TRANSNAV
http://www.transnav.eu

the International Journal
on Marine Navigation
and Safety of Sea Transportation

Volume 13
Number 4
December 2019

DOI: 10.12716/1001.13.04.18

# Let Us Prepare the Officer of the Watch on Jamming and Spoofing

A. Felski
*Polish Naval Academy, Gdynia, Poland*

ABSTRACT: The general accessibility and high accuracy of GPS caused that for a dozen or so years it is applied commonly, not only in marine navigation. We can ascertain that in this regard there exists the monopoly. However, now it is apparently that this system can be easily disturbed, what testify numerous reports. The problem has been treated as troubles in land navigation, however nowadays became every-day reality on coastal waters as well, especially on the Mediterranean and Black Seas and Persian Gulf.

Officers who survived this tell that the first impulse in such situation is to verify GPS receiver, regardless of the situation around the ship. The concentration of the officer's attention on the GPS receiver, especially on coastal waters creates the threat for the ship, however in this situation appear other threats which many officers does not associate with GPS. Usually on the present ship GPS receiver is not only the source of positioning information. It is a source of information for many other devices, so inappropriate work of it generates problems with many other processes on the ship. Today question is who on the bridge can notice GPS problems and how? There are receivers which do not inform about the problem, or present not realistic data. Sometimes only ECDIS picture shows some abnormality, for example still the same position while ship is under the way.

On the paper the analysis of possibly aspects of the problem is discussed. Presented analysis goes to the conclusion that should be prepared some procedure how to proceed in case of the lack of GPS signals, as well as the watch officer should be prepared to act in such situation. This is a task for marine academies.

## 1 INTRODUCTION

Reliable positioning is recognized as one of the fundamental requirements for the safety at sea. For almost 50 years after the WW2 hyperbolic systems (Decca, Loran etc.) dominated in sea navigation. However since first Navy Satellite Navigation System (Transit) this state gradually changed and now, for many years Global Navigation Satellite Systems are recognized as the primary source in positioning. In fact we observe real monopoly of GPS in this field.

On the other hand we know that these systems have a weak resistance on many disturbances [1]. So reliance on a single position source when its vulnerability is known, bring us to not acceptable risk. It is especially essential when many devices on the ship require position input to its work. This is not only mariners' problem, as today many crucial aspects of the society life is domineered by GPS. This statement refers not only to the navigation, nevertheless in the general feeling the system is treated as the element of the navigational infrastructure. A lot of critical infrastructure applications involving safety, security, and the economic flow of goods is dependent from Positioning, Navigation and Timing systems as well.

For many applications, like cellular phones, its use is essential and the most of users is familiar with it.

The absolutely new perspective in this aspect draws to us the appearance of unmanned ships. From the one side we cannot to allow, that unmanned ship will sail without positioning data, when experienced man can manage this for some time. The second aspect of this problem is possibility to capture the unmanned ship by pirates, what was demonstrated as opportunity by Iranian forces against US Predator drone in 2013 by means of manipulations with GPS signals [10].

## 2 KINDS OF DISTURBANCES AND THE SCALE OF THE PROBLEM

GPS was built as the interference proof thanks to the use of the technique of wide spectrum. But already in the first half of 90-these first report about the possibility of the disturbance of GPS signal has been published [Falen, 1994]. Then possibilities of interferences was foreseen. As far as in 2001 the report of the American Department of the Trade widely analyses potential possibilities of the interference of the signal GPS with broadband wireless communication systems, than in 2011 Royal Academy of Engineering report [Global Navigation, 2011], [Space Weather, 2013] as the greatest threat attends the problem of the intended perturbation of GPS signal with portable devices. Today is clear, that Space-based PNT systems have many limitations, among which interference, jamming, meaconing and spoofing are mentioned as real and most essential.

Figure 1. The most common “personal” jammers. Source: [gpsworld.com].

The problem of anti-GPS activity isn’t a new threat. The roots of this and similar technologies can be find in the WW2 era and later, in Cold War. The first attempts to produce some “radio-noise” for counteract against enemy radio transmission we can observe during the WWII. Later, attempt to transmit fake radar echoes to build false picture on the enemy radar screen – in seventies.

Generally speaking there are three options to disturb GPS signal in intentional mode: jamming, meaconing and spoofing [Cameron, 2014].

