IMPACT AND DETECTION OF GPS JAMMERS AND COUNTERMEASURES AGAINST JAMMING

Muhammad Atif Farid[1], Mukhtar Ahmad[1] , Sheeraz Ahmed [3, 4] , Saqib Shahid Rahim[2, 4]

[1]Islamia College, Peshawar, Pakistan
[2]Abasyn University, Peshawar, Pakistan
[3]Iqra National University, Peshawar, Pakistan
[4]Career Dynamics Research Centre, Peshawar, Pakistan

***Abstract*— Most of the systems that we use in our daily life, including critical sectors like, military, civilian forums, aviation and commercial industries are widely dependent on GPS services. Despite of providing countless services, GPS system under certain circumstances are vulnerable to both intentional and unintentional interferences. GPS jamming is the act of intentionally transmitting electromagnetic waves of same spectral band like GPS, with a high power in the direction of a victim GPS receiver, with the intention of denying the operation of GPS services. This paper describes a detailed evaluation of currently available GPS jammers and their impact on various GPS receiver stages. The case of intermediate power jamming is also evaluated, which is the most critical case, since user is still able to find a navigational solution. Various GPS jamming incidents of real life are also described and a review of jamming detection measures is also given. At the end a review of possible methods of jamming countermeasure and possible future work is stated.**

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

I. Introduction

Signals received from Global Navigation Satellite system (GNSS) are extremely weak powered signals, due to which these signals are too much vulnerable to both intentional and unintentional interference. It means even a small intentionally or unintentionally caused interference can cause severe issues. If we talk of jamming, then jamming is a type of intentional radio-frequency interference caused by devices called jammers. So in jamming intentionally powerful electromagnetic waves are transmitted toward a target receiver so its operation of receiving signals can be denied [1]. In this literature our main concern will be GPS intentional interference caused by deliberate jamming devices. Similarly, according to new research a jamming attack can be even more destructive if a simple jammer is combined with information of GPS signals in order to produce a more complex jamming signal. For example, a jamming device can be hooked up with a GPS receiver with the help of which a jammer can access all critical information that can be retrieved by a GPS receiver. So, now a jammer can produce even sophisticated and more effective jamming attack, such an attack is called Systematic jamming [2].

Jammers can deny the receivers operation in a wide geographical radius, even up to several kilometers. Knowing these facts, we can say that jammers are a real threat to all satellite navigation systems like GPS. On the other hand, unintentional interference can come through other television, very high frequency (VHF) transmitters, other personal and daily routine electronic devices [3]. Consequently, GPS is vulnerable to both intentional and unintentional as well as effects on signals due to ionosphere and signal blockage, and all these effects are dominantly noticeable to users who use single frequency.

II. Effect of Atmosphere

There is a distance of 13000 miles between GPS satellites and a GPS receiver. All this distance available between the satellite and the receiver contains errors and biases. The pseudorange is corrupted by the satellite clock offset and atmospheric biases from the ionosphere and troposphere. Ionosphere cause delay due to the presence of charged particles and radiation from the sun. While the troposphere presents variation in atmospheric pressure, partial water vapors, temperature and various weather events which altogether effects the signal [4]. The effect of

atmosphere on GPS signals is illustrated in figure 1.

III. Jamming Signals

On the basis of jamming signals reference [1] has divided jammers as following.

Group I: Jammers with Continuous Wave signal: these kind of jammer transmits a continuous wave (CW) signal.

Group II: Jammers with single saw-tooth chirp signals: these jammers transmit a frequency modulated signal with a saw-tooth time-frequency (TF) evolution.

Group III: Jammers with multi-saw-tooth chirp signals: these jammers transmit a frequency modulated signal. But its time-frequency evolution is even more complex and it is determined by the combination of several saw-tooth signals.

Group IV: Jammers producing chirp with signal frequency bursts. These type of jamming devices transmits a frequency-modulated signal. Frequency bursts enlarges the frequency band affected by the jamming signal.

