Fortified Control-Plane Encapsulation with Session-Key Derivation for Secure IP Mesh Routing

G. Amponis, P. Radoglou-Grammatikis, T. Lagkas, V. Argyriou,
A. Sarigiannidis, N. Kazakli, T. Boufikos, P. Sarigiannidis

Presenter: **T. Boufikos**

tboufikos@k3y.bg

Outline

- Introduction & Motivation
- OLSR & Quantum Cryptography Background
- PQC-Enhanced OLSR Design
- Implementation & Evaluation
- Discussion & Conclusions

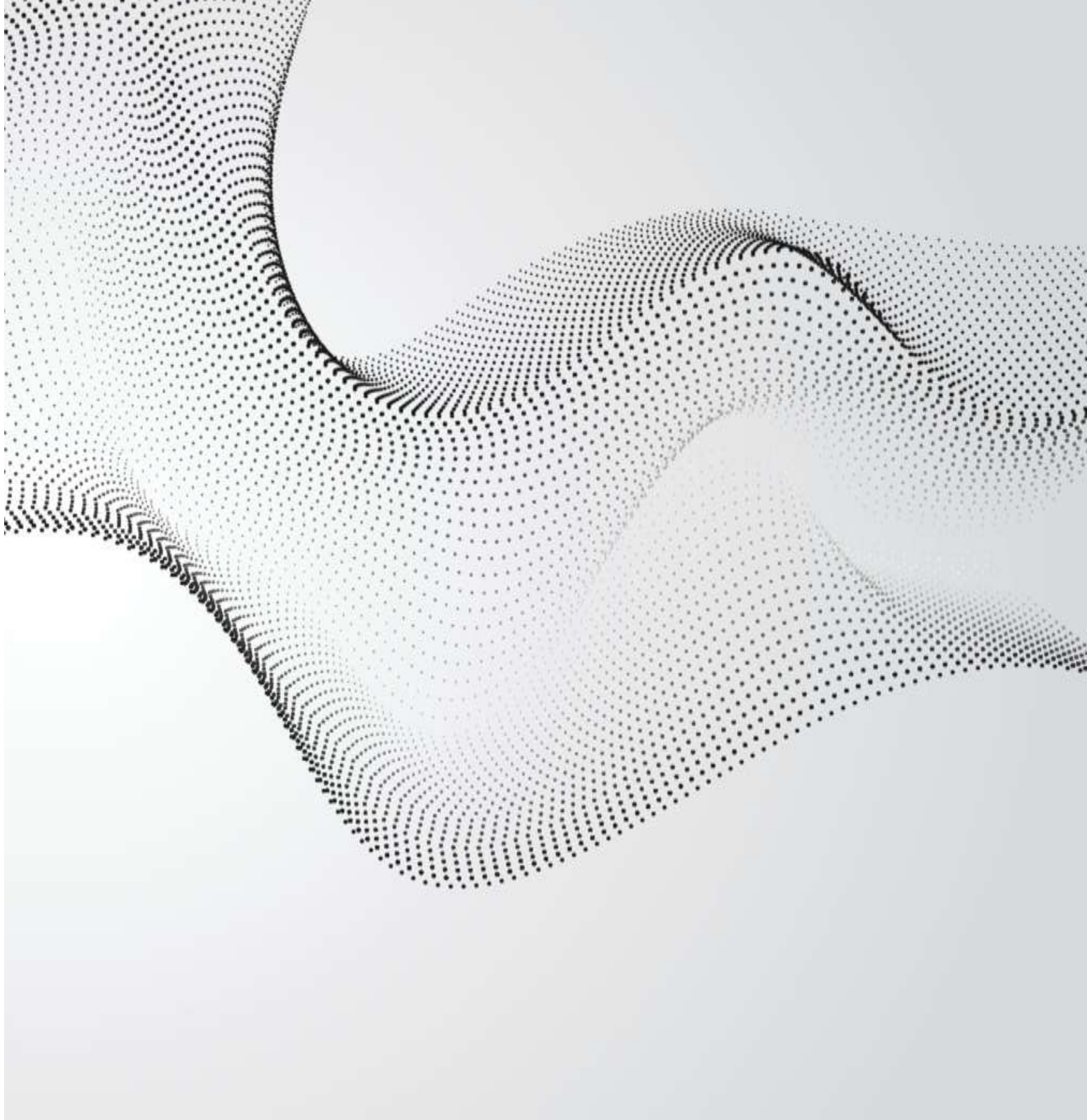
Introduction & Motivation

Mesh networks are widely deployed in community and tactical systems.

