Detection of Spoofed GPS Signals at Code and Carrier Tracking Level

Antonio Cavaleri
Politecnico di Torino, Electronics Department
Corso Duca degli Abruzzi 24, 10129 Torino, Italy
e-mail: antonio.cavaleri@polito.it

Beatrice Motella, Marco Pini and Maurizio Fantino
Istituto Superiore Mario Boella
Via P.C. Boggio 61, 10138 Torino, Italy
e-mail: surname@ismb.it

Abstract— **Due to the large amount of different new applications based on GNSS systems, the issue of interference monitoring is becoming an increasing concern in the satellite navigation community. Threats for GNSS can be classified as *unintentional interference*, *jamming* and *spoofing*. Among them, spoofing is more deceitful because the target receiver might not be able to detect the attack and consequently generate misleading position solutions. Different kind of spoofing attacks can be implemented depending on their complexity. The paper analyzes what is known as *intermediate spoofing attack*, by means of a spoofer device developed at the Navigation Signal Analysis and Simulation (NavSAS) laboratory. The work focuses on the spoofing detection, performed by implementing proper *signal quality monitoring techniques* at code and carrier tracking level.**

Keywords- Spoofing; Software Defined Radio Receiver; Signal Quality Monitoring; Ratio Test

I. INTRODUCTION AND BACKGROUND

Though Global Navigation Satellite Systems (GNSS), like GPS and Galileo, are based on Direct Sequence Spread Spectrum (DS-SS) technique, which brings an intrinsic robustness, signals broadcast by the constellations arrive at the antenna with an extremely low signal power level (i.e., approximately 20 dB below the noise floor), that makes GNSS-based civil infrastructures vulnerable to different disturbs. Interfering signals, either intentional due to jamming attacks, or unintentional caused by other Radio Frequency (RF) emitters, represent a severe threat for GNSS receivers. Scope of jamming is to obscure the navigation signals and prevent the availability of the signal in space. On the other hand, the intent of intentional transmission is more surreptitious and consists in providing the receiver with misleading signals, fooling the receiver to use counterfeit signals in space and compute erroneous positions. Such a transmission is referred to spoofing. While the GPS P-code is encrypted and therefore hard to spoof, the civilian GPS signal, the C/A code, is easier to spoof because the signal structure, the codes, and the modulation are open to the public.

A detailed classification of civilian spoofers can be found in [1], where they are listed as *simplistic*, *intermediate*, and *sophisticated*, depending on their complexity and the level of robustness required to the associated anti-spoofing techniques. A simplistic spoofer is basically a GNSS signals generator that transmits signals not consistent with the satellites in view. The intermediate and sophisticated spoofers add synchronization blocks, which make the counterfeit signals consistent with the real ones and result in spoofing attacks more difficult to detect.

In [1], authors remark that GNSS spoofing represents a growing risk for civilian applications. Spoofing is more sinister than other intentional interferences because the target receiver might not be able to detect an attack and consequently generate misleading position solutions.

The simplest spoofer is composed by a GPS signal generator connected to a transmitting antenna. This type of spoofer can be detected, because it is not able to synchronize the generated signals with the constellation in view. In this way, the transmitted signal is not consistent (in frequency, phase, code and data message) with the genuine signals received at the target receiver. In addition, this spoofer requires a GPS signal generator, generally implemented in hardware, which likely implies high costs.

In the case of an intermediate spoofing attack [1][2], the spoofing device has knowledge of the geometry of the satellites in view, Doppler shift, navigation data bits and received signal power. As described in [2][3], the spoofer simultaneously attacks each tracking channel of the target receiver by firstly performing code-phase alignment and then forcing the tracking loops to track the counterfeit signals [2]. A practical implementation of an intermediate spoofer combines a GPS software receiver with a transmitting RF front end. The high level of flexibility and the clear advantages coming from the Software Defined Radio (SDR) approach facilitated the development of PC-based receivers, where all the functionalities are performed on conventional general purpose processors. If appropriately modified, software receivers become spoofers by reversing the receiving chain, adding proper offsets to each satellite signal [3] and irradiating a modified version of the received signal. By the knowledge of the GPS time and the position of the target receiver's antenna, it is possible to generate counterfeit GPS signals that are code and frequency aligned with the authentic signals. As stated in [2], in this case the defense of the target receiver is significantly harder to implement than in the case of simplistic attacks.

