Beiträge aus der Informationstechnik

Mobile Nachrichtenübertragung
Nr. 112

Anton Schösser

Network Digital Twins for Spectrum Anomaly Detection in Licensed Band Private Networks

VOGT

Dresden 2026

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

Bibliographic Information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.dnb.de.

Zugl.: Dresden, Techn. Univ., Diss., 2026

Die vorliegende Arbeit stimmt mit dem Original der Dissertation „Network Digital Twins for Spectrum Anomaly Detection in Licensed Band Private Networks“ von Anton Schösser überein.

© Jörg Vogt Verlag 2026
Alle Rechte vorbehalten. All rights reserved.

Gesetzt vom Autor

ISBN 978-3-95947-092-6

Jörg Vogt Verlag
Niederwaldstr. 36
01277 Dresden
Germany

Phone: +49-(0)351-31403921
Telefax: +49-(0)351-31403918
e-mail: info@vogtverlag.de
Internet : www.vogtverlag.de

Technische Universität Dresden

Network Digital Twins for Spectrum Anomaly Detection in Licensed Band Private Networks

Dipl.-Ing.
Anton Schösser (geb. Krause)

der Fakultät Elektrotechnik und Informationstechnik der
Technischen Universität Dresden

zur Erlangung des akademischen Grades

Doktoringenieur
(Dr.-Ing.)

– genehmigte Dissertation –

Vorsitzende:	Prof. Dr. rer. nat. habil. Elizabeth von Hauff
Gutachter:	Prof. Dr.-Ing. Dr. h.c. Gerhard Fettweis
	Prof. Dr.-Ing. Peter Rost
Mitglied der Kommission:	Prof. Dr.-Ing. habil. Gerald Gerlach
Tag der Einreichung:	02.06.2026
Tag der Verteidigung:	22.09.2026

Abstract

Wireless connectivity is rapidly becoming a cornerstone of modern industrial environments, driving advanced manufacturing processes and automation. In this context, private wireless networks operating in licensed bands are gaining significant traction. However, the reliance on such solutions requires their seamless operation, even under adverse circumstances. One critical challenge arises from the open nature of the wireless transmission medium, which makes these networks vulnerable to interference caused by illegitimate transmissions in licensed bands. Such interference may occur unintentionally or even intentionally, referred to as jamming. To ensure the resilience of wireless networks, it is therefore crucial to continuously monitor the spectrum and to detect these illegitimate transmissions, which are termed as anomalies.

State-of-the-art spectrum anomaly detection methods often rely on supervised learning to identify specific patterns or signatures of known anomalies. While being effective for well-defined scenarios, it is challenging to guarantee their robustness against novel or varied patterns. Unsupervised methods, by contrast, detect deviations from learned normal behavior without relying on predefined patterns, offering flexibility and adaptability to new threats. However, this generality often comes at the cost of lower detection fidelity, as distinguishing between benign outliers and true anomalies becomes challenging.

To overcome these limitations, this thesis adopts the spirit of unsupervised detection – thus avoiding dependence on specific patterns – while introducing a fundamentally novel concept: contextual awareness in the spectrum anomaly detection process. Rather than identifying anomalies solely because they are uncommon, the proposed approach compares each observation against a context-specific reference. This reference is provided by a network digital twin (NDT), a concept that has emerged alongside the development of 6G networks and functions as a real-time virtual replica of the physical network environment. By leveraging the NDT, the anomaly detection process gains a dynamic and accurate baseline, enabling more precise and contextually informed identification of spectrum anomalies.

The further contributions of this thesis focus on the investigation and evaluation of the proposed concept, carried out in two stages. First, simulations were conducted to establish a proof of concept using received power as an indicator for spectrum anomalies. These simulations demonstrated the feasibility of the concept and provided initial insights, though the practical relevance of received power as an indicator is limited

due to its coarse granularity. Upon this foundation, the second stage introduces the channel frequency response (CFR) as a more sensitive and informative indicator within the proposed framework. Its suitability is validated through a channel measurement campaign conducted in the presence of a jammer, confirming the CFR's sensitivity to interference. Leveraging this data in a detection framework, the proposed approach achieved significant outperformance compared to baseline methods. Further validation through link-level simulations demonstrated the robustness of CFR-based detection, particularly for scenarios involving large bandwidths and low signal-to-noise ratios (SNRs), where this approach consistently outperformed the benchmark method.

