

## Review

# Security by Light in Sensor Networks: A Structured Review of Optical and Photonic Security Mechanisms

Ramin Irani <sup>1,\*</sup> , Siamak Khatibi <sup>2</sup>  and Shahryar Eivazzadeh <sup>1</sup> 

<sup>1</sup> Department of Computer Science, Blekinge Institute of Technology, SE-371 79 Karlskrona, Sweden; shahryar.eivazzadeh@bth.se

<sup>2</sup> Department of Technology and Aesthetics, Blekinge Institute of Technology, SE-371 79 Karlskrona, Sweden; siamak.khatibi@bth.se

\* Correspondence: ramin.irani@bth.se

## Abstract

Sensor networks increasingly combine exposed sensing nodes, optical communication, photonic hardware, near-sensor inference, and distributed infrastructure monitoring. This changes the security problem from protecting packets alone to establishing device provenance, measurement integrity, link confidentiality and availability, trustworthy inference, physical situational awareness, lifecycle control, and governance. This structured review with documented scoping searches examines *security by light*: mechanisms in which optical or photonic phenomena directly realize, constrain, compute, or observe a security-relevant function. The review synthesizes screened evidence across photonic roots of trust, visible-light communication and LiFi security, photonic intelligence, reservoir and chaotic photonics, and distributed photonic sensing infrastructure. Searches across arXiv, IEEE Xplore, ACM Digital Library, and Scopus yielded 228 deduplicated candidate records, of which 187 were retained as core evidence and eight as contextual evidence. To avoid overstating heterogeneous photonic work, retained records were separated into direct security evidence, security-adjacent capability evidence, background/framework evidence, and excluded records. The central result is architectural: light-enabled mechanisms are most defensible when they provide explicit, confidence-rated evidence to conventional security engineering. In this paper, confidence-rated evidence means evidence whose security interpretation is tied to a stated asset, adversary or failure mode, evidence role, validation setting, robustness limits, deployment fit, and reproducibility condition. This avoids treating optical novelty, spatial confinement, analog complexity, or high-dimensional dynamics as assurance by themselves. The paper develops an auditable taxonomy, evidence appraisal rubric, mechanism-family synthesis, integration architecture, maturity analysis, and research agenda for incorporating light-enabled mechanisms into secure sensor-networked systems.



Academic Editors: Kamran Siddique, Ka Lok Man and Zahid Akhtar

Received: 26 May 2026

Revised: 23 June 2026

Accepted: 26 June 2026

Published: 1 July 2026

**Copyright:** © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

**Keywords:** security by light; sensor networks; photonic security; visible-light communication; LiFi; physical unclonable functions; optical neural networks; reservoir computing; optical chaos; distributed fiber sensing; cyber-physical security

## 1. Introduction

Sensor networks are evolving from simple data-acquisition systems into distributed cyber-physical systems. They now combine exposed sensing nodes, optical front ends, embedded inference, gateways, cloud services, and safety-relevant decision loops. This

shift changes the security problem. A sensor network no longer needs only protected packets. It also needs trustworthy device identity, measurement integrity, resilient local inference, lifecycle control, and protection against physical manipulation of exposed sensing hardware and infrastructure. These requirements are well recognized in wireless sensor network, IoT, cyber-physical-system, and operational-technology security guidance [1–6].

At the same time, optical and photonic technologies have moved closer to the sensing edge. Modern systems increasingly use optical links, photonic integrated circuits, optical fingerprints, in-sensor processing, photonic edge intelligence, and distributed fiber sensing to acquire, transport, and interpret data [7–9]. These developments create an opportunity to reconsider sensor-network security from a hardware-and-physics perspective. Light can carry information, but it can also constrain propagation, expose tampering, generate device-specific responses, compute analog transforms, and observe physical space.

This survey uses the term *security by light* for mechanisms in which optical or photonic phenomena directly realize, constrain, compute, or observe a security-relevant function. The scope is intentionally broader than optical communication security. It includes photonic roots of trust, visible-light communication (VLC) and LiFi physical-layer security, attack-aware photonic intelligence, reservoir and chaotic photonic transforms, and distributed photonic sensing for intrusion or tamper telemetry. It excludes ordinary cryptographic protocols that merely run over an optical bearer without relying on an optical security property.

Light-enabled mechanisms can strengthen security when they are tied to explicit assets, adversaries, validation settings, lifecycle controls, and conventional security mechanisms. Optical novelty, spatial confinement, analog complexity, or high-dimensional dynamics are not security assurance by themselves. This distinction matters because the reviewed literature contains both direct security evidence and security-adjacent photonic capability. A VLC secrecy-rate paper, a photonic PUF paper, an adversarial ONN paper, a chaotic reservoir paper, and a DAS intrusion paper support different kinds of claims. Treating them as equivalent would overstate the field.

VLC and LiFi security surveys discuss leakage, jamming, rogue transmitters, and physical-layer secrecy [10,11]. PUF and hardware-security surveys analyze challenge-response behavior, unclonability, helper data, and key derivation [12,13]. Optical neural network and photonic-computing reviews focus on architectures, training, nonlinearities, and implementation constraints [14,15]. Reservoir-computing perspectives explain nonlinear dynamical processing and emerging hardware directions [16]. Distributed-fiber-sensing surveys cover infrastructure monitoring, DAS event recognition, and sensing performance [17–19]. These surveys are necessary background, but they do not by themselves provide a security-role synthesis across device identity, optical-link protection, photonic inference assurance, nonlinear optical transforms, and infrastructure telemetry for sensor-networked systems.

This survey makes five contributions:

- It defines security by light as a cross-layer security concept for sensor-networked systems.
- It provides a structured narrative review with documented scoping searches across arXiv, IEEE Xplore, ACM Digital Library, and Scopus.
- It develops a three-axis taxonomy organized by security role, optical mechanism, and deployment layer, with evidence roles used to calibrate claims.
- It gives a deep mechanism-family synthesis for photonic roots of trust, VLC/LiFi security, photonic intelligence, reservoir and chaotic photonics, and photonic sensing infrastructure.

- It proposes integration patterns, maturity criteria, explicit answers to the research questions, and a research agenda focused on attacker-aware validation, reproducible benchmarking, lifecycle integration, false-alarm control, privacy, and governance.

### *Positioning Relative to Existing Surveys*

The gap identified is that sensor-network security needs a system-layered synthesis. A designer must decide whether a photonic PUF belongs at onboarding, whether a VLC fingerprint can support transmitter authentication, whether a photonic classifier is trustworthy enough to influence policy, whether a chaotic transform has a meaningful leakage argument, and whether a DAS alarm is mature enough to change trust in nearby assets. Existing surveys typically answer one part of that question. This paper connects the parts. Table 1 positions this paper relative to adjacent survey types.

**Table 1.** Positioning of this review relative to adjacent survey types.

| Survey Type                                | Typical Focus                                                                                                                    | Why It Does Not Replace This Review                                                                                                                                                                               |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLC/LiFi security surveys                  | Optical wireless leakage, eavesdropping, jamming, secrecy rate, rogue transmitters, and channel-security countermeasures [10,11] | They treat light primarily as a communication medium and usually do not integrate optical identity, photonic inference, nonlinear transforms, and distributed sensing into a sensor-network security architecture |
| Photonic PUF and hardware-security surveys | Challenge-response behavior, unclonability, helper data, fuzzy extraction, and device identity [12,13]                           | They cover roots of trust but not optical-link protection, photonic inference assurance, or infrastructure-scale telemetry                                                                                        |
| Photonic computing surveys                 | ONN architectures, integrated platforms, calibration, nonlinearities, and scalability [14,15]                                    | They establish computing capability, but security claims require separate attacker-aware and fault-aware evaluation                                                                                               |
| Reservoir and chaos surveys                | Dynamical processing, synchronization, nonlinear memory, and chaos communication [16,20]                                         | They explain mechanism potential but not the sensor-network evidence chain from optical transform to security decision                                                                                            |
| Distributed-fiber-sensing surveys          | DAS/DFOS event recognition, telecom-fiber reuse, and infrastructure monitoring [17–19]                                           | They establish sensing maturity, but not the security logic that turns physical telemetry into trust decisions                                                                                                    |
| This review                                | Security role, optical mechanism, deployment layer, evidence quality, integration pattern, and maturity                          | It synthesizes light-enabled identity, channel protection, inference assurance, nonlinear transforms, and infrastructure telemetry under one security-first framework                                             |

The paper is organized as follows. Section 2 defines the review method. Section 3 presents security requirements and threat models. Section 4 develops the taxonomy. Sections 5–9 synthesize the five mechanism families. Section 10 presents the evidence-to-policy integration architecture. Section 11 provides the comparative evaluation, maturity analysis, and research agenda. Section 12 answers the research questions, and Section 13 concludes.

## **2. Scope and Review Method**

This article is written as a structured narrative review supported by documented scoping searches. It does not claim to be a fully exhaustive systematic review of all optical-security, photonic-hardware, and cyber-physical-security literature. The methodological aim is narrower: to identify, screen, and compare mechanism families in which light or photonic phenomena make a direct or materially relevant contribution to sensor-network security. The review therefore emphasizes traceability of the search logic, explicit separation of evidence roles, and conservative interpretation of security claims. A full PRISMA-style

systematic or scoping review protocol [21,22] was not used because the paper does not evaluate one narrowly bounded intervention, outcome, technology class, or empirical domain. Instead, it compares heterogeneous mechanism families across photonic hardware identity, optical wireless security, photonic inference, nonlinear optical transforms, and distributed sensing. For this reason, a structured state-of-the-art review with documented scoping searches was considered more appropriate than an exhaustive systematic review protocol.

### 2.1. Research Questions

The review is organized around five research questions:

- **RQ1:** Which sensor-network security functions can be implemented, strengthened, or materially informed by optical and photonic mechanisms?
- **RQ2:** Which light-enabled mechanism families have direct security evidence, and which are mainly security-adjacent enabling technologies?
- **RQ3:** Which deployment layers best match each mechanism family?
- **RQ4:** What evidence exists for attacker awareness, robustness, calibration burden, scalability, lifecycle integration, and deployment realism?
- **RQ5:** Which research gaps prevent light-enabled mechanisms from becoming dependable security controls?

### 2.2. Review Scope and Boundaries

The inclusion boundary was security-functional rather than purely optical. A record was considered in scope when it connected an optical or photonic phenomenon to at least one security-relevant function: identity and provenance, optical-link protection and keying, measurement or inference assurance, protected nonlinear transformation, intrusion or tamper telemetry, lifecycle control, or governance-relevant evidence. Ordinary cryptographic protocols that simply run over an optical channel were excluded unless the optical channel or photonic hardware materially changed the security argument.

Two boundary choices are important. First, quantum optical security and quantum key distribution were not treated as a separate mechanism family because they form a mature and specialized field with different assumptions, metrics, and deployment literature. Such records were considered only when they directly affected the sensor-network integration question. Second, light-based attacks against cameras, LiDAR, photodiodes, optical receivers, or optical front ends were considered only when they clarified measurement integrity, photonic inference assurance, or optical-link security. The paper is therefore not a general survey of optical sensor attacks, but it does use attack evidence when it changes the interpretation of a light-enabled security mechanism.

### 2.3. Databases, Search Logic, and Audit Trail

Searches were conducted in May 2026 across arXiv, IEEE Xplore, ACM Digital Library, and Scopus. IEEE Xplore and ACM Digital Library were included because sensor-network security, physical-layer security, embedded systems, and cyber-physical-security work are strongly represented there. arXiv was included to capture recent preprint-stage work in photonic intelligence, optical wireless security, and photonic hardware security. Scopus was included as the broad bibliographic index used to capture optics, photonics, sensing, and distributed-fiber-sensing records that may appear across specialist publisher platforms. Because publisher-level specialist databases such as Optica Publishing Group, SPIE Digital Library, SpringerLink, ScienceDirect, and Web of Science were not searched as independent sources, the search should be interpreted as a documented scoping strategy rather than an exhaustive systematic search across all possible venues.

Five mechanism families guided the search: photonic roots of trust; optical wireless, VLC, and LiFi security; secure sensing and photonic intelligence; reservoir and chaotic photonics for security; and photonic sensing infrastructure for intrusion monitoring. Broad standalone words such as *optical*, *photonic*, *fiber*, or *security* were avoided as independent anchors because they produced many records unrelated to the review question. Instead, searches combined mechanism terms with security-function terms. Table 2 summarizes the query logic. The core Boolean query strings used for the search are reported in Table 3. The source-specific fielding adjustments are described below, and the resulting deduplicated screening counts are reported in Figure 1 and Table 4.

**Table 2.** Search-family logic used to construct the source-specific queries. The core Boolean strings are summarized in Table 3, and the resulting deduplicated screening counts are reported in Figure 1 and Table 4.