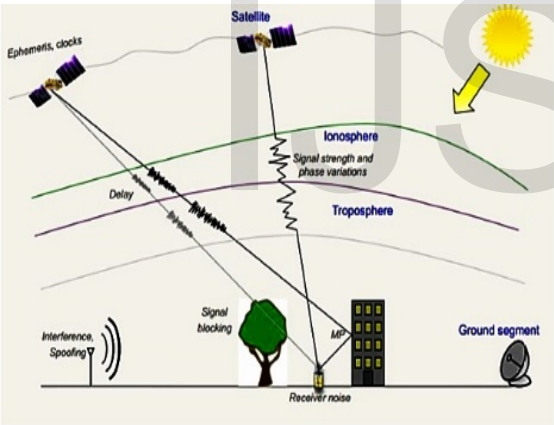


Figure 1: Impact of atmosphere on GPS signals [4]

IV. GPS Jamming Devices

Jamming signals that can disrupt GPS services can be broadcasted by a large variety of devices which can have various characteristics and properties as shown in figure 2. A classification of jammer devices based on the device characteristics is given in [1]. Here jammers are divided into three categories.

Class I: cigarette lighter jammers. These jammer devices are designed to be plugged into a car cigarette lighter with a 12 Volt power supply.

Class II: Subminiature version A (SMA) battery powered jammers. These jammer devices are powered by a battery. Battery is connected to an external antenna through an SMA connector.

Class III: non-SMA battery jammers. These jammer devices are powered by a battery and uses an integrated antenna for transmission of signals.

Although the previous two classifications captured most jammer characteristics, according to [1] the following aspects of jamming devices should also be taken in account.

a. Single-frequency jammers versus multiple-frequency jammers:
   Multiple-frequency jammers can affect several GNSS bands simultaneously.
b. Single-antenna versus multiple-antenna jammers:
   Some jammer devices are equipped with several antennas. So it can broadcast signals in different frequency bands.
c. Single-system versus multiple-system jammers:
   Some jammer devices can simultaneously affect GNSS services and other communications systems, for example Universal Mobile Telecommunication systems (UMTS) and Global System for Mobile Communications (GSM).

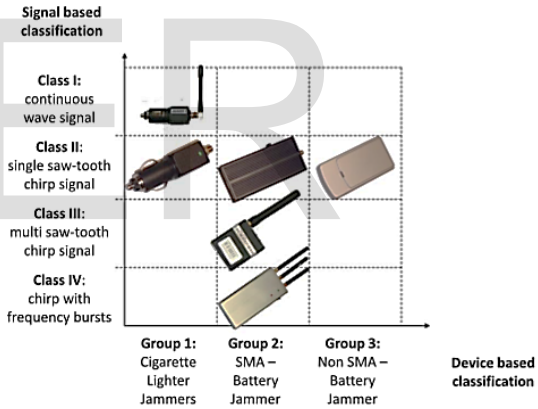


Figure 1: Classification of jammer devices on the basis of signal type and device characteristics [1].

V. Practical Examples of Jamming from Real World

GPS currently is our main tool of navigation, most of our daily use applications are entirely dependent on GPS. According to reference [5] 14 of 16 critical sectors of our daily life are crucially dependent on GPS. Jamming a GPS receiver nowadays has not remained that big of a deal, since different models of GPS jammers with different specifications are available online and are not that expansive. Similarly, there are tutorials available on different websites and on YouTube, teaching how to jam different devices and drones [6]. While on the other hand testing an anti-jamming technique is not an easy task, since there is always a danger of unintentional interference in open testing environment and also getting a permission from government bodies for an

experimental open environment jamming transmission is not an easy task [7]. Various famous jamming events have already taken place, a brief description of these illicit activities is described below.

A famous incident of jamming occurred at airport of Newark, New York, U.S. This time a UPS truck driver was using a personal protection device (PPD) on a highway near to airport. Due to which airport's ground based augmentation system (GBAS) was effected. As a result, planes trying GPS assisted landing were facing problems. Although the truck driver was unaware of the consequences, but still he was arrested [8].

Another famous incident of jamming happened when South Korea faced massive GPS jamming from North Korea. According to report in 16 days of jamming from North Korea, over 1000 planes and over 250 ships experienced GPS services disruption [8].

