Security Considerations for IPv6 over OWC

draft-choi-6lo-owc-security-03

for draft-ietf-6lo-owc

Munhwan Choi, Younghwan Choi (ETRI)

IETF 124, Montreal, November 2025

Status of ‘draft-choi-6lo-owc-security’

- draft-choi-6lo-owc-security-00 (IETF 121, Dublin, November 2024)
  - Introduced as a new I.D.
- draft-choi-6lo-owc-security-01 (IETF 122, Bangkok, March 2025)
  - Eavesdropping, Data Integrity, DoS Attacks
  - Authentication and Access Control, Energy-Security Trade-off, Secure Routing
- draft-choi-6lo-owc-security-02 (IETF 123, Madrid, July 2025)
  - Editorial updates without structural changes
- **draft-choi-6lo-owc-security-03 (IETF 124, Montreal, November 2025)**
  - **‘Data integrity’ removed and merged into confidentiality and interference related parts**
  - **‘Interference/jamming’ added**

Quick Overview of OWC (1/2)

Ref.#1: Short-Range Optical Wireless Communications (OWC) ?

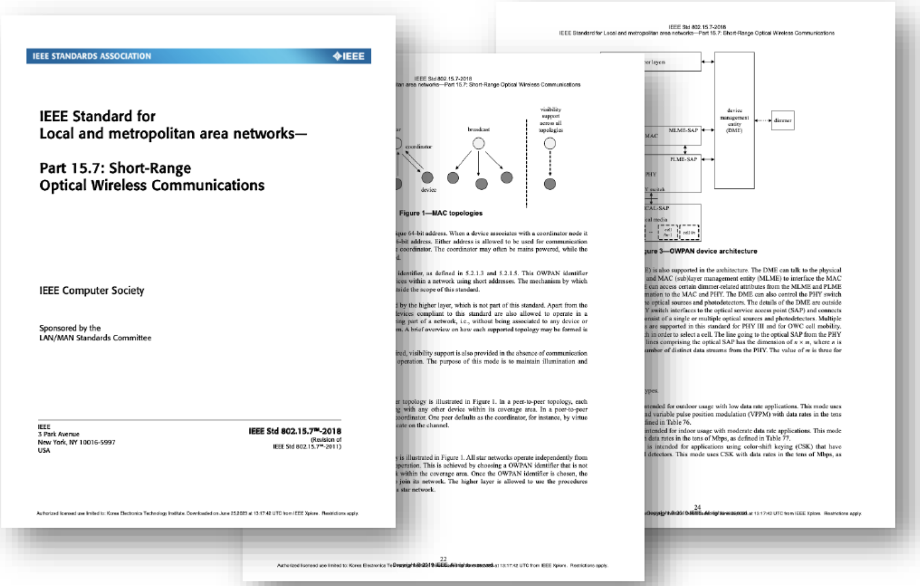
- **OWC** uses **intensity modulation of optical sources**, such as **Light Emitting Diodes (LEDs)**.
- **OWC** combines lighting and **bidirectional data communications**.
- **OWC** can be applied to various domains including area **lighting, signboards, streetlights, vehicles, traffic signals, displays, LED panels, and digital signage, smart phones** …
- **OWC** devices can be powered by **limited energy sources (e.g., battery or energy harvesting)** for energy-efficient services.

from
IPv6 over OWC
presentation
slides

Quick Overview of OWC (2/2)

Ref.#2: OWC v.s. IEEE 802.15.7

- OWC is defined by **IEEE 802.15.7 standard** providing six key characteristics, including



Visible Light Communication (VLC),
Short-Range Bidirectional Communication,
Line-of-Sight (LOS) &
Non-Line-of-Sight (NLOS) Support,
High and Low Data Rates,
Energy Efficiency,
and Secure Communication.

from
IPv6 over OWC
presentation
slides

Possible (Key) Security Risks

- Based on the key characteristics of IEEE 802.15.7

• **Signal leakage** through glass or reflection • **Eavesdropping / Data interception** via optical exposure	• **PHY downgrade** or misconfiguration exploited for weaker **access control** • Modulation **spoofing / unreliable synchronization**
• **Insider access** within illumination zone • Device **impersonation / authentication bypass**	• **Power exhaustion / DoS** through dimming control • **Energy–security trade-off** causing timing instability
• **Unintended reception** or **relay interference** via reflection • Risk of **path misrouting or** false signal relaying	• Limited **encryption strength / key management** scope • Susceptible to **optical interference or jamming** when unprotected

Mapping between Characteristics and Security Considerations

Security Considerations→ ↓Characteristics	Eavesdropping /Data Interception	DoS Attacks	Authentication /Access Control	Energy Trade-off	Interference /Jamming	Relations
Visible Light Comm. (VLC)	√				√	Reflected or leaked light can reach unintended receivers, leading to eavesdropping risks.
Short-Range Bidirectional Comm.		√	√		√	Short range limits exposure but allows close-range spoofing or DoS attempts.
LOS /NLOS Support	√	√			√	Reflected paths expose data to interception and can cause unstable links or jamming.
High & Low Data Rates			√		√	Switching between data rates may weaken authentication and increase interference sensitivity.
Energy Efficiency		√		√	√	Power-saving or dimming control can trigger DoS and reduce encryption strength.
Secure Comm.	√		√	√	√	Encryption and key management form the foundation for all other security protections.

Future Plans

- Update the **existing Security Considerations** into I.D.-04.
- Propose the candidate contents in **§ 7 (Security Considerations)** of **draft-ietf-6lo-owc-06** (in IETF 125)

Thank you.

Welcome any Comments!!