

Li-Fi Communication in the Context of Zero Trust Security Models

Ljubinko Stojanović, Vesna Radojčić, Petar Spalević, University Sinergija, Bijeljina

Abstract — Greater decentralization of modern IT environments, driven by distributed infrastructure, IoT devices, etc., has highlighted the limitations of traditional perimeter-based security models, which are based on the assumption that the internal network is trusted, while threats exist exclusively outside of it. Implicit trust and broad internal access that perimeter environments have can create – and do create – favorable conditions for lateral movement, insider misuse, and unauthorized access. This paper examines Zero Trust Architecture (ZTA) as a security paradigm designed to address these weaknesses. In parallel, the paper analyzes Li-Fi (Light Fidelity) communication as an alternative wireless technology whose physical properties, including spatial signal limitation and reduced penetration through walls, offer significant cybersecurity advantages compared to conventional radio-frequency systems, but since the physical environment alone does not guarantee protection, cryptographic protection mechanisms in Li-Fi environments are emphasized. By combining the Zero Trust model with Li-Fi communication and secure key management mechanisms, a layered approach is provided for securing sensitive internal wireless communication against eavesdropping, message manipulation, and unauthorized access.

Keywords – ZTA (Zero Trust Security Models), Li-Fi (Light Fidelity), Perimeter, Unauthorized Access, Encryption

I. INTRODUCTION

The digitalization of infrastructure has fundamentally weakened the boundaries of the traditional network. Enterprises, currently, increasingly operate through cloud platforms, distributed infrastructure with employees located in different locations; therefore, security models are structurally no longer adequate. The paper from 2020 confirms this, stating that "this complexity has outstripped legacy methods of perimeter-based network security as there is no single, easily identified perimeter for the enterprise" [1] and also that "zero trust security models assume that an attacker is present in the environment and that an enterprise-owned environment is no different – or no more trustworthy – than any nonenterprise-owned environment" [1]. Zero Trust Architecture (ZTA), a term first introduced by John Kindervag [2], [3], emerged as a structural response, built on the principle of "verify and never trust" [3]. Security paradigms have historically developed reactively – as a response to new threats and attacks. According to the paper from "The concept of cybersecurity emerged alongside the development of computer networks and digital communication systems," with early security focused on physical access control of ARPANET mainframe systems [4].

The drawback of perimeter-based models, fundamentally, is their binary trust model. Entities within the network boundaries receive implicit permanent trust (if the user is outside the network → considered untrusted; if the user is inside the network → automatically considered trusted) without additional verification of identity or access context. In practice, a compromised computer within the network can freely access other systems. Once it breaches the perimeter, it can move through the network, and so-called lateral movement becomes relatively simple. As a result, "unauthorized lateral movement within the environment has been one of the biggest challenges" [1]. The CCDCOE Insider Threat Study [5] confirms the previous statement based on the analysis of the Snowden and Manning cases, where it is seen that the greatest damage was caused precisely by users with legitimate access (implicit, permanent trust) granted by the perimeter.

The evolution and change of threats in decentralized IT systems have created a completely different set of attack vectors and adversarial methodologies that differ fundamentally from the threats that formed the basis for the structure of traditional, perimeter-oriented security architectures. [6] In traditional enterprise security models, the perimeter refers to the conceptual and technical boundary that separates the organizational internal network – assumed to be trusted – from external, untrusted networks such as the public internet; the perimeter model envisions the network as a fortress where the interior is secure, and all entrances are controlled and filtered. [7] Perimeter protection is achieved through technical mechanisms such as Firewalls, Gateway proxies, Intrusion detection/prevention systems (IDS/IPS), and virtual private networks (VPN). [8] Therefore, perimeter-oriented security architectures were built on the principle of strong external defense and relatively permissive internal access. [9] Once a user authenticates and passes the perimeter boundary, they are often granted broad lateral movement privileges within the internal network. The perimeter model emerged in an era when business infrastructure was physically centralized, applications were hosted locally, employees worked within enterprise facilities, and the network topology was relatively static, making defense of a clearly identifiable boundary technically feasible and operationally rational. [10]