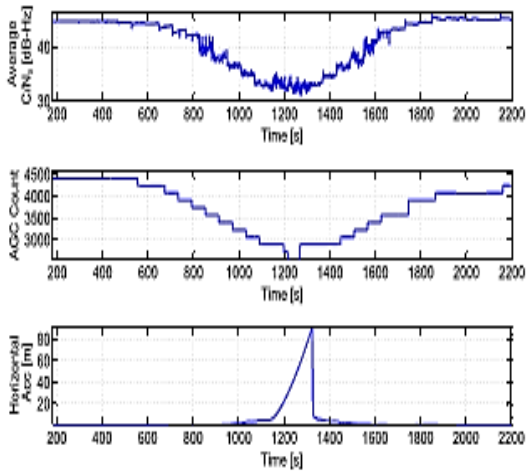
GPS services were disrupted all across San Diego, California in January 2007. It effected many sectors like air traffic flow, traffic management systems, bank departments and naval medical centers. Reason for this mysterious disruption of GPS signals was found after three days, it was found that two Navy ships in San Diego harbor were conducting a practice jamming exercise [9].

VI. JAMMING IMPACT ON GPS RECEIVERS

Mostly jammers try to completely deny GNSS service in a targeted geographical location, by transmitting enough strong power. For such a case GNSS services are completely denied and the user are well aware of attack. For an intermediate jamming attack in which the power values are low enough to decrease receiver's efficiency, but not low enough to loose lock or completely deny GNSS-based applications. Such a case is most dangerous one since targeted receiver is still able to present navigation, but the results are faulty and are containing biases and errors [1]. Figure 3 shows the impact result of a jamming signal on a highly sensitive GNSS receiver (various metrics that are sensitive to the jamming attack are given).

A. *Jamming Impact on the Front-End Stage of GPS Receiver*

The first receiver stage effected by the jamming is the front end. The main feature of front end stage is to filter out the incoming signal. Receivers nowadays are multi-bit hence require an auto gain control (AGC) between the analog to digital converter (ADC) and analog portion of front-end [1]. As shown in previous figure 3 jamming effects the AGC and as a result ADC output is modified. From figure 4 it is clearly noticed that ADC output is deviating from Gaussian distribution, however still ADC is able to compress the input signal. The front-end stage of GPS receiver is made up of highly non-linear components, due to which in the presence of a jamming signals these non-linear components are may led to work outside their normal regions,



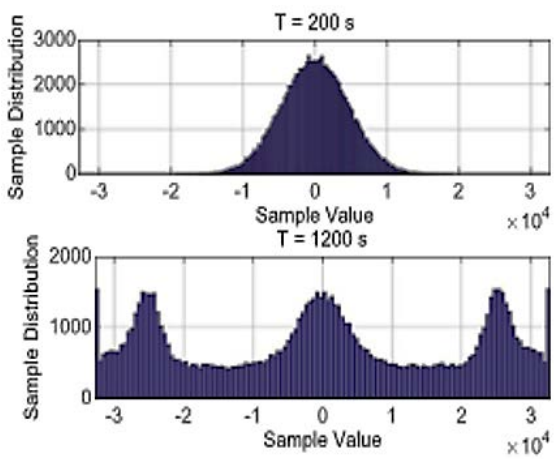
resulting in non-linear effects and results.

Figure 3: Due to impact of jamming on highly sensitive GPS receiver's different metrics are deviated from their nominal operations [1]

Figure 4: Output of ADC not following Gaussian distribution

B. *Impact of Jamming On the Acquisition Stage*

The main duty of acquisition stage is providing a rough estimate of the code delay of signal and to provide a rough estimation of Doppler frequency. Similarly, correlation of the input signal with its local copies of code and carrier is one of the major tasks done by the acquisition block. So an evaluation is done on the bi-dimensional function called cross-ambiguity function (CAF). In the absence of interference or jamming, when GNSS signal is present a dominant single appears in the CAF [1]. Figure 5 presents CAF both in the presence and absence of jamming.



C. *Jamming Impact on Tracking Stage*

After the acquisition stage the signals are next fed into the tracking stage. The duty of the tracking stage is to find the fine parameters of the processed signal. Jamming has a quite big impact on the findings of tracking stage causing misleading measurements and errors. Generally closed-loop architectures are used in tracking stage, where tracking loops are utilized to track down different components of signals [1]. Loop discriminators use the correlator output to determine error in between actual signal parameters and the estimated signal parameters. Under normal conditions in the absence of jamming loop-discriminators output is driven to zero, while in the presence of jamming discriminators output gives some reading which identifies jamming as shown in figure 6.

