XX Congreso Nacional de Ciencias y Tecnología
APANAC 2025
40 años de ciencias y tecnología

ISSN: 2805-1807
XX Congreso Nacional de Ciencia y Tecnología
30 de septiembre al 3 de octubre 2025

Estado de la Detección de Interferencias en el Arreglo de Antenas GNSS del CENAMEP AIP

Solis Betancur, Raúl Fernando
CENAMEP AIP
Ciudad de Panamá, Panamá
ORCID: 0000-0003-1043-4294

Abstract

Nowadays we rely on satellite and terrestrial systems to perform Positioning, Navigation and Timing, but this reference infrastructure is beginning to be attacked using interference on GPS signal. Because of that the CENAMEP AIP Primary Time and Frequency Laboratory has begun working on detecting these interference signals, using atomic clocks, GNSS equipment and developing software to help in detecting and perform mitigation actions. Upon completion of this work, we can detect and identify the types of interference received, leading to the implementation of mitigation measures, so we can conclude that the continuity of UTC(CNMP) can be ensured in the face of these types of events.

Keywords: UTC(CNMP), interferences, timing, cybersecurity, GPS.

Resumen

Actualmente dependemos de sistemas satelitales y terrestres que nos permitan desarrollar Posicionamiento, Navegación y Temporización, pero esta infraestructura de referencia está comenzando a ser atacada empleando interferencia en las señales de GPS. Por ello el Laboratorio Primario de Tiempo y Frecuencia del CENAMEP AIP ha comenzado a trabajar en la detección de estas señales empleando relojes atómicos equipamiento GNSS y desarrollando programas que ayuden a detectar y realizar acciones de mitigación. Al terminar el trabajo, pudimos detectar e identificar los tipos de interferencias recibidas conduciendo a la implementación de medidas de mitigación, con lo que pudimos concluir que se puede asegurar la continuidad del UTC(CNMP) frente a este tipo de eventos.

Palabras claves: UTC(CNMP), interferencias, sincronización, ciberseguridad, GPS.

https://doi.org/10.33412/apanac.2025.61

1. INTRODUCCIÓN

El auge del consumo de tecnologías basadas en Posicionamiento, Navegación y Temporización (PTN) empleando GNSS (Global Navigation Satellite System) como el GPS ha traído como consecuencia, la exploración de formas de interferir estos sistemas, causando problemas en acceso, afectando la sincronización de sistemas o la seguridad en los aeropuertos [1]. En Panamá, desde el año 2022 ha existido un incremento sustancialmente peligroso de estas interferencias [2], sin que se haya logrado establecer políticas nacionales de control o mitigación de estos problemas, algo que pudiese estar causando afectaciones en el desarrollo de servicios avanzados [3]. En la Figura 1, se muestra un ejemplo de estos eventos interferencias y su efecto. En la Figura 1, a la izquierda se muestra el evento a partir de datos abiertos de aviones, y procesada en la página https://gpsjam.org/. A la derecha se muestra un salto en las mediciones de tiempo en las señales L1 y L2 de GPS con respecto al UTC(CNMP), para las mismas fechas.