A more sophisticated spoofing attack can be accomplished by using multiple transmitting antennas. With this solution, the spoofing module within the GPS receiver might control the relative carrier phases among the transmitting antennas and

978-1-4244-8739-4/10/$26.00 ©2010 IEEE

succeed in severe attacks, difficult to detect. On the other hand, the design and realization of such a multi-antennas spoofing device is not straightforward and might imply significant efforts.

Intermediate spoofing and the associated signal processing countermeasures required to detect an attack are the focus of this work. The paper starts describing different spoofing attack models. Some detection techniques, already proposed in literature (e.g.: Data bit latency defense, Vestigial signal defense [2]), are briefly reviewed. After assessing the effects of an intermediate spoofing attack on both signal acquisition and tracking, the paper explains how signal quality monitoring [5] represents a suitable solution for the detection of counterfeit signals, with the aim of raising a warning flag, if needed. Signal quality monitoring refers to proper algorithms, to be implemented within the GPS receivers, able to monitor the quality of the received GPS signal and warn users in case of any degradation or incorrectness. Generally, signal quality algorithms involve some measurements at the correlators output and a decision process that compares such measurements with predefined thresholds. Among all, reference [5] gives the theoretical background of the decision process and introduces a threshold mask, built around the shape of the correlation function, in order to detect the presence of distortions in real time. The paper presents some metrics (and simple algorithms) that could be used to monitor the quality of the received signal, protecting GNSS receivers against spoofed signals.

After this introduction, Section II presents the state-of-the-art of the techniques able to detect or partially prevent a spoofing attack. Section III recalls the basics of the acquisition and tracking process, and Section IV analyses the effect of an intermediate spoofing attack on the code and carrier tracking. The strategy to apply the algorithm of the signal quality monitoring to the spoofing detection is explained in Section V. A simulation example is also shown. Section VI summarizes the conclusions.

II. Overview of Defense Techniques against Spoofing Attacks

Different techniques have been proposed as spoofing countermeasures during the last decade. In literature a reasonable number of papers is dedicated to countermeasures based on cryptography. Signal authentication effectively binds a digital signature in the transmitted signals, protecting receivers from spoofing attacks. Among all, reference [7] describes different levels of authentication for the next generation of civilian GNSS signals. In [8] authors present a new authentication method, based on public spreading code (PubSCA). In addition to digitally signed navigation data, some security codes are embedded in the ranging signal, in definite time slots. These codes are broadcast according to the spread spectrum modulation and are received completely buried under the noise floor, like all GNSS signals. As a consequence, a spoofer equipped with standard receiving hardware has no chance to interpret them. All the methods based on authentication can ensure a high level of security but they do not provide sufficient protection against all possible spoofing scenarios. In fact, if authentication prevents signal-synthesis attack [9], like the intermediate spoofing, it might be not sufficient in case of the so-called replay attacks (i.e.: a receiver stores the raw samples at the front end output, then it replays and retransmits them at RF, without any additional processing). Furthermore, sophisticated spoofer devices, equipped with directional antennas, might be able to rise the RF signal above the noise floor and determine the security spreading codes [10]. All methods that foresee cryptographic on the transmitted signals require modification of the signal structure. Such changes appear extremely unlikely in the short term. Probably GPS will not incorporate authenticated signatures directly into the transmitted signals, due both to institutional priorities and to long procurement and deployment cycles. The European Galileo system, which will employ such features on a fee-based service on the E6 bandwidth, is still at a number of years from operational capability [10] and the level of signal authentication has not been defined yet.

Together with signal authentication, there is a significant interest towards standalone receiver-based defenses. Generally, all of them work at the base band signal processing and determine if the received signal is genuine or not.

As described in [2], a possible defense takes advantage of the difficulty of a spoofer to retransmit the GPS data bits in real-time. This defense consists in continuously monitoring the bit synchronization in the navigation message decoding, raising a flag if a bit sign transition is detected unexpectedly. However intermediate spoofers can prevail this protection either attempting to predict the data bit message (e.g.: like in the case of the lab spoofing device presented in [3]) or jamming the target receiver for a short period, forcing the loose of lock on the real signals. Another interesting technique introduced by T. Humphreys *et. al* in [1] is known as vestigial signal defense. The basic assumption behind this method is that during a spoofing attack, at least one counterfeit and one genuine PRN are present during or after lift-off. Therefore, the receiver can continuously monitor a reduce search space around the current tracking signal and detect the presence of a secondary peak. In case a vestigial signal is detected, the receiver raises a warning. This technique requires additional processing capabilities, as it involves weak signal acquisition, for each tracked PRN.