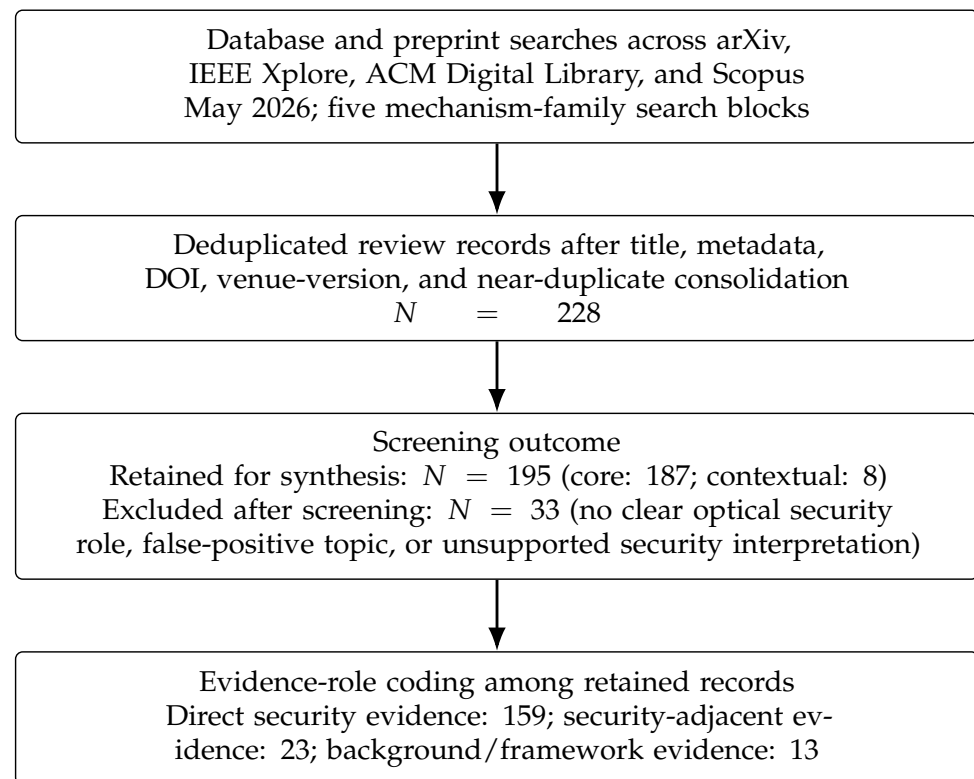
| Family                          | Mechanism Anchors                                                                                                               | Security-Function Anchors                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Photonic roots of trust         | Optical PUF, photonic PUF, speckle, scattering, optical fingerprint, silicon photonic PUF, material PUF                         | Authentication, unclonability, provenance, anti-counterfeiting, supply-chain assurance, modeling attack, helper data          |
| VLC/LiFi security               | Visible light communication, VLC, LiFi, optical wireless, LED fingerprint, optical channel, underwater visible light            | Eavesdropping, jamming, secrecy, physical-layer security, rogue transmitter, key extraction, bootstrapping                    |
| Photonic intelligence           | Optical neural network, photonic neural network, diffractive neural network, photonic accelerator, in-sensor photonic computing | Adversarial attack, fault attack, nonideality, robustness, calibration, trustworthy inference, security                       |
| Reservoir and chaotic photonics | Optical reservoir, photonic reservoir, laser chaos, electro-optic chaos, chaotic carrier, time-delay signature                  | Secure communication, concealment, leakage, key distribution, synchronization, entropy, protected transform                   |
| Photonic sensing infrastructure | Distributed acoustic sensing, distributed fiber-optic sensing, OTDR, phase-sensitive OTDR, PON sensing, DWDM sensing            | Intrusion detection, perimeter security, tamper detection, event classification, infrastructure monitoring, physical security |

**Table 3.** Core Boolean query strings used to operationalize the search-family logic. Source syntax was adjusted to each database fielding convention, but the mechanism and security-function anchors were kept consistent.

| Family                          | Representative Search String                                                                                                                                                                                                                                          |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Photonic roots of trust         | ("optical PUF" OR "photonic PUF" OR "optical fingerprint" OR speckle OR scattering) AND (authentication OR unclonability OR provenance OR "supply-chain assurance" OR "modeling attack")                                                                              |
| VLC/LiFi security               | ("visible light communication" OR VLC OR LiFi OR "optical wireless" OR "LED fingerprint") AND (eavesdropping OR jamming OR secrecy OR "physical-layer security" OR "key extraction" OR bootstrapping)                                                                 |
| Photonic intelligence           | ("optical neural network" OR "photonic neural network" OR "diffractive neural network" OR "photonic accelerator" OR "in-sensor photonic") AND ("adversarial attack" OR "fault attack" OR nonideality OR robustness OR calibration OR "trustworthy inference")         |
| Reservoir and chaotic photonics | ("optical reservoir" OR "photonic reservoir" OR "laser chaos" OR "electro-optic chaos" OR "chaotic carrier" OR "time-delay signature") AND ("secure communication" OR concealment OR leakage OR "key distribution" OR synchronization OR entropy)                     |
| Photonic sensing infrastructure | ("distributed acoustic sensing" OR "distributed fiber-optic sensing" OR OTDR OR "phase-sensitive OTDR" OR "PON sensing" OR "DWDM sensing") AND ("intrusion detection" OR "perimeter security" OR "tamper detection" OR "event classification" OR "physical security") |

The source-specific fielding reflected database constraints. arXiv searches used title and abstract fields. IEEE Xplore searches used title, abstract, and index-term variants according to query family. ACM Digital Library searches used title, abstract, and author-keyword fields. Scopus searches used title, abstract, and keyword fields. Records were exported with bibliographic metadata where possible. Search results were then screened

by title and abstract, followed by full-text or extended-context review for records retained after the first screening pass.



**Figure 1.** Search and screening flow. Core/contextual status and evidence-role status are different coding dimensions: 187 core plus 8 contextual records form the 195 retained records; these retained records were then interpreted as direct, adjacent, or background/framework evidence.

**Table 4.** Search-and-screening account used for synthesis. Counts are deduplicated at the review-record level after final manual screening.

| Family                  | N          | Core       | Contx.   | Excl.     | Dominant Evidence                                                                |
|-------------------------|------------|------------|----------|-----------|----------------------------------------------------------------------------------|
| Photonic roots of trust | 52         | 47         | 1        | 4         | Authentication, provenance, PUF modeling, and optical fingerprint evidence       |
| VLC/LiFi security       | 110        | 93         | 0        | 17        | Eavesdropping, jamming, secrecy, fingerprinting, and keying evidence             |
| Photonic intelligence   | 12         | 9          | 0        | 3         | Direct attack and fault evidence plus adjacent inference platforms               |
| Reservoir and chaos     | 20         | 10         | 7        | 3         | Protected-link evidence plus adjacent transform and source-separation evidence   |
| Fiber sensing           | 34         | 28         | 0        | 6         | Intrusion evidence plus adjacent deployment, coexistence, and standards evidence |
| <b>Total</b>            | <b>228</b> | <b>187</b> | <b>8</b> | <b>33</b> | Family-level search and screening totals                                         |

*Note:* The evidence-role coding applies only to the 195 retained records: 159 were treated as direct security evidence, 23 as security-adjacent capability evidence, and 13 as background/framework evidence. This note is separated from the family-level search totals to avoid mixing the two coding dimensions.

#### 2.4. Deduplication and Screening

A *review record* was defined as a unique intellectual contribution relevant to one mechanism family. Duplicate and near-duplicate records were consolidated using DOI, title, author list, venue, year, and substantive overlap. When conference and journal versions appeared to report the same contribution, the most complete or archival version was retained as the primary record unless the earlier version contained distinct security

evidence. Preprints were retained when they provided timely evidence not yet available in archival form, but their maturity interpretation was kept conservative.

Records were included when they met three conditions: (i) an optical or photonic mechanism was central rather than incidental; (ii) a security role, attack, fault, trust, or governance implication could be identified; and (iii) the record contributed evidence, terminology, or a boundary condition for sensor-networked systems. Records were excluded when they used generic optical, photonic, fiber, or communication terminology without a security-relevant function; when the security interpretation depended only on unsupported claims of complexity or physical obscurity; or when the work was unrelated to sensor-network deployment layers.

Figure 1 gives the screening flow used for the synthesis. The counts are reported at the deduplicated review-record level after final manual screening. Core/contextual status describes how centrally the record is used in the synthesis, whereas direct/adjacent/background status describes the evidence role assigned during appraisal. These are independent coding dimensions: a contextual record may still clarify a boundary condition, and a core record may still be direct, adjacent, or background/framework evidence depending on the claim it supports.

The final counts differ from an unfiltered bibliography. Some source records were retained as core evidence, some were retained as contextual evidence, and some were excluded even when they contained optical or security vocabulary. For example, a VLC physical-layer pitfalls paper was re-screened and retained because it explicitly analyzes VLC attacker models and the limits of adapting RF physical-layer security mechanisms to VLC [23]. By contrast, generic sensing or communication papers without a security role were excluded.

## 2.5. Evidence Roles and Appraisal

A central methodological decision was to separate evidence role from topic relevance. A paper could be relevant to photonics but weak as security evidence. Conversely, a short attack or fault paper could be highly relevant because it clarified the security boundary of a mechanism. The review uses the evidence levels in Table 5. These levels calibrate the strength of claims made in the synthesis; they are not a quality ranking of the papers themselves.

**Table 5.** Evidence appraisal rubric used to calibrate synthesis and maturity claims.

| Evidence Level                                      | Operational Coding Criteria                                                                                                                                                                        | Permitted Claim Type                                              |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Direct empirical or prototype security evidence     | The protected asset or trust function is stated; the attacker, fault, or misuse condition is explicit; a security metric is reported; and experimental, field, or prototype validation is provided | Demonstrated behavior for the tested mechanism and setting        |
| Analytic or simulation security evidence            | The threat model and metric are explicit, but validation is primarily analytical, numerical, or simulation-based                                                                                   | Conditional security performance under stated assumptions         |
| Security-adjacent architecture or platform evidence | The photonic capability is relevant to a security workflow, but the paper does not directly evaluate a security task or attacker/fault model                                                       | Feasibility, design constraint, or research opportunity           |
| Survey, standard, or framework evidence             | The source provides review synthesis, terminology, lifecycle guidance, governance framing, or standards context                                                                                    | Positioning, terminology, governance, or lifecycle interpretation |
| Excluded or weakly related evidence                 | No clear optical security role, false-positive topic, generic optical/communication result, or unsupported security interpretation                                                                 | Not used as support for paper claims                              |

To make the term *confidence-rated evidence* operational, each evidence item was interpreted as an audit record

$$e = \langle A, T, M, L, R_e, V, B, D, P, \tau \rangle,$$

where  $A$  is the protected asset or trust function,  $T$  is the adversary, fault, or misuse condition,  $M$  is the optical or photonic mechanism,  $L$  is the deployment layer,  $R_e$  is the evidence role from Table 5,  $V$  is the validation setting,  $B$  records robustness or calibration boundaries,  $D$  records deployment and lifecycle fit,  $P$  records reproducibility conditions, and  $\tau$  records freshness or context of the evidence. This notation is not intended as a cryptographic proof of security. It is a traceability device that prevents a photonic capability claim from being promoted to a security-control claim unless the asset, threat, validation, boundary, and deployment assumptions are visible.

For each retained work, extraction focused on security function, optical mechanism, adversary or failure mode, validation setting, deployment layer, evidence role, and principal limitation. The mechanism-family sections below use direct evidence for demonstrated security claims and adjacent evidence only for architectural plausibility or future research needs. Mechanism-level claims are therefore phrased according to the confidence-rating scheme in Table 6: direct evidence supports demonstrated or conditional security claims, whereas security-adjacent evidence is used only to motivate integration patterns, design constraints, or future research needs. This is why the paper sometimes treats two technically similar papers differently: one may contain an attacker model and security metric, while the other may only show photonic functionality.

**Table 6.** Confidence-rating scheme used to connect evidence roles to mechanism-level claims.

| Rating    | Typical Evidence Basis                                                                                                           | Permitted Paper Wording                                                      | Security Interpretation                                                                                       |
|-----------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| C1-Low    | Security-adjacent platform evidence, survey/framework evidence, or incomplete attacker/failure specification                     | “may support”, “is relevant to”, “creates an opportunity for”                | Architectural plausibility only; not a demonstrated security control                                          |
| C2-Medium | Analytic or simulation security evidence with explicit assumptions, or prototype evidence with limited deployment realism        | “conditionally supports”, “under stated assumptions”, “for the tested model” | Security-relevant behavior is credible but assumption-sensitive                                               |
| C3-High   | Direct empirical, prototype, or field security evidence with stated asset, attacker/failure mode, metric, and validation setting | “demonstrates in the tested setting”, “provides direct evidence for”         | Demonstrated security behavior for the validated mechanism and context, still requiring lifecycle integration |

## 2.6. Methodological Boundaries

Five limitations shape interpretation. First, database fielding and export behavior differ across sources, especially for manual exports. Second, conference and journal versions can appear as duplicate or near-duplicate records. Third, specialist optics and photonics publisher platforms were not searched independently of Scopus, so the search is auditable but not exhaustive. Fourth, mechanism families differ in validation culture: VLC security is often analytic or simulation-heavy, PUF work mixes laboratory prototypes and modeling studies, photonic intelligence includes attack/fault evidence plus platform demonstrations, chaos work mixes communication experiments and transform studies, and DFOS work includes field-like sensing evidence. Fifth, evidence maturity cannot be inferred from publication count alone. It depends on threat-model clarity, validation setting, reproducibility, environmental robustness, deployment realism, and lifecycle fit.

