Contemporary GPS Security Mechanisms

Rejo Mathew

Abstract*: GPS (Global Positioning System) plays a big role in day to day activities. From navigation to tracking devices, all are dependent on GPS. As the attacks on GPS have increased so the review of GPS security plays a vital role in research. This paper looks at different spoofing generation methods. The idea is to discuss the single antenna, multiple antenna and other factors that are susceptible to interference. Based on the type of vulnerability the solutions are described in detail. This paper focusses on the current anti-jamming and anti-spoofing GPS mechanisms. This paper presents a comprehensive analysis of all the techniques along with the pros and cons of each method.

***Keywords* : GPS, Global Positioning System, GPS Security, GPS Anti-Spoofing**

I. INTRODUCTION

GPS is the most accurate, cost-effective and widely used ubiquitous location tracking technology in civil and military applications. Mobiles, radios, watches and numerous devices are equipped with this technology making it a lucrative target for attackers. Backward compatible technology along with a standard signal structure makes it most vulnerable. [1] Even though research was going on for very long serious research work started only recently with advances in technology which has increased the jamming and spoofing attacks. GPS signals are constantly interrupted by spoofing and jamming signals. A jammer with only 1 Watt power can disable a complete GPS system within 25 kilometers. [2] Anti-jamming technology implements methods depending on the type of interference – For narrowband signal interference adaptive filters [3][4], neural networks [5], wavelet transform [6] is used. To mitigate wideband interference, higher SNR is required [7][8][9]. For highly dynamic environments the space-time adaptive processing (STAP) method is used. [10][11][12]. In spoofing the attacker generates fake signal similar to authentic receiver signal to fool the GNSS receiver thereby giving wrong time and location information to the GPS. Spoofing is flexible, feasible, well hidden, cost-effective and difficult to detect unlike jamming as shown by various researchers like T.E. Humphrey [13][14][15][16], Baziar [17]. This paper reviews spoofing techniques and its countermeasures. This paper is organized as follows. Section II shows the classification of spoofing generation techniques followed by Section III discusses the anti-spoofing mechanisms in detail followed by Analysis of each technique in Section IV. Concluding remarks are presented in Section V

Revised Manuscript Received on December 15, 2019.

***** Correspondence Author

Rejo Mathew*, Information Technology, Mukesh Patel School of Technology Management and Engineering, NMIMS (Deemed-to-be) University, Mumbai, India. Email: rejo.mathew@nmims.edu

II. SPOOFING TECHNIQUES

In spoofing the spoofer replicates the radio frequency carrier, spreading/psuedo random noise code and data bits of true original signal. The different ways to generate spoofing signals are mentioned below,

A. Open-Loop Signal Simulator Attack

In this technique the spoofer induces the victim to lock into wrong signals. Initially the receiver is jammed to disrupt normal tracking of true signals. Then the self-consistent spoofer signals are generated using GNSS signal simulator which lock the receiver to false signal during re-acquisition.

B. Spoofer with Known Geometry Relative to Victim

In this technique the spoofer knows the position of the victim, and can completely drag-off original signal. The victim receives the fake signal which are doppler-matched and code-phased to the original signal by the spoofer before transmission. Spoofer begins at low power which gradually rises till it can capture the tracking loops. Finally, the attacker takes off the signal in a self-consistent way. Authors in [50][51] have proposed algorithms to counter this attack

C. Meaconing Attack

In this technique a one piece antenna called meaconer is used. A meaconer can spoof even hidden signals. The meaconing signal is collected at a different location or time, which is superposed on the clean targeted signal. The meaconing signal aims to divert the target receiver into an incorrect and wrong navigation signal by overlapping the original received with incorrect one.

D. True-Signal Nulling Attack

Many spoofers use the technique called nulling. The spoofer generates dual signals. First signal works as an ensemble of all spoofed signals to produce wrong information. The second one is the inverse of the main one. Thus, K_s = 2K. Out of which one half of K signals are spoofers and other half are ones used to nullify. In nulling attack the receiver is attacked with a nulling signal so that the original signal gets completely dragged off the position and later when the spoofing is successful the nulling signal is cancelled (because of 180 degree phase shift).

E. Receiver-based spoofing

In this spoofing attack the synchronization is key. The spoofed signal is based on the three dimension pointing vector of transmitter. It is really hard to discriminate true signal from false ones. In this method signal strength of the spoofer should be higher than the signal strength of the original signal but not exceeding threshold of GPS signal.