- Jamming seems to be the easiest method, as its sense is to produce enough power of the radio noise in receiver’s spectrum. This is truth, that GPS receiver works even below of the noise level, however the Signal to Noise ratio is limited. If the ratio of the noise is over the limit in spite of all the receiver does not receive the useful signal.
- Meaconing means a manipulation in the time of the delivery of satellite signals to the receiver, in fact - introducing some delay to their propagation. Finally coordinates of the position will be incorrectly calculated, as this process based on the time of signal propagation.
- Spoofing is the method of transmitting to the receiver signals which seems to be GPS signals, however there are produced out of the system – not by satellites, but by enemy generator. Reportedly for this the perfect means are GPS simulators. The threat of spoofing for GPS was discussed many times by specialist, during open discussed, as well as probably in the closed bodies. For long time many specialist argued that in reality spoofing is “too hard” to conduct it in a real conditions. Today many evidences show, that it works.

As jamming need simple devices, nowadays this is observed in many areas and for different reason. Complaints of Scottish fishermen almost ten years ago prove that NATO produces such disturbances for its own exercises. On the other hand, according to public pronouncements of Prime Ministers of Finland and Norway in February this year, after last NATO exercises, Russia acts so in case of exercises of pact forces. Many experienced ship officers report such evidences in the west part of Mediterranean Sea in 2017 and 2018.

For long time Spoofing has been treated as not workable, up to 2013, when Psiaki with his team demonstrate it in famous experiment on Mediterranean Sea [Psiaki, 2016]. In this experiment the team from University of Texas (Radionavigation Laboratory) were carried out an experiment where GPS-guided drone was fooled into “thinking” its altitude was increasing and this caused it to lower the flight and finally – landing. In 2014 the same team demonstrated how yacht could be steered off-course by means of spoofing attack. In this experiment yacht’s GPS receiver was spoofed into “believing” that it was veering off its course, set northwards to Venice, and heading south to Libya at a very high speed [Cameron, 2014].

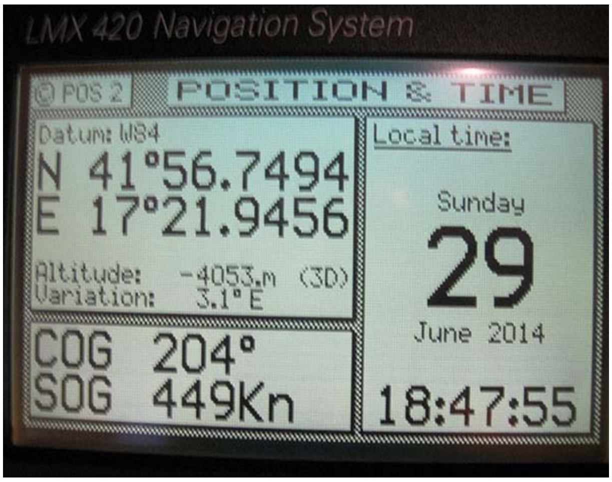

Figure 2. Photo of GPS receiver on the spoofed yacht. Reader should notice altitude of the yacht (minus 4000 meters) and speed (449 knots). Source: [Cameron, 2014].

In this context it is worthy to mention two facts from the life of US Armed Forces. In 2011, Iran announced that it had captured a highly classified drone (Predator) belonging to the CIA by fooling its GPS to make it land in Iran instead of Afghanistan. Next year two U.S. Navy patrol boats wandered into Iranian waters. The Iranian military intercepted the boat and captured 10 U.S. sailors. The seamen were released the next day, but no military official was able to explain why the boats equipped by well-trained military personnel had strayed from their intended path. The incident prompted speculation that Iran had sent false GPS signals to lure the sailors onto another course, however it would not have been easy for the Iranians to hijack the military GPS receiver, as military signals are heavily encrypted, contrary to C/A signals. Any way accident is still not explained.

Two or three years later Pokemon Go, a new mobile phone game appeared. Then in Moscow young people discovered something strange, namely that around the Kremlin their smartphones still show position on Wnukowo airport! They quickly discovered that around the Kremlin three transmitters of false signals are distributed.

