6lo
Internet-Draft
Intended status: Informational
Expires: 23 April 2026

M. Choi, Ed.
Y. Choi
ETRI

20 October 2025

Security considerations for IPv6 Packets over Short-Range Optical Wireless Communications
draft-choi-6lo-owc-security-03

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.

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 have unique security considerations arising from their directional and line-of-sight (LOS) or non-line-of-sight (NLOS) operation and from the physical characteristics of optical media. These characteristics may lead to signal leakage, environmental interference, fragmentation-related vulnerabilities due to small-MTU PHYs, and limited support for multicast transmission.

This section summarizes the main security considerations for IPv6 transmission over OWC, particularly in 6LoWPAN-based deployments using IEEE 802.15.7.

2.1. Eavesdropping and Data Interception

OWC communications may be susceptible to interception when the line-of-sight (LOS) or non-line-of-sight (NLOS) optical path is unobstructed or partially reflective. Signal leakage through transparent or reflective surfaces can expose transmitted data to unauthorized observation.

Mitigation techniques include the use of directional transmission, end-to-end encryption, and optimized transmission power to reduce unintended optical exposure. Beam steering, adaptive modulation, and narrow beam divergence can further enhance confidentiality by limiting signal spread beyond the intended receiver’s field of view.

2.2. Denial of Service (DoS) Attacks

OWC networks may experience service disruption caused by high-intensity optical interference, physical obstruction, or excessive background illumination. Such conditions can reduce link availability or, in severe cases, lead to a denial of service.

To maintain network availability, OWC devices should detect abnormal interference, adjust modulation parameters, or reroute traffic through alternate multi-hop paths when optical links are impaired.

2.3. Authentication and Access Control

Unauthorized participation or message manipulation within an OWC network can compromise network trust and stability. Mutual authentication using IPv6-based Datagram Transport Layer Security [RFC9147] and device identity verification based on IEEE 802.15.7 link-layer addresses should be implemented to ensure that only legitimate devices can join and exchange IPv6 traffic.

Address registration and Neighbor Discovery procedures must be protected against spoofing, replay, and unauthorized modification. Proof of address ownership and link-layer binding are recommended in multi-hop topologies to prevent address hijacking or impersonation.

2.4. Energy Efficiency and Security Trade-off

OWC devices often operate under strict energy constraints, so security mechanisms must minimize computational and transmission overhead while maintaining the required protection level.

Lightweight cryptographic protocols, such as authenticated encryption schemes and reduced-overhead DTLS 1.3 handshakes [RFC9147], are recommended for low-power microcontrollers to reduce processing cost without compromising data confidentiality or integrity.

When designing for constrained nodes, the general principles for limited-resource environments should be applied so that protocol complexity does not exceed available power or processing capacity. Adaptive adjustment of security parameters, including encryption strength or key lifetime, can help maintain an effective balance between energy efficiency and security robustness throughout network operation.

2.5. Secure Routing in Multi-hop Networks

In multi-hop OWC networks, the integrity and authenticity of routing information must be preserved to ensure reliable data forwarding. Attacks on intermediate nodes or routing control messages can cause packet loss, route manipulation, or network partitioning. Routing protocols should authenticate participating nodes and validate routing updates to prevent the injection of false routes or unauthorized relays.

OWC devices are expected to apply lightweight security mechanisms that verify routing information while minimizing processing and energy overhead.

2.6. RF/Optical Interference and Jamming

Although OWC operates primarily in the optical domain, practical deployments often coexist with RF-based wireless systems in the same environment.

In such mixed conditions, high-intensity optical signals or strong RF emissions may interfere with OWC transceivers, causing service disruption or degraded performance. OWC systems need mechanisms to detect and respond to abnormal interference levels-such as adaptive modulation control, alternative routing, or temporary link isolation-to maintain network availability.

When interference is detected, recovery procedures should restore normal operation without compromising ongoing secure sessions or data integrity.

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