Impact and Detection of GPS Spoofing and Countermeasures against Spoofing

Mukhtar Ahmad
Capital University of Science and Technology
Islamabad, Pakistan

Muhammad Atif Farid
Islamia College Peshawar
Peshawar, Pakistan

Sheeraz Ahmed
Iqra National University
Peshawar, Pakistan

Khalid Saeed
Shaheed Benazir Bhutto University
Sheringal, Pakistan

M. Asharf
Capital University of Science and Technology
Islamabad, Pakistan

Usman Akhtar
UET Peshawar
Peshawar, Pakistan

Abstract --- As GPS signals are weak broad casted signal over wireless channels therefore they are vulnerable to in-band interference. Even a low power interference can spoof the GPS, which can cause destruction. Because of the above discussed reasons spoofing and anti-spoofing techniques are the emerging issues of the field of GPS. Generally, the spoofer try to generate or mimic the actual GPS signals to mislead a GPS receiver and spoofing works since the targeted receiver is not aware of it. Spoofing is becoming easier and cheaper because of advancement in SDR (software defined receiver) technology.

Keywords --- Detection, Global Positioning System (GPS), Global Navigation Satellite System (GNSS), Interference, Jamming, Position, Signals, Satellite, Spoofing.

I. INTRODUCTION

GPS now a day is an essential part of our navigation and positioning systems. These days each aircraft, cargo ships, even vehicle and mobile phones are equipped with GPS. Being such widely used and essential tool GPS is becoming an attractive target for criminals and hackers. Since GPS signals come from satellites that are 1300 miles away, the atmosphere in between also contains biases and errors, and induces errors in GPS signals. These biases and errors also effect GPS communication adversely [1]. Similarly satellites signals are so extremely weak that they are vulnerable to any kind of intentional and unintentional radio frequency interference [2]. To commence a spoofing attack, the spoofer first transmit counterfeit signals that are code-phase aligned according to original GPS signals but are at a power which is below and hidden in the noise floor. After that the power of spoofing signals is increased by the spoofer so that it is slightly greater than that of authentic signals [3]. By this moment the victim receiver's tracking loops are in control of spoofer and now spoofer can slowly take the spoofing signals away from the original GPS signals. The victim receiver can be stated now completely owned by the spoofer, once the spoofing signals has moved the receiver 2 microseconds in time or 600 meters in distance away from the authentic navigation solution [4]. If the spoofer attempts the attack according to the above stated condition it will be called a synchronous attack otherwise it will be asynchronous spoofing attack as shown in Fig. 1.

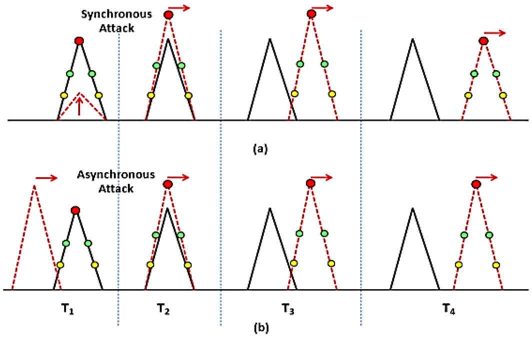

Fig. 1. (a) Synchronous spoofing attack. (b) Asynchronous spoofing attack [3]

II. Vulnerability of GPS Dependent Infrastructure against Spoofing Attack

Keeping in mind the ease with which a spoofing source can affect some GPS receivers, it suggests that infrastructure which is GPS-dependent is also vulnerable to GPS-spoofing attacks, since it is directly connected to GPS itself. Just for example the power grid and telecommunication network both these systems depends upon GPS time-reference receivers for retrieving accurate and precise timing [4]. Similarly, many other applications acquiring position, time and velocity are dependent on GPS services.

A. Vulnerability of Telecommunication Network

Code division multiple access (CDMA) cell-phone base stations depends upon GPS timing for their required tower-

978-1-5386-9509-8/19/$31.00 ©2019 IEEE

to-tower synchronization. The achieved synchronization helps in preventing communicating towers to interfere with each other, hence the process of call hand-off is possible. If a particular's tower timing is disrupted more than 10 microseconds from actual timing, all hand-off processes of the victim tower are disrupted [4]. A spoofing source can induce a 10 microsecond deviation in time within 30 minutes for a typical CDMA tower. Similarly, a coordinated spoofing network could also cause multiple of neighboring telecommunication towers to interfere with each other.