The limitations of this method includes curtailing the self-jamming effect, subduing data bit variations and aligning the frequency and phase of carrier signal in line with GPS signals [16].

F. Sophisticated receiver based spoofing

It is a complex spoofing method but most effective. Here, spoofer collects the victim's position (centimeter level) to precisely synchronize the spoofed signal with original. This spoofing can defeat direction of arrival anti-spoofing using multiple antennas. But realization of this spoofing is difficult because alignment and synchronization of carrier phase might happen only for few regions where the target antenna is located. It becomes tough due to topology changes of receivers [18].

G. Spoofing in Signal Processing

GPS has a backward compatible generic structure and standard signal features for all GPS satellites. The receiver signal strength is monitored by the automatic gain control (AGC) block. Due to which powerful spoofing signals lead to higher receiver gain creating fake signals that mislead GPS receivers [19].

H. Spoofing by changing Data Frame

GPS has a well-known standard frame structure. The frame has calendar, position and trajectory information. This data does not vary for short periods; E.g. for 750 seconds the information remains constant [1]. New data frame is created by the spoofer. The spoofer can manipulate status bits to ensure rejection of authentic incoming GPS signals [20].

I. Spoofing by changing Navigation and Position levels

The spoofer inserts fake measurements into the receivers which affects the position, velocity, and time (PVT) solution. The product of range residuals and geometric factor is proportional to the PVT error. In [21] a vulnerability index against spoofing (VIAS) based on original GPS constellation and spoofer positon is the geometric factor. VIAS fluctuates based on the position and time and increases with increase in position dilution of precision (PDOP) value. Anti-spoofing methods can incorporate this index in the design itself. Hand-offs in CDMA/GSM cellular systems get disturbed by affected GPS receivers.

III. ANTI-SPOOFING

It can be classified into detection and mitigation. Detection mechanism mainly recognizes and discriminates actual from the spoofing signal and the mitigation mechanism helps in neutralizing the effect of spoofing signal and helps the victim to re-gain its position, time, velocity etc. Gamba [52] successfully tested the open spoofing dataset TEXTBAT for correctness. First we discuss the Spoofing detection techniques and later Spoofing Mitigation Methods

A. C/N_0 monitoring

In this technique a C/N_O (C/N_O: SNR ratio) measurements is used to check the quality of the receiver signal. Satellite changes and ionosphere deviations affects the received power, but when a high power spoofing signal is there, the C/N_O may experience sudden chance indicating the presence of spoofer signal. The timing info is stored by the receiver. [22]

B. Absolute power monitoring

A variable path loss between the targeted victim and spoofer makes it difficult for the spoofer to generate the exact power as it should not exceed the power of authentic signal. [19] Max. Received power at earth is nearly 153dBW L1 frequency.[23] This method is more accurate than C/N_O monitoring, as even 2bB signal are detected. [22] This technique depends completely on accurate detection of the amplitude of the received signal. Hardware complexity is added. Dynamic range of GPS signals limits the accurate measurement of wave patterns. [42]

C. Received power variations vs receiver movement

The inverse square law of propagation states that the power density of an electromagnetic wave is proportional to the inverse of the square of the distance from a point source. Satellites range up to twenty thousand kilometers from the earth. So the receiver movement has no change in the receiver power as compared to original. However the spoofing signal antenna is much close to receiver antenna. Received C/N_O of spoofing signal is affected by the proximity of spoofer and victim. If the location of transmitter and receiver is same, then their movements wont impact the variations in evaluation and measurements of spoofing signals, this is also one of the disadvantage of this technique. [21] [42][43]

D. L1/L2 power level comparison

GPS signals disperse at the ionosphere where the dual-frequency (L1 = 1575 MHz, L2 = 1228 MHz) is generated. Receiver can avoid delay caused in ionosphere through a combination of L1 and L2 which is linear in nature [24] GPS receivers track both signal levels but simple spoofers generate only level one signal causing lot of energy difference between L1 and L2 signal. But not all GPS receiver generate L1 and L2 signals. [19]

E. Synthetic Array spoofing discrimination

In this technique a single receiver with antenna is shifted and taken along different trajectories path, which forms a structure of a synthetic antenna array.[25] The signal phase which is obtained is compared to each other using the correlation matrix which is made earlier. The hardware complexity is low as several antennas are not involved. However, some modifications are needed to be applied to successfully discriminate the spoofer signal.