- Unencrypted OLSR control messages expose the network to eavesdropping and message forgery.
- Conventional security overlays rely on RSA/ECC, but these are vulnerable to quantum attacks (Shor’s algorithm).
- The ‘store now, decrypt later’ threat means adversaries may record control traffic today to break it once quantum computers mature.

Issue	Impact
Unencrypted HELLO/TC	Topology leakage, spoofing
RSA/ECC reliance	Broken by quantum algorithms
Store-now-decrypt-later	Retroactive compromise of traffic

Background: OLSR & Mesh Networking



- Proactive link-state routing for MANETs via OLSR.
- HELLO messages discover neighbours and detect links.
- TC messages disseminate topology information via MPRs.
- Unencrypted control plane leaves mesh vulnerable.

Quantum Threat & Post-Quantum Cryptography

- Shor's algorithm breaks RSA/ECC, motivating quantum-safe cryptography.
- CRYSTALS-Kyber (Kyber512) is a lattice-based KEM selected by NIST for PQC.
- ChaCha20-Poly1305 AEAD offers 256-bit security and high performance without hardware acceleration.
- Together, Kyber512 and ChaCha20-Poly1305 provide confidentiality, integrity and authenticity against classical and quantum adversaries.

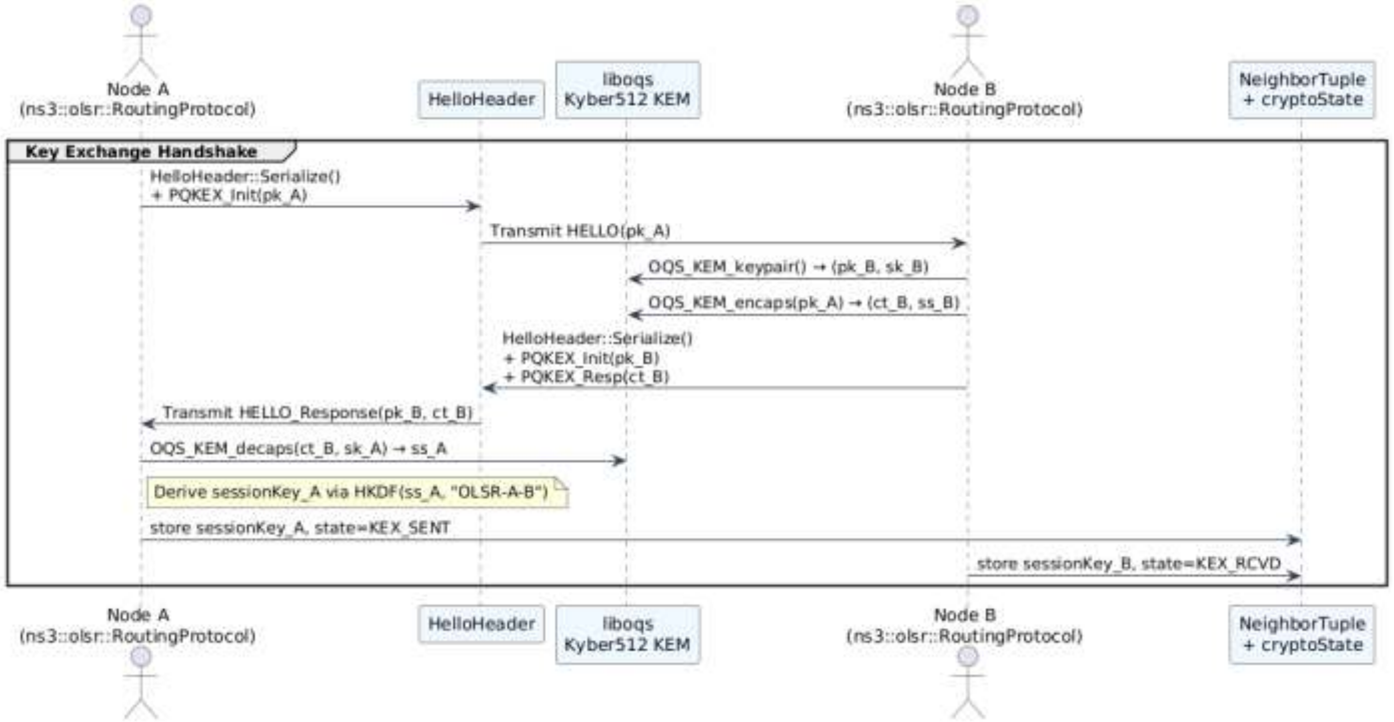
Primitive	Function
Kyber512 (KEM)	Session key establishment
ChaCha20-Poly1305	Encrypt & authenticate
HKDF	Derive symmetric key
TLVs 0x0F/0x10/0x11	Extend OLSR control fields