In [6], authors describe three different methods to detect a counterfeit signal during a replay attack. Since the final goal of a spoofer is to mislead the computation of the PVT solution at the target receiver, a possible way to recognize the drifting of the GNSS positions is through the aid of external sensors. In this case, the drawback is that all sensors suffer from internal noise that tends to introduce errors in the estimation of user's position. Therefore, they can be only used for the assessment of position for a short period of time. As a consequence, a second method that authors suggested is to check the presence of anomalies in the receiver's clock offset estimation, that can be due to the delay introduces by the spoofer. The third method relies on the difficulty of a spoofer to assess the Doppler frequency of the GPS receiver's location precisely. Therefore when the Doppler estimation overcomes a certain shift the target receiver can detect a malicious attempt to spoof it.

III. Fundamentals on GNSS Signal Acquisition and Tracking

GNSS receivers sample the analog signal at the output of the Intermediate Frequency (IF) filter and split the signal over different digital channels. The signal processing on the stream of samples at the output of the RF front end is based on the estimate of a 2-D correlation function, called Cross Ambiguity Function (CAF) [11]. The detection of a correlation peak within the CAF corresponds to the satellite acquisition and allows for a first raw estimate of the Signal-In-Space (SIS) parameters, namely code phase and Doppler shift. These parameters are then finely estimated over time by digital tracking loops, which synchronize the incoming carrier and spreading code with local replicas. It is recognized that such a synchronization corresponds to find the values of code phase and Doppler shift that maximize the CAF. The better is the synchronization, the more accurate is the computed user position. Clearly, distortions on the correlation peak due to external sources (i.e.: interfering signals, multipath, counterfeit signals in spoofing attacks) affect the accuracy of code and carrier tracking and deteriorate the pseudorange estimates.

A. Signal Acquisition

The signal acquisition corresponds to the search of the correlation peak in time and frequency domain. All acquisition systems for GNSS receivers are based on the Maximum Likelihood (ML) estimation theory and in practical implementations they evaluates only the code delay and the Doppler shift, ignoring both the unknown values of navigation data bit and carrier phase.

During the acquisition phase the receiver tests all the possible alignments, and if the tested PRN is included in the incoming signal, the correlation peak is detected. As stated in many books on GNSS signal processing, the signal acquisition is actually a two-dimensional search in time (code phase) and frequency. In fact, the correlation peak is detected only when the Doppler shift on the incoming carrier is estimated.

A large amount of literature proposes different techniques to perform the signal acquisition. Modern acquisition strategies, mainly for software implementations, are based on the Fast Fourier Transform (FFT). The FFT is used to efficiently evaluate the correlation between the incoming signals and the local codes, implementing fast acquisition techniques. Among all references, see [12] for details.

B. Code and Carrier signal tracking

The signal tracking relies on the signal correlation properties. Once the signal acquisition has detected the correlation peak, the receiver refines the estimates of code phase and Doppler shift and continuously tracks changes into the future. Considering one digital channel, the samples at the front end output are generally processed by the coupled loops composed by a Delay Lock Loop (DLL) and a Phase Lock Loop (PLL). Figure 1 shows the block diagram of a classical tracking system for GNSS receivers, which is well explained in [13].

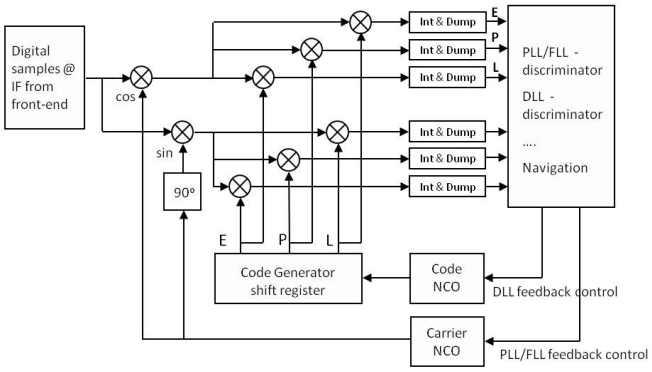

Figure 1: Block diagram of conventional code and carrier tracking loops

The DLL synchronizes the local and the incoming PRN codes, while the PLL generates an estimate of the phase and frequency of the received carrier. Both the loops must successfully track their respective signals, allowing the GNSS receiver to operate properly. Once the PLL is locked, the receiver decodes the navigation message at the output of the In-phase prompt correlator, performs carrier phase measurements on the basis of the local carrier, and updates a system of counters for pseudorange computation.