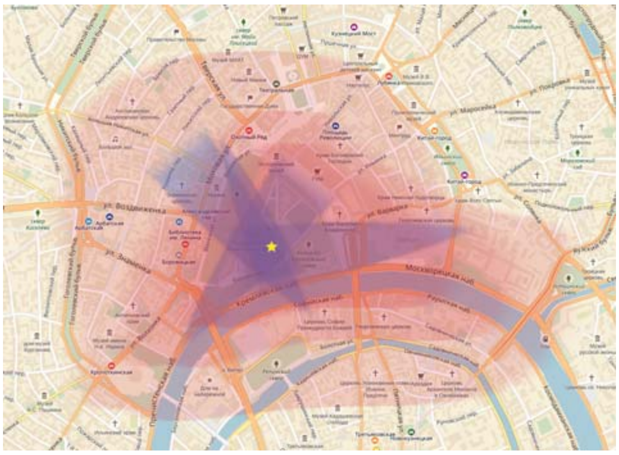

Figure 3. Distribution of spoofers around the Kremlin. Source: [The Kremlin, 2016].

In summer 2018 widely was commented the spoofing incident at Black Sea, near Novorossiysk. Almost 20 ships signaled at the same time completely false coordinates, presented by the GPS receiver, causing impression of the stable work of the receiver. The armed conflict in Syria has been blamed for much of the disruptions of its shores [Goward, 2018]. Similar evidences of jamming or spoofing has been observed also in Jeddah, Haifa, Strait of Hormuz as well.

The fact that the vast majority of marine GPS receivers in the world relied solely on the unencrypted C/A code became a cause for concern. Especially where biggest part of ships and many waters can be treated as elements of critical infrastructure.

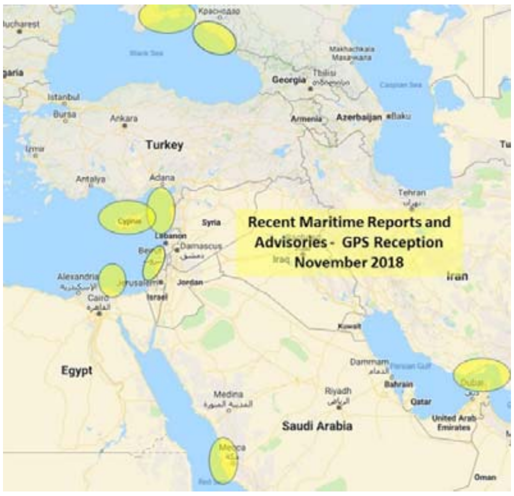

Figure 4. Examples of serious incidents in GPS disruptions in 2018. Source: [Goward, 2018].

## 3 SOLUTION OF THE PROBLEM

Many people still believed that it is too hard to build so complex equipment necessary to perform the spoofing attack, and this is out of reach for potential terrorists. In fact, commonly accessible, low-cost software-defined radio (SDR) enables spoofing if couple with open-source GPS simulation software! In the web exists details how to perform basic spoofing, and examples how they spoofed a drone. These may not be the most sophisticated setups, but it's good enough to do the job in many cases. There is no doubt that many states use this tactics in the everyday practice. Regarding the possibility of the common usage of jamming there cannot be doubts.

The treats of vulnerability of GNSS systems is commonly criticized and equally criticized is dependence on one source of information. In this situation, for example in 2015, U.S. House of Representatives in Resolution 1678 approved a resolution that would require establishment of a "strong, difficult-to-disrupt terrestrial system to complement GPS, and to serve as another source of PNT when GPS isn't available" [H.R.1678]. This has been noticed not only in US, and has led many institutions to look for alternative solutions that allow an application to maintain the efficiencies and effectiveness gained from the loss of their space-based systems and augmentations. As well within the framework of the e-Navigation project necessary of back-up system is notified. In this situation it is natural that at present a lot of international projects are executed in this field. The most attractive in this context seems to be AIS, DGPS and Loran modernization. The common basis for this options are well coordinated time stamps. According to the opinion of some specialists [Barlet et al., 2017], [Ward et al., 2015] new version of Loran (enhanced Loran, e-Loran) is declared by US officials and British General Lighthouse Authority (GLA) as the most perspective system and from this reason some money are intended for development works. Similar works are driven also in South Korea. At the moment e-Loran, which was introduced by American company Ursa Nav in the mid-1990s seems to be close to realization.

But Nederland's proposal Eurofix is investigated too, and this solution was installed already in the beginning of XXI century in Saudi Arabia [Cameron, 2015]. However at the moment, and probably for some next years this is still a future. The matter of consequence is the scale of introduction of such solutions worldwide, because we remember that radio-navigation systems never existed neither in South America, nor in Africa.

## 4 CONSEQUENCES OF THE PROBLEMS WITH GPS AND SUGGESTIOINS

From examples mentioned above we must draw a conclusion that difficulties with the utilization of the GPS become a commonplaceness. The unstable work, false signals or the inaccessibility of the GPS become a problem of our life. So today the practical question appears: how the officer of the watch should behave in such situation? How many officers are ready to recognize [Felski, 2016] presence of jamming? I heard many tales of persons who had such adventures on the bridge. Almost all they tell that in the first moment they began to analyze reasons of the faulty operation of the GPS receiver, and in that time the ship began to change course. What happened? The answer is simple: the autopilot received data about the bearing to next waypoint (WPT) and treated this as new Course Over Ground (COG), however incorrect GPS fix caused the wrong information, which is not recognized by autopilot as incorrect.

Similar, unforeseeable events, especially in the Integrated Navigational Bridge (IBS) or Integrated Navigation System (INS) can happen [Barlet et al., 2017]. There are differences between IBS and INS, but for this analysis let's skip them. So IBS (or INS) is commonly defined as sets of mutually joint sensors and executive elements which make possible the access to the information and the steering by ship from one workstation. What is crucial here is the phrase "mutually joint" that means the complicated dataflow and the mutual influence of one element on the second one.

In that case watch officer should be familiar with processes of the dataflow among the receiver GPS, with the automatic pilot, ECDIS, ARPA, AIS, as well as with the gyrocompass and log. Essential for analysis of possibly consequences of disturbances in GPS work is the sentence of SOLAS Chapter V, Reg 19, para 6 *"Integrated bridge systems shall be so arranged that failure of one sub-system is brought to the immediate attention of the officer in charge of the navigational watch by audible and visual alarms, and does not cause failure to any other sub-system. In case of failure in one part of an integrated navigational system, it shall be possible to operate each other individual item of equipment or part of the system separately" [SOLAS].* In such situation the watch keeper will be concerned with cancelling of all alarms firstly, that the uneasy captain will come on the bridge. However the problem is not in alarms, but in the reason why alarms are activated! This seems to be self-evident and simple that [Roper, 2017]:

- Watch keepers must be familiar with the operation of IBS (or INS) and in particular must be familiar with the alarms and be able to operate any override arrangements in case of a system failure;
- If a sub-system of an INS fails the watch keeper should be able to operate all the other components of the system independently.

Unfortunately life is more complicated, and in practice not all officers are efficient in this matters. Of course watch keepers must be knowledgeable in the configuration of the system and trained in performing this individually. This is the fact, that even on sister's ship the configuration of the system can be different, because in the past some person changed something according to personal fancy. Easy suggestion is, that clearly written instruction for the systems must be available on the bridge.

The most vital question is to specify devices which receive data from GPS receiver and to make sure that backup system works. As positioning system on busy waters the radar can be indicated as an attractive backup option for GNSS. This is obligatory equipment on the board, and usually stays in use, but paradoxically, when ECDIS is in use, many officers have a problem to transfer the position from radar to ECDIS.

Please remember, that nowadays ship has a lot of devices which should be supported by additional data and what in the past was performed by different devices, not GPS. One of less associated with GPS is gyrocompass which often takes the latitude and speed for the calculation of the speed correction.

This is trivial and universally well-known, that situational awareness to include verified position, is vital for safe navigation. So no matter how good and reliable is GPS, watch keepers should use alternative methods and systems for crosschecking data from the system. This is an important rule, not only in the face of GPS disruptions. Still manual checks and other back-up methods for positioning must be exercised on a regular basis.

The second threat is in ARPA. The proper work of this device needs data about the heading and speed of the ship. Today this can be transmitted as SOG and COG from GPS receiver. So when GPS is disrupted some problems with ARPA will occur either. It is truth, that SOLAS requires speed and distance measuring devices which should be connected with ARPA. However this device must work at the moment and be connected with ARPA. Is it so every time? By the way, some company offers today satellite speedometer which is in fact GPS receiver showing only the speed, but in some level vulnerable as standard receiver…

In such circumstances an experienced master may suggest to use the Parallel Indexing method of work with radar. This is very efficient tool when approaching the coast to confirm position or determine turning waypoints [Bole et al., 2014] but how many watch keepers are ready to use so old technique? Different investigations into cases where vessels have run aground have often shown that, when radar was being used as an aid to navigation, inadequate monitoring of the ship's position was a contributory factor. Parallel Index techniques provide the means of continuously monitoring a vessel's position in relation to a pre-determined passage plan, not checking whether GPS works or not. It is proper to instruct practicing this in clear weather during straightforward passages, so that watch-keepers remain thoroughly familiar with the technique and confident in its use in more demanding situations.