Architecture Overview

- **Security Shim Layer**
  Acts as an interceptor between IP and OLSR logic. All control-plane packets pass through it for cryptographic processing.
- **Inbound Processing**
  1. Detects presence of TLVs:
     - 0x0F: Kyber Public Key
     - 0x10: Kyber Ciphertext
     - 0x11: AEAD Payload
  2. Performs:
     - Kyber512 key exchange (via liboqs)
     - ChaCha20-Poly1305 decr. + tag verification
  3. If valid → forward to OLSR core; else → discard.
- **Outbound Processing**
  - Captures raw HELLO/TC payloads from OLSR core
  - Encrypts using ChaCha20-Poly1305 with session key
  - Appends AEAD TLV (0x11) to packet before IP transmission
- **Key Material Management**
  - Maintains per-neighbor state machine (e.g., INIT, KEX_RCVD, SECURE, BLACKLIST)
  - Derives session keys via HKDF over Kyber shared secrets
- **Compatibility**
  - Non-secure legacy nodes ignore unknown TLVs
  - OLSR routing logic remains unchanged

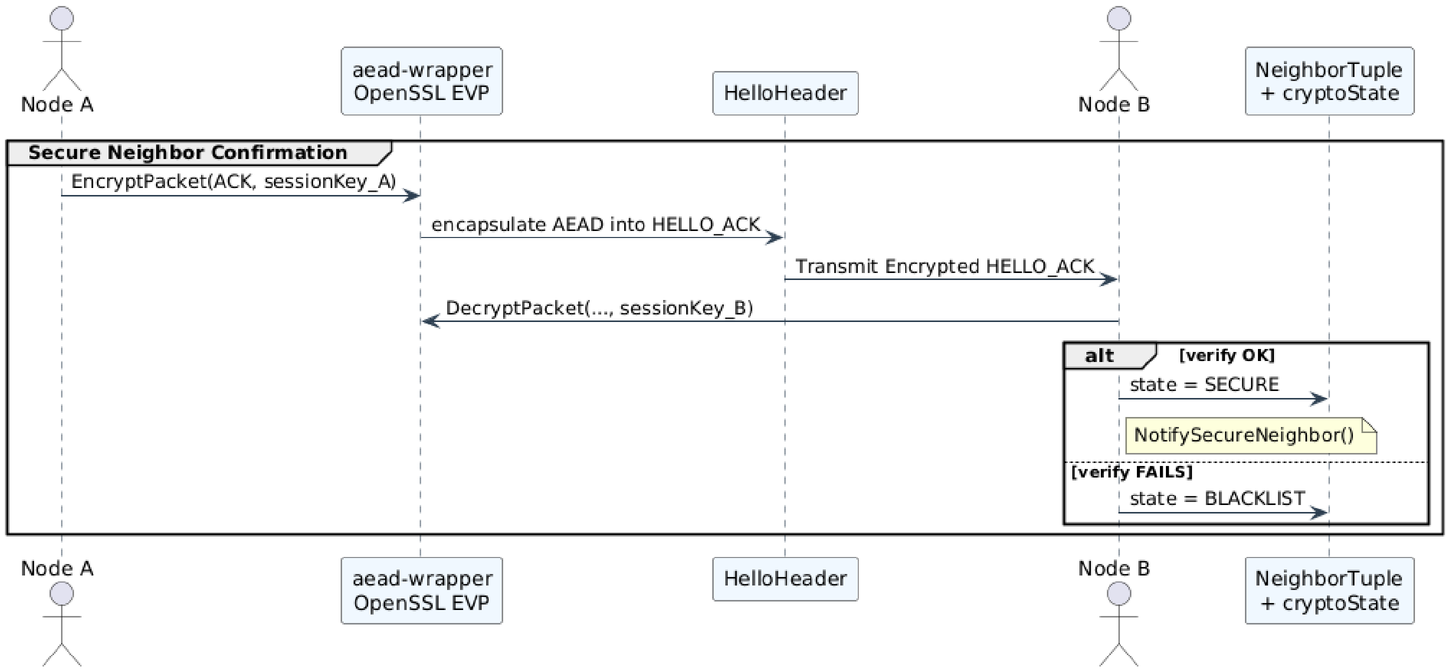
Element	Purpose
Security Shim	Between IP and OLSR, handles all crypto
Kyber512 (liboqs)	Key exchange via TLVs 0x0F, 0x10
ChaCha20-Poly1305	AEAD for HELLO/TC (TLV 0x11)
HELLO (Handshake)	Carries pubkey + ciphertext
HELLO/TC (Steady)	Encrypted with sesskey, AEAD-protected
Neighbor State	Tracks: INIT, KEX_RCVD, SECURE, BLACKLIST
HKDF	Derives sess key from shared secret
Failure Handling	Tag fail → drop packet, blacklist peer
OLSR Core	Unchanged; gets only verified payloads
Legacy Support	Unknown TLVs are safely ignored

