IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 31 March 2023, accepted 2 May 2023, date of publication 8 May 2023, date of current version 16 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3274487

RESEARCH ARTICLE

Open-RAN Fronthaul Transport Security Architecture and Implementation

DANIEL DIK[1,2], (Graduate Student Member, IEEE), AND MICHAEL STÜBERT BERGER[2], (Member, IEEE)

[1]Comcores ApS, 2800 Kongens Lyngby, Denmark
[2]Department of Electrical and Photonics Engineering, Technical University of Denmark, 2800 Kongens Lyngby, Denmark

Corresponding author: Daniel Dik (danro@dtu.dk)

This work was supported in part by Comcores ApS, and in part by Innovationsfonden Denmark under Grant 0153-00126A.

ABSTRACT The main innovations for next-generation cellular networks are in the Radio Access Network (RAN). Here, the base station functionalities are split between a Radio Unit (RU) and a Distributed Unit (DU), resulting in a virtualized architecture where functions can be centralized close to the core for performance improvement and function extendibility. The fronthaul is the interface between RUs and DUs. It transports very sensitive data and is constrained by strict performance requirements. The clear-text nature of the fronthaul protocols and its direct encapsulation over Ethernet exposes the fronthaul to Layer 2 threats and vulnerabilities that can significantly threaten the operation of the RAN. This paper presents a detailed analysis of the transport network security in the fronthaul. It describes the threats and vulnerabilities that the fronthaul is exposed to and their overall network impact, thereby, elucidating the urgent need for Layer 2 security mechanisms. This paper introduces MACsec as a potential solution to protect the fronthaul. It outlines MACsec's capabilities and limitations for threats protection, and its implementation challenges in the fronthaul network. Finally, this paper proposes three hardware architectures to fully secure the fronthaul using MACsec and evaluates their feasibility in Field-Programmable Gate Array (FPGA) devices and their impact on the network performance.

INDEX TERMS FPGA, Fronthaul, MACsec, open-RAN, security.

I. INTRODUCTION

The fifth generation (5G) and future cellular network specifications are driven by non-consumer services applications. These include massive Machine-Type Communications (mMTC), such as support for billions of Internet of Things (IoT) devices, and Ultra-Reliable Low Latency Communications (URLLC) applications, for example, industrial automation and autonomous vehicles [1], [2]. 5G also provides a range of improvements for faster mobile broadband services. To support all these new verticals, there is a need for network architecture innovations in the Core Network (CN) and in the Radio Access Network (RAN). This includes Cloud RAN, Virtual RAN, Open RAN, Service-based CN architecture, Software Defined Networking (SDN), Network Function Virtualization (NFV), network slicing, and cloud and edge computing [3], [4]. The convergence of these and more technologies promises great innovation in the network and in the applications that it can serve. However, it also leads to a larger attack surface where the exploitation of threats and vulnerabilities could cause the network to malfunction [5], [6]. Therefore, there is an urgent need to analyze all the security aspects across the whole 5G system, including threats to the user equipment, air interface, edge network, backhaul connectivity, core network, and external networks.

One of the main innovations for 5G and next-generation networks is in the RAN where the base station functionalities are split [7]. This leaves only a few physical functionalities in the antenna location which results in a new RAN virtualized architecture where functions can be centralized close to the 5G core. Therefore, resource sharing between Radio Units (RUs) is possible. This enables simpler RUs implementation requirements and easier function extendibility, which makes it possible for multiple vendors to provide base station

The associate editor coordinating the review of this manuscript and approving it for publication was Miguel López-Benítez.

solutions. However, additional specifications are needed to ensure interoperability.

The need for further specifications has given rise to various Open RAN initiatives. The most prominent is the Open-RAN (O-RAN) Alliance [8]. The O-RAN Alliance was established in 2018 and unites mobile network operators, vendors, and research and academic institutions from all around the world to standardize the RAN as an open, intelligent, virtualized, and fully interoperable ecosystem. The O-RAN Alliance defines RAN specifications with an emphasis on interfaces and implementation guidelines. Specifically, those which are not detailed in the 3rd Generation Partnership Project (3GPP) recommendations and are important for interoperability. This will result in the sourcing of network infrastructure components from different suppliers, ensuring interoperability, and driving higher innovation at lower costs.