Tracking the incoming signal over time corresponds to continuously estimate the value of code phase and Doppler shift that maximize the CAF. Such an estimate is the core of conventional GNSS signal processing, which appears very sensitive to CAF distortions. For example, in satellite navigation it is well known the problem associated to multipath propagation. The presence of multipath leads to a CAF distortion along the code phase, which results in a degraded synchronization between the incoming and the local codes. Another example of CAF distortion is shown in [14], where authors demonstrated that even an inaccurate choice of the sampling frequency lead to a deteriorated correlation peak, which causes positioning errors on the order of tens meters.

The following section investigates the CAF distortion under a spoofing attack.

IV. Effect of Intermediate Spoofing Attacks on Code and Carrier Tracking

During an intermediate spoofing attack, when the spoofing device synchronizes the real and the counterfeit signals and forces some of the channels of the target receiver to lock the false signals, the CAF results distorted. Intermediate spoofers accurately reproduce the code phase, frequency and navigation data bits [1] and furtively align the correlation peak to the genuine one. After the alignment, the counterfeit signal power is gradually increased until it begins to control the tracking loops. This process generates a CAF distortion.

Figure 2 shows a set of three CAFs evaluated after the acquisition stage, at sequential time instants during a spoofing attack (i.e., @ 49.25, 49.6, and 49.95 s from the beginning of the processed data set).

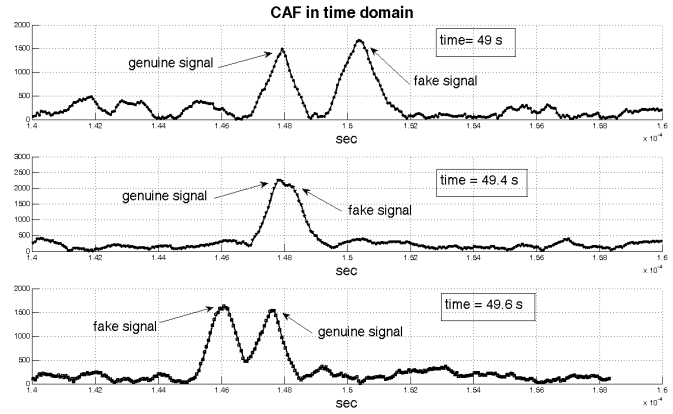

Figure 2: A sequence of frames showing the CAF in the code phase domain during an intermediate spoofing attack

Figure 2 refers to a data collection performed in lab (Figure 3), where counterfeit signals have been injected after the receiving antenna, using a RF combiner. These signals were generated with a lab-spoofing device [3], capable of code-phase align authentic and counterfeit signals. Note that this test well represents a situation where the spoofer and the victim receiver are placed onboard of the same platform (Limpet spoofer) [7].

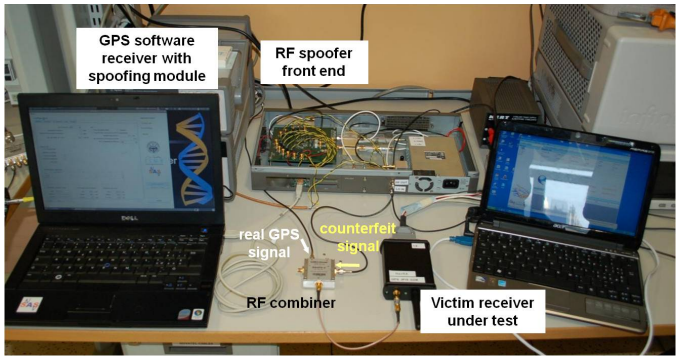

Figure 3: Spoofing attack experiment performed in laboratory

Thanks to the frequency consistency between the counterfeit and the genuine signals, the two correlation peaks have the same Doppler shift. For this reason the CAF in Figure 2 is represented along the code phase, expressed in seconds. In the first frame the counterfeit peak is approaching the genuine one from the right side (i.e.: its code phase is decreasing). In the second frame the alignment is successfully achieved. Both signals have the same code phase, the two peaks appear superimposed and the CAF distortion is recognizable. In our test the perfect signal alignment occurred after 49.65 s from the beginning of the data collection. In that instant, if the power of the counterfeit signal is slightly higher the real one, the code tracking loop locks the false signal. In the last frame the counterfeit signal has further decreased its code phase and the two peaks are moving away from each other. Note that if the signal lift-off was successful, that digital channel is now controlled by the spoofer and the receiver computes erroneous pseudoranges.