F. Multi-antenna spoofing detection

In this technique the theoretical and practical values of the phase difference between two antennas are matched and compared every hour to discriminate the spoofing threats [15]. Spoofing signal is detected and mitigated using antenna array based on their spatial correlation and also this technique increases hardware complexities as, it needs several antennas. Major drawback is it takes 1 long hour to detect the signal. This also increases computational complexities and tracking and calculating is a tiring task. Direction and preset values of antenna array knowhow is crucial. [26]. A multiple antenna spoofer will fool this technique. To overcome such limitations authors in [44][45] have proposed new techniques.

Author in [46] has proposed a prediction based adaptive algorithm for GPS Spoofing detection.

G. PRN Code and Data Bit Latency

In this technique the navigation data bits information is kept confidential and spoofer has no idea or data related to it. So firstly, the decoding of signal is done then a duplicate spoofer signal is readied which takes some time. GPS bits generated could be predicted by the spoofer most of the times considering that pre-existing information is available before sending out counterfeit signals. [16] [27] [28]

H. L1/L2 Signals Relative Delay

All frequencies are converted to non-traceable format before transmission. Both signals are correlated and received with relative delay. There is a propagation delay in L2 which is generally greater than L1. So the GPS receiver already knows the approx. relative delay of correlation peaks. Both frequencies have to be accurately spoofed by the attacker to counter it. [19]

I. Signal Quality Monitoring (SQM)

GPS correlation peak quality is monitored using SQM technique which is in multipath fading conditions [29]. Spoofing attacks affects the correlator output similar to multipath components [30]. In [18][31][32] for line-of-sight condition SQM is used by authors to detect spoofing. The ratio and delta SQM test will highlight the changes in peaks to confirm presence of spoofing. If there exists multiple path propagation then this method fails to distinguish between spoofed and multipath signals. This is also one of the drawbacks of SQM.

J. Consistency Check in comparison with Other Navigation and Positioning Technologies

Low cost inertial measurement unit (IMU) devices helps detect interference [15][33]. GPS signal solutions are matched to the solutions from mobile cellular networks or Wireless Fidelity (Wi-Fi). Receivers becomes more complex due to this hardware and software modifications [34]. The drawback is that cellular networks which work on different location technology lack accuracy. A minor gap amongst spoofer and authentic signal position makes it useless.

K. Cryptographic Authentication

The civil and military based services use this method to detect unavoidable spoofing threats. Latest techniques involve encrypting pseudorandom noise signals (PRN) which is similar to GPS P (Y) code. Even though it is secure but it cannot be used for existing signals as it needs signal modifications. Encrypting Navigation message (NAM) is also secure but it requires decryption of navigation data. As large modifications have to be made to almost all GPS signal structure which uses this cryptographic authentication technique, so it is not considered very useful. [20][23][27] [35][41]

L. Consistency Check in Code and Phase Rates

In this method the Doppler frequency and code delay rate are checked for consistency for being affected based on their relative positions [31]. A poor quality spoofer lacks consistency between Doppler frequency and code delay rate. [36]

M. Received Ephemeris Consistency

In this method the navigation message is compared to the data positioning of all satellites. if there is any inconsistency or error in this data , it warns of a probability of an attack.

N. Consistency Check in GPS Clock.

The navigation message consists of timing information. This information should be consistent. If GPS is spoofed, then the matching between GPS clock and time from other satellite fails.

O. Open Sourced Vector Tracking Based Receiver

Authors in [63] proposed a viable and effective GPS spoofing generator using a vector tracking based software defined receiver. It can cover all open sky satellites with high quality of concealment.

Further mitigation methods are discussed in detail,

A. Vestigial Signal Detection

Total information is required to suppress the authentic and original GPS signal therefore it becomes difficult for spoofer. In Vestigial mitigation [16] Firstly, the incoming data is duplicated by the receiver into a buffer memory. Secondly, the GPS signal chosen by the receiver is tracked and part of signal is nullified. Third, the receiver performs action acquisition on the buffered data. But there is a lot of hardware and software requirement for additional tracking of signals. [36] Real vestigial signal remains undetectable due to poor resolution of bits and heavy signals.

B. Anti-spoofing from multilayer perspective

The anti-spoofing techniques is divided into three layers, namely Signal processing, data bit and position solution, Navigation levels. Spoofer has to control and overcome all these levels to attack with a spoofing signal. Future methods could include inputs at various levels in order to eliminate spoofing.

