GNSS Signal Monitoring and Security of Supply of GNSS-Based Services

GNSS signal monitoring and security of supply of GNSS-based services

Saajasto Mika[1], Kaasalainen Sanna[1], Mäkelä Maija[2,1]
, Bhuiyan, M. Zahidul H.[1], Koivula Hannu[1], Kirkko-Jaakkola Martti[2,1]
, and Kuusniemi Heidi[3,1]

[1] Finnish Geospatial Research Institute, Espoo, Finland,
[2] Nordic Inertial Oy, Akaa, Finland
[3] School of Technology and Innovations, University of Vaasa, Finland

Abstract. The global GNSS markets are expected to grow considerably in future, thus the number of threats against GNSS services will also increase. Understanding how GNSS services are utilized on a national level is crucial for the resilience, safety and quality of these services.
This study summarises interviews of authorities and specialists in the given GNSS segments, national and international research on related GNSS markets and analysis of related technologies. We provide an introduction to the current state of GNSS-based services, important shortcomings related to security of supply, and the GNSS user needs in relation to GNSS security of supply. We discuss ways to mitigate threats aimed against GNSS services, for example GNSS monitoring and provide suggestions to improve the security of supply of GNSS services.
The GNSS markets are becoming increasingly vulnerable to interference, thus resilient navigation and timing solutions are needed. The authentication services of the Galileo-system are aimed to solve these problems, but they are not fully operational. The security of supply and the safety of the GNSS-based services should become a key feature in national cyber-security planning.

Keywords: GNSS · Security of Supply · Critical Infrastructure

1 Introduction

The need for resilient Positioning, Navigation, and Timing (PNT) has been steadily increasing. This particularly applies to services and applications related to critical infrastructure requiring precises time synchronisation, such as power grids, telecommunications, and financial transactions. The need for resilience is also evident in services that require precises location information such as search and rescue (SAR) and aviation. The COVID-pandemic introduced a new category of apps that are aware of context. To help fight the spread of the virus, authorities started to utilise anonymous location data to track areas where people moved, to create hot-spot maps. These maps were then used by applications to warn people and help them to avoid crowded areas [8]. Context-aware features

can also be used in financial services for secure authentication. Utilising user location information it is possible to see if, for example, an online purchase was done in a typical region for the user. A purchase from another country can then be labelled a possible fraud, increasing the protection for both customer and the company providing services [23].

PNT-solutions are commonly obtained from Global Navigation Satellite Systems (GNSS), because of the ease of use and availability. However, the vulnerability of GNSS systems has also been globally increasing as a result of interference from different sources [10, 26, 13]. These events and their mitigation have been widely studied [65, 55, 58] and it has been shown that there is no single source behind the interference events [5]. Interference can result from ionospheric variations, other (possibly faulty) equipment operating at Radio Frequencies (RF) close to satellite navigation signals, or malicious RF-interference. The intentional Radio Frequency Interference (RFI) events can be divided into two categories: signal jamming, where the GNSS signal is completely or partially obfuscated by noise [37], and spoofing, i.e., broadcasting a counterfeit signal [57]. The effects caused by GNSS jamming depend on the strength of the jamming signal, a weak signal will decrease the signal to noise of the measurements, increasing the uncertainty of the computed location or time solution. A more powerful jamming signal, for example from a military grade jamming device, is aimed to completely deny the use of GNSS signals. While both weak and strong jamming attacks can target several, or all, available GNSS signals, the more common weaker jamming attacks are typically caused by small hand held devices installed in cars or trucks and usually only target one frequency band.

The aim of a spoofing attack is fundamentally different compared to a jamming attack. Jamming is meant to deny service, but a spoofing attack tries to force a receiver to show incorrect location or time information. In recent years, the most common incidents attributed to GNSS spoofing have been related to illegal activities, for example by passing transport sanctions [2]. However, as seen in the incident from Shanghai, where several ships were spoofed to report them following a circular pattern, the aim of the spoofing attack is not always clear. As discussed in the article, there might be criminal intent involved, or it might be a test campaign for state level electronic warfare. However, a spoofing attack of this magnitude demonstrated high theoretical understanding and technological capabilities of the attackers [46, 36].

To protect the end users, the European GNSS service Galileo offers different services to secure or authenticate the navigation signal [22]. These services will be available for both civilians in the form of Open Service Navigation Message Authentication (OSNMA) and Commercial Authentication Service (CAS), and for governmental agencies or other safety-critical services via the Public Regulated Service (PRS). In spite of these security measures, GNSS could still be compromised by, e.g., a strong space weather event (see [68, 9] for potential effects of such events) or because of a system-wide malfunction, such as the event in 2014, where GLONASS satellites were sending incorrect broadcast messages. This system level malfunction caused some receiver types to also lose the GPS

signals, causing total loss of PNT [29]. Therefore, positioning based on other sensors or hybrid navigation solutions is an active fields of research, especially in the automotive industry [62]. In addition to resilient and precise location information, many critical infrastructures are increasingly dependent on precise time synchronisation, which is crucial for telecommunication networks, power grids, and financial sector [53, 39]. This increases the need for precise and resilient PNT solutions. In particular, security of supply has become a concern in the Arctic region, where there are strong ionospheric phenomena and the GNSS signal strength is weaker, because satellite orbits are not optimised for use at high latitudes. The need for improved resilience is further emphasised with the advance of intelligent transportation and the growing number of applications utilising the Internet of Things (IoT) [38]. Many of the IoT solutions have been focusing on consumer products, like wearable electronics, but industrial applications, for example controlling lighting or machine operations, logistical applications, for example tracking of goods, or even agricultural applications for tracking livestock, are becoming increasingly common. In the 3rd Generation Partnership Project (3GPP), it has been estimated that 75 % of the IoT applications would require or benefit greatly from positioning information [1]. The required accuracy depends on the application, but typical ranges are from a few meters to hundreds of meters. Meter level accuracy would be easily achieved with a GNSS chip set, but for IoT devices, the typical power consumption of these chips can be too high. However, there are emerging novel solutions to enable GNSS for low-power IoT devices, for example assisted GNSS technologies where for example satellite ephemeris data is transferred over cellular network [24].

The advancements in satellite technology have given rise to small, cost effective satellites, that are mainly deployed to the Low Earth Orbit (LEO) instead of the Medium Earth Orbit (MEO) typically utilized by communication and navigation satellites. Because of the lower altitude, any satellite constellation operating at LEO needs to have a higher number of satellites compared to constellations at MEO. The increased number of satellites and the closer proximity to the receivers provides a higher signal strength and better satellite geometry coverage, which are expected to increase the accuracy and robustness of PNT-services. However, the LEO-PNT concept is still under research and no real LEO-PNT systems are currently available [56]. In addition to the currently missing LEO-systems, there are currently no dedicated LEO-PNT signals. However, three possibilities exists. The first option is to use the LEO signals as signals of opportunity, and no PNT information is transmitted. In this case the angle of arrival of the signal or the Doppler shift can be used to estimate position. Secondly, it is possible to transmit a GNSS like signal, possibly in another frequency band, since current GNSS bands are heavily used. The third option is to create a dedicated LEO-PNT signal that would be optimised for LEO constellations. The challenges and possibilities provided by these approaches are evaluated in [56].