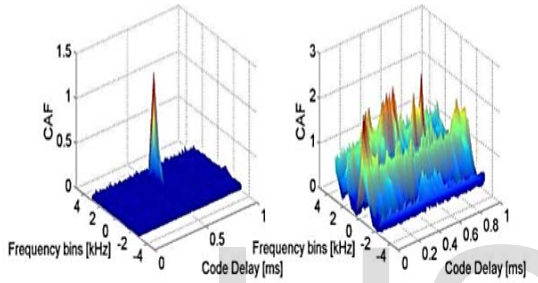


Figure 2: CAF in the absence of jamming (left) and in the presence of jamming (right) [1].

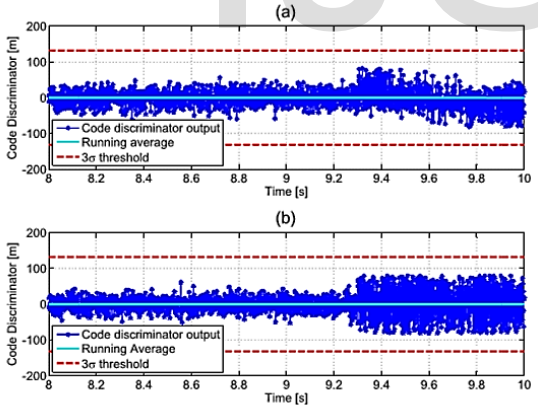
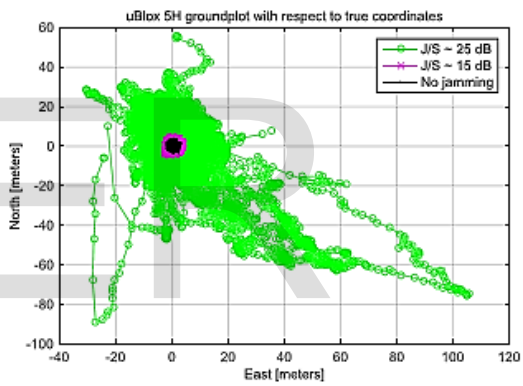


Figure 3: GPS L1 C/A tracking performance: code discriminator output in the presence of a 130-dBW in-band CWI (top) and in the presence of a single-saw-tooth chirp signal at 130 dBW (bottom) [1].

D. *Jamming Impact On the Acquired Position*

According to reference [10] the impact of a jamming attack on a GPS receiver varies according to different available environments. According to experimental results a jamming attack is most deadly in a free-space environment, while its effectiveness reduces as used in complex suburban and urban environments. A J/S value of 47 dB and 27 dB are boundaries of tracking and acquisition processes respectively, comparative to a GPS signal level of -157 dBW [11]. Considering all these facts Table 1 shows the experimental results for boundaries of acquisition and tracking in free-space, suburban and urban environment [10]. In the experiment boundary distances for acquisition and tracking phases are given as a function of Effective Isotropic Radiated Power (EIRP), according to free-space model and COST-231 Hata model.

Knowing the fact that interfered, jammed signal still can pass the acquisition stage and the tracking stage of the GPS receiver. The GPS receiver would be able to present an output position. Which will be degraded due to the fact that it is based on interference based inputs. An error in the position solution is strongly dependent on the algorithm, which is followed to acquire this position solution. Jamming either reduces the accuracy of the acquired position solution or results in complete loss of lock. Reference [1] has presented an experiment shown in figure 7 Employing jamming free condition, minimum



jamming condition, and heavy jamming condition.

Figure 4: Positioning results of u-blox 5H receiver [1].

VII. JAMMING DETECTION

Despite the impact of jamming on various receiver stages. Here in this section various jamming detection methods are proposed. Jamming detection is important since in some cases the GPS receiver under attack is not aware of such an attack.

A. *Hardware Indications*

Knowing the fact that jamming influences various hardware components, in particular auto gain control (AGC) under jamming condition reduces its gain in order to successfully minimize error of quantization and to represent a powerful input signal effectively utilizing limited bits [1]. According to this method let Gagc[n] be the count of auto gain control at some instant of time n. So we can set a simple criterion for jamming detection that is considering N consecutive samples of AGC count. If all the samples of Gagc[n] are well below

a certain defined threshold, the presence of jamming can be declared.

B. Digital Signal Processing

Jamming detection method is classified as a good method, if it can raise early warning against the possible attack. At the output of RF front-end portion various digital signal processing methods apply on the samples of signals and it is an early stage of processing so like this an early warning can be raised against possible attack of jamming. In case of jamming an interfering signal will be impinging the GPS receiver antenna with power level more than the nominal operation ranges. Using spectral analysis, comparing jamming condition with nominal conditions the impinging high power jamming signal can be detected [1].