At its core, Li-Fi is a wireless optical network created as an extension of visible light communication (VLC) that transforms lighting fixtures into access points and integrates with the existing network ecosystem. [11] It has proven to be „an efficient solution for wireless communication, offering advantages such as superior cybersecurity [12].“

II. CONCEPT OF ZERO-TRUST ARCHITECTURE

The Zero Trust Architecture (ZTA) represents a security model based on the assumption that no element within the system possesses implicit trust. „No user, device, or application – not even those inside the network – should be automatically trusted.” [13] The fundamental principle of ZTA is expressed as „never trust, always verify,” which means that every connection and request for access to resources is verified in real time. [13] [14] The National Institute of Standards and Technology (NIST) defines Zero Trust Architecture as „an enterprise cybersecurity architecture based on zero trust principles and designed to prevent data breaches and limit internal lateral movement of attackers,” [1] viewing the network as potentially compromised and applying the strictest criteria for identity verification and authorization of every request for resource access. [13], [15] Conventional perimeter-based security models assume that threats originate outside the network, treating the internal environment as inherently secure. However, IT systems – including cloud services, IoT devices – are geographically and technologically distributed, and thus the network boundary practically does not exist. As a result, traditional measures such as Firewalls and VPNs are insufficient to prevent and protect against threats originating from within [14], [1], and Zero Trust Architecture (ZTA) has emerged as a paradigm representing the „presence of an attacker within the environment” [1] and requiring continuous verification of the identity of all users, regardless of their location. ZTA is based on a set of technical principles that NIST classifies as seven fundamental tenets, defining how an organization should protect data and resources regardless of network context:

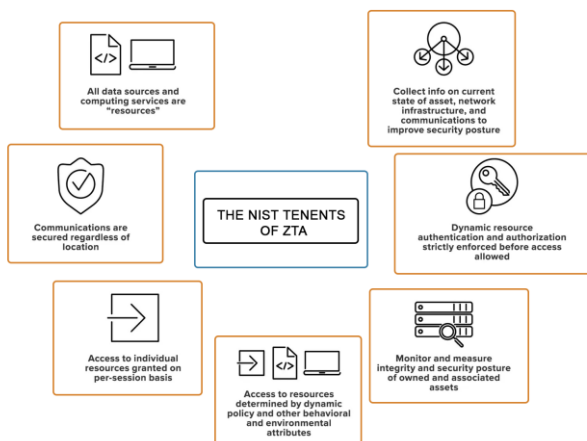


Illustration 1. NIST tenets of Zero Trust Architecture. [16]

According to the National Institute of Standards and Technology, the key elements of the ZTA model include control points (Policy Enforcement Points – PEP), a decision-making module (Policy Engine – PE), and a component responsible for implementing decisions (Policy Administrator

– PA). [1] The set of control points forms the control layer of the network, separated from the data flow, so that every connection is verified through an autonomous decision system. The Policy Engine collects information from various sources (databases, device management systems, etc.) and applies a trust algorithm to approve or deny the access request – the policy is established for a specific resource based on initial rules and additional real-time factors. [15]

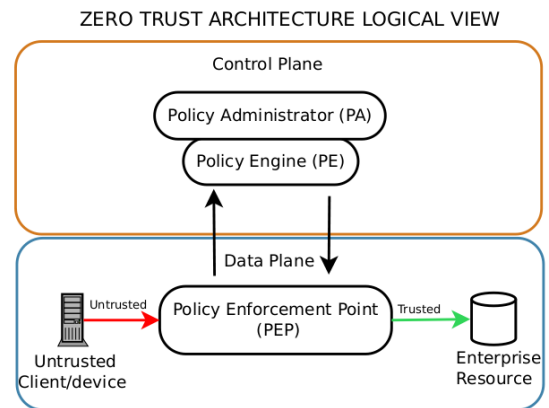


Illustration 2. Zero Trust Architecture logical view [17]

