REASON – Resilience and Security of Geospatial Data for Critical Infrastructures

Sanna Kaasalainen[a], Maija Mäkelä[a], Laura Ruotsalainen[b], Titti Malmivirta[b], Thomas Fordell[c], Kalle Hanhijärvi[c], Anders Wallin[c], Thomas Lindvall[c], Sergey Nikolskiy[a,b], Martta-Kaisa Olkkonen[a], Jesperi Rantanen[a], Sonja Lahtinen[a], M. Zahidul H. Bhuiyan[a] and Hannu Koivula[a]

[a] *Finnish Geospatial Research Institute, Geodeetinrinne 2, 02430 Masala, Finland*
[b] *University of Helsinki, Pietari Kalmin katu 5, 00560 Helsinki, Finland*
[c] *VTT Technical Research Centre of Finland Ltd, National Metrology Institute VTT MIKES, Tekniikantie 1, Espoo, FI-02044 VTT, Finland*

Abstract

Critical infrastructures are becoming increasingly dependent on accurate and continuous position, navigation, and timing (PNT) services provided by Global Navigation Satellite Systems (GNSS). PNT services are critical for, e.g., stock market, electricity transmission, banking and security information systems, building industry, logistics and transport (maritime and road transport as well as aviation), wireless communications, and rescue services. These critical services will not be available or they will need to rely on backup services if GNSS signals are unavailable in the area. This makes these services vulnerable when it comes to disruption in GNSS signals as a result of natural or intentional interference, or occurrence of unexpected GNSS constellation level problems. This calls for continuous monitoring of the GNSS signal quality so that any anomalies can be detected, isolated, and reported to authorities and a seamless shift to back-up solutions can be made.

This study aims at improving the security of supply of the services that rely on GNSS-enabled PNT by the use of emerging Machine Learning methods (such as Deep Learning) for improved situational awareness in GNSS throughout Finland. The study is based on a GNSS-Finland monitoring platform, which uses the permanent GNSS reference network in Finland (FinnRef) to detect and localize the disruptions in the GNSS signals. Using the big data available from GNSS-Finland, Deep Learning (DL) methods will be developed to investigate possible trends in signal quality, and to detect or predict signal anomalies. This will provide an assessment of the continuity and forecast of critical failures in positioning and timing information and thus improve the resilience of critical PNT-dependent services and operations in Finland. For the improved resilience of timing services, we also aim to explore solutions for cost-effective, fibre-optic time transfer to a large number of geographical locations as well as develop software-defined-radio-based technologies for monitoring low-frequency timing signals and other signals of opportunity. As a future effort, case studies in critical locations are planned in collaboration with end users, both for monitoring the GNSS signal quality and to explore the potential of using back-up timing services.

Keywords

Resilience, Security, GNSS, Timing

ICL-GNSS 2021 WiP Proceedings, June 01–03, 2021, Tampere, Finland
EMAIL: maija.makela@nls.fi (M. Mäkelä); laura.ruotsalainen@helsinki.fi (L. Ruotsalainen); thomas.fordell@vtt.fi (T. Fordell); sergey.nikolskiy@helsinki.fi (S. Nikolskiy); martta-kaisa.olkkonen@nls.fi (M. Olkkonen)
ORCID: 0000-0002-2900-6655 (M. Mäkelä); 0000-0002-4057-4143 (L. Ruotsalainen); 0000-0002-9195-2984 (T. Fordell); 0000-0002-3068-5392 (K. Hanhijärvi); 0000-0002-7947-2021 (A. Wallin); 0000-0002-4076-6815 (T. Lindvall); 0000-0003-0410-626X (S. Nikolskiy); 0000-0002-5302-081X (M. Olkkonen); 0000-0002-3801-1018 (M.Z.H. Bhuiyan)

1. Introduction

Critical infrastructures are in the core of security of supply, as their failure will seriously affect national security, economic security, and public health and safety. There is an increasing number of infrastructures and services for which accurate Position, Navigation, and Time (PNT) information from GNSS is crucial [1, 2]. These include banking transactions, stock markets, telecommunications, and electricity transmission systems, which require accurate timing for synchronization. Accurate and reliable positioning is needed in rescue operations, building sites, aviation, and logistics. These operations also need to build and maintain situational awareness, which is not possible without reliable and accurate location or time information. The fact that critical services rely on GNSS renders these services vulnerable to disruptions and interference [3, 4]. The disruption in GNSS will result in unavailability of these services in the area, which means that GNSS itself is considered a critical infrastructure and gets regulated and monitored by authorities [5].

Position from GNSS is calculated from the time of arrival, which causes GNSS also to provide precise timing. Each satellite is synchronized to the system time scale of the respective constellation, which is traceable to different UTC(k) realizations. The system time scales are often related to each other: there are conversion parameters between Galileo and GPS system times available from Galileo. If there is a failure in either in the ranging signals or the conversion parameters, there will be a disruption in time-critical systems. Such an incident took place in 2016 [3], when Global Positioning System (GPS) satellites were broadcasting erroneous time correction parameters, causing problems in, for example, digital radio broadcasts in the United Kingdom.

In this Work-in-Progress paper we present the REASON project, which is a joint effort of the Finnish Geospatial Research Institute (FGI), University of Helsinki and the National Metrology Institute VTT MIKES. We explore the potential of Machine Learning methods (such as Deep Learning) for GNSS in providing GNSS situational awareness from GNSS signal data. We also discuss the technologies and related research that will likely enable Finland to improve crisis preparedness and security of supply in terms of robust location and time information. We will introduce the FinnRef network and the GNSS-Finland service, look at the research related to machine learning methods in GNSS fault detection and diagnosis (FDD), and explore alternatives to GNSS-based timing. We describe the results and outcomes we expect to get in the REASON project, and the impact it will have on the end users in terms of improved cyber security, situational awareness, and critical operations. The specific research objectives in REASON are:

- To study the potential of Artificial Intelligence (AI) methods and Big Data in GNSS situational awareness.
- To develop AI methods for GNSS disturbance detection and localization, including both intentional and unintentional interference.
- To develop alternatives to GNSS-based time dissemination on a large scale in a cost-effective manner.

In Section 2 we describe the FinnRef monitoring network and the GNSS-Finland Service. Section 3 discusses machine learning approaches in GNSS FDD. Section 4 covers the alternatives to GNSS-based time. Section 5 discusses the outcomes we expect to obtain in this project and Section 6 concludes this study.