The main idea here is that while in normal condition the analogue to digital converter (ADC) follows Gaussian distribution as shown in figure 3.4. The probability density function (pdf) of the output samples deviates from Gaussian distribution while jamming signals are present. So jamming can be detected by checking the probability density function of the output samples from the ADC for a Gaussian distribution.

C. Post Correlation Domain Detection

In the presence of jamming the carrier to noise ratio or the C/No measurements of the receiver can be reduced [1]. Therefore, C/No measurements can also be used as an indication for jamming presence. In the presence of a jamming signal the mean C/No reading is effected severely, so by comparing the C/No values of jamming situation to one in the absence of jamming, a jammer can be detected. Considering the C/No values from all satellites jointly results in a better detection as compare to considering the C/No value of an individual satellite.

Detection of a jamming situation through this technique is having a limitation called C/No ambiguity problem. Which is that C/No based detectors can work well in static conditions and they cannot perform well in dynamic situations. The reason is that in case of dynamic situation they cannot discriminate between the reduced strength of signal and the increased level of interference. Because the C/No reading falls both in the case of jamming and reduced signal strength due to motion.

VIII. GPS Jamming Mitigation Options

Being such an essential tool and a daily driver for users of all ages, GPS jamming continues to be a very severe issue for all its users. Reference [12] has given a detailed taxonomy of all the different alternatives and various anti-jamming methods as shown in figure 5. The threat of jamming can be reduced or mitigated by improving the user equipment in a way so it can have jamming rejection and gain producing antennas. Similarly, more robustness against jamming can be achieved by use of correlators at receiver signal processing stages. Overall performance of GPS can be increased by using either a stronger signal in GPS operation or utilizing the features allowing more processing gain. Other ways for a robust performance of GPS includes illuminating the jamming source by attacking the interferer directly and utilizing other navigational systems that do not include GPS signal reception, so the navigational solutions by these systems can be cross checked for accuracy [12].

This paper focuses on methods which includes user equipment improvement and methods that are used to strengthen the transmitted signal. User equipment improvement methods includes the use of currently available signal of GPS, with their current statistics. While strengthening the transmitted signal includes various techniques by which we can improve the signal quality of transmitted signal well enough, so the effect of jamming on these signals is mitigated in a safe range.

A. Adaptive Antennas

All GPS receivers, no matter what kind it is utilizes an antenna for reception of the transmitted signals by the GPS satellites. A simple GPS receiver antenna is one with single-element with a fixed pattern. This kind of antenna deals all the signals (both GPS signals and jamming) in the same manner, due to which interference can neither be discriminated nor detected using this kind of antenna. A better approach is to use multi-element antennas, having the capability to shape adaptively a pattern in response to present signal environment [12].

1. Nulling Antenna System

Multi-element antennas are capable of forming a deep nulls aimed towards the direction of jamming sources, hence direction from which jamming signals are arriving can be nulled-out by this kind of approach [12]. Concept of nulling antenna is shown in figure 8.

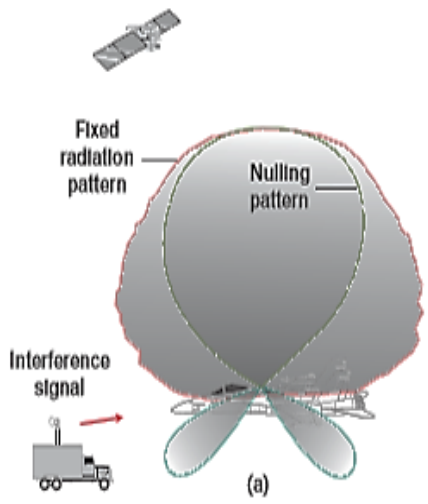


Figure 5: Nulling antenna system for jamming mitigation [12]

2. Beam Former Antenna System

A better approach for the multi-element antenna system is to not only direct a null beam towards the jamming source but also combining coherently the components of the authentic signals of satellite seen at each element of antenna. With the help of which a helpful gain of antenna in the direction of satellite is presented [12]. Hence a beam is formed in the direction in which satellite signals are present. Concept of beam former antenna system is shown in figure 9.