B. Power-Grid Vulnerability

Real-time measurements of voltages and current phasors results in a higher efficiency of power distribution across the grid. For the stated purpose Phasor measurement (PMU's) unit have been proposed as a smart-grid technology. To time-stamp their measurements PMU's rely on GPS. After time-tamp measurements are then sent to central station for processing. Variations in measured phase angles could be caused if a spoofer can disrupt the PMU's time-stamp. Power flow or stability estimates are distorted because of these variations, in such a way that grid operators would take false actions such as shutting down or powering electricity generators, which can cause damage to power-grid equipment or cause blackouts [4].

III.What Is the Main Difference Between Jamming and Spoofing?

GPS jamming refers to the act of intentionally directing electromagnetic waves in the direction of a navigational receiver system with the aim to prevent or disrupt signal reception [5]. So jammers who will to disrupt GNSS services, broadcast their interference signal in the frequency band utilized in navigation by satellites. Sometimes interference due to other communication can be a reason of denial of GNSS services in a geographical location, but jamming refers to intentional approach of interfering GNSS services in some location.

While Spoofing of a GPS receiver refers to a deliberate and intentional transmission of fake/false GNSS signals with the intention of fooling a GNSS receiver so it can retrieve a wrong Position, Velocity and Time (PVT) data [5]. Unlike jamming the main intention behind a spoofing attack is to secretly force a GNSS receiver to track down the fake GNSS signals with the main objective to providing wrong navigational solution.

IV.Various Spoofing Generation Techniques

A. Spoofer That Simulates GPS Signals

In this category of spoofers GPS signal simulator connected with a RF front-end is used. The simulator is used to copy the authentic/actual signals of GPS. Spoofers in this category are having signals which are unsynchronized to actual GPS signal that's why these can be discriminated. But still these can mislead a commercial GPS receiver by using higher power spoofing signals [6], [4].

B. Receiver-Based Spoofer

Receiver based spoofer consists of a spoofing transmitter connected to a GPS receiver. These spoofers first synchronizes itself with the currently available signals of GPS. After that they generate a spoofing signal targeted towards the receiver antenna of the target. This kind of spoofing signal is difficult of discriminate because of matching signal delay and strength. The spoofer faces the difficulties like aligning the phase and the carrier frequency to the authentic signal. Spoofer within a small distance from the target antenna can cause real damage because they are accurately synchronized to the actual GPS signals [6], [4]. Fig. 2 shows the basic setup of this kind of receiver based spoofers.

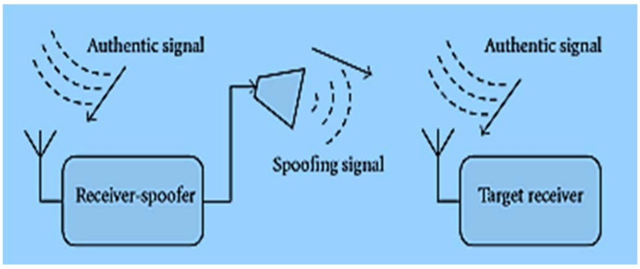

Fig. 2. Receiver based spoofers, first they receive authentic GPS signal produce spoofing signals that are aligned to authentic GPS signals [6].

C. Sophisticated Receiver-Based Spoofing

These are the most complicated and effective spoofers, as they are having extremely precise knowledge the receiver antenna phase center of their target. These types of spoofers not only copy the spatial distribution of visible satellites, but also their mutual alignment and content [4]. The effective region of this kind of spoofer is very small because array manifold synchronization and of carrier phase alignment is acquired only for a small area. Similarly, this kind of spoofing technique becomes impossible in many cases because of movement and geometry of the targets receiver antenna [6].

V. How Vulnerable is GPS against a Spoofing Attack?

The GPS vulnerability against a spoofing attack can actually be figured out in the following operational layers of current GPS receivers.

A. Vulnerability of GPS at Signal Processing Level

Various readings of a GPS signal are publically known like its modulation, transmission frequency, signals bandwidth, pseudorandom noise (PRN) signals etc. Similarly most GPS receivers do have an automatic gain control (AGC), these AGC units increase the GPS vulnerability. As the receiver input gain against the more powerful spoofing signals is automatically adjusted by the AGC units [6]. Being aware of all these GPS features for a civilian use, a GPS spoofer can easily generate fake signals in order to spoof the receiver.

