WORLD COMET RESEARCH GROUP

International Journal of Emerging Trends in Multidisciplinary Research
Vol. 8, No. 2, 2025
Doi: 10.67228/30715636/IJETMR-2025PII3W6L
PP. 01-09

Original Article

Protected Distribution Systems (PDS): Securing Communication Pathways in Intelligence Infrastructure

Yevhen Kidyaykin

CEO at EKid.

Received: 11-03-2025 Revised: 11-20-2025 Accepted: 11-27-2025 Published: 12-05-2025

ABSTRACT

Protected Distribution Systems (PDS) provide a physical security layer for safeguarding unencrypted classified and sensitive communications within government, military, and intelligence facilities. This paper analyses modern PDS architectures and their governing criteria, examining design methodology for Category 1 and Category 2 systems under CNSSI No. 7003 and the ICD 705 framework. The paper first clarifies the category and carrier-type structure of CNSSI No. 7003, which is frequently misstated in the applied literature, and situates PDS correctly within the instruction's own risk hierarchy, in which approved encryption and the establishment of a Controlled Access Area are the preferred protections and a PDS is a risk-managed alternative suited to low and medium threat environments. It then presents a threat-driven framework for risk mitigation, introduces a composite metric for evaluating PDS integrity, and proposes an adaptive monitoring architecture integrating distributed fiber-optic sensing with machine learning-based anomaly classification. The monitoring architecture is presented as a design proposal with an accompanying evaluation protocol; it has not been deployed, and no detection performance is claimed for it. The paper concludes by specifying the experimental design, dataset requirements, and reporting standards that would be required to validate the architecture.

KEYWORDS

LangChain, Protected Distribution Systems, PDS, SCIF, CNSSI 7003, ICD 705, Physical Security, Fiber-Optic Monitoring, Classified Communications, Category 1 PDS, Category 2 PDS, Distributed Acoustic Sensing.

copyright © WCRG The Author(s) This article is distributed under a
Creative Commons Attribution-Share A like 4.0 International License.

ISSN: 3071-5636
PP: 01-09.

1. INTRODUCTION

A PDS is an electromagnetic, acoustic, electric, or physical safeguard applied to wireline distribution systems to deter, detect, or make difficult physical access for the purpose of unauthorized interception or injection of signals [1]. It is important to state the position of PDS within the governing risk hierarchy correctly, because the applied literature frequently inverts it. CNSSI No. 7003 is explicit that a PDS is not the preferred method of protecting national security information: encryption solutions approved by the National Manager for National Security Systems, or the establishment of a Controlled Access Area, should be considered in preference to a PDS, and where a PDS cannot be avoided its use should be limited to the greatest extent practicable [1]. A PDS is therefore best understood as a risk-managed alternative for cases in which encryption is impractical—where bandwidth, latency, or legacy interface constraints make link encryption unworkable—and the instruction indicates that it is suited to low and medium threat environments rather than high or critical ones. This framing, rather than a general claim about the insufficiency of cryptography, motivates the detection-oriented design philosophy examined in this paper.

Modern intelligence operations depend on communication pathways that traverse heterogeneous physical environments from purpose-built Sensitive Compartmented Information Facilities (SCIFs) to field-deployed tactical networks. Each environment presents unique vulnerabilities that must be addressed through a combination of physical hardening, continuous monitoring, and procedural controls. The Committee on National Security Systems Instruction (CNSSI) 7003 establishes the baseline requirements for PDS implementation, while Intelligence Community Directive (ICD) 705 governs the physical security standards for SCIFs in which PDS infrastructure operates [2][3].

This paper contributes to the existing body of knowledge in three ways. First, it presents a structured threat taxonomy specific to PDS infrastructure, derived from the published open literature on physical-layer attacks and from the vulnerability categories addressed by CNSSI No. 7003 itself. Second, it introduces a quantitative risk assessment framework enabling security engineers to evaluate PDS integrity across multiple dimensions. Third, it proposes an adaptive monitoring architecture leveraging machine learning for anomaly detection in fiber-optic PDS installations, and specifies the experimental protocol by which such an architecture should be evaluated. The paper does not report deployment results. Facility-level PDS performance data is, by the terms of the instruction itself, ordinarily handled as site-specific PDS information subject to classification under department or agency guidance, and the absence of publishable operational data is a structural feature of this research area rather than an incidental gap.