### 3. Security Requirements and Threat Model for Sensor-Networked Systems

Security in sensor-networked systems is not limited to confidentiality of packets in transit. Measurements are collected by exposed devices, transformed by local computation, transported through heterogeneous links, interpreted by edge or cloud services, and often used to trigger physical actions. An attack may therefore target identity, measurement provenance, optical inputs, local inference, physical infrastructure, or lifecycle processes rather than only network traffic.

#### 3.1. Security Requirements

The first requirement is trustworthy device identity and lifecycle control. Exposed sensors, gateways, replaceable optical modules, and field-installed components can be captured, counterfeited, swapped, or recommissioned over long lifetimes. IoT and WSN security guidance treats identity, configuration, update, and key management as core risks [1–3]. Photonic roots of trust are relevant because they can add physical identity evidence to enrollment, onboarding, replacement checks, and re-attestation.

The second requirement is measurement integrity and provenance. In cyber-physical systems, false, delayed, or misattributed data can be as damaging as data theft. NIST cyber-physical and operational-technology guidance treats abnormal process data, sensor manipulation, denial of service, and unsafe actuation as security-relevant because they directly affect physical operation [4–6]. Light-enabled mechanisms matter only when they clarify whether a device, measurement path, optical event, or local inference result should be trusted.

The third requirement is optical-link confidentiality, integrity, and availability. VLC and LiFi links may have spatial constraints that differ from RF links, but practical security cannot rest on room confinement alone. Reflections, gaps, windows, receiver sensitivity, rogue transmitters, and jamming can change the attack surface [23–26]. Optical wireless security must therefore be analyzed as a direct mechanism family.

The fourth requirement is trust in local and edge intelligence. As sensor networks move toward in-sensor, pre-sensor, and near-sensor processing, the security boundary includes model parameters, optical input encoding, calibration state, laser sources, memory, electronic control, and fallback behavior [8,27]. Photonic inference can reduce latency, but it can also become an attack surface.

The fifth requirement is infrastructure-level situational awareness. Distributed photonic sensing can detect vibration, intrusion, cable disturbance, and route-level events over long distances, including through deployed telecom fibers [28–30]. This makes DAS and DFOS relevant to security, but only if alerts are reliable enough to support policy, verification, or incident response.

#### 3.2. Connection to IoT Security Architecture, Zero Trust, and Cyber-Physical Resilience

The security-by-light framing is intended to complement, not replace, established cybersecurity architecture. In zero-trust architecture, access decisions are made per request and depend on explicit identity, device state, policy, and contextual evidence rather than implicit network location [31]. Light-enabled evidence can therefore be interpreted as an additional physical or cyber-physical signal that helps a policy engine evaluate device authenticity, link exposure, inference trust, or infrastructure state. Similarly, IoT security baselines and cybersecurity frameworks emphasize device identity, secure configuration, update capability, vulnerability management, monitoring, incident response, and governance [3,32,33]. Photonic roots of trust, VLC/LiFi fingerprints, photonic fault indicators, and DAS/DFOS events are useful only when they are mapped to these conventional security functions.

The same interpretation applies to cyber-physical resilience and digital-twin security. Cyber-physical frameworks treat trustworthiness, lifecycle, physical process state, safety, and security as coupled concerns [34]. Digital twins and AI-enabled IoT systems increase the need for trustworthy measurement streams, model-state integrity, and continuous validation because decisions may be made from synchronized physical and virtual representations or from near-edge AI models [35,36]. Security by light contributes to this architecture by providing confidence-rated physical evidence, not by becoming a parallel security architecture. The evidence-to-policy model in Section 10 is therefore a bridge between photonic mechanisms and mainstream cybersecurity control, resilience, and governance frameworks.

### 3.3. Threat Model

The threat model spans five layers. At the device layer, an adversary may capture a node, extract stored credentials, replace a legitimate component, insert a counterfeit module, or query a PUF repeatedly to learn a model. Photonic roots of trust address this layer by adding optical identity evidence, but the evidence must survive environmental variation, modeling attacks, and reader compromise [37–39].

At the sensing layer, an adversary may inject false optical inputs, blind a detector, saturate a front end, spoof environmental features, or exploit calibration drift. This includes attack patterns against cameras, LiDAR-like front ends, photodiodes, optical receivers, and vision-oriented sensing modules when the attack changes measurement integrity or inference reliability. At the optical-link layer, an adversary may eavesdrop through reflected paths, use a high-sensitivity receiver, jam visible-light channels, inject rogue optical signals, or manipulate key-extraction assumptions. At the photonic-compute layer, an adversary may perturb optical inputs, exploit physical nonidealities, induce laser faults, corrupt memory, or compromise control electronics around a photonic accelerator [40–45]. At the infrastructure layer, an adversary may disturb, tap, cut, or physically approach optical assets. Distributed fiber sensing can supply physical telemetry, but it must handle nuisance events, false alarms, privacy, and response integration. Table 7 summarizes the threat-to-mechanism mapping used in the synthesis.

**Table 7.** Threat -to-mechanism crosswalk for security by light.

| Threat or Requirement                                                   | Relevant Family                 | Security Interpretation                                                                                                                    |
|-------------------------------------------------------------------------|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Counterfeit replacement, captured node, or untrusted module             | Photonic roots of trust         | Optical uniqueness supports identity only when repeatability, modeling resistance, protected readout, and lifecycle controls are validated |
| Eavesdropping, jamming, rogue transmitter, or weak keying               | VLC/LiFi security               | Optical propagation, transmitter behavior, and channel conditions become part of link-security evidence                                    |
| False optical input, adversarial perturbation, drift, or hardware fault | Photonic intelligence           | Optical inference can support screening only when the inference path is evaluated as attackable hardware                                   |
| Protected transforms, entropy, synchronization, or concealment          | Reservoir and chaotic photonics | Nonlinear dynamics become security-relevant only through leakage, attacker, and baseline analysis                                          |
| Intrusion, tamper, route disturbance, or physical approach              | Photonic sensing infrastructure | Fiber telemetry can inform trust decisions only when alerts are confidence-rated and response-ready                                        |

## 4. Light-Enabled Security Taxonomy

The taxonomy uses three axes: security role, optical mechanism, and deployment layer. A fourth interpretation column records the evidence condition needed before the

mechanism can be treated as a security control. The taxonomy is intentionally security-led. It prevents a common error in emerging photonic-security work: assuming that a mechanism is secure because it is optical, complex, analog, high-dimensional, or hard to visualize.

#### 4.1. Axis I: Security Role

The security-role axis asks what the optical mechanism is supposed to do for the security architecture. The roles are identity and provenance, optical-link protection and keying, photonic inference assurance, secure transforms and entropy, and infrastructure telemetry. Each role corresponds to a different security question. Identity asks whether a device, module, path, or tag is genuine. Link protection asks whether optical propagation or transmitter behavior can reduce leakage or improve availability. Inference assurance asks whether a photonic processor can be trusted under adversarial and physical perturbation. Transform and entropy mechanisms ask whether nonlinear dynamics provide defensible security-relevant processing. Infrastructure telemetry asks whether optical-sensing events can support physical-security decisions.

#### 4.2. Axis II: Optical Mechanism

The optical-mechanism axis describes the physical source of evidence: scattering, speckle, material disorder, photonic fabrication variation, LED or circuit fingerprints, constrained optical propagation, optical beamforming, artificial noise, photonic neural computation, reservoir dynamics, laser or electro-optic chaos, distributed Rayleigh backscatter, and fiber event classification. Mechanisms differ physically, but the review treats them comparably by asking what security property they support and under which assumptions.

#### 4.3. Axis III: Deployment Layer

The deployment layer can be a sensor device, replaceable module, optical transceiver, optical link, access point, gateway, edge accelerator, deployed fiber route, or infrastructure corridor. The same mechanism can have different security meaning at different layers. For example, an LED fingerprint may authenticate a VLC transmitter at the link layer, while a fiber fingerprint can verify a physical path. DAS can monitor a corridor, but its output becomes security evidence only when integrated with policy and response. Table 8 summarizes the resulting light-enabled security taxonomy.

**Table 8.** Taxonomy of light-enabled security mechanisms.

| Security Role                      | Optical Mechanism                                                                                 | Deployment Layer                                         | Evidence Condition                                                                               |
|------------------------------------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Identity and provenance            | Optical PUFs, photonic PUFs, speckle, scattering, material disorder, LED fingerprints             | Device, module, tag, transceiver, access point           | Requires repeatability, modeling resistance, protected enrollment, and lifecycle controls        |
| Optical-link protection and keying | VLC/LiFi propagation, optical beamforming, artificial noise, jamming, RIS/IRS, channel randomness | Room, vehicle, underwater link, gateway, access point    | Requires eavesdropper geometry, receiver assumptions, availability model, and protocol binding   |
| Photonic inference assurance       | ONNs, diffractive networks, photonic accelerators, nonideality-aware inference, fault detection   | Sensor front end, access layer, edge accelerator         | Requires adversarial, fault, drift, calibration, and fallback evaluation                         |
| Secure transforms and entropy      | Reservoir computing, laser chaos, electro-optic chaos, image transforms, chaotic keying           | Link, gateway, processor, transform module               | Requires leakage metrics, attacker observation model, synchronization assumptions, and baselines |
| Infrastructure telemetry           | DAS, DFOS, OTDR, PON/DWDM sensing, fiber event classification                                     | Fiber route, perimeter, corridor, utility infrastructure | Requires false-alarm control, localization, privacy handling, and incident-response integration  |

## 5. Photonic Roots of Trust: PUFs, Optical Fingerprints, and Lifecycle Identity

Photonic roots of trust are the most direct example of security by light. They use disorder, fabrication variation, scattering, speckle, nonlinear response, or device-specific optical behavior as authentication material. The general idea follows physical one-way functions and PUFs: a physical object produces responses that are easy to verify through measurement but difficult to clone or predict without the object [12,46]. In photonic versions, light probes microscopic structure, waveguide disorder, spectral response, material randomness, or path-dependent scattering.

This family is attractive for sensor networks because exposed nodes often cannot rely only on stored digital secrets. A captured or replaced node may present valid software credentials if those credentials are extracted. A photonic PUF or optical fingerprint adds a physical evidence channel. It can support device enrollment, module replacement checks, supply-chain assurance, re-attestation, and in some cases key derivation. In the confidence-rating terminology of Table 6, modeling-attack and prototype authentication studies are treated as direct evidence for identity claims, while label, material, or platform demonstrations without explicit attacker or lifecycle evaluation are treated as security-adjacent evidence.

### 5.1. From Optical Uniqueness to Root of Trust

Optical uniqueness is not enough. A root of trust requires repeatability for the legitimate device, separation among devices, resistance to cloning or emulation, and a protected protocol around enrollment and verification. Early optical one-way functions established the intuition that random optical media can produce hard-to-clone challenge–response behavior [46]. Later work made the measurement and assurance problem more explicit. Lio et al. quantified sensitivity and unclonability in optical PUFs, showing that physical perturbations could produce measurable response separation [47]. This kind of quantification is essential because visual complexity alone does not establish security.

Integrated photonic PUFs move the concept toward deployable sensor-network hardware. Grubel et al. demonstrated a silicon photonic PUF based on nonlinear interactions in a chaotic microcavity [48]. Tarik et al. advanced the deployment argument by demonstrating scalable and CMOS-compatible silicon photonic PUFs for supply-chain assurance [49]. Mahdian et al. framed silicon photonic PUFs as hardware-assurance mechanisms for optical systems, which is especially relevant to photonic modules and trusted interfaces [50].

### 5.2. Device Classes and Deployment Fit

The screened literature indicates four deployment-relevant classes. For readability, Table 9 splits the first class into two subgroups: integrated silicon photonic PUFs and nonlinear or amorphous-silicon PUFs. These are not intended as two separate deployment classes but as two evidence subgroups within integrated photonic roots of trust. The first is integrated silicon or amorphous-silicon photonic PUFs. These are natural candidates for photonic modules, secure chipllets, optical transceivers, and sensor nodes because the security primitive can be close to the physical sensing or communication hardware [38,48–50]. The second is material, label, or metasurface PUFs for anti-counterfeiting and object identity. Cholesteric reflectors, multilevel polymer PUFs, all-silicon multidimensional optical PUFs, and FRET-based quantum-dot PUFs illustrate the range of optical label designs [51–54]. The third is programmable or reconfigurable photonic PUFs, which offer flexibility but introduce control-plane risk because programmability expands the state that must be protected [55]. The fourth is fiber or subsystem fingerprinting, where the trusted object is an optical path, reader, or subsystem rather than only an endpoint device [56,57].