Key Exchange Handshake



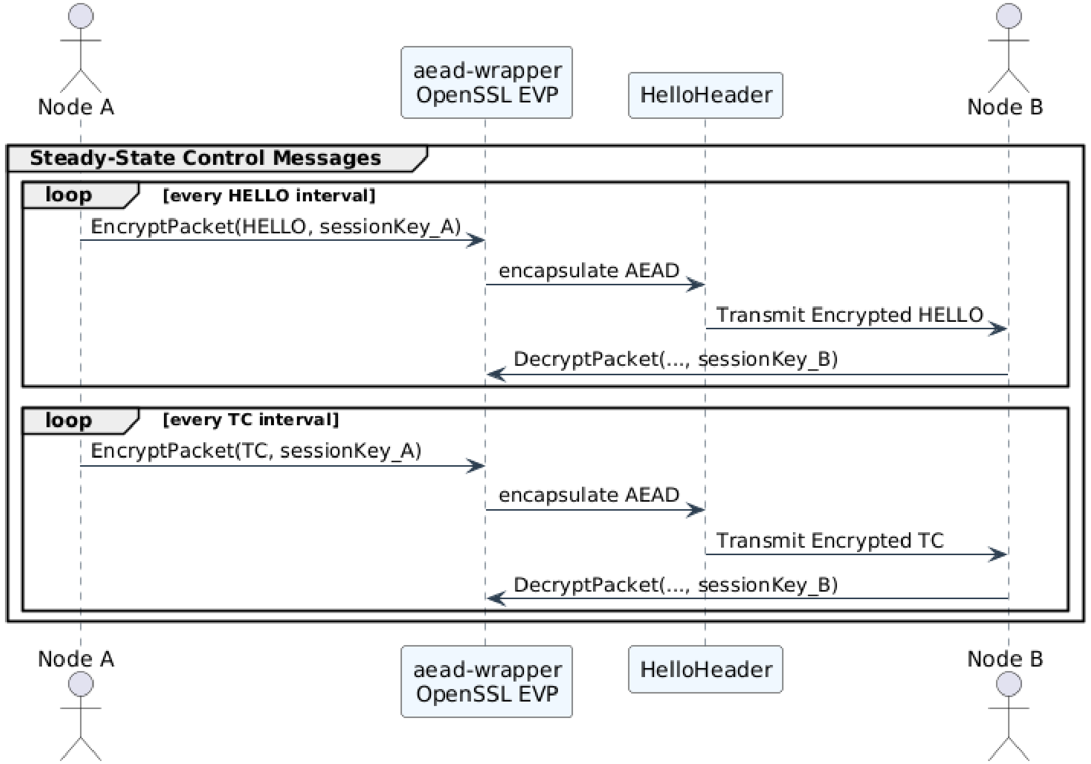
1. Node A generates a Kyber key pair (pk_A, sk_A) and sends pk_A.
2. Node B responds with its pub key pk_B and a KEM ciphertext ct_B derived from pk_A.
3. Both nodes derive a shared secret via HKDF and store a session key.
4. Node A sends an AEAD-protected ACK to confirm secure neighbour.

Secure Neighbor Confirmation



1. Once the key is established, every HELLO and TC msg is wrapped with ChaCha20-Poly1305.
2. An AEAD TLV (0x11) carries a 12-byte nonce, the ciphertext and a 16-byte auth tag.
3. Receivers decrypt and verify tags; invalid messages are dropped
4. The data plane remains unaffected because only control packets are encapsulated.