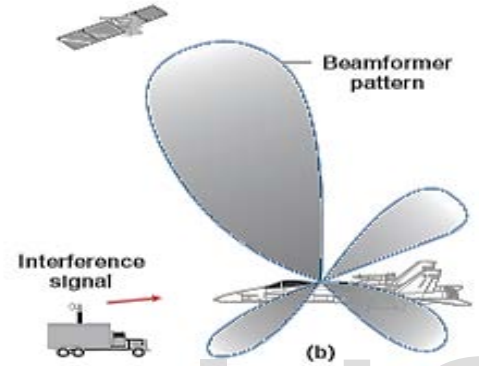


Figure 6: Beam former antenna system for jamming mitigation [12]

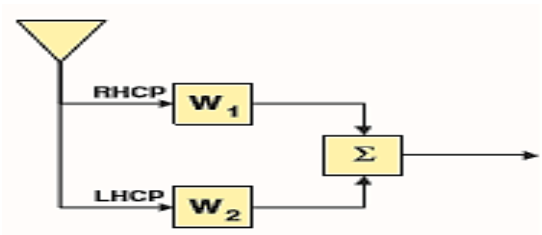
Several factors are taken in account while choosing an antenna sub-system for a GPS receiver. A multi-element antenna system is not only costlier, but also increases the receiver size. For various applications we cannot afford too large size of receiver or increased cabling. Although these methods increase receiver size and complexity, but adaptive antenna methods are capable of reducing the interference successfully.

3. Polarimeters

Another adaptive antenna method is polarimeter, shown in figure 10. In polarimeter output from a single antenna is fed into two output feed elements. So two different polarization outputs can be generated. Both these elements will observe the jammer in a different manner. Producing a signal difference that can be used to cancel out the jamming effect. Similar to jamming cancellers (discussed later in literature), polarimeters are mostly effective against single jammer. Although for some specific geometries their result can also be effective against multiple jammers too [13]. Basic concept of polarimeters is shown in figure 10.

4. Jamming Cancellers

One of the easiest way of mitigating the presence of a jammer is using a jamming canceller. The canceller uses two antennas, one directed towards the jammer (with minimum or absence of GPS signals) and second directed towards both the jamming source and GPS signals. If the gain and phase of output of the jammer-only antenna is adjusted with a weight (W) in a manner so it is equal and opposite to the output of jamming plus signal antenna. When both are added the jamming signal will be canceled out. Basic setup of a GPS cancellers is shown in figure 11. Cancellers are very effective for the case when jamming comes from a local source. For applications where both GPS signals and jamming signals come from the



same side, co-side cancellers will be required [13].

Figure 7: Basic concept of polarimeters [13]

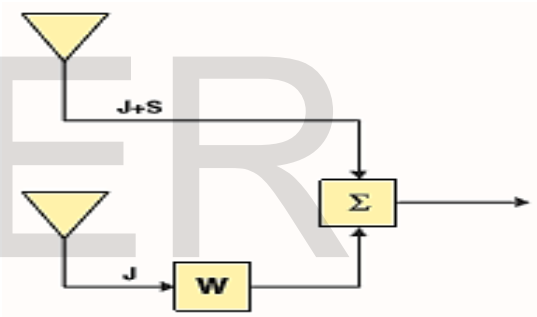


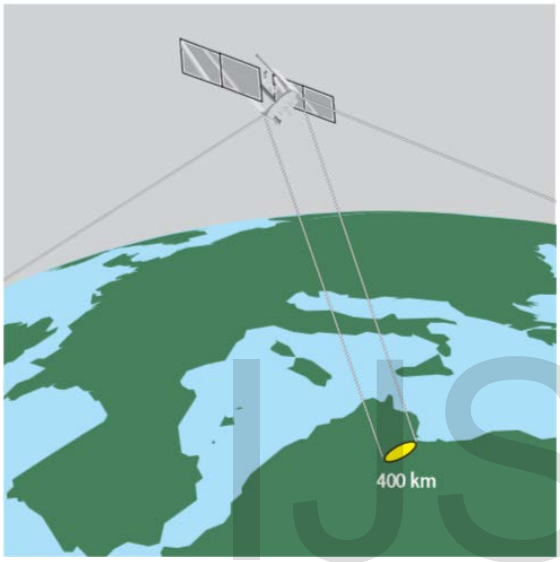
Figure 8: Jamming canceller [13]

B. Satellites with Spot-Beam

Being aware of the fact that the power received by the GPS receivers is quite low since the signals come from quite a distance, consequently even a relatively small interference can deny GPS services in a large geographical area. One possible solution to this issue is to increase the GPS signal strength up to a significant value. This stated approach is having a potential of overcoming the issues of interference, but at the same time the increased power GPS signals will become an interferer itself for other systems. To overcome such a problem a high-gain narrow-beam antenna is considered by a new class of GPS satellites [12]. The spot-beam of this new class of satellites will impact on a relatively small target geographical location (i.e. an area associated in a military operation) as shown in figure 12. For now, it is too early to estimate the cost and complexity of such a narrow-beam satellite system, especially when other effective alternates are possible.

