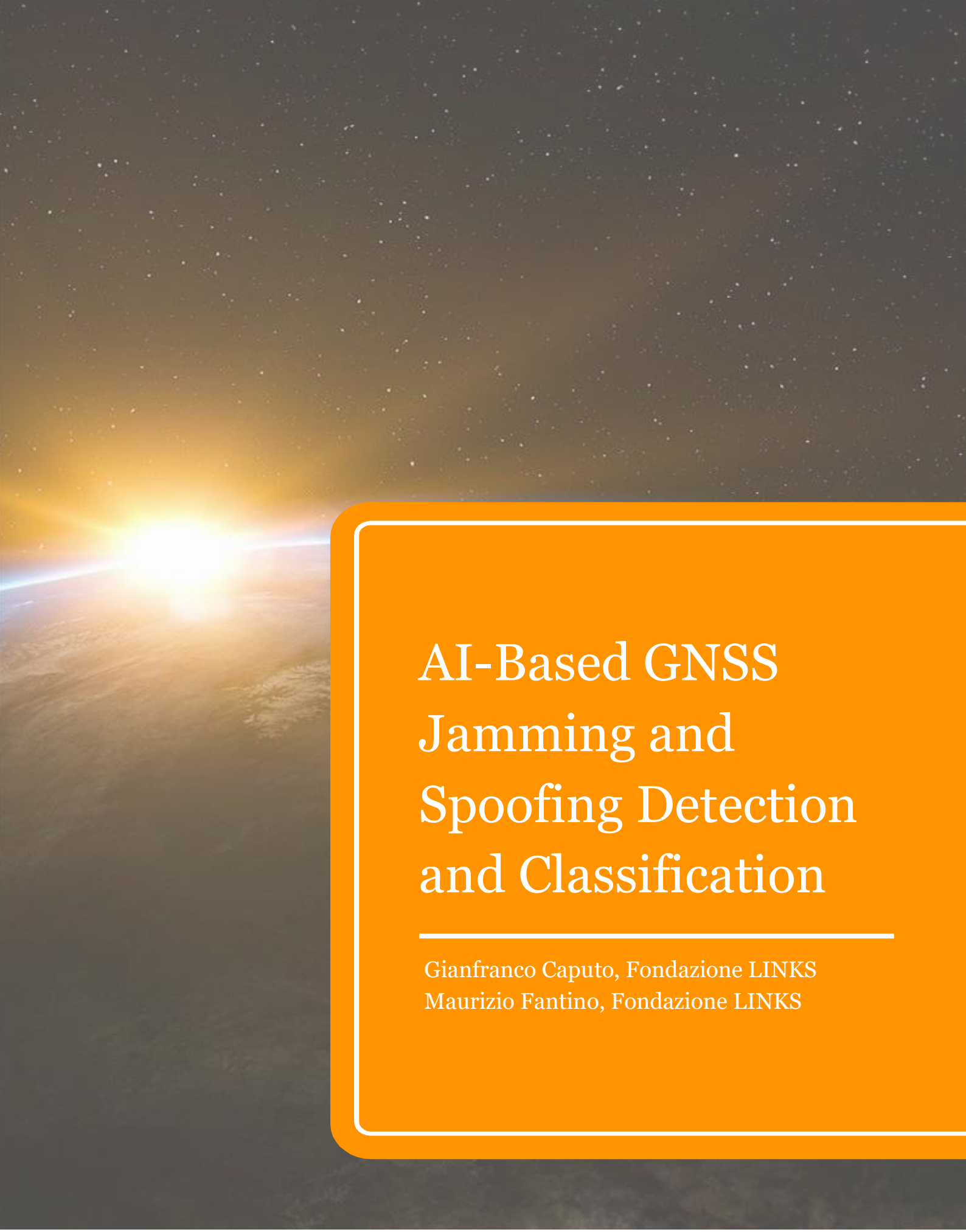

AI-Based GNSS Jamming and Spoofing Detection and Classification

Gianfranco Caputo, Fondazione LINKS
Maurizio Fantino, Fondazione LINKS

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe Research and Innovation Programme under the Grant Agreement No. 101073909.

AI-Based GNSS Jamming and Spoofing Detection and Classification

Gianfranco Caputo and Maurizio Fantino (Fondazione LINKS)

AI-based GNSS interference detection is proposed over conventional techniques since AI algorithms can significantly address the gaps in GNSS jamming and spoofing detection, improving the reliability and trustworthiness of GNSS-dependent applications, especially within the target organization (CI).

