International Journal of Electronics and Microcircuits

E-ISSN: 2708-4507
P-ISSN: 2708-4493
IJEM 2024; 4(1): 31-33

www.microcircuitsjournal.com
Received: 06-01-2024
Accepted: 09-02-2024

Fatemh Alfaraj
Department of Electrical Engineering, College of Engineering, Qassim University, Qassim, Saudi Arabia

Rawan Alhashem
Department of Electrical Engineering, College of Engineering, Qassim University, Qassim, Saudi Arabia

Correspondence
Fatemh Alfaraj
Department of Electrical Engineering, College of Engineering, Qassim University, Qassim, Saudi Arabia

In-depth study on enhancing security through optical wireless communication channels

Fatemh Alfaraj and Rawan Alhashem

Abstract
Optical Wireless Communication (OWC) offers a promising alternative to traditional wireless communication methods, with the potential for high-speed data transmission and enhanced security measures. This paper presents an in-depth study of the current state and future prospects of securing data transmission through OWC channels, including Visible Light Communication (VLC), Infrared Communication (IRC), and Ultraviolet Communication (UVC). We examine the inherent security features of OWC, such as its limited propagation range and line-of-sight requirement, and discuss advanced cryptographic techniques and protocols tailored for OWC systems. The study aims to provide a comprehensive understanding of how OWC can fortify security in various applications, from secure military communications to consumer electronics and beyond.

Keywords: Optical wireless communication (OWC), visible light communication (VLC), infrared communication (IRC)

Introduction
The rapid evolution of wireless communication technologies has ushered in an era of unprecedented connectivity and convenience. However, this progress also brings to the forefront significant security vulnerabilities, with traditional radio frequency (RF) communication channels increasingly susceptible to interception, unauthorized access, and eavesdropping. As the demand for secure communication channels escalates, particularly in sensitive applications such as military, healthcare, and financial services, the need for innovative solutions has become paramount. Optical Wireless Communication (OWC), utilizing light to transmit data, emerges as a promising alternative, offering unique advantages in terms of security, bandwidth, and signal fidelity. This in-depth study delves into the potential of OWC to enhance security, exploring its fundamental principles, comparing it with traditional RF communications, and investigating the latest advancements and techniques that fortify its security capabilities. Through a comprehensive analysis of the technology's inherent characteristics and the application of cutting-edge security protocols, this research aims to highlight the role of OWC in shaping the future of secure wireless communication (Jenila C, *et al*. 2021) [1].

Objective of paper
To analyse the Enhancing Security through Optical Wireless Communication Channels.

Overview of Optical Wireless Communication
Fundamentals of OWC: OWC technology utilizes light-emitting diodes (LEDs) or laser diodes to transmit data through the air, a vacuum, or transparent media. It can achieve high data rates, making it suitable for bandwidth-intensive applications. Unlike RF communications, which can suffer from spectrum scarcity and interference, OWC operates in a spectrum that is unregulated and vast, offering immense potential for future wireless communications (Yadav P, *et al*. 2021) [2].

Types of Optical Wireless Communication
OWC can be classified based on the spectrum range it utilizes for communication: Infrared Communication (IRC), Visible Light Communication (VLC), and Ultraviolet Communication (UVC). Each type has distinct characteristics, making them suitable for different applications (Celik A, *et al*. 2022) [3].

1. Infrared Communication (IRC)
IRC uses infrared light for data transmission, which is invisible to the human eye. It is commonly used for short-range communication applications, such as remote controls, wireless mouse devices, and short-link data communication between mobile devices. Infrared communication offers the advantage of low power consumption and the ability to operate in areas with strict electromagnetic interference (EMI) regulations, but it is limited by its range and susceptibility to interference from external light sources (Soderi S, *et al*. 2021) [4].

2. Visible Light Communication (VLC)
VLC employs visible light, typically from LEDs, to transmit data. It has gained attention for its potential to integrate with lighting infrastructure, effectively turning light sources into data transmission devices. VLC can be used for indoor positioning systems, internet access in places where RF communication is restricted, and vehicle-to-vehicle communication. Its main advantages include high data rates, inherent security due to light's inability to penetrate opaque objects, and dual-use functionality in lighting and communication. However, VLC requires line-of-sight (LOS) and is affected by ambient light interference.

3. Ultraviolet Communication (UVC)
UVC leverages ultraviolet light, specifically the non-line-of-sight (NLOS) UV spectrum, for communication. This technology can provide secure point-to-point communication over short and medium distances. UVC is particularly useful in scenarios where LOS is not possible due to obstacles or in outdoor environments for secure tactical communications. The main benefits of UVC include its ability to diffuse through the atmosphere and around obstacles, providing NLOS communication capabilities, and its resistance to interference from sunlight and artificial light sources (Khoshafa MH, *et al*. 2023) [5].

