Network Working Group
Internet-Draft
Intended status: Informational
Expires: 2 October 2026

Nikesh Patel
Independent

2 April 2026

Open Mesh Protocol (OMP): A Multi-Radio Proximity Mesh Networking Architecture and Problem Statement

draft-patel-omp-proximity-mesh-00

Abstract

This document describes the Open Mesh Protocol (OMP), a proposed open standard for device-native proximity mesh networking spanning multiple radio technologies simultaneously. Existing proximity wireless mesh standards -- including Wi-Fi Aware (NAN), Bluetooth Mesh, and Thread -- each operate over a single radio technology and serve specific application domains. No existing open standard provides a unified multi-radio mesh routing protocol spanning BLE, WiFi Direct, and LoRa with per-device cryptographic identity independent of any central registry or carrier relationship. This document describes the OMP architecture, specific technical implementations, and the gap in the current standards landscape that OMP addresses. It is submitted as an Informational Internet-Draft to establish a public prior art record and to invite community discussion on whether a new working group or individual submission track is appropriate for this work.

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 2 October 2026.

Table of Contents

1. Introduction

The Internet connects every device to anywhere on Earth. Cellular connects every device to everyone on Earth. Neither standard provides what this document addresses: a local network layer that connects devices to what is physically nearby -- without infrastructure, without servers, without subscriptions -- and that grows stronger as more devices join it.

Wireless mesh networking has been studied since the early 1990s [RFC3561] [RFC3626]. Multiple routing protocols have been standardised by the IETF MANET working group. IEEE 802.11s [IEEE80211s] defined a mesh standard for WiFi that achieved consumer deployment through home mesh router systems. The Bluetooth SIG published Bluetooth Mesh in 2017 for IoT applications. The Thread Group published Thread in 2014 for smart home applications. Wi-Fi Alliance published Wi-Fi Aware (NAN) in 2015 for proximity service discovery.

Despite this body of work, a specific gap remains unaddressed: no open standard exists for a unified, general-purpose proximity mesh networking protocol that:

- Operates simultaneously across multiple radio technologies (BLE, WiFi Direct, LoRa, licensed shared spectrum)
- Provides per-device cryptographic identity without central registry, SIM, or carrier relationship
- Supports multi-hop mesh routing (not merely service discovery or point-to-point connection)
- Targets always-on fixed infrastructure as primary relay nodes with smartphones as clients
- Serves general-purpose human communication and proximity applications rather than IoT sensor or smart home automation exclusively

This document describes the Open Mesh Protocol (OMP) -- a proposed architecture to fill this gap -- and submits it as prior art and a starting point for community discussion.

2. Problem Statement

Existing proximity networking standards have the following limitations relevant to this proposal:

Wi-Fi Aware (NAN) [WIFAWARE]: Operates over WiFi only. Provides service discovery and point-to-point datapath establishment. Does not provide multi-hop mesh routing. Does not provide per-device cryptographic identity. Does not operate over BLE, LoRa, or licensed spectrum.

Bluetooth Mesh [BTMESH]: Operates over BLE only. Uses managed flooding rather than reactive multi-hop routing. Uses shared network keys assigned by a central provisioner rather than per-device asymmetric cryptographic identity. Designed for IoT sensor and smart home automation applications.

Thread [THREAD]: Operates over IEEE 802.15.4 only. Requires Thread-specific chipsets. Designed for smart home IoT applications. Does not operate over WiFi Direct or BLE advertising in the standard proximity networking context.

IEEE 802.11s [IEEE80211s]: Operates over WiFi only. Defines mesh routing for WiFi backhaul. Does not address BLE, LoRa, or multi-radio operation.

MANET routing protocols [RFC3561] [RFC3626]: Define routing algorithms that work correctly. Do not define a unified physical layer strategy, cryptographic identity system, or deployment mechanism for proximity networking specifically.

Reticulum [RETICULUM]: A cryptography-based networking stack using public-key-hash addressing, X25519 key exchange, Ed25519 signatures, and HKDF key derivation over multiple radio types. The closest existing open implementation to OMP's goals. OMP's specific differences from Reticulum are described in Section 5.

MeshCore [MESHCORE]: An open-source multi-hop packet routing system using Ed25519 for node identity with node addresses derived from public key hashes. Operates over LoRa with BLE bridging to smartphones.

3. Prior Work and Relationship to Existing Standards

OMP builds on extensive prior work and does not claim novelty in the following areas:

- Reactive mesh routing: AODV [RFC3561], OLSR [RFC3626], BATMAN-adv [BATMAN], IEEE 802.11s HWMP [IEEE80211s]
- Cryptographic primitives: Ed25519 [RFC8032], X25519 [RFC7748], HKDF-SHA256 [RFC5869], AES-256-GCM [NIST-GCM]
- Public-key-hash addressing: Reticulum [RETICULUM], GNUnet, Tor onion addresses
- Energy-aware mesh routing: Jing and Lee (2004), CMMBCR, EBLM, and the extensive battery-aware AODV literature
- Multi-radio mesh routing: Draves, Padhye, Zill (MobiCom 2004), WCETT, IEEE 802.21

OMP's specific technical contributions -- described in Sections 5 through 9 -- are the specific combination of these elements applied to a unified multi-radio proximity mesh protocol with a fixed-infrastructure-first deployment model and a CC0 open standard commitment.