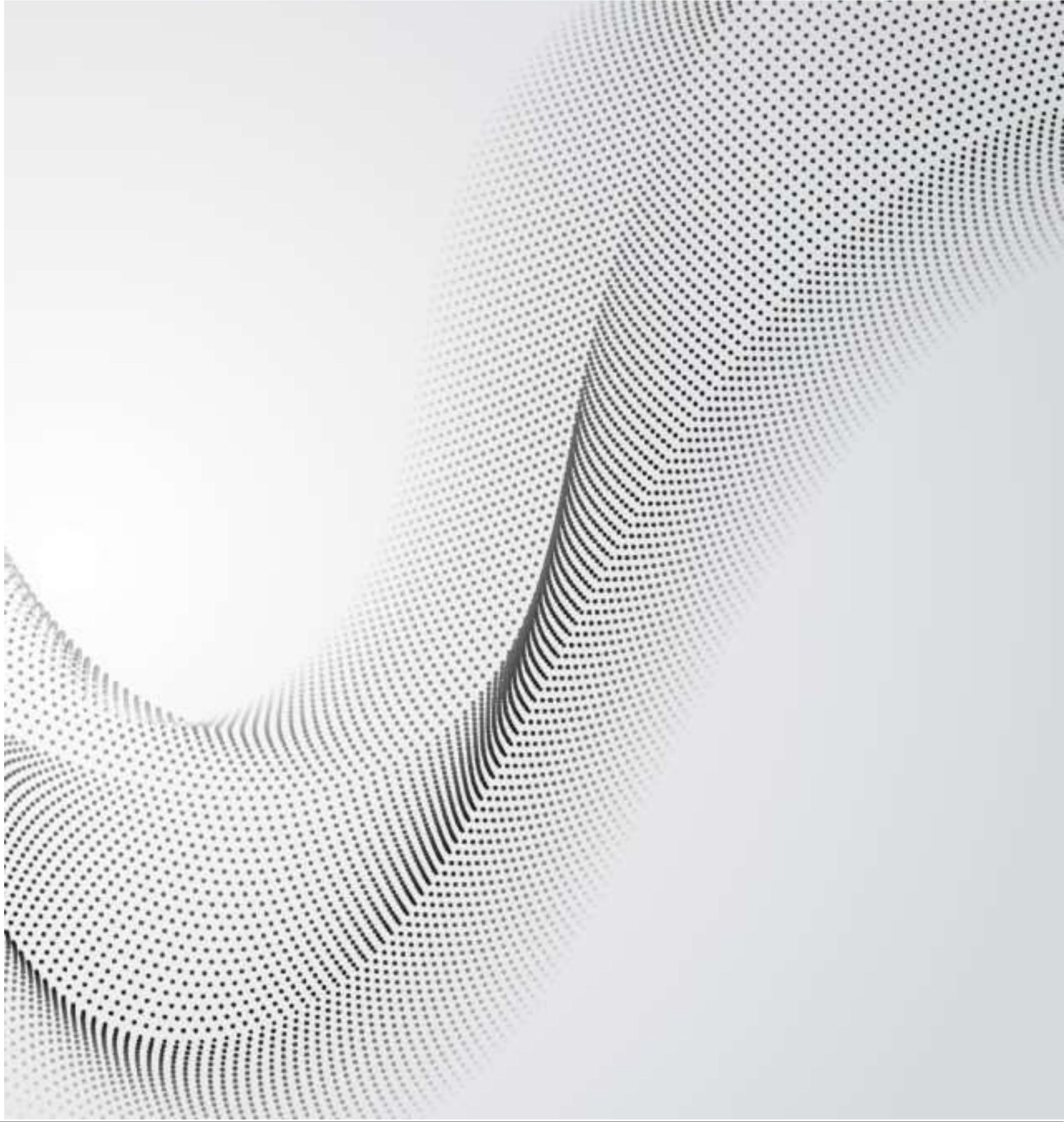
Steady-State Control Messages



1. Periodic HELLO and TC messages encrypted with sessionKey
2. Encrypted payloads encapsulated in TLV 0x11
3. Receiver decrypts and verifies tag
4. Secure communication maintained until rekeying
5. Protects against topology leakage and forgery

Implementation & Evaluation

- NS3-based simulation framework
- OLSR HELLO and TC message re-structuring
- Evaluation in high- and low-mobility scenarios
- Dynamic overhead evaluation based on network size.



Evaluation Setup

Network & Mobility

- Nodes placed in a 500×500 m area (static grid or Random Waypoint mobility).
- Mobility speeds: low mobility (1 m/s) and high mobility (10 m/s).
- Network sizes from 10 to 50 nodes.
- IEEE 802.11g WiFi with log-distance path loss.

Simulation & Metrics

- Instrumented control packets to measure per-node overhead (bits/s).
- Handshake time measured from KEX_RCVD to SECURE state.