Note that, in order to make the attack successful, the counterfeit signal power level has to be properly tuned. In fact, it has to be smaller than the genuine signal's before the alignment. On the contrary, when both the signals are concurrent, the power should be increased in order to lift-off the correlators and take the control of the tracking.

The CAF computed in the frequency domain, at the three sequential time instants is shown in Figure 4. Since the two signals are perfectly aligned in frequency (i.e.: the lab spoofing device was able to process the signal on air and synchronize the false signal), the CAF does not present any distortion. Only if the real and the counterfeit signals were not consistent in frequency, the shape of the CAF observed in the frequency domain would result corrupt.

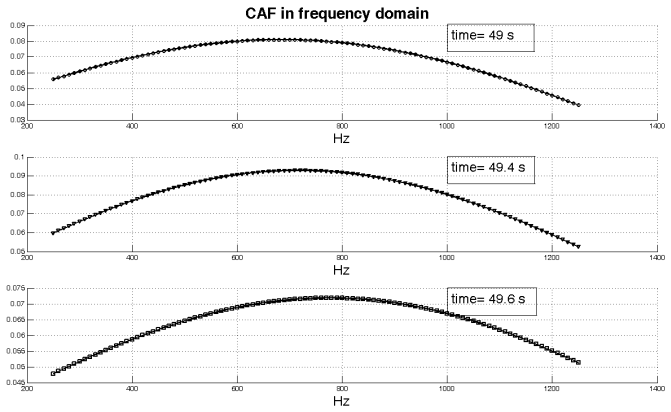

Figure 4: A sequence of frames showing the CAF in the frequency domain during an intermediate spoofing attack.

CAF distortions have considerable effects on code and carrier tracking. Figure 5 shows the absolute values of the Early, Prompt and Late correlators during the spoofing attack. The figure refers to the processing of a second order DLL with bandwidth equal to 2 Hz, coupled with a costas PLL with a bandwidth of 15 Hz. The integration time was set to 10 ms.

The different moments of the attack shown in Figure 2 are labeled with the numbers 1, 2 and 3.

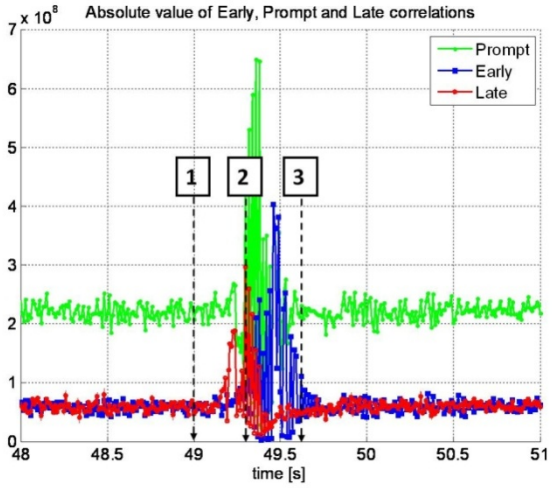

Figure 5: Absolute values of the Early (blue), Prompt (green) and Late (red) correlators, during an intermediate spoofing attack

The effect of the code-phase alignment of the counterfeit signals results in a distorted early-minus-late discriminator, which is non linear. In this case, the DLL is not able to generate a suitable feedback control signal proportional to the delay between the real PRN and the local Prompt code, at the end of the integration period. Under these circumstances the code synchronization of the real signal becomes problematic as it is shown in Figure 5 around 49.5 s. This unusual effect is simply due to the distorted correlation and can be used for spoofing detection. A similar effect can also be monitored on the carrier tracking loop.