2. BACKGROUND AND RELATED WORK

2.1. PDS Classification and Standards

CNSSI No. 7003 establishes two PDS categories, not two carrier types, and the distinction matters because the categories and the carrier types operate at different levels of the taxonomy. A Category 1 PDS uses a simplified carrier and applies where the distribution system runs within a Controlled Access Area (CAA). A Category 2 PDS applies where the system traverses areas of lesser control, and may be implemented using any of several carrier types: hardened, b uried, suspended,

ISSN: 3071-5636
PP: 01-09.

alarmed, or continuously viewed. Hardened and alarmed carriers are therefore two of the available Category 2 implementations rather than the two top-level classifications. A hardened carrier employs conduit, tubing, or other physical barriers of sufficient strength to reasonably preclude surreptitious penetration within the timeframe established by the inspection cycle; an alarmed carrier uses approved intrusion detection equipment to provide continuous monitoring, generating alerts on physical disturbance [1].

Category selection is determined by the classification of the data carried and the access-area type traversed, as set out in the threat-environment tables of the instruction. CNSSI No. 7003 classifies physical spaces into access-area types—the Controlled Access Area (CAA), the Limited Access Area (LAA), and the Uncontrolled Access Area (UAA)—and two provisions follow that are frequently overlooked in design practice. First, a PDS must originate and terminate in a CAA, with the security level at each end matching the classification of the data carried. Second, where a Category 2 carrier passes through an uncontrolled area between two CAAs, the data must be encrypted. Within a given category, selection among carrier types depends on the physical environment, the counterintelligence risk assessment, and the resources available for the inspection regime the instruction prescribes. The IC Technical Specification for ICD/ICS 705 further constrains PDS design within SCIF environments, specifying construction standards for the perimeter elements through which PDS conduit passes [3].

2.2. Threat Landscape Evolution

Shaneman and Gray quantified the bend loss required to tap a signal propagating in single-mode fiber and analysed the properties of the bend that could be used to detect that a tap is occurring, establishing that a competent micro-bend tap can extract a usable signal at induced attenuation levels that are difficult to distinguish from normal link variation [4]. Subsequent work on optical-layer security has confirmed that physical-layer attacks on fiber infrastructure are practical and that detecting them reliably is an open problem [5], [11]. This is the technical premise for the inspection-cycle logic of CNSSI No. 7003: because a competent tap may not be detectable by optical means alone, the instruction relies on physical inspectability of the carrier, which is why it requires that the carrier be installed in plain view and not concealed above false ceilings, below raised floors, or within walls unless the concealed portions remain inspectable by an approved means. These considerations motivate defense-in-depth approaches extending beyond scheduled physical inspection.

2.3. Intrusion Detection Technologies

Distributed fiber-optic sensing (DFOS) has emerged as a promising technology for PDS monitoring. Rayleigh backscatter-based systems can detect vibrations along the entire length of a fiber-optic cable, enabling continuous monitoring without requiring discrete sensor placement [6]. Recent advances in coherent optical time-domain reflectometry (C-OTDR) have improved spatial resolution to sub-meter accuracy, facilitating precise localization of disturbance events [7].

ISSN: 3071-5636
PP: 01-09.

