Journal of Engineering Technology and Applied Physics

GNSS Interference Environment in Malaysia: A Case Study

Ooi Wei Han*, Shahrizal Ide Moslin and Wan Aminullah
Department of Space Technology and Engineering, Malaysian Space Agency (MYSA), Kuala Lumpur, Malaysia.
**Corresponding author*: ooiweihan@mysa.gov.my
https://doi.org/10.33093/jetap.2021.3.1.3
Manuscript Received: 19 Dec 2020, Accepted: 4 March 2021, Published: 15 June 2021

***Abstract* - Global Navigation Satellite Systems or GNSS is a space technology that has become an essential element nowadays for positioning, navigation & timing (PNT) with wide range of applications in many civilian sectors as well as across military. The reliability, accuracy and availability of GNSS are highly important especially for critical and precise positioning applications. However, the signals from space are weak and it can be easily blocked, disrupted or compromised by several other threats including intentional and unintentional interferences or jamming. GPS jammer is widely available off the shelf with an affordable price and capable of interfering the GPS signal, and many authorities worldwide have raised concerns and a lot of efforts and research have been put in place to reduce and mitigate the threats. In Malaysia, understanding and countering threats to GNSS/GPS based applications will be a new and unfamiliar discipline for public and organizations. This study intended to provide an overview of the GNSS interferences environment in a local study area, in terms of interference type and the number of activity pattern that were detected. A system called Detector V1 has been used in this study. The result showed that significant interference cases happened in the study area and some of the high power interferences may impact GNSS tracking and precision of the positioning output. The role objective of having this done is to create a public awareness regarding the threat of GNSS interferences to the local users. The content also includes the proposed initiative to overcome the issue.**

Keywords—GPS, GNSS, signal, interference, detector, awareness

I. INTRODUCTION

Nowadays, the Global Navigation Satellite System (GNSS) has become essential source of positioning, navigation and timing information for both civilian and military in many other sectors. It's capable of delivering position accuracy from few meter to centimeters levels, depending on the type of antennas, signal frequencies used and procedures followed. Apart from that, the increasing dependence on GNSS is globally recognized, and indeed, some countries are developing and upgrading their own global navigation systems, such as Global Positing System (GPS) operated by United States of America; the Russian Globalnaya Navigazionnaya Sputnikovaya Sistema (GLONASS), the China's BeiDou Navigation Satellite System and EU's Galileo Satellite Navigation System.

The reliability, accuracy and availability of GNSS are extremely important especially for critical and precise positioning applications. However, GNSS signals from space are weak and can be easily blocked, disrupted and compromised by several threats including man-made interference and jamming, faking of GNSS signals and the manipulation of position and timing information. Most of the user do not realized that devices are vulnerable to disruption and interference.

Several cases of the real risk of GNSS jamming incidents have been recorded worldwide in the past few years. For example, in 2009, engineers noticed that GNSS receivers for a new navigation aid at the Newark airport, USA would lose signal during certain times of the day. The authority investigated the problem and after two months discovered that a local truck driver had installed jammer in the vehicle that emanating radio signals within the restricted MHz band. When the truck passed the airport area in daily routine, the airport's systems would temporarily halted. The driver claimed that he installed and operated the jammer to prevent his employer from tracking his movements. This incident must be avoided in order to ensure the operational of airport are not interrupted and ensure the safety of the passengers [1]. The second example was occurred in the UK in 2010. Two men were jailed for a total of 16 years after they admitted being part of a criminal gang that robbed 40 trucks and their loads with a total value of £6 million. They had used GPS jammers to prevent the vehicles from being tracked after thefts

Published by MMU PRESS. URL: https://journals.mmupress.com/index.php/jetap/index

[2]. Apart from that, GNSS jamming incidents also occurred towards military system. In North Korea, GNSS jamming was performed on three confirmed occasions along the border during military exercises in March 2011, August and December 2010. A significant number of aircraft and ships have been affected [3]. Meanwhile in Jun 2017, the US Maritime Administration filed a report after the master of a ship off the coast of Russia discovered that the ship's GPS had set the wrong spot and location due to spoofing system. The captain discovered that at least 30 other ships nearby were affected by the same problem [4].

GNSS receiver manufacturers have placed tremendous efforts into study to solve the issue of signal interference and jamming. They produce receivers with signal degradation mitigation solution or equip with addition sensors. Besides significant improvements, local interference from nearby receiver persists, which means the problems need to be resolved in the future [6].