2. FinnRef and GNSS-Finland Service

The FinnRef network consists of 47 continuously operating GNSS stations. It works as a fundamental geodetic infrastructure that is used for the needs of the national reference frames and for positioning related services. The stations are equipped with GNSS antennas and receivers that enable tracking of all satellites and signals available.

One of the purposes of the FinnRef network is providing data for DGNSS and RTK positioning. This data is offered as real-time streams transmitting RTCM messages of various types. A subset of those messages, namely signal observations, ephemerides and positions computed at reference stations, allows continuous monitoring of GNSS performance at each station. Since GNSS is utilized in almost all industries while being vulnerable to disruptions on both local and system level, the need for such monitoring has increased. Furthermore, open access to this information is important to allow all users utilizing PNT to conduct their work more effectively. In the years 2020-2021, a monitoring system called GNSS-Finland Service was created and made publicly available [6]. This work was carried out in the scope of the project GNSS-Finland Service funded by Ministry of Transport and Communications of Finland and Finnish Transport and Communications agency (Traficom) [7]. Figure 1 shows the main view of the service presenting reference stations along with signal status information.

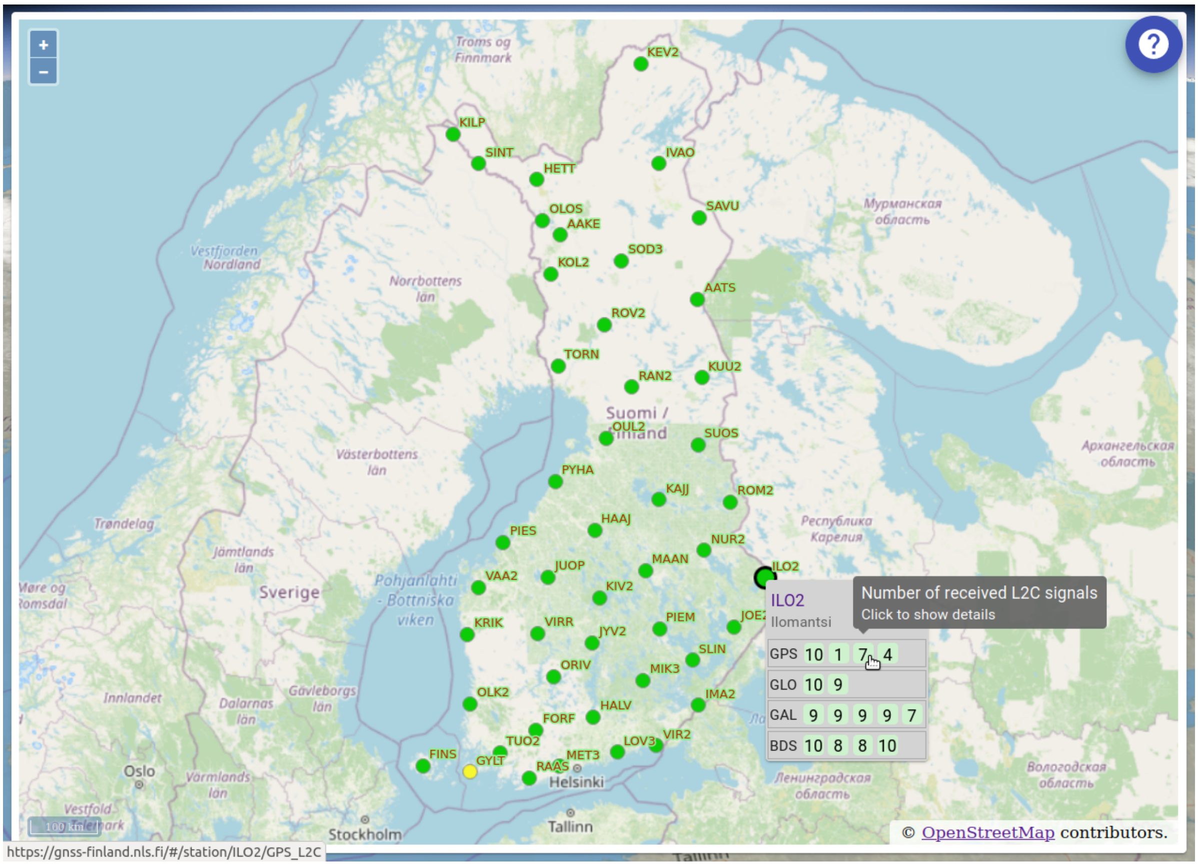

Figure 1: GNSS-Finland Service, available at https://gnss-finland.nls.fi/#/map.

The service monitors the following key performance indicators:

- strength of GNSS signals based on Carrier-to-Noise density Ratio (CNR),
- health status of satellites based on parameters transmitted in ephemerides,
- position deviation relative to the known station position.

This information is presented in user interfaces and also served via an API for third-party software. A set of analysis tools have been implemented to detect predefined anomalies such as interference, abnormal position bias and significant changes in satellites' health status. In case of detection of these events, a notification with detailed information is sent to authorized users.

The service is made scalable in different ways. Since it uses standard RTCM messages as input data, other reference stations or networks can be seamlessly added in the loop. Besides, it has modular open architecture which allows connecting new analysis tools.

During the development and exploitation of the service, a number of phenomena has been observed including interference events at different stations and impacts of high geomagnetic activity on GNSS signals.

3. Fault Detection and Diagnostics in GNSS

Fault Detection and Diagnosis (FDD) means the process of detecting errors in the system and identifying their sources. In this section different FDD methods for interference and GNSS system level fault situations are discussed, with an emphasis on approaches utilizing machine learning techniques. Effective detection and mitigation of different GNSS fault situations improves the resilience of critical services depending on GNSS.

3.1. Interference Detection and Mitigation

Interference, especially deliberately generated, can seriously compromise operations of critical infrastructures and services relying on GNSS. Interference sources for GNSS signals can be classified into unintentional or deliberate sources. Intentional interference can be further classified into jamming or spoofing and their effect on the signal depends on the specific equipment and methods used. Unintentional interference may be caused by multipath propagation, atmospheric disturbances or radio transmitters operating at the same signal frequency bands as GNSS. Different interference types deteriorate the signal with varying ways and extent, and thereby their mitigation methods also differ. Therefore, it is essential to use FDD for detecting when the signal is disrupted and what is causing the disruption.