C. Receiver Autonomous Integrity Monitoring (RAIM)

Spoofer signals add some random number ranges to the authentic signal. The variations induced by spoofer are detected and eliminated using RAIM method. [37] For some spoofing measurements this method is successful but if spoofing measurements increases then this method fails. [18]

D. *Multi antenna Beam Forming and Null Steering*

Array processing method is used by a multi antenna receiver to shape its beam from the GPS satellite. Null beam is used to nullify the spoofer signal by the receiver when spoofing is detected [16]. In this way spoofing signals can be mitigated using this method. Authors in [47][48][49] have proposed a spoofing mitigation strategy by dynamic receivers using spoofing cancellation algorithm.

E. Broadcast Digital Signature in Navigation Message

It is a practical solution. Simply broadcast a digital signature data from QZSS Navigation. QZSS signals can be used to authenticate the GPS. Other GNSS signals can also be authenticated. This technique does not need any hardware modification. Only software /firmware modifications needed for control and user systems. [38]

F. Anti-jamming and Anti-spoofing technique

Authors in [53] proposed a GNSS jamming and spoofing suppression algorithm based on multiple antennas but it suffered from high calculation costs. Authors in [39] proposed a computationally non intensive method. It projects the received signals in the orthogonal subspace of the jamming followed by compressed sensing to detect any interference. Finally, the receiver uses multi-beam forming to nullify the spoofing. [40] In compressed sensing high frequency components could get away in sampling as opposed to fixed rate sampling due to under-sampling.

G. Multi- Antenna Early Detection and Mitigation

Authors in [58] proposed an early detection and mitigation mechanism that combines array processing and multipath detection algorithms. Spoofing detection is based on evaluating spatial and steering vectors. Adaptive beamforming is used for mitigation of interference.

IV. RESULTS AND DISCUSSIONS

Overall analysis of all the techniques are shown in the Table below.

TABLE I. **SUMMARY OF INTERFERENCE DETECTION METHODS**

Name of Method	Technique	Capability/Modification	Pros	Cons
C/N_0 Monitoring	High C/N_0	C/N_O Monitoring	Simple Cost-Effective Low complexity	If spoofer signal despreads this fails Higher accuracy needed.
Absolute power monitoring	Higher Amplitude	Absolute Amplitude Measurement	Accurate Faster than C/N_O	Hardware Complexity more Dynamic GPS Signal Range limits performance Medium complexity
Received power variations vs receiver movement	Power Variations versus distance	Antenna movement tracking C/N_O Monitoring	Simple Accurate No hardware complexity	Receiver movement may not translate to changes in received C/N_0 of spoofing signal Fails for static GPS Receivers Only few scenarios covered
L1/L2 power level comparison	L1 signal dection. No L2 spoofer signal	L2 reception	Detects single band spoofer	Cannot detect L1 and L2 changes For both bands detection hardware changes Not Practical Costly to implement double band
Synthetic Array spoofing discrimination	Pairwise correlation in synthetic array	Antenna movement Measuring Correlation coefficient	Ideal for multipath conditions Low complexity	Better performance in spatial domain Accuracy based on measurements
Multi-antenna spoofing detection	Phase difference in antennas	Multiple antennas and measurements needed Monitoring at certain time intervals	Ideal for single transmit antenna Best performance	Long time to give result Calibrated antenna with known array orientation Hardware complexity – More antenna Complex computations Multiple antenna spoofer wins over
PRN Code and Data Bit Latency	Delay in data bits	Data bit delay Analysis	Easy to detect Standard method	Medium Complexity Easy to spoof as data bits available early Standard GPS data frame structure
L1/L2 Signals Relative Delay	Delay in data bits	Data bit delay Analysis	Easy to detect Encrypted P(Y) Tough for spoofer to generate both signals	Medium Complexity Time taken is more
Signal Quality Monitoring (SQM)	Shape of correlation peaks of signals	Multiple Correlations	Powerful and Effective for LOS conditions	Medium Complexity Fails in multipath conditions
Consistency Check in comparison with Other Navigation and Positioning Technologies	Spoofing Soltion Paramater check for consistency	Work with different Navigation and Positioning technology	Simple devices used Commonly used	High Complexity Working with Mobile or Wi-Fi is difficult Performance depends on accuracy Limited coverage and capacity
Cryptographic Authentication	Signal Authentications	Different Authentications	Used for civil and military applications Simple techniques	High Complexity Not ideal for short term Modification in Hardware Modification in Signal Structure
Consistency Check in Code and Phase Rates	Checking of phase rate and generated code	Monitor and Calculate the changes	Low Complexity Easy to detect low quality spoofers	Needs constant monitoring and data input High End modern spoofers can win over
Received Ephemeris Consistency	Navigation Message check	Monitor for changes	Low Complexity Easy to detect	Performance depends on accuracy Location specific