The vulnerability of different critical infrastructures to GNSS disruptions has been an increasing concern also beyond Finland. [34] has mapped the needs

for PNT in critical infrastructures and services in the United States, ranging from agriculture to emergency services in terms of positioning and navigation, and from electricity grids to financial services in terms of timing. The estimated costs of a long term GNSS outage are estimated to be more than 1 billion dollars a day. The report states that mitigating long term disruptions is very challenging as no single alternative PNT approach is sufficient to meet the positioning requirements of different critical infrastructures. They recommend that temporary short-term disruptions are mitigated by PNT users, and encourage adaptation of alternative PNT sources and resilience by system design in order to be prepared for long term GNSS outages. Also United Kingdom is exploring new ways to protect critical infrastructures [28]. Similarly, the International Civil Aviation Organization (ICAO) urges addressing GNSS interference, as it has a significant impact on flight operations and air traffic management [35].

Several GNSS interference monitoring approaches have been proposed as means for dealing with harmful interference. GNSS reference networks can be used to monitor the signal on a large scales [51], and machine learning approaches can be used to detect more subtle signal phenomena [38]. Also crowdsourcing [47, 50] with smartphones and interference detection using Low Earth Orbit (LEO) satellites [49] could be suitable for large scale wide area GNSS monitoring. Current approaches for spoofing detection focus on methods based on receiver signal processing [57]. Project STRIKE3 [65] has defined standardized way to report GNSS interference events in terms of event date, duration, region, frequency band etc. This standard can be adapted also for crowd-sourcing approach [47].

The occurrence of interference events is very common. A monitoring campaign within STRIKE3 project in 21 different countries and 48 different sites observed interference at all sites [4], located in city areas and nearby major roads. The interference incidents occurred more often than anticipated, even though they were often short in duration and only low power.

As GNSS disruptions can have serious consequences, for example airplane crash [35], and thus, critical infrastructure and operations need protection. By utilising signal monitoring and alert systems, GNSS end users can be more resilient towards disruptions in PNT.

The accuracy needs and other requirements, for example availability of navigation signals, are typically well know within specific industry, for example aviation, but these requirements might not be well known for other industries. The lack of collective overview of the needs and requirements of the GNSS sector and markets as a whole can become problematic especially for policy makers or companies trying to enter the markets.

Secondly, an overview providing a deeper understanding of the needs of critical infrastructure can be used to streamline future purchases of equipment that is required to maintain sufficient positioning or time synchronisation accuracy on a national level. Comprehensive and detailed market reviews for GNSS subfields are available, but the information is still scattered and there is a clear lack of a collective overview of the users needs and requirements over the GNSS field

as a whole. Furthermore, reports from specific GNSS sectors do not necessarily take into account specific needs of individual member states. For example, the arctic region presents certain challenges that require specific response from Nordic policy makers to ensure safe and efficient operations.

The aim of this article is to provide a collective overview of the GNSS user needs and requirements from the viewpoint of the security of supply. We have carried out an extensive end user survey to map the GNSS accuracy and availability needs in different sectors in Finland and combine this information with European and international scenarios from EGNSS (European Global Navigation Satellite System) market reports and existing literature. We will demonstrate the need and benefits of a situational awareness service with a jamming case study in Finland, to find out how a GNSS signal quality monitoring service can contribute to the security of supply of GNSS services. We will also assess the next steps and future work needed to improve the situation. The paper is organized as follows: the end user perspective and the security of supply are discussed in Sect. 2. A case study of GNSS monitoring and threat identification in Finland is presented in Sect 3, followed by a discussion and conclusions in Sects. 4 and 5, respectively.

2 GNSS security of supply

The European Union Agency for Space Program (EUSPA) has been collecting information from GNSS user segment by organising a User Consultation Platform (UCP), which aims to promote discussion within various fields on their needs for PNT solutions, and the required accuracy. As a part of the ongoing REASON project (Resilience and security of geospatial data for critical infrastructures) [38], the Finnish GNSS experts and stakeholders were interviewed to better understand the unique requirements and user needs in the Finnish context. The user groups that were interviewed consisted of private companies working in the GNSS segment, for example receiver manufacturers, but also companies that utilise GNSS as a part of their appliances or sell added value services, for example precise point positioning (PPP) corrections. In addition to GNSS industry, governmental institutes and companies involved in maintaining critical infrastructure were also interviewed. This group included, for example telecommunication and power grid operators and emergency services. Finally, scientific experts from research institutes and universities were interviewed to better understand the direction of research and educational readiness. As many of the interviewed entities operate in safety critical operations or are directly involved in national security, we will use the answers anonymously. All of the interviewed private companies provided their answers as industry standards and not as their own needs and requirements, thus the results are given anonymously. Furthermore, the user needs and requirements in many fields are very similar with those reported in the UCP, thus we present a collective summary which combines both the UCP reports and the interview results gained during the RESON project.

2.1 Accuracy and reliability needs of GNSS user segment

Because of the availability of GNSS services and the new opportunities provided by technological advancements, the needs and requirements of the end users have become more specific. In the following sections, overviews on the specific needs and requirements of the various fields are discussed and the required PNT accuracy is listed in Table 1.

We also discuss applications that might not need time synchronisation, but accurate time is crucial to ensure, for example, continuous telecommunication operations. On the other hand, in certain fields the precision needs are secondary, while continuous availability of GNSS has become the priority. Information on possible interference or service blackouts was a re-occurring need in the interviews of the Finnish GNSS field, and was reported as an operation critical service for companies. An early warning system could be used to prepare for temporary blackouts or to give valuable time to deploy the secondary backup systems. In the interviews from the REASON project, many of the end users also expressed the increasing need of resilient GNSS services, mainly because of strict tolerance requirements. For example in construction sector, the accuracy tolerance can be within 5 cm level, thus even a small disturbance in the availability of precises GNSS solution can bring the construction project to a halt.

The next generation GNSS services currently under research and development, can address the needs of many users, however, adopting these new technologies might not be straight forward. For example in aviation domain, any new technological implementations have to go through rigorous testing and validation process, and often requiring changes in legislation, which can be time consuming. For example, although the LEO-PNT concepts are expected to improve availability of navigation signals, and thus increase the security, their adaption to aviation domain will take time.

Time and synchronization The timing and time synchronization sector cover many critical operations of a modern society: electricity grids, telecommunications, and financial sector (banking and stock exchange). Several other heavily used applications have become more reliant on accurate time over the recent years: for example public transportation, wastewater systems, and television broadcasts [20].

Because of the variety of different applications and systems that require timing or synchronization services, the level of accuracy required for the services varies from one application to another. However, for the operators working in critical infrastructure, for example power grids operators, the required time synchronisation over the grid is at a micro second level. Thus, because of the known vulnerabilities, these operators should have their own emergency systems [67, 27, 60]. In Finland the telecommunication operators and electricity transmission stations maintain their own grand-master clocks to ensure sufficient time synchronization in case the national time service is inoperative. The need of accurate time has been identified as a critical requirement and for example investigations carried out in Great Britain and the United States have recommended that the

national time should not be maintained by a single laboratory, but rather a system of interlinked time laboratories is recommended [67, 27, 60]. Based on the investigation, a interlinked system of four time laboratories is currently under development in the Great Britain, and a similar system of decentralised time synchronisation services is used in Sweden.

- Telecommunication networks - Considering 5G systems, the time needs to be synchronized to an accuracy of 1.1 μs over the entire network with additional requirements of compensating for delay variation and jitter [20]. A synchronization accuracy worse than 1.1 μs will also affect the availability of the older network types (4G, 3G). Time synchronization of 100 ns is required for fibre-networks to detect defects that cause asymmetry in the optics and a similar accuracy of 100 ns is required for in certain satellite communication systems. The International Telecommunication Union (ITU) has documented a recommendation G.8272 (ITU G.8272/Y.1367 (11/18) and G.8272/Y.1367 (2018) Amendment 1 (03/20)) stating that the reference time signal of the network should be accurate to within 100 ns, when compared against a primary time standard, such as the Universal Coordinated Time (UTC). The recommendation also places requirements for the stability of the used time signals. Because of the need for high synchronization accuracy, any services that can detect and warn about GNSS interference are recommended to secure continuous operational stability.
- Finance – In the European Union, the time synchronization required by banks and stock exchanges is regulated by the MiFID2 directive (Directive 2014/65/EU), which places strict requirements for timestamps and time synchronization [20]. The exact time requirements depend on the nature of the trade operations in question. For example, in high frequency trading, HFT, the number of transactions can reach hundreds of thousands per second, which requires a high timing accuracy in the range of [100, 200] ns. On the other hand, for more conventional trading options the legally required granularity of the timestamps is 1 μs. The finance sector are legally required to be able to trace their time back to UTC time, but GPS time is not fully traceable to UTC [20]. Thus, NTP and PTP server time solutions are used.
- Electricity transmission - The GNSS time is used for measurements of the network status, but also to probe for possible faults along a transmission line [20]. For the current needs of the transmission networks, the GNSS time accuracy of 1 μs is sufficient. For applications using NTP/PTP protocols, and possibly for future upgraded technologies, it is recommended to deploy several GNSS receivers in the network sub-stations. Because of the importance of the electricity transmission, it is advised to deploy a backup system for the time synchronization.

Positioning The availability of GNSS positioning has helped to define rules and safety regulations, for example in aviation and enabled the development of new technologies, such as autonomous vehicles. The required positioning accuracy will naturally vary from one application to another, but the need for centimetre

level accuracy has significantly increased. At the same time, GNSS solutions have become more common in our everyday lives: many sports equipment track the position and velocity, and other services, such as augmented reality games (for example Pokemon GO) rely on user position to show specific content. Because the vast number of different applications and user needs, the entries are presented on a general level.

- Aviation - Although safe flying is possible without any GNSS systems, the efficiency and available capacity of the airports will be compromised and smaller airports cannot operate without GNSS support [16]. For example, a flight from the city of Tallin, Estonia, to Savonlinna in Finland had to be canceld several times in spring 2023, because of degraded GNSS signal availability. Because of its small size, the Savonlinna airport relays on GNSS equipment for landing operations, and without backup systems, safe landing could not be guaranteed. The EU decree 2018/1048 obliges member countries to move towards using GNSS at airports, but for example in Finland the change is still on strategic planning level (TRAFICOM publications 12/2021). The importance of GNSS is evident during landing and lift-off, but the required positioning accuracy can be on meter scale. On the contrary, precise time information can be crucial especially for large airports, not only for scheduling purposes but also for possible backup electricity grids and other safety critical applications. During flight, the positioning accuracy is relaxed to a few hundred meters [33]. However, continuous availability of location solution is expected with availability from 95% up to 99.999%.
  A new emerging trend in civil use of airspace are drones. Although there are some rules and regulations that limit where and how the drones can be flown, for example flying BVLOS, Beyond Visual Line of Sight, and no-fly zones around airports, the regulatory space, even on EU-level, is still evolving. The requirements on GNSS services are therefore unclear, but it is likely that they will reflect the general requirements of civil aviation.
- Maritime - GNSS systems are commonly used in maritime operations, and with increasing research on autonomous ships, the need for location services will increase in the future [17]. There are several auxiliary systems in use ranging from optical viewing to sonar systems. Therefore, failures in GNSS will not completely stop maritime traffic, as the auxiliary systems are sufficient for navigation, especially at open sea, where distances are larger and typical sailing speeds provide several minutes of reaction time. Accurate GNSS positioning and velocity information is needed in coastal waters and harbours, where accurate traffic control is required to assure safety of operations. The accuracy ranges from 100 m in open ocean conditions to 1 m in port operations and closed water ways but can be as high as 0.1 m for marine engineering needs. The vessels are also required to update their heading periodically, up to every 2 s depending on the sailing speed. Because of the increasing need for accurate GNSS information, there are initiatives to utilize EGNOS (European Geostationary Navigation Overlay Service) in maritime operations. In Finland, the FGI (Finnish Geospatial Research Institute) and

the FTIS (Finnish Transport Infrastructure Agency) are supporting ESSP (European Satellite Services Provider) to study the performance of EGNOS in the Gulf of Finland. EGNOS services will provide additional benefits for cargo optimization, as altitude information can be used for more efficient cargo distribution on-board transport vessels [42].

- Road users - GNSS and related services are widespread among the road users, although mobile phone applications have replaced integrated systems in many day-to-day situations [19]. The constant influx of positioning data transferred over networks have allowed new services that provide road user with real time information of road conditions or traffic jams. The need for accurate and resilient location information has thus become an everyday need, which will soon increase with self-driving cars. For safety systems such as collision avoidance, an accuracy of 1 m is generally sufficient. However, for automated solutions the location information has to be accurate to a level of $\sim$20 cm [43, 19]. The need for resilient positioning services has become apparent, as detailed by the Finnish Transport and Communications Agency (TRAFICOM), who have estimated that a severe interference in GNSS can stagnate land transportation. If 10% of all cars will be autonomous within 10 years, a GNSS interference that causes these cars to stop will partially halt the road traffic. The need of cybersecurity for road users was further underlined when the taxi services of a major city were hacked in early September 2022. A cyberattack against the online services of one of largest taxi companies operating in the area sent dozens of cars to a single location, causing a significant traffic jam [7].
- Railroads - The EU railway control systems are being updated with modern digital ones [18]. As a part of the digitisation, the 3$^{\text{rd}}$ level of the European Rail Traffic Management System (ERTMS) control systems utilize GNSS to provide accurate positioning. The use of GNSS in rail traffic was suggested in the account written by the European Parliament: satellite navigation could especially be used for tracking rail traffic to improve rail safety, and it should thus be a high priority for member states. The ERTMS system should be operational throughout the EU before 2040. For tracking applications, an accuracy in range of 1 to 10 meters is often enough, whereas structural monitoring and infrastructure surveying require centimetre level accuracy. The new GNSS systems for rail roads should also take into account GNSS interference, which could cause significant delays. In Finland, the Digital rail road (Digirata) [59] project is piloting approaches for train traffic control with GNSS and new 5G solutions.
- Construction and Agriculture - The availability of GNSS and the advances in receiver technology have opened new revenues for precision agriculture [15]. For example, the path of a farm machine can be programmed to follow the shape of the field in specific patterns or the planting of crops can be controlled in a predefined efficient way. On larger scales, GNSS can be used to control the daily operations of all farm machines in ways that optimize productivity. For construction workers, GNSS can be used to position the foundations of buildings or to precisely control the operating hand of heavy machinery.

The applications that utilize GNSS positioning have different needs for positioning accuracy, but for both agriculture and construction work, there are applications where centimetre level accuracy is needed. The research on autonomous cars will likely reflect on both agriculture and construction, with autonomous operations further increasing the need for accurate positioning services.

Table 1. GNSS user requirements and needs. The values are based on the EUSPA market reports and Finnish GNSS end user interviews.

Industry	Users	Positioning	Timing
Telecom	Telecommunications, data transfer	-	100 ns - 1 μs
Finance	Banks, stock exchange	-	100 ns - 1 μs
Electricity	Digital electricity stations	-	1 μs
Aviation	Civil aviation	$\sim$1 m	-
Maritime	Shipping industry	1 - 10 m	2 s
Road user	Navigation, autonomous driving	10 cm - 1 m	-
Rail roads	Civil transportation, rail transport	1 - 10 m	-
Constr. Agri.	Precision agriculture, construction sites	1 cm - 1 m	-

3 Case study: Finland

Following the trends of recent years, the number of companies that either provide or utilize GNSS-based services has been steadily increasing. Therefore, it is only natural to expect that the demand for robust location or timing services will also continue to increase. This increasing trend is not only seen in Finnish markets, but it is a global phenomenon (markets expected to grow to 405 B € by 2031 from the 150 B € revenue estimated for 2021 [21]). It is evident that the companies involved in GNSS markets have a solid understanding of the needs of their customers and the required know-how to provide, for example, nature friendly positioning devices utilizing solar power.

It is noteworthy that in Finland companies operating in the GNSS and related fields are often strongly involved with the public sector, supporting governmental agencies on different levels, and providing scientific research. Thus, governmental support and understanding of the needs, capabilities, and requirements of these companies are crucial to ensure the growth of the market segment. Some solutions have already been provided, such as the GNSS-Finland service [52], but the need for new services is expected to increase in the near future. The free collaboration among different stakeholders working with positioning and timing solutions, and to a larger extent, the whole Finnish space segment, allows effective planning and development of new projects and services. The opportunities provided by new GNSS services, for example the Galileo PRS service, are being

utilized, and there is a growing interest into research and development of new kind of receivers. The PRS service is expected to greatly improve the security of GNSS-based positioning and timing services throughout Europe. However, the PRS-service is only available for governmental entities, but Galileo OSNMA and CAS are available for general public. Although OSNMA and CAS are not as secure as PRS, they will offer increased security and robustness for many everyday PNT-services.

The National Land Survey of Finland maintains a GNSS situational awareness service, GNSS-Finland [52]. The GNSS-Finland service [51] was developed to provide 24/7 signal quality monitoring using the permanent FinnRef GNSS network [44]. The idea of using reference stations is similar to that in the COLOSSUS (Crowd-Sourced Platform for GNSS Anomaly Identification, Isolation and Attribution Analysis) project funded by the European Space Agency (ESA) [31]. Integrity monitoring using reference stations is often based on the measurement of the Carrier-to-Noise density Ratio (CNR), which is a simple parameter derived as receiver observable and available in all GNSS receivers [45].

3.1 GNSS threats in the Finnish context

The number of GNSS jamming incidents has been steadily increasing during the recent years, especially those involving small personal privacy devices (PPD). These devices are meant to conceal, e.g., personal location data to be used by employers. The range of the devices can be wide resulting in collateral damage. Several incidents of PPD's used in cars driving next to airports have been reported, which have caused delay in airport operations. Large-scale GNSS interference is relatively uncommon, but based on aviation pilot reports, hot spots of GNSS interference can be identified near European borders [12].

A similar trend of increasing small-scale GNSS interference has been reported in Finland, but there have only been two major interference events during the last few years. In the fall of 2018 [63], reports from northern Finland stated difficulties in gaining a location fix and the authorities issued a NOTAM (Notice To Airmen) warning covering most of Northern Finland. Another large-scale GNSS incident was in the spring of 2022, affecting large areas of eastern Finland [64, 32]. For several days, GNSS signals were degraded to a level that prevented smaller airports from operating and caused personal sportswear to report illogical exercise routes [14]. An airline was reported to have cancelled several flights. The lack of GNSS prevented safe landing operations, as the destination airport was small and did not have alternative navigation equipment. Based on these reports, it is evident that eastern Finland was affected by large scale jamming and spoofing. Although the impact was considerable for small airports, the impact of a large-scale GNSS interference event on a major airport like Helsinki-Vantaa would not completely deny planes from landing. It would still make it more difficult to operate safely, causing significant delays and loss of revenue.

A key benefit of GNSS signal monitoring is in improving the resilience against threats targeting critical infrastructure. Attacks against GNSS can place human life at risk or lead to significant financial loss, further underlining the need of

signal monitoring to understand the possible threats. For example, most goods transported to Finland are carried via waterways, which are mostly narrow, especially in the Archipelago Sea. Therefore, a spoofing attack on a cargo ship can have catastrophic results: loss of human life, environmental damage, loss of revenue, and a potential block of the shipping route. Spoofing attacks on vessels have been reported before. In an incident in Black Sea incident [30], several ships reported their GPS receivers to indicate them to be at a nearby airport while sailing at open sea. Another example is from Shanghai [48], where the captain of an American container ship reported that the ships AIS showed a nearby vessel jumping from one position to another. A visual observation revealed that the jumping ship was stationary at the dock. Further research on the AIS data from all nearby vessels showed that the locations of the vessels had been spoofed following a circular pattern. In total over 300 vessels had been affected on the same day that the American ship made the report. Furthermore, to exclude possible problems with the AIS of the American container ship, the researchers used data from a smartphone fitness app that records user location. The data showed the user location to follow a similar circular pattern as seen in the AIS data, pointing to a large-scale spoofing attack. However, a recent study on the cybersecurity of the AIS has shown that the system is vulnerable against attacks utilising radio frequency links, and that the attack can be carried out with a low cost setup [41].

In addition to accurate location, critical infrastructures of a modern society depend on precise time information. Smart power grids, telecommunication, and stock exchanges all require time synchronisation at microsecond level. It is therefore evident that these applications are vulnerable against spoofing or time synchronisation attacks. In a recent paper, [69] studied different spoofing based attacks, and how to defend against them in the context of smart power grids. It was found that a defence-in-depth method is necessary to provide sufficient level of protection, as none of the defensive precautions suggested could provide good results against all of the attack methods studied. In the Finnish context, VTT MIKES (Technical Research Centre of Finland, metrology centre) provides the official Finnish realisation of the UTC (Universal Time Coordinated) time. The UTC is a 24 hour time standard, which is kept to a high synchronisation globally by national time laboratories utilising extremely precise atomic clocks and taking into account for example the Earth's rotation. Thus the generation of the UTC time is a international effort coordinated by the International Bureau of Weights and Measures (BIPM). The UTC time 0:00 is defined as midnight at Earth's zero meridian, which passes through Greenwich in England, linking the UTC with the Greenwich Mean Time (GMT) system.

National time laboratories distributes their own realisation of the UTC time which in the Finnish context is called UTC(MIKE). The time difference between the UTC time and the national Finnish time is plus 2 or 3 hours, depending on the daylight saving time. The official Finnish time is distributed from a single laboratory, but for example, telecommunication operators maintain their own grand master clocks. These clocks are required to operate independently for two

weeks in a case of an emergency. To increase the robustness of the time synchronisation services, a model where the official time is maintained with an interlinked system of several time laboratories would be beneficial. An interlinked system has been developed in Sweden [60], where the Swedish national time UTC(SP) is distributed from several different locations. In the United Kingdom, a system of several interconnected time laboratories is currently under development [27] and a similar system for time distribution was also recommended by a research done in the United States of America [67].

As the use of GNSS-based services is increasing, the number of interference events is growing as well. However, the currently available technology to localize interference signals is both costly and unwieldy. More research and development are needed to make the equipment more widespread. Combining small and light consumer grade detectors with the GNSS-Finland service could be a solution to create a denser monitoring network, which would allow a more robust and accurate detection system. Such a network could also be used to monitor and model space weather, separate local and large-scale phenomena, and give predictions of the possible cause (man-made versus natural). Long term continued monitoring would also improve our response against severe space weather, and other possibilities not yet been realised are likely to turn up.

3.2 Interference monitoring with GNSS-Finland

An example of interference detection provided directly by the GNSS-Finland service is presented in Fig. 1, which shows the CNR (Carrier-to-Noise density Ratio) of Glonass G1 frequency recorded at one of the FinnRef stations in 2021. There is a significant decrease in the CNR at 9.30AM local time, which was detected by the service. An alert was issued when the CNR reached a threshold value pre-set by the service user. This time, the Glonass G1 was the only frequency band with problems, while the rest of the systems were functional. A similar incident was recorded two weeks later, and the data combined with information from CCTV surveillance cameras showed the cause to be a truck approaching the site, first at 100 m and then at 10 m distance from the receiver (both incidents are visible in Fig. 1).

The incident in Fig. 1 is an example of a typical use case of a GNSS situational awareness service. The cause of the interference is not available from the CNR-plot, and more information is required to determine the cause, i.e., whether it is intentional or caused by a natural phenomenon or by a malfunctioning device. In this case, additional information from the CCTV was enough to solve the case, but in most situations, it would be necessary to analyse the frequency spectrum to identify the sources of intentional interference. A database of frequency spectra has been collected in the STRIKE3-project to enable a classification scheme [11]. Antenna arrays and information from other sensors (such as in this case) have also been used to localize the source [3].

GNSS interference is mainly detected from the Automatic Gain Control (AGC), CNR, or by analysing the frequency data when available [25, 6]. Antenna solutions, such as Directional antennas or Controlled Reception-Pattern

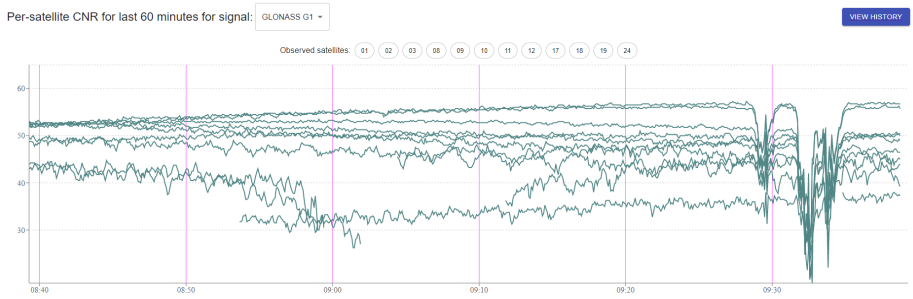

Fig. 1. Carrier-to-Noise density Ratio vs. time of Glonass G1 signal showing the significant decrease in CNR right after 9.30AM local time, as seen in the data directly provided by the GNSS-Finland Service.

Antennas (CRPA), can also be used to mitigate interference. To be able to identify a jamming signal, the RF spectrum of the signal should be available, but CNR-based detection is so far mostly provided by reference stations. For an improved characterization and identification of error sources, the following parameters usually available in reference station data would provide more information:

- Comparison of position and time information (to estimate the positioning performance)
- Satellite orbit information for monitoring system performance [40]
- Dual frequency positioning for estimating ionospheric errors (cf. [61])
- AGC values have been shown to correlate with GNSS jamming (e.g., [45]). A reduced AGC value was also defined as an event detection criterion in the STRIKE3 project. [65].
- The frequency spectrum of the receiver
- Sudden changes in the RTK (Real-Time Kinematic) correction values should also be monitored
- Historic information on past interference events would also help to classify an incident

Comparing these cases with those where jamming has been reliably identified will also provide a statistical way to assess the possibility of intentional jamming even in the cases where the RF spectrum were not available. If on-site GNSS jamming detection or localization is not available and the detection would only be based on a reference network, a reliable jamming identification is likely to be a result of a combination of parameters.

4 Discussion

Several studies carried out independently in Sweden, Great Britain, and USA [67, 27, 60] have reached a similar conclusion: modern societies are extremely

dependent on accurate positioning and especially time information provided by GNSS systems. Power grids and financial sector require nanosecond level accuracy to operate. At the same time, GNSS satellites are vulnerable against natural phenomena, such as solar storms, for which the occurrences and strength are difficult to predict. A major solar storm that strikes the Earth can potentially black out all GNSS systems and services. There is also an increase in local occurrences of GNSS jamming as a result of the crisis in the Eastern Europe [32]. In such events, it is critical to have a working network of back-up systems that can secure the critical infrastructure. Typically these secondary or back-up systems are used alongside GNSS or they can be used to provide sufficient positioning accuracy if GNSS is unavailable. Another method is to monitor the GNSS signals to better understand typical errors and develop mitigation techniques based on these observations.

There is a wide range of backup systems from terrestrial radio beacon networks (enhanced long range navigation, eLORAN) to sensor and hybrid positioning. A recent addition to the terrestrial radio network solution was presented by [66], who propose a two component system for providing a PNT solution in dense urban environments where GNSS signals suffer degradation caused by multi path effects and blocked signal due to high buildings. The proposed system uses a wide band radio signal for ranging and a optical fiber link between the ground stations to distribute accurate time information. The results are promising, but the system is still in prototype phase, but could offer a regional solution for accurate PNT.

The studies led by Great Britain and USA proposed a terrestrial radio beacon network, eLORAN, as the most cost-effective back-up system for GNSS-based navigation (e.g., [27] and references therein). With the advances in both receiver technologies and signal design, eLORAN could achieve a navigation accuracy of $\sim$8 meters and a timing accuracy below 1 μs. The timing accuracy can be further improved to $\sim$100 ns by applying differential corrections [54]. Although the positioning accuracy is not comparable with modern GNSS-based solutions, eLORAN can provide a sufficient backup solution for many applications. A widespread eLORAN network could also be used as an auxiliary system in support of GNSS, for example as DGNSS stations.

In addition to auxiliary systems, monitoring the quality of the GNSS signal can help in mitigating the vulnerabilities of GNSS systems. The COLOSSUS (Crowd-Sourced Platform for GNSS Anomaly Identification, Isolation and Attribution Analysis) project that started 2017 aims at global GNSS error mapping with CORS (Continuously Operating Reference Stations) networks [31]. The detected errors and the related information will be uploaded to a database, which can be used to study the regional differences of GNSS errors. As the COLOSSUS project aims to create a global network of stations, the density of the stations will be naturally low compared to, for example many national monitoring station networks. Thus local level faults will be hard to detect, but detection large scale phenomena or system level faults will be faster and easier. In Finland, the GNSS-Finland service utilises CNR data produced by the national FinnRef-network

[51] for GNSS interference detection. However, only a fraction of the available data is currently being included in the GNSS-Finland service. For example, historic information about disruptions in GNSS signal is available through FinnRef stations but this information is not logged by the service. Such information is valuable and GNSS market stakeholders have expressed interest in it. Other interesting information that could be derived from the GNSS-Finland data include the cause of interference, time information, and the possible inclusion of EGNOS (and PRS service in the future) monitoring information. This kind of signal quality control would require a large database and would improve the related services. This is the case especially for EGNOS, for which regional quality control would result in significant improvements in service quality, especially in the Northern regions, where the availability of the signal is already limited. The Galileo High Accuracy Service (HAS) is planned to become operational by 2024. Performance monitoring of Galileo HAS signals would be vital for knowing if the performance meets its expectation in the mid-to-high latitude region.

4.1 Future of location and time-based services

With the introduction of 5G-signal and Artificial Intelligence -based processing solutions, future systems such as IoT and autonomous transportation are likely to utilize cloud computing (or Big Data in general) to a greater extent than is currently being done. This will further emphasize the need for improved cybersecurity. However, these technologies require considerably more computational power and are not well suited for many consumer grade solutions, where low energy consumption is a critical requirement. For example adding modern navigation message authentication services to mobile phones would require considerable increase in requred computational operations. Assisted GNSS technologies seem to be a promising solution, but will likely require more research before they can be adapted to consumer products. Furthermore, server-side solutions for navigation will likely be a good fit for several IoT applications, but the transfer of data between the servers and the various IoT devices will require further work to assure the speed and safety of the provided services.

Other significant future developments are quantum navigation and the use of Low-Earth-Orbit (LEO) satellites for positioning. These technologies are currently being studied to a large extent. The advantage of using LEO satellites is their closer proximity to Earth, so that the signal strength is higher. Because LEO satellites are smaller, they are cheaper to build allowing more extensive constellations to be deployed. However, dedicated LEO constellations for PNT do not currently exist, and there are several open research questions related to the LEO constellations. Should these be stand-alone systems, or assisting current GNSS systems? Should the signal be broadcast at the GNSS frequencies, or should these satellites use higher (or lower) frequency bands? There are several large research and development projects currently starting in Europe, thus the LEO concept and the capabilities of these constellations will become much clearer within the next 5 years. Quantum navigation is expected to provide high precision and secure navigation and timing solutions, but the problem with the

current technology is the amount of needed supporting electronics, and thus the size of the systems.

The advancing receiver technology will increase the use of multi-constellation multi-frequency (MCMF) receivers. They will improve the stability of the services provided, especially in the timing domain, but the improved accuracy and availability will likely increase the use for location-based services. New services like Galileo OSNMA and PRS, particularly if combined with global monitoring effort, will offer increased resilience and security for both location and timing applications. However, even the most modern receivers are still not fully utilising the advantages provided by MCMF. For example, many receivers are still using GPS L1 channel as a primary, thus if this channel is not available due to signal jamming, the receiver stops providing a PNT solution. Although many receivers can detect and inform the user that they are detecting signal jamming (or spoofing), further research and development is required for receivers to be able to reliably identify jamming and spoofing and to stop using the affected frequency bands and only rely on the 'clean' frequency bands for PNT.

The accuracy needs of the GNSS end user summarised in Table 1, show a clear need for precises positioning and time synchronisation. There is also a clear need to increase the robustness and resilience of both location and time based services, as growing number safety critical services depend on GNSS-based systems. The future services offered by the Galileo constellation, PRS, OSNMA, and CAS, combined with the expected improvements provided by the emerging LEO-constellations (better signal strength, increased satellite coverage, and new services), will create a new type of markets, which will offer Secure and Precises Navigation as a Service (SaPNaaS). However, even these services cannot provide PNT under heavy jamming of spoofing attack. Combined with the increasing requirements on accurate positioning and time synchronisation needs, it is recommended that a system-of-systems approach is implemented, especially for safety critical system and national critical infrastructures. The quality-to-price ratio of inertial sensors, gyroscopes, and other MEMS (Micro-Electro-Mechanical Systems) based sensors has been steadily improving, thus adding additional sensor to support traditional GNSS based receivers will provide additional resilience, but will require more processing power from computers. Furthermore, fiber-optical systems or Chip-scale atomic clocks (CSAC), should be deployed to support GNSS based time synchronisation to systems that are critically dependant on precise time synchronisation. The individual components of this system-of-systems approach are well studied, but combining them together in a efficient manner and taking into account the increasing amount of data and security concerns can be challenging.

5 Conclusions

GNSS technologies have come a along way, and services based on GNSS solutions have become an everyday part of our lives. As the popularity of GNSS increases, so do the threats affecting GNSS-based services and the need for robust and

resilient location and time information. The constant increase in demand in turn requires constant adaptation and development of new techniques and technology. This need for new technological solutions has become more apparent during the last decade, as our lives are more and more reliant on digital solutions.

The availability and safety of GNSS-based services is relatively good throughout Finland, although as we have discussed here, there are certain vulnerabilities and shortcomings that we have identified. We have attempted to offer guidelines and suggestions on how to further improve the situation. As discussed, the need for improved national level time synchronisation and a denser monitoring network for GNSS signals are two of the issues that should be focused on. Although the end user study was carried out in Finland, many of the findings can also be applied elsewhere too as many services run similarly in other countries as well.

The Finnish and international research will greatly improve the resilience and robustness of GNSS-based positioning and timing. International monitoring efforts will improve our understanding of the threats that these services face. GNSS constellations are expensive to create and maintain. Supporting technologies, such as cube satellites and hybrid or sensor-based navigation, will see an increase in interest in the future. The same goes for technologies based on quantum physics. In Finland, the GNSS markets, development, and research efforts will follow these trends, assuming that there will be enough experts to fill the required positions.

Acknowledgment

This work has been supported by Academy of Finland special funding for research into crisis preparedness and security of supply (project REASON - Resilience and Security of Geospatial Data for Critical Infrastructures, decision number: 338042) and National Emergency Supply Agency of Finland program Digital Security 2030.

References

1. 3GPP: Positioning for the internet of things: A 3gpp perspective (2016), https://arxiv.org/ftp/arxiv/papers/1705/1705.04269.pdf
2. Anatoly Kurmanaev: How fake gps coordinates are leading to lawlessness on the high seas (2022), https://www.nytimes.com/2022/09/03/world/americas/ships-gps-international-law.html
3. Axell, E.: Gnss interference detection (May 2014), https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--3839--SE
4. Bhuiyan, M.Z.H., Ferrara, N.G., Thombre, S., Hashemi, A., Pattinson, M., Dumville, M., Alexandersson, M., Axell, E., Eliardsson, P., Pölöskey, M., Manikundalam, V., Lee, S., Reyes Gonzalez, J.: H2020 STRIKE3: Standardization of Interference Threat Monitoring and Receiver Testing - Significant Achievements and Impact. European Microwave Association (2019)

5. Bhuiyan, M.Z.H., Ferrara, N.G., Hashemi, A., Thombre, S., Pattinson, M., Dumville, M.: Impact Analysis of Standardized GNSS Receiver Testing against Real-World Interferences Detected at Live Monitoring Sites. Sensors **19**(6), 1276 (Jan 2019). https://doi.org/10.3390/s19061276
6. Borio, D., Dovis, F., Kuusniemi, H., Lo Presti, L.: Impact and detection of gnss jammers on consumer grade satellite navigation receivers. Proceedings of the IEEE **104**(6), 1233–1245 (2016). https://doi.org/10.1109/JPROC.2016.2543266
7. Cybernews: Hackers created an enormous traffic jam in moscow (Sep 2022), https://cybernews.com/cyber-war/hackers-created-an-enormous-traffic-jam-in-moscow/
8. Czech Technical University: Fremen adviser, application to avoid crowds (2023), https://cs.fel.cvut.cz/en/news/detail/1572
9. Demyanov, V., Yasyukevich, Y.: Space weather: risk factors for Global Navigation Satellite Systems. Solar-Terrestrial Physics **7**(2), 28–47 (Jun 2021). https://doi.org/10.12737/stp-72202104
10. Dovis, F.: GNSS interference threats and countermeasures. Artech House (2015)
11. Dumville, M., Pattinson, M., Manikundalam, V., Eliardsson, M., Payne, D., Towlson, O.: Strike3 d6.2: Threat database analysis report (Jan 2019), http://gnss-strike3.eu/downloads/STRIKE3_D6.2_Threat_database_Analysis_Report_public_v1.0.pdf
12. EUROCONTROL: Does radio frequency interference to satellite navigation pose an increasing threat to network efficiency, cost-effectiveness and ultimately safety? (Mar 2021), https://www.eurocontrol.int/sites/default/files/2021-03/eurocontrol-think-paper-9-radio-frequency-intereference-satellite-navigation.pdf
13. Eurocontrol: Radio frequency interference to satellite navigation: An active threat for aviation? (Mar 2021), https://www.eurocontrol.int/sites/default/files/2021-03/eurocontrol-think-paper-9-radio-frequency-intereference-satellite-navigation.pdf
14. Euronews: Planes and smartwatches near finland's russian border had gps issues, and not for the first time (Mar 2022), https://www.euronews.com/next/2022/03/16/planes-and-smartwatches-near-finland-s-russian-border-had-gps-issues-and-not-for-the-first
15. EUSPA: Report on agriculture user needs and requirements (2021), https://www.gsc-europa.eu/sites/default/files/sites/all/files/Report_on_User_Needs_and_Requirements_Agriculture.pdf
16. EUSPA: Report on aviation user needs and requirements (2021), https://www.gsc-europa.eu/sites/default/files/sites/all/files/Report_on_User_Needs_and_Requirements_Aviation.pdf
17. EUSPA: Report on maritime and inland waterways user needs and requirements (2021), https://www.gsc-europa.eu/sites/default/files/sites/all/files/Report_on_User_Needs_and_Requirements_Maritime.pdf
18. EUSPA: Report on rail user needs and requirements (2021), https://www.gsc-europa.eu/sites/default/files/sites/all/files/Report_on_User_Needs_and_Requirements_Rail.pdf
19. EUSPA: Report on road user needs and requirements (2021), https://www.gsc-europa.eu/sites/default/files/sites/all/files/Report_on_User_Needs_and_Requirements_Road.pdf

20. EUSPA: Report on time and synchronisation user needs and requirements (2021), https://www.gsc-europa.eu/sites/default/files/sites/all/files/Report_on_User_Needs_and_Requirements_Timing_Synchronisation.pdf
21. EUSPA: Euspa eo and gnss market report 2022 (2022), https://www.euspa.europa.eu/sites/default/files/uploads/euspa_market_report_2022.pdf
22. EUSPA: Galileo services (euspa). https://www.gsc-europa.eu/galileo/services (2022)
23. EUSPA: Euspa market report on eo and gnss 2022 (2023), https://www.euspa.europa.eu/sites/default/files/uploads/euspa_market_report_2022.pdf
24. EUSPA/GSA: Power-efficient positioning for the internet of things (2020), https://www.euspa.europa.eu/sites/default/files/uploads/gsa_internet_of_things_white_paper.pdf
25. Ferrara, N.G., Bhuiyan, M.Z.H., Söderholm, S., Ruotsalainen, L., Kuusniemi, H.: A new implementation of narrowband interference detection, characterization, and mitigation technique for a software-defined multi-GNSS receiver. GPS Solutions **22**(4) (Aug 2018). https://doi.org/10.1007/s10291-018-0769-z, https://doi.org/10.1007/s10291-018-0769-z
26. Glomsvoll, O., Bonenberg, L.K.: Gnss jamming resilience for close to shore navigation in the northern sea. Journal of Navigation **70**(1), 33–48 (2017). https://doi.org/10.1017/S0373463316000473
27. GOS: Satellite-derived time and position: A study of critical dependencies. Government Office for Science (2018)
28. GOV.UK: Government to explore new ways of delivering 'sat nav' for the UK (2020), https://www.gov.uk/government/news/government-to-explore-new-ways-of-delivering-sat-nav-for-the-uk
29. GPS-world: The system: Glonass in april, what went wrong (2014), https://www.gpsworld.com/the-system-glonass-in-april-what-went-wrong/
30. GPS World: Spoofing in the black sea: What really happened? (Oct 2017), https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/
31. GPS World: Esa to use cors networks for global error mapping (2019), https://www.gpsworld.com/esa-to-use-cors-networks-for-global-error-mapping/
32. GPS World: Finnish airline finds gps interference near russian border (Mar 2022), https://www.gpsworld.com/finnish-airline-finds-gps-interference-near-russian-border/
33. GSA: Egnos safety of life service definition document issue 3.4 (Apr 2021), https://www.gsc-europa.eu/sites/default/files/sites/all/files/egnos_sol_sdd_in_force.pdf
34. Homeland Security: Report on Positioning, Navigation, and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System (GPS) (2020)
35. ICAO: An urgent need to address harmful interferences to gnss (2019)
36. Inside GNSS: Sinister spoofing in shanghai (2019), https://insidegnss.com/sinister-spoofing-in-shanghai/
37. Islam S., Bhuiyan M.Z.H., T.S., S., K.: Combating Single-Frequency Jamming through a Multi-Frequency, Multi-Constellation Software Receiver: A Case Study for Maritime Navigation in the Gulf of Finland. Sensors **22** (2022). https://doi.org/https://doi.org/10.3390/s22062294
38. Kaasalainen, S., Mäkela, M., Ruotsalainen, L., Malmivirta, T., Fordell, T., Hanhijärvi, K., Wallin, A., Lindvall, T., Nikolskiy, S., Olkkonen, M.K., et al.: Reason-resilience and security of geospatial data for critical infrastructures. In: CEUR Workshop Proceedings. vol. 2880 (2020)

39. Kankaanpaa, J.P.: Gnss related threats to power grid applications (3 2021), https://urn.fi/URN:NBN:fi-fe202103096912
40. Kazmierski, K., Sośnica, K., Hadas, T.: Quality assessment of multi-GNSS orbits and clocks for real-time precise point positioning. GPS Solutions **22**(1) (Nov 2017). https://doi.org/10.1007/s10291-017-0678-6, https://doi.org/10.1007/s10291-017-0678-6
41. Khandker, S., Turtiainen, H., Costin, A., Hämäläinen, T.: Cybersecurity attacks on software logic and error handling within ais implementations: A systematic testing of resilience. IEEE Access **10**, 29493–29505 (2022). https://doi.org/10.1109/ACCESS.2022.3158943
42. Khatun, A., Thombre, S., Bhuiyan, M.Z.H., Bilker-Koivula, M., Koivula, H.: Preliminary study on utilizing gnss-based techniques for enhanced height estimation for vessels in finnish waterways. FTIA publications **18** (2021), https://urn.fi/URN:ISBN:978-952-317-854-0
43. Kirkko-Jaakkola, M., Marila, S., Thombre, S., Honkala, S., Koivula, H., Kuusniemi, H., Söderholm, S.: Hybridization of gnss and on-board sensors for validating the aurora ecosystem. Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation pp. 2172–2185 (Sep 2019). https://doi.org/10.33012/2019.16916, https://doi.org/10.33012/2019.16916
44. Koivula, H.: Finnish permanent GNSS network FinnRef - evolution towards a versatile positioning service. Doctoral thesis, School of Engineering (2019), http://urn.fi/URN:ISBN:978-952-60-8630-9
45. Larsen, S.S., Jensen, A.B.O., Olesen, D.H.: Characterization of carrier phase-based positioning in real-world jamming conditions. Remote Sensing **13**(14), 2680 (Jul 2021). https://doi.org/10.3390/rs13142680, https://doi.org/10.3390/rs13142680
46. Mark Harris: Ghost ships, crop circles, and soft gold: A gps mystery in shanghai (2019), https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/
47. Miralles, D., Moghadam, M.S., Akos, D.M.: GNSS Threat Monitoring and Reporting with the Android Raw GNSS Measurements and STRIKE3. In: Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019). pp. 275–289 (Sep 2019). https://doi.org/10.33012/2019.16984
48. MIT Technology Review: Ghost ships, crop circles, and soft gold: A gps mystery in shanghai (Nov 2019), https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/
49. Murrian, M.J., Narula, L., Humphreys, T.E.: Characterizing Terrestrial GNSS Interference from Low Earth Orbit. In: Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019). pp. 3239–3253 (Sep 2019). https://doi.org/10.33012/2019.17065
50. Nguyen, H.L., Troglia Gamba, M., Falletti, E., Ta, T.H.: Situational Awareness: Mapping Interference Sources in Real-Time Using a Smartphone App. Sensors **18**(12), 4130 (Dec 2018). https://doi.org/10.3390/s18124130
51. Nikolskiy, S., Bredenbeck, A., Rikkinen, T., Vallet, J., Koivisto, M., Honkala, S., Bhuiyan, Z., Thombre, S.: Gnss signal quality monitoring based on a reference station network. In: 2020 European Navigation Conference (ENC). pp. 1–10 (2020). https://doi.org/10.23919/ENC48637.2020.9317361
52. NLS: Gnss-finland service (Mar 2021), https://gnss-finland.nls.fi
53. NPL: A complete guide to time stamping regulations in the financial sector. https://www.npl.co.uk/products-services/time-frequency/npltime/guide (2019)

54. Offermans, G., Bartlett, S., Schue, C.: Providing a resilient timing and utc service using eloran in the united states. NAVIGATION **64**(3), 339–349 (2017). https://doi.org/https://doi.org/10.1002/navi.197, https://onlinelibrary.wiley.com/doi/abs/10.1002/navi.197
55. Pattinson, M., Dumville, M., Ying, Y., Gabrielsson, B., Waern, Å., Hill, S., Lee, S., Bhuiyan, M.Z.H., Kuusniemi, H., Poloskey, M., Shivaramaiah, N., Kibe, S., Gonzalez, J.R.: Standardisation of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation. In: European Navigation Conference 2016. p. 7 (2016)
56. Prol, F.S., Ferre, R.M., Saleem, Z., Välisuo, P., Pinell, C., Lohan, E.S., Elsanhoury, M., Elmusrati, M., Islam, S., Çelikbilek, K., Selvan, K., Yliaho, J., Rutledge, K., Ojala, A., Ferranti, L., Praks, J., Bhuiyan, M.Z.H., Kaasalainen, S., Kuusniemi, H.: Position, navigation, and timing (pnt) through low earth orbit (leo) satellites: A survey on current status, challenges, and opportunities. IEEE Access **10**, 83971–84002 (2022). https://doi.org/10.1109/ACCESS.2022.3194050
57. Psiaki, M.L., Humphreys, T.E.: GNSS Spoofing and Detection. Proceedings of the IEEE **104**(6), 1258–1270 (Jun 2016). https://doi.org/10.1109/JPROC.2016.2526658
58. Pullen, S., Gao, G.X.: Gnss jamming in the name of privacy potential threat to gps aviation. Inside GNSS **35**, 34–43 (2012)
59. Pylvanainen, J., Lehtola, J., Nieminen, T., Brotherus, M., Sandelin, E., Wallin, J., Artukka, J.: Towards digital and intelligent rail transport – final report of the digi rail study. Publications of Ministry of Transport and Communications **6** (2020), http://urn.fi/URN:ISBN:978-952-243-589-7
60. Rieck, C., Jaldehag, K., Ebenhag, S.C., Jarlemark, P., Hedekvist, P.O.: Time and frequency laboratory activities at rise. Proceedings of the 51st Annual Precise Time and Time Interval Systems and Applications Meeting pp. 169 – 180 (2020). https://doi.org/https://doi.org/10.33012/2020.17297
61. Rovira-Garcia, A., Ibáñez-Segura, D., Orús-Perez, R., Juan, J.M., Sanz, J., González-Casado, G.: Assessing the quality of ionospheric models through GNSS positioning error: methodology and results. GPS Solutions **24**(1) (Nov 2019). https://doi.org/10.1007/s10291-019-0918-z, https://doi.org/10.1007/s10291-019-0918-z
62. Ruotsalainen, L., Renaudin, V., Pei, L., Piras, M., Marais, J., Cavalheri, E., Kaasalainen, S.: Toward autonomous driving in arctic areas. IEEE Intelligent Transportation Systems Magazine **12**(3), 10–24 (2020). https://doi.org/10.1109/MITS.2020.2994014
63. The Barents Observer: Pilots warned of jamming in finnmark (Nov 2018), https://thebarentsobserver.com/en/security/2018/11/pilots-warned-jamming-finnmark
64. The Guardian: Finland reports gps disturbances in aircraft flying over russia's kaliningrad (Mar 2022), https://www.theguardian.com/world/2022/mar/09/finland-gps-disturbances-aircrafts-russia
65. Thombre, S., Bhuiyan, M.Z.H., Eliardsson, P., Gabrielsson, B., Pattinson, M., Dumville, M., Fryganiotis, D., Hill, S., Manikundalam, V., Pölöskey, M., Lee, S., Ruotsalainen, L., Söderholm, S., Kuusniemi, H.: GNSS Threat Monitoring and Reporting: Past, Present, and a Proposed Future. The Journal of Navigation **71**(3), 513–529 (May 2018). https://doi.org/10.1017/S0373463317000911
66. Tiberius, C., Janssen, G., Koelemeij, J., Dierikx, E., Diouf, C., Dun, H.: Decimeter positioning in an urban environment through a scalable optical-wireless

network. NAVIGATION: Journal of the Institute of Navigation **70**(3) (2023). https://doi.org/10.33012/navi.589, https://navi.ion.org/content/70/3/navi.589

67. USA-PNT-ABS: Protect, toughen, and augment: Global positioning system for users (Sep 2018)
68. Xue D., Y.J., Z., L.: Potential impact of gnss positioning errors on the satellite-navigation-based air traffic management. Space Weather **20** (2022). https://doi.org/https://doi.org/10.1029/2022SW003144
69. Zhang, H., Peng, S., Liu, L., Su, S., Cao, Y.: Review on gps spoofing-based time synchronisation attack on power system. IET Generation, Transmission & Distribution **14**(20), 4301–4309 (2020). https://doi.org/https://doi.org/10.1049/iet-gtd.2020.0253, https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-gtd.2020.0253