Implementation

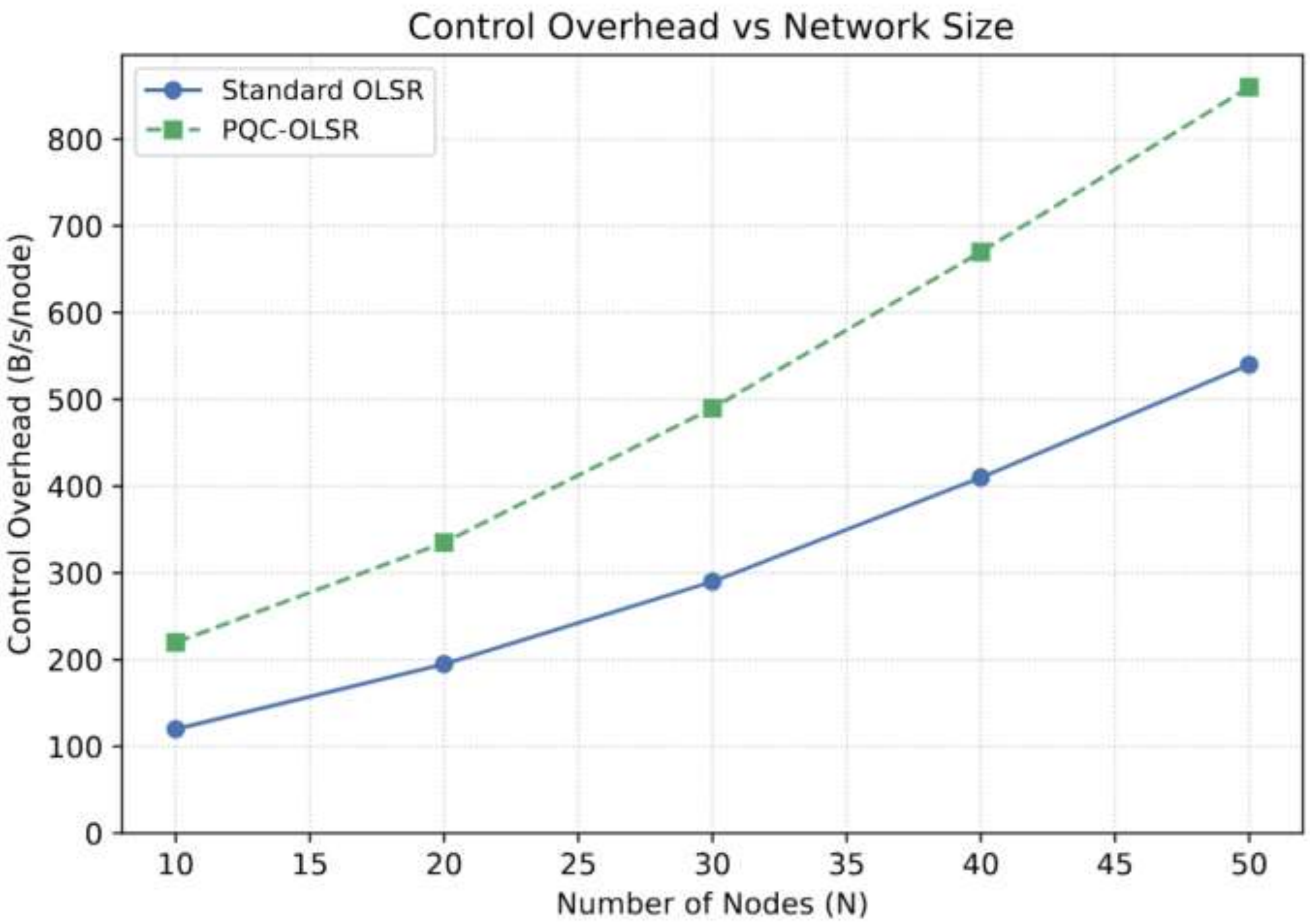
- Integrated into the OLSR module as a security shim without altering core routing logic.
- Uses liboqs for Kyber512 KEM operations and OpenSSL EVP for ChaCha20-Poly1305.
- Public keys (800 B) and ciphertexts (768 B) exchanged via TLV 0x0F/0x10; derived keys drive AEAD.
- Handshake Phase (HELLO):
  - TLV 0x0F: Kyber512 Public Key (800 B)
  - TLV 0x10: Kyber512 Ciphertext (768 B)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          OLSR Common Message Header (Type=TC, etc.)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Advertised Neighbor Seq Num (ANSN)    | Reserved     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Advertised Neighbor Main Address 1 (4 bytes)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Optional Metric 1 / Padding                                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
-                              ...                              -
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Advertised Neighbor Main Address N (4 bytes)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Optional Metric N / Padding                                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| TLV Type=0x11| TLV Length=Var| Nonce (12 bytes)               |
| (AEAD Data)  | (Variable)    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              |               | Encrypted TC Payload           |
|              |               | (Specific Hdr + Advert. Nbrs)  |
|              |               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              |               | Authentication Tag (16 bytes)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        OLSR Common Message Header (Type=HELLO, etc.)          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Htime | Willing | Link Code | Resvd |       Link Message Size |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Neighbor Interface Address 1 (4 bytes)              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Optional Link Metric 1 / Padding                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
-                              ...                              -
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Neighbor Interface Address N (4 bytes)              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Optional Link Metric N / Padding                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| TLV Type=0x0F| TLV Length=800| Kyber Public Key (pk)          |
| (KEM PubKey) | (800 bytes)   | (Value continues...)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| TLV Type=0x10| TLV Length=768| Kyber Ciphertext (ct)          |
| (KEM Cipher) | (768 bytes)   | (Value continues...)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| TLV Type=0x11| TLV Length=Var| Nonce (12 bytes)               |
| (AEAD Data)  | (Variable)    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              |               | Encrypted HELLO Payload        |
|              |               | (Specific Hdr + Neighbor Info) |
|              |               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              |               | Authentication Tag (16 bytes)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

