

Authentication and Access Control in Li-Fi-Based Wireless Networks

Ljubinko Stojanović, Petar Spalević, University Sinergija, Bijeljina

Abstract — Light Fidelity (Li-Fi) represents an emerging wireless communication paradigm that operates within heterogeneous network environments characterized by high mobility, multi-user access, and frequent handovers between technologies. While Li-Fi offers significant advantages in terms of bandwidth and spatial confinement through optical „attocell” domains, these same characteristics introduce a distinct and complex security landscape.

Threat models emphasize the importance of the attacker’s spatial position and optical visibility, going beyond the traditional division into internal and external actors. Active and passive attacks, including interception through reflection and light leakage, etc., can exploit the physical characteristics of the system to compromise the confidentiality and integrity of communication. Special focus is placed on the CIA+Auth model (confidentiality, integrity, availability, and authentication) as the basis for designing secure systems. The ABAC model provides greater flexibility and suitability for Li-Fi environments due to the ability to include contextual factors such as location, time, and risk level.

Keywords – CIA (Confidentiality, Integrity, Availability), Li-Fi (Light Fidelity), Authentication, Access Control

I. INTRODUCTION

In practice, we can encounter two standardization lines: 1. The IEEE 802.11bb standard from 2023 formally introduced light communications into the IEEE 802.11 ecosystem [1], thereby bringing Li-Fi closer to existing Wi-Fi network architectures and security mechanisms; 2. The IEEE 802.15.7 standard for short-range optical wireless links (PHY/MAC) [2].

Security requirements in Li-Fi networks are based on protecting communication against eavesdropping, jamming, spoofing, and node compromise, while adapting to the physical and operational behavior of the light medium [3]. The conclusion drawn in the contemporary literature on optical wireless links is that the „physical confinement of light” [1] exists, but it is not a sufficient security guarantee – reflections [4], light leakage [5], etc. From this follows the fundamental requirement – Li-Fi networks must have a cryptographically clear model (CIA+Auth) independent of assumptions about LoS/NLoS [1].

II. SECURITY THREATS IN LI-FI SYSTEMS

Li-Fi is treated as part of heterogeneous networks with mobility, handover, and multi-user access; while the optical layer provides high capacity in „attocell” [1] domains. Based on such an architecture, a) vertical handover between technologies [6], [1] and b) shared AAA policies between access domains [7] are introduced. Threat models according to the VLC/Li-Fi security literature are explicitly classified by spatial position and optical visibility, and not only by network privileges (outsider/insider) [5], and can be divided roughly, for the purpose of requirements design, into: 1) outsider threat [5] – does not possess network privileges nor cryptographic keys (attempts interception through leakage/reflections or jamming); 2) insider threat – possesses access to the light-covered zone or is a group member (e.g. possesses a group key [8]) and these attacks can be classified more into the domain of abuse of legitimate privileges, especially when group keys are concerned; 3) active threat with an optical injector [5] – uses an LED or laser source (or a compromised „smart” luminaire) for spoofing [9] or jamming, which is particularly important for „smart lighting” – IoT ecosystems [1]; 4) passive threat with enhanced optics (uses receivers to improve SNR and intercept weak reflected components), while attacks can be divided into: 1) interception through reflections and light leakage (sniffing) which can escalate into spoofing or Man-in-the-Middle (MITM) [10]; 2) jamming (optical interference); 3) spoofing/impersonation of light sources [9]; 4) side channels (e.g. optical emanations) [5].

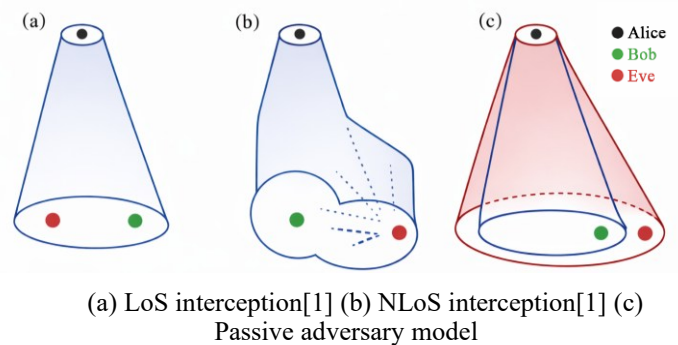


Illustration 1. Sniffing attack scenario [11]