**Table 9.** Representative photonic roots-of-trust approaches and deployment interpretation.

| Approach                            | Representative Evidence                  | Security Role                                                    | Main Caution                                                                  |
|-------------------------------------|------------------------------------------|------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Integrated silicon photonic PUFs    | Grubel; Tarik; Mahdian [48–50]           | Chip, module, and supply-chain identity                          | Readout, packaging, drift, and enrollment become security-critical            |
| Nonlinear or amorphous-silicon PUFs | Kilic; Atakhodjaev; Henderson [38,39,58] | Modeling-resistance evidence for integrated PUF designs          | Results are design-specific and should not be generalized to all optical PUFs |
| Optical labels and material PUFs    | Arenas; Nocentini; Wang; Kim [51–54]     | Anti-counterfeiting, object identity, lightweight authentication | Field readout and environmental repeatability must be demonstrated            |
| Programmable photonic PUFs          | Karydis [55]                             | Reconfigurable physical identity and multi-state trust           | Reconfiguration control becomes part of the attack surface                    |
| Fiber and subsystem fingerprints    | Yao; Nadimi Goki [56,57]                 | Path, link, or subsystem verification                            | Stability, tamper awareness, and reader trust determine authentication value  |

### 5.3. Modeling Resistance and Machine Learning Attacks

The main scientific shift in photonic roots of trust is from uniqueness claims toward attacker-aware evaluation. If an attacker can collect enough challenge–response pairs and learn a predictive model, a visually complex optical PUF may still fail as a security primitive. This is why modeling-resistance papers are central to the maturity of the family. Albright et al. analyze learnability of optical PUFs through a learning-with-errors perspective, showing why PUF security depends on the physical response distribution and the challenge space [37]. Kilic et al. investigate machine learning attacks against amorphous-silicon photonic PUFs and relate resistance to nonlinear response [38]. Atakhodjaev et al. and Henderson et al. provide design-specific evidence that nonlinear silicon or photonic PUFs can resist tested learning attacks under stated settings [39,58].

The correct conclusion is not that photonic PUFs are generally secure against machine learning. The conclusion is that photonic PUF security must be evaluated like cryptographic engineering in physical hardware: define attacker access, bound query exposure, report modeling baselines, account for noise and helper data, and connect the PUF output to an authenticated protocol.

### 5.4. Lifecycle Integration

For sensor networks, the strongest deployment role is lifecycle security. A photonic root of trust can be enrolled during manufacturing or commissioning, verified during onboarding, rechecked during maintenance, and used to support revocation or replacement decisions. This maps to trusted onboarding guidance, which treats device identity and posture verification as prerequisites for credential provisioning and lifecycle management [59,60]. The PUF is not the onboarding protocol. It is a physical evidence source used by the protocol.

Several practical issues remain. Helper data and fuzzy extraction may be necessary when noisy responses are stabilized as cryptographic keys [13]. The reader or verifier must be trusted, because a compromised reader can leak challenges or responses. Environmental drift and packaging variation must be part of acceptance testing. A fleet-scale deployment also needs revocation, update, re-enrollment, and auditability. These are not weaknesses unique to photonic PUFs, but they determine whether optical uniqueness becomes operational security.

## 6. Optical Wireless, VLC, and LiFi Security

VLC and LiFi security deserve a full mechanism-family section because the screened evidence base shows dense direct security work on eavesdropping, jamming, secrecy, artificial noise, fingerprints, key extraction, and LiFi-assisted bootstrapping. The security contribution comes from optical propagation, illumination constraints, transmitter hardware, receiver placement, and channel conditions. These are physical properties, not merely data-link details. Most mechanism-level claims in this section are therefore C2 or C3 claims: leakage experiments and transmitter-fingerprint studies provide direct evidence for tested settings, while secrecy-rate, jamming, RIS/IRS, and key-extraction results remain conditional on geometry, receiver assumptions, and protocol binding.

### 6.1. Limitations of Room-Confinement Assumptions

VLC is often described as naturally secure because light does not penetrate opaque walls. That statement is incomplete. Classen et al. experimentally showed that VLC transmissions can be intercepted through reflected paths, gaps, and windows, including cases where the eavesdropper is outside the direct beam [24]. Marin-Garcia et al. further analyze practical eavesdropping scenarios in VLC systems [25]. Classen et al. also argue that RF physical-layer-security mechanisms cannot simply be transferred to VLC without modeling VLC-specific attacker capabilities, blockage, reflections, and receiver hardware [23]. Rogue-transmitter work adds an integrity dimension: the optical channel can be attacked not only by listening but also by injecting unauthorized visible-light signals [26].

The implication is precise. VLC and LiFi can reduce some exposure compared with RF in some environments, but security depends on geometry, surfaces, receiver field of view, sensor sensitivity, illumination constraints, mobility, and adversary placement. A secure sensor-network design should specify those assumptions rather than relying on generic confinement language.

### 6.2. Secrecy, Jamming, and Artificial Noise

The physical-layer-security literature uses secrecy rate, jamming, beamforming, artificial noise, and reflective-surface control to shape what legitimate and illegitimate receivers can observe. Mostafa and Lampe show friendly jamming as a means to improve VLC secrecy under optical constraints [61]. Pham et al. study artificial-noise design for VLC channels with clipping, explicitly accounting for LED dynamic-range effects [62]. Guo et al. study RIS-aided physical-layer security for VLC, showing how controllable optical reflection can shape secrecy assumptions [63].

These mechanisms support direct security claims only under stated channel models. Many studies assume knowledge of eavesdropper channels, fixed geometry, or simulation settings. In sensor networks, the practical question is how secrecy mechanisms behave under changing room layout, lighting constraints, mobility, device aging, and limited receiver information. The evidence is therefore strong for the existence of optical wireless countermeasures but more conditional for deployment-ready security.

### 6.3. Transmitter Fingerprints and Optical Device Identity

VLC and LiFi also connect naturally to identity. LED fingerprints and optic fingerprints use transmitter-specific behavior as a device-identification signal. Shi et al. demonstrate LED fingerprint extraction and identification for VLC systems [64]. Chen et al. propose optic fingerprints that use inherent circuit and optical characteristics of VLC devices for physical-layer identification [65]. These works shift optical wireless security from channel secrecy alone to transmitter provenance.

The design caution mirrors PUFs. A fingerprint is useful only if it remains stable under temperature, aging, drive circuits, replacement, and maintenance. It also needs a protocol role. A gateway can use an LED fingerprint to detect an unexpected transmitter, but the fingerprint should complement cryptographic authentication and logging rather than replace them.

#### 6.4. Key Extraction and LiFi-Assisted Bootstrapping

Optical channel randomness can also support key extraction or bootstrapping. AquaKey uses underwater visible-light channel variation for symmetric key extraction and demonstrates reliable key generation under its experimental conditions [66]. This is direct evidence that optical channel conditions can contribute to key material in a specific environment. It does not imply that arbitrary VLC links have enough reciprocal randomness for key extraction.

LiFi-assisted bootstrapping extends the idea by using a local optical channel to help secure another wireless protocol. LightGuard illustrates this direction by using LiFi as a physical-layer bootstrapping channel for WiFi security, but it should be treated as preprint-stage demonstration evidence until archival and independent validation are available [67]. The architectural value is still important: optical locality can help bootstrap trust, but only when the resulting protocol has authentication, replay protection, downgrade handling, and fallback behavior. Table 10 summarizes the main VLC and LiFi security directions and their conditions.

**Table 10.** VLC and LiFi security mechanisms and evidence interpretation.

| Direction                          | Representative Evidence       | Security Contribution                                                         | Main Condition                                                                                 |
|------------------------------------|-------------------------------|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Leakage and eavesdropping analysis | Classen; Marin-Garcia [24,25] | Replaces room-confinement intuition with attacker and geometry analysis       | Receiver placement, reflections, gaps, and sensitivity must be modeled                         |
| VLC-specific PLS pitfalls          | Classen [23]                  | Shows that RF PLS assumptions can fail when transferred to VLC                | Use for attacker-model and mechanism-pitfall claims, not as standalone empirical leakage proof |
| Jamming, artificial noise, and RIS | Mostafa; Pham; Guo [61–63]    | Shapes optical information available to legitimate and illegitimate receivers | Simulation assumptions and eavesdropper channel knowledge must be explicit                     |
| LED and optic fingerprints         | Shi; Chen [64,65]             | Adds optical transmitter identity evidence                                    | Aging, temperature, drive circuitry, and replacement affect stability                          |
| Key extraction and bootstrapping   | AquaKey; LightGuard [66,67]   | Uses optical locality or channel variation for keying workflows               | Context-specific and still requires authenticated protocol design                              |

## 7. Secure Sensing and Photonic Intelligence

Photonic intelligence moves computation into or near the optical sensing path. It can reduce latency, energy, and raw-data movement, but it also makes optical inference part of the security boundary. This section separates two claims: photonic inference as a platform capability, and assurance of photonic inference under attack or fault. Accordingly, platform-capability papers are treated as C1 security-adjacent evidence unless they evaluate an explicit adversarial, fault, calibration, or drift condition; attack and fault studies are treated as C2 or C3 evidence depending on validation realism.

#### 7.1. Platform Capability and Security Relevance

Optical neural networks and photonic processors can perform linear operations, convolution-like transforms, image classification, and pre-sensor computation with high

optical bandwidth [14,15]. In-sensor photonic intelligence and photonic edge intelligence extend this idea to sensing systems, where optical computation can occur before full digitization or before raw data leave the device [7,8]. Wang et al. and Huang et al. illustrate image sensing and pre-sensor optical computation directions that can reduce data movement and latency [68,69]. Baek et al. provide broader edge-intelligence context for why near-sensor processing matters in distributed systems [27].

These works support architectural plausibility. They show why photonic intelligence could help a sensor network screen events close to the physical signal. They do not by themselves establish security. A fast optical classifier is a security component only when its inputs, model, calibration, faults, and outputs are evaluated under security assumptions.

### 7.2. Attack Surface of Photonic Learning Systems

Direct security evidence comes from attack and fault studies. Li et al. show that diffractive neural networks can be vulnerable to physical adversarial examples [40]. Jiao et al. analyze adversarial attacks on optical neural networks [41]. Chen et al. develop physics-aware adversarial evaluation, which is important because optical perturbations are constrained by physical propagation rather than arbitrary digital pixel changes [42]. These studies show that optical inference does not escape adversarial-machine-learning problems. It changes their physical form.

Photonic accelerators introduce additional hardware attack surfaces. De Magalhaes et al. analyze attacks on photonic AI hardware [43]. Nishida et al. study laser fault attacks, and Queiroz et al. examine memory faults in photonic neural-network contexts [44,45]. Lu et al. show that photonic nonidealities can affect adversarial behavior and may sometimes contribute to robustness in specific settings [70]. The correct interpretation is conditional: physical nonidealities can matter for defense, but they do not create universal robustness.

### 7.3. Use in Sensor Networks

In sensor networks, photonic intelligence is most defensible as a confidence-rated policy input. It can flag an abnormal optical waveform, classify a local event, estimate confidence before forwarding data, or trigger fallback sampling. It should not be a single point of trust. A policy layer should compare photonic inference with device identity, network telemetry, conventional anomaly detection, and infrastructure context. This is especially important for safety-relevant systems, where a high-speed but poorly calibrated optical model could amplify an attack or fault. Table 11 summarizes the evidence types and security interpretation for photonic intelligence.

**Table 11.** Photonic-intelligence evidence and security interpretation.

| Evidence Type                   | Representative Evidence                      | Supports                                                               | Does Not Support by Itself                     |
|---------------------------------|----------------------------------------------|------------------------------------------------------------------------|------------------------------------------------|
| Photonic inference platforms    | Fu; Zhang; Zhou; Wang; Huang [7,14,15,68,69] | Feasibility of near-sensor optical computation                         | Security robustness or trusted decision-making |
| Physical adversarial evaluation | Li; Jiao; Chen [40–42]                       | Need for optical-domain attack models                                  | General security of all ONNs                   |
| Hardware and fault attacks      | De Magalhaes; Nishida; Queiroz [43–45]       | Photonic accelerators as physically attackable systems                 | Security of unrelated platforms or protocols   |
| Nonideality-aware defense       | Lu [70]                                      | Physical nonidealities can affect attack transfer in specific settings | Universal adversarial defense                  |

## 8. Optical Reservoir Computing, Chaotic Photonics, and Secure Transforms

Reservoir and chaotic photonics attract security interest because they provide high-dimensional dynamics, synchronization behavior, entropy-like signals, and difficult-to-invert transformations. These properties can be useful, but they are not security proofs. A security claim requires an adversary, an observable channel, a leakage metric, and a comparison baseline. For this reason, this section assigns higher confidence only to studies that include leakage, time-delay-signature, synchronization, or attacker-observation analysis; transform or source-separation papers without such analysis remain C1 security-adjacent evidence.

### 8.1. Chaos Communication and Protected Links

Chaos communication is the most established security-relevant direction in this family. Mirasso et al. review chaos-based encryption and communication concepts [20]. Argyris et al. demonstrate chaos-based optical communication over commercial fiber networks, showing that synchronized chaotic carriers can support protected optical links under stated conditions [71]. Mao et al. demonstrate high-rate optical chaos communication over long fiber transmission using semiconductor lasers [72]. These works provide direct evidence that chaotic optical links can be built and recovered by legitimate receivers.

The assurance question is what an attacker observes and what can be inferred. If the evaluation only shows that the legitimate receiver can recover the signal, it does not fully establish confidentiality. Stronger claims require leakage analysis, key or parameter secrecy assumptions, synchronization robustness, and comparison with conventional cryptographic or coding baselines.

### 8.2. Time-Delay Signatures and Leakage

Time-delay signatures illustrate how a physical feature can become a security-relevant leakage channel. Cheng et al. study time-delay concealment in electro-optic chaos [73]. Huang et al. analyze electro-optic chaos systems designed to be immune to time-delay signatures [74]. Gong et al. show time-delay signature extraction using reservoir computing from short and noisy time series [75]. Together, these works support a mature security principle: concealment claims should be tested against increasingly strong extraction methods.