B. *Vulnerability of GPS at Data Bit Level*

Various parts of the navigation frame such as almanac (the information of status and time of the entire constellation of satellites), telemetry information, and satellite ephemeris (data with the help of which the position of each satellite in orbit can be calculated) do not change rapidly. Like satellite ephemeris information is accessed in a minute but it do not changes for about 12.5 minutes. This kind of stability helps the spoofer to regenerate the GPS data frame easily [6].

VI. Practical Use of Spoofers in Real World

Various GPS spoofing events have already occurred, some of the famous GPS spoofing events are given below.

In the ''Iran – U.S. RQ – 170 incident'' the Iranian forces captured a U.S Lockheed Martin RQ-170 Sentinel unmanned aerial vehicle (UAV) by the help of a GPS spoofer in December 2011. This incident was first denied by the U.S military, but was confirmed later on after few days [5].

In 2013 and 2014, University of Austin, Texas, researchers utilized their own-built GPS spoofer for spoofing demonstration. They successfully demonstrated spoofing a drone and a yacht worth $ 80 million. The researchers caused the yacht to go in zigzag motion, even though the autopilot was still reporting the straight course [5].

VII. Proposed Anti-Spoofing Techniques

Anti-spoofing techniques can generally be divided into two main categories. Which are spoofing detection and its mitigation/counter-measure [6]. Spoofing mitigation deals with neutralizing or performing countermeasures against the spoofing signals, so that the effects of the detected spoofer can be eliminated. While detection of spoofing deals with discrimination of the spoofing signals, so that presence of a spoofer can be detected.

A. *Spoofing Detection*

Unlike jamming, in the case of spoofing normally the neither the GPS receiver nor the user is aware of the GPS attack. Due to this fact detection of spoofing is also a big challenge. Various methods with the help of which a spoofing attack can be discriminated are given below as.

1. Methods Based On Power Monitoring Of Signals

a) C/No Monitoring

C/No measurements characterize the quality of the received signal. In normal conditions there is no variation in the power measurements of the received signal but, when a spoofer with high power tries to misleads/attacks the GPS the received C/No may suddenly change. So we can check for a spoofing attack by simply constantly monitoring the C/No measures [6].

b) Absolute Power Monitoring

The estimate of transmitted power required to impose sufficient effect on the victim's receiver is a difficult job for a GPS spoofer. Similarly not exceeding the typical power level while imposing spoofing is a hard guess to make. Therefore receiving an absolute power higher than expected/nominal signal power of GPS is evidence of presence of spoofing attack [6]. Hence a check on a spoofing attack can be set by constantly monitoring the absolute power received by the GPS receiver.

c) Receiver Power Variation versus Receiver Movement

The case of a free space propagation the received power of a signal is inversely proportion to square the propagation distance. Now the satellites of GPS constellation are about 20,000 kilometers away from the surface of earth. Therefore movement of the receiver should not cause any considerable change in the power of the received signal, on the other hand a spoofer is much near to the receiver antenna as compare to the authentic satellite, so the movement of the receiver antenna should cause a considerable difference in the received power of the spoofing signal C/No [6]. A comparison between the C/No of both spoofing signal and authentic GPS signal due to relative motion of receiver antenna is shown in Fig. 3.

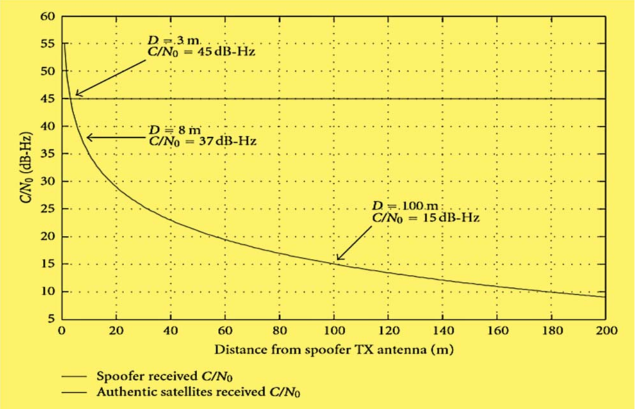

Fig. 3. Variation of authentic and spoofing received C/No versus distance of GPS receiver from spoofing source [6].

d) Comparison of L1/L2 Power Levels

The difference between various signals of GPS is predefined in different frequency bands. Many GPS receivers by various manufacturers are capable to monitoring both L1 and L2 frequencies of GPS. In case of a low-complex spoofer only L1 0signals are produced. So for this case any big difference in L1 and L2 power levels or complete absence of L2 frequency is the proof of presence of the spoofing [6].