In Illustration 1[11], different interception (sniffing) attack scenarios are shown, which can escalate into spoofing or Man-in-the-Middle (MITM) attacks [10]. Alice is the transmitter, Bob is the receiver, and Eve is the attacker. In (a) a scenario of an interception attack is shown where Alice (transmitter) sends data to Bob (receiver) and any other receiver (in this

case Eve - attacker) can receive the signal and intercept the message. The scattering of light caused by surfaces that produce it (scattering) is shown in (b). The attacker is outside the zone covered by the emission from Alice, in a corner of the room or outside it – Eve can in this way receive enough

information for interception. In (c) Eve functions as a passive entity and receives the signal without direct interaction with it – such a scenario opens the possibility for attackers not only to intercept traffic, but also to actively interact with the network.

Table 1. Comparative Analysis of Li-Fi Security Standards and Protocols

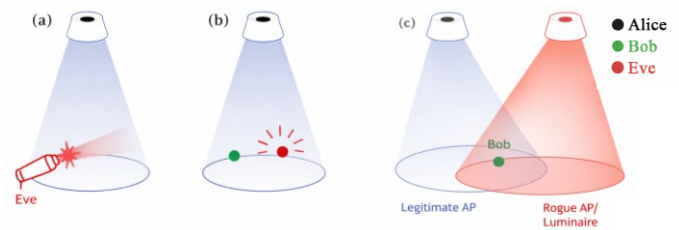
Item	Year	Standard / Source	Focus	Method	Advantages	Disadvantages	Applicability in Li-Fi
IEEE 802.11bb [12]	2023	IEEE standard	Introduction of Li-Fi into WLAN	802.11 Light Communications	Easier integration with existing WLAN/AAA systems	Security details are not clearly specified in public summaries	High
IEEE 802.15.7 [13]	2018	IEEE standard	Link-layer security in OWC	PHY/MAC for OWC	Basic standard for VLC/Li-Fi systems	Key management is not defined	Medium to high
802.15.7 MAC security [14]	2011/2018	IEEE 802.15.7	Confidentiality, integrity, anti-replay	AES-128 CCM*, MIC, frame counter	Multiple security levels, replay protection	Does not protect all headers, key management not defined	High
IEEE 802.1X [15]	2020	IEEE standard	Network access control	Port-based access control	Mature AAA model	Requires additional infrastructure	High
EAP-TLS 1.3 [16]	2022	IETF RFC 9190	Mutual authentication and key exchange	TLS 1.3 over EAP	Strong identity and robust security	Certificates can be large and difficult to deploy	High
TLS 1.3 [17]	2018	IETF RFC 8446	Transport security	TLS 1.3	Standard and strong data protection	Does not address physical attacks on the Li-Fi link	High
EDHOC [18]	2024	IETF RFC 9528	Lightweight authentication for IoT	Compact AKE	Suitable for constrained devices	Requires a compatible IoT ecosystem	High
OSCORE [19]	2019	IETF RFC 8613	End-to-end protection of CoAP messages	COSE-based protection	Protects data even through gateways/proxies	Does not handle network access control	High
EPLSSBJ [20]	2019	IEEE TIFS	Eavesdropping protection	Beamforming + jamming	Improves secrecy performance	Depends on attacker and channel assumptions	High
VL-Watchdog [21]	2022	IEEE IoT Journal	Spoofing attack detection	Redundant coding + monitoring	Practical detection of fake light sources	Increased complexity and additional hardware	High
BGPFA [22]	2023	Optics Communications	Secure handover and authentication	Group authentication + reauthentication + quick rejoin	Reduced latency and fewer interruptions	Focused on a specific scenario	High

Table 2. Classification of Attacks in Li-Fi Systems [11]

Attack Category	Representative Attacks
Physical Attacks	Rogue access point (rogue luminaire), jamming, signal injection, sensor blinding/saturation, light leakage exploitation
Passive Attacks	Snooping, sniffing, eavesdropping, reflection-based interception, traffic analysis
Active Attacks	Man-in-the-Middle (MITM), spoofing, replay attack, frame injection, DoS/DDoS attacks, authentication flooding, deauthentication/disassociation
MAC Layer Attacks	MAC spoofing, beacon spoofing, association hijacking, frame collision exploitation
PHY Layer Attacks	Optical jamming, optical injection, signal distortion, photodetector saturation, interference attacks