### 8.3. Reservoir-Assisted Transforms and Keying Primitives

Reservoir-assisted secure communication and transforms are promising but heterogeneous. Liu et al. study reservoir-based secure communication [76]. Zhu et al. propose security-enhanced electro-optic chaos using reservoir ideas [77]. Zaminga et al. address optical chaotic recovery [78]. Jiang et al. use optical reservoir computing for image transformation, and Shao et al. discuss optical chaos key-distribution primitives [79,80]. A recent source-separation chaotic optical communication architecture by Zhu et al. is relevant as contextual or adjacent evidence for reservoir-based decryption architecture, but this review does not treat it as direct proof of attacker-side security assurance without stronger leakage validation [81]. Table 12 summarizes the security-relevant value and assurance gaps for reservoir and chaotic photonics.

**Table 12.** Reservoir and chaotic photonics for security-relevant transformations.

| Direction                            | Representative Evidence          | Security-Relevant Value                                        | Assurance Gap                                                        |
|--------------------------------------|----------------------------------|----------------------------------------------------------------|----------------------------------------------------------------------|
| Chaos communication                  | Mirasso; Argyris; Mao [20,71,72] | Protected-link demonstrations and recoverable chaotic carriers | Attacker-side leakage and parameter inference need explicit analysis |
| Time-delay signature control         | Cheng; Huang; Gong [73–75]       | Makes a known chaos-system leakage channel measurable          | Concealment must be tested against stronger extraction methods       |
| Reservoir-assisted secure transforms | Liu; Zhu; Zaminga; Jiang [76–79] | Synchronization, recovery, and transform components            | Requires baseline comparison and adversary observation model         |
| Key-distribution ingredients         | Shao [80]                        | Optical keying primitive and entropy-related direction         | Must be integrated with authentication and randomness validation     |
| Contextual source separation         | Zhu [81]                         | Reservoir-based decryption architecture evidence               | Not direct security assurance without leakage validation             |

## 9. Photonic Sensing Infrastructure for Safety and Security Monitoring

Distributed photonic sensing is the most deployment-facing family in the review. DAS, DFOS, phase-sensitive optical time-domain reflectometry, PON sensing, and DWDM sensing can monitor long physical routes and infrastructure [9,17,18,82]. This makes photonic sensing relevant to security, but the evidence must be interpreted carefully. A deployed sensing substrate is not automatically a validated security-control input. Intrusion and field-sensing papers can support C2 or C3 sensing-performance claims, but they support lower-confidence security-decision claims unless false-alarm handling, incident-response interfaces, privacy constraints, and cross-site transfer are specified.

### 9.1. From Securing Devices to Securing Space

Photonic sensing expands security from endpoint trust to spatial awareness. A fiber route can detect vibration, intrusion, cable tamper, or disturbance near assets. This is important for sensor networks deployed along pipelines, railways, perimeters, utilities, telecom routes, and restricted corridors. The security value is not only that the fiber detects an event. The value is that the event can change trust in nearby devices, trigger verification, dispatch response, or correlate physical and cyber evidence.

### 9.2. Intrusion Evidence, Deployment Evidence, and Standards Evidence

The evidence separates into three groups. The first is intrusion-detection evidence. Several intrusion-oriented studies support detection, localization, and classification of intrusion-like or perimeter events using fiber-optic sensing [28,83–85]. The second is deployment and coexistence evidence. Han et al. and Kotrla et al. show the relevance of telecom-cable and deployed-network sensing, while Tang et al. and Wang et al. address PON and DWDM service-oriented sensing [9,29,30,82]. The third is standards and operational-interface evidence. Wakisaka et al. discuss ITU-T work relevant to DFOS, which helps operationalization but does not validate intrusion analytics by itself [86].

AI-assisted event interpretation adds another layer. Jeong et al., Cao et al., and Wu et al. show how graph diffusion, AI/ML, and multitask learning can improve distributed-sensing event interpretation [19,87,88]. These methods are useful, but they inherit the same security questions as other inference systems: domain shift, label scarcity, nuisance events, adversarial conditions, and calibration.

### 9.3. Policy-Ready Security Telemetry

The main integration challenge is to turn sensing alerts into policy-ready evidence. A DAS event should carry location, confidence, event type, uncertainty, and operational context. It may lower trust in nearby devices, trigger re-attestation, request camera verification, initiate maintenance, or escalate incident response. It should not automatically become a security decision without false-alarm management and governance. This is also a privacy issue: wide-area fiber sensing can reveal human activity and operational patterns, so access control, retention, auditability, and acceptable-use policy are necessary [89,90]. Table 13 summarizes the evidence types and security interpretation for photonic sensing infrastructure.

**Table 13.** Photonic sensing infrastructure evidence and security interpretation.

| Evidence Type                     | Representative Evidence             | Security Value                                          | Main Limitation                                                      |
|-----------------------------------|-------------------------------------|---------------------------------------------------------|----------------------------------------------------------------------|
| Perimeter and intrusion detection | He; Mahmoud; You; Pankti [28,83–85] | Detects and localizes intrusion-like events             | False alarms, weather, nuisance events, and site transfer            |
| Telecom and deployed-fiber reuse  | Han; Kotrla; Tang [9,29,30]         | Uses existing infrastructure as security telemetry      | Must coexist with communication operations and maintenance           |
| Standards and sensing services    | Wakisaka; Wang [82,86]              | Supports operational interfaces and deployment pathways | Standards do not validate security analytics by themselves           |
| AI-assisted event interpretation  | Jeong; Cao; Wu [19,87,88]           | Improves classification and anomaly interpretation      | Domain shift, label scarcity, and confidence calibration remain open |

## 10. System Integration and Evidence-to-Policy Architecture

The mechanism-family sections show that light-enabled security is not a single technology. It is an evidence architecture. Photonic roots of trust, VLC/LiFi security, photonic inference, reservoir or chaotic transforms, and distributed fiber sensing all produce different types of evidence. Their practical value depends on whether this evidence is consumed by onboarding protocols, gateway policy, cryptographic workflows, anomaly detection, fallback logic, incident response, and governance. In this architecture, *confidence-rated evidence* is the policy-facing representation of an optical or photonic observation after it has been annotated with its asset, threat/failure mode, evidence level, validation setting, calibration boundary, lifecycle relevance, and reproducibility condition.

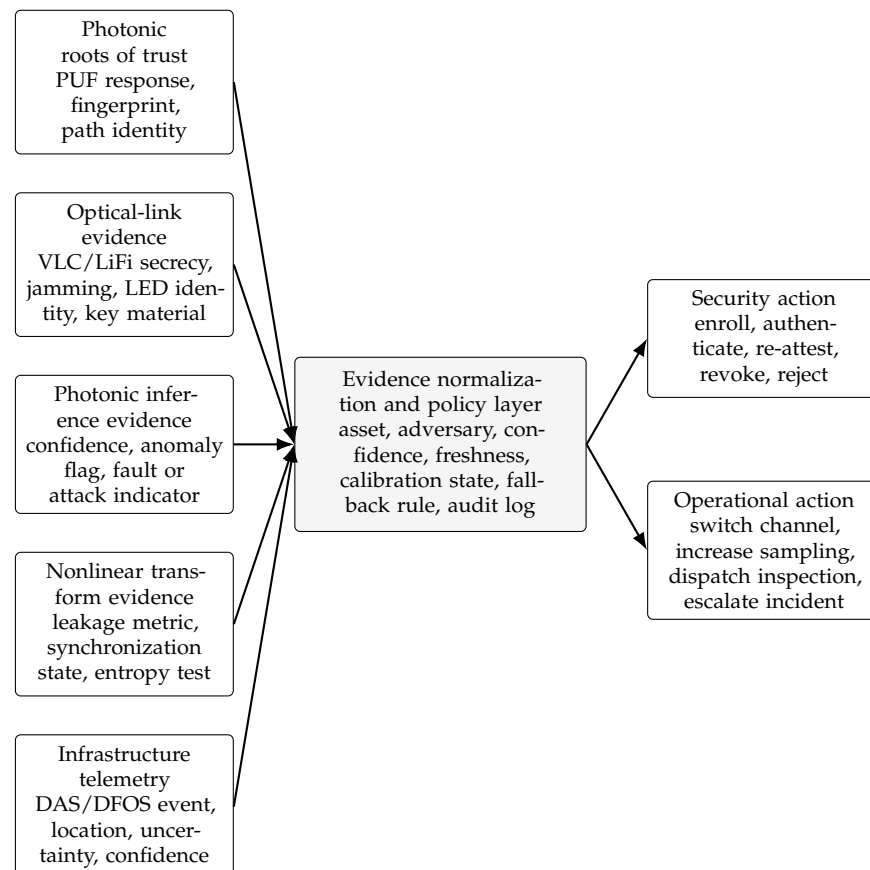
### 10.1. Integration Principles

Four principles guide integration. First, use layered trust rather than single-point trust. A photonic PUF, an LED fingerprint, a photonic classifier, or a DAS alarm should normally complement rather than replace cryptographic authentication, access control, and monitoring. Second, design for lifecycle. Enrollment, onboarding, re-attestation, update, replacement, retirement, and audit determine whether an optical primitive remains useful over time [59,60]. Third, enforce security at resource boundaries. This is consistent with zero-trust thinking, where resource access is continuously evaluated rather than assumed from location [31]. Fourth, require fallback and auditability. If an optical mechanism loses calibration, produces low confidence, or conflicts with other telemetry, the system should enter a restrictive and reviewable state rather than silently accepting the optical output.

### 10.2. Integration Patterns

Four recurring patterns follow from Figure 2. *Device-anchored trust* places photonic roots of trust at device, module, or path boundaries; it is strongest for supply-chain assur-

ance, exposed nodes, replaceable sensing heads, and optical modules [49,50,57]. *Optical-link protection* treats the optical channel as a security surface, combining VLC/LiFi leakage analysis, jamming state, fingerprinting, key extraction, and optical bootstrapping with authenticated protocols. *Photonic inference as policy input* uses a photonic front end or accelerator to estimate confidence, detect abnormal optical inputs, classify events, or trigger fallback; this pattern is plausible only when adversarial, fault, drift, and calibration behavior are measured [42,44,70]. *Infrastructure-aware security overlay* uses distributed photonic sensing to provide spatial context so that DAS or DFOS events can adjust trust in nearby assets, request re-attestation, trigger inspection, or correlate cyber alerts with physical disturbance.



**Figure 2.** Evidence-to-policy architecture for security by light. The optical or photonic mechanism is treated as an evidence source. The policy layer decides how that evidence changes authentication, trust, fallback, monitoring, or incident response. The four integration principles from Section 10.1—layered trust, lifecycle design, resource-boundary enforcement, and fallback/auditability—are operationalized at this policy layer.

Table 14 summarizes the four integration patterns associated with this evidence-to-policy architecture.

**Table 14.** System integration patterns for light-enabled security.

| Pattern                         | Optical Evidence                                                        | Security Action                                                                  | Main Limitation                                           |
|---------------------------------|-------------------------------------------------------------------------|----------------------------------------------------------------------------------|-----------------------------------------------------------|
| Device-anchored trust           | PUF response, optical fingerprint, path identity                        | Enroll, authenticate, re-attempt, revoke, or reject device/module                | Does not validate ongoing measurement integrity by itself |
| Optical-link protection         | VLC secrecy state, jamming state, LED fingerprint, optical key material | Adapt link policy, authenticate transmitter, bootstrap keys, or switch channel   | Assumptions about geometry and protocol binding must hold |
| Photonic inference policy input | Optical classifier confidence, attack detector, fault detector          | Trigger local filtering, fallback, or incident workflow                          | Inference path is itself attackable and drift-prone       |
| Infrastructure-aware overlay    | Fiber event, DAS anomaly, route disturbance                             | Adjust trust zone, dispatch verification, correlate physical and cyber telemetry | False alarms and privacy can dominate operational value   |

## 11. Comparative Evaluation, Maturity, and Research Agenda

Comparing light-enabled mechanisms is difficult because the families differ in physics, metrics, validation setting, and deployment layer. A PUF paper may report false acceptance and response stability. A VLC paper may report secrecy rate. A photonic intelligence paper may report adversarial accuracy or fault detection. A chaos paper may report synchronization quality or leakage indicators. A DAS paper may report event classification and false alarms. These metrics cannot be pooled, but they can be interpreted through common evaluation dimensions. To make this comparison explicit, this paper uses a structured qualitative scoring scheme. The scoring is not a universal quantitative performance metric; it is a transparency device that shows which dimensions drive the maturity judgment for each mechanism family.

### 11.1. Cross-Cutting Evaluation Dimensions

The first dimension is security assurance: the protected asset, adversary, security metric, and validation setting. The second is operational performance: latency, energy, throughput, footprint, calibration, and maintenance burden. The third is environmental robustness: temperature, aging, alignment, illumination, turbulence, site conditions, and drift. The fourth is deployment fit: where the mechanism belongs in the network and which protocol or policy consumes it. The fifth is reproducibility: whether results can be checked beyond one bench setup, one device batch, one simulated geometry, or one field site. Table 15 summarizes these cross-cutting evaluation dimensions.