3.1.1. Position domain

Traditionally, GNSS FDD has been implemented using conventional signal processing methods, such as Fast Fourier Transform based methods [8] or wavelet decomposition [9]. Unfortunately, such methods as well as corresponding time domain processing methods [10] tend to unintentionally rule out other data sources of interest. At present, Machine Learning (ML) is actively used for analysing radio signals. Research has been mainly concentrating in the detection domain and the occurrence of interference from a pre-defined source has been searched for.

Hsu [11] used Support Vector Machines (SVMs) for classifying the signal into clean, multipath and non-line-of-sight (NLOS) in static scenarios. Semanjski et al [12] used SVMs for spoofing detection, and found out that the separation among manipulated and authentic signals is altogether a complex task that is difficult to be implemented using traditional ML methods. The power of Deep Learning (DL) over such conventional supervised ML methods is in its character of automatically finding the relevant signal features to be used in inference. Therefore, the ML research in the signal domain has shifted into developing DL based methods.

When it is known that a jammer is present, the jammer type (Amplitude Modulated, chirp, narrow-band, etc) may be classified using ML. Ferre et al. [13] converted the signal into spectrogram images and used a Convolutional Neural Network (CNN) for detecting the presence of jamming and the jammer type with good results. Multipath detection has also been improved using CNNs. Munin et al. [14] developed a CNN based method and tested it using simulated scenarios with good results. Cross Ambiguity Function evaluated at the delay/Doppler grid can be considered as an image and fed into CNN for spoofing detection with promising performance [15]. However, CNNs were initially developed for image processing and thereby they are able to process the spatial dimension of the data, but not the temporal one. However, the temporal dimension brings valuable information for the detection of signal abnormalities and is therefore essential to be exploited as well for the best performance.

Two types of DL models, non-recurrent models based on delay elements in the feedforward direction and recurrent models with delayed feedback can do the time inclusion. Time-Delayed Neural Networks (TDNN) belong to the first type. They are one-dimensional convolutional networks applied to time series. TDNNs have been used for implementing Receiver Autonomous Integrity Monitoring (RAIM) for detecting anomalous events in GNSS, such as receiver clock bias jumps or ephemeris errors [16]. Long Short Term Memory (LSTM) methods are recurrent models and capable for learning long-term dependencies in the data. They have proved to provide superior performance for addressing the temporal dimension, however they are more complex to train and build than TDNNs. Previously, LSTM based methods have been developed for GNSS spoofing detection [17] and for implementing RAIM for static positioning scenarios [18]. In our research, we will address GNSS FDD for real-life positioning. Detection of signal anomalies requires a system that is able to remember information for long periods of time, namely what kind of changes is the signal experiencing over time. Therefore, we will develop a LSTM based anomaly detector that is able to identify the interference source and predict the system failure well in advance for initiating the process for mitigation.

3.1.2. Time domain

Methods for FDD in position solution described above largely apply also to time solutions. While interference to the signal compromises both position and time solution, the time component can be specifically spoofed, which affects the operation of many critical infrastructures dependent on accurate timing [19, 20, 21].

Methods have been developed to find interfered time solutions in for example [22] and [23] where the authors also mitigate the affected solution. In [23] authors base their solution to robust estimation method which can effectively correct the spoofed time solution for stationary device while it requires only low memory and does not require tuning of parameters to specific attacks.

Using a ML approach, in [24] multi-layer perceptron neural network is implemented to detect time synchronization attacks and correct the spoofed time solution. The authors show that the neural network based solution is better than the algorithmic methods they are comparing and still requires only little memory or computational power from the device.

3.2. System Level Fault Detection and Mitigation

In absence of interference, faults in GNSS may occur also due to problems on navigation satellites and the orbit and clock parameters they are transmitting. Despite of the health parameters transmitted by the navigation satellites, problems affecting the GNSS on a large scale are not always easily observed by a single navigation receiver without additional measures. Applying FDD also to issues rising from the navigation satellite system makes critical operations less vulnerable in such situations.

On receiver side, conventional solutions to GNSS system level FDD include Receiver Autonomous Integrity Monitoring (RAIM) and information transmitted by Satellite Based Augmentation Systems (SBAS), in addition to simply utilizing the health information in the satellite broadcast data. However, also SBAS might be experiencing problems and thus be unaware of the ephemeris being faulty, and the satellite health information can be outdated. This situation may happen, for example, due to unannounced satellite maneuvers or GNSS ground segment uploading faulty ephemeris parameters.

Regarding conventional GNSS timing integrity monitoring approaches, key timing performance indicators are defined in [25] in terms of timing accuracy and frequency stability, as well as integrity and availability. Utilizing Timing RAIM (T-RAIM) is shown to detect faulty observations, and it enables a timing receiver to achieve sufficient performance even with a low cost oscillator. In [26] timing performance is tested under threat conditions such as jamming and spoofing, erroneous navigation messages and ionospheric errors. Approaches such as utilizing a Kalman filter on oscillator during GNSS holdover triggered by detection of spoofing or jamming, utilizing EGNOS transmissions to exclude faulty satellites, crosschecking solution between constellations and utilizing dual frequency measurements are shown to help mitigating the effect of different threats on GNSS timing performance.

In the context of GNSS monitoring networks, such as FinnRef, erroneous ephemerides can be detected combining measurements made by several monitoring stations. For instance, a test statistic for single satellite ephemeris health has been developed based on the difference of true distance between two monitoring stations and a computed distance based on the ephemeris to be evaluated, pseudorange measurements, station locations and law of cosines [27]. A test statistic based on double difference carrier phase observations has been developed in [28]. In case of short baseline between monitoring stations, the statistic in normal conditions has a normal distribution with zero mean, whereas faulty ephemeris will result in distribution with non-zero mean [28]. Test statistic based on carrier phase is more sensitive to ephemeris faults compared to code measurements, but requires ambiguity resolution.

Considering navigation satellite clock anomaly detection, for example consecutive carrier phase observations can be used to eliminate phase ambiguity and to obtain time-differenced phase offset between the satellite and a receiver connected to a hydrogen maser clock [29]. In this work comparison of Kalman filter predictions and actual observations of clock phase and frequency offset are used to develop two test statistics for fault detection.