In Malaysia, understanding and countering threats to GNSS based applications might be a new and unfamiliar discipline for many organizations. Since users increasingly relying on GNSS, understanding and mitigation of the threats become a critical risk management activity for manufacturers, applications providers as well as the end users. There is a need for users to understand the potential threats or risks affecting GNSS based applications, and ensuring that appropriate steps are taken to mitigate.

The aim of the study is to create public awareness on the threat of GNSS interferences to the local users. It was intended to provide an overview of the GNSS interferences environment via Detector V1 system in the study area, to detect and analysis the interference types and the number of activity pattern that were detected. Several suggestions for initiatives were discussed at the end of the study.

II. Typical Jammer Characterization

In most country, using a jammer is illegal. Jammers are gaining popularity because it can prevent road tolling or insurance billing in some country, as well as tracking and location-based monitoring. GNSS jammer is capable to transmit a strong signal that overrides or obscures the GNSS signal being jammed. This kind of jammer is widely available off the shelf with an affordable price and the device can prevent a tracking unit from determining and reporting a location and speed in less than minute.

Usually, the jammer (Fig. 1) is poorly designed and without manufacturer data, battery operated, comes with external antenna with omnidirectional radiation pattern and emitted single chirp signal, which the frequency increases or decreases with time. The cheaper jammer is single antenna device that able to interfere only L1 GNSS signal frequency that is used by most users. The device may raise noise power up to 50dB in a frequency band of 1570 MHz. Apart from that, more expensive devices have multiple antennas capable of attacking two or three GNSS signal frequencies (e.g. L1 and L2) within a radius of few hundred meters. This kind of devices usually come with additional feature which able to jam the cell phone and Wi-Fi reception.

The current development of the jammer is more advanced and it is possible to transmit even high powers. Not only does the jammer lead to a major threat to the military, such as veering away guided missiles and etc., industrial and civilian transport, but criminals such as car hijacking cases have also been pushed out because of its ability to disable the GNSS signals at all times.

Fig. 1. Several type of commercial jammer in the market.

III. SETUP AND DATA COLLECTION

In this case study, the Detector V1 system (Fig. 2) was used for monitoring and characterization of GNSS interference at 24/7. The system was originally developed by UK NSL for research purposes. The system consists of components of the probe device and GNSS L1 receiver at site, and a computer process engine. Once interference is detected, this triggers an event and the power readings and GNSS tracking information are logged for the duration of the event, as well as the start and end time of the raw data.

Meanwhile, the system was setup in building close to Sepang in Selangor. The Detector V1 is about hundred meters from major roads and few hundred meters away from multi-storey car park. Data collection for this study began in the period from 2019 to May 2020.

Fig. 2. Detector V1 and GNSS L1 receiver used in the study.

IV. RESULT AND ANALYSIS

In this study, the focus was to investigate the number of activity pattern of jamming cases that were detected over the observation period. The analysis was included the interference signal types of each cases and time duration, calculated power level, as well as determined the priority level.

Across the monitoring period in 2019 (January to October), almost 7000 cases of interference were detected in total including jamming. There was a lot of variation on interference occurred on all days, ranging from lowest 5 cases

to the highest 480 cases per day. Low activity was shown most of the day (less than 30 cases), but several hundreds of cases were found in few days. In fact, cases can take place any day and time of day except less on Saturday, Sunday and overnight.

The following Fig. 3 showed the monitoring results in signal classification types. The majority of cases were caused by wideband (WB) and narrowband (NB) signals, with 4339 cases and 1411 cases. It followed by chirp signals 467 cases which are typical of jammers, 108 cases as Code-division multiple access (CDMA) and 692 cases as other sources. Some of these cases may just be low power noise and not significant.

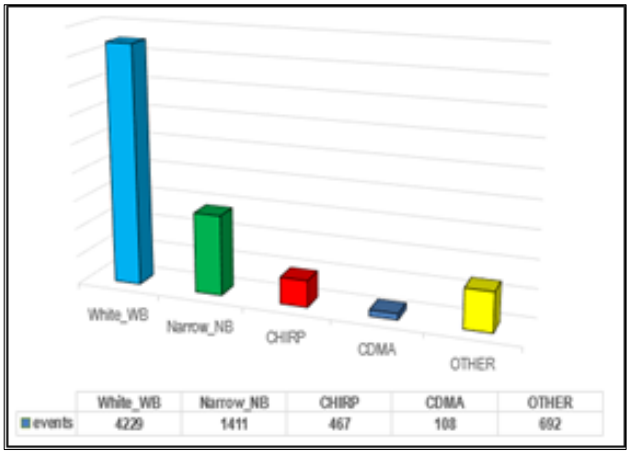

Fig. 3. Type of interference cases recorded in 2019.