**Table 15.** Cross-cutting evaluation dimensions used in this review.

| Dimension                | Question                                                  | Examples of Required Evidence                                                            |
|--------------------------|-----------------------------------------------------------|------------------------------------------------------------------------------------------|
| Security assurance       | What is protected, from whom, and under what assumptions? | Attacker model, leakage metric, false acceptance, attack success, fault outcome          |
| Operational performance  | Can the mechanism operate at the required layer?          | Latency, power, footprint, throughput, calibration overhead, maintenance burden          |
| Environmental robustness | Does the security property survive realistic conditions?  | Temperature, aging, alignment, mobility, illumination, weather, site variation           |
| Deployment fit           | Which system component consumes the optical evidence?     | Onboarding, gateway policy, edge fallback, incident response, lifecycle workflow         |
| Reproducibility          | Can the result be checked or compared?                    | Public settings, datasets, challenge-response statistics, geometry, code, repeated sites |

Table 16 defines the ordinal scoring criteria used for the maturity synthesis.

**Table 16.** Structured scoring criteria used to support the qualitative maturity analysis. Each dimension is scored as 0 = weak or absent evidence, 1 = partial or assumption-sensitive evidence, and 2 = strong evidence for the reviewed setting.

| Dimension                    | 0                                                                   | 1                                                                               | 2                                                                                              |
|------------------------------|---------------------------------------------------------------------|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Evidence directness          | Security relevance is mainly adjacent or conceptual                 | Analytic, simulation, or limited prototype security evidence                    | Direct empirical, prototype, or field security evidence for a stated setting                   |
| Attacker/failure awareness   | No explicit adversary, fault, or misuse condition                   | Partial attacker/failure model or limited misuse case                           | Explicit attacker, fault, leakage, or misuse model linked to metric                            |
| Validation realism           | Abstract model or narrow bench condition                            | Simulation or laboratory validation with stated assumptions                     | Field-like, prototype, or experimentally realistic validation                                  |
| Robustness/calibration       | Little evidence of drift, noise, aging, geometry, or site variation | Some robustness or calibration conditions reported                              | Robustness boundaries are measured and used in interpretation                                  |
| Lifecycle/policy integration | No clear consumer of the optical evidence                           | Possible integration point stated but not operationalized                       | Onboarding, access control, fallback, incident response, or governance role is explicit        |
| Reproducibility              | Conditions, data, geometry, or code is insufficiently specified     | Partial reproducibility through reported parameters or limited public artifacts | Settings, datasets, challenge statistics, geometry, or procedures enable meaningful comparison |

### 11.2. Maturity and Research Priorities

The maturity view is qualitative because validation cultures differ across mechanism families. It is not a ranking of scientific importance. It indicates how close the evidence is to a dependable security-control role. The criteria in Table 16 are applied in Table 17, which combines maturity interpretation with the research agenda to avoid repeating the same family-level conclusions in separate tables.

**Table 17.** Structured comparative maturity assessment for light-enabled security mechanism families. Scores use the criteria in Table 16; the maturity label remains a structured expert synthesis rather than a pooled quantitative performance score.

| Family                          | ED | AF | VR | RC | LP | RP | Total | Maturity Interpretation and Priority Before Dependable Security-Control Use                                                                                                              |
|---------------------------------|----|----|----|----|----|----|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Photonic roots of trust         | 2  | 2  | 1  | 1  | 1  | 1  | 8/12  | Prototype to early subsystem. Priority: evaluate modeling attacks, environmental drift, helper data, protected readers, enrollment, revocation, and lifecycle.                           |
| VLC/LiFi security               | 2  | 2  | 1  | 1  | 1  | 1  | 8/12  | Analytic to prototype, with selected experimental evidence. Priority: validate realistic geometry, mobility, receiver placement, reflections, jamming, and protocol binding.             |
| Photonic intelligence           | 1  | 2  | 1  | 1  | 0  | 1  | 6/12  | Early security-assurance stage. Priority: report attack, fault, calibration, drift, fallback behavior, and security-task datasets when outputs influence decisions.                      |
| Reservoir and chaotic photonics | 1  | 1  | 1  | 0  | 0  | 1  | 4/12  | Concept to early prototype. Priority: move beyond security by complexity through leakage metrics, attacker observations, baselines, randomness validation, and protocol-level arguments. |
| Photonic sensing infrastructure | 2  | 1  | 2  | 1  | 1  | 1  | 8/12  | Deployment-oriented as sensing, lower as security-decision input. Priority: quantify false alarms, localization uncertainty, cross-site transfer, privacy, and response interfaces.      |

ED = evidence directness; AF = attacker/failure awareness; VR = validation realism; RC = robustness/calibration; LP = lifecycle/policy integration; RP = reproducibility. A score of 0–4 indicates mainly conceptual or security-adjacent maturity; 5–7 indicates conditional or early security-assurance maturity; 8–10 indicates prototype or deployment-oriented maturity under stated assumptions; 11–12 would indicate strong field-ready security-control evidence, which was not observed for any complete family in this review.

These maturity dimensions should be interpreted as horizontal requirements across all mechanism families rather than as an additional mechanism category. Reproducibility, benchmark transparency, privacy, governance, lifecycle reporting, and explicit threat assumptions influence the confidence that can be assigned to every family in Table 17. A mechanism with strong laboratory evidence may therefore still receive a limited maturity interpretation if these cross-cutting conditions are weakly reported or absent.

Across all families, the same evaluation discipline is needed: state the protected asset, adversary, deployment layer, assumptions, and failure mode. This is especially important for reservoir and chaotic photonics, where synchronization, concealment, and time-delay behavior must be related to explicit leakage and attacker observations [73–75]. It is also important for VLC/LiFi, where leakage and secrecy depend on physical geometry rather than only nominal room confinement [23–25,62]. Finally, it is necessary for distributed photonic sensing, where a fiber event becomes security evidence only when confidence, location, false-alarm behavior, and operational meaning are clear [28,29,84,86].

Privacy and governance cut across the mechanism families. Light-enabled security can expand observability over devices, infrastructure, and human activity. Governance should address access control, data minimization, retention, auditability, acceptable use, and AI risk management [89,90]. This is especially important when distributed fiber sensing and photonic inference feed operational decision systems.

## 12. Synthesis of Research Questions

Table 18 summarizes the answers to the research questions. Confidence reflects the screened evidence base and appraisal rubric, not a claim of field-wide completeness.

**Table 18.** Answers to the research questions.

| RQ  | Answer                                                                                                                                                                                                                                                                           | Confidence                                               | Remaining Limitation                                                                                             |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| RQ1 | Light can support identity and provenance, optical-link protection and keying, photonic inference assurance, secure transforms, and infrastructure telemetry.                                                                                                                    | Moderate to high for roles, lower for end-to-end systems | Roles are clearer than complete deployed architectures                                                           |
| RQ2 | Direct evidence is strongest for VLC/LiFi security and photonic roots of trust; photonic intelligence has important attack/fault evidence; reservoir/chaos includes more mixed and adjacent evidence; sensing is mature as telemetry but less mature as security-decision input. | Moderate                                                 | Evidence types differ by family and cannot be pooled quantitatively                                              |
| RQ3 | Devices and modules fit roots of trust; links fit VLC/LiFi; access and edge layers fit photonic inference; gateways fit transforms; corridors and routes fit DAS/DFOS.                                                                                                           | High for deployment mapping                              | Multi-layer integration evidence remains sparse                                                                  |
| RQ4 | Attacker awareness is best developed in VLC/LiFi, PUF modeling, and ONN attack studies; robustness, lifecycle, site transfer, privacy, and policy evidence remain uneven.                                                                                                        | Moderate                                                 | Many studies are simulation-heavy, laboratory-limited, site-specific, or lack reproducible evaluation conditions |
| RQ5 | Main gaps are explicit security semantics, lifecycle integration, realistic optical geometry, trustworthy photonic inference, leakage-aware chaos evaluation, policy-ready sensing telemetry, reproducible benchmarks, and governance.                                           | High as synthesis judgment                               | Priorities should be updated as field deployments and benchmark datasets mature                                  |

## 13. Conclusions

This review examined security by light as a structured design space for sensor-networked systems. The evidence supports five roles: physical identity and provenance, optical-link protection and keying, assurance of photonic inference, nonlinear transforms and synchronization, and infrastructure-scale physical telemetry. The contribution is not a claim that light replaces conventional security engineering. It is a framework for deciding where optical and photonic mechanisms can add defensible evidence to a layered security architecture.

The most important conclusion is that optical evidence must be interpreted according to its security role. Photonic roots of trust provide identity evidence only when modeling resistance, protected readers, helper data, and lifecycle integration are addressed. VLC and LiFi mechanisms provide optical-link evidence, but operational claims depend on geometry, receiver assumptions, and authenticated protocol binding. Photonic intelligence is relevant when evaluated as an attackable inference substrate, not merely as a fast optical classifier. Reservoir and chaotic photonics offer protected-link and transform components

only when leakage and attacker observations are explicit. Distributed photonic sensing is comparatively mature as sensing infrastructure, but its security value depends on false-alarm control, cross-site transfer, privacy, and response integration.

The architectural implication is that light-enabled mechanisms are strongest as confidence-rated evidence sources. Their dependable use requires conventional cryptography, secure onboarding, access control, monitoring, fallback, incident response, and governance. Future work should therefore make security semantics explicit, validate against realistic adversaries, report reproducible physical conditions, and design interfaces that turn optical evidence into auditable security decisions.

**Author Contributions:** Conceptualization, R.I. and S.K.; methodology, R.I., S.K. and S.E.; formal analysis, R.I.; investigation, R.I.; resources, S.K.; data curation, R.I.; writing—original draft preparation, R.I.; writing—review and editing, S.K., S.E. and R.I.; visualization, R.I.; supervision, S.K.; project administration, S.K. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was co-funded by the Swedish Knowledge Foundation (KK-stiftelsen) through the Strategic Innovation Graduate School in Cyber Security (SIGS-CyberSec), Grant Agreement No. 20220129-H-01.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** No new empirical datasets were generated by this paper. The review is based on publicly available publications, standards, and bibliographic records. The core search strings, source fielding, screening flow, and deduplicated screening counts are reported in Section 2, Figure 1, and Tables 2–4.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## Abbreviations

The following abbreviations are used in this paper:

|      |                                         |
|------|-----------------------------------------|
| AI   | Artificial intelligence                 |
| CMOS | Complementary metal–oxide–semiconductor |
| DAS  | Distributed acoustic sensing            |
| DFOS | Distributed fiber-optic sensing         |
| DWDM | Dense wavelength-division multiplexing  |
| FRET | Förster resonance energy transfer       |
| IoT  | Internet of Things                      |
| IRS  | Intelligent reflecting surface          |
| ONN  | Optical neural network                  |
| OTDR | Optical time-domain reflectometry       |
| PLS  | Physical-layer security                 |
| PON  | Passive optical network                 |
| PUF  | Physical unclonable function            |
| RIS  | Reconfigurable intelligent surface      |
| VLC  | Visible-light communication             |
| WSN  | Wireless sensor network                 |

## References

1. Butun, I.; Morgera, S.D.; Sankar, R. A Survey of Intrusion Detection Systems in Wireless Sensor Networks. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 266–282. <https://doi.org/10.1109/SURV.2013.050113.00191>.
2. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things Security: A Survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. <https://doi.org/10.1016/j.jnca.2017.04.002>.