C. *Spectral Filters*

Spectral filters, also called temporal filters, notch filters, adaptive transversal filter is shown in figure 13 with m spectral taps. Considering a CW jammer, after passing the antenna output through a fast Fourier transform (FFT) it is converted to frequency domain. We get white-noise with a single peak at the jammers frequency. Once the jammer's frequency peak is notched out, the output signal returned back to time domain by taking inverse transform. Hence we can get rid of jamming signal [13]. These filters are completely ineffective against the broadband jammers. Broadband jammers do not appear as a single peak,

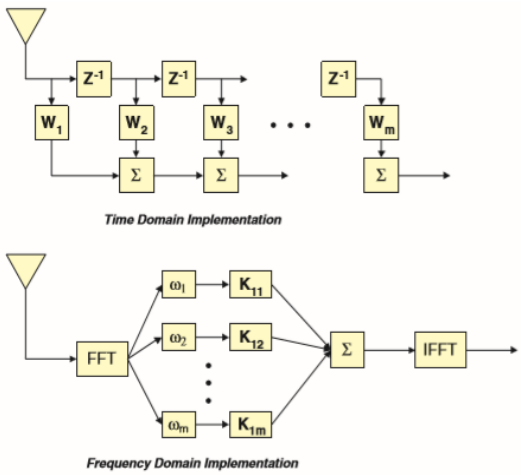


but are spread over entire spectrum of GPS. Since spectral filters work with single dominant peak, so here in the case of broadband jammers the spectral filters are of no use.

Figure12: Basic concept of Spot-beam satellite system, with satellite signals impinging of relatively small area [12]
Figure 13: Block diagram of spectral filters, time domain implementation (upper) and frequency domain implementation (lower) [13]

D. *Space-Time Adaptive Processor (STAP)*

STAP is basically combination of the ability of spatial nulling against all jammer types and the ability of spectral filters to eliminate large numbers of continuous wave (CW) jammers. The resulted technique named STAP, shown in figure 14 is one of the most powerful anti-jamming technique [13].



The reflection of interfering signals from metallic surfaces present near the antenna array motivates to use the tapped delay lines. Each antenna array element is electromagnetically different from others (difference is a function of frequency) because of these metallic surfaces. The array structure become a frequency-dependent spatial filter just because of these tapped delay lines [12].

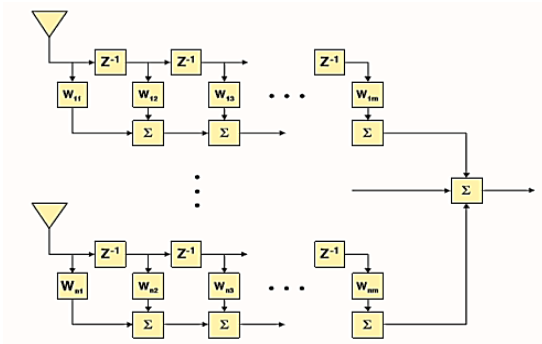


Figure 14: Spatial temporal adaptive processing (STAP) a combination of Spectral filtering and Spatial nulling [13]