The table systematizes different categories of threats in the Li-Fi environment according to the level at which they operate

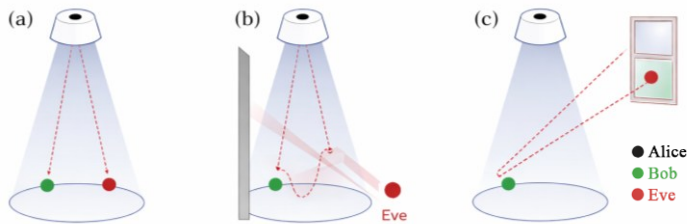
and the manner in which the attack is carried out. The classification includes physical, passive, and active approaches, as well as attacks directed at specific communication layers.



(a) External optical jamming; (b) In-cell jamming; (c) Rogue luminaire/infrastructure jamming

Illustration 2. Jamming attack scenario

In scenario (a), the attacker Eve is located outside the direct Line-of-Sight (LoS) path, but uses a strong light source (e.g. a laser or a directed LED) toward Bob. Unlike (a), where Eve is outside the LoS, in scenario (b) Eve is located within the same attocell zone as Bob and generates interference using her own device (LED transmitter) with the same or similar modulation, causing an increase in BER (Bit Error Rate) and a drop in SNR (Signal-to-Noise Ratio). Bit Error Rate (BER) directly describes the reliability of data transmission. In its most basic form, BER is defined as the ratio of the number of incorrectly detected bits to the total number of transmitted bits in a communication system. In a Li-Fi system, where high data transmission rates are targeted, BER represents a trade-off between spectral efficiency and reliability. If a low BER is required, it is necessary either to increase SNR by increasing power or applying filtering, or to sacrifice part of the spectral efficiency by using simpler modulation. A high SNR means that the signal power is much greater than the noise power, while a low SNR leads to the signal being comparable to noise, meaning that the receiver has difficulty distinguishing bits, which results in an increase in Bit Error Rate (BER). [1]



(a) LoS snooping; (b) Reflection-based snooping; (c) Light leakage snooping

Illustration 3. Snooping attack scenario

In scenario (a), Eve is located within the illumination cone (LoS) and directly receives the signal that Alice sends to Bob. Eve uses a photodetector to receive the signal and compromises confidentiality without active interaction with the network. Signal scattering (diffuse reflection) shown in (b) reaches Eve who is located outside the LoS zone, reconstructs the signal where the quality is weaker, but still usable. Also, signal scattering occurs due to the reflection of light from surfaces (walls, floor, glass) [1]. In scenario (c), Eve is located outside the physical space (window) and, based on light leakage, intercepts communication without physical access to the space.

III. CIA+AUTH

CIA (confidentiality, integrity, availability) is a practical model for defining the objectives of information security and measuring the consequences of compromise – unauthorized disclosure (C), unauthorized modification (I), and interruption/slowing of service (A). [23] There are at least 3 steps of access control: 1. identification – the user says „who they are”; 2. authentication – the user proves identity; 3. authorization – the system decides what is permitted [24]. Authentication by itself does not guarantee either confidentiality or integrity, but without authentication it is difficult or even impossible to consistently enforce

authorization, audit, and accountability. Authentication reduces the probability of unauthorized access to data by making it harder for an attacker to present themselves as an authorized user – session theft, password theft, or a compromised token; it links modifications to identity and enables control of „who changed what,” digital signatures (PKI) [23], stronger audit trails, and non-repudiation mechanisms in high-stakes transactions, and it can help in defense against abuse, but it can also threaten availability if it is poorly designed. [25]

A single compromised identity typically leads to: (1) unauthorized reading (C), (2) unauthorized modifications and fraud (I), and (3) operational disruptions (A) through privilege escalation, configuration changes, or locking out legitimate users. Incidents show that even when „production data” does not leak, an attacker can compromise the availability and integrity of internal tools through a compromised account.