3. Fagan, M.; Megas, K.N.; Scarfone, K.; Smith, M. *IoT Device Cybersecurity Capability Core Baseline*; NIST Interagency Report 8259A; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020. <https://doi.org/10.6028/NIST.IR.8259A>.
4. Cyber-Physical Systems Public Working Group. *Framework for Cyber-Physical Systems: Volume 2, Working Group Reports*; NIST Special Publication 1500-202; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017. <https://doi.org/10.6028/NIST.SP.1500-202>.
5. McCarthy, J.; Powell, M.; Stouffer, K.; Tang, C.; Zimmerman, T.; Barker, W.; Ogunyale, T.; Wynne, D.; Wiltberger, J. *Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection*; NIST Interagency Report 8219; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020. <https://doi.org/10.6028/NIST.IR.8219>.
6. Stouffer, K.; Pease, M.; Tang, C.; Zimmerman, T.; Pillitteri, V.; Lightman, S.; Hahn, A.; Saravia, S.; Sherule, A.; Thompson, M. *Guide to Operational Technology (OT) Security*; NIST Special Publication 800-82r3; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023. <https://doi.org/10.6028/NIST.SP.800-82r3>.
7. Zhou, H.; Li, D.; Lee, C. Technology Landscape Review of In-Sensor Photonic Intelligence: From Optical Sensors to Smart Devices. *AI Sens.* **2025**, *1*, 5. <https://doi.org/10.3390/aisens1010005>.
8. Zhang, S.; Jiang, X.; Wu, B.; Zhou, H.; Xu, W.; Zhou, H.; Ruan, Z.; Dong, J.; Zhang, X. Photonic Edge Intelligence Chip for Multi-Modal Sensing, Inference and Learning. *Nat. Commun.* **2025**, *16*, 10136. <https://doi.org/10.1038/s41467-025-65151-x>.
9. Tang, R.; Rao, Y.; Wu, H.; Geng, Y.; Jing, Q.; Xie, L.; He, P.; Li, Z.; Zou, S.; Hua, T.; et al. Seamless Integration of Distributed Acoustic Sensing and Passive Optical Networks for Human Intrusion Monitoring. *Commun. Eng.* **2026**, *5*, 105. <https://doi.org/10.1038/s44172-026-00662-z>.
10. Blinowski, G.J. Security of Visible Light Communication Systems—A Survey. *Phys. Commun.* **2019**, *34*, 246–260. <https://doi.org/10.1016/j.phycom.2019.04.003>.
11. Arfaoui, M.A.; Soltani, M.D.; Tavakkolnia, I.; Ghayeb, A.; Safari, M.; Assi, C.M.; Haas, H. Physical Layer Security for Visible Light Communication Systems: A Survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1887–1908. <https://doi.org/10.1109/COMST.2020.2988615>.
12. McGrath, T.; Bagci, I.E.; Wang, Z.M.; Roedig, U.; Young, R.J. A PUF Taxonomy. *Appl. Phys. Rev.* **2019**, *6*, 011303. <https://doi.org/10.1063/1.5079407>.
13. Dodis, Y.; Ostrovsky, R.; Reyzin, L.; Smith, A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM J. Comput.* **2008**, *38*, 97–139. <https://doi.org/10.1137/060651380>.
14. Fu, T.; Zhang, J.; Sun, R.; Huang, Y.; Xu, W.; Yang, S.; Zhu, Z.; Chen, H. Optical Neural Networks: Progress and Challenges. *Light. Sci. Appl.* **2024**, *13*, 263. <https://doi.org/10.1038/s41377-024-01590-3>.
15. Zhang, H.; Song, Y.; Chen, S.; Bai, Y.; Xu, X.; Huang, C.; Wang, J.; Chen, H.; Moss, D.J.; Xu, K. Integrated Platforms and Techniques for Photonic Neural Networks. *Npj Nanophotonics* **2025**, *2*, 40. <https://doi.org/10.1038/s44310-025-00088-z>.
16. Yan, M.; Huang, C.; Bienstman, P.; Tino, P.; Lin, W.; Sun, J. Emerging Opportunities and Challenges for the Future of Reservoir Computing. *Nat. Commun.* **2024**, *15*, 2056. <https://doi.org/10.1038/s41467-024-45187-1>.
17. Minardo, A.; Bernini, R.; Berruti, G.M.; Breglio, G.; Bruno, F.A.; Buontempo, S.; Campopiano, S.; Catalano, E.; Consales, M.; Coscetta, A.; et al. Innovative Photonic Sensors for Safety and Security, Part I: Fundamentals, Infrastructural and Ground Transportations. *Sensors* **2023**, *23*, 2558. <https://doi.org/10.3390/s23052558>.
18. Zhu, H.H.; Liu, W.; Wang, T.; Su, J.W.; Shi, B. Distributed Acoustic Sensing for Monitoring Linear Infrastructures: Current Status and Trends. *Sensors* **2022**, *22*, 7550. <https://doi.org/10.3390/s22197550>.
19. Cao, L.; Abedin, S.; Cui, G.; Wang, X. Artificial Intelligence and Machine Learning in Optical Fiber Sensors: A Review. *Sensors* **2025**, *25*, 7442. <https://doi.org/10.3390/s25247442>.
20. Mirasso, C.R.; Vicente, R.; Colet, P.; Mulet, J.; Perez, T. Synchronization Properties of Chaotic Semiconductor Lasers and Applications to Encryption. *Comptes Rendus Phys.* **2004**, *5*, 613–622. <https://doi.org/10.1016/j.crhy.2004.03.007>.
21. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *BMJ* **2021**, *372*, n71. <https://doi.org/10.1136/bmj.n71>.
22. Tricco, A.C.; Lillie, E.; Zarin, W.; O'Brien, K.K.; Colquhoun, H.; Levac, D.; Moher, D.; Peters, M.D.J.; Horsley, T.; Weeks, L.; et al. PRISMA Extension for Scoping Reviews (PRISMA-ScR): Checklist and Explanation. *Ann. Intern. Med.* **2018**, *169*, 467–473. <https://doi.org/10.7326/M18-0850>.
23. Classen, J.; Steinmetzer, D.; Hollick, M. Opportunities and Pitfalls in Securing Visible Light Communication on the Physical Layer. In Proceedings of the 3rd Workshop on Visible Light Communication Systems, New York, NY, USA, 3–7 October 2016; pp. 19–24. <https://doi.org/10.1145/2981548.2981551>.
24. Classen, J.; Chen, J.; Steinmetzer, D.; Hollick, M.; Knightly, E. The Spy Next Door: Eavesdropping on High Throughput Visible Light Communications. In Proceedings of the 2nd International Workshop on Visible Light Communications Systems; Association for Computing Machinery: New York, NY, USA, 2015; pp. 9–14. <https://doi.org/10.1145/2801073.2801075>.

25. Marin-Garcia, I.; Guerra, V.; Perez-Jimenez, R. Study and Validation of Eavesdropping Scenarios over a Visible Light Communication Channel. *Sensors* **2017**, *17*, 2687. <https://doi.org/10.3390/s17112687>.
26. Blinowski, G.J. The Feasibility of Launching Rogue Transmitter Attacks in Indoor Visible Light Communication Networks. *Wirel. Pers. Commun.* **2017**, *97*, 5325–5343. <https://doi.org/10.1007/s11277-017-4781-3>.
27. Baek, Y.; Bae, B.; Shin, H.; Sonnadara, C.; Cho, H.; Lin, C.Y.; Mu, Y.; Shen, C.; Shah, S.; Wang, G.; et al. Edge Intelligence through In-Sensor and Near-Sensor Computing for the Artificial Intelligence of Things. *Npj Unconv. Comput.* **2025**, *2*, 25. <https://doi.org/10.1038/s44335-025-00040-6>.
28. Mahmoud, S.S. Practical Aspects of Perimeter Intrusion Detection and Nuisance Suppression for Distributed Fiber-Optic Sensors. *IEEE Trans. Instrum. Meas.* **2023**, *72*, 2517311. <https://doi.org/10.1109/TIM.2023.3284133>.
29. Han, S.; Huang, M.F.; Li, T.; Fang, J.; Jiang, Z.; Wang, T. Deep Learning-Based Intrusion Detection and Impulsive Event Classification for Distributed Acoustic Sensing Across Telecom Networks. *J. Light. Technol.* **2024**, *42*, 4167–4176. <https://doi.org/10.1109/JLT.2024.3401244>.
30. Kotrla, S.R.; Huang, M.F.; Fang, J.; Han, S.; Lynn, J.; Ip, E.; Mundt, J.A.; Wang, T. Leveraging Deployed Telecom Cables for Distributed Fiber Sensing Topologies and Applications. *J. Opt. Commun. Netw.* **2026**, *18*, B72–B84. <https://doi.org/10.1364/JOCN.585523>.
31. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. *Zero Trust Architecture*; NIST Special Publication 800-207; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020. <https://doi.org/10.6028/NIST.SP.800-207>.
32. European Union Agency for Network and Information Security. *Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures*; Technical report; ENISA: Athens, Greece, 2017.
33. National Institute of Standards and Technology. *The NIST Cybersecurity Framework 2.0*; Technical report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2024. <https://doi.org/10.6028/NIST.CSWP.29>.
34. Griffor, E.R.; Greer, C.; Wollman, D.A.; Burns, M.J. *Framework for Cyber-Physical Systems: Volume 1, Overview*; NIST Special Publication 1500-201; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017. <https://doi.org/10.6028/NIST.SP.1500-201>.
35. Wang, Y.; Su, Z.; Guo, S.; Dai, M.; Luan, T.H.; Liu, Y. A Survey on Digital Twins: Architecture, Enabling Technologies, Security and Privacy, and Future Prospects. *arXiv* **2023**, arXiv:2301.13350.
36. Aouedi, O.; Vu, T.H.; Sacco, A.; Nguyen, D.C.; Piamrat, K.; Marchetto, G.; Pham, Q.V. A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions. *arXiv* **2024**, arXiv:2406.03820. <https://doi.org/10.48550/arXiv.2406.03820>.
37. Albright, A.; Gelfand, B.; Dixon, M. Learnability of Optical Physical Unclonable Functions through the Lens of Learning with Errors. *IEEE Trans. Inf. Forensics Secur.* **2025**, *20*, 886–897. <https://doi.org/10.1109/TIFS.2024.3518065>.
38. Kilic, V.; Macfarlane, N.; Stround, J.; Metais, S.; Alemohammad, M.; Cooper, A.B.; Foster, A.C.; Foster, M.A. Machine Learning Resistant Amorphous Silicon Physically Unclonable Functions (PUFs). *arXiv* **2024**, arXiv:2402.02846.
39. Henderson, J.M.; Henderson, E.R.; Harper, C.A.; Shahoei, H.; Oxford, W.V.; Larson, E.C.; MacFarlane, D.L.; Thornton, M.A. A Photonic PUF's Resilience to Multiple-Valued ML Attacks. In *Proceedings of the 2024 IEEE 54th International Symposium on Multiple-Valued Logic (ISMVL)*; IEEE: Piscataway, NJ, USA, 2024; pp. 161–166. <https://doi.org/10.1109/ISMVL60454.2024.00039>.
40. Li, Y.; Yu, C. Late Breaking Results: Physical Adversarial Attacks of Diffractive Deep Neural Networks. In *Proceedings of the 2021 58th ACM/IEEE Design Automation Conference (DAC)*; IEEE: Piscataway, NJ, USA, 2021; pp. 1374–1375. <https://doi.org/10.1109/DAC18074.2021.9586204>.
41. Jiao, S.; Song, Z.; Xiang, S. Adversarial Attacks on an Optical Neural Network. *IEEE J. Sel. Top. Quantum Electron.* **2023**, *29*, 7700306. <https://doi.org/10.1109/JSTQE.2022.3207056>.
42. Chen, R.; Li, Y.; Lou, M.; Fan, J.; Tang, Y.; Sensale-Rodriguez, B.; Yu, C.; Gao, W. Physics-Aware Machine Learning and Adversarial Attack in Complex-Valued Reconfigurable Diffractive All-Optical Neural Network. *Laser Photonics Rev.* **2022**, *16*, 2200348. <https://doi.org/10.1002/lpor.202200348>.
43. De Magalhaes, F.G.; Nikdast, M.; Nicolescu, G. Integrated Photonic AI Accelerators Under Hardware Security Attacks: Impacts and Countermeasures. In *Proceedings of the 2023 IEEE 66th International Midwest Symposium on Circuits and Systems (MWSCAS)*; IEEE: Piscataway, NJ, USA, 2023; pp. 806–810. <https://doi.org/10.1109/MWSCAS57524.2023.10406049>.
44. Nishida, K.; Midoh, Y.; Miura, N.; Kawakami, S.; Orailoglu, A.; Shiomi, J. PrometheusFree: Concurrent Detection of Laser Fault Injection Attacks in Optical Neural Networks. In *Proceedings of the 31st Asia and South Pacific Design Automation Conference (ASP-DAC)*; IEEE: Piscataway, NJ, USA, 2026; pp. 1152–1159. <https://doi.org/10.1109/ASP-DAC66049.2026.11420436>.
45. de Queiroz, M.G.; de Melo, L.A.; Costa, M.V.; Pappalardo, S.; Pavanello, F.; O'Connor, I.; Bosio, A. Case Study: Improving the Robustness of Photonic Neural Networks Against Memory Faults. In *Proceedings of the 2026 IEEE 27th Latin American Test Symposium (LATS)*; IEEE: Piscataway, NJ, USA, 2026; pp. 1–2. <https://doi.org/10.1109/LATS70329.2026.11480369>.
46. Pappu, R.; Recht, B.; Taylor, J.; Gershenfeld, N. Physical One-Way Functions. *Science* **2002**, *297*, 2026–2030. <https://doi.org/10.1126/science.1074376>.