4. OMP Architecture Overview

OMP defines a proximity networking protocol where:

- Any OMP-capable device discovers, authenticates, and communicates with nearby devices without internet, servers, or subscriptions

- Messages are routed across a self-assembling multi-hop mesh
- The mesh grows stronger as more devices join -- each node added increases coverage, redundancy, and capacity
- Primary relay nodes are always-on fixed infrastructure (routers, IoT gateways) rather than smartphones
- Smartphones and mobile devices are clients of the mesh infrastructure, not relay nodes
- The protocol defines transport and identity only; applications are built on top

The protocol operates in parallel with and as a complement to cellular and internet infrastructure. It does not require either to function, and provides capabilities neither can provide: local network awareness at device resolution without server intermediation.

5. Cryptographic Identity System

Each OMP node generates an Ed25519 key pair [RFC8032] at first initialisation. The private key is a 32-byte random seed stored in the device's secure element or TEE where available. The public key is the corresponding 32-byte compressed Edwards curve point.

The Node ID is computed as:

```
Node ID = SHA-256(Ed25519_public_key)
```

producing a 32-byte (256-bit) stable identifier. This uses the full (non-truncated) SHA-256 output, providing 256-bit collision resistance. The Node ID is stable across all radio interfaces and network topologies -- it identifies the device, not the radio or location.

Relationship to Reticulum: Reticulum [RETICULUM] uses a 16-byte truncated SHA-256 hash derived from a combined 512-bit keyset (256-bit X25519 + 256-bit Ed25519). OMP uses a full 32-byte SHA-256 hash derived from only the Ed25519 signing key. This separation allows X25519 encryption keys to be rotated independently of node identity.

Session key establishment between two nodes A and B:

1. Each node generates or retrieves its X25519 key pair
2. Nodes exchange X25519 public keys via the KEY_EXCHANGE message
3. Shared secret = X25519(A_private, B_public) = X25519(B_private, A_public)
4. Session key = HKDF-SHA256(
   IKM = shared_secret,
   salt = empty,
   info = min(Node_ID_A, Node_ID_B) || max(Node_ID_A, Node_ID_B)
)

The HKDF info field uses lexicographic ordering of Node IDs (comparing byte sequences from index 0) to ensure both nodes independently derive the same session key regardless of which initiated the exchange.

All payload encryption uses AES-256-GCM [NIST-GCM] with:
- 96-bit random nonce per message
- 128-bit authentication tag
- Session key as encryption key

6. Multi-Radio Transport Selection

OMP nodes capable of multiple radio interfaces apply the following transport selection policy, evaluated in order:

1. If node battery < LOW_BATTERY_THRESHOLD (default: 20%):
   Select BLE regardless of payload size, to avoid WiFi Direct Group Owner negotiation overhead

2. Else if payload_size > LARGE_PAYLOAD_THRESHOLD (default: 512 bytes):
   Select WiFi Direct

3. Else if UWB ranging data available AND distance < UWB_THRESHOLD (default: 15 metres):
   Select UWB

4. Else if target node within BLE range:
   Select BLE

5. Else:
   Select LoRa

Fixed infrastructure nodes (mains-powered) skip rule 1 and advertise their power status in the capability flags field of the discovery beacon (Section 7).

The radio type also contributes a penalty to the routing metric (Section 8), allowing the routing layer to prefer higher-throughput paths when multiple routes are available.

7. Discovery Beacon Structure

OMP nodes advertise their presence via BLE manufacturer-specific advertising data (AD Type 0xFF). The field structure within the manufacturer-specific data payload is:

Byte(s)	Field	Description
0-3	Node ID prefix	First 4 bytes of SHA-256 Node ID
4	Capability flags	Bit 0: 0=battery, 1=mains power Bit 1: WiFi internet gateway Bit 2: Cellular internet gateway Bit 3: Voice profile supported Bits 4-7: Reserved
5	Neighbour count	Known mesh neighbours (0-255)
6	Battery state	0-100 percent; 0xFF = mains power
7-8	Reserved	Set to 0x00
9-28	Service data	Application-layer advertisement

Total: 29 bytes within manufacturer-specific AD structure. This fits within the 31-byte BLE advertising PDU constraint (2 bytes consumed by AD length and type fields).

Fixed infrastructure nodes (mains-powered) set Capability flags bit 0 to 1 and Battery state to 0xFF.

8. Routing Metric

OMP uses a reactive routing protocol based on AODV [RFC3561] principles, modified for multi-radio and battery-aware operation.

The Mesh-Metric for a path is the sum of per-hop costs:

```
Hop-Cost = (W_hop) +
           ((100 - link_quality_percent) * W_lq) +
           radio_type_penalty +
           battery_penalty
```

Where:

- W_hop = 10 (configurable)
- W_lq = 1 (configurable)
- link_quality_percent: estimated packet delivery ratio (0-100)
- radio_type_penalty: BLE=0, WiFi Direct=0, LoRa=20, licensed spectrum=0
- battery_penalty: added when relay node battery < BATTERY_AVOID_THRESHOLD (default: 30%), to discourage routing through low-battery nodes; suggested value: 50

Lower Mesh-Metric indicates a preferred path. Route Request (RREQ) messages accumulate Mesh-Metric as they propagate. The destination selects the lowest-metric path when sending the Route Reply (RREP).

