since it includes the around 1 megabit sending information to every one of five companions, unsurpassed a verification bid is made, the terrorizing of forget about look at by acting up friends would be diverse to keep.

3. Antenna Array Technique:

For Direction of Arrival (DoA) estimation when selecting antenna array, several component use into deliberation. 1st is sensors number. There are two sensors which are used in phased delay discrimination [7] and for an AOA [angle of arrival] restricted assessment will be necessary. Reliability monitoring technique is base on spatial severance of interference and legal signals owing to the difference in their angles of arrivals [8, 9].

Same phase shifts are feasible for baseline symmetrical azimuths when such an array use. Adding together the third non-in-line component to the array eliminates the azimuth latent ambiguity. Yet extra essentials are required for instantly recognizable two-dimensional DoA estimation. On the other side the sensors number must not be moreover high.

The recipient structure in the radio wire exhibit case comprises of a few receiving wires each associated with a different radio recurrence (RF) down-change divert and digitizer unit in a stage lucid mode more often than not using a solitary oscillator [7]. The radio wire components detachment in such cases is about half of the bearer wavelength and the radio wire exhibit is viewed as a solitary collector unit for a particular application [7]

There are some restrictions in antenna array size. While the space among sensors is larger than half wavelength, befall the phase characteristic. A closely-spaced sensors number is large increases mutual coupling.

Also more signal processing paths are required in this case, which increases computational abstruseness and hardware.

4. Spatial Processing Technique:

Here several tract to acquire the DoA or Aoa estimation. They are including mechanically or electronically restricted reception pattern antennas, phase interfere geometry, subspace-based methods. Mickle these potential require extra signal processing block. In GNSS receivers accessible on the market, signal processing blocks are typically incorporated interested in one chip with no any exterior admittance to received signals sample. Because of that the greatest approach to evaluate the performance of DoA assessment is to use a software receiver with an analog front-end. Off-the-shelf chip-scale GPS front ends are presented, until now they typically make available only one or two bit output determination, which is adequate for GPS signal reception, but it might be excessively low for DoA application [19]. It's superior to utilize a separate preamplifier and an analog down converter imitate to high-determination of multi - channel digitizer.

In view of the fact that spoofing signals are practically for eternity radiated from a single source, they appear to the receiver from the same direction, no issue if it is a line-of-sight or a reflected signal. On the other side, authentic signals from GPS satellites incoming from diverse directions within the whole hemisphere, supercilious the clear view of the sky. Basing on this assumption, GPS spoofing is detected when multiple received signals [19] have the same or very similar DoAs.

Azimuth and altitude, which stand for two-dimensional DOAs, are phase delays non linear function. Because of that a relative involving the phase delay estimation error and the DoA estimation error depends on relative orientation between signal source and receiver antenna. Therefore for GPS spoofing detection it is additionally dependable to evaluate the phase delays than to assess the actual DoAs.

4. Cryptographic Techniques:

The authentication conception represents a cryptography adjunct detection method to feasible spoofing attack. It needs the cryptographically secure position appearance in the received signal (security code or digital signature) and it involve authentication two these are follows: i) Code origin and ii) Code timing.

Using the recent stand alone receiver position authenticity can't be allege, which solely exploit civil GNSS signal (GPS L1 Signal). Some solution have been proposed but most of them are basal on a client – server approach in which the beyond characteristic of forbidden insertion GNSS signal (e.g., military GPS L1 P/Y code, GPRS signal) are cross compared among discrete location in order to authenticate the civil signal.

It is legitimate to without that a position authentication structure will be contrive in the incoming days within the GNSS signal itself, as an added value of GNSS system and stand alone estimation capable to comply receiver.

III. Conclusion

In this review paper, learn about some basics about the different kind of spoofing attack. Mainly this paper focuses on the different detection techniques of the spoofing attack. GNSS spoofing is a beginning danger, not yet saw, all things considered, circumstances. All things considered, significantly potential dangers survive beside transportation and upcoming elegant network control the board frameworks and lesser dangers beside make safe illegal labels and prepare manage frameworks, among various remaining risk to accessible cell phone foundation. GNSS spoofing is as of now difficult to do in the field. This may seem farfetched, given the far greater complexity of an intermediate-level spoofer, but the multifaceted nature is to a great extent in the product and hand-held GPS test systems like the Cast and Aeroflex items are becoming littler. Provided that this is true, our developing reliance on GNSS applications in key territories, for example, the Smart Grid, may go under genuine risk. The spoofing countermeasures subjective evaluations utilizing values running from low to high. Where signal preparing is the fundamental line of barrier, Doppler move testing is the most exceedingly evaluated and has been tried. RAIM or consistency keeps an eye on GNSS signal no longer suffice, and in spite of the fact that they ought not be ceased, the spoofing danger has now proceeded onward from the counterfeit of individual satellites to whole heavenly bodies. Cryptographically protections for the most part don't suffice for regular citizen use; they stay doubtful and fragmented, despite the fact that the military evaluation SCE strategy is exceptionally viable. Among the rest of the resistances the point of landing (AOA) guard is evaluated most astounding on common sense and adequacy, and late work proposes that this methodology is experiencing a something of a restoration.