Several publications discuss ML in improving and predicting navigation satellite ephemeris information as well as satellite clock offset information. Following the idea of comparing expected and obtained parameters utilized in existing GNSS FDD approaches, these ML methods can likely be utilized also for FDD purposes. Comparison of predicted and actual parameters, regardless of the prediction method, should enable detection of at least abrupt fault situations.

For example, satellite orbits and clocks can be predicted forward in time for duration of several days using a Kalman filter approach [30]. The objective in this work is to reduce the

Time to First Fix in standalone navigation receivers without assisted GNSS. The presented approach has been refined in several following articles such as [31, 32, 33]. CNNs can be utilized to estimate and correct the residual radial, tangential and normal errors in Kalman filter orbit predictions, that occur due to for example some unmodeled forces affecting the satellites [34]. Image-like input for the CNN is generated based on difference between the predicted satellite positions and position based on the broadcast ephemeris. Combining the Kalman filter prediction and CNN correction, the 95% error quantile of Signal in Space Range Error (SISRE) is less than 8 m even for prediction duration of one week for GPS satellites.

A Least Squares SVM (LSSVM) can be utilized to predict clock offset based on broadcast ephemeris data, among other approaches [35]. In this work, for prediction duration of one week for GPS satellites, the LSSVM clock offset prediction differs from broadcast ephemeris for equivalent of less than 5 m 68% of the time. This is more than 55% improvement compared to extrapolating clock correction in old ephemeris. However, it should be noted that for example a Kalman filter approach for prediction performs better than LSSVM for many of the satellites discussed in the paper. Also, in [36] a RNN-style NARX neural network is used to predict satellite clock offset up to 24 hours based on precise satellite clock bias (SCB) obtained from International GNSS Service (IGS). The RMS prediction error in that case is less than 0.5 ns on average. In [37] a LSTM is used to predict the single difference SCB values based on precise IGS clock products for up to three days. LSTM model results in less than 1.6 ns RMS prediction error, and also has the lowest time complexity compared to the alternatives discussed.

Comparing the ephemeris and clock information to the corresponding predictions it will be possible to detect system level problems on orbit and clock information. Furthermore, the predictions could be used instead of broadcast data in fault situations, and help in the case of harsh signal conditions, such as jamming, where the broadcast data demodulation might not be possible. This type of approach might also be useful in detecting record and replay type spoofing attacks, in which case there would likely be a difference between the predicted and received ephemeris.

4. Robust Backup for GNSS-based Timing Methods

Many critical infrastructures rely especially on accurate GNSS-based time, and are thus vulnerable to any problems in GNSS signals. For this reason, in this work we will study also alternative methods for accurate and cost effective time dissemination on a large scale. The potential approaches are discussed in this section. Utilizing one of these alternatives will reduce the reliance of critical facilities to GNSS-based time, and thus prevent potentially catastrophic consequences in case of failure of GNSS.

The most accurate long-distance time and frequency transfer is done using point-to-point fibre-optic links [38, 39, 40, 41]. As long as the third parties do not have knowledge of the fibre route or access to it, fibre-optic links are also highly secure, since jamming and spoofing from the outside is very difficult, if not impossible. The downsides of fibre links are that not only are they costly but the number of geographical locations that can be reached is very limited due to the limited channel capacity of telecom networks. Thus, one of the objectives of this work is to develop techniques for sending timing signals through the telecom fibre network to a large number of distant endpoints.

The starting point for this is to use the direct sequence spread spectrum (DSSS) technique, similar to what is used in GNSS [42] and in Two-Way Satellite Time and Frequency Transfer (TWSTFT) [43, 44], to realize code-division multiple access (CDMA) on a single telecom channel [45]. Here the difference to GNSS is that each receiver sends a signal back to the transmitter, which is then used to calculate the two-way optical path delay based on the unique codes of each receiver. The measured delay is communicated to the receivers as their clock offset or the timing signal sent out is pre-compensated.

The spread spectrum signal is generated by modulating the carrier phase by a unique and known pseudorandom noise (PRN) bit sequence. The received signal is cross correlated with the known bit sequence allowing for reception with low signal-to-noise ratio. As is evident from the Shannon and Hartley channel-capacity theorem, lowering of the signal to noise ratio can be compensated by increasing transmitted bandwidth [46]. The spread spectrum technique allows for additional process gain by averaging the received signal. Large signal attenuation can be tolerated, which, in turn, should enable time transfer far outside the normal telecom communication bands, enabling a geographically dense fibre-optic time transfer network.

In addition to GNSS and fibre-optic time transfer, low-frequency (LF) transmitters are also operated by several countries. The most prominent examples in Europe are DCF77 in Mainflingen, Germany, operating at 77.5 kHz [47, 48] and the Time from NPL, also known as MSF, operating at 60 kHz from Anthorn, UK [49]. LF signals have large coverage and can be received with low-cost hardware. DCF77 even employs spread-spectrum signal processing, as part of the signal is phase modulated by a PRN sequence [48]. LF signals provide only one-way communication, and the timing signals suffer from diurnal variation in signal strength and delay, especially for the ionosphere-reflected sky wave [50]. Due to bandwidth limitations in the LF band, timing accuracy and stability are inferior to GNSS [50]. Nevertheless, they provide a potential backup for timing especially if their signal quality and time deviations can be monitored.

In addition to traditional over-the-air timing signals, also the use of Signals of Opportunity (SoOp) together with a software-defined radio (SDR) will be addressed for timing purposes. SDR receiver can be used to collect opportunistic non-GNSS short-range signals. These signals can be acquired from many sources combining radio frequency signals that are available in the infrastructure, such as long-term evolution, digital television, cellular, AM/FM radio signals or WiFi networks and Bluetooth [51]. Other short-range radio links can be introduced by demand, like hand-held ultra-wide band (UWB) transceivers. In long-haul telecommunications, separate fibers are used for the up- and down-streams. Utilizing SoOp at both ends of fiber links, the error of open-air signals can be quantified.