Contemporary GPS Security Mechanisms

Name of Method	Technique	Capability/Modification	Pros	Cons
Consistency Check in GPS Clock.	Check for clock inconsistency	Synchronize and Monitor for changes	Low Complexity Easy to detect	Performance depends on accuracy Location specific
Open Source Vector based Receiver	Check for inconsistency	Software based receiver	Open Source Software Receiver based spoofing detection Non overlapped Spoofing detection	Susceptible to frequent attacks

TABLE – II : SUMMARY OF INTERFERENCE MITIGATION TECHNIQUES

Name of Method	Technique	Capability/Modification	Pros	Cons
Vestigial Signal Detection	Vestige of authentic signal used	Receive Multiple signals	Simple to understand Effective for less number of channels	High Complexity Hardware and Processing changes needed Limited bit resolution High power spoofing signals are not covered
Multilayer perspective	Investigate at all levels	Investigate at all levels	Spoofer has to overcome all three levels	Other new cross layer techniques not covered Hardware and Processing changes needed
Receiver Autonomous Integrity Monitoring (RAIM)	Identify and eliminate outlier measurements	Collect and manage residuals	Medium complexity	When spoofed measurements are large this method fails
Multi antenna Beam Forming and Null Steering	Steering Null signal towards spoofer	Collect signal from all channel and antenna	Better methods than above Low complexity multi antenna methods used	Medium Complexity Fails in case of Multi-Antenna Spoofer Affects power of authentic signals
Broadcast Digital Signature in Navigation Message	Broadcast a digital signature based on satellite signal to be authenticated	Software and Firmware to be modified. Additional Authentication Data Center needed	Best method currently implemented Practical Solution Need to check only when required Can be used for all existing signals No hardware modification	Software and Firmware to be modified QZSS signal needs to be present or an alternative to be shortlisted
Antijamming and Antispoofing method	Receiver estimates the direction of arrival and spoofing using compressed sensing followed by multi-beam forming to nullify the spoofing	Despreading and Multibeaming	Anti-jamming and Anti-spoofing together Detection is accurate than other existing methods Better interference suppression method Suitable for all practical applications Low computational costs	Additional steps increases time Needs four satellites to calculate position High frequency components could get away due to undersampling
Multi Antenna for Early Detection and Mitigation	Comparing vectors and adaptive beamforming (Linearly Constrained Minimum Variance)	Steering Vector Tracking	Spoof signals identified before carry-off phase Maximum Likelihood Principle Better control on antenna array pattern Phase calibration is not needed	Vector Tracking should be accurate. Medium complexity DOA of spoofed signal should not match DOA of original Works only in Multipath Free scenario Tradeoff between hardware and signal processing complexity

V. CONCLUSION

From the analysis it is clear that the better solution is the one which is robust, scalable, cost effective, and can intelligently handle interference of any kind. Relying on external factors and devices should be avoided for better and accurate results. All the updates should be over the air (OTA) to avoid future overheads. The combination of anti-jamming and anti-spoofing solution which is accurate, integrated as software avoids any kind of complexity and is practically feasible. Even though this paper summarizes GPS attacks and its countermeasures still there is a long way to go. News like Spoofing in Black Sea [54], Pokemon Go GPS Hacking [55], GPS technology under bigger attack [56] and uncertainty in laws for GPS tracking and GPS usage [57] are going to increase in days to come. Higher number of attacks and more susceptibility needs high quality research and advance methods to counter them. For spoofing detection machine learning [59], maximum likelihood estimation [60], and co-operation of multiple detections [61] [62] proved effective but depend on prior information about the signal features. Mechanism showed in [63] is comprehensive and covers all missing aspects.

