6lo
Internet-Draft
Intended status: Informational
Expires: 5 January 2026

M. Choi, Ed.
Y. Choi
ETRI

4 July 2025

Security considerations for IPv6 Packets over Short-Range Optical Wireless Communications
draft-choi-6lo-owc-security-02

Abstract

IEEE 802.15.7, "Short-Range Optical Wireless Communications" defines wireless communication using visible light. It defines how data is transmitted, modulated, and organized in order to enable reliable and efficient communication in various environments. The standard is designed to work alongside other wireless communication systems and supports both line-of-sight (LOS) and non-line-of-sight (NLOS) communications. This document describes security considerations for short-range optical wireless communications (OWC) using IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) techniques.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 5 January 2026.

Copyright Notice

Table of Contents

1. Introduction

The rapid growth of the Internet of Things (IoT) has led to a significant increase in the number of wireless communication technologies utilized for real-time data collection and monitoring in various industrial domains, such as manufacturing, agriculture, healthcare, transportation, and so on. This trend highlights the importance of wireless communication in facilitating real-time data exchange and analysis, ultimately contributing to enhanced operational efficiency and decision-making processes across different industrial sectors.

Optical Wireless Communications (OWC) stands as one of the potential candidates for IoT wireless communication technologies, extensively applied across various industrial domains. The IEEE802.15.7 standard outlines the procedures for establishing bidirectional communications between two OWC devices. Furthermore, IEEE 802.15.7 delineates a comprehensive OWC standard, encompassing features like Visible Light Communication (VLC), Short-Range Communication, Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS) Support, High and Low Data Rates, Energy Efficiency, and Secure Communication.

This document describes security considerations for IPv6 over Optical Wireless Communications.

2. Security Considerations

Optical Wireless Communication (OWC) systems introduce unique security concerns due to their use of directional, line-of-sight (LOS) visible or infrared light and their physical-layer characteristics. These include vulnerability to signal leakage, sensitivity to environmental interference, fragmentation-related risks, and lack of native multicast support. This section outlines key security considerations relevant to IPv6 transmission over OWC, particularly in 6LoWPAN-based deployments using IEEE 802.15.7.

2.1. Eavesdropping and Data Interception

Since OWC relies on optical signals, communications can be susceptible to interception when the line-of-sight (LOS) path is unobstructed. Mitigation techniques include directional communication, encryption of data, and limiting transmission power to reduce signal leakage. Additionally, employing beam steering technologies, narrow optical beam divergence, and end-to-end encryption at the IPv6 adaptation layer may be used to help preserve data confidentiality. Signals may also leak indirectly through reflective surfaces or transparent barriers such as glass.

2.2. Data Integrity

Environmental factors such as ambient light interference, obstacles, multipath reflections, and LED modulation inconsistencies can degrade OWC data integrity. Robust error detection and correction mechanisms at the PHY layer combined with IPv6-level integrity protection are recommended. In addition, to ensure the integrity of header-compressed IPv6 packets, the SCHC compression context should be securely managed and protected from unauthorized modifications or corruptions. It is also important to ensure consistency of SCHC context across constrained devices, especially in star and multi-hop topologies where centralized or distributed synchronization is required.

2.3. Denial of Service (DoS) Attacks

OWC can experience physical jamming attacks via high-intensity optical noise or physical obstruction, potentially disrupting communications. Mitigations include incorporating PHY-layer interference detection mechanisms and adaptive modulation schemes, as well as implementing network-layer redundancy through alternative IPv6 routing paths via multi-hop OWC topologies. In addition, OWC networks using small MTU PHYs (e.g., PHY1 in Section 3.4 and 4.6) may be vulnerable to fragmentation-based DoS attacks. To mitigate such risks, appropriate bounds on packet reassembly and timeout-based

validation mechanisms can be applied to prevent resource exhaustion or buffer misuse during the reassembly process.

2.4. Authentication and Access Control

Unauthorized OWC device access can lead to unauthorized data transmissions or network compromise. Mutual authentication using IPv6-based Datagram Transport Layer Security [RFC9147] and device identity verification through IEEE 802.15.7 link-layer addresses with IPv6 interface may be applied. In addition, secure mechanisms or lightweight alternatives should be considered to protect IPv6 Neighbor Discovery messages from spoofing, replay, or unauthorized modification.

2.5. Energy Efficiency and Security Trade-off

Due to limited energy resources in OWC devices, security mechanisms should minimize energy overhead. Lightweight cryptographic protocols optimized for low-power microcontrollers (e.g., lightweight authenticated encryption schemes, reduced-overhead DTLS [RFC9147] handshake) and adaptive security levels depending on the device’s operational context can be selectively applied. Context-specific lightweight security protocols designed for constrained environments may also be applied to enable secure communication with minimal computational and energy overhead.

2.6. Secure Routing in Multi-hop Networks

In multi-hop OWC networks, the integrity and authenticity of routing information is essential. Attacks on intermediate nodes or routing messages can compromise data delivery, causing eavesdropping, packet dropping, or routing loops. Therefore, security-aware routing mechanisms and lightweight node authentication approaches may be applied to ensure reliable and trustworthy communication paths, particularly in topologies with limited infrastructure support.

3. IANA Considerations

None.

4. References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Acknowledgements

We are grateful to the members of the IETF 6lo Working Group.

Authors' Addresses

Munhwan Choi (editor)
Electronics and Telecommunications Research Institute
218 Gajeongno, Yuseung-gu
Daejeon
34129
South Korea
Phone: +82 42 860 6539
Email: mhchoi@etri.re.kr

Younghwan Choi
Electronics and Telecommunications Research Institute
218 Gajeongno, Yuseung-gu
Daejeon
34129
South Korea
Phone: +82 42 860 1429
Email: yhc@etri.re.kr