SDR was envisioned as a new wireless standard approximately 15 years ago, but the advent of SDR has posed new challenges in design, power consumption and standards production. Due to its complexity and aforementioned challenges, it is by no means suitable for all possible situations. Promisingly however, it was recently proposed as error mitigation in coordinated universal time (UTC) determination. The observed variation of diurnal patterns in the generation of UTC with TWSTFT can be as high as 2 ns [52]. According to their hypothesis, the contributor in diurnals could be related to the satellite time and ranging equipment (SATRE) modem. Therefore, they suggest replacing the receive modems with SDR to reduce noise. Ref. [53] demonstrated the ability to use a hybrid waveform combining GNSS and SoOp in varying situations, both in free space and indoor navigation. For this purpose, they introduced Advanced Software Radio (ASR) platform designed for portable solutions like unmanned aerial navigation (drone) or robust surface navigation (rover).

Currently, traceability to international Coordinated Universal time (UTC) is provided via the continuous key comparison "CCTF-K001.UTC" between National Metrology Institutes (NMIs) or Designated Institutes (DIs) of Member States of the International Bureau of Weights and Measures (BIPM), or laboratories associate of the General Conference on Weights and Measures (CGPM). In practice, time is compared either via dedicated TWSTFT [43] or GNSS precise-point positioning [54]. Local UTC(k) time-scales are typically created by correcting the frequency of a free-running atomic clock (e.g. a hydrogen maser) using a fine-grained frequency synthesizer (named micro-stepper or micro-phase stepper). Active hydrogen masers under stable environmental conditions (temperature, humidity) typically show linear frequency drift of 10^{-16} to 10^{-15} per day, which must be corrected using the micro-stepper continuously. SDRs can be used to accurately measure the phase difference between multiple local clocks [55, 56]. Phase and frequency difference measurements act as inputs to a clock-ensemble algorithm where the frequency of each free-running clock is modelled using e.g. a Kalman filter approach. An open hardware micro-stepper is being developed by VTT MIKES [57].

Accurate absolute frequencies for the free-running clocks in a maser ensemble or a clock network can be provided via frequency comparison to a primary or secondary frequency standard realizing a frequency traceable to the definition of the International System of Units (SI) second with a known uncertainty. VTT MIKES is developing an optical clock based on an electric quadrupole transition in the $^{88}Sr^{+}$ ion, a secondary representation of the SI second. Characterization of the systematic frequency shifts caused by, e.g., blackbody radiation, is currently ongoing. An initial evaluation of the uncertainty budget is planned for 2021.

Optical clocks do not yet operate continuously and are thus not directly used to generate time scales, only to steer the local oscillator that generates the time scale. Simulations show that by operating an optical clock, e.g., 6 h three times per week or 12 h once a week, one can achieve a performance similar to that of a continuously-operating Cs fountain [58]. A higher optical-clock uptime ratio of 46% has been shown to lead to superior stability compared to a Cs-based time scale [59]. In a pioneering experiment, a time scale was steered by an optical clock operating 10^4 s per week for 6 months, leading to sub-ns agreement with Terrestrial Time (TT) after five months [60]. A low optical-clock availability sets stringent requirements on the maser. This can be addressed by replacing the maser by a clock ensemble [61].

Another important application of optical clocks is to contribute to International Atomic Time (TAI). This is done by comparing the optical clock with a hydrogen maser contributing to TAI and submitting the data to BIPM for evaluation and inclusion in Circular T. So far only a few optical clocks have been reported to BIPM.

5. Anticipated Results

In this work machine learning and especially deep learning methods will be developed in order to enhance GNSS situational awareness. We will utilize the big data available from GNSS-Finland and FinnRef monitoring network, described in Section 2, to generate novel insights into GNSS status. Using a network of receivers together with ML methods will likely enable detection of signal phenomena invisible to a single receiver. Furthermore, we will develop a robust alternative to GNSS-based timing methods in order to improve resilience in critical infrastructures requiring precise timing. The REASON project objectives are illustrated in Figure 2. The specific research questions we want to answer are:

1. Based on both current and historical data patterns, is it possible to use AI/ML approaches to predict satellite navigation signal unavailability or failure?

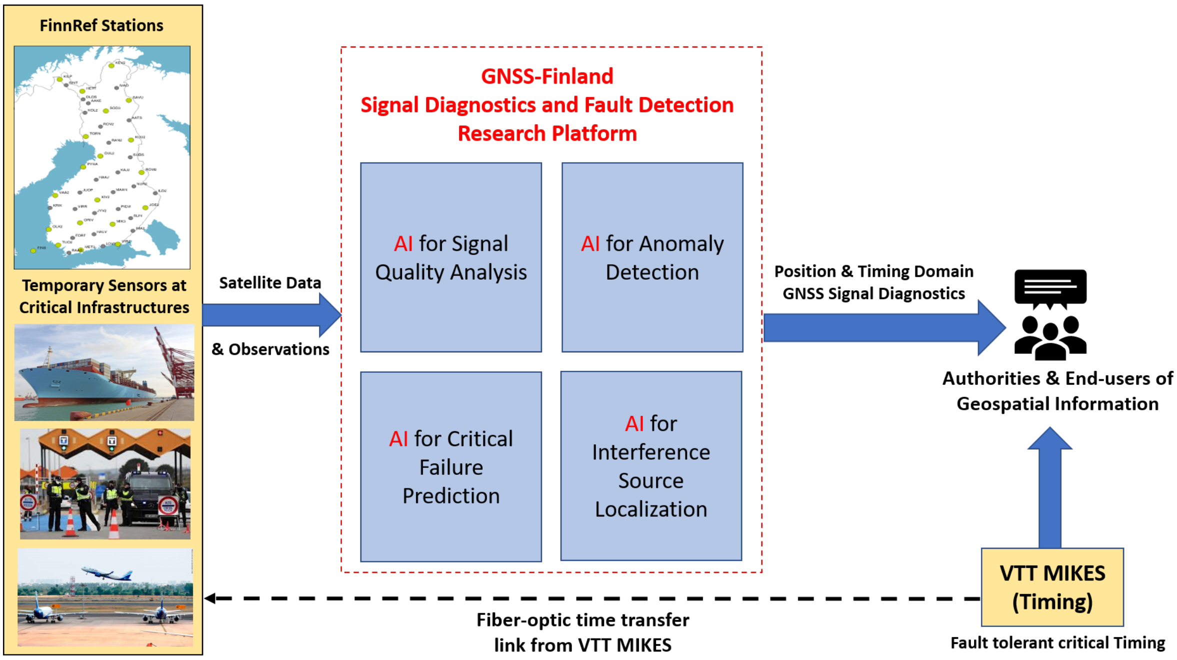

Figure 2: Illustration of REASON objectives

2. How to use AI/ML techniques to localize intentional interference to satellite navigation signals?
3. In case of catastrophic failure of GNSS, what back-up solutions can be developed especially for accurate timing dissemination, and within what timeframe these can be implemented?
4. How to distribute reliable and accurate time independent of GNSS in a cost-effective manner to numerous and distant geographical locations?