III. LI-FI (LIGHT FIDELITY) COMMUNICATION OVERVIEW

In a Li-Fi system, the transmitter is usually an LED light source (or a group of LEDs as in a lighting fixture), while the receiver is a photodetector (PD) consisting of one or more photodiodes (or a group of photodiodes). Data is transmitted by modulating the current of the LED, which changes the light intensity, and the photodetector converts the light intensity into an electrical current. [11]

A Li-Fi system uses light photons instead of RF waves, so the signal requires optical visibility or reflections in order to reach the receiver. Unlike radio waves, light does not penetrate opaque obstacles (e.g., walls) [11], which means that the coverage of a Li-Fi network is limited to the room in which the light source is located. [12] The advantage of this property is that there is no mutual interference between neighboring rooms, and security is improved (the signal is „contained” within the room). The drawback, however, is sensitivity to signal blockage – if an obstacle appears between the LED and the photodiode, the direct signal will be interrupted. In such situations, reception is possible through diffuse reflections from walls or the ceiling, but with a significantly weaker signal level. [12] Because of this, Li-Fi systems usually require multiple lighting fixtures within a single room in order to ensure good coverage regardless of the user’s position. The Li-Fi channel consists of two types of paths: a direct path with a line of sight (Line-of-Sight, LOS) and indirect paths without direct visibility (Non-Line-of-Sight, NLOS) [18] created by reflections from surfaces within the room.

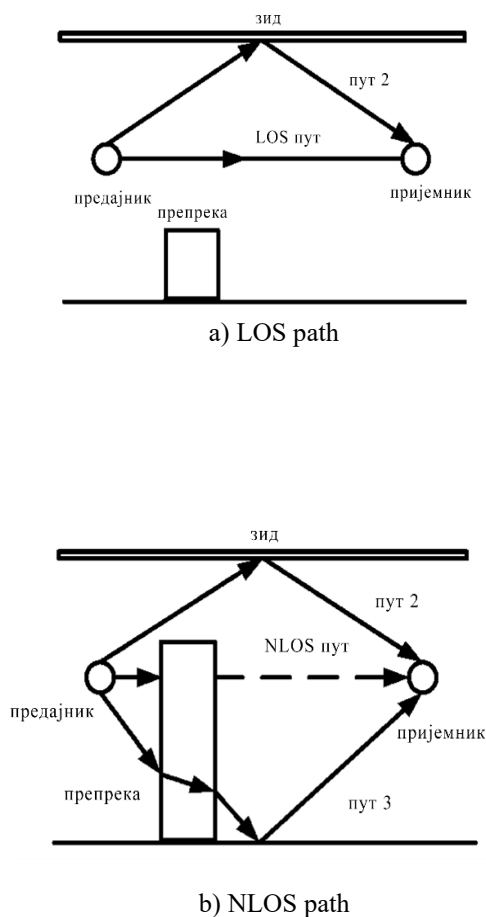


Diagram 1. Schematic diagram of signal propagation paths within a room with obstacles (LOS and NLOS) [11]

The limited range and the signal contained within the room naturally increase security against remote attacks (e.g., an attacker standing outside the room cannot eavesdrop on the connection, unlike in Wi-Fi systems [11]). In addition, it is important to emphasize that the Li-Fi connection is limited to the illuminated zone, i.e., it is easier to physically control user access (e.g., motion detectors in the room). [12] On the other hand, in the case where light passes through a window or similar openings, the signal can be intercepted from the immediate surroundings, which indicates that, without encryption, there is still a risk of interception. [11]

Encryption can be implemented in the application software itself before the data enters the Li-Fi interface (SSL/TLS tunnel, or VPN, or some other tool) – advantage: high flexibility and independence from the physical characteristics of the connection; disadvantage: it depends on the built-in cryptography on end devices and reduced performance (additional processing) [20]. At the MAC layer level, Li-Fi devices can use standards similar to Wi-Fi mechanisms. IEEE 802.15.7 standards for visible optical communication allow the use of encryption that is otherwise applied in wireless networks (AES, WPA2 [11]). The advantage of this encryption is in terms of standardization and a smaller impact

on the physical layer (entire MAC frames are encrypted before modulation), but latency increases [20].

The most important cryptosystem for Li-Fi is AES (Advanced Encryption Standard). It is also considered an industry standard and is usually used with an authenticated mode (e.g., CCM or GCM). Advanced Encryption Standard (AES) is a symmetric block cryptography algorithm that is an international standard for the security of digital data. [21] It replaced DES, which was widely used but was replaced due to its short key length. It makes all actions that an entity may use more difficult, preventing code breaking by entities that should not have access to the information. Other symmetric algorithms include Blowfish and older Rivest ciphers such as RC4, RC5, and RC6. [20] These algorithms are mentioned in the literature as examples that can be applied within the Li-Fi framework. The application of appropriate cryptographic algorithms enables a high level of protection: the use of AES-128-GCM [23], for example, in demonstration Li-Fi systems protects against eavesdropping and unauthorized modifications. This project combines authenticated encryption and persistent key management to ensure the confidentiality and integrity of Li-Fi-transmitted data. By using AES-128-GCM and secure session-key provisioning between the Raspberry Pi Pico and the host, it establishes a protected communication channel resistant to unauthorized access and message tampering.

IV. CONCLUSION

This paper examined the limitations of traditional perimeter-based security models in the context of modern, decentralized IT environments and highlighted the necessity for more adaptive and resilient security paradigms. In this regard, Zero Trust Architecture (ZTA) was analyzed as a contemporary approach that eliminates implicit trust and enforces continuous verification of all entities, regardless of their location within or outside the network.

In parallel, the paper explored Li-Fi (Light Fidelity) communication as an emerging wireless technology with inherent physical-layer security advantages. Due to its reliance on visible light, Li-Fi offers spatial confinement of the signal, reduced penetration through physical barriers, and lower susceptibility to remote interception compared to conventional radio-frequency systems. However, it was emphasized that these physical properties alone are not sufficient to ensure complete security, which necessitates the implementation of robust cryptographic mechanisms.

The main contribution of this paper lies in highlighting the complementary nature of ZTA and Li-Fi technologies. While ZTA provides a strong logical and architectural security framework based on strict access control and continuous authentication, Li-Fi enhances security at the physical layer by limiting signal exposure. Their combined application enables a layered security approach that significantly reduces the risk of eavesdropping, unauthorized access, and lateral movement within internal networks.

Future research directions should focus on the development of integrated architectures that explicitly combine ZTA principles with Li-Fi communication systems in

real-world environments. Additionally, experimental validation of such models through simulations or prototype implementations is necessary to evaluate performance, scalability, and resistance to advanced attack scenarios.

REFERENCES

- [1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, National Institute of Standards and Technology, 2020, pp. 1, 4, 6-7.
- [2] F. Mensah, "Zero Trust Architecture: A Comprehensive Review of Principles, Implementation Strategies, and Future Directions in Enterprise Cybersecurity," *International Journal of Academic and Industrial Research Innovations (IAIRI)*, vol. 10, 2024, pp. 340.
- [3] J. Kindervag, *No More Chewy Centers: Introducing the Zero Trust Model of Information Security*, Cambridge, MA, USA: Forrester Research Inc., 2010, pp. 9.
- [4] S. N. Asha, B. Asiya Banu, and M. J. Swetha, "Cybersecurity: Evolution, challenges, and future directions in digital security," *World Journal of Advanced Research and Reviews*, vol. 10, no. 01, 2021, pp. 428.
- [5] M. Kont, M. Pihelgas, J. Wojtkowiak, L. Trinberg, and A.-M. Osula, *Insider Threat Detection Study*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2018.
- [6] D. Kipkoech and S. Ng'etich, A Survey of Security in Zero Trust Network Architectures, *GSC Advanced Research and Reviews*, vol. 22, 2025, pp. 182-183.
- [7] S. Pagadala Sekar, Integrating software-defined perimeter and zero trust in platform engineering: A security framework for modern infrastructure, *World Journal of Advanced Engineering Technology and Sciences*, vol. 15, no. 02, 2025, pp. 357-379.
- [8] R. Chandramouli, *Guide to a Secure Enterprise Network Landscape*, NIST Special Publication 800-215, National Institute of Standards and Technology, Gaithersburg, MD, 2022, pp. 5.
- [9] P.-Y. Chen, S. Choudhury, L. Rodriguez, A. O. Hero III, and I. Ray, Enterprise Cyber Resiliency Against Lateral Movement: A Graph Theoretic Approach, *arXiv preprint*, 2019, pp. 1-2.
- [10] M. Chauhan and M. Sharma, A Comprehensive Survey on Zero Trust Architecture: Advancements, Challenges, and Future Trends, *Journal of Emerging Technologies and Innovative Research (JETIR)*, vol. 12, no. 6, 2025, pp. 321-322, 324.
- [11] Lj. Stojanović, LI-FI Systems, Master's thesis, Faculty of Computer Science and Informatics, Sinergija University, Bijeljina, Republic of Srpska, 2025, pp. 1, 3, 15-20.
- [12] Lj. Stojanović, V. Radojčić, S. Mitrović, and P. Spalević, Li-Fi Technology for Cybersecurity Solutions + SEON, 2025, pp. 56-58.
- [13] S. Mushtaq, M. Mohsin, and M. M. Mushtaq, A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains, *Sensors (Basel)*, vol. 25, no. 19, 2025, pp. 2, 5.
- [14] M. L. Gambo i A. Almulhem, Zero Trust Architecture: A Systematic Literature Review, *arXiv preprint*, 2025, pp. 1, 3, 25, 28.
- [15] M. A. Azad, S. Abdullah, J. Arshad, H. Lallie, and Y. H. Ahmed, „Verify and trust: A multidimensional survey of zero-trust security in the age of IoT,” *Internet of Things*, vol. 27, 2024, p. 101227.
- [16] M. Heath and S. Vinberg, What Is Zero Trust Architecture (ZTA)?, F5 Labs, Figure 1: NIST tenets of zero trust architecture, [Online]. Available: <https://www.f5.com/labs/articles/what-is-zero-trust-architecture-zta>.
- [17] A. Blanc, My take on Zero Trust – SP 800-207, Blog Inforeseau.com, 2019, [Online]. Available: <https://blog.inforeseau.com/my-take-on-zero-trust-sp-800-207>.
- [18] S. Ullah, S. U. Rehman, and P. H. J. Chong, "A comprehensive open-source simulation framework for LiFi communication", *Sensors*, vol. 21, no. 7, 2021, pp. 2, 4-6.
- [19] Lj. Stojanović, V. Radojčić, and P. Spalević, Li-Fi, AI and IoT Technologies in Creating Sustainable Business, 2025, pp. 62-63, 65.
- [20] M. M. Msallam and R. Samet, A Review of Security Methods in Light Fidelity Technology, *Proceedings of Engineering and Technology Innovation*, vol. 27, 2024, pp. 6-8, 9, 12.
- [21] T. Sukiman, C. Sandy, R. Meiyanti, R. Rizal, and S. Anshari, Implementation of AES Algorithm for Text Message Encryption and Decryption Process, *Gameology and Multimedia Expert*, vol. 3, no. 1, 2026, pp. 25-27.
- [22] N. Kumar, P. Lalwani, H. Lamkuche, G. Samara, H. Abu Mariah, and N. Patel, Deep Learning Based Analysis of the Key Scheduling Algorithm of AES Cipher, 2026, pp. 1975.
- [23] Iotauth, „Lifi-auth,” GitHub repository, [Online]. Available: <https://github.com/iotauth/lifi-auth>.