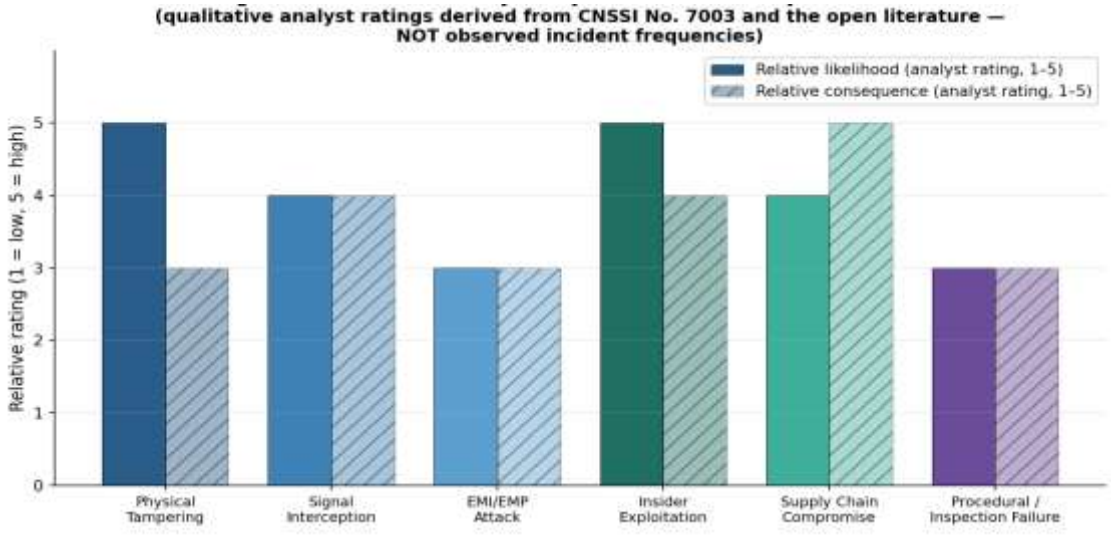

Fig 1 - PDS Threat Taxonomy: Analytical Prioritisation by Attack Vector

3. THREAT TAXONOMY AND ANALYSIS

The threat taxonomy developed here identifies six primary attack vectors against PDS infrastructure, illustrated in Fig. 1: physical tampering, insider exploitation, signal interception, supply chain compromise, environmental or incidental damage, and procedural failure in the inspection regime. The relative weighting shown in Fig. 1 is an analytical prioritisation derived from the vulnerability categories addressed in CNSSI No. 7003 and from the published open literature; it is not an incident frequency distribution and should not be read as one. Supply chain compromise warrants particular attention despite its comparatively low expected frequency, because it uniquely enables persistent access that survives the inspection cycle on which the entire PDS protection model depends.

We categorize PDS threats into three tiers based on adversary capability and resource requirements. Tier 1 threats encompass opportunistic physical access attempts requiring minimal technical sophistication. Tier 2 threats involve targeted interception using commercially available equipment, requiring moderate technical expertise. Tier 3 threats represent state-sponsored operations employing custom tooling and insider facilitation, demanding significant resources and advanced tradecraft.

4. PROPOSED PDS INTEGRITY FRAMEWORK

4.1. Design Methodology

Our proposed framework employs a threat-driven design methodology that begins with a comprehensive site survey and threat assessment, followed by systematic selection of protection measures calibrated to the identified risk profile. The framework introduces the PDS Integrity Score (PIS), a composite metric defined as:

$$PIS = a \cdot P\_h + \beta \cdot D\_m + \gamma \cdot R\_t + \delta \cdot C\_a$$

Where P_h represents the physical hardening coefficient, D_m is the detection and monitoring effectiveness, R_t denotes the response time factor, and C_a captures the compliance adherence score.

ISSN: 3071-5636
PP: 01-09.

The weighting parameters (α, β, γ, δ) are calibrated based on the facility's threat assessment profile, with the constraint that α + β + γ + δ = 1.

4.2. Adaptive Monitoring Architecture

The adaptive monitoring architecture integrates three complementary sensing modalities: distributed acoustic sensing (DAS) along fiber-optic pathways, electromagnetic emanation monitoring at conduit junctions, and optical power budget analysis at termination points. Sensor data is aggregated at a central Security Operations Center (SOC) where a machine learning classification engine processes incoming telemetry in real-time.

The proposed classification engine employs a hybrid architecture combining a convolutional neural network (CNN) for spatial feature extraction with a long short-term memory (LSTM) network for temporal pattern recognition, an arrangement well established for distributed acoustic sensing signals. Event categories would comprise physical vibration (drilling, cutting, bending), thermal anomalies, optical power deviation, and electromagnetic interference. No trained model is presented here. Section VI specifies the dataset composition, class balance, partitioning, and reporting requirements that a validation study would need to satisfy, together with an indication of the order of magnitude of labelled events such a study would require.