978-1-5386-9509-8/19/$31.00 ©2019 IEEE

2. Spatial Processing For Spoofing Detection

The authentic signals of a GPS are transmitted from different directions and from different satellites while the spoofer transmit several spoofing signal by a single antenna in a single direction. Therefore, the spatial correlation of different signals can be checked using a spatial processing technique.

a) Multi-Antenna Spoofing Discrimination

Reference [7] presents a technique in which phase difference between two fixed antennas is observed for around an hour. Knowing the satellite movement trajectory and antenna array, knowing all this information theoretical phase difference is calculated. The calculated phase difference is then compared to practically available ones, which are observed by the antenna array. Both these results are compared to detect the presence of spoofing.

In [8] for the sake of detection and mitigation of spoofing signals an antenna array is used, so it can detect spoofing signals on the basis of their spatial correlation. The output phase measurements of the correlator for different PRN signals are compared mutually. So the ones that are received from the same spatial region are discriminated.

b) Spoofing Discrimination Using Synthetic Array

There is a spoofing discrimination technique in which a single antenna GPS receiver held in hand is moved along a random trajectory. The motion in this random trajectory forms a synthetic antenna array structure, as shown in Fig. 4. A coefficient metric is used to continuously compare the amplitude and phase which are received corresponding to different PRN signals. Spoofing signals are detected after acquiring different PRN signals in the received signal sets [6].

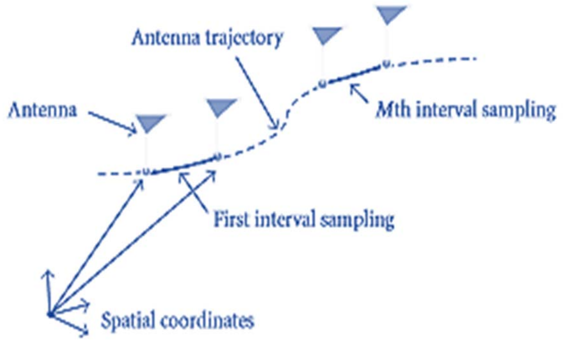

Fig. 4. Synthetic antenna array structure formed by moving a handheld GPS receiver [6].

3. Spoofing discrimination using Time of arrival (TOA)

Relative delay in signal arriving time can also be used to discriminate spoofing from authentic signals the methods are proposed as.

a) Delay Bit Latency and PRN Code

For the case in which a receiver based spoofer is used and the spoofer isn't having any prior data of navigation bits. Then the spoofer have to first retrieve the information from the GPS signal and then generate a spoofing signal, which costs some time. Hence there will exist a delay between the authentic signal and the received spoofer signal at the receiver side. Therefore a spoofing attack might be present if any data bit transition happening at time instants with spacing other than 20 millisecond. There are some cons in this technique that the data frame of GPS is already well known so the spoofer can predict the data before it starts the spoofing activity [6].

b) The Relative Delay of L1/L2 Signals

As encrypted codes are sent by GPS satellites on both L1/L2 frequencies so, there is a relative delay caused by various frequency responses of ionosphere. Therefore if a GPS receiver capable of tracking both frequency bands correlates both received frequencies there should be only a single correlation peak. Similarly L2 band signal is having more propagation delay than the L1 band signal, and the delay is known to the GPS receiver [6]. In order to defeat this countermeasure the spoofer needs to generate the signals on both L1 and l2 frequencies.

4. Spoofing Discrimination Using Signal Quality Monitoring (SQM)

The SQM technique is used previously for monitoring the quality of correlation peak in multi-path fading environment. The correlator output is also affected in the similar way by a spoofing attack on a tracking receiver. Therefore the SQM techniques can be used to discriminate an attack of spoofing on receivers that are in line-of-sight (LOS) conditions.

Various SQM tests can also be used to check for abnormal flatness or asymmetry of correlation peaks of GPS that are imposed to spoofing attack [9]. A spoofing attack tries to deceive the receiver towards tracking its fake correlation peaks after once the receiver has initially locked onto the authentic correlations peaks. SQM technique is very effective anti-spoofing technique for LOS conditions, while its effectiveness is reduced in multipath condition since it cannot differentiate between the multipath and spoofing attack.

a) Consistency Check with Other Navigation and Positioning Technologies

Another way of checking for the presence of a spoofer is comparing the signal extracted by GPS to other positioning technologies like WIFI or other networks, so if the information from both the sources do no match there is a high chance of presence of spoofing. Or simply data from inertial measurement unit (IMU) unit can be used for discriminating the spoofing signal, since IMU measurements can also be used to obtain navigational solution [3]. But this all increases the complexity of software and hardware similarly data from networks or Wi-Fi is not that accurate.

b) Cryptographic Authentication

We can add an authentication technique to Check for spoofing for both military and civil GPS systems. This technique is currently used for military GPS. Similarly it can be added to civil GPS, but a modifications in the GPS signal structure is required for most of the cryptographic authentication techniques [4].