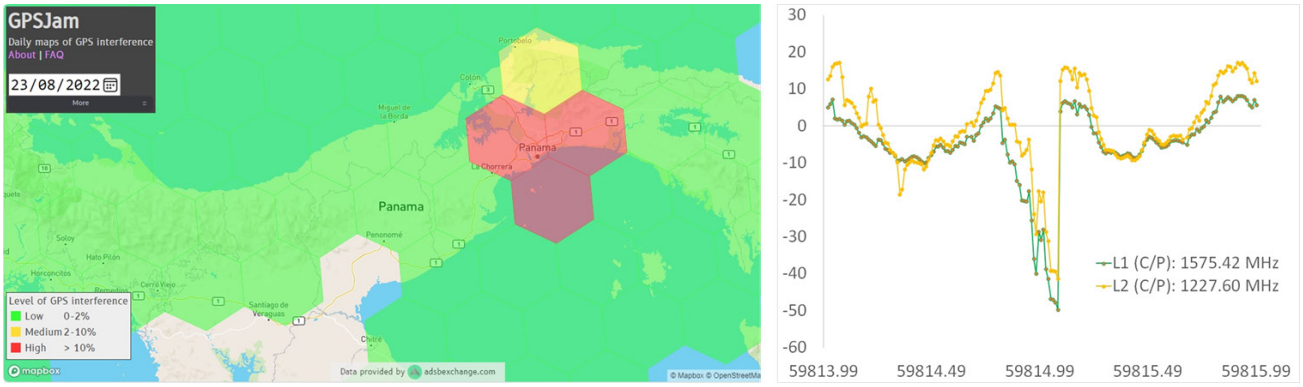

Figura 1. Vista de los eventos registrados para el 22 de agosto de 2022 donde se registra una exposición a interferencia.

Y estas interferencias motivaron una serie de investigaciones en términos de análisis y la mitigación del impacto que estas interferencias causarían a los procesos de comparación entre laboratorios y la supervisión de señales GPS realizadas en el Laboratorio Primario de Tiempo y Frecuencia (LPTF), el cual es el encargado de la realización del UTC(CNMP), empleando la técnica de vista común, basada en mediciones GPS como medio de comparación [4], con ello se podrá mitigar su impacto, asegurando una realización y diseminación del UTC(CNMP) confiable para Panamá.

2. MÉTODO

A. Qué tipo de interferencias se piensan buscar

Como se está trabajando en detectar señales que pudieran causar interferencia (de manera

https://doi.org/10.33412/apanac.2025.61

accidental o de manera intencionada) se decidió trabajar, desde el punto de intencionalidad, en dos posiciones: 1) Señales de origen no intencional: Señales que podrían afectarnos, pero su naturaleza no intencional, comparten otras frecuencias y no tienden a repetirse en el tiempo. 2) Señales de origen intencional: Señales que podrían afectarnos, pero por su naturaleza intencional, están enfocada en señales GNSS y tienden a repetirse en el tiempo. Ahora, desde el punto de vista de interferencias, trabajamos directamente en dos temas: 1) Detección de posibles señales de Jamming: Detección de señales que tienen afectación directa sobre la relación portadora y ruido (C/No), por satélite o por grupo completo, realizando un incremento de potencia en banda ancha (MHz) o en banda estrecha (kHz), y 2) Detección de posibles señales de Spoofing: Detección de señales que tienen afectación directa en la determinación de la ubicación empleando un satélite o por grupo completo.

B. Equipamiento empleado para detectar interferencias

Para realizar el proceso de detección, el recurso empleado para realizar las mediciones, análisis y detección es el siguiente:

- Relojes Atómicos (Microchip 5071A): Con ellas se evita que el receptor se discipline al tiempo de GPS, permitiendo analizar las perturbaciones provenientes de las señales GPS.
- Receptores Satelitales (PikTime TTS-5, Septentrio PolaRx5TR y SIMRV): son receptores satelitales optimizados para trabajar realizando mediciones entre 30 segundos a 2 minutos midiendo señales de las constelaciones GPS (Estados Unidos), GLONASS (Rusia), GALILEO (Unión Europea) y BeiDou (China), y disciplinados a los Relojes Atómicos.
- Programas especializados locales (TTSMon y Supervisor Interferencias): programas desarrollados localmente en C# los cuales se mejoraron para incluir la detección de interferencias empleando datos provenientes de los receptores satelitales.
- Licencia BlueSky (Microchip): para el receptor Microchip S650 que permite detectar situaciones de Jamming o Spoofing solo en señales GPS.