Meanwhile, the duration of interference cases was showed in the Fig. 4, and the duration of about 6153 cases were found to be very short, which less than 20 seconds. 637 cases in 20 to 40 seconds, 55 cases in 40 to 60 seconds and 62 cases in more than a minute. The short of duration cases can came from typical of jammers found in moving vehicles, exceptions where the source seems to be stationary and last more than 60 seconds.

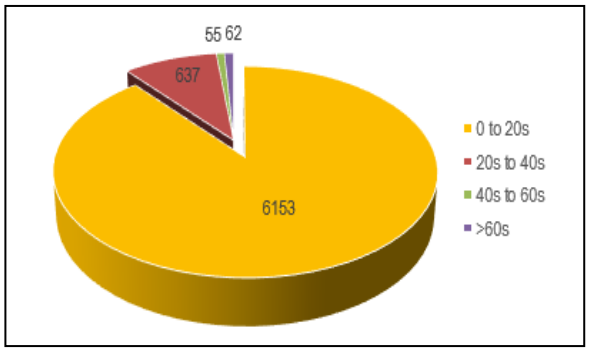

Fig. 4. Duration of interference cases recorded.

Furthermore, when taking into account only the high priority interference cases with high power or suspicious signal patterns as showed in Fig. 5, there are a total 553 cases including chirp signals (467 cases), as well as other high-power types from wideband and narrowband signals. Most of the cases interfered by medium and high power up to 6dB and above may have an impact on the GNSS L1 tracking and positioning accuracy calculations.

In the meantime, in 2020 (until May), nearly 3800 cases were detected and from the record, there was a lot of variation of interference on all days, ranging from lowest 5 cases to the highest 480 cases per day. Indeed, it was in an average of below 20 cases most days. On 16 April 2020, there was much more activity than hundreds of cases have been detected. These instances are of short duration and tend to be the same signal source (narrowband). Fig.6 showed the daily number of cases during the observation period. Less cases were detected during April and May most of the days when the Movement Control Order was enforced in response to the pandemic COVID-19 in the country.

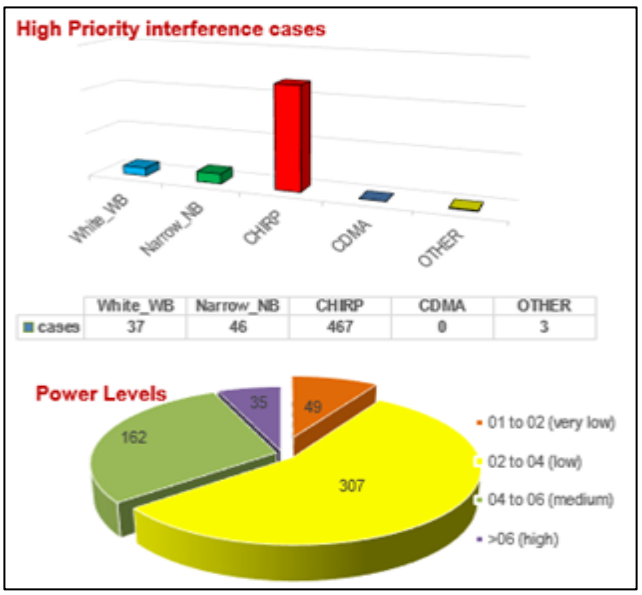

Fig. 5. High priority interference cases with high power signal patterns.

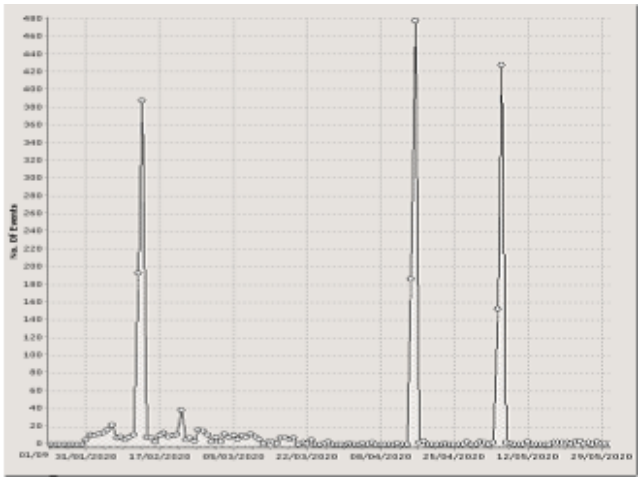

Fig. 6. Daily number of cases in the period from Jan-May 2020.