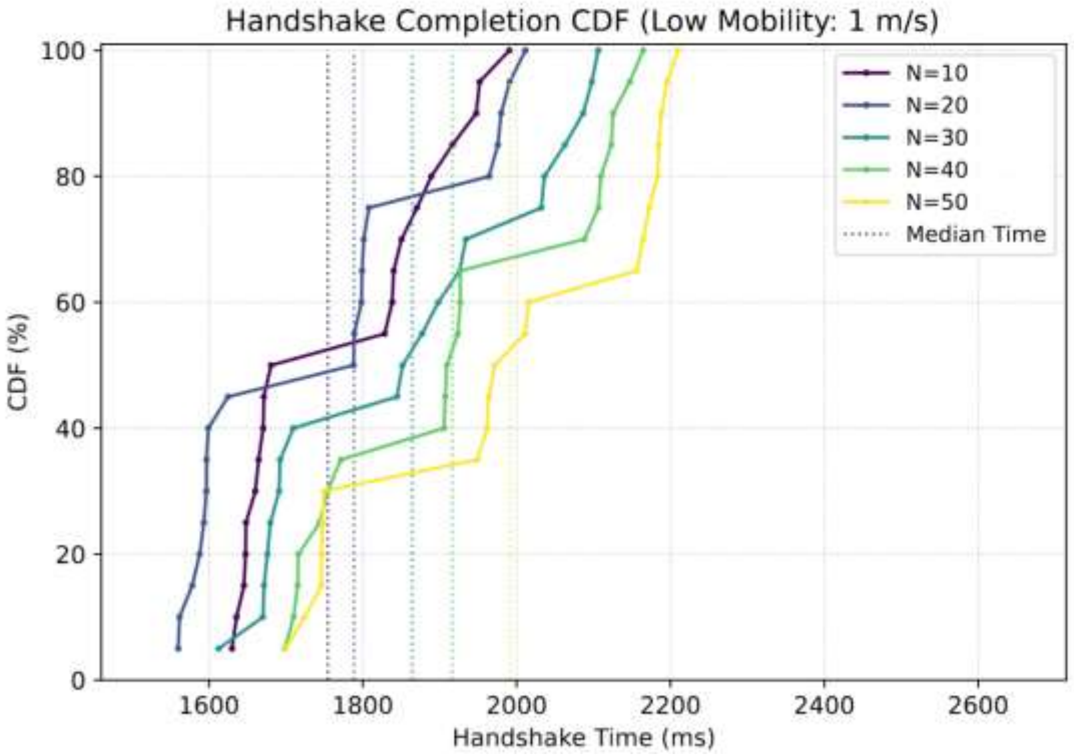
- AEAD overhead per message: 12 B nonce + 16 B authentication tag.
- Simulated 1 ms delay per PQC operation (Encapsulate/Decapsulate/Encrypt/Decrypt) to approximate computation cost.
- TLVs appended after core HELLO/TC headers without modifying base format.
- Backward Compatibility:
- Legacy nodes skip unknown TLVs without breaking.
- Steady-State Phase (HELLO/TC):
  - TLV 0x11: AEAD payload → Nonce (12 B) | Ciphertext | Tag (16 B)