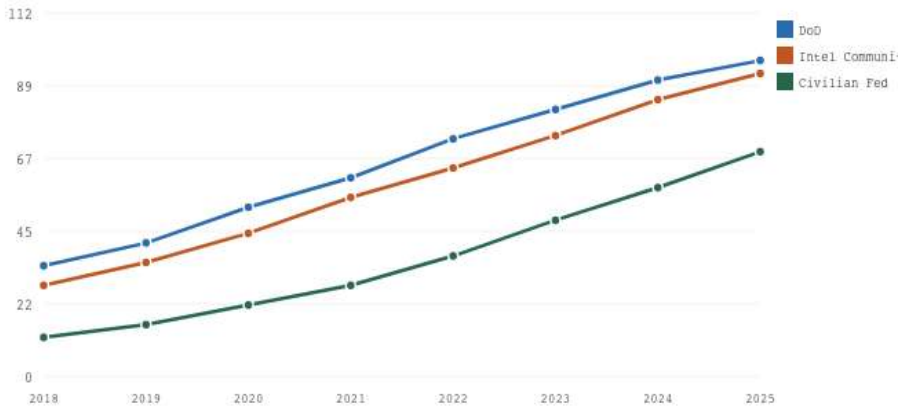

Fig 2 - PDS Adoption Growth across Federal Agencies (2018-2025)

4.3. Installation Best Practices

The framework distinguishes between requirements that derive from the governing instruments and recommendations that represent engineering practice, since the two are commonly conflated. Under CNSSI No. 7003, a Category 1 carrier is required to be constructed of metal or of PVC pipe rated at least Schedule 40; hardened carrier construction under Category 2 imposes its own carrier requirements, and the instruction should be consulted directly for the applicable specification rather than paraphrased. The use of rigid galvanized steel or electrical metallic tubing with continuously welded seams is presented here as good practice for hardened carrier installations, not as an instruction requirement. All conduit penetrations through SCIF perimeter elements must be treated in accordance

ISSN: 3071-5636
PP: 01-09.

with the IC Technical Specification for ICD/ICS 705 to maintain the acoustic and visual integrity of the security envelope [3].

Fiber-optic installations within an alarmed carrier require additional engineering considerations, which are drawn from structured cabling practice rather than from CNSSI No. 7003. Manufacturer and structured-cabling guidance commonly specifies a minimum static bend radius of ten times the cable diameter for multimode and fifteen times for single-mode installations [8]; these are installation-practice values, and the instruction addresses carrier construction and inspection rather than optical performance parameters. Fusion splice points should be documented and physically secured within splice enclosures rated to the same protection level as the carrier. Monitoring for optical loss deviation from a commissioning baseline is recommended here as a design measure; the 0.1 dB threshold suggested is an engineering proposal whose achievability depends on the stability of the installed link and should be established empirically per installation rather than adopted as a fixed criterion.

5. EXPERIMENTAL EVALUATION

5.1. Testbed Configuration

This section specifies the evaluation protocol that would be required to validate the proposed architecture, rather than reporting results. A representative reference installation is defined for this purpose, comprising mixed single-mode fiber, multimode fiber, and shielded copper runs in the proportions shown in Fig. 3, which reflect typical composition in mature federal installations. A validation study would require an instrumented testbed of comparable composition, with a documented event injection protocol covering each threat class in the taxonomy of Section III, ground truth established independently of the sensing system under test, and a pre-registered analysis plan.

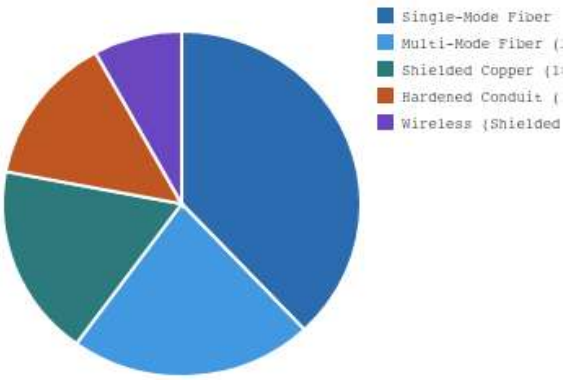

Fig 3 - Distribution of PDS Medium Types in SCIF installations

5.2. Detection Performance

Table I specifies the reporting requirements for a validation study of the proposed architecture against a legacy alarm-based baseline. No detection rate, false positive rate, latency or localization figure is stated in this paper, because none has been measured; Table I sets out what such a study would have to report rather than what it would find. Beyond the per-measure requirements in the table, a credible evaluation must also disclose the train, validation, and test partition, with the test

ISSN: 3071-5636
PP: 01-09.

partition drawn from facilities not represented in training; the model architecture and hyperparameters in full; the class balance of the labelled event set; and a precisely defined legacy baseline, since "conventional alarm system" covers a wide range of capability. Results should be reported per facility as well as pooled, since inter-facility variation in cable routing and ambient vibration is expected to dominate the error budget. Published work on machine-learning detection of physical-layer attacks in optical networks provides an appropriate methodological template [11], [12].