When categorized in medium and high priority cases, there are 221 cases out of a total of about 3800 cases involving chirp or jammers signals and other types with high power sources (Fig.7). Apart from that, most cases occurred within a short time period of less than 40 seconds, with the exception of a few cases (about 10) that were more than 60 seconds.

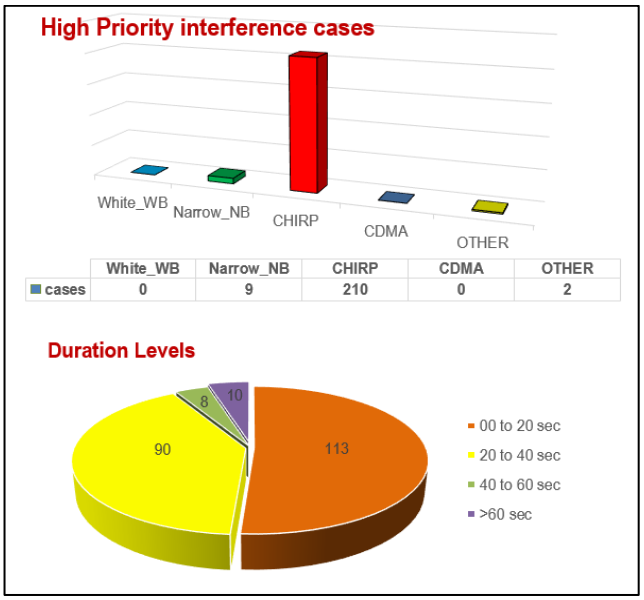

Fig. 7. Duration of interference cases recorded.

V. CONCLUSION AND RECOMMENDATIONS

In conclusion, the GNSS interference incidents through the Detector V1 system from 2019 to May 2020 were generally presented in this case study. It could be the preliminary step towards mitigating the effects of jamming by detecting the presence of a jammer or other signal types. Through this study, it was noticed that the main source of interferences comes from chirp type of signals and the small frequency range of narrow and wide band signals. Several interference incidents detected with the high power are high enough to have significantly impacts on the positioning calculations. The variation in their power levels over time show that they are coming from mobile sources typical of jammers found in moving vehicles.

The main goal of the work is to create public awareness on the threat of GNSS signal interferences to the local users. This GNSS interference phenomenon is no longer regarded as a local or regional issue, but as an international concern. Several systems have been developed all over the world to detect jamming and interference incidents such as GAARDIAN in Britain, GPS Jamming Detection and Location system (JLOC) in the US and etc. Thus, the understanding and R&D of GNSS signal interference and integrity should be further established and deepened. National inter-agency cooperation and supervision could be established to mitigate the issue of interference as well as to customize the relevant policy particularly during disruption of continuous positioning due to GNSS interference. In addition, strengthening the relevant acts to control the use of illegal jammer and protecting the GNSS device in the country while at the same time being a matter of serious concern to law enforcement, since the commercial jammer can be easily obtained at an affordable price.

ACKNOWLEDGEMENT

The authors would like to thank NSL for providing the detector system to make this study and data collection possible.

REFERENCES

[1] J. Warburton and C. Tedeschi, "GPS Privacy Jammers and RFI at Newark: Navigation Team AJP-652 Results," Federal Aviation Administration, 2011.

[2] "GPS Jamming: No Jam Tomorrow," in *The Economist*, 12 Mar 2011.

[3] GPS World Staff, "Massive GPS Jamming Attack by North Korea," in *GPS World*, 8 May 2012.

[4] H. David, "Ships Fooled in GPS Spoofing Attack Suggest Russian Cyber Weapon," in *NewScientist*, 10 August 2017.

[5] D. Mark, "Interference Monitoring Summary for STRIKE3," unpublished.

[6] B. Matej, D. Franc and P. Polona, "Evaluating The Vulnerability of Several Geodetic GNSS Receiver Under Chirp Signal L1/E1 Jamming," Sensor, vol. 20, no. 3, pp. 814, 2020.

[7] A. Erik, "GNSS Interference Detection," in *report FOI-R-3839-SE*, February 2014.

[8] G. Buesnel, "The Challenges for Resilient PNT in 2020," *Coordinates,* vol. XVI, no. 1, 2020.

[9] K. Helmi, "Effects of GNSS Jammers and Potential Mitigation Approaches," in *2012 United Nations/Latvia Workshop on the Applications of GNSS*, 2012.

[10] K. Kida and H. Shinichi, "China's Version of GPS Now Has More Satellites Than US Original," in *Nikkei Asia*, 19 August 2019. Available: https://asia.nikkei.com/Business/China-tech/China-s-version-of-GPS-now-has-more-satellites-than-US-original.