REFERENCES

1. X. J. Cheng, K. J. Cao, J. N. Xu, and B. Li, "Analysis on forgery patterns for GPS civil spoofing signals," in Proceedings of the 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT '09), pp. 353–356, Seoul, Korea, November 2009
2. X. Chen, G. Zhang, C. Jiang, and S. Wu, "GNSS augmentation by FM radio symbiosis," IEEE Access, vol. 6, no. 99, pp. 5162–5169, 2018.
3. C. H. Kang, S. Y. Kim, and C. G. Park, "A GNSS interference identification using an adaptive cascading IIR notch filter," GPS Solutions, vol. 18, no. 4, pp. 605–613, 2014.
4. Y.-R. Chien, "Design of GPS anti-jamming systems using adaptive notch filters," IEEE Systems Journal, vol. 9, no. 2, pp. 451–460, 2015.
5. M. R.Mosavi and F. Shafiee, "Narrowband interference suppression for GPS navigation using neural networks," GPS Solutions, vol. 20, no. 3, pp. 341–351, 2016.
6. M. R. Mosavi, M. J.Rezaei,M.Pashaian, andM. S. Moghaddasi,"A fast and accurate anti-jamming system based on wavelet packet transform for GPS receivers," GPS Solutions, vol. 21, no.2, pp. 415–426, 2017.
7. S. Daneshmand, T. Marathe, and G. Lachapelle, "Millimetre level accuracyGNSS positioning with the blind adaptive beamforming method in interference environments," Sensors, vol. 16, no. 11, pp. 1824–1842, 2016.
8. Y. Wan, F. Chen, J. Nie, and G. Sun, "Optimum reference element selection for GNSS power-inversion adaptive arrays," IEEE Electronics Letters, vol. 52, no. 20, pp. 1723–1725, 2016.
9. J. Arribas, C. F. Prades, and P. Closas, "Multi-antenna techniques for interference mitigation in GSS signal acquisition," Eurasip Journal on Advances in Signal Processing, vol. 1, no. 1,pp. 143–152, 2013.
10. F. Chen, J. Nie, B. Li, and F. Wang, "Distortionless spacetime adaptive processor for global navigation satellite system receiver," IEEE Electronics Letters, vol. 51, no. 25, pp. 2138-2139, 2015.
11. L.-W. Chen and J.-S. Zheng, "A broadened and deepened antijamming technology for high-dynamic GNSS array receivers," IEICE Transactions on Communications, vol. E99B, no. 9, pp.2055–2061, 2016.
12. B. Zhang, H. Ma, X.-L. Sun, Q. Tan, and H. Pan, "Robust antijamming method for high dynamic global positioning system receiver," IET Signal Processing, vol. 10, no. 4, pp. 342–350, 2016.
13. M. L. Psiaki and T. E. Humphreys, "Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies," IEEE Spectrum, vol. 53, no. 8, pp. 26–53, 2016.
14. A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," Journal of Field Robotics, vol. 31, no. 4, pp. 617–636, 2014.
15. P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: experimentalresults of a multi-antenna receiver defense against a portable civil GPS spoofer," in Proceedings of the Institute of Navigation—International Technical Meeting (ITM '09), pp.124–130, Anaheim, Calif, USA, January 2009.
16. T. E.Humphreys, B.M. Ledvina,M. L. Psiaki, B.W. O'Hanlon, and P.M. Kintner, "Assessing the spoofing threat: development of a portable gps civilian spoofer," in Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS '08), pp. 2314–2325,Savannah, Ga, USA, September 2008
17. A. R. Baziar,M.Moazedi, andM. R.Mosavi, "Analysis of single frequency GPS receiver under delay and combining spoofing algorithm,"Wireless Personal Communications, vol. 83, no. 3, pp.1955–1970, 2015.
18. B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing device for legacy civil GPS receivers," in Proceedings of the Institute of Navigation—International Technical Meeting (ITM '10), pp. 698–712, USA, January 2010.
19. H. Wen, P. Y. R. Huang, J. Dyer, A. Archinal, and J. Fagan,"Countermeasures for GPS signal spoofing," in Proceedings of the 18th International TechnicalMeeting of the Satellite Division of The Institute of Navigation (ION GNSS '05), pp. 1285–1290,California, USA, September 2005.
20. X. J. Cheng, J. N. Xu, K. J. Cao, and W. Jie, "An authenticity verification scheme based on hidden messages for current civilian GPS signals," in Proceedings of the 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT '09), pp. 345–352, Seoul, Korea, November 2009.