1. Introduction

Nowadays, positioning systems, are widely implemented in all areas of our lives, and are not only used for positioning and navigation purposes anymore, but also for purposes of time synchronization in different applications, such as financial transaction systems, communication and electric grid networks In the context of Critical Infrastructures (CI) monitoring targeted in ATLANTIS project, positioning systems are essential to provide high accurate reliable positioning and timing information. GNSS (Global Navigation Satellite System) is currently the most reliable source for positioning services. GNSS refers to a constellation of satellites providing signals from space that transmit positioning and timing data to GNSS receivers.

GNSS (Global Navigation Satellite System) is currently the most reliable source for positioning services, serving as the backbone for ensuring the seamless operation of such critical infrastructures. GNSS refers to a constellation of satellites providing signals from space that transmit positioning and timing data to GNSS receivers, a technology that has become indispensable in the face of growing demands for real-time accuracy and reliability in critical infrastructures [1]. The reliance on GNSS for critical infrastructure monitoring, as evidenced by its comprehensive adoption in the ATLANTIS project, is a testament to the vital role of precise, real-time positioning and timing information in maintaining the integrity, safety, and efficiency of these essential services.

In the framework of the ATLANTIS, the challenges posed by evolving threats to satellite navigation and timing systems are addressed through the development of AI-driven algorithms to support the detection and wherever possible the classification of a threat. These AI algorithms are designed to meet stringent requirements, to learn and adapt from new data and to proof the necessary reliability to cope with the stringent requirement of critical sectors, including transport, energy, telecoms, health, logistics, supply chain, and border control which are the main target of ATLANTIS.

2. The Current State of Affairs in Jamming and Spoofing Techniques

Conventional jamming and spoofing detection techniques involve a variety of methods, which can be classified in four main categories:

- **Signal Strength Monitoring**: a sudden increase or decrease in signal strength can indicate jamming. This method is simple but not always reliable, as natural fluctuations in signal strength can occur even without interference.
- **Spectrum Analysis**: analysing the spectrum of the received signals can reveal the presence of interference, because jamming typically shows up as unexpected spikes in the spectrum.
- **Time-of-Arrival Analysis**: comparing the time of arrival of signals from different satellites can reveal discrepancies caused by spoofing, even though this method requires precise timekeeping and can be computationally intensive.
- **Angle-of-Arrival (AoA) Techniques**: by measuring the direction from which signals are coming, AoA techniques can detect spoofing attempts that typically come from a different direction than the legitimate satellite signals, even though this method requires antenna arrays and sophisticated signal processing.

While the traditional techniques applied to implement the aforementioned methods are effective in many scenarios, they often lack the adaptability and advanced analytical capabilities of AI-based systems.

Moreover, many advanced solutions are not easily scalable or affordable for widespread use, particularly in consumer or low-budget applications, and the rapidly evolving nature of jamming and spoofing means that current technologies (employ?) may quickly become obsolete.

As attacking techniques become more sophisticated, there's an increasing trend towards integrating these traditional methods with more advanced AI and machine learning algorithms to enhance detection and response capabilities.

3. The Role of AI-Based Detection and Classification

The rapid advancement and integration of AI technologies have dramatically transformed the landscape of GNSS jamming and spoofing detection. Traditional methods, while effective to an extent, often fall short in the face of sophisticated and dynamically evolving threats. The incorporation of AI and machine learning algorithms into detection systems presents a formidable response to these challenges, offering unparalleled adaptability, accuracy, and efficiency [2][3].

AI-based detection and classification systems leverage complex data patterns to distinguish between legitimate and malicious interference, reducing false positives and enhancing the reliability of GNSS services. For instance, Convolutional Neural Networks (CNNs) have been applied to analyse synthetic GNSS signals combined with real-world jamming scenarios [4], demonstrating the potential for high accuracy in interference classification. These

approaches utilize a combination of image and statistical features to distinguish between different types of jamming and spoofing attacks, showcasing the versatility and depth of analysis possible with AI technologies [5].

Innovations in this field have explored various architectures and models to optimize performance and computational efficiency. The exploration of CNN architectures with lower computational loads indicates a move towards making these technologies more accessible and implementable in real-time systems, including those constrained by hardware capabilities, such as GNSS chipsets. The discussion extends to the potential of transformer models, which, despite their complexity, offer promising avenues for direct analysis of raw samples, further broadening the scope of detection mechanisms.