Fixed infrastructure nodes (mains-powered) contribute zero battery_penalty and are therefore preferred as relay nodes, which aligns with the deployment architecture (Section 9).

9. Deployment Model

OMP’s primary deployment target is always-on fixed infrastructure: routers running OpenWrt [OPENWRT] or equivalent open-source Linux firmware, commercial mesh WiFi base stations, and always-on IoT gateway devices. These devices have:

- Mains power -- no battery constraint
- No operating system background process restrictions
- No dependency on mobile platform vendor APIs (iOS, Android)
- Permanent radio availability

Smartphones and mobile devices operate as OMP clients, connecting to nearby fixed nodes via BLE or WiFi Direct. They benefit from the mesh infrastructure without constituting its backbone.

This architecture resolves the failure modes of prior smartphone-first mesh attempts:

- iOS background restrictions do not apply to fixed infrastructure
- Battery drain under relay load does not occur at mains-powered nodes
- Critical mass is achievable via firmware updates to existing deployed hardware without user action

The reference implementation target is an OpenWrt package that enables any OpenWrt-compatible router to function as an OMP mesh node.

10. Open Questions for Community Discussion

This document is submitted to invite community input on the following open questions:

a) Is this problem statement within scope of an existing IETF working group (MANET, ROLL, 6lo, DINRG) or does it warrant a new chartered working group?

b) Should OMP’s HKDF info field construction (lexicographic Node ID ordering) be specified differently to align with existing IETF key derivation conventions?

c) What is the appropriate relationship between OMP and Reticulum [RETICULUM], which addresses similar goals with a different addressing model?

d) Should the voice profile (Opus codec, carrier-free calling) be defined in this document or in a separate profile document?

e) What conformance test suite requirements should be defined for an OMP certification programme?

11. Security Considerations

OMP uses per-device asymmetric cryptographic identity (Ed25519) rather than shared network keys. This provides the following security properties:

- Node impersonation requires knowledge of the private key, which never leaves the device
- Session keys are ephemeral -- compromise of one session does not compromise past or future sessions
- No central authority holds keys -- there is no provisioner to compromise
- No carrier or infrastructure provider holds identity -- there is no SIM to clone or carrier to compel

Known limitations of OMP v0.1 requiring further work:

- RREQ flooding has no backoff mechanism -- dense deployments require flood control
- Relay node signature verification requires a public key gossip protocol not yet specified
- Multicast group key management is not yet defined
- Clock synchronisation in isolated mesh (no internet) is not yet specified

12. IANA Considerations

This document has no IANA actions at this time.

A future revision will request assignment of a BLE manufacturer-specific AD type identifier for OMP discovery beacons.

13. References

13.1. Normative References

[RFC3561] Perkins, C., Belding-Royer, E., and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, DOI 10.17487/RFC3561, July 2003, <https://www.rfc-editor.org/info/rfc3561>.

[RFC3626] Clausen, T. and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, DOI 10.17487/RFC3626, October 2003, <https://www.rfc-editor.org/info/rfc3626>.

[RFC5869] Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC 5869, DOI 10.17487/RFC5869, May 2010, <https://www.rfc-editor.org/info/rfc5869>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/info/rfc7748>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/info/rfc8032>.

13.2. Informative References

[BATMAN] Neumann, A., Aichele, C., Lindner, M., and S. Wunderlich, "Better Approach To Mobile Adhoc Networking (B.A.T.M.A.N)", IETF Internet-Draft (expired), 2008.

[BTMESH] Bluetooth Special Interest Group, "Mesh Protocol Specification v1.1", 2023, <https://www.bluetooth.com/specifications/specs/mesh-protocol-1-1/>.

[IEEE80211s] IEEE, "IEEE Standard for Information technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Specific requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 10: Mesh Networking", IEEE Std 802.11s-2011, 2011.

[MESHCORE] Hester, K. et al., "MeshCore -- Lightweight multi-hop packet routing for embedded LoRa devices", <https://github.com/ripplebiz/MeshCore>, 2024.

[NIST-GCM] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", NIST Special Publication 800-38D, 2007.

[OPENWRT] OpenWrt Project, "OpenWrt -- Linux distribution for embedded devices", <https://openwrt.org>.

[RETICULUM] Qvist, M., "Reticulum Network Stack", <https://github.com/markqvist/Reticulum>, 2017-2026.

[THREAD] Thread Group, "Thread Specification v1.3", 2022, <https://www.threadgroup.org/support>.

[WIFAWARE] Wi-Fi Alliance, "Wi-Fi Aware Specification v3.1", 2022, <https://www.wi-fi.org/file/wi-fi-aware-specification>.

Author’s Address

Nikesh Patel
Independent
Mauritius

Email: npukuk@gmail.com