# The Cost of Zero Trust: A Comparative Analysis of MACsec and IPsec Architectures for Secure Open Fronthaul

**Mahesha Viduranga Malmalabaduge,** Atif Ahmed,
Madhura Adeppady, and Aloizio Da Silva
maheshav@vt.edu, atifahmed@vt.edu, madhura@vt.edu, aloiziops@vt.edu
Commonwealth Cyber Initiative (CCI), Virginia Tech, USA

**19th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '26)**
Saarbrücken, Germany

# Content

1. Motivation and Introduction
2. Security Protocols Background
3. Threat Analysis
4. Methodology:
   i. Test Setup and Kernel-Space Settings
   ii. DPDK/VPP IPsec performance and S-Plane Stability
5. Evaluation:
   i. Kernel Space
   ii. DPDK/VPP IPsec
   iii. S-Plane Stability
6. Conclusion and Future works

# Motivation and Introduction

## Open Fronthaul (OFH) Disaggregation

Closed P2P fiber –> shared packet-switched network

Carries C/U/S/M-Planes on COTS hardware

Zero Trust recommended by O-RAN Alliance & 3GPP

## Strict OFH Timing Budget

**< 100 µs**

*one-way latency · nanosecond-precision PTP sync*

## Three Core Challenges We Address

i

Can encryption meet < 100 µs O-RAN timing budgets under realistic bursty 5G NR workloads?

ii

Which protocols enable multi-hop cloud deployment while complying with these timing constraints?

iii

Can nanosecond-precision PTP sync survive heavy crypto loads on commodity COTS hardware?

Commonwealth Cyber Initiative

cyberinitiative.org

# Security Protocols Background

## MACsec

*IEEE 802.1AE · Layer 2*

**32 B**

OVERHEAD · per frame

- In-place Ethernet frame encryption
- SecTag (8-16 B) + ICV (16 B)
- Hardware offload friendly
- Requires L2 adjacency (P2P)

## IPsec Transport

*ESP · Layer 3*

**34-50 B**

OVERHEAD · per packet

- Encrypts payload, keeps IP header
- ESP header (8 B) + IV (8 B) + ICV (16 B)
- Routed but exposes endpoints
- Kernel XFRM processing

## IPsec Tunnel

*ESP + outer IP · Layer 3*

**54-70 B**

OVERHEAD · per packet

- Encapsulates entire IP packet
- Adds 20 B outer IP header
- Full topology hiding (Zero Trust)
- ~2× MACsec overhead

Commonwealth Cyber Initiative
cyberinitiative.org

# Threat Analysis

## OFH Threat Landscape

**Eavesdropping**
*IQ-sample interception*

**Integrity and Replay**
*Injection and Replay Attack*

**Topology Mapping**
*Targeted DoS on control nodes*

## Header Visibility Across Protocols

| Field / Property | MACsec | Transport | Tunnel |
|---|---|---|---|
| MAC Addresses | Visible | Visible | Visible |
| IP Addresses | Encrypted | Visible | Hidden* |
| L2 Topology Hiding | ✗ | ✗ | ✗ |
| L3 Topology Hiding | ✓ | ✗ | ✓ |
| Multi-hop Support | ✗ | ✓ | ✓ |
| Payload Eavesdrop. Protection | ✓ | ✓ | ✓ |

**Key Insight: Only IPsec Tunnel Mode provides full Zero-Trust topology hiding across routed multi-hop fronthaul.**

Commonwealth Cyber Initiative
cyberinitiative.org

# Methodology: Test Setup and Kernel-Space Setting

**Test setup:**

- **O-DU Emulator:** Intel NUC Extreme (i9-9980HK)
- **O-RU Emulator:** Intel NUC (i7-1165G7)
- **NIC:** Intel X520-DA2 (82599ES) dual-port 10 GbE
- **Link:** 10 Gbps SFP+ over OM4 multimode fiber

## Phase 1: Kernel-Space Evaluation

### Configurations Tested

**Baseline** - Unencrypted Ethernet

**MACsec** - IEEE 802.1AE, AES-256-GCM

**IPsec Transport** - ESP-only

**IPsec Tunnel** - Full encapsulation

*Loads: 0.5–3.0 Gbps · 30 runs × 30 s · Mean ± SD, 95% CI*

### Traffic Generation & Metrics

**iperf3** - UDP throughput / reliability

**sockperf** - P99 tail-latency / PDV

**tcpreplay** - Realistic 5G NR PCAP (MATLAB)

**Metrics:** P99 latency, jitter (σ of inter-arrival), FLR, CPU sys-time / interrupts

Commonwealth Cyber Initiative

cyberinitiative.org

# Methodology: DPDK/VPP IPsec performance and S-Plane Stability

### Phase 2: DPDK/VPP IPsec

- **VPP v24.10** bypasses Linux kernel network stack entirely
- NIC bound to **vfio-pci** for direct hardware access
- AES-256-GCM with **Intel AES-NI / multi-buffer crypto**
- **Tools:** VPP ping (latency) · Cisco TRex (PCAP replay)

