Security in W-DALI networks

General information about W-DALI wireless network

The W-DALI wireless network is built upon the LumenRadio MiraMesh wireless network platform, specifically designed for mission-critical applications like lighting control and building automation. MiraMesh incorporates LumenRadio's patented cognitive coexistence technology, ensuring optimal resilience against disturbances and minimal interference with other wireless networks.

Link-layer encryption

MiraMesh networks implement robust security measures to ensure the confidentiality and integrity of data transmission. One of the key security features is the utilization of link-layer encryption, which guarantees that all messages exchanged between devices are encrypted. This effectively prevents unauthorized access, eavesdropping, and packet injection.

To establish secure links between W-DALI devices, MiraMesh networks employ AES with a minimum key length of 128 bits and CCM mode. This cryptographic algorithm not only provides encryption but also ensures authentication of packets. Only W-DALI devices possessing the network's AES keys can access and inject data, thereby safeguarding the network from unauthorized entities.

Furthermore, MiraMesh networks incorporate the current network time as a seed for encryption, which is randomized at each network startup. This dynamic encryption mechanism renders replay attacks futile, as attackers cannot exploit repeated encrypted packets.

Adaptive frequency hopping

In addition to encryption, MiraMesh networks employ “Cognitive Coexistence” a LumenRadio patented feature which is an evolution of adaptive frequency hopping. This functionality not only helps avoid unintentional interference but also mitigates malicious jamming attacks. By continuously monitoring the spectrum and adapting which channels to use, MiraMesh networks present significant challenges to potential attackers attempting to disrupt the network through jamming. The complex task of establishing the hopping sequence and the constant adaptation make it difficult for attackers to follow and interfere with the network.

Extra layer of security

While not the primary security feature, the proprietary nature of MiraMesh technology and its limited knowledge within the hacker community provide an additional layer of protection. Unlike more widely known wireless technologies such as Bluetooth, WiFi, RFID/NFC, LoRa, and IR, MiraMesh networks have minimal existing tools and libraries for attacking them. Any potential attacker targeting a MiraMesh network would need to start from scratch, making these networks less vulnerable compared to others.

LumenRadio AB
Johan Willins gata 6
SE-416 64 Gothenburg
Sweden

www.lumenradio.com
sales@lumenradio.com

Phone: +46 31 301 03 70