21. J. C. Juang, "GNSS spoofing analysis by VIAS," in *Coordinates* Magazine, *2011.*
22. A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G.Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power and C/N_0 observables," *International* Journal of Satellite Communications and Networking,vol. 30, no. 4, pp. 181–191, 2012.
23. E. D. Kaplan and C. J. Hegarty, *Understanding GPS Principles and Applications*, Artech House, Boston, Mass, USA, 2nd edition, 2006.
24. Ahmed E. Ragheb and Ayman F. Ragab," Enhancement of GPS Single Point Positioning Accuracy Using Referenced Network Stations", World Applied Sciences Journal 18 (10): 1463-1474, 2012
25. J. Nielsen, A. Broumandan, and G. Lachapelle, "Spoofing detection and mitigation with a moving handheld receiver," *GPS World*, vol. 21, no. 9, pp. 27–33, 2010.
26. C. E. McDowell, "GPS Spoofer and Repeater Mitigation System using Digital Spatial Nulling—US Patent 7250903 B1," 2007.
27. S. C. Lo and P. K. Enge, "Authenticating aviation augmentation *system broadcasts*," *in* Proceedings of the IEEE/ION Position, Location andNavigation Symposium (PLANS '10), *pp.* 708–717, IndianWells, Calif, USA, May 2010.
28. S. Lo, D. De Lorenzo, P. Enge, D. Akos, and P. Bradley, "Signal Authentication, a secure civil GNSS for today," *GNSS magazine*, pp. 30–39, 2009.
29. *R. E. Phelts,* Multicorrelator techniques for robust mitigation of threats to GPS signal quality [Ph.D. thesis], *Standford* University, Palo Alto, Calif, USA, 2001.
30. D. Shepard and T. Humphreys, "Characterization of receiver response to a spoofing attack," in *Proceedings of the 24th* International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS '11), *p. 2608, Portland, Ore,* USA, September 2011.
31. A. Cavaleri, B. Motella, M. Pini, and M. Fantino, "Detection of spoofed GPS signals at code and carrier tracking level," in Proceedings of the 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC '10), *pp. 1–6, Dec 2010.*
32. A. Cavaleri, M. Pini, L. Lo Presti, and M. Fantino, "Signal quality monitoring applied to spoofing detection," in *Proceedings* of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS '11), Portland, Ore, USA, September 2011.
33. A. Jafarnia-Jahromi, T. Lin, A. Broumandan, J. Nielsen, and G. Lachapelle, "Detection and mitigation of spoofing attack on a vector based tracking GPS receiver," in *Proceedings of the* International Technical Meeting of The Institute of Navigation, Newport Beach, Calif, USA, January 2012.
34. *M. G. Petovello,* Real-time integration of a tactical-grade IMU and GPS for high-accuracy positioning and navigation [Ph.D.*thesis*], Department of Geomatics Engineering, University of Calgary, Alberta, Canada.
35. L. Scott, "Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Systems," in *Proceedings of the 16th* International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS '03), *Portland, Ore,* USA, September 2003.
36. S. Moshavi, "Multi-user detection for DS-CDMA communications," IEEE Communications Magazine, *vol. 34, no. 10, pp.*124–135, 1996.
37. H. Kuusniemi, A. Wieser, G. Lachapelle, and J. Takala, "User-level reliability monitoring in urban personal satellitenavigation," IEEE Transactions on Aerospace and Electronic Systems, vol. 43, no. 4, pp. 1305–1318, 2007
38. Dinesh Manandhar,Ryosuke Shibasaki,"Dangers of Spoofing and Anti-Spoofing Solutions", Center for Spatial Information Science (CSIS), University of Tokyo, Japan 2017.
39. Qiong Yang, Yi Zhang, Chengkai Tang and Jie Lian,"A Combined Antijamming and AntiSpoofing Algorithm for GPS Arrays", Published in International Journal of Antennas and Propagation, 9 pages, vol 2019.
40. Candès, Emmanuel J., Romberg, Justin K., Tao, Terence, "Robust Uncertainty Principles: Exact Signal Reconstruction from Highly Incomplete Fourier Information", Published in IEEE Trans. Inf. Theory. 52 (8): 489–509. 2006