### Phase 3: S-Plane Stability

- PTP IEEE 1588v2 master–slave with **hardware timestamping (ptp4l)**
- 60-s test runs at each load (1-10 Gbps)
- Master offset (ns) ± SD, min/max excursions
- MTU 1500 & 9000 (jumbo)

**Four Deployment Architectures Evaluated**

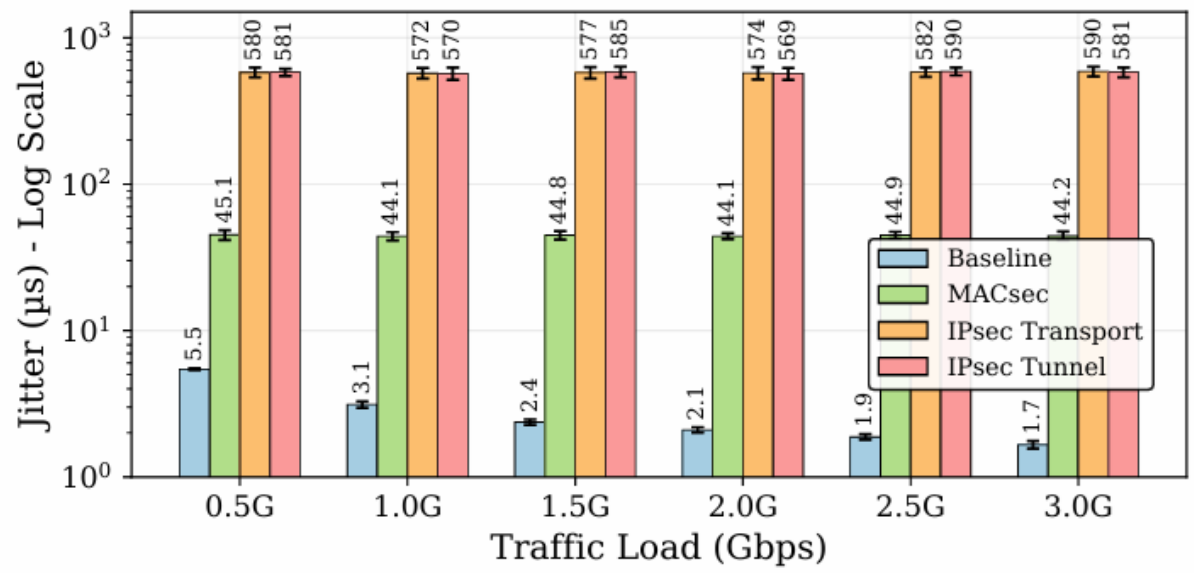
| Config | Port 1 | Port 2 | Architecture |
|---|---|---|---|
| A | PTP (kernel) | DPDK IPsec | Dual-Port Physical Separation |
| B | PTP + Kernel IPsec | Unused | Single-Port Virtual (shared) |
| C | Kernel IPsec | PTP (kernel) | Kernel + Physical Separation |
| D | PTP (PF) + DPDK IPsec (VF) | Unused | Single-Port SR-IOV |