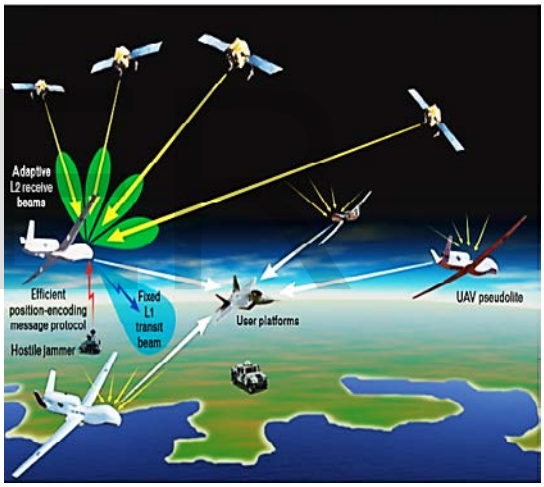


Figure15: Basic military pseudolite system

A. *A Military Pseudolites System*

As discussed above, adaptive antennas can increase the cost as well as the complexity of GPS receivers. Keeping in mind such large number of worldwide users utilizing this costly equipment, and each user must be equipped with this costly circuitry. An alternative is being presented, in a military pseudolites system a stronger signal is presented to all users present in the operation area. Although we know that each military pseudolite transmitting this strong signal is costlier, as compared to an adaptive antenna approach. But the fact is that a set of four such pseudolites can cover a much larger area with a large number of users, and the users need to have just a little modification in their receivers. So comparatively the overall cost will be minimum in comparison to adaptive antenna setup [12]. Figure

15 illustrates the basic concept of a military pseudolite system.

IX Conclusion

When we talk of navigation, GPS provides accurate and easy navigation like never before, GPS provides an accuracy that neither of others systems can provide. No matter where on earth you are using a GPS receiver you navigate easily and accurately. These days most of our daily routine and critical sectors, like military and aviation industry are highly dependent on GPS navigation. In this paper first of all the potential threat of GPS jamming is discussed, the vulnerability of a GPS receiver to a jamming attack is discussed and the effect of jamming on various receiver stages is described. After that various methods of jamming detection are described, it is shown that jamming can be detected at almost every stage of GPS receiver. The case of intermediate power jamming is emphasized the most, since a GPS receiver is still able to present navigation, which is based upon wrong pseudoranges. At the end different countermeasures against GPS jamming are described. A strong anti-jamming technique is one which can raise an early warning against a jamming attack and which can prevent the GPS receiver from a jamming attack, STAP is considered as a strong anti-jamming technique since it contains both the qualities of spatial nulling and adaptive filtering. Although STAP increases the built and computational complexity of a GPS receiver, but it is one of the best measures that can be taken against GPS jamming.

References

[1] 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.

[2] JAMES T.CURRAN, MONICA NAVARRO, MICHELE BAVARO, PAU CLOSAS,''A Look at the Threat of Systematic Jamming of GNSS,'' Inside GNSS Magazine, pp. 46-53, 2018.

[3] Muhammad Aamir Malik M Hassan Sajjad Malik "GLOBAL NAVIGATIONSATELLITE SYSTEM SOFTWARE DEFINED RADIO,'' Department of Electrical Engineering Institute of Space Technology, Islamabad 2014.

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

[5] Scott L (2018), ''Approaches for Resilient Positioning, Navigation and Timing (PNT),''. Association of Old Crows; [accessed 2018 Oct 15]. http://crows.org/item/gps-interference-origins-ffects-and-mitigations.html.

[6] Russon MA (2015), ''Wondering how to hack a military drone? It´s all on Google,'' [accessed 2018 Oct 04]. http://www.ibtimes.co.uk/wonderinghow-hack-military-drone-its-all-google-1500326.

[7] Cole Johnson, Chiawei Lee, Marcea Ascencio, ''Developmental Test NAVFEST: A Large-Scale, Multi-Aircraft, GPS Jamming Test Event,'' United States Air Force US Air Force Test Center, Edwards AFB, CA 2018.

[8] Alexander RÜGAMER and Dirk KOWALEWSKI, ''Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!'' (n.d.). Retrieved from.

[9] Jeff Coffed,'' The Threat of GPS Jamming, the Risk to an Information Utility,'' EXELIS Magazine, pp. 1-11, January 2014.

[10] Faria LA; Silvestre CAM; Correia MAF; Roso NA ''GPS Jamming Signals Propagation in Free-Space, Urban and Suburban Environments,'' J Aerosp Tecnol Manag, 10: e0618. doi: 10.5028/jatm.v10.870, 2018.

[11] Kaplan E, Hegarty C (2006) Understanding GPS: principles and applications. Norwood: Artech House.

[12] Jay R. Sklar,''Interference Mitigation Approaches for the Global Positioning System,'' LINCOLN LABORATORY JOURNAL, pp.167-179, 2003.

[13] Steve Rounds,'' Jamming Protection of GPS Receivers,'' GPS World Magazine, pp. 38-45, February 2004.