Cryptographic anti-spoofing techniques are able to differentiate the spoofing signals from the authentic GPS signals. Cryptographic methods rely on the unpredictable nature of frequencies that modulate the GPS signals. Cryptographic authentication techniques involves many cross-checks and separate detectors, each capable of determining the spoofing attack. Fig. 5 determines how cryptographic verification block, timing consistency check, security-code estimation and replay attack (SCER) block, and jamming to noise (J/No) detection all work together.

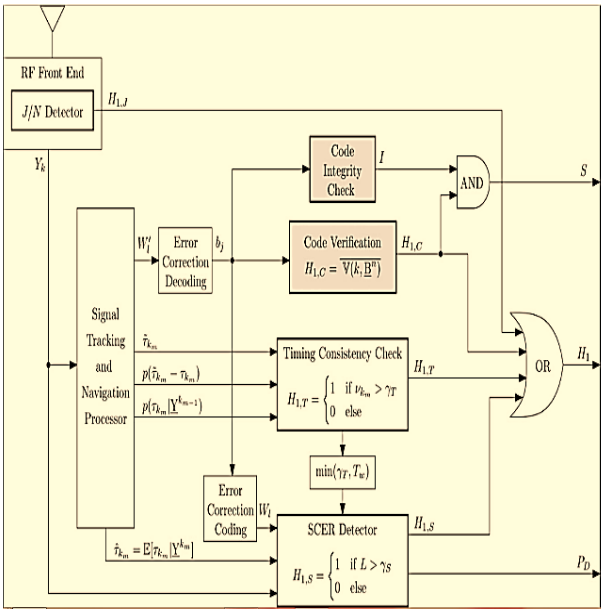
RF Front End
J/N Detector
$H_{1,J}$
Y_k
Code Integrity Check
I
AND
S
Signal Tracking and Navigation Processor
W_l'
Error Correction Decoding
b_j
Code Verification
$H_{1,C} = \overline{\mathrm{V}}(k, \underline{\mathrm{B}}^n)$
$H_{1,C}$
$\hat{\tau}_{k_m}$
$p(\hat{\tau}_{k_m} - \tau_{k_m})$
$p(\tau_{k_m} | \underline{\mathrm{Y}}^{k_{m-1}})$
Timing Consistency Check
$H_{1,T} = \begin{cases} 1 & \text{if } \nu_{k_m} > \gamma_T \\ 0 & \text{else} \end{cases}$
$H_{1,T}$
OR
H_1
$\min(\gamma_T, T_w)$
Error Correction Coding
W_l
SCER Detector
$H_{1,S}$
$\hat{\tau}_{k_m} = \mathrm{E}[\tau_{k_m} | \underline{\mathrm{Y}}^{k_m}]$
$H_{1,S} = \begin{cases} 1 & \text{if } L > \gamma_S \\ 0 & \text{else} \end{cases}$
P_D

Fig. 5. cryptographic verification block, timing consistency check, security-code estimation and replay attack (SCER) block, and jamming to noise (J/No) block all working together for GPS signal authentication [4].

c) Precision P(Y) Code Dual-Receiver Correlation

In this technique the precision P(Y) code which is unknown encrypted is correlated between two civil GPS receivers. Exploiting the known code-phase and carrier-phase relationship.

In this dual-receiver technique two receivers are utilized, one is located at a secure location. The duty of this receiver is to track down the authentic L1 frequency coarse acquisition C/A code while also receiving the encrypted precision P(Y) code. Here the secure receiver exploit the known phase and timing relationship between the precision P(Y) and coarse acquisition C/A code in order to isolate the precision P(Y) code. The secure receiver then sends the raw samples of the isolated P(Y) code over a secure connection to the second receiver which is facing the spoofing attack. The receiver under attack correlates the locally generated samples of P(Y) code to the ones send by the secure receiver. If there is a spoofing attack underway the power of correlation drops below a statistical level, and receiver under spoofing attack detects the attack [4].