Commonwealth Cyber Initiative xG TESTBED

Commonwealth Cyber Initiative
cyberinitiative.org

# Evaluation: Kernel Space

**Jitter under realistic 5G NR traffic (µs, log scale)**




***Note:** IPsec bars sit ~5-6× above the O-RAN HPF 100 µs threshold (log scale)*

**MACsec**

*~44 µs jitter · P99 38-77 µs to 2.5 G*

**Meets O-RAN High100 budget**

**Kernel IPsec**

*580-590 µs jitter · ~13× MACsec*

**Violates 100 µs budget by ~6×**

**Throughput Wall**

**1.65 Gbps** @ MTU 1500 (>20% loss)

**5.75 Gbps** @ MTU 9000 (jumbo)

*Kernel IPsec CPU-bound: cannot reach line rate*

Commonwealth Cyber Initiative

cyberinitiative.org

# Evaluation: DPDK/VPP IPsec

**Jitter Reduction vs Kernel IPsec**

**10×**

*45–66 µs · comparable to MACsec · routed multi-hop*

**1,088** clocks / pkt
*<2.5% variation (AES-NI / AVX-512)*

**8.5-11.5** µs avg latency
*well below O-RAN 100 µs threshold*

**>10** Gbps line-rate
*0% packet loss · MTU 9000*

## Jitter across traffic loads: DPDK/VPP vs Kernel IPsec (µs)

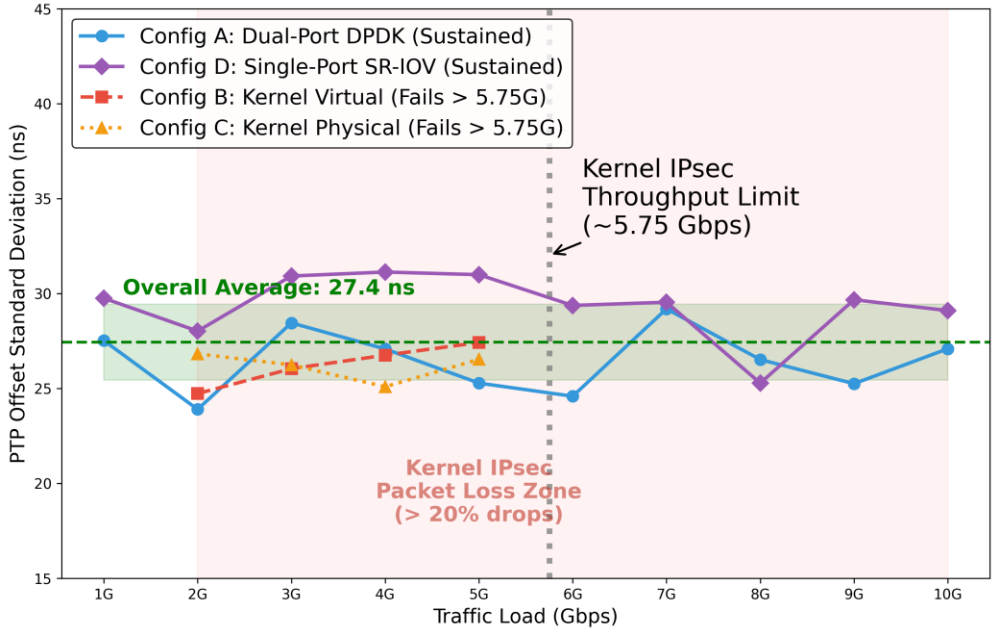
| Load | Network Jitter (µs) | | | Processing (Clocks/Pkt) | | |
|---|---|---|---|---|---|---|
| | Mean | SD | 95% CI | Mean | SD | 95% CI |
| 0.5G | 65.95 | 20.89 | ±8.44 | 1108 | 8 | ±3 |
| 1.0G | 45.13 | 20.29 | ±9.24 | 1086 | 5 | ±2 |
| 1.5G | 60.66 | 21.28 | ±14.30 | 1085 | 5 | ±4 |
| 2.0G | 50.13 | 22.79 | ±12.14 | 1087 | 5 | ±3 |
| 2.5G | 53.45 | 26.48 | ±16.82 | 1088 | 4 | ±2 |
| 3.0G | 50.01 | 23.18 | ±13.38 | 1084 | 5 | ±3 |



Commonwealth Cyber Initiative
cyberinitiative.org

# Evaluation: S-Plane Stability

## PTP offset SD vs traffic load (ns)




| Metric | Config A (Dual-Phys) | Config B (Kern+Virt) | Config C (Kern+Phys) | Config D (SR-IOV) |
|---|---|---|---|---|
| Mean Offset (ns) | -0.83 | -1.29 | -0.28 | 0.16 |
| Avg StdDev (ns) | 26.49 | 26.38 | 25.9 | 29.38 |
| Max \|Offset\|(ns) | 75 | 84 | 71 | 83 |
| Max Tested Load | 10Gbps | 5.75Gbps | 5.75Gbps | 10Gbps |
| O-RAN Class C | ✓ | ✓ | ✓ | ✓ |

**Physical separation**

*provides NO measurable benefit*

**SR-IOV (Config D)**

*scales to 10 Gbps with +3 ns only*

**Hardware timestamping**

*isolates PTP from software path*

Commonwealth Cyber Initiative xG Testbed

Commonwealth Cyber Initiative
cyberinitiative.org

# Conclusion and Future works

## MACsec

*Optimal for P2P L2-adjacent links*

- ~44 µs jitter
- Hardware-offloaded
- × No multi-hop support

## Kernel IPsec

*Fails O-RAN timing*

- ~580 µs jitter
- L3 topology hiding
- × XFRM stack bottleneck

## DPDK/VPP IPsec

*Best of both worlds*

- 45–66 µs jitter (10× kernel)
- Full Zero-Trust topology hiding
- Line-rate 10 Gbps on COTS

**Key Takeaway:** The IPsec performance wall is an OS artifact not protocol-inherent. DPDK/VPP bridges MACsec-level determinism with multi-hop cloud routing without SmartNICs or FPGAs.

**Future Work**

*Multi-hop fronthaul topologies · Attack scenarios via network emulators · Real propagation delays & impairment profiles*

Commonwealth Cyber Initiative
cyberinitiative.org

# Thank You

*Questions & Discussion*

**Mahesha Viduranga Malmalabaduge, Atif Ahmed, Madhura Adeppady, Aloizio Da Silva**

maheshav@vt.edu, atifahmed@vt.edu, madhura@vt.edu, aloiziops@vt.edu

*Commonwealth Cyber Initiative · Virginia Tech*

Funded by **NTIA NOFO1 ACCoRD Project** · Visit **www.ccixgtestbed.org**

Commonwealth Cyber Initiative

cyberinitiative.org