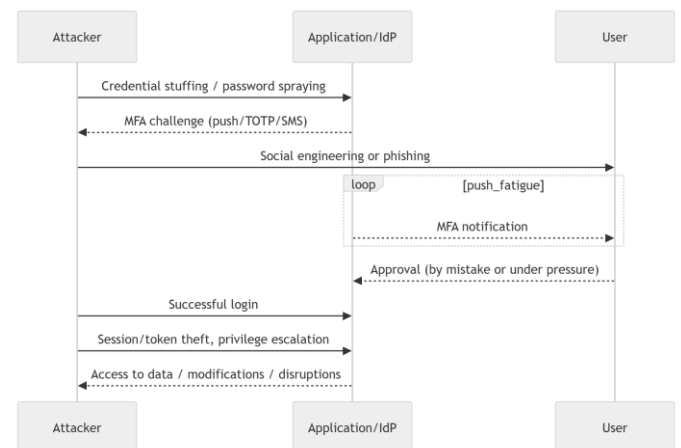


Diagram 1. MFA Bypass Attack

The role-based access control (RBAC) model introduces the idea that access decisions are based on the user's function/role within the organization, whereby users obtain privileges through role assignment (administrator, editor, manager), rather than through ad-hoc access lists per object. Here, privileges are not discretionary „ownership” of the user, but are centrally defined through organizational functions. [26] Unlike RBAC, the attribute-based access control (ABAC) model formalizes authorization as the evaluation of policies over a set of attributes of subjects (users or devices), object attributes, and environmental conditions. According to NIST, it is a method where a subject's request to perform operations on an object is approved or denied based on assigned subject attributes, assigned object attributes, and policies expressed over those attributes. What makes it relevant for Li-Fi are environmental conditions. Environmental conditions in the NIST framework are described as stationary context independent of the subject and object, and can explicitly include current time, user location, and threat state – thereby naturally incorporating decision factors. [27]

There are 2 reasons why ABAC is more practical than RBAC: 1. Li-Fi cells are small and user mobility is expected

[1], so handover is frequent, which makes static policies based only on roles less efficient [4]. In such an environment, authorization that includes conditions such as: „while the user is in zone X / during working hours / under low risk” is more naturally expressed as an ABAC rule than as a multitude of specialized roles. [27] 2. The Li-Fi/VLC ecosystem naturally enables relatively precise contextualization of location [1] [2], and at the same time VLC-based systems can achieve accuracy on the order of 10 cm in controlled conditions [1], which makes „location” a realistic candidate for an attribute in policy.

IV. CONCLUSION

This paper analyzed security in Li-Fi systems, where the context is modern wireless networks, with a particular focus on threats arising from the specific physical and communication characteristics of the optical medium. Although Li-Fi, due to the spatial confinement of the light signal and non-penetration through physical obstacles, has an advantage over conventional RF systems, this is not sufficient. Reflections, light leakage, jamming, spoofing of sources, node

compromise, and others confirm the requirement for a comprehensive and cryptography-based network model.

In parallel, the importance of the CIA+Auth model as a basis for defining security requirements in Li-Fi networks was considered, due to characteristics such as the protection of confidentiality, integrity, and availability, which cannot be effective without clearly defined mechanisms of identification, authentication, and authorization, especially in modern Li-Fi systems which, due to user mobility, frequent handover processes, and the need for contextual decision-making, exceed the capabilities of static access control, and in this sense, models such as RBAC and particularly ABAC provide a significant foundation for establishing flexible and precise access management in optical networks.

Future research should be focused on the development of integrated security architectures for Li-Fi systems that would combine physical protection of the optical layer with advanced authentication models and contextual authorization.