Moreover, AI-based systems are not limited to pre-processing GNSS signals but also extend to post-correlation measurements, such as Carrier-to-Noise density ratio (C/No) [6], further enriching the data pool from which these systems can learn and adapt. This adaptability is crucial, as the nature of jamming and spoofing attacks continuously evolves, necessitating detection systems that can learn from new patterns and threats dynamically.

The development and refinement of AI-based GNSS jamming and spoofing detection systems [7] represent a significant step forward in securing GNSS infrastructure. By leveraging advanced machine learning algorithms and neural network architectures, these systems offer a robust defence mechanism capable of adapting to and mitigating the ever-changing landscape of GNSS threats. As these technologies continue to evolve, their integration into GNSS security protocols will play a pivotal role in maintaining the integrity and reliability of critical positioning, navigation, and timing services.

4. The Research and Development Path in ATLANTIS

To implement an AI model that effectively detects and classifies different types of GNSS jamming and spoofing threats, a structured approach has been followed, which encompasses several critical phases.

The first step, defined as RFI Generation, involves producing a comprehensive dataset that include examples of GNSS signals under various conditions, such as normal operations, jamming, spoofing and combined threats. This has been achieved by collecting real-world GNSS signal data or synthetic data generated with a simulation tool such as the IFEN Generator, combined with several interference scenarios generated using a Universal Software Radio Peripheral (USRP), along with GNU-Radio Software (or possibly a hardware single-chirp jammer), to create a diverse range of conditions. See Figure 1 below.

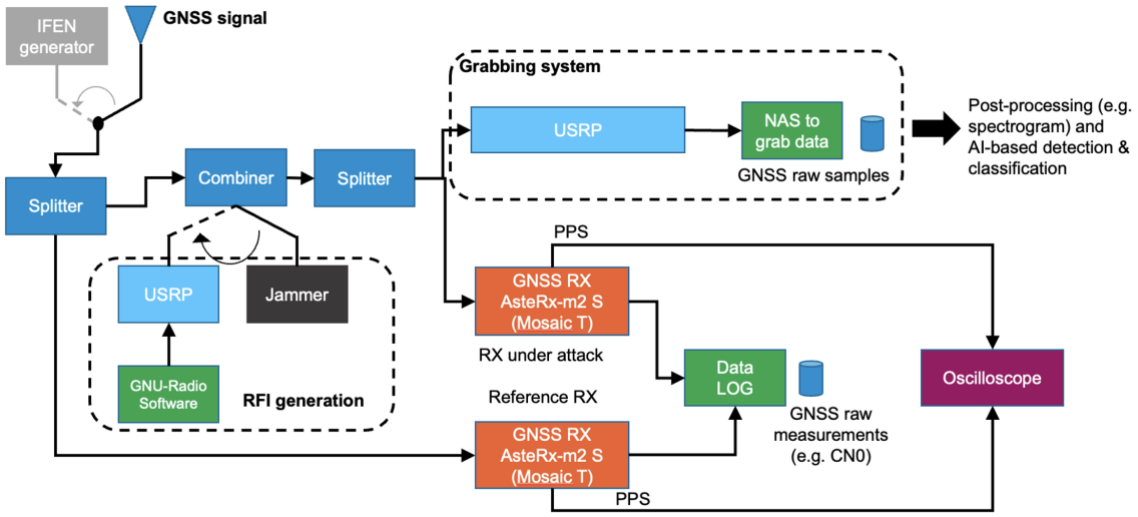

Figure 1. A conceptual block diagram of the laboratory testbench used to generate and capture data.

The second step, defined as Grabbing System, involves capturing the resulting signal with a second USRP, and recording raw samples in a high-speed storage device (NAS).

Once the data is collected, it needs to be prepared for AI processing. This involves converting the GNSS signals into formats that are suitable for AI models, such as spectrograms (see, for example, Figure 2) and feature vectors that capture relevant signal characteristics: key statistical features indicative of jamming and spoofing activities, such as anomalies in signal strength, frequency spikes, and discrepancies in signal arrival times, are extracted during this phase.

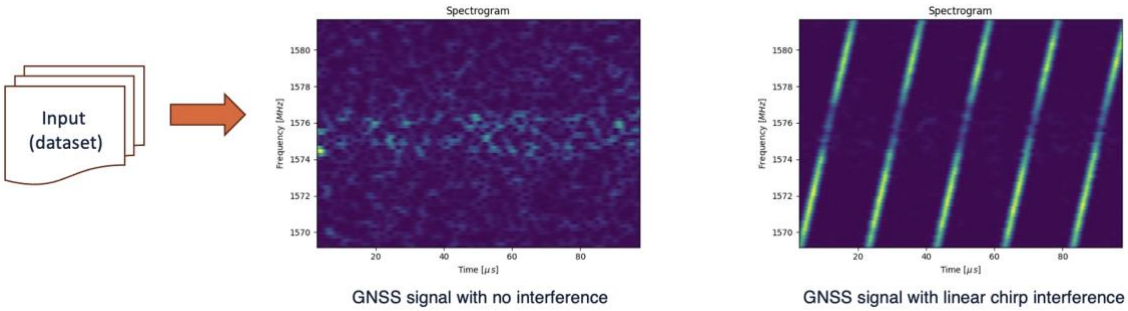

Figure 2. Examples of spectrograms of normal and jammed signals.

Choosing the right AI model is crucial for effectively addressing the complexity of the data and the computational resource constraints. Convolutional Neural Networks (CNNs) have been found effective for classifying interference patterns in an image-based format produced from the spectrogram of the signal. See Figure 3.

Depending on the data and resources, other models like Deep Neural Networks (DNNs) or traditional machine learning models may also be appropriate to detect anomalies on the spectrum of the signal. The models have been trained using the prepared datasets, with a focus on employing supervised learning techniques where the interference type for each data point is known.

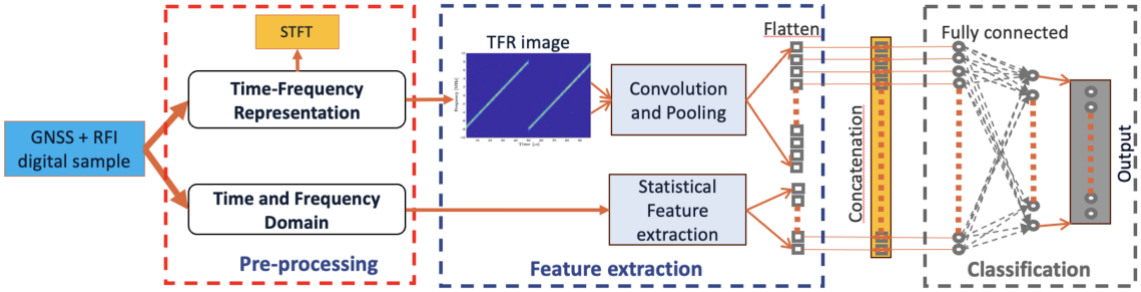

Figure 3. Diagram block of feature aided CNN classifier.

After training, the models have been tested using a separate dataset to evaluate their effectiveness in detecting and classifying jamming and spoofing threats accurately. Further activity may involve optimizing the models through hyperparameter tuning, model ensemble strategies, and feature selection to improve their performance while considering the computational complexity for real-time deployment.

5. The Challenges and Barriers

Implementing AI-based GNSS jamming and spoofing detection systems is an intricate process, filled with a variety of challenges. One of the primary hurdles lies in gathering and preparing a comprehensive and diverse dataset. This dataset is crucial for training AI models, but obtaining real-world data on jamming and spoofing, which are rare and illegal, is difficult. In fact, GNSS services like GPS, GLONASS, Galileo, and BeiDou operate under international regulations. However, the rapid pace of technological advancement in AI often outstrips the evolution of these regulatory frameworks, leading to a gap between what's technically possible and what's legally permissible.

Moreover, regulations vary significantly across different countries and regions, adding another layer of complexity. A system developed in one country might not be immediately applicable or legal in another, due to different regulatory standards and requirements. This poses a significant challenge for developers aiming for wide-scale implementation of their systems.

Since jamming GNSS signals is illegal in most jurisdictions, researchers and developers face a significant hurdle in acquiring authentic data for training and testing their AI models, nevertheless for the purpose of training and tuning AI models, the generation of synthetic but realistic interference does not invalidate the goodness and the quality of the work, which can then be applied to real-life conditions.

6. The Benefits and Impact

The implementation of AI-based GNSS jamming and spoofing detection technology holds significant potential for enhancing security, safety, and optimizing various business processes. By accurately identifying interference, these systems can substantially improve the reliability and trustworthiness of GNSS-dependent applications, especially within the target organization (CI).