5. 5. Code and Phase Rates Consistency Check

In the absence of spoofing attack, the code delay rate and the Doppler frequency are consistent since both they are being affected by same movement in between receiver and the GPS satellite. A cheap and low quality spoofer might not be able to keep stable this consistency. So the trick can be done by simply checking the output for consistency of the phase locked loop (PLL) filter and the delay locked loop (DLL) filter. The DLL and PLL filter outputs are estimates of delay and phase rates respectively [6].

a) Consistency Check of the Received Ephemeris Information

The navigational message of the satellites received by the GPS receiver contains corresponding to position of other satellites some ephemeris information. If there is any inconsistency found among the ephemeris data of various GPS satellites is proof of an unsynchronized spoofing attack [6]. While in the case of a complex synchronized spoofing attack this method fails.

b) Clock Consistency Check of GPS

The GPS clock information is found in the navigation message of each PRN signal. Which is in nominal situation consistent to that of other GPS satellites [6]. So if any inconsistency in extracted among GPS clock information of different satellites is a proof of spoofing attack.

B. Spoofing Mitigation

Spoofing mitigation methods are the countermeasures that are taken to cancel out the effect of spoofing signals on authentic GPS signals.

1. Detection of the Vestigial Signal

Complete suppression of an authentic GPS signal by a spoofer is quite difficult, since it requires the precise measure of antenna phase center position of the GPS receiver relative to antenna phase center of spoofing source. In maximum spoofing cases the vestige of the original GPS signals still remains even after a successful lift-off by a spoofing source. In vestigial signal detection a software based technique is implemented which is described as follow. First of all the incoming digitized front-end data is copied by the receiver in the buffer memory. Then the receiver selects one of

978-1-5386-9509-8/19/$31.00 ©2019 IEEE

GPS signals being tracked. Then the local generated version in the buffered data is removed by the receiver. After this an acquisition is performed by the receiver on the buffered data for the same selected PRN signal. The stated technique is quite same to successive interference cancellation (SIC). The issue with this stated technique is that it increases the processing and hardware complexity of receiver.

Similarly, for the case of GPS weak signals and high power spoofing attack the authentic vestige of GPS might not be still detectable, in such a situation the stated anti-spoofing technique might not work [6].

2. Multi Antenna Null Steering and Beam Forming Techniques

Array processing techniques can be used by a multi-antenna GPS receiver to shape its beam. So once the direction of the spoofing signal is detected the receiver can direct a null towards its source of generation and mitigate its threatening effects [10]. In another method called McDowell's method once the spatial correlation between different received signal pairs is determined the spoofing can then be discarded [8]. However these methods can increase the hardware and computational complexity of receivers. Since after processing the despread version of all received authentic and spoofing GPS signals the proper gain vector can only be achieved.

There is another spoofing mitigation technique proposed that filters out the spoofing signals on the basis of the spatial signature based on their spatial power after correlating different received signals from various antennas. Assuming that the several PRN signals are transmitted by the spoofer module. In which each PRN signal is having a power level comparable to that of authentic ones. Since all spoofing signals are coming from the same direction a steering null vector can be extracted corresponding to spoofing signals [10].

Fig. 6 shows average SNR of the spoofing signals and the authentic signals versus the average spoofing power. Results are shown for both the case of single antenna and proposed double antenna. For the case of single antenna the average SNR of authentic GPS signals is inversely proportional to average spoofing power. While the case of double antenna is totally different, here authentic signal's SNR remains stable while SNR of spoofing signals is always below the detectable threshold.

3. Receiver Autonomous Integrity Monitoring (RAIM)

In presence of spoofing signals fake pseudoranges are constantly injected in authentic GPS signals due to which the measurements are not consistent so a receiver autonomous integrity monitoring (RAIM) is performed by most of GPS receivers, in order to detect and then reject the fake signals and to gain consistency.

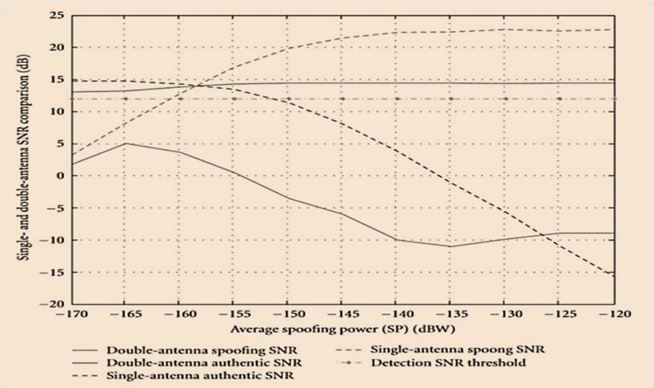

Fig. 6. Average SNR of the spoofing signals and the authentic signals versus the average spoofing power [10].