Section 3 discusses existing research and potential machine learning approaches related to questions 1. and 2. To be more specific, both interference and system level faults will be addressed for both position and time domain in development of novel DL approaches for FDD.

DL methods will be developed and applied to detect and mitigate GNSS fault situations in a comprehensive manner. So far GNSS FDD methods have been developed for detecting incidences caused by certain interference sources. As far as we know, this will be the first comprehensive solution capable to detect and identify all interference types using deep learning on a nationwide scale. Furthermore, using machine learning to detect distortions in timing signals will be one of the first contributions to this end.

The different deep learning techniques are expected to be more sensitive in detection of signal anomalies and other phenomena, thus lowering detection threshold compared to current approaches. Furthermore, in this project we will move from monitoring signal quality and detecting anomalies to prediction of future problems in navigation signals.

In Section 4 possible alternatives to GNSS-based time are introduced regarding research questions 3. and 4. We expect to find cost effective ways of sending timing signals through the fiber optic networks to a large number of distant endpoints and to develop software defined radio approaches for monitoring low-frequency, open-air broadcasts and other signals of opportunity for timing purposes.

The approaches developed will enable GNSS situational awareness throughout Finland. Accurate and timely information of GNSS status will enable end users and critical infrastructures to safely utilize GNSS, knowing when they can trust the signal quality. In case of interference or fault situations, end users will be warned as fast as possible or even ahead of time, so they can switch to alternative means of PNT. The users requiring accurate timing information will have a robust alternative to GNSS time.

6. Conclusion

This Work-in-Progress paper provides a first-hand overview on the usage and challenges related to positioning and timing among a wide group of end users in different branches such as security, finance, power and construction industries, rescue services, transport, and cyber security. Our end user has indicated that a holistic understanding of the timing services is missing. In this work the anticipated results of the REASON project have been discussed, as the research is still ongoing.

The methods that will be developed in this work will improve detection and mitigation of anomalies in GNSS at both receiver level and system level. This study presents the state-of-the-art ML based GNSS anomaly detection methods and outlines plans for developing a novel LSTM based method capable to detect and identify all GNSS interference types from the signal. We have discussed potential approaches to ML usage especially in improving GNSS timing security, and have presented alternatives to GNSS-based time dissemination.

When complete, our results will enhance cyber security, situational awareness, and safety in critical operations.

Acknowledgments

This work has been funded by the Academy of Finland.

References

[1] 'Resilient PNT for Critical Infrastructure, 2020. URL: https://www.dhs.gov/sites/default/files/publications/resilient_pnt_for_critical_infrastructure_fact_sheet_508.pdf.
[2] Timing, 2019. URL: https://www.gps.gov/applications/timing/.
[3] A. Mujunen, J. Aatrokoski, M. Tornikoski, J. Tammi, GPS Time Disruptions on 26-Jan-2016, Technical Report, 2016. URL: http://urn.fi/URN:ISBN:978-952-60-6703-2.
[4] A. Morrison, N. Sokolova, J. E. Håkegård, T. H. Bryne, L. Ruotsalainen, A Multi-Site Quad-Band Radio Frequency Interference Monitoring Alerting and Reporting System, in: 2020 European Navigation Conference (ENC), IEEE, 2020, pp. 1–10.
[5] YLE: ANS Finland issued a warning to air traffic due to GPS disturbances in Lapland, 2018. URL: https://www.helsinkitimes.fi/finland/finland-news/domestic/15944-yle-ans-finland-issued-a-warning-to-air-traffic-due-to-gps-disturbances-in-lapland.html.
[6] GNSS-Finland Service, 2021. URL: https://gnss-finland.nls.fi/.
[7] GNSS-Finland Service project at National Land Survey of Finland, 2020. URL: https://www.maanmittauslaitos.fi/en/research/gnss-finland-service.

[8] Y. Zhang, C. Bartone, Multipath mitigation in the frequency domain, in: Proceedings of the ION PLANS (IEEE Cat. No.04CH37556), 2004, pp. 486—-495.

[9] M. Elhabiby, A. El-Ghazouly, N. El-Sheimy, A new wavelet based multipath mitigation technique, in: Proceedings of the ION GNSS, volume 2, 2008, pp. 625—-631.

[10] P. Y. Hwang, G. A. Mcgraw, J. R. Bader, Enhanced differential GPS carrier smoothed code processing using dual frequency measurements, Navigation (1999).

[11] L.-T. Hsu, GNSS multipath detection using a machine learning approach, in: 2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC), IEEE, 2017, pp. 1–6.

[12] S. Semanjski, I. Semanjski, W. D. Wilde, A. Muls, Use of Supervised Machine Learning for GNSS Signal Spoofing Detection with Validation on Real-World Meaconing and Spoofing Data—Part i, Sensors (2020).

[13] R. Morales Ferre, A. de la Fuente, E. S. Lohan, Jammer classification in GNSS bands via machine learning algorithms, Sensors 19 (2019) 4841.

[14] E. Munin, A. Blais, N. Couellan, Convolutional neural network for multipath detection in GNSS receivers, in: 2020 International Conference on Artificial Intelligence and Data Analytics for Air Transportation (AIDA-AT), IEEE, 2020, pp. 1–10.

[15] P. Borhani-Darian, H. Li, P. Wu, P. Closas, Deep Neural Network approach to detect GNSS Spoofing Attacks, in: Proceedings of International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2020), 2020.

[16] D. Kim, J. Cho, Improvement of Anomalous Behavior Detection of GNSS Signal Based on TDNN for Augmentation Systems, Sensors 18 (2018) 3800.

[17] R. Calvo-Palomino, A. Bhattacharya, G. Bovet, D. Giustiniano, Short: LSTM-based GNSS Spoofing Detection Using Low-cost Spectrum Sensors, in: Proceedings of the IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks, 2020, pp. 273–276.