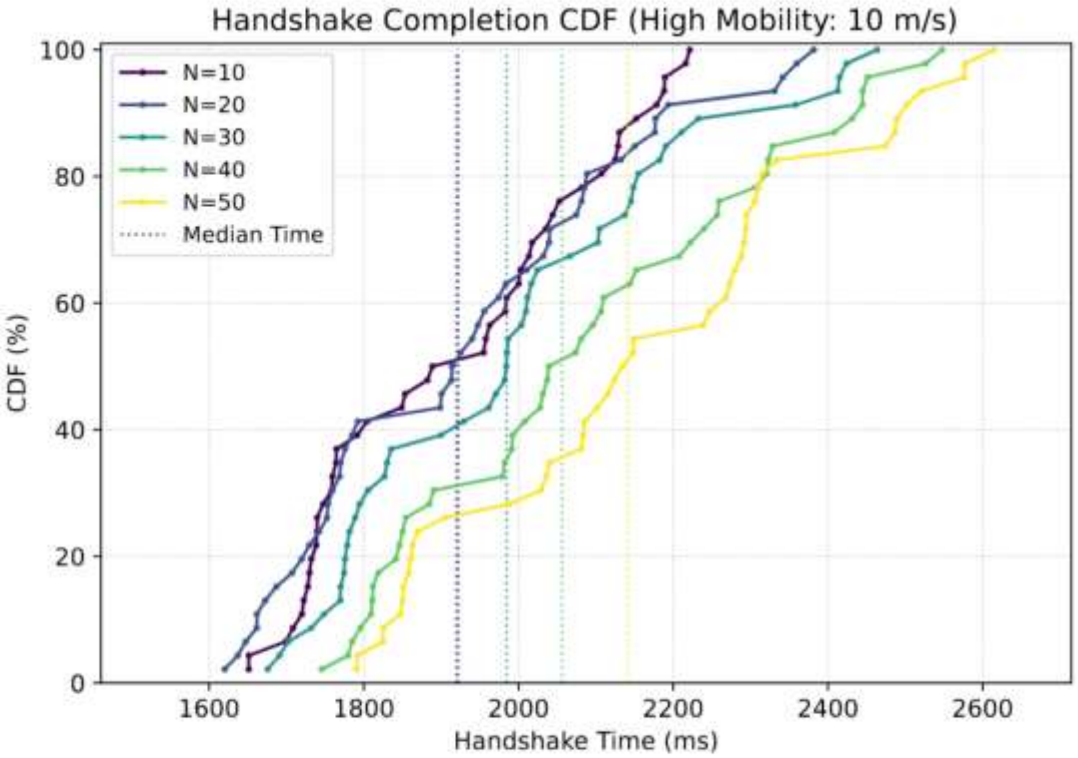
Results: Control Plane Overhead



- Baseline OLSR overhead increases with network size due to HELLO traffic and topology dissemination.
- PQC-OLSR overhead is significantly higher because each neighbour pair exchanges an 800 B public key and 768 B ciphertext during the handshake.
- Additional overhead comes from a 12 B nonce and 16 B tag appended to every secured HELLO/TC message.
- Despite the cost, the overhead scales linearly and provides confidentiality and integrity for the control plane.

Results: Handshake Completion Time





- In low mobility (1 m/s), handshake times cluster around 1.6–2.3 s; larger networks experience slightly longer delays.
- High mobility (10 m/s) shifts the distribution rightwards (1.8–2.6 s) and increases variance due to frequent neighbour changes.
- Even under dynamic conditions, handshake latencies remain within acceptable OLSR timescales.

Discussion

- Integrating PQC into the OLSR control plane is feasible but increases control overhead.
- Cryptographic delay has modest impact; handshake latency remains within protocol timescales.
- High mobility and larger networks amplify handshake variance, potentially delaying secure connectivity.
- Data plane performance is not affected (only control packets are encapsulated).
- Security gains (confidentiality, integrity, neighbour authentication) must be balanced against overhead in resource-constrained meshes.

Conclusion & Future Work

Conclusions:

- ✓ Presented a post-quantum secure extension of OLSR combining Kyber512 KEM and ChaCha20-Poly1305 AEAD via TLVs.
- ✓ Demonstrated practical implementation within ns-3 using standard cryptographic libraries.
- ✓ Evaluated control overhead and handshake latency across network sizes and mobility regimes.
- ✓ Security benefits outweigh overhead for many scenarios, providing confidentiality, integrity and authentication.

Future Extensions:

- ➢ Develop efficient rekeying and revocation mechanisms for dynamic networks.
- ➢ Design protocol-agnostic security layers to extend PQC protection beyond OLSR.
- ➢ Integrate Layer-3 control-plane security with data-plane protection for end-to-end security.

Thank you

XTRUST-6G is co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Smart Networks and Services Joint Undertaking. Neither the European Union nor the granting authority can be held responsible for them.
This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI)