Resilient Multi-Sensor Navigation for Safety-Critical Ground and Low-Altitude Transportation: From Solitary Defender to Byzantine-Adaptive Collective Intelligence

An AI-Enhanced Information-Theoretic Framework for GNSS Spoofing Detection & Mitigation

PhD supervisor : Maan EL BADAOUI EL NAJJAR
maan.el-badaoui-el-najjar@univ-lille.fr

Research Context and Motivation

Global Navigation Satellite Systems (GNSS) have revolutionized positioning technologies over the past two decades, becoming a game-changer to numerous applications ranging from personal navigation to asset tracking. However, the transition of GNSS from convenience-oriented to safety-critical systems, particularly in Ground and Low-Altitude Transportation Systems (GLATS), necessitates a comprehensive reevaluation of its reliability and integrity. While GNSS provides, for cheap and without prior knowledge, positioning information, its vulnerabilities in complex environments pose significant risks to system integrity and safety. These vulnerabilities can be categorized into two main types: 'natural' and 'artificial' phenomena among them intentional interference. Natural phenomena affecting GNSS performance include (without being exhaustive): Non-Line-Of-Sight (NLOS) reception, multipath effects, signal diffraction, ionospheric scintillation, signal blockage in urban canyons.

These "natural" vulnerabilities have been extensively studied, and significant progress has been made in mitigating their effects[1]. Our team has contributed to this field by developing advanced detection and mitigation techniques for NLOS reception and multipath effects, which are particularly prevalent in urban environments [2] [3] [4]. Despite these advancements, intentional interference remains a critical concern, with jamming and spoofing emerging as significant threats:

- Jamming: Deliberate or unintentional interference with GNSS signals, potentially rendering the positioning system inoperable [5] [6] [7] [8].
- Spoofing: Transmission of false GNSS-like signals to deceive the receiver, leading to erroneous position and timing information [9] [10].

The severity of these threats has increased due to the democratization of software-defined radio (SDR) technology and the increasing availability of GNSS simulation tools. Recent geopolitical events have highlighted this vulnerability, with documented cases of GNSS interference and spoofing in conflict zones and around critical infrastructure[11] [12]. To address these challenges, the field has increasingly turned to multi-sensor fusion approaches. By combining GNSS with other sensors such as Inertial Measurement Units (IMUs), LiDAR, and cameras, one can leverage the strengths of each technology while mitigating their individual weaknesses. This approach has shown promising results in improving the robustness of navigation systems [13][14][15]. However, while multi-sensor fusion offers significant advantages, the vulnerabilities of GNSS remain a critical concern, particularly during a too-long unavailability. A successful spoofing attack on an autonomous vehicle could potentially lead to catastrophic consequences, not only for the affected vehicle and passengers but also for surrounding people and goods. The sophisticated nature of modern spoofing attacks increase the need for advanced detection techniques [16][17][18]. The current context, marked by increased cyber-warfare activities and the targeting of critical navigation systems, makes addressing these vulnerabilities particularly timely and crucial. Thus, ensuring the integrity and reliability of navigation systems against intentional malicious attacks is paramount.

Research Objectives

This research aims to develop robust detection and mitigation strategies for GNSS vulnerabilities at a systemic level, focusing on multi-sensor fusion systems. The specific objectives are:

- Formulate an information-theoretic framework for GNSS spoofing detection in multi-sensor environments.
- Develop and validate Byzantine-resilient algorithms for collaborative spoofing detection in multi-vehicle scenarios.
- Create comprehensive annotated datasets of GNSS spoofing scenarios for single and multi-vehicle contexts.
- Design and implement machine learning models for adaptive spoofing detection and classification.
- Evaluate the effectiveness of the developed framework through extensive simulations and controlled experiments.

Our approach will leverage information theory, advanced machine learning techniques, and multi-sensor fusion to create a comprehensive framework for spoofing detection and mitigation. The project will address both single-vehicle and multi-vehicle scenarios, recognizing that collaborative approaches can enhance detection capabilities while introducing new challenges in terms of information sharing and trust-scale (Byzantine Generals Problem).

A key aspect of this research will be the formulation of the GNSS spoofing detection problem through information theory principles. This approach will provide a rigorous mathematical framework for quantifying and optimizing information flow within collaborative vehicle networks, enabling the development of adaptive trust models and robust consensus mechanisms. By leveraging information-theoretic concepts, we aim to create a unified methodology that enhances resilience against spoofing attacks while capitalizing on the collective intelligence of multi-vehicle multi-modal systems.

A significant portion of this work will focus on creating comprehensive annotated databases of GNSS spoofing scenarios. These databases will be essential for training and validating machine learning algorithms, and will include data from multiple sensor modalities including GNSS, IMU, and LIDAR measurements. The CRIStAL laboratory's PRETIL platform provides an ideal environment for this research, offering extensive experimental capabilities through equipped Renault ZOE vehicles, drones, and a sophisticated digital twin environment. The platform's SAFRAN SKYDEL GNSS simulation technology enables the generation of complex spoofing and jamming scenarios in a controlled environment.

The creation of these datasets will require careful experimental design, systematic data collection, and meticulous annotation processes. The combination of real-world testing capabilities and controlled simulation environment will enable the development of robust, comprehensive datasets that capture both naturalistic driving conditions and precisely controlled spoofing scenarios. This dual approach to data collection will be crucial for developing and validating machine learning algorithms that can perform reliably in real-world applications.

Research Methodology and Timeline

The PhD project, spanning 36 months, will be approached as a comprehensive project with various identified and non-exhaustive phases. This structure allows for flexibility and adaptability, enabling iterative loops between phases as new insights are gained throughout the rich research process. Demonstrating the PhD candidate's maturity, the research strategy anticipates and plans for inherent uncertainties in cutting-edge scientific research. If emerging technologies or newly published research significantly impact the project's direction, the subsequent phases may be adjusted accordingly. This adaptive approach ensures that the research remains at the forefront of the field throughout its duration.

Phase #1: Foundation and Literature Review (4 months)

This initial phase will establish a solid theoretical foundation through a comprehensive systematic literature review. The review will explore existing approaches to spoofing detection, with particular attention to

information-theoretic methods and multi-vehicle scenarios. The candidate will develop detailed mind maps to identify research gaps and opportunities, leading to the publication of a systematic review paper. This phase will also include familiarization with existing tools and frameworks, along with a clear definition of research boundaries and constraints.

Milestone 1: Literature review paper submitted

Phase #2: Platform Familiarization and Algorithms Enhancement and Development (4 months)

This phase will emphasize gaining familiarity with the algorithms, sensors, and simulation facilities available at the CRIStAL laboratory. The candidate will work closely with the PRETIL platform, including the Renault ZOE vehicles and their sensor suites. They will also become proficient in using the CARLA simulator and SAFRAN's SKYDEL GNSS and Spoffing simulation technology. During this period, initial detection and mitigation algorithms will be developed, focusing on tightly coupling GNSS and IMU data (with optional LIDAR integration), along with implementing a diagnostic layer for anomaly detection.

Milestone 2: Initial core-algorithm prototype developed

Phase #3: Development of Theoretical Framework (10 months)

This phase will concentrate on developing the core theoretical framework, involving the formulation of information-theoretic models and geometric gain estimation techniques. The candidate will explore advanced concepts such as Jensen-Shannon and Rényi divergences, linking these parametric divergences to the Byzantine fault tolerance problem in multi-vehicle scenarios. Key activities will include:

- Investigating divergence measures to quantify information reliability and detect anomalies in vehicle sensors measurements.
- Formulating information-theoretic models for spoofing detection in both single-vehicle and multi-vehicle environments.
- Developing trust models and consensus mechanisms inspired by the Byzantine Generals Problem for collaborative spoofing detection.

This phase will result in a unified theoretical foundation for the proposed spoofing detection and mitigation framework, supported by rigorous mathematical formulations. Note that an iterative approach will be adopted between the theoretical framework development and the experimental validation phase (phase 5). Initial concepts will be tested early, allowing for refinements based on preliminary results.

Milestone 3: Theoretical framework formulated and co-validated

Phase #4: Dataset Creation and Machine Learning Development (6 months)

This crucial phase will focus on creating comprehensive annotated datasets for training and validating machine learning models, capturing various spoofing scenarios in both single-vehicle and multi-vehicle contexts. The candidate will design and implement sophisticated data collection protocols, ensuring a wide range of environmental conditions, spoofing techniques, and sensor configurations are represented. Key activities will include:

- Designing diverse spoofing scenarios using the SAFRAN's SKYDEL GNSS simulation technology ;
- Collecting real-world driving data using the PRETIL platform's Renault ZOE vehicles ;
- Developing a robust annotation pipeline for labeling spoofing events and relevant sensor data ;
- Implementing and training various machine learning models, including deep learning architectures, for spoofing detection and classification.

The resulting datasets will be a valuable contribution to the research community, enabling further advancements in GNSS spoofing detection and mitigation.

Milestone 4: Comprehensive dataset created and initial ML models trained

Phase #5: Experimental Validation (8 months)

This phase will involve comprehensive testing of the developed approaches, including trials in both single-vehicle and multi-vehicle configurations. Data collection from real-world driving scenarios will be conducted using the PRETIL platform's Renault ZOE vehicles. However, for spoofing scenarios, all tests will be performed in a controlled laboratory environment to ensure safety and repeatability. Key activities will include:

- Designing a comprehensive test protocol covering various spoofing scenarios and environmental conditions ;
- Conducting extensive simulations using the CARLA simulator and SKYDEL GNSS simulation technology ;
- Performing controlled laboratory experiments to validate the performance of the developed algorithms ;
- Analyzing the effectiveness of the collaborative detection approach in multi-vehicle scenarios ;
- Evaluating the system's resilience under extreme spoofing scenarios and in challenging urban environments.

This phase will provide crucial empirical evidence for the effectiveness of the developed framework, identifying strengths and areas for improvement.

Milestone 5: Experimental validation completed and results analyzed

Phase #6: Analysis and Thesis Writing (4 months)

The final phase will focus on critical analysis of the results, identification of limitations and potential improvements, and compilation of the findings into a comprehensive thesis. The candidate will also prepare journal publications and conference presentations to disseminate the research outcomes to the broader scientific community. Key activities will include:

- Conducting in-depth analysis of experimental results ;
- Identifying limitations of the current approach and proposing future research directions ;
- Writing and submitting research papers to high-impact journals and conferences ;
- Compiling the complete research findings into a cohesive doctoral thesis ;
- Preparing for the thesis defense.

Milestone 6: Thesis draft completed and final defense scheduled

In addition to these milestones, regular intermediate deliverables such as annual progress reports will be established to ensure steady progress. These deliverables will serve as checkpoints to ensure steady progress and allow for timely adjustments to the research direction if needed. The PhD candidate will be encouraged to take initiative in proposing and leading these deliverables, fostering a sense of ownership and autonomy in the research process.

Dissemination Plan:

The research outcomes will be disseminated through at least 2 journal articles in high-impact publications such as IEEE Transactions on Intelligent Transportation Systems , four conference papers at venues like ION GNSS+ and FUSION, and multiple poster presentations. Key algorithms will be made available as open-source contributions to foster community engagement and further development.

Skills and Tools

The PhD candidate will develop and utilize a wide range of skills and tools throughout this research project, including:

- Programming: Proficiency in MATLAB and Python for algorithm development and data analysis ;
- ROS: Experience with the Robot Operating System middleware for integrating and managing multiple sensor inputs under Linux based OS ;
- Estimation Theory: Advanced knowledge of Kalman filtering and its variants for sensor fusion ;
- Probability and Statistics: Strong foundation in probability theory and statistical analysis ;
- Decision Theory: Understanding and application of decision-making frameworks in uncertain environments ;
- Fault Diagnosis: Techniques for Fault Detection and Isolation (FDI) and Fault Detection and Exclusion (FDE) ;
- Information Theory: Deep understanding of entropic measures, divergences, and their applications ;
- Machine Learning: Experience with various ML techniques, particularly those applicable to anomaly detection and classification ;
- Version Control: Experience with Git for collaborative software development ;
- Scientific Writing: Ability to produce high-quality research papers and technical reports .

This comprehensive skill set will enable the candidate to tackle the complex challenges of GNSS spoofing detection and mitigation in multi-sensor, multi-vehicle environments, while contributing novel theoretical frameworks to the field.

Impact and Applications

The outcomes of this research will significantly contribute to enhancing the safety of GNSS-based navigation systems and the reliability of the overall transportation system. The developed frameworks and datasets will provide valuable resources for future research in this field, while practical implementations will offer immediate proof of concept. The PhD candidate will join a dynamic research team with expertise in navigation systems, information theory, and machine learning. They will have access to state-of-the-art GNSS simulation equipment, high-performance computing resources, and multiple sensor platforms. If you're ready for the PhD adventure and consider yourself a "scienthusiast" - someone who is eager to continuously learn, question, and seek answers - then this opportunity might be perfect for you. We're looking for a candidate who is passionate about teamwork, eager to gain knowledge by exploring the intricacies of GNSS and machine learning, and ready to dive into the world of research. If you're excited about the idea of pushing the boundaries of science and technology, and you're prepared for the challenges and rewards of a PhD journey, we encourage you to reach out to us.

Citations

[1] Zidan, J., Adegoke, E. I., Kampert, E., Birrell, S. A., Ford, C. R., & Higgins, M. D. (2020). GNSS vulnerabilities and existing solutions: A review of the literature. IEEE Access, 9, 153960-153976.

[2] Makkawi, K., Ait-Tmazirte, N., El Badaoui El Najjar, M., & Moubayed, N. (2021). Adaptive diagnosis for fault tolerant data fusion based on α-rényi divergence strategy for vehicle localization. Entropy, 23(4), 463.

[3] Harbaoui, N., Makkawi, K., Ait-Tmazirte, N., & El Najjar, M. E. B. (2024). Context Adaptive Fault Tolerant Multi-sensor fusion: Towards a Fail-Safe Multi Operational Objective Vehicle Localization. Journal of Intelligent & Robotic Systems, 110(1), 26.

[4] El Mawas, Z., Cappelle, C., & El Najjar, M. E. B. (2022, July). Fault tolerant cooperative localization using diagnosis based on Jensen Shannon divergence. In 2022 25th International Conference on Information Fusion (FUSION) (pp. 1-8). IEEE.

[5] Kuusniemi, H., Airos, E., Bhuiyan, M. Z. H., & Kröger, T. (2012). GNSS jammers: How vulnerable are consumer grade satellite navigation receivers?. European Journal of Navigation, 10(2), 14-21.

[6] Borio, D., & Gioia, C. (2021). GNSS interference mitigation: A measurement and position domain assessment. NAVIGATION: Journal of the Institute of Navigation, 68(1), 93-114.

[7] Qin, W., & Dovis, F. (2021). Situational awareness of chirp jamming threats to GNSS based on supervised machine learning. IEEE Transactions on Aerospace and Electronic Systems, 58(3), 1707-1720.

[8] Kazim, S. A., Marais, J., & Tmazirte, N. A. (2023, September). On the parameterization of single pole adaptive notch filter against wide range of linear chirp interference. In Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023) (pp. 3861-3877).

[9] Rothmaier, F., Chen, Y. H., Lo, S., & Walter, T. (2021). GNSS spoofing detection through spatial processing. Navigation, 68(2), 243-258.

[10] Mawas, Z. E., Tmazirte, N. A., Cappelle, C., & Najjar, M. E. B. E. (2024, September). Assessing GNSS Spoofing Impact on A Safety-Critical Land Transportation Localization Function Within a Cooperative Fleet: An End-Users Focused Experimental Study. In Proceedings of the 37th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2024) (pp. 3414-3427).

[11] Ieropoulos, V. (2024, September). The impact of GPS interference in the Middle East. In 2024 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 732-736). IEEE.

[12] Wiseman, J. (2022). GPSJAM GPS/GNSS Interference Map. https://gpsjam.org

[13] Ceccato, M., Formaggio, F., Laurenti, N., & Tomasin, S. (2021). Generalized likelihood ratio test for GNSS spoofing detection in devices with IMU. IEEE Transactions on Information Forensics and Security, 16, 3496-3509.

[14] Rothmaier, F., Chen, Y. H., Lo, S., & Walter, T. (2021, January). GNSS spoofing mitigation in the position domain. In Proceedings of the 2021 International Technical Meeting of The Institute of Navigation (pp. 42-55).

[15] Dasgupta, S., Rahman, M., Islam, M., & Chowdhury, M. (2022). A sensor fusion-based GNSS spoofing attack detection framework for autonomous vehicles. IEEE Transactions on Intelligent Transportation Systems, 23(12), 23559-23572.

[16] Wu, Z., Zhang, Y., Yang, Y., Liang, C., & Liu, R. (2020). Spoofing and anti-spoofing technologies of global navigation satellite system: A survey. IEEE Access, 8, 165444-165496.

[17] Borhani-Darian, P., Li, H., Wu, P., & Closas, P. (2024). Detecting GNSS spoofing using deep learning. EURASIP Journal on Advances in Signal Processing, 2024(1), 14.

[18] Pardhasaradhi, B., Yakkati, R. R., & Cenkeramaddi, L. R. (2022). Machine learning-based screening and measurement to measurement association for navigation in GNSS spoofing environment. IEEE Sensors Journal, 22(23), 23423-23435.