[18] Y. Sun, RAIM-NET: A Deep Neural Network for Receiver Autonomous Integrity Monitoring, Remote Sensing 12 (2020) 1503. doi:10.3390/rs12091503.

[19] D. P. Shepard, T. E. Humphreys, A. A. Fansler, Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks, International Journal of Critical Infrastructure Protection 5 (2012) 146–153.

[20] B. Moussa, M. Debbabi, C. Assi, Security assessment of time synchronization mechanisms for the smart grid, IEEE Communications Surveys & Tutorials 18 (2016) 1952–1973.

[21] D.-Y. Yu, A. Ranganathan, T. Locher, S. Capkun, D. Basin, Short paper: Detection of GPS spoofing attacks in power grids, in: Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks, 2014, pp. 99–104.

[22] A. Khalajmehrabadi, N. Gatsis, D. Akopian, A. F. Taha, Real-time rejection and mitigation of time synchronization attacks on the global positioning system, IEEE Transactions on Industrial Electronics 65 (2018) 6425–6435.

[23] J. Lee, A. F. Taha, N. Gatsis, D. Akopian, Tuning-free, low memory robust estimator to mitigate GPS spoofing attacks, IEEE control systems letters 4 (2019) 145–150.

[24] N. Orouji, M. Mosavi, A multi-layer perceptron neural network to mitigate the interference of time synchronization attacks in stationary GPS receivers, GPS Solutions 25 (2021) 1–15.

[25] M. Kirkko-Jaakkola, S. Thombre, S. Honkala, S. Söderholm, S. Kaasalainen, H. Kuusniemi, H. Zelle, H. Veerman, A. Wallin, Evaluating the robustness of EGNSS based timing services, Institute of Electrical and Electronics Engineers, 2017.

[26] S. Honkala, S. Thombre, M. Kirkko-Jaakkola, H. Zelle, H. Veerman, A. E. Wallin, E. F. Dierikx, S. Kaasalainen, S. Söderholm, H. Kuusniemi, Performance of EGNSS-Based Timing in Various Threat Conditions, IEEE Transactions on Instrumentation and Measurement 69 (2019) 2287–2299.

[27] J. Ahn, Y. J. Lee, D. H. Won, H.-S. Jun, C. Yeom, S. Sung, J.-O. Lee, Orbit Ephemeris Failure Detection in a GNSS Regional Application, International Journal of Aeronautical and Space Sciences 16 (2015) 89–101.

[28] L. Li, X. Liu, C. Jia, C. Cheng, J. Li, L. Zhao, Integrity monitoring of carrier phase-based ephemeris fault detection, GPS Solutions 24 (2020) 1–13.

[29] S.-W. Lee, J. Kim, Y. J. Lee, Protecting signal integrity against atomic clock anomalies on board GNSS satellites, IEEE Transactions on Instrumentation and Measurement 60 (2011) 2738–2745.

[30] M. Seppänen, J. Ala-Luhtala, R. Piché, S. Martikainen, S. Ali-Löytty, Autonomous prediction of GPS and GLONASS satellite orbits, NAVIGATION, Journal of the Institute of Navigation 59 (2012) 119–134.

[31] A. Pukkila, J. Ala-Luhtala, R. Piché, S. Ali-Löytty, GNSS orbit prediction with enhanced force model, in: 2015 International Conference on Localization and GNSS (ICL-GNSS), IEEE, 2015, pp. 1–6.

[32] H. Leppäkoski, S. Rautalin, X. Zhang, S. Ali-Löytty, R. Piché, Extended prediction of QZSS orbit and clock, in: 2016 International Conference on Localization and GNSS (ICL-GNSS), IEEE, 2016, pp. 1–7.

[33] S. Rautalin, S. Ali-Löytty, R. Piché, Latent force models in autonomous GNSS satellite orbit prediction, in: 2017 International Conference on Localization and GNSS (ICL-GNSS), IEEE, 2017, pp. 1–6.

[34] J. Pihlajasalo, H. Leppäkoski, S. Ali-Löytty, R. Piché, Improvement of GPS and BeiDou extended orbit predictions with CNNs, in: 2018 European Navigation Conference (ENC), IEEE, 2018, pp. 54–59.

[35] J. Pihlajasalo, H. Leppäkoski, S. Kuismanen, S. Ali-Löytty, R. Piché, Methods for Long-Term GNSS Clock Offset Prediction, in: 2019 International Conference on Localization and GNSS (ICL-GNSS), IEEE, 2019, pp. 1–6.

[36] Y. Liang, J. Xu, F. Li, P. Jiang, Nonlinear Autoregressive Model with Exogenous Input Recurrent Neural Network to Predict Satellites' Clock Bias, IEEE Access 9 (2021) 24416–24424.

[37] B. Huang, Z. Ji, R. Zhai, C. Xiao, F. Yang, B. Yang, Y. Wang, Clock bias prediction algorithm for navigation satellites based on a supervised learning long short-term memory neural network, GPS Solutions 25 (2021) 1–16.

[38] Ł. Śliwczyński, P. Krehlik, A. Czubla, Ł. Buczek, M. Lipiński, Dissemination of time and RF frequency via a stabilized fibre optic link over a distance of 420 km, Metrologia 50 (2013) 133. URL: https://iopscience.iop.org/article/10.1088/0026-1394/50/2/133. doi:10.1088/0026-1394/50/2/133.

[39] A. Bercy, F. Stefani, O. Lopez, C. Chardonnet, P.-E. Pottie, A. Amy-Klein, Two-way optical frequency comparisons at 5×10^{-21} relative stability over 100-km telecommunication network fibers, Phys. Rev. A 90 (2014) 061802. URL: https://link.aps.org/doi/10.1103/PhysRevA.90.061802. doi:10.1103/PhysRevA.90.061802.

[40] C. Lisdat, G. Grosche, N. Quintin, C. Shi, S. M. F. Raupach, C. Grebing, D. Nicolodi, F. Stefani, A. Al-Masoudi, S. Dörscher, S. Häfner, J.-L. Robyr, N. Chiodo, S. Bilicki, E. Bookjans, A. Koczwara, S. Koke, A. Kuhl, F. Wiotte, F. Meynadier, E. Camisard,

M. Abgrall, M. Lours, T. Legero, H. Schnatz, U. Sterr, H. Denker, C. Chardonnet, Y. L. Coq, G. Santarelli, A. Amy-Klein, R. L. Targat, J. Lodewyck, O. Lopez, P.-E. Pottie, A clock network for geodesy and fundamental science, Nat. Commun. 7 (2015) 12443. URL: http://www.nature.com/articles/ncomms12443. doi:10.1038/ncomms12443.

[41] A. Abuduweili, X. Chen, Z. Chen, F. Meng, T. Wu, H. Guo, Z. Zhang, Sub-ps resolution clock-offset measurement over a 114 km fiber link using linear optical sampling, Opt. Express 28 (2020) 39400–39412. URL: http://www.opticsexpress.org/abstract.cfm?URI=oe-28-26-39400. doi:10.1364/OE.411569.

[42] C. J. Hegarty, GNSS signals — An overview, in: 2012 IEEE International Frequency Control Symposium Proceedings, 2012, pp. 1–7. doi:10.1109/FCS.2012.6243707.

[43] A. Bauch, Time and frequency comparisons using radiofrequency signals from satellites, Comptes Rendus Physique 16 (2015) 471–479. URL: https://www.sciencedirect.com/science/article/pii/S1631070515000201. doi:https://doi.org/10.1016/j.crhy.2015.02.006, the measurement of time / La mesure du temps.

[44] Y. Huang, H. Tsao, Design and Evaluation of an Open-Loop Receiver for TWSTFT Applications, IEEE Transactions on Instrumentation and Measurement 64 (2015) 1553–1558. doi:10.1109/TIM.2015.2415111.

[45] M. J. Wouters, L. Marais, Time-transfer over optical fibre using pseudo-random noise ranging, in: 2014 European Frequency and Time Forum (EFTF), 2014, pp. 308–311. doi:10.1109/EFTF.2014.7331494.

[46] M. Sha, Y. Xie, The Simulation Study of the Spread-Spectrum System, in: Proceedings of the 2015 4th International Conference on Computer, Mechatronics, Control and Electronic Engineering, Atlantis Press, 2015/11, pp. 833–836. URL: https://doi.org/10.2991/iccmcee-15.2015.152. doi:https://doi.org/10.2991/iccmcee-15.2015.152.

[47] D. Piester, A. Bauch, J. Becker, A. Hoppmann, Time and Frequency Broadcast With DCF77, in: Proceedings of the 43rd Annual Precise Time and Time Interval Systems and Applications Meeting, 2011, pp. 185–196. URL: https://www.ion.org/publications/abstract.cfm?articleID=10784.

[48] D. Engeler, Performance analysis and receiver architectures of DCF77 radio-controlled clocks, IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control 59 (2012) 869–884. doi:10.1109/TUFFC.2012.2272.

[49] NPL, MSF radio time signal, 2021. URL: https://www.npl.co.uk/msf-signal.

[50] P. Dolea, P. V. Dascal, T. Palade, O. Cristea, Aspects regarding the use of LF radio transmitters for time dissemination, in: 2014 11th International Symposium on Electronics and Telecommunications (ISETC), 2014, pp. 1–4. doi:10.1109/ISETC.2014.7010763.

[51] M. Maaref, J. Khalife, Z. M. Kassas, Integrity monitoring of LTE signals of opportunity-based navigation for autonomous ground vehicles, in: Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018), 2018, pp. 2456–2466.

[52] Z. Jiang, V. Zhang, Y.-J. Huang, J. Achkar, D. Piester, S.-Y. Lin, W. Wu, A. Naumov, S.-h. Yang, J. Nawrocki, et al., Use of software-defined radio receivers in two-way satellite time and frequency transfers for UTC computation, Metrologia 55 (2018) 685.

[53] M. B. Mathews, P. F. MacDoran, A Software Defined Radio Solution for Hybrid GPS/Signals of Opportunity Navigation, in: Proceedings of the 26th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2013), 2013, pp. 1539–1548.

[54] G. Petit, Z. Jiang, Precise Point Positioning for TAI computation, in: 2007 IEEE International Frequency Control Symposium Joint with the 21st European Frequency and Time Forum, 2007, pp. 395–398. doi:10.1109/FREQ.2007.4319104.

[55] J. A. Sherman, R. Jördens, Oscillator metrology with software defined radio, Review of Scientific Instruments 87 (2016) 054711. URL: https://doi.org/10.1063/1.4950898. doi:10.1063/1.4950898.

[56] K. Hanhijärvi, A. E. Wallin, Software Defined Radio Based Phase Meter for Frequency Metrology, in: Proceedings of the XXXV Finnish URSI Convention on Radio Science, 2019. URL: https://www.ursi.fi/2019/.

[57] A. E. Wallin, High-resolution frequency/phase-microstepper for timing laboratories, 2021. URL: https://ohwr.org/project/microstepper.

[58] J. Yao, T. E. Parker, N. Ashby, J. Levine, Incorporating an Optical Clock Into a Time Scale, IEEE Trans. Ultrason., Ferroelectr., Freq. Control 65 (2018) 127–134. doi:10.1109/TUFFC.2017.2773530.

[59] C. Grebing, A. Al-Masoudi, S. Dörscher, S. Häfner, V. Gerginov, S. Weyers, B. Lipphardt, F. Riehle, U. Sterr, C. Lisdat, Realization of a timescale with an accurate optical lattice clock, Optica 3 (2016) 563–569. URL: http://www.osapublishing.org/optica/abstract.cfm?URI=optica-3-6-563. doi:10.1364/OPTICA.3.000563.

[60] H. Hachisu, F. Nakagawa, Y. Hanado, T. Ido, Months-long real-time generation of a time scale based on an optical clock, Sci. Rep. 8 (2018) 4243. URL: https://www.nature.com/articles/s41598-018-22423-5. doi:10.1038/s41598-018-22423-5.

[61] J. Yao, J. A. Sherman, T. Fortier, H. Leopardi, T. Parker, W. McGrew, X. Zhang, D. Nicolodi, R. Fasano, S. Schäffer, K. Beloy, J. Savory, S. Romisch, C. Oates, S. Diddams, A. Ludlow, J. Levine, Optical-Clock-Based Time Scale, Phys. Rev. Applied 12 (2019) 044069. URL: https://link.aps.org/doi/10.1103/PhysRevApplied.12.044069. doi:10.1103/PhysRevApplied.12.044069.