RAIM technique at position solution level can be used as an anti-spoofing technique. However RAIM can only be effective, if a few spoofing pseudoranges are present among many original pseudoranges. Otherwise RAIM technique might cancel out the authentic pseudoranges in order to decrease the residuals [6].

4. Using Adaptive Filtering For Spoof Cancellation

The block diagram of spoofing cancellation by the help of adaptive filtering system is shown in Fig. 7. The basic concept behind spoofing mitigation is of subtracting the spoofing signal after estimating it, from the input signal which is combination of both the authentic and spoofing signals. This anti-spoofing technique will only work if the source which is introducing the spoofing signals is present itself. As shown in the block diagram first received signal that are received by the GPS receiver are processed by RF filters, than are filtered down and are sampled into the digital intermediate frequency (IF) signal. Then the correlation function is performed in the phase-lock-loop (PLL) and delay-lock-loop (DLL) by the tracking module. The duty of estimating the correlation parameter of the spoofing signal is done by spoof estimator. It is all done with the help of a modified adaptive filters by employing a duplicated signal and a digital IF signal [11].The estimated signal parameters are then sent to the correlation decomposer. And the spoof cancellation area determines the correlation values of the spoofing signal. The estimated signal is then recreated at the modified adaptive filter. And is subtracted from the correlation value of the received signal which actually is a combination of both spoofing and authentic signals. Hence in this way spoofing is mitigated by the help of adaptive filters, and we get a spoofing-free signal [11].

VIII. A Multilayer Perspective of Anti-Spoofing Techniques

The anti-spoofing techniques from a multilayer perspective can be divided into three different categories. Namely, the signal processing level, data bit and position solution level and navigation level. Spoofing issue can be investigated at any of the above three mentioned levels [6].

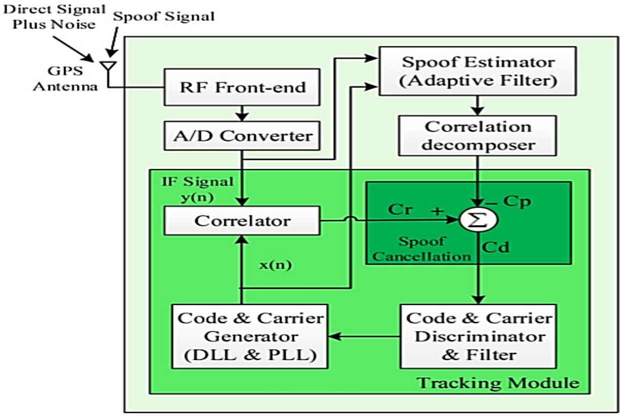

Fig. 7 Block diagram of adaptive filtering system used for spoofing mitigation [11].

IX.Spoofing/Anti-Spoofing Test Scenarios

Creating spoofing/anti-spoofing scenarios is challenging since in GPS band the outdoor radio frequency (RF) transmission is prohibited. Therefore in order to test spoofing/anti-spoofing system in the presence of authentic satellite signals special considerations should be taken. A few spoofing/anti-spoofing test scenarios are described below as.

A. Indoor Retransmission of GPS Signals

In this scenario to receive authentic GPS signals a rooftop antenna is used. Those signals are then amplified and retransmitted indoor by another antenna for this case a spoofer antenna is placed indoor so rules are not violated. This setup do not act as real spoofing conditions, especially multi-antenna spoofing, but still this is appropriate [7]. Basic setup of GPS indoor signal retransmission is shown in Fig. 8.

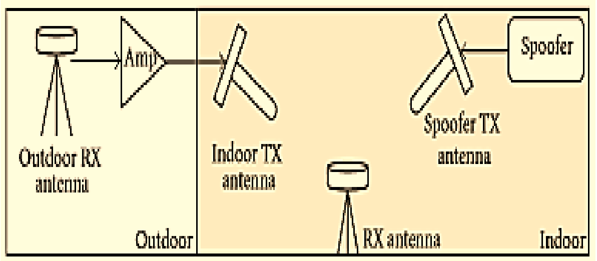

Fig. 8 GPS indoor signal retransmission used for spoofing test scenario [6].