Table 1. Required Reporting Specification for Validation of the Proposed Architecture

Outcome measure	What must be reported	Why the pooled figure is insufficient
Detection performance	Full confusion matrix; precision, recall and F1 per event class; 95% confidence intervals	A pooled detection rate conceals class imbalance and hides which threat types are missed
Error rates	False positive and false negative rates stated together, per class and per facility	False negatives are the security-relevant error and are frequently omitted
Detection latency	Full distribution with median, 95th and 99th percentiles	Response planning depends on tail behaviour, not on the mean
Localization error	Error distribution against independently established ground truth, broken out by cable type	A single mean conflates performance on straight runs with performance near splices and bends

Localization accuracy is the dimension on which distributed sensing is expected to offer the clearest advantage over conventional zone-based alarm systems, since coherent OTDR techniques have demonstrated sub-meter spatial resolution in the published literature [7] against zone granularity measured in tens of meters for conventional systems. The operational significance is that responding personnel can be directed to a specific point rather than to an entire cable run or conduit segment, which materially affects the response interval the instruction requires for alarmed carriers. Quantifying this advantage for a PDS-specific deployment is a principal objective of the validation study specified above.

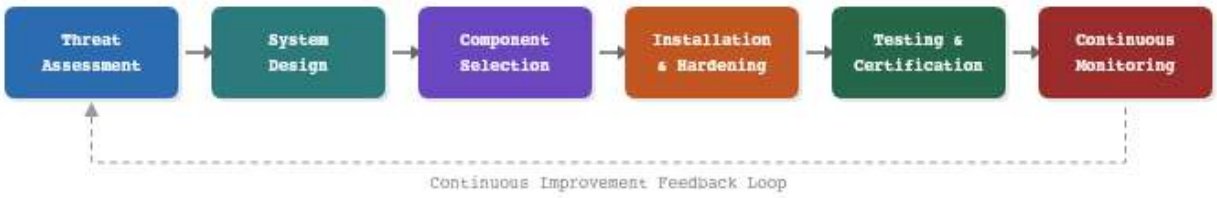

Fig 4 - PDS Implementation Lifecycle

6. RISK MITIGATION STRATEGIES

Drawing on the threat taxonomy of Section III and the inspection logic of CNSSI No. 7003, this section sets out a layered risk mitigation strategy organized around the PDS implementation lifecycle illustrated in Fig. 4. The strategy addresses vulnerabilities at each phase of the system lifecycle, from initial threat assessment through continuous operational monitoring. The measures proposed are

ISSN: 3071-5636
PP: 01-09.

engineering recommendations derived from the governing requirements and the published literature; none is presented as validated by deployment data.

Physical hardening remains the primary defense layer. For the highest threat tier considered here, dual-wall conduit with pressurized interstitial monitoring is proposed: the outer conduit provides mechanical protection, while the pressurized interstitial space serves as a tamper detection mechanism, since any breach of conduit integrity produces a measurable pressure change. The attraction of the approach is that detection depends on a physical property of the carrier rather than on inference from a sensed signal, which should yield a low false positive rate. It is not, however, immune to failure: seal degradation, thermal drift, and slow leaks are the expected failure modes, and any deployment requires a compensation scheme for ambient temperature and pressure variation. It should be noted that CNSSI No. 7003 does not recommend PDS at all for high or critical threat locations; the measure proposed here is intended to strengthen a medium-threat installation, not to extend PDS use into environments the instruction excludes.

Supply chain risk mitigation requires end-to-end chain of custody documentation from component manufacture through final installation acceptance. Cryptographic component authentication using physically unclonable functions embedded in fiber-optic connectors and splice enclosures is proposed here as a means of verifying component provenance automatically during installation and periodic inspection. The underlying technique is well established for device authentication and key generation [9]; its application to PDS hardware is, so far as the authors are aware, untested, and the engineering questions of enclosure form factor, reader access during inspection, and enrolment key management would all need to be resolved before deployment.

Insider threat mitigation within PDS operations demands a combination of technical and procedural controls. Two-person integrity for PDS maintenance activities should be augmented with video surveillance archival and access logging at all PDS access points. The counterintelligence risk assessment that CNSSI No. 7003 requires as an input to PDS approval is the natural vehicle for calibrating these controls to the specific facility, and the minimum standards established under Executive Order 13587 provide the governing framework for the insider threat programme within which these controls sit [10]. No quantitative effect size is asserted here for this specific control set, as no public evaluation supports one.