In terms of security and safety, one of the most immediate benefits is in aviation and land/maritime navigation: air traffic relies heavily in GNSS and any disruption due to jamming or spoofing poses a serious risk; similarly, in land/maritime navigation, where GNSS is crucial for precise location tracking, such technology can prevent potential accidents caused by misleading location data. In ATLANTIS project this aspect will be addressed on the Large-Scale Pilot #1 on the French-Italian border: being the Fréjus Tunnel a major transalpine roadway, in the event of accidents or emergencies within the tunnel, GNSS technologies play a crucial role in coordinating emergency response efforts. Jamming or spoofing attacks could disrupt communication and navigation, hindering timely response and rescue operations. Detection systems can ensure that emergency services maintain access to accurate positioning and timing information, facilitating efficient response.

Moreover, in the realms of banking and telecommunications, the significance of AI-based solutions, is rooted in their reliance on precise timing: the banking sector uses (among other techniques such as NTP servers) GNSS-based timestamping for synchronizing financial transactions across various networks and locations. Accurate time signals are vital to maintain the integrity of these transactions, and any discrepancies caused by GNSS timing errors or manipulations could lead to financial irregularities, affecting everything from stock trading to everyday banking operations. In the ATLANTIS project this aspect will be addressed on the Large-Scale Pilot #2 on the premises of Caixa Bank in Barcelona: implementing GNSS jamming and spoofing detection as part of a comprehensive cybersecurity strategy enhances the resilience of banking operations, safeguarding the timing integrity and ensuring that transactions are accurately timestamped and processed in the correct sequence.

Similarly, in telecommunications and electric grids, GNSS signals are crucial for synchronization. They ensure that data packets are transmitted and received in a timely and coordinated manner across the network. Disruptions or inaccuracies in GNSS signals can lead to network and power outages, poor quality of service, and even impact critical infrastructures such as hospitals, or communication services. Implementing AI-based detection systems in these sectors can greatly reduce the risk of such disruptions, ensuring the reliability of essential services that underpin the modern economy and public safety.

7. Future Outlook

The scalability, adaptability, and precision of AI-based GNSS jamming and spoofing detection technology are key factors that define its future prospects. As the security landscape evolves and the sophistication of jamming and spoofing methods increase, the ability of technology to adapt and scale becomes increasingly important for critical infrastructures.

The adaptability of AI-based systems is particularly significant in the face of changing security threats. AI's learning capabilities allow these systems to continuously evolve and respond to new types of jamming and spoofing attacks. As attackers develop more sophisticated methods, AI-based detection systems can learn from these new patterns, ensuring they remain effective in identifying and mitigating threats. This ongoing learning

process is pivotal in maintaining the integrity of GNSS services in an ever-changing security environment.

8. Conclusions

Positioning systems are essential in CI infrastructure monitoring. However, conventional jamming and spoofing detection techniques often lack the adaptability and advanced analytical capabilities of AI-based systems and are not easily scalable or affordable for widespread use. In ATLANTIS we propose the use of AI techniques in GNSS interference detection. To test our approach, we have setup a lab experiment that simulates jamming and spoofing GNSS signal and collects data for training of AI models. The final outcomes of this work will be a systematic evaluation of different AI methods in the context of GNSS interference detection, that could significantly contribute in the enhances of the critical infrastructures' reliability.

References

[1] https://www.euspa.europa.eu/newsroom/news/new-galileo-inspired-opportunities-critical-infrastructures-management-presented-itsf

[2] VOIGT, J. M. Classification of GNSS jammers using machine learning: Multivariate time series and image classification based approaches. MS thesis. 2021.

[3] Morales Ferre, R.; de la Fuente, A.; Lohan, E.S. Jammer Classification in GNSS Bands Via Machine Learning Algorithms. Sensors 2019, https://doi.org/10.3390/s19224841

[4] Ebrahimi Mehr, Iman (Arman); Dovis, Fabio (2023). A Deep Neural Network Approach for Detection and Classification of GNSS Interference and Jammer. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.22212121.v1

[5] Ebrahimi Mehr, Iman (Arman), A. Minetto, F. Dovis, A Navigation Signals Monitoring, Analysis and Recording Tool: Application to Real-Time Interference Detection and Classification, ION GNSS 2023.

[6] A. Elango, S. Ujan and L. Ruotsalainen, "Disruptive GNSS Signal detection and classification at different Power levels Using Advanced Deep-Learning Approach," ICL-GNSS 2022. https://doi.org/10.1109/ICL-GNSS54081.2022.9797026

[7] Borhani-Darian, Parisa, Li, Haoqing, Wu, Peng, Closas, Pau, "Deep Neural Network Approach to Detect GNSS Spoofing Attacks," ION GNSS+ 2020. https://doi.org/10.33012/2020.17537

Front cover image by Arek Socha via Pixabay.
https://pixabay.com/users/qimono-1962238