These findings represent an important step toward enhancing the resilience of private wireless networks in industrial environments, ensuring robust operation even under adverse circumstances. By leveraging NDTs, this work lays the foundation for more adaptive and intelligent spectrum monitoring solutions in next-generation communication systems.

Kurzfassung

Die drahtlose Konnektivität wird zunehmend zu einem Grundpfeiler moderner industrieller Umgebungen und treibt fortschrittliche Fertigungsprozesse sowie Automatisierung voran. In diesem Kontext gewinnen private drahtlose Netzwerke, die in lizenzierten Frequenzbändern betrieben werden, erheblich an Bedeutung. Allerdings erfordert die Abhängigkeit von solchen Lösungen deren reibungslosen Betrieb, selbst unter widrigen Umständen. Eine wesentliche Herausforderung hierbei ergibt sich aus der offenen Natur des drahtlosen Übertragungsmediums, die diese Netzwerke anfällig für Störungen durch illegitime Übertragungen in lizenzierten Frequenzbändern macht. Solche Störungen können unbeabsichtigt oder absichtlich auftreten, wobei Letzteres als Jamming bezeichnet wird. Um die Resilienz drahtloser Netzwerke zu gewährleisten, ist es daher entscheidend, das Spektrum kontinuierlich zu überwachen und diese illegitimen Übertragungen, die als Anomalien bezeichnet werden, zu erkennen.

Moderne Methoden zur Erkennung von Spektrumanomalien basieren häufig auf überwachtem Lernen, um spezifische Muster oder Signaturen bekannter Anomalien zu identifizieren. Während diese Ansätze in klar definierten Szenarien effektiv sind, ist es schwierig, ihre Robustheit gegenüber neuen oder variierenden Mustern zu gewährleisten. Unüberwachte Methoden hingegen erkennen Abweichungen vom erlernten Normalverhalten, ohne auf vordefinierte Muster angewiesen zu sein, und bieten somit Flexibilität und Anpassungsfähigkeit an neue Bedrohungen. Diese Allgemeingültigkeit geht jedoch oft auf Kosten einer geringeren Erkennungsgenauigkeit, da die Unterscheidung zwischen harmlosen Ausreißern und tatsächlichen Anomalien schwierig wird.

Um diese Einschränkungen zu überwinden, verfolgt diese Arbeit den Ansatz des unüberwachten Lernens – und vermeidet damit die Abhängigkeit von spezifischen Mustern – und führt gleichzeitig ein grundlegend neues Konzept ein: Kontextbewusstsein im Prozess der Spektrumanomalieerkennung. Anstatt Anomalien ausschließlich aufgrund ihrer Seltenheit zu identifizieren, vergleicht der vorgeschlagene Ansatz jede Beobachtung mit einem kontextspezifischen Referenzwert. Diese Referenz wird durch einen Network Digital Twin (NDT, digitaler Zwilling eines Netzwerks) bereitgestellt, ein Konzept, das im Zuge der Entwicklung von 6G-Netzwerken entstanden ist und als virtuelle Echtzeit-Abbildung der physischen Netzwerkumgebung fungiert. Durch die Nutzung des NDTs erhält der Anomalieerkennungsprozess eine dynamische und präzise Referenz, die eine genauere und kontextuell informierte Identifikation von Spektrumanomalien ermöglicht.

Die weiteren Beiträge dieser Arbeit konzentrieren sich auf die Untersuchung und Bewertung des vorgeschlagenen Konzepts, die in zwei Phasen durchgeführt wurden. Zunächst wurden Simulationen implementiert, um einen Machbarkeitsnachweis zu erbringen, wobei die empfangene Leistung als Indikator für Spektrumanomalien verwendet wurde. Diese Simulationen zeigten die Machbarkeit des Konzepts und lieferten erste Erkenntnisse, obwohl die praktische Relevanz der empfangenen Leistung als Indikator aufgrund ihrer groben Granularität begrenzt ist. Auf dieser Grundlage führt die zweite Phase die Übertragungsfunktion des Funkkanals als einen empfindlicheren und informativeren Indikator innerhalb des vorgeschlagenen Rahmens ein. Seine Eignung wurde durch eine Kanalmesskampagne in Anwesenheit eines Störsenders validiert, die die Empfindlichkeit der Kanalübertragungsfunktion gegenüber Störungen bestätigte. Durch die Nutzung dieser Daten in einem Erkennungsrahmen übertraf der vorgeschlagene Ansatz die Basismethoden signifikant. Weitere Validierungen durch Link-Level-Simulationen zeigten die Robustheit der Übertragungsfunktion-basierten Erkennung, insbesondere in Szenarien mit großen Bandbreiten und niedrigen Signal-zu-Rausch-Verhältnissen, in denen dieser Ansatz die Benchmark-Methode konsequent übertraf.

Diese Ergebnisse stellen einen wichtigen Schritt zur Verbesserung der Widerstandsfähigkeit privater drahtloser Netzwerke in industriellen Umgebungen dar und gewährleisten einen robusten Betrieb selbst unter widrigen Umständen. Durch die Nutzung von NDTs legt diese Arbeit den Grundstein für adaptivere und intelligentere Spektrumüberwachungslösungen in Kommunikationssystemen der nächsten Generation.

Acknowledgment

This work would not have been possible without the support of many people whom I would like to thank.

First, I want to express my gratitude to my doctoral advisor, Prof. Gerhard Fettweis, for granting me the opportunity to pursue my PhD at the Vodafone Chair Mobile Communications Systems and for providing insightful discussions and guidance throughout the journey.

I also want to thank my group leader, Dr. Philipp Schulz, for his support and mentorship throughout this time. His insightful feedback, encouragement, and willingness to engage in discussions were very valuable to me throughout my doctoral journey.

I would like to extend my thanks to my colleagues at the chair, who fostered a warm and collaborative atmosphere, making my time here truly enjoyable. This thesis would also not have been possible without the support of the administrative team. I greatly enjoyed the collegial environment and the excellent research conditions at the chair. My appreciation also goes to the partners involved in 6G-CampuSens, who made this project a positive and collaborative experience.

Special thanks go to my wife, Delia, and my family and friends for their unconditional support. Their patience, encouragement, and belief in me have been a constant source of strength. I am grateful that they were always there when I needed them most and that they helped me find a balance during my PhD.

Contents

1 Introduction **1**
- 1.1 Motivation . . . 1
- 1.2 Problem Definition . . . 2
- 1.3 Contribution & Outline . . . 5

2 Related Work **7**
- 2.1 Network Digital Twins in the Context of 6G . . . 7
- 2.2 Spectrum Anomaly Detection Approaches . . . 8
  - 2.2.1 Machine Learning Approaches . . . 9
  - 2.2.2 Other Approaches . . . 11
- 2.3 Conclusion . . . 12

3 System Model **15**
- 3.1 Proposed Concept of a Network Digital Twin for Spectrum Anomaly Detection . . . 15
  - 3.1.1 Rationale for Network Digital Twins in Spectrum Anomaly Detection 15
  - 3.1.2 Architecture of the Anomaly Detection System . . . 16
  - 3.1.3 Detecting Anomalies as Deviations between the Real World and the Digital Twin . . . 20
- 3.2 Evaluation Metrics . . . 23

4 Leveraging the Received Power for Anomaly Detection **27**
- 4.1 Initial Insights Using a Log-Distance Path Loss Model . . . 28
  - 4.1.1 System Model Specification . . . 28
  - 4.1.2 Adjustment and Specification of the Digital Twin . . . 30
  - 4.1.3 Detection Methodology . . . 33
  - 4.1.4 Results . . . 37
- 4.2 Investigations Using Ray Tracing Simulation . . . 39
  - 4.2.1 An Introduction to Ray Tracing . . . 40
  - 4.2.2 System Model Specification . . . 41
  - 4.2.3 Adjustment and Specification of the Digital Twin . . . 45
  - 4.2.4 Detection Methodology . . . 46

4.2.5 Results . . . 46
4.3 Conclusion . . . 48

5 Enhancing the Detection Fidelity Using Detailed Channel Information 53
5.1 Introduction and General Considerations on Leveraging Detailed Channel Information for Spectrum Anomaly Detection . . . 54
5.1.1 Key Idea . . . 54
5.1.2 Detection Concept . . . 56
5.1.3 Prerequisites and Further Considerations . . . 57
5.2 Channel Measurements under the Impact of a Jammer . . . 61
5.2.1 Measurement Scenario and Setup . . . 62
5.2.2 Initial Insights into the Measurement Data . . . 65
5.3 Spectrum Anomaly Detection Using the Channel Frequency Response in an Experimental Setup . . . 66
5.3.1 System Model Specification . . . 67
5.3.2 Detection Methodology . . . 71
5.3.3 Results . . . 81
5.3.4 Complexity Considerations . . . 86
5.3.5 Intermittent Conclusion . . . 86
5.4 Investigating Channel-based Anomaly Detection on the Link Level . . . 87
5.4.1 System Model Specification . . . 88
5.4.2 Data Preparation and Analysis . . . 94
5.4.3 Detection Methodology . . . 97
5.4.4 Results . . . 100
5.4.5 Intermittent Conclusions . . . 102
5.5 Summary and Conclusion . . . 103

6 Conclusion and Outlook 107
6.1 Key Results and Conclusion . . . 107
6.2 Future Work . . . 109

A Appendix 111
A.1 Jammer Configuration by Measurement Round . . . 111
A.2 Architecture and Hyperparameters of the Autoencoder for the Channel Frequency Response . . . 112

Bibliography 115

Publications of the Author 127

List of Figures 129

List of Tables 131

List of Symbols 133

List of Acronyms 135

1 Introduction

1.1 Motivation

Wireless communications have become an essential part of everyday life, seamlessly connecting people and devices. This transformative technology is now rapidly gaining traction in industrial sectors, where private wireless networks are emerging as a foundational element of the factory of the future. By enabling unprecedented levels of flexibility, these networks help to unlock significant improvements in efficiency and cost savings [Ros+18; LPD19; WBV21; Kie+22; Mic+25]. Key applications include flexible production lines, cooperative robots, and teleoperation use cases which demonstrate the vast potential of wireless connectivity to revolutionize manufacturing processes [Ale+19; Gun+21; Che+21].

An attractive option for deploying such wireless networks is the operation in licensed spectrum. Licensed spectrum provides exclusive access rights which enable more predictable network performance compared to unlicensed spectrum [Are+24]. In this context, regulatory authorities have allocated dedicated frequency bands specifically for local and private network deployments. One prominent example is the 3.7 – 3.8 GHz band in Germany, which is reserved for industrial and campus networks [BNe23].

However, the benefits of wireless connectivity come at a cost. Unlike wired systems, its inherently open transmission medium makes it vulnerable to intentional attacks such as jamming and spoofing or other external disturbances such as misconfigured neighboring networks or transmitters. Particularly critical use cases within industrial environments present attractive targets for adversaries aiming to disrupt operations. A variety of attacks have been described [Lic+18; AF20; PZ22] and have also been executed successfully in the literature [Ali+22; BM22; Flo+23; Sko+24]. Regardless of its cause and no matter whether the wireless network operates in licensed or unlicensed spectrum, such interfering signals can severely degrade the communication quality or even interrupt the network operation. Keeping the industrial processes that rely on the private networks in mind, this can lead to costly production downtimes [Mic+25]. For this reason, it is essential to constantly monitor the spectrum of the wireless network [Mic+25] with the

aim of detecting any kind of signal that is emitted illegitimately in the licensed band, referred to as an anomaly.

The key objective of this thesis is to develop a detection approach that is signal-agnostic – meaning it does not rely on identifying specific signal characteristics or patterns typically assumed in state-of-the-art jammer detection methods [Loh+24]. To maintain high detection fidelity despite this requirement, the proposed concept leverages contextual awareness in the detection process, incorporating information from multiple domains that are implicitly linked to the spectrum. In the scope of this thesis, the term *detection fidelity* is defined as a generic measure for the capability of a system to detect spectrum anomalies. It is used here as an umbrella term for the various metrics that are commonly applied for the evaluation (accuracy, receiver operating characteristics (ROC), $f1$-score, ...) of detection problems.

One promising approach to integrate contextual awareness is hereby to leverage a network digital twin (NDT), a concept that has gained increased attention with the rise of sixth generation (6G) mobile network research. This concept is especially appealing for private networks in the industrial domain, where extensive information is available due to automated processes. Potentially, even a digital twin (DT) for production purposes may already be in operation, providing valuable contextual data to enhance the detection of spectrum anomalies. Based on this motivation, a detailed specification of the problem is provided in the next section.

1.2 Problem Definition

This thesis focuses on spectrum anomaly detection in licensed band private networks. The term "spectrum" refers to a range of electromagnetic frequencies and the signals transmitted within it. A licensed band is a portion of the radio spectrum allocated by a regulatory body to a specific entity [Rag22]. Within this context, devices authorized by the licensed entity to transmit in the band are referred to as legitimate transmitters (LTXs) throughout this thesis. Despite the regulatory framework, there is no guarantee that unauthorized signals will not be transmitted illegally within a licensed band. In this thesis, any illegitimate transmission of a radio signal in a licensed band is considered an anomaly. Consequently, an indicator for identifying such unauthorized transmissions needs to be developed. Considering a quantitative metric for this purpose, the anomaly detection problem can be interpreted as an outlier detection problem. A classical and widely used definition for an outlier is provided by D. Hawkins:

> "[An outlier is] an observation which deviates so much from other observations as to arouse suspicions that it was generated by a different mechanism."
> - [Haw80]

Relating this to anomaly detection, it implies that the indicator metric deviates substantially from the scenario where only legitimate signals are present whenever an illegitimate signal occurs, with the additional transmitter representing the distinct generation mechanism. Thus, the objective is to find a meaningful indicator which is sensitive to the presence of an illegitimate transmitter.

As outlined in Sec. 1.1, interfering signals are an issue for (almost) all wireless networks. However, the detection of such spectrum anomalies is particularly relevant for private networks such as in factories, which need to fulfill demanding requirements and where quality of service degradation has severe consequences. Thus, the scope of this thesis is explicitly limited to wireless networks in factories or similar scenarios. Hence, the architecture of the detection system and simulation environments are designed accordingly. For the simulations, network specifications loosely orient on regulations for non-public networks (NPNs) in Germany. Similar NPN regulations have been established in many countries worldwide, making the proposed detection system architecture and simulation results broadly transferable across different regulatory environments. To provide a better understanding of the anomalies that shall be detected, specific examples that are in scope and out of scope are provided in Tab. 1.1.

Tab. 1.1.: Relevant and out of scope examples of spectrum anomalies

In scope	Out of scope
5G NPN with unintended interference from another close-by network	Unlicensed band scenarios (e.g., coexistence of WiFi and Bluetooth), where interfering signals are expected
All kinds of jamming (naive and smart)	Denial of service attacks using legitimate devices, e.g., generate extreme traffic demands with legitimate devices
Spoofing / overshadowing attacks [LN21]	

To provide additional context, the important case of jammers is examined in greater detail. Jamming signals can manifest in various forms, with common classifications distinguishing characteristics in time, frequency, and signal intelligence. Fig. 1.1 presents three example jammer types within a time-frequency grid. The first type is the sweep jammer, a basic example that can be easily implemented without specific knowledge of the target system. This jammer is typically straightforward to detect, as its pattern

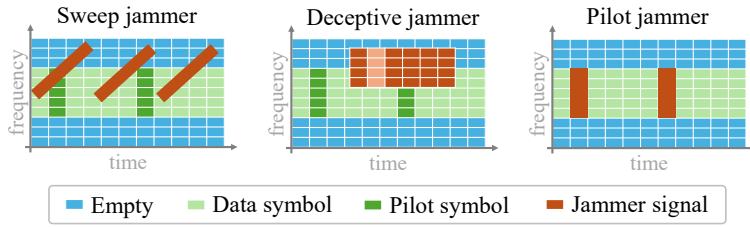

Fig. 1.1.: Exemplary jammer types visualized in a time-frequency grid.

markedly deviates from the standard transmission pattern. More complex is the deceptive jammer, which conceals itself by transmitting signals that mimic legitimate ones; such signals can, for instance, be generated using MATLAB and emitted via a software-defined radio (SDR). The final type represents so-called smart jammers, which possess extensive system knowledge, enabling them to synchronize with the target system and selectively disrupt specific signal components, such as pilot symbols. These smart jammers are considered highly effective while remaining difficult to detect. This overview serves only as a brief introduction, given the field's considerable breadth. Interested readers are referred, for example, to [PZ22; Cla11; Lic+18].

Having defined what is to be detected, further constraints need to be clarified. From the impact perspective, three degrees of anomaly severity can be defined. The first one is a very weak anomaly that causes no or only a negligible impact. In the intermediate case, the anomaly causes a significant impact on the system's performance, for example, decreased throughput or increased latency. Yet, a data exchange via the wireless link is possible. Since there is still communication and therefore cooperation possible, a detection of an anomaly in this stage is crucial in order to execute coordinated countermeasures, for instance, switching the channel, the radio access technology, or entering a controlled safety mode on the application side. In the most severe case, the anomaly signal is rather strong and completely interrupts the communication. This makes it difficult to take countermeasures, but still, the anomaly detection helps to quickly identify the root cause in the troubleshooting process. From those considerations, it can be concluded that the objective is not only to detect anomalies of the last category, but a particular emphasis should be on the intermediate case, where the detection is key to maintaining a smooth system operation. Overall, it can be said that for an intentional jammer there is a tradeoff between impact and detectability. Please note that since jamming is the most prominent case of spectrum anomalies, and spectrum anomaly detection should therefore inherently be able to detect jammers, the terms *jammer* and *spectrum anomaly* are used interchangeably in this thesis.

1.3 Contribution & Outline

The increasing importance of wireless connectivity, particularly in industrial settings, draws attention not only to the question of how the communication requirements can be fulfilled, but also how they can be fulfilled in a *resilient* way. Hereby, this thesis contributes in the following ways:

- An overview of recent works on spectrum anomaly detection and network digital twins (NDTs) is provided in **Chapter 2**.
- Based on this, a novel concept for detecting spectrum anomalies in licensed band private networks is proposed in **Chapter 3**. The concept is based on the principle that an NDT is implemented which estimates some representation of the spectrum. The estimation is compared against measurements in the real world, and significant deviations indicate spectrum anomalies. The proposed concept allows to detect interfering signals without further specification of the characteristics of the signal that is to be detected. In the chapter, the system architecture is discussed and the abstract procedure is presented.
- The focus in **Chapter 4** is on gaining initial insights from simulations when using the received power as indicator for spectrum anomalies. The system model is refined accordingly and the concept is evaluated twofold using simulation. Initially, a simple yet general log-distance path loss (LDPL) model is employed, and afterwards, ray tracing in a specific factory-like scenario is utilized. The detection in both simulation frameworks is evaluated eventually.
- To enhance the detection fidelity, the channel represented by the channel frequency response (CFR) is employed as indicator for spectrum anomalies in **Chapter 5**. A channel measurement campaign under the presence of a jammer has been executed therefore, covered in the first part of this chapter. In the second part, jamming detection is investigated using the pure channel data. The chapter is concluded by link-level simulations that utilize the measured channel data.
- **Chapter 6** concludes this work, highlights relevant findings and points out potential topics worthwhile further investigation.