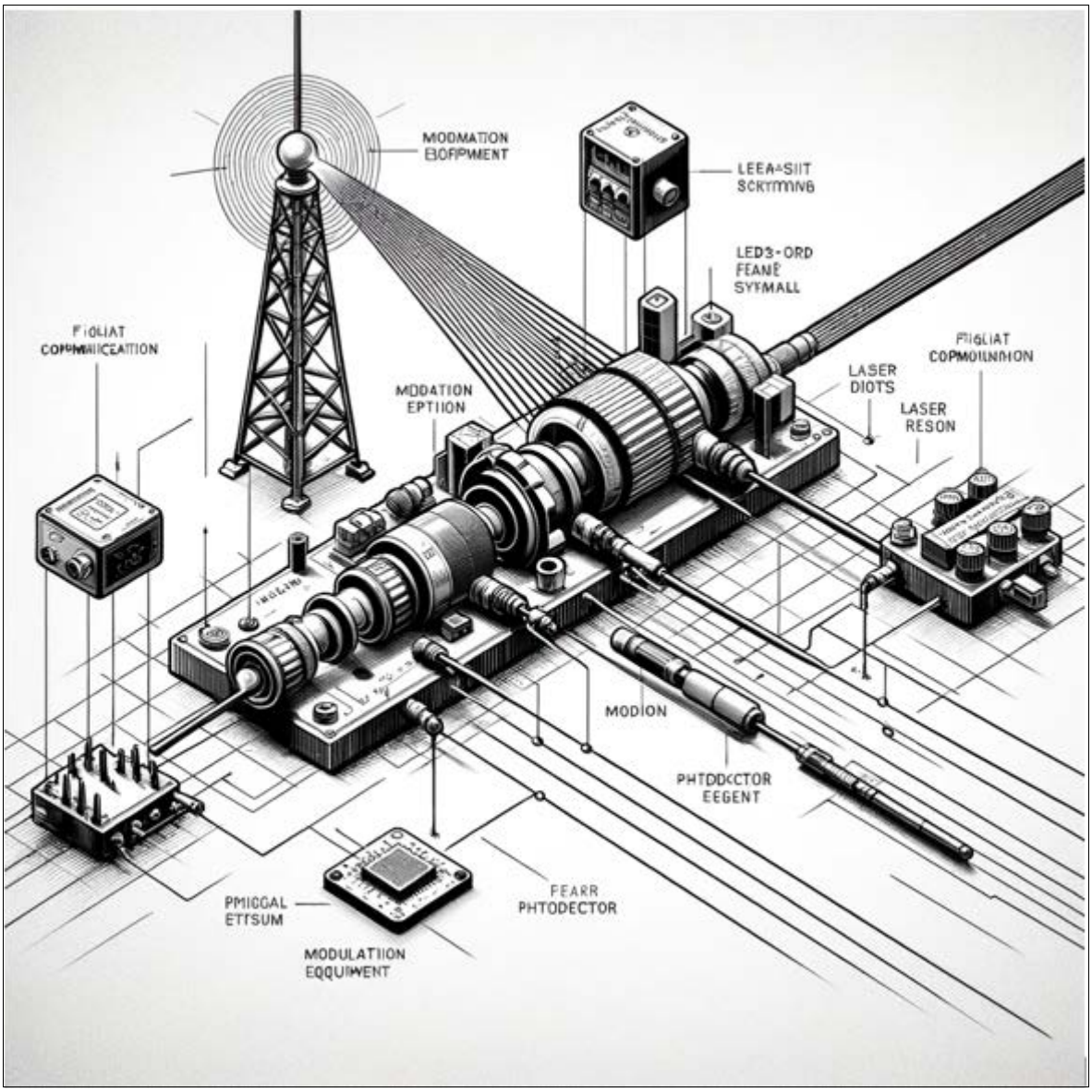

Fig 1: Optical Wireless Communication

Challenges in OWC Security
Optical Wireless Communication (OWC) systems, despite their numerous advantages over traditional wireless communication methods, face distinct security challenges. These challenges arise from both the physical nature of OWC technologies and the network environments they

operate within. Understanding these challenges is crucial for developing effective security measures and protocols tailored to OWC systems. Below are some of the key challenges in securing OWC systems (Leccese F, *et al*. 2021) [6].