41. T. E. Humphreys, "Detection strategy for cryptographic gnss anti-spoofing," Published in IEEE Transactions on Aerospace and Electronic Systems, vol. 49, no. 2, pp. 1073–1090, 2013
42. D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," NAVIGATION:Journal of the Institute of Navigation, vol. 59, no. 4, pp. 281–290,2012.
43. K. D.Wesson, J.N. Gross, and T. E. Humphreys, "GNSS signal authentication via power and distortion monitoring," IEEE Transactions on Aerospace & Electronic Systems, vol. 49, no. 2,pp. 1073–1090, 2017.
44. M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, "GNSS spoofing detection: Correlating carrier phase with rapid antenna motion," GPSWorld, vol. 24, no. 1, pp. 53–58, 2013.
45. M. L. Psiaki, B. W. OHanlon, S. P. Powell et al., "GNSS spoofing detection using two-antenna differential carrier phase," in Proceedings of the 27th ITM ION, pp. 2776–2800, Florida,USA,2014.
46. C.H.Kang, S.Y.Kim, andC.G. Park, "Adaptive complex-EKF based DOA estimation for GPS spoofing detection," IET Signal Processing, vol. 12, no. 2, pp. 174–181, 2018.
47. A. Broumandan, A. Jafarnia-Jahromi, and G. Lachapelle, "Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver," GPS Solutions,vol. 19, no. 3, pp. 1–13, 2015.
48. F. Wang, H. Li, and M. Lu, "GNSS spoofing countermeasure with a single rotating antenna," IEEE Access, vol. 5, no. 99, pp.8039–8047, 2017.
49. Y. Hu, S. Bian, B. Li, and L. Zhou, "A novel array-based spoofingand jamming suppression method for GNSS receiver," IEEE Sensors Journal, vol. 18, no. 7, pp. 2952–2958, 2018.
50. J.Li, J.Zhang, S. Chang, andM.Zhou, "Performance evaluation ofmultimodal detectionmethod for GNSS intermediate spoofing," IEEE Access, vol. 4, pp. 9459–9468, 2016.
51. M. R.Mosavi, Z.Nasrpooya, andM. Moazedi, "Advanced antispoofing methods in tracking loop," Journal of Navigation, vol.69, no. 4, pp. 883–904, 2016.
52. M. Troglia Gamba, M. D. Truong, B. Motella, E. Falletti, and T.H. Ta, "Hypothesis testing methods to detect spoofing attacks: a test against the TEXBAT datasets," GPS Solutions, vol. 21, no.2, pp. 1–13, 2017.
53. S. Han, L. Chen, W. Meng, and C. Li, "Improve the security of GNSS receivers through spoofing mitigation," IEEE Access, vol.5, no. 99, pp. 21057–21069, 2017
54. Michael Jones, Spoofing in the Black Sea: What really happened?, Oct 11,2017. Accessed on May 20,2019.[Online]. Available: https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/
55. Frankie Youd,10 Pokemon Go Hidden Tricks That Still Work And 10 That Got Banned, Nov 17, 2018. Accessed on May 20, 2019.[Online]. Available: https://www.thegamer.com/pokemon-go-tricks-still-work-banned/
56. Oleg Petrovesky, HPE Security Research,GPS technology is more at risk from cyber attack than ever before, Sept 14, 2016. Accessed on May20,2019.[Online]Available:https://www.virusbulletin.com/blog/2016/september/turns-out-gps-technology-more-vulnerable-cyberattack-ever-security-expert-demonstrates/
57. "GPS Location Privacy", Oct 2018,Accessed on May 20,2019. [Online] Available: https://www.gps.gov/policy/privacy/
58. Jaroslaw Magiera, "A Multi-Antenna Scheme for Early Detection and Mitigation of Intermediate GNSS Spoofing," MDPI Journals, Sensors 2019, issue 10, 2411, 2019
59. Li, W.; Huang, Z.; Lang, R.; Qin, H.; Zhou, K.; Cao, Y. "A Real-Time Interference Monitoring Technique for GNSS Based on a Twin Support Vector Machine Method" Sensors 2016, 16, 329.
60. Wang, F.; Li, H.; Lu, M. "GNSS Spoofing Detection and Mitigation Based on Maximum Likelihood Estimation" Sensors 2017, 17, 1532.
61. Tao, H.; Li, H.; Lu, M."A Method of Detections' Fusion for GNSS Anti-Spoofing" Sensors 2016, 16, 2187.
62. Xu, B.; Jia, Q.; Luo, Y.; Xu, B.; Hsu, L.-T. Intelligent GNSS LOS/Multipath/NLOS Classifiers based on Correlator, RINEX and NMEA-level Measurements. Remote Sens. 2019, 11, 1851.
63. Qian Meng,Li-Ta Hsu,Bing Xu,Xiapu Luo and Ahmed El-Mowafy "GPS Spoofing Generator Using an Open Sourced Vector Tracking-Based Receiver" Sensors 2019, 19(18), 3993

AUTHORS PROFILE

Rejo Mathew, is M-Tech in Information Technology from NMIMS University. He has rich industry experience in Telecommunications working with Orange - France Telecom for five years. He has authored two books and 40 international research papers in IEEE, Elsevier, Springer, ACM. He is a reviewer in various international conferences and referred journals. His research interest includes Wireless Networking, Internet of Things, Security and performance issues of communication systems.