C. Metodología empleada para detectar las interferencias

Se empleó una metodología de tres fases para aprender, desarrollar e implementar los procesos necesarios para detectar y responder a las posibles interferencias: Fase de Aprendizaje: Fase donde se implementa y emplea la licencia BlueSky para captar datos, observar que es “normal” en este tipo de mediciones, y establecer valores de referencia. Fase de Adecuación: Fase donde se adecua el programa TTSMon para obtener datos de mediciones GNSS a través del archivo CGGTTS [5] y el SIMRV. Además, se desarrolla el programa “Supervisor Interferencias” que emplea cURL para extraer datos del BlueSky para analizar, formatearlos y que otros programas los empleen también. Y Fase de validación e implementación: En esta fase, mediante la Gestión del Conocimiento adquirido, se procede

https://doi.org/10.33412/apanac.2025.61

a implementar las medidas y adecuar los procedimientos para que, al detectar interferencia intencional y no intencional, se pueda actuar pertinentemente al escenario establecido

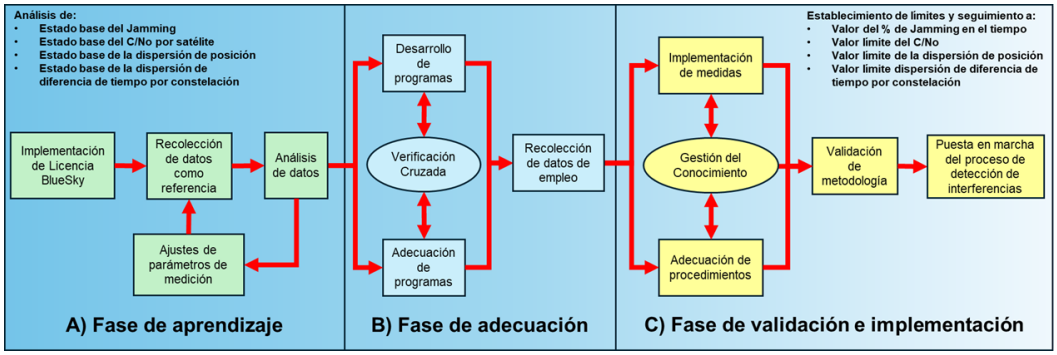

Figura 2. El proceso de desarrollo del sistema de detección de interferencias se realizó en 3 fases que abarcaron casi 14 meses. Todo esto con el objetivo de detectar y clasificar las interferencias.

3. RESULTADOS

A. Mejoras en las técnicas de detección

Se logro implementar mejoras en la detección de interferencias. El programa TTSMon se actualizó para darle, inicialmente, seguimiento a cada satélite y distintas frecuencias de GPS y analizar individualmente su comportamiento. Se desarrollo y validó el programa Supervisor Interferencias para monitorear los datos del Microchip S650 con BlueSky, y obteniendo los datos de Jamming, Dispersión de la Posición y el C/No con periodos más cortos y de manera automatizada. Se logró mejorar los protocolos internos, ya que una vez que los programas detectan automáticamente anomalías, se puede ir inmediatamente al análisis de espectro del PolaRx5TR a verificar que está pasando.

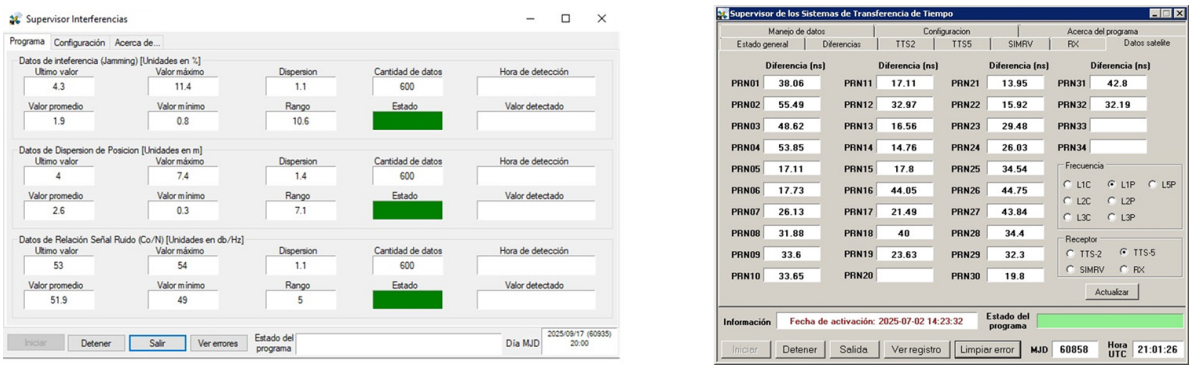

Figura 2. Programas desarrollados y actualizados en el LPTF permiten mejorar los análisis y detecciones de posibles interferencias o posibles fallos individuales de satélites.

https://doi.org/10.33412/apanac.2025.61

Y se adecuaron los receptores para brindar información concerniente en términos de trabajo y estabilidades. También se activó la herramienta OSNMA para autentificar satélites GALILEO y evitar Spoofing (mostrado en la Figura 3, imagen de la izquierda).

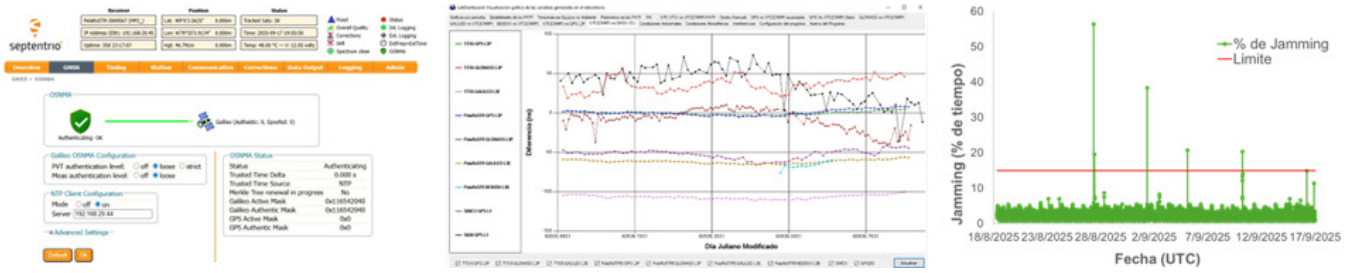

Figura 3. Vista del trabajo desarrollado para implementar técnicas de detección y mitigación.

En la Figura 3, la imagen del centro muestra el seguimiento a las diferencias de tiempo en base a los receptores y las constelaciones GNSS analizadas en el día. Mientras que la imagen de la derecha muestra con espacio de 2 minutos datos medidos de intensidad en Jamming (tomando en cuenta el espectro inicial considerado como limpio y normal).

B. Tipos de interferencias detectadas en el arreglo de antenas del CENAMEP AIP

Las medidas implementadas no solo permitieron detectar interferencia, sino que permitieron clasificarlas en tres tipos principales de interferencias incidentes sobre el arreglo de antenas GNSS: 1) Interferencias de barrido: Son señales de interferencia que cambian el ancho de banda, pero se mueven a lo largo del espectro de señales de GPS. En la Figura 4, la imagen de la izquierda muestra un ejemplo de ello. 2) Interferencias de banda estrecha: Son señales de interferencia con anchos de banda muy estrechos (posiblemente no superan los kHz) y tienen duraciones de tiempo desde algunos segundos hasta algunos minutos. En la Figura 4, la imagen del centro muestra un ejemplo de ello. 3) Interferencias de banda ancha: Son señales de interferencia que tienen un ancho de banda de cerca del MHz y tienen duraciones de segundos. En la Figura 4, la imagen de la derecha muestra un ejemplo de ello.
Con respecto a las posibles interferencias tipo Spoofing, no se pudo detectar directamente y de manera repetitiva una interferencia de este tipo, pero se puede detectar su influencia en los cambios en la dispersión de la posición. En la Figura 4 se puede apreciar que el receptor PolaRx5TR posee un analizador de espectro que muestra en tiempo real sus medidas, en la banda analizada. Con ello podemos ir identificando frecuencias, intensidades y mecanismos de interferencias tipo Jamming.

https://doi.org/10.33412/apanac.2025.61

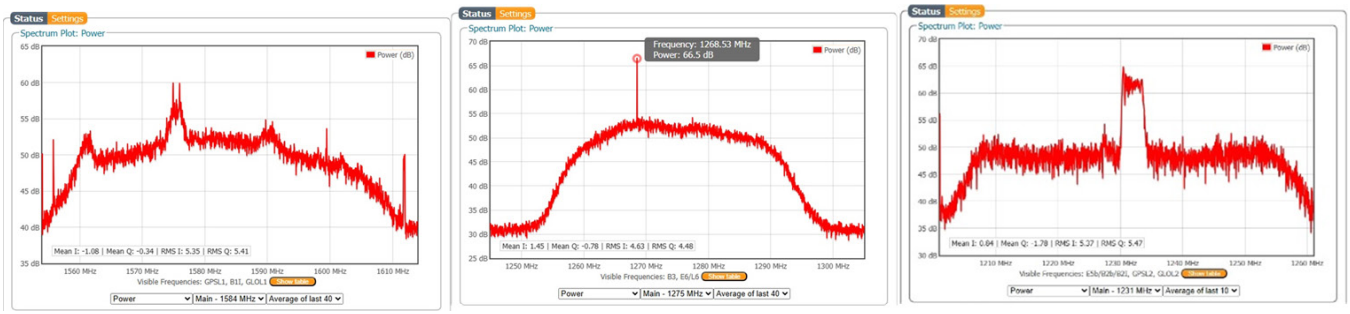

Figura 4. Vista del analizador de espectro del receptor PolaRx5TR.

C. Estrategias adoptadas frente a posibles interferencias

Las estrategias adoptadas para mitigar interferencias: 1) Descartar constelaciones GNSS o satélites puntualmente, 2) Mejorar los filtros Notch (si se localiza incrementos de señales por encima de 55 dB, se emplea esta información para aplicar un sistema de mitigación empleando amplificadores y así mantener la integridad de las mediciones) para potencias, 3) Incrementar el Mask Angle (ángulo empleado como límite de horizonte) para descartar la posición de la fuente, 4) Desconectar la antena físicamente en caso de que las potencias de interferencia fuesen extremas y 5) Llevar registro mediante los archivos RINEX y CGGTTS, con lo cual se podrán tomar más acciones y controles.

4. CONCLUSIONES

Con el desarrollo de este trabajo, el LPTF adquiere valiosas herramientas para mantener en control sus procesos y optimizarlos, ya que al saber si hay interferencia o no, se puede descartar si los receptores están teniendo algún tipo de problemas como desperfectos o situaciones anómalas en equipos auxiliares (conectores, cables, etc.), algo que antes se les podría atribuir a los receptores porque se desconocía del impacto directo de las interferencias en las mediciones. Ahora, al conocer el tipo impacto, podemos actuar de manera cónsona para mantener la seguridad del UTC(CNMP) como del equipamiento GNSS del CENAMEP. Todo esto para preservar la integridad y robustecer las capacidades del LPTF.

Referencias

[1] C. Clausnitzer. “GPS/GNSS Jamming/Spoofing”. Federal Aviation Administration. Accedido el 14 de octubre de 2025. [En línea]. Disponible: https://www.faa.gov/air_traffic/flight_info/aeronav/acf/media/Presentations/24-01-GPS-Interference.pdf

[2] J. Wiseman. “GPSJAM GPS/GNSS Interference Map”. GPSJAM GPS/GNSS Interference Map. Accedido el 14 de octubre de 2025. [En línea]. Disponible: https://gpsjam.org/

[3] R. F. Solís Betancur, Propuestas de Nuevas Capacidades de Medición y Calibración en Tiempo y Frecuencia, APANAC, pp. 141-147, sep. 2023.

https://doi.org/10.33412/apanac.2025.61

[4] R. F. Solís Betancur, Calibración de receptores GNSS multicanal, APANAC, pp. 313-318, sep. 2023.
[5] P. Defraigne y G. Petit, “CGGTTS-Version 2E : an extended standard for GNSS Time Transfer”, Metrologia, vol. 52, n.º 6, p. G1, octubre de 2015. Accedido el 14 de octubre de 2025. [En línea]. Disponible: https://doi.org/10.1088/0026-1394/52/6/g1

Autorización y Licencia CC

https://doi.org/10.33412/apanac.2025.61