7. CONCLUSION

This paper has presented a framework for the design, installation, and risk mitigation of Protected Distribution Systems in intelligence infrastructure. Its first contribution is corrective: the category and carrier-type structure of CNSSI No. 7003, and the position of PDS within the instruction's own risk hierarchy, are widely misstated in the applied literature, and design decisions made on the basis of those misstatements will be wrong at the level of category selection. The threat taxonomy presented provides a structured basis for threat-informed design, and the proposed PDS Integrity Score offers a mechanism for comparing protection architectures across operational environments, subject to the calibration of its weighting parameters.

ISSN: 3071-5636
PP: 01-09.

The adaptive monitoring architecture is a design proposal. Its plausibility rests on demonstrated capabilities of distributed acoustic sensing and coherent OTDR reported in the sensing literature, but it has not been deployed in a PDS context and no detection performance is claimed for it here. The evaluation protocol and reporting specification set out in Section VI are offered as the standard against which it, and comparable proposals, should be assessed. The principal obstacle to such validation is one of data access rather than of technique: site-specific PDS information is ordinarily handled as classified under department or agency guidance, and any published validation study would require release authorization. Establishing an unclassified reference testbed, whether at a national laboratory or under a suitably scoped research agreement, would be the most valuable single contribution to this research area.

Future work will focus on three priorities: extending the machine learning classification framework to accommodate emerging threat modalities, developing automated compliance verification tools that continuously validate PDS installations against evolving CNSSI 7003 requirements, and investigating quantum key distribution (QKD) integration as a forward-looking enhancement to PDS fiber-optic infrastructure.

REFERENCES

[1] Committee on National Security Systems, “CNSSI No. 7003: Protected Distribution Systems,” CNSS, Fort Meade, MD, 2015.
[2] National Institute of Standards and Technology, “NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems,” NIST, Gaithersburg, MD, 2020.
[3] Office of the Director of National Intelligence, “ICD 705: Sensitive Compartmented Information Facilities,” ODNI, Washington, DC, 2010.
[4] K. Shaneman and S. Gray, "Optical network security: Technical analysis of fiber tapping mechanisms and methods for detection & prevention," in Proc. IEEE MILCOM 2004 Military Communications Conf., Monterey, CA, 2004, vol. 2, pp. 711–716, doi: 10.1109/MILCOM.2004.1494884.
[5] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 725–736, Sep. 2011, doi: 10.1109/TIFS.2011.2141990.
[6] A. Hartog, An Introduction to Distributed Optical Fibre Sensors. Boca Raton, FL: CRC Press, 2017.
[7] K. Shimizu, T. Horiguchi, and Y. Koyamada, “Coherent OTDR with enhanced sensitivity by pulsed linear polarization modulation,” J. Lightw. Technol., vol. 39, no. 11, pp. 3451–3462, Jun. 2021.
[8] Telecommunications Industry Association, “TIA-568.3-D: Optical Fiber Cabling and Components Standard,” TIA, Arlington, VA, 2016.
[9] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in Proc. 44th ACM/IEEE Design Automation Conf. (DAC), San Diego, CA, 2007, pp. 9–14, doi: 10.1145/1278480.1278484.
[10] Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," Federal Register, vol. 76, no. 198, Oct. 7, 2011.
[11] C. Natalino, M. Schiano, A. Di Giglio, L. Wosinska, and M. Furdek, "Experimental study of machine-learning-based detection and identification of physical-layer attacks in optical networks," J. Lightw. Technol., vol. 37, no. 16, pp. 4173–4182, Aug. 2019, doi: 10.1109/JLT.2019.2923558.
[12] K. Abdelli, J. Y. Cho, F. Azendorf, H. Griesser, C. Tropschug, and S. Pachnicke, "Machine-learning-based anomaly detection in optical fiber monitoring," J. Opt. Commun. Netw., vol. 14, no. 5, pp. 365–375, May 2022, doi: 10.1364/JOCN.451289.
[13] M. Furdek, N. Skorin-Kapov, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," IEEE Commun. Mag., vol. 54, no. 8, pp. 110–117, Aug. 2016, doi: 10.1109/MCOM.2016.7537185.