100 Gbps Multi-Tenant FPGA-based MACsec Aggregation to Secure the Open-RAN Fronthaul

D. Dik[1,2], R. D. Oliveira[3], E. Arabul[3], C. Vrontos[3], M. S. Berger[1], R. Nejabati[3], D. Simeonidou[3]

[1] Department of Electrical and Photonics Engineering, Technical University of Denmark, Kgs. Lyngby, Denmark, danro@dtu.dk
[2] Comcores ApS, Kgs. Lyngby, Denmark
[3] High Performance Network Group, University of Bristol, Woodland Road, Bristol, United Kingdom

Abstract *This paper proposes an FPGA-based hardware architecture with MACsec to secure dynamic 100 Gbps Open-RAN Fronthaul networks, where multiple channels are aggregated with independent MACsec protection. The architecture respects the fronthaul delay budget with a fixed pipeline latency of 537.6 ns.*

Introduction

New specifications for the Radio Access Network (RAN) are being defined by the Open-RAN (O-RAN) Alliance to enable deployments of O-RAN-based open interfaces and multi-vendor interoperability in 5G RAN infrastructures. The specifications are based on the split of base station functionalities. This results in an O-RAN Remote Unit (O-RU) implementing lower physical functions, and an O-RAN Distributed Unit (O-DU) implementing higher physical functions. The connectivity in the O-RAN infrastructure between these two units is the O-RAN Fronthaul (O-FH)[1].

The O-FH carries information divided into four planes. First, a Control Plane (C-Plane) for control messages over eCPRI. Second, a User Plane (U-Plane) for user data over eCPRI. Third, a Synchronization Plane (S-Plane) for periodic synchronization with PTP. Finally, a Management Plane (M-Plane) for configuration. The O-FH has strict performance requirements that serve as Key Performance Indicators (KPI) consisting of latency, bandwidth, frame loss, and time accuracy.

At the link layer, Ethernet is the standard technology for the O-FH network[2]. According to the specification, the three CUS-Planes are directly encapsulated over Ethernet, while the M-Plane is transported as application over TCP and IP. In terms of topology, the O-FH network can vary from a point-to-point interface to a more complex network of switches. This supports resource sharing between O-RUs and multi-tenant aggregation. Moreover, the O-FH network can be of a multi-provider nature where intermediate switches are managed by different suppliers[3].

Having the CUS-Planes directly encapsulated over Ethernet is beneficial from an interoperability perspective. Nevertheless, the clear-text nature of the carried content, together with the multiple network topology options expose the O-FH to Layer 2 threats that can significantly risk the operation of the RAN[4],[5]. In this context, previously we have demonstrated[6] that Media Access Control Security (MACsec)[7] is a suitable candidate to secure the O-FH due to its security features and operation on Ethernet frames. Furthermore, we proposed a MACsec hardware (HW) architecture that meets the O-FH performance defined in[3]. However, the design hasn't been evaluated for dynamic large-scale O-FH networks. These types of networks include multi-user 100 Gbps aggregation over Optical Transport Networks (OTNs)[8],[9].

Commercial OTN HW aggregators exist with Advanced Encryption Standard (AES) capabilities to protect 100 Gbps links[10]–[12]. However, they don't have support for the O-FH. Moreover, AES alone provides only confidentiality but does not address the security features of authentication, integrity, and replay protection that are indispensable in the O-FH. Additionally, these equipment secures the aggregated traffic in the 100 Gbps port, being a limitation for multi-tenant architectures with Security-as-a-Service features that require independent protection to each client[13],[14].

In this scenario, the main contribution of this paper is a 100 Gbps multi-tenant MACsec aggregation HW architecture for the O-FH. The main goal is to provide Security-as-a-Service to multiple O-RUs with independent MACsec protection among them. This paper evaluates the feasibility of the architecture for its implementation on Field-Programmable Gate Array (FPGA) and its performance impact on a dynamic large-scale OTN-based O-FH network.

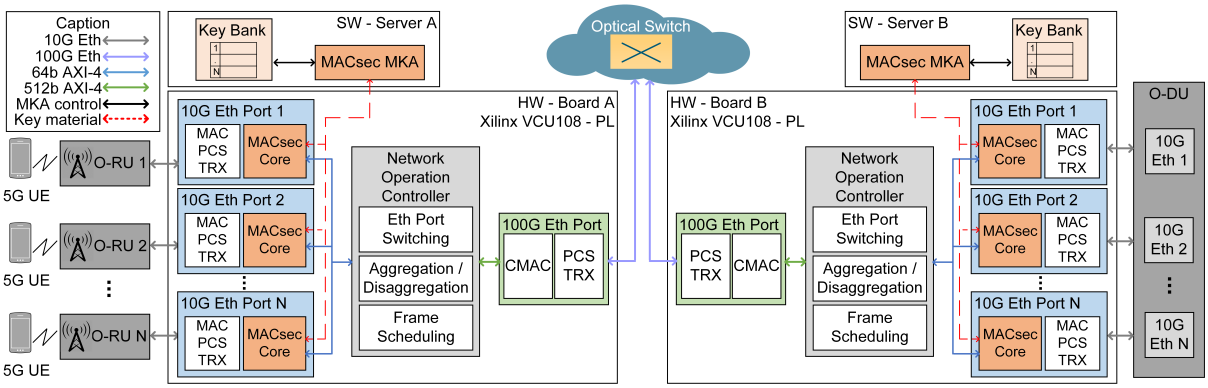

Fig. 1: Top-level system architecture of 100 Gbps MACsec Aggregation for the O-FH

System Architecture

Fig. 1 illustrates the proposed system architecture. It consists of a HW domain and a software (SW) domain. The HW domain implements the fronthaul data processing pipeline which includes three main subsystems: 10G Ethernet Port, Network Operation Controller (NOC), and 100G Ethernet Port. Each 10G Ethernet Port subsystem serves a 10 Gbps O-RU or O-DU client. This subsystem includes the MACsec HW core that implements our design, providing a secure MAC service to its corresponding O-RU/O-DU data plane. As a result, the data to and from the O-RU/O-DU is protected with authentication, confidentiality, integrity, and replay protection. The NOC subsystem performs aggregation and disaggregation of the traffic from all the 10 Gbps O-RU/O-DU clients. It also includes functions of port switching and frame scheduling to map data to the corresponding port at the correct bit rate and time. Finally, the 100G Ethernet Port subsystem provides the CMAC service to the aggregated data for the 100 Gbps interface. The SW domain implements the MACsec Key Agreement (MKA) protocol, which is a companion protocol that performs MACsec control plane for peer authentication and key negotiation[15]. It authenticates each 10G Port and provides security keys to the MACsec Core for data protection and verification.

The architecture proposed in this paper was implemented as Register Transfer Level (RTL), whose source code was written in SystemVerilog Hardware Description Language (HDL). The Xilinx Board VCU108, which includes the Virtex UltraScale XVCU095 FPGA, was used to implement the design[16]. For the experimental setup, two Xilinx boards were used to implement the proposed architecture; one board serving the O-RU clients and one serving the O-DU side. The two boards were connected through an Optical Cross Connect (OXC). The O-DU clients and radio controller software were provided by Accelleran, while the O-RU clients were from Benetel (RAN 650). For the User Equipment (UE), in-house developed Multiple Radio Access Technology (multi-RAT) Customer Premises Equipment (CPE) devices were used.

Tab. 1: FPGA utilization results

Core	LUTs (FPGA %)	FFs (FPGA %)
10G*	4,358 (0.81%)	1,550 (0.14%)
MACsec	141,472 (26.32%)	28,655 (2.67%)
NOC	8,230 (1.53%)	12,401 (1.15%)
100G	1,523 (0.28%)	3,437 (0.32%)

*10G Eth Port without MACsec Core

Results: FPGA Evaluation

This section evaluates the architecture implementation in FPGA devices in terms of resource utilization and internal pipeline latency. The results are reported in Tab. 1 and Tab. 2. The resource utilization results are the output of the logic synthesis process executed by Xilinx Vivado 2020.2 using the resource utilization report. Tab. 1 reports the resource utilization of a single 10G Ethernet Port without MACsec, the MACsec Core standalone, the NOC, and the 100G Ethernet Port. The report is given in terms of Look-up Tables (LUTs) and Flip-Flops (FFs).

It can be seen that the MACsec Core has the highest resource consumption. This is due to the pipelined implementation of its AES-GCM subcomponent designed for very high speeds. The AES-GCM itself occupies 77% of the LUTs and 64% of the FFs of the total MACsec Core utilization. A single instance of the 10G Ether-

Tab. 2: FPGA internal pipeline latency

Core	SoF in to SoF out (ns)
10G*	171.2
MACsec	144
NOC	67.2
100G	155.2
Total	**537.6**

*10G Eth Port without MACsec Core

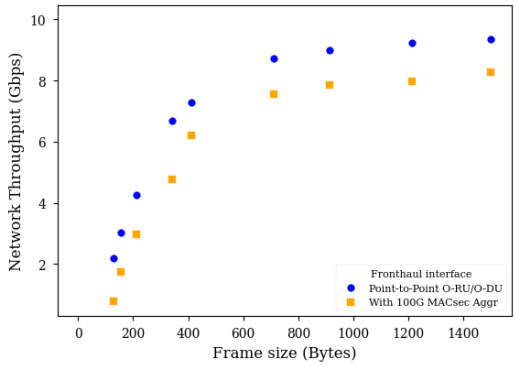

Fig. 2: Fronthaul throughput evaluation

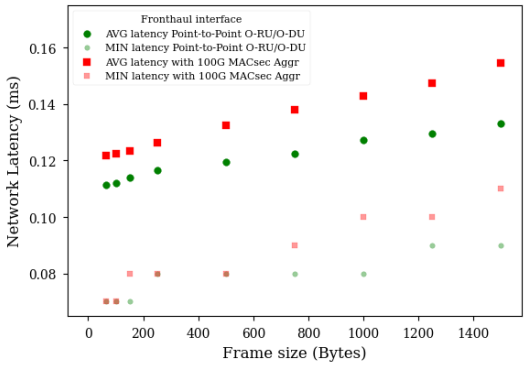

Fig. 3: Fronthaul round-trip latency evaluation

net Port subsystem including the MACsec Core serves one O-RU/O-DU client. To support various clients, multiple instances of the 10G Ethernet Port subsystem are required. This doesn't apply to the NOC neither to the 100G Ethernet Port as they only require one instance regardless of the number of clients. The Xilinx Board VCU108 and the FPGA Mezzanine Cards (FMCs) used in this setup support up to 16 cages for 10G Ethernet Ports and a maximum resource utilization of 537,600 LUTs and 1,075,200 FFs. Therefore, due to the constrained resource utilization of this board and FPGA, theoretically, up to 16 O-RU/O-DU clients are possible to be aggregated, with 3 of them protected with MACsec. However, if a bigger FPGA is used, such as the Xilinx Versal VP2802 with 3,349,120 LUTs available[17], all 16 O-RU/O-DU clients could be protected with MACsec. Moreover, the MACsec AES-GSM subcomponent can have its pipeline optimized targeting a reduction of the resource utilization.

The FPGA internal pipeline latency is the time a subsystem takes to process a frame from the input of the start of frame (SoF in) to the output of the start of frame (SoF out). Tab. 2 shows the latency for each subsystem, all with a fixed latency regardless of the frame size. This offers a constant data throughput to the O-FH interface. However, an impact by the frame size can be expected depending on the buffering capacity of the FPGA and embedded memory. Hence, further analysis of the buffering impact shall be conducted. The strictest latency requirement defined in the O-FH is a maximum one-way frame delay of 25 μs for Ultra-low latency use cases[3]. Thus, the total latency of 537.6 ns added by the architecture represents a minimal contribution to the delay budget.

Results: Network Throughput and Latency

This section analyzes the impact of the proposed architecture on the O-FH network performance. Data throughput and latency were measured from the O-RU to the O-DU. Fig. 2 and Fig. 3 illustrate the achieved throughput and latency with and without the proposed architecture. It was observed that the throughput and delay increase for bigger frame sizes. With the proposed architecture, a maximum throughput of 8.28 Gbps was achieved, which represents an average line rate reduction of 13% compared to the benchmark point-to-point scenario without FPGA. This is due to the overhead contribution by the NOC aggregation, MACsec, and internal FPGA buffering. The network latency increases by an average of 11% with a maximum latency of 0.15 ms. According to Fig. 3, the average latencies with and without MACsec are very similar within a sub-miliseconds precision. There is an average added delay when applying MACsec of about 0.01 ms and very often the round-trip time for both cases were overlapping, we also show the minimum latency required in each case, making it more evident that the added delay is between 0.01 and 0.02 ms and most significant for bigger frames.

Conclusions

We proposed and implemented a 100 Gbps multi-tenant MACsec HW architecture for the O-FH. It was shown that the architecture is feasible for FPGAs with the support of multiple O-RU/O-DU clients fully protected using MACsec. The architecture has a fixed internal pipeline delay of 537.6 ns offering a constant FPGA datapath throughput and a minimal delay contribution to the O-FH budget. It was demonstrated that the impact of the architecture on the O-FH network performance is low without interrupting the RAN service. The overall network throughput impact was 13%, bringing the rate to a maximum value of 8.28 Gbps. The network latency was increased by 11% with a maximum added delay of 20 μs.

Acknowledgements

This work is supported by Comcores ApS, by Innovationsfonden Denmark through grant 0153-00126A, and by the EU-funded project 5G COMPLETE (871900).

References

[1] O-RAN Alliance, "O-RAN Control, User and Synchronization Plane Specification", O-RAN Alliance, Technical Specification O-RAN.WG4.CUS.0-R003-v11.00, Mar. 2023. [Online]. Available: https://orandownloadsweb.azurewebsites.net/specifications.

[2] IEEE, "IEEE Standard for Packet-based Fronthaul Transport Networks", *IEEE Std 1914.1-2019*, pp. 1–94, 2020. DOI: 10.1109/IEEESTD.2020.9079731.

[3] O-RAN Alliance, "Xhaul Transport Requirements", O-RAN Alliance, Technical Specification O-RAN.WG9.XTRP-REQ-v01.00, Feb. 2021, Available: https://orandownloadsweb.azurewebsites.net/specifications.

[4] D. Dik and M. S. Berger, "Transport Security Considerations for the Open-RAN Fronthaul", in *Proceedings of 2021 IEEE 4th 5G World Forum (5GWF)*, 2021, pp. 253–258. DOI: 10.1109/5GWF52925.2021.00051.

[5] J. Y. Cho, A. Sergeev, and J. Zou, "Securing Ethernet-Based Optical Fronthaul for 5G Network", in *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES'19)*, ser. ARES '19, Canterbury, CA, United Kingdom: ACM, 2019, ISBN: 9781450371643. DOI: 10.1145/3339252.3341484.

[6] D. Dik and M. S. Berger, "Open-RAN Fronthaul Transport Security Architecture and Implementation", *IEEE Access*, 2023, In Press.

[7] IEEE, "IEEE Standard for Local and Metropolitan Area Networks - Media Access Control (MAC) Security", *IEEE Std 802.1AE-2018 (Revision of IEEE Std 802.1AE-2006)*, pp. 1–239, 2018. DOI: 10.1109/IEEESTD.2018.8585421.

[8] Coriant. "The Role of OTN Switching in 100G & Beyond Transport Networks Managing Bandwidth for Long Haul and Metro Network Evolution". (2016), [Online]. Available: https://www.ofcconference.org/getattachment/90c0e6a4-08c1-45fb-a7f2-2957d444dc7d/The-Role-of-OTN-Switching-in-100G-Beyond-Transpo.aspx (visited on 04/05/2023).

[9] E. Arabul, R. Oliveira, A. Emami, *et al.*, "100 Gbps Quantum-Secured and O-RAN-Enabled Programmable Optical Transport Network for 5G Fronthaul", English, *IEEE/OSA Journal of Optical Communications and Networking*, Mar. 2023, ISSN: 1943-0620.

[10] M. Dworkin, E. Barker, J. Nechvatal, *et al.*, "Advanced Encryption Standard (AES)", NIST, Computer Security Standard, Cryptography. FIPS 197, Nov. 2001. DOI: https://doi.org/10.6028/NIST.FIPS.197.

[11] ADVA. "FSP 3000 : Open Optical Transport". (2021), [Online]. Available: https://www.adva.com/en/products/open-optical-transport (visited on 04/05/2023).

[12] IDQ. "Centauris CN9000 Series". (Jan. 2021), [Online]. Available: https://www.idquantique.com/quantum-safe-security/products/centauris-cn9000-series/ (visited on 04/05/2023).

[13] R. Dangi, A. Jadhav, G. Choudhary, N. Dragoni, M. Mishra, and P. Lalwani, "ML-Based 5G Network Slicing Security: A Comprehensive Survey", English, *Future Internet*, vol. 14, no. 4, 2022, ISSN: 1999-5903. DOI: 10.3390/fi14040116.

[14] R. D. Oliveira, E. Arabul, R. Wang, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Demonstration of a Resilient and Quantum-Secured Time-Shared Optical Network with Multi-Level Programmability", in *2022 Optical Fiber Communications Conference and Exhibition (OFC)*, 2022, pp. 1–3.

[15] IEEE, "IEEE Standard for Local and metropolitan area networks–Port-Based Network Access Control", *IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004)*, pp. 1–205, 2010. DOI: 10.1109/IEEESTD.2010.5409813.

[16] Xilinx. "VCU108 Evaluation Board User Guide (UG1066)". (Feb. 2019), [Online]. Available: https://docs.xilinx.com/v/u/en-US/ug1066-vcu108-eval-bd (visited on 04/05/2023).

[17] Xilinx. "Xilinx Versal Premium Series". (Oct. 2022), [Online]. Available: https://www.xilinx.com/products/silicon-devices/acap/versal-premium.html#productTable (visited on 04/05/2023).