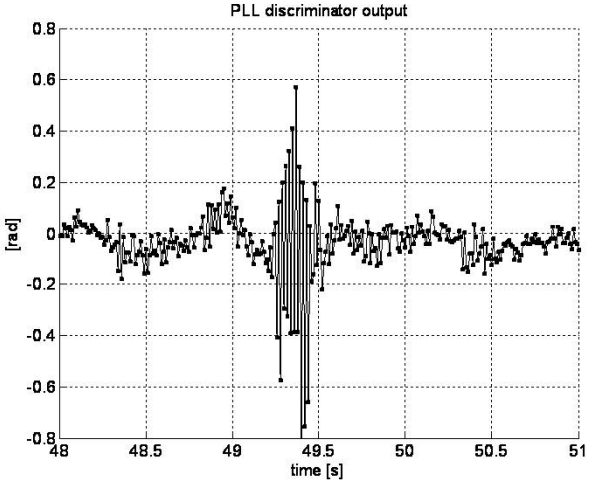

Figure 6: PLL Discriminator output, during an intermediate spoofing attack

Figure 6 shows the output of the Costas PLL discriminator, during the spoofing attack. Although the counterfeit signals are frequency synchronized to the real ones, when the correlation peaks collide, the Costas PLL discriminator is not able to generate a correct feedback. As for the DLL, if the power of the counterfeit signal increases, the PLL loop is forced to unlock the real signal.

V. Signal Quality Monitoring as Detection Mechanism

The CAF distortion due to an intermediate spoofing attack is not far distant to the effect of a strong multipath, which arrives in-phase with the LOS. In satellite navigation, the process dedicated to detect signal distortions, which assures a certain level of accuracy, reliability and robustness of the estimated position, is generally addressed as *signal quality monitoring*. Techniques for evaluating the quality of the estimated position solution, namely how well the solution of a problem is known, can be based on the observation of several different parameters and they can be assessed at different navigation system levels. The quality monitoring has been usually applied to detect malicious signal as multipath. A large amount of work has been presented in [4][15]. In [5], Fantino *et. al* mathematically described what happens to the autocorrelation function during events that degrade the signal quality, especially in multipath propagation. The same approach can be used to characterize the CAF distortion during the signal lift-off. As an intermediate spoofing attack affect the conventional signal processing of code and carrier tracking loops, a proper detection mechanism can be implemented at this level to detect spoofed GPS signals. Such signal quality technique involves proper measurements at the correlators output and a decision process that compare such measurements with predefined thresholds. In literature, several metrics are proposed [4][15], since many are the possibilities to combine the correlation values. As in [5], we used the *Ratio Test* metric, considering its capability to detect the correlation distortions.

The Ratio Test metric is:

$$R_\delta = \frac{E_i^{\frac{\delta}{2}} + L_i^{\frac{\delta}{2}}}{\alpha P_i}$$

where:

- E_i, L_i and P_i represents the Early, Late and Prompt correlator output over the in-phase branch;
- δ is the correlator spacing between E_i and L_i
- α is the correlation main peak slope. Considering the GPS C/A code this is equal to 1.

Figure 7 shows the behavior of the Ratio Test metric for a period of 60 seconds, where the intermediate spoofing attack occurs after 49.2 second. A threshold is built around the shape of the metric function and can be used to detect in real time the presence of a distortion. The figure shows how an attack can be easily detected through such a metric. The value of the threshold can be easily derived according to the theory presented in [5], given a determinate false detection probability.

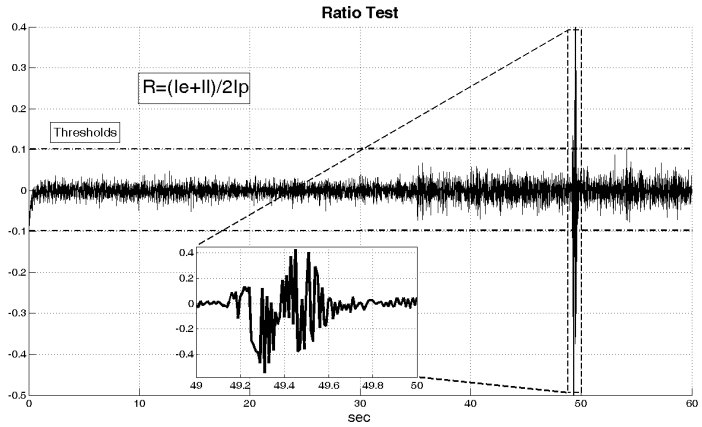

Figure 7: Ratio Test metric behaviour during a Spoofing attack

VI. CONCLUSIONS

The paper has analyzed an *intermediate spoofing attack* at baseband level, mainly at the acquisition and tracking stages. The attack has been performed through an experiment carried out in laboratory, by using a fully software GPS receiver-spoofer prototype. Taking into account proper *signal quality monitoring techniques*, commonly used to detect interferences (e.g.: multipath) or anomalies in the received signal, goal of the work has been making evidence of how the quality monitoring approach can be exploited to detect a spoofing attack.