REFERENCES

- [1] Lj. Stojanović, LI-FI Systems, Master's thesis, Faculty of Computer Science and Informatics, Sinergija University, Bijeljina, Republic of Srpska, 2025, pp. 5, 11, 14-19, 47-49, 50.
- [2] Lj. Stojanovic, V. Radojčić, and P. Spalević, *Li-Fi, AI, and IoT Technologies in Creating Sustainable Business*, 2025, pp. 63-64.
- [3] Lj. Stojanović, V. Radojčić, S. Mitrović and P. Spalević, Li-Fi Technology for Cybersecurity Solutions + SEON, 2025, pp. 56-58.
- [4] H. Haas, L. Yin, C. Chen, S. Videv, D. Parol, E. Poves, H. Alshaer, and M. S. Islam, „Introduction to indoor networking concepts and challenges in LiFi,” *Journal of Optical Communications and Networking*, vol. 12, no. 2, 2020, pp. 193-196.
- [5] J. Classen, J. Chen, D. Steinmetzer, M. Hollick, and E. W. Knightly, „The Spy Next Door: Eavesdropping on High Throughput Visible Light Communications,” in Proc. 2nd Int. Workshop on Visible Light Communication System, Paris, France, Sep. 2015, pp. 11-14.
- [6] J. Sanusi, A. Aibinu, S. Adeshina, and S. Idris, „Review of Handover in Li-Fi and Wi-Fi Networks”, 2020, pp. 956-960.
- [7] X. Wu, M. D. Soltani, L. Zhou, M. Safari, and H. Haas, „Hybrid LiFi and WiFi Networks: A Survey,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, 2021, pp. 1399-1401.
- [8] X. Zhang, G. Klevering, X. Lei, Y. Hu, L. Xiao, and G. Tu, „The Security in Optical Wireless Communication: A Survey,” *ACM Computing Surveys*, vol. 55, no. 12, 2023, pp. 9.
- [9] J. Chen and T. Shu, „VL-Watchdog: Visible Light Spoofing Detection With Redundant Orthogonal Coding,” *IEEE Internet of Things Journal*, vol. 9, no. 13, 2022, pp. 9859-9862.
- [10] V. Guerra, J. Rabadan, L. Palmas, and D. G. Canaria, „Data Sniffing Over an Open VLC Channel,” in Proc. IEEE Int. Conf. on Consumer Electronics (ICCE), 2012, pp. 1-6.
- [11] E. Ramadhani, „A Mini Review of LiFi Technology: Security Issue,” *International Journal of Computer and Information System (IJCIS)*, vol. 3, no. 3, 2022, pp. 92.
- [12] IEEE, „IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Light Communications,” IEEE Std 802.11bb-2023, 2023.
- [13] IEEE, „IEEE Standard for Local and Metropolitan Area Networks—Part 15.7: Short-Range Optical Wireless Communications,” IEEE Std 802.15.7-2018, 2019.
- [14] G. J. Blinowski, „Practical Aspects of Physical and MAC Layer Security in Visible Light Communication Systems,” *International Journal of Electronics and Telecommunications*, vol. 62, no. 1, 2016.
- [15] IEEE, „IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control,” IEEE Std 802.1X-2020, 2020.
- [16] J. Preuß Mattsson and M. Sethi, „EAP-TLS 1.3: Using the Extensible Authentication Protocol with TLS 1.3,” RFC 9190, 2022.
- [17] E. Rescorla, „The Transport Layer Security (TLS) Protocol Version 1.3,” RFC 8446, 2018.
- [18] G. Selander, J. Preuß Mattsson, and F. Palombini, „Ephemeral Diffie-Hellman Over COSE (EDHOC),” RFC 9528, 2024.
- [19] G. Selander, J. Preuß Mattsson, F. Palombini, and L. Seitz, „Object Security for Constrained RESTful Environments (OSCORE),” RFC 8613, 2019.
- [20] S. Cho, G. Chen, and J. P. Coon, „Enhancement of Physical Layer Security With Simultaneous Beamforming and Jamming for Visible Light Communication Systems,” *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, pp. 2633-2648, 2019.
- [21] J. Chen and T. Shu, „VL-Watchdog: Visible Light Spoofing Detection With Redundant Orthogonal Coding,” *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9858-9871, 2022.
- [22] X. Wang, C. Gan, S. Wu, Y. Chen, and Y. Chen, „Bi-group pre-handover authentication model solving signaling congestion of subway LiFi network,” *Optics Communications*, vol. 536, art. no. 129384, 2023.
- [23] National Institute of Standards and Technology (NIST), „Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events (Executive Summary),” NIST Special Publication 1800-26A, 2020, pp. 1-3.
- [24] CERT, „Višefaktorska autentifikacija,” CERT.hr-PUBDOC-2018-12-370, Dec. 2018, pp. 3-10.
- [25] OWASP Foundation, „Authentication Cheat Sheet,” OWASP Cheat Sheet Series. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
- [26] D. F. Ferraiolo and D. R. Kuhn, „Role-Based Access Controls,” in Proc. 15th National Computer Security Conference (NCSC), Baltimore, MD, USA, 1992, pp. 555-563.
- [27] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, „Guide to Attribute Based Access Control (ABAC) Definition and Considerations,” NIST Special Publication 800-162, 2014, pp. 5-17.