B. Using Recorded Data for Spoofing and Without RF Transmission

Here in this case no actual RF transmission happens. First real GPS signals are digitized, and are then recorded on a hard drive After that these stored signals are fed into the GPS receiver-spoofer which tracks the available GPS signals and produces spoofing signals. Then these (digitized spoofing and GPS signals) are combined into a quantized bit stream. Then by interleaving (data reordering technique), original data is combined with output of bit stream. The result is then fed into targeted receiver [6]. Basic setup of ‘’spoofing without RF transmission using recorded data’’ is shown in Fig. 9.

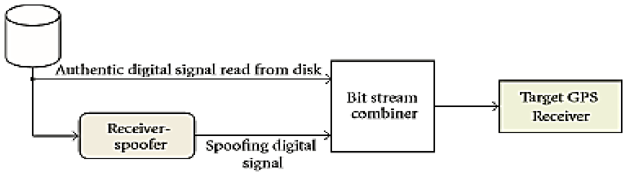

Fig. 9. Using recorded GPS data for spoofing test scenario [6]

C. Combining the Authentic and Spoofing Signals Using RF Combiners

RF power combiners can be used to combine the original signal from the GPS and locally generated spoofing signal. A network of attenuators and amplifiers can be used to adjust the resulted spoofing signal. Basic setup of the stated technique is shown in Fig. 10.

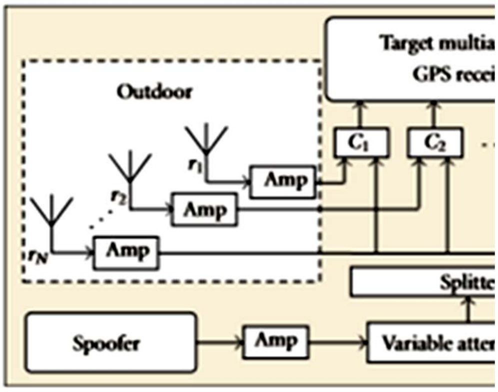

Fig. 10. Using RF combiners for a multi-antenna GPS spoofing test scenario [6].

X. Conclusion

In this paper first of all difference between a synchronous and asynchronous spoofing attack is presented. Then the vulnerability of GPS dependent infrastructure is discussed and various spoofing generation techniques are presented. It is showed that how vulnerable a GPS receiver is to a spoofing attack and which receiver stages are effected by a spoofing attack. Here the anti-spoofing techniques are divided into spoofing detection and countermeasure to spoofing. A detailed survey of both spoofing detection techniques and spoofing mitigation techniques is presented. At the end a spoofing/anti-spoofing test scenarios are presented. GPS spoofing detection and mitigation is relatively difficult to tackle with as compared to GPS jamming, an ideal anti-spoofing is one with less computational complexity, but high effectiveness.

978-1-5386-9509-8/19/$31.00 ©2019 IEEE

References

[1] Oeystein Glomsvoll, ''Jamming Of Gps & Glonass Signals,'' Department of Civil Engineering, Nottingham Geospatial Institute, September 2014.

[2] Daniele Borio, Fabio Dovis, Heidi Kuusniemi, and Letizia Lo Presti,"Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers," in proceedings of IEEE, Vol. No. 6, June 2016.

[3] 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.

[4] Kyle Wesson, Daniel Shepard, and Todd Humphreys,'' Straight Talk on Anti-Spoofing Securing the Future of PNT,'' GPS World Magazine, vol. 23, no. 1, pp. 32-63, 2012.

[5] Alexander RÜGAMER and Dirk KOWALEWSKI, '' Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!''.

[6] Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gerard Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Anti-spoofing Techniques," Hindwi Publishing Corporation International Journal of Navigation and Observation Volume 2012, Article ID 127072, 16 pages.

[7] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: experimental results 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.

[8] C. E. McDowell, "GPS Spoofer and Repeater Mitigation System using Digital Spatial Nulling—US Patent 7250903 B1," 2007.

[9] 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 SatelliteDivisionoftheInstituteofNavigation(IONGNSS'11), Portland, Ore, USA, September 2011.

[10] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A low complexity GNSS spoofing mitigation technique using a double antenna array,"GPS World Magazine, vol. 22, no. 12, pp. 44–46, 2011.

[11] M.R. Mosavi, Z. Nasrpooya and M. Moazedi,'' Advanced Anti-Spoofing Methods in Tracking Loop,'' THE JOURNAL OF NAVIGATION (2016), 69, 883–904. © The Royal Institute of Navigation 2016.

978-1-5386-9509-8/19/$31.00 ©2019 IEEE