47. Lio, G.E.; Nocentini, S.; Pattelli, L.; Cara, E.; Wiersma, D.S.; Rührmair, U.; Riboli, F. Quantifying the Sensitivity and Unclonability of Optical Physical Unclonable Functions. *Adv. Photonics Res.* **2023**, *4*, 2200225. <https://doi.org/10.1002/adpr.202200225>.
48. Grubel, B.C.; Bosworth, B.T.; Kossey, M.R.; Sun, H.; Cooper, A.B.; Foster, M.A.; Foster, A.C. Silicon Photonic Physical Unclonable Function. *Opt. Express* **2017**, *25*, 12710–12721. <https://doi.org/10.1364/OE.25.012710>.
49. Tarik, F.B.; Famili, A.; Lao, Y.; Ryckman, J.D. Scalable and CMOS Compatible Silicon Photonic Physical Unclonable Functions for Supply Chain Assurance. *Sci. Rep.* **2022**, *12*, 15653. <https://doi.org/10.1038/s41598-022-19796-z>.
50. Mahdian, M.A.; Taheri, E.; Mojaver, K.R.; Nikdast, M. Hardware Assurance with Silicon Photonic Physical Unclonable Functions. *Sci. Rep.* **2024**, *14*, 25591. <https://doi.org/10.1038/s41598-024-72922-x>.
51. Arenas, M.; Demirci, H.; Lenzini, G. Cholesteric Spherical Reflectors as Physical Unclonable Identifiers in Anti-Counterfeiting. In *Proceedings of the 16th International Conference on Availability, Reliability and Security*; Association for Computing Machinery: New York, NY, USA, 2021. <https://doi.org/10.1145/3465481.3465766>.
52. Nocentini, S.; Rührmair, U.; Barni, M.; Wiersma, D.S.; Riboli, F. All-Optical Multilevel Physical Unclonable Functions. *Nat. Mater.* **2024**, *23*, 369–376. <https://doi.org/10.1038/s41563-023-01734-7>.
53. Wang, K.; Shi, J.; Lai, W.; He, Q.; Xu, J.; Ni, Z.; Liu, X.; Pi, X.; Yang, D. All-Silicon Multidimensionally-Encoded Optical Physical Unclonable Functions for Integrated Circuit Anti-Counterfeiting. *Nat. Commun.* **2024**, *15*, 3203. <https://doi.org/10.1038/s41467-024-47479-y>.
54. Kim, K.; Moon, Y.; Kim, Y.K.; Shin, S.; Bi, J.C.; Jung, J.Y.; Jang, B.C.; Ju, B.K. Optical Physical Unclonable Functions Based on Förster Resonant Energy Transfer in Multi-Color Quantum Dots. *Commun. Mater.* **2025**, *6*, 270. <https://doi.org/10.1038/s43246-025-00984-z>.
55. Karydis, G.A.; Sarantoglou, G.; Charbonnier, B.; Castany, O.; Brision, S.; Wilmart, Q.; Mesaritakis, C.; Bogris, A. Programmable Photonic Chips as Versatile Physical Unclonable Functions. In *Proceedings of the 2025 Conference on Lasers and Electro-Optics Europe and European Quantum Electronics Conference (CLEO/Europe-EQEC)*; IEEE: Piscataway, NJ, USA, 2025; p. 1. <https://doi.org/10.1109/CLEO/Europe-EQEC65582.2025.11109826>.
56. Yao, Z.; Mauldin, T.; Heffernan, G.; Xu, Z.; Liu, M.; Wei, T. Low-Cost Optical Fiber Physical Unclonable Function Reader Based on a Digitally Integrated Semiconductor LiDAR. *Appl. Opt.* **2019**, *58*, 6211–6216. <https://doi.org/10.1364/AO.58.006211>.
57. Nadimi Goki, P.; Civelli, S.; Parente, E.; Caldelli, R.; Mulugeta, T.T.; Sambo, N.; Secondini, M.; Potì, L. Optical Identification Using Physical Unclonable Functions. *J. Opt. Commun. Netw.* **2023**, *15*, E63–E73. <https://doi.org/10.1364/JOCN.489889>.
58. Atakhodjaev, I.; Bosworth, B.T.; Grubel, B.C.; Kossey, M.R.; Villalba, J.; Cooper, A.B.; Dehak, N.; Foster, A.C.; Foster, M.A. Investigation of Deep Learning Attacks on Nonlinear Silicon Photonic PUFs. In *Proceedings of the Conference on Lasers and Electro-Optics*; Optica Publishing Group: Washington, DC, USA, 2018; pp. 1–2.
59. Symington, S.; Mulugeta, B.; Polk, W.; Souppaya, M.; Marron, J. *Foundational Concepts in Trusted IoT Device Network-Layer Onboarding: Enhancing Internet Protocol-Based IoT Device and Network Security*; NIST Interagency Report 8350; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2025. <https://doi.org/10.6028/NIST.IR.8350>.
60. Marron, J.; Fagan, M.; Souppaya, M.; Watrobski, P.; Mulugeta, B.; Symington, S.; Klosterman, J.; Rearick, C.; Deane, C.; Harkins, D.; et al. *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security*; NIST Special Publication 1800-36; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2025. <https://doi.org/10.6028/NIST.SP.1800-36>.
61. Mostafa, A.; Lampe, L. Securing Visible Light Communications via Friendly Jamming. In *Proceedings of the 2014 IEEE Globecom Workshops*; IEEE: Piscataway, NJ, USA, 2014; pp. 524–529. <https://doi.org/10.1109/GLOCOMW.2014.7063485>.
62. Pham, T.V.; Hranilovic, S.; Ishihara, S. On the Design of Artificial Noise for Physical Layer Security in Visible Light Communication Channels With Clipping. *IEEE Trans. Wirel. Commun.* **2024**, *23*, 16062–16075. <https://doi.org/10.1109/TWC.2024.3436534>.
63. Guo, D.; Xin, G.; Wu, Q.; Zhang, J. RIS-Aided Physical Layer Security for Visible Light Communication Systems. *IEEE Photonics J.* **2026**, *18*, 7900206. <https://doi.org/10.1109/JPHOT.2026.3651843>.
64. Shi, D.; Zhang, X.; Vladimirescu, A.; Shi, L.; Huang, Y.; Liu, Y. A Device Identification Method Based on LED Fingerprint for Visible Light Communication System. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*; Association for Computing Machinery: New York, NY, USA, 2020. <https://doi.org/10.1145/3407023.3409214>.
65. Chen, X.; Liu, Z.; Zhang, X.; Wang, Y.; Shi, D.; Liu, X. Optic Fingerprint: Enhancing Security in Visible Light Communication Networks. In *Proceedings of the IEEE INFOCOM 2024-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*; IEEE: Piscataway, NJ, USA, 2024. <https://doi.org/10.1109/INFOCOMWKSHPS61880.2024.10620698>.
66. Zhang, L.; Wang, P.; Cui, M.; Wei, J.; Tian, Y.; Zhang, J.; Xiong, J.; Wang, L. AquaKey: Exploiting the Randomness of the Underwater Visible Light Communication Channel for Key Extraction. In *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*; Association for Computing Machinery: New York, NY, USA, 2024; Volume 8. <https://doi.org/10.1145/3643557>.
67. Xu, S.; Du, Y.; Zhang, M.; Cui, H.; Liew, S.C. LightGuard: Transparent WiFi Security via Physical-Layer LiFi Key Bootstrapping. *arXiv* **2026**, arXiv:2604.01092.

68. Wang, T.; Sohoni, M.M.; Wright, L.G.; Stein, M.M.; Ma, S.Y.; Onodera, T.; Anderson, M.G.; McMahon, P.L. Image Sensing with Multilayer Nonlinear Optical Neural Networks. *Nat. Photonics* **2023**, *17*, 408–415. <https://doi.org/10.1038/s41566-023-01170-8>.
69. Huang, Z.; Shi, W.; Wu, S.; Wang, Y.; Yang, S.; Chen, H. Pre-Sensor Computing with Compact Multilayer Optical Neural Network. *Sci. Adv.* **2024**, *10*, eado8516. <https://doi.org/10.1126/sciadv.ado8516>.
70. Lu, H.; Yin, Z.; Bhoumik, P.; Banerjee, S.; Chakrabarty, K.; Gu, J. The Unlikely Hero: Nonidealities in Analog Photonic Neural Networks as Built-In Adversarial Defenders. In *Proceedings of the Asia and South Pacific Design Automation Conference (ASP-DAC)*; Association for Computing Machinery: New York, NY, USA, 2025; pp. 1295–1301. <https://doi.org/10.1145/3658617.3697771>.
71. Argyris, A.; Syvridis, D.; Larger, L.; Annovazzi-Lodi, V.; Colet, P.; Fischer, I.; Garcia-Ojalvo, J.; Mirasso, C.R.; Pesquera, L.; Shore, K.A. Chaos-Based Communications at High Bit Rates Using Commercial Fibre-Optic Links. *Nature* **2005**, *438*, 343–346. <https://doi.org/10.1038/nature04275>.
72. Mao, X.; Fan, X.; Wang, L.; Fu, S.; Wang, Y.; Wang, A. 86-Gb/s Optical Chaos Communication Over 100-km Fiber Transmission Using Semiconductor Lasers. In *Proceedings of the 49th European Conference on Optical Communications (ECOC 2023)*; IEEE: Piscataway, NJ, USA, 2023; pp. 5–8. <https://doi.org/10.1049/icp.2023.1833>.
73. Cheng, M.; Gao, X.; Deng, L.; Liu, L.; Deng, Y.; Fu, S.; Zhang, M.; Liu, D. Time-Delay Concealment in a Three-Dimensional Electro-Optic Chaos System. *IEEE Photonics Technol. Lett.* **2015**, *27*, 1030–1033. <https://doi.org/10.1109/LPT.2015.2405564>.
74. Huang, H.; Li, Z.; Gao, X.; Cheng, M. An Enhanced Electro-Optic Chaos Secure Communication System Immune to Time Delay Signature Extraction. *IEEE Photonics J.* **2022**, *14*, 7209407. <https://doi.org/10.1109/JPHOT.2021.3139725>.
75. Gong, S.; Zhu, J.; Chen, S.; Wang, J.; Cheng, M.; Gao, X. Time Delay Signature Extraction of Optical Time-Delay Chaos Systems From Short and Noisy Time Series. *IEEE Photonics J.* **2025**, *17*, 7200207. <https://doi.org/10.1109/JPHOT.2024.3516115>.
76. Liu, J.; Zhang, J.; Wang, Y. Secure Communication via Chaotic Synchronization Based on Reservoir Computing. *IEEE Trans. Neural Netw. Learn. Syst.* **2024**, *35*, 285–299. <https://doi.org/10.1109/TNNLS.2022.3173516>.
77. Zhu, P.; Wang, H.; Ji, Y. Security Performance Enhancement Chaotic Optical Communication System Based on Reservoir Computing for Physical-Layer Security. *J. Light. Technol.* **2024**, *42*, 8628–8639. <https://doi.org/10.1109/jlt.2024.3435457>.
78. Zaminga, S.; Martinez, A.; Huang, H.; Rontani, D.; Morichetti, F.; Melloni, A.; Grillot, F. Optical Chaotic Signal Recovery in Turbulent Environments Using a Programmable Optical Processor. *Light. Sci. Appl.* **2025**, *14*, 131. <https://doi.org/10.1038/s41377-025-01784-3>.
79. Jiang, X.; Xie, Y.; Liu, B.; Chai, J.; Ye, Y.; Song, T.; Feng, M.; Yuan, H. Image Transformation Based on Optical Reservoir Computing for Image Security. *Expert Syst. Appl.* **2024**, *237*, 121376. <https://doi.org/10.1016/j.eswa.2023.121376>.
80. Shao, W.; Cheng, M.; Luo, H.; Deng, L.; Yang, Q.; Liu, D. High-Speed Secure Key Distribution With Polarization Modulation Boosted by Broadband Optical Chaos. In *Proceedings of the 2021 Asia Communications and Photonics Conference (ACP)*, Shanghai, China, 24–27 October 2021; pp. 1–3.
81. Zhu, P.; Wang, H.; Ji, Y. A Novel Source Separation Chaotic Optical Communication Architecture Based on Deep Cascade Time-Delay Reservoir Computing. *J. Light. Technol.* **2026**, *44*, 4381–4392. <https://doi.org/10.1109/JLT.2026.3674193>.
82. Wang, J.; Lau, A.P.T.; Lu, C. Sensing as a Service: Can In-Band Distributed Fiber Optic Sensing Coexist With Coherent Metro DWDM Communication Network? *J. Light. Technol.* **2026**, *44*, 1712–1720. <https://doi.org/10.1109/JLT.2025.3647287>.
83. He, T.; Sun, Q.; Zhang, S.; Li, H.; Yan, B.; Fan, C.; Yan, Z.; Liu, D. A Dual-Stage-Recognition Network for Distributed Optical Fiber Sensing Perimeter Security System. *J. Light. Technol.* **2023**, *41*, 4331–4340. <https://doi.org/10.1109/JLT.2022.3222472>.
84. You, J.; Men, Y.; Liu, Y.; Zhang, K.; Yu, M.; Li, Y.; Fang, Q.; Zhou, R.; Li, X.; Chen, H. DAS-Based Perimeter Intrusion Detection Using 2D-CNN With SKAttention Mechanism. *IEEE Sensors J.* **2025**, *25*, 41320–41328. <https://doi.org/10.1109/JSEN.2025.3614201>.
85. Pamukti, B.; Afifah, S.; Liaw, S.K.; Sung, J.Y.; Chu, D. Intelligent Pattern Recognition Using Distributed Fiber Optic Sensors for Smart Environment. *Sensors* **2025**, *25*, 47. <https://doi.org/10.3390/s25010047>.
86. Wakisaka, Y.; Di Rosa, G.; Fan, Q.; Rochat, E.; Sandmann, A.; Liu, X.; Wey, J.S. ITU-T G.681: The First Distributed Fiber Optic Sensing Standard for In-Service Terrestrial Optical Networks. *J. Opt. Commun. Netw.* **2026**, *18*, B1–B8. <https://doi.org/10.1364/JOCN.586758>.
87. Jeong, S.; Kim, H.; Kim, Y.H.; Park, C.S.; Jung, H.; Kim, H.K. Spatiotemporal Anomaly Detection in Distributed Acoustic Sensing Using a GraphDiffusion Model. *Sensors* **2025**, *25*, 5157. <https://doi.org/10.3390/s25165157>.
88. Wu, H.; Wang, Y.; Liu, X.; Sun, Y.; Yan, G.; Wu, Y.; Rao, Y. Smart Fiber-Optic Distributed Acoustic Sensing (sDAS) With Multitask Learning for Time-Efficient Ground Listening Applications. *IEEE Internet Things J.* **2024**, *11*, 8511–8525. <https://doi.org/10.1109/JIOT.2023.3320149>.

89. National Institute of Standards and Technology. *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0*; Technical report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020. <https://doi.org/10.6028/NIST.CSWP.01162020>.
90. Tabassi, E. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*; NIST Trustworthy and Responsible AI NIST AI 100-1; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023. <https://doi.org/10.6028/NIST.AI.100-1>.

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.