IV. References

1. Motella, Beatrice, Marco Pini, and Fabio Dovis. "*Investigation on the effect of strong out-of-band signals on global navigation satellite systems receivers.*" GPS Solutions 12, no. 2 (2008): 77-86.
2. Shepard, Daniel. "*Characterization of receiver response to spoofing attacks*." PhD diss., 2011.
3. Wildemeersch, M., E. Cano Pons, A. Rabbachin, and J. Fortuny Guasch. "*Impact study of unintentional interference on GNSS receivers.*" EC Joint Research Centre Dovis, Fabio, ed. GNSS Interference Threats and Countermeasures. Artech

House, 2015.Scientific and Technical Reports, Institute for the Protection and Security of the Citizen, European Union (2010).

4. Morales Ferré, Rubén, and Gonzalo Seco Granados. "*Analysis of GNSS replay-attack detectors exploiting unpredictable symbols.*" (2018).
5. Scott, Logan. "Spoofing*: upping the anti*." Inside GNSS. Thought Leadership Series (2013): 18-19.
6. Humphreys, Todd E., Brent M. Ledvina, Mark L. Psiaki, Brady W. O'Hanlon, and Paul M. Kintner. "*Assessing the spoofing threat: Development of a portable GPS civilian spoofer*." In Radio navigation Laboratory Conference Proceedings. 2008.
7. S. Daneshmand, A. Jafarnia, A. Broumandan, and G. Lachapelle, "*A low-complexity GPS anti-spoofing method using a multi-antenna array,*" in Proc. ION GNSS 2012, Nashville, TN, USA, Sep. 17–21, 2012, p. 11
8. A. Jafarnia-Jahromi, "*GNSS Signal Authenticity Verification in the Presence of Structural Interference*," Ph.D. dissertation, Dept. Geomatics Eng., Univ. Calgary, Calgary, AB, Canada, Sep. 2013.
9. E. McMilin, D. S. De Lorenzo, T. Walter, T. H. Lee, and P. Enge, "*Single antenna GPS spoof detection that is simple, static, instantaneous and backwards compatible for aerial applications*," in Proc. ION GNSS + 2014, Tampa, FL, USA, Sep. 9–12, 2014
10. J. Nielsen, V. Dehghanian, and G. Lachapelle, "*Effectiveness of GNSS spoofing countermeasure based on receiver CNR measurements,*" Int. J. Navig. Observations, vol. 2012, p. 9, 2012, Art. no. 501679.
11. A. Jafarnia, A. Broumandan, J. Nielsen, and G. Lachapelle, "*GPS spoofer countermeasure effectiveness based on using signal strength, noise power and C=N0 observables,*" Int. J. Satellite Commun. Netw., vol. 30, no. 4, pp. 181–191, Jul. 2012. [12] A. Jafarnia, A. Broumandan, J. Nielsen, and G. Lachapelle, "Pre-despreading authenticity verification for GPS L1 C/A signals," J. Inst. Navig., vol. 61, no. 1, pp. 1–11, 2014.
12. S. L. Cho, M. Y. Shin, S. Lim, D. H. Hwang, S. J. Lee, and C. Park, "*Design of a TOA-based anti-spoofing method for GPS civil signal,*" presented at the ION GNSS PNT Symp., 2008.
13. P. F. Swaszek, S. A. Pratz, B. N. Arocho, K. C. Seals, and R. J. Hartnett, "*GNSS spoof detection using shipboard IMU measurements,*" in Proc. ION GNSS + 14, Tampa, FL, USA, Sep. 8–12, 2014, pp. 745–758.
14. E. McMilin, D. S. De Lorenzo, T. Walter, T. H. Lee, and P. Enge, "*Single antenna GPS spoof detection that is simple, static, instantaneous and backwards compatible for aerial applications,*" in Proc. ION GNSS + 2014, Tampa, FL, USA, Sep. 9–12, 2014.
15. S. Daneshmand, A. Jafarnia Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "*GNSS spoofing mitigation in multipath environments using space-time processing,*" presented at the European Navigation Conference (ENC2013), Vienna, Austria, Apr. 23–25, 2013.
16. J. C. Juang, "*Analysis of global navigation satellite system position deviation under spoofing,*" IET Radar, Sonar, Navig., vol. 3, no. 1, pp. 1–7, Feb. 2009.
17. E. G. Manfredini, F. Dovis, and B. Motella, "*Validation of a signal quality monitoring technique over a set of spoofed scenarios*," in Proc. 7th ESA Workshop Satellite Navig. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC), 2014, pp. 1–7.
18. T. E. Humphreys, "*Detection strategy for cryptographic GNSS anti-spoofing,*" IEEE Trans. Aerosp. Electron. Sys., vol. 49, no. 2, pp. 1073–1090, Apr. 2013. [20] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," J. Navig., vol. 59, no. 4, pp. 281–290, 2012, Winter, Institute of Navigation.
19. Broumandan, Ali, Ali Jafarnia-Jahromi, Saeed Daneshmand, and Gérard Lachapelle. "*Overview of spatial processing approaches for GNSS structural interference detection and mitigation*." Proceedings of the IEEE 104, no. 6 (2016): 1246-1257.