After an analysis on the distortion of the CAF function in time and frequency domains and the PLL Discriminator output, the Ratio Test metric, presented in [5], has been applied to detect the attack of the spoofer. When the Ratio Test value exceeds a predefined threshold a flag can be raised to alert the target receiver user. Simulations results based on lab tests experiments have been presented.

As next step of the analysis, a decision process based on statistical hypothesis (such as Neumann-Person or Bayesian theory) can be investigated and implemented. Moreover, other possible detection countermeasures, to be applied at baseband, have to be studied. Examples are the use of multicorrelator structure, to detect anomalies in the received signal, or the linear combinations of correlators, to look for asymmetries in the correlation peak.

REFERENCES

[1] T. E. Humphreys at al., "Assessing the spoofing threat: development of a portable GPS civilian spoofer," in the Proc. of ION GNSS 2008, 16-19 September 2008, Savannah, GA.

[2] B. M. Ledvina at al., "An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers," in the Proc. of National Technical Meeting - ION NTM 2010, 25-27 January 2010, San Diego, CA.

[3] M. Nicola, L. Musumeci, M. Pini, M. Fantino. P. Mulassano, "Design of a GNSS Spoofing Device Based on a GPS/Galileo Software Receiver for the Development of Robust Countermeasures", ENC GNSS 2010, Braunschweig, Germany, 19-21 October 2010

[4] Phelts P, Akos D, Enge P (2000) Robust Signal Quality Monitoring and Detection of Evil Waverforms. 13th Int. Tech. Meeting of the Satellite Division of the U.S. Inst. of Navigation, Salt Lake City, Utah, 19-22 September, 1180-1190.

[5] M. Fantino at al., "Signal Quality Monitoring: Correlation Mask Based on Ratio Test Metrics for Multipath Detection," in the Proc. of International Global Navigation Satellite Systems Society, IGNSS Symposium 2009, 1-3 December 2009, Surfers Paradise, Australia.

[6] P.Papadimitratos and A.Jovanovic, "GNSS-based Positioning: Attacks and Countermeasures", MILCOM 2008.

[7] Scott,L. "Anti-Spoofing and Authenticated Signal Architecture for Civil Navigation Systems", ION GPS2003, Portland, Oregon USA, 2003.

[8] G.W.Hein, Avila-Rodriguez J-A., et al. "Authenticating GNSS Proofs against Spoofs", InsideGNSS, pp.71-78, Sept/Oct 2007.

[9] M.G. Kuhn, "An Asymmetric Security Mechanism for Navigation Signals", IH 2004, LNCS 3200, pp.239-252, 2004.

[10] G.X. Gao, D. M.Akos, T. Walter, and P. Enge, "GIOVE-B on the Air: Understanding Galileo's New Signals," Inside GNSS, pp. 34-37, May/June 2008.

[11] B. Motella, L. Lo Presti, M. Petovello, "The math of ambiguity: what is the acquisition ambiguity function and how is it expressed mathematically?," *Inside GNSS*, June 2010, pp 20-28

[12] J.B. Tsui, *Fundamentals of Global Positioning System Receivers - A Software Approach*, JohnWiley Sons, Inc 2000, ISBN: 0471381543

[13] P. Misra, P. Enge, *Global Positioning System. Signal, Measurements and Performance*, Second Edition, Ganga-Jamuna Press 2006, ISBN: 0-9709544-1-7

[14] M. Pini, D.M. Akos, "Effect of Sampling Frequency on GNSS Receiver Performance," *Journal of The Institute of Navigation*, Summer 2006, Vol. 53, No 2, pp.85-95

[15] Mitelman AM (2004), Signal Quality Monitoring for GPS Augmentation System, Ph.D Dissertation Stanford University