## 5 CONCLUSIONS

In this text I try to pay attention of the readers on the importance of disrupters in GPS accessibility and correct preparation of officers of the watch in this context. Over the recent years the problem of intentional disturbances in GPS work grows, and the awareness of unforeseeable results of this becomes unusually important. Such threat extorts the preparation of the officer on the bridge to evaluating of the complication, which can be caused by the lack of GPS signals.

Thus one can propose, that training scheme will take into account such aspects as:

- Understanding the mechanism of jamming and spoofing;
- The skill to diagnose of jamming or spoofing symptoms;
- Efficient setting-up and reconfiguring of the integrated navigation system;

But also he should be competent in radar use in the manner which is archaic in the opinion of many young watch keepers.

## BIBLIOGRAPHY

Bartlett S., Offermans G., Schue C. *A Wide-Area Multi-Application PNT Resiliency Solution.* (Accessible at: http://gpsworld.com/innovation-enhanced-loran/ (30-03-2017).

Bhattacharjee S. *What is Integrated Bridge System (IBS) on Ships*? Accessible at: https://www.marineinsight.com/marine-navigation/what-is-integrated-bridge-system-ibs-on-ships/ (26.01.2019).

Bole A., Wall A., Norris A. *Radar and ARPA manual. Radar, AIS and target tracking for marine radar users*. Elseviere, 2014.

Cameron A. *e-Loran Progresses Toward GPS Back-Up Role in U.S. & Europe*. GPS World June 25, 2015.

Cameron A. *Spoofer and Detector: Battle of the Titans at Sea.* GPS World August 5, 2014.

*Extreme space weather: impacts on engineered systems and infrastructure*, Royal Acad. of Engineering, London 2013, [online], http://www.raeng.org.uk, (12.09.2014).

Falen, G. L. Analysis and Simulation of Narrowband GPS Jamming Using Digital Excision Temporal Filtering. (Master's thesis) Air University, Air Force Institute of Technology, Ohio, 1994.

Felski A. *Methods of Improving the Jamming Resistance of GNSS Receiver*. Annual of Navigation 23/2016.

*Global Navigation Space Systems: reliance and vulnerabilities*. The Royal Academy of Engineering, London 2011. Available at: http://www.raeng.org.uk/gnss (12.09.2014).

Goward D. *Expert Opinion: Spoofing attack reveals GPS vulnerability*. GPS World, 2017. Accessible at: http://gpsworld.com/expert-opinion-spoofing-attack-reveals-gps-vulnerability/ (10.01.2018).

Goward D. GPS disrupted for maritime in Mediterranean, Red Sea. GPS World, 2018. Accessible at: https://www.gpsworld.com/gps-disrupted-for-maritime-in-mediterranean-red-sea/ (24.01.2019).

*H.R. 1678: National Positioning, Navigation, and Timing Resilience and Security Act of 2015*, House of Representatives bill in the United States. Congress, Washington, D.C.

Psiaki M.L., Humphreys T.H.; Brian Stauffer B. *Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies*. IEEE Spectrum, vol. 53, Issue 8, 2016.

Roper M. *Good navigation practices – How one vessel master managed safe navigation during a GPS outage*. Access at: http://mariners.coastguard.dodlive.mil/2017/09/21/92120 17-good-navigation-practices-how-one-vessel-master-managed-safe-navigation-during-a-gps-outage/ (24.01.2019).

http://gpsworld.com/gnss-systeminnovation-know-your-enemy-12475/. (21.02.2019).

http://solasv.mcga.gov.uk/regulations/regulation19.htm (20.02.2019).

http://solasv.mcga.gov.uk/ (20.02.2019).

Scott L., *Spoofs, Proofs & Jamming*, ‘Inside GNSS’, September/October 2012, pp. 42–53.

*Space Weather Full Report*. Royal Academy of Engineering, London, 2013. Access at: http://www.raeng.org.uk/publications (15.07.2014).

*The Kremlin eats GPS for breakfast*. The Moscow Times, 21.10.2016. Access at: https://themoscowtimes.com/articles/the-kremlin-eats-gps-for-breakfast-55823 (24.01.2019).

Ward N., Hargreaves C., Williams P., Bransby M. *Can eLoran Deliver Resilient PNT?* Proceedings of The Institute of Navigation 2015 Pacific PNT Meeting, Honolulu, Hawaii, April 20–23, 2015, pp. 1051–1054.