Line-of-Sight (LOS) and Eavesdropping

OWC, particularly Visible Light Communication (VLC), requires a clear line-of-sight (LOS) between the transmitter and receiver. While this LOS requirement can enhance security by limiting the potential for unintended recipients to intercept the signal, it also presents challenges. For instance, an eavesdropper with a direct view of the OWC signal could potentially capture the data without disrupting the communication, making eavesdropping difficult to detect.

Physical Layer Security

The security of the physical layer is a significant concern for OWC systems. The propagation of light signals can be affected by environmental factors such as fog, dust, and ambient light, potentially degrading the signal integrity and making the system more susceptible to physical layer attacks, such as signal interception and manipulation.

Network Layer Security

In multi-user environments, securing the network layer of OWC systems becomes complex. The broadcast nature of OWC, especially in scenarios involving VLC, means that signals can be available to any receiver within the LOS. Ensuring data integrity and privacy requires robust encryption and secure key distribution methods that are efficient and scalable for OWC architectures.

Quantum Attacks

With the advent of quantum computing, traditional cryptographic techniques may become vulnerable. OWC systems, like other communication technologies, will need to evolve to incorporate quantum-resistant cryptographic algorithms to safeguard against future quantum attacks.

Interference and Jamming

While OWC is less susceptible to traditional RF interference, it can still be affected by optical interference or jamming. Malicious sources of light could disrupt the communication channel, leading to denial-of-service (DoS) attacks. Addressing these challenges requires the development of adaptive OWC systems capable of mitigating interference through dynamic modulation techniques and error correction.

Data Integrity and Authentication

Ensuring the integrity of the data transmitted over OWC channels and the authentication of communicating parties is paramount. This challenge involves not only securing the data from unauthorized modifications but also verifying that the data originates from a legitimate source, which is particularly critical in applications like secure payments or confidential communications.

Conclusion

The comprehensive study on enhancing security through Optical Wireless Communication (OWC) channels substantiates the potential of OWC to significantly bolster communication security. It underscores that the inherent characteristics of OWC, such as line-of-sight operation and limited range, naturally limit potential eavesdropping and unauthorized access, making it a highly secure medium for data transmission. The research highlights advancements in encryption protocols and modulation techniques tailored for OWC, further strengthening its security capabilities. However, it also identifies challenges such as signal interference and physical barriers, recommending continued innovation in OWC technology to overcome these hurdles. The study advocates for integrating OWC with existing communication infrastructures to enhance security without compromising on performance or accessibility. Future directions include exploring advanced encryption methods, improving signal reliability in diverse environments, and expanding the use cases for OWC in both indoor and outdoor applications.

References

1. Jenila C, Jeyachitra RK. Green indoor optical wireless communication systems: Pathway towards pervasive deployment. Digital Communications and Networks. 2021 Aug 1;7(3):410-44.
2. Yadav P, Kumar S, Kumar R. A comprehensive survey of physical layer security over fading channels: Classifications, applications, and challenges. Transactions on Emerging Telecommunications Technologies. 2021 Sep;32(9):e4270.
3. Celik A, Romdhane I, Kaddoum G, Eltawil AM. A top-down survey on optical wireless communications for the internet of things. IEEE Communications Surveys & Tutorials. 2022 Nov 8;25(1):1-45.
4. Soderi S, De Nicola R. 6G networks physical layer security using RGB visible light communications. IEEE Access. 2021 Dec 30;10:5482-96.
5. Khoshafa MH, Maraqa O, Moualeu JM, Aboagye S, Ngatched T, Ahmed MH, *et al*. RIS-Assisted Physical Layer Security in Emerging RF and Optical Wireless Communication Systems: A Comprehensive Survey. arXiv preprint arXiv:2403.10412; c2024 Mar 15.
6. Leccese F, Spagnolo GS. State-of-the art and perspectives of underwater optical wireless communications. Acta IMEKO. 2021 Dec 30;10(4):25-35.
7. Ali MF, Jayakody DN, Chursin YA, Affes S, Dmitry S. Recent advances and future directions on underwater wireless communications. Archives of Computational Methods in Engineering. 2020 Nov;27:1379-412.
8. Naser S, Bariah L, Muhaidat S, Sofotasios PC, Al-Qutayri M, Damiani E, *et al*. Toward federated-learning-enabled visible light communication in 6G systems. IEEE Wireless Communications. 2022 Feb;29(1):48-56.
9. Escribano FJ, Wagemakers A, Kaddoum G, Evangelista JV. A spatial time-frequency hopping index modulated scheme in turbulence-free optical wireless communication channels. IEEE Transactions on Communications. 2020 Apr 13;68(7):4437-50.