The architecture for the New Radio that the O-RAN Alliance has defined is based on functional split option 7-2x of the baseband station processing chain [9]. This results in a redistribution of lower and higher layer functionalities between new O-RAN components as illustrated in Fig. 1. The base station is divided into two units. The O-RAN Radio Unit (O-RU) implements lower physical functions. The O-RAN Distributed Unit (O-DU) implements higher physical functions. The connectivity in the O-RAN infrastructure between these two units is the O-RAN Fronthaul (O-FH). The O-FH carries very sensitive information between the O-RU and the O-DU. This information is divided into four data planes; Control Plane, User Plane, Synchronization Plane, and a Management Plane. These data planes impose strict high-performance requirements.

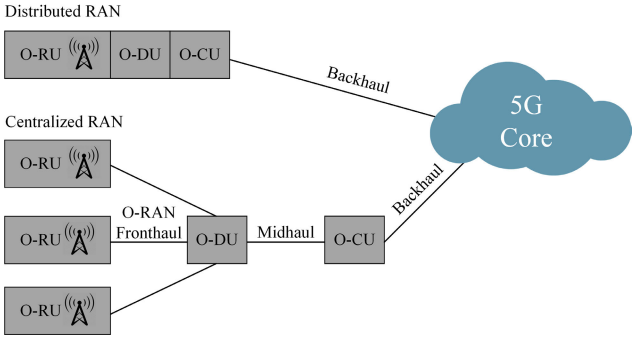


FIGURE 1. O-RAN transport network architecture. Split of base station functionalities results in new RAN units, O-RU implementing lower physical functions, and O-DU implementing higher physical functions, with the O-FH as the interface between them.

Ethernet is the preferred packet-based technology for the transport of the data planes traffic in the O-FH. This is because of its ubiquitous applications and the ability to mix different types of traffic. Consequently, the Common Public Radio Interface (CPRI) in 4G LTE between the Remote Radio Unit (RRU) and BaseBand Unit (BBU) has been replaced by the Ethernet-based enhanced CPRI (eCPRI) interface for radio control and user data.

The clear-text nature of the data planes and its direct encapsulation over Ethernet exposes the O-FH to Layer 2 threats and vulnerabilities that can significantly risk the operation of the RAN. For example, a Man-in-the-Middle could impersonate a legitimate synchronization message and inject a false clock into the network causing a degradation of the time service. This can result in a complete Denial-of-Service of the network. Hence, there is an urgent need for Data Link Layer security mechanisms to protect the O-FH from any type of threat.

An O-RAN Alliance Security Work Group had been put together to address the security aspects of the O-RAN Architecture. Its core objective is to define security specifications for each component and interface. As recognized in the O-RAN Security Threat Modeling and Remediation Analysis 4.0, the O-FH interface has its own specific threats and vulnerabilities [12]. The most recent specifications from October 2022 have greatly advanced the security needs of the industry. They have defined security requirements that are focused mainly on authentication and less on confidentiality and integrity concerns. However, based on the identified threats and vulnerabilities, confidentiality and integrity are equally important. On the other hand, another Work Group within the O-RAN Alliance defines no requirements for security. They argue that the high requirements for delay, time, and bandwidth in the O-FH do not permit security solutions to be used [10].

Media Access Control Security (MACsec) is a Layer 2 security protocol standardized by the IEEE that operates on Ethernet frames [13]. Its features of authentication, confidentiality, and integrity make it a potential candidate to protect the O-FH. However, the O-FH has multiple requirements that could challenge the use of MACsec. These requirements can be divided into two groups: security and performance. Security requirements are the security features that are indispensable for the O-FH to be protected against potential threats and attacks. Performance requirements are the network aspects of the O-FH for its operation, such as network topologies and data protocols.

The main challenges that are essential for MACsec to address are a) the compatibility of MACsec security functions with all the threats in the O-FH transport network, and b) the impact of MACsec on the performance of the different O-FH topologies and protocols. While MACsec may provide the necessary features to protect the O-FH, it could limit the operation of the protocols under the various possible topologies. Thus, the capability of MACsec to fully secure the O-FH while satisfying its requirements needs to be analyzed [14].

The literature on the security of 5G networks suggests that there are potential threats to the O-FH that may be protected by MACsec because of the suitability of its security features [15], [16]. However, the literature lacks a comprehensive analysis of those threats and their precise impact on the O-FH network. Furthermore, the specific compatibility of MACsec with the O-FH has not been fully investigated. This includes the challenges it faces in respecting the strict performance

requirements. White papers exist with commercial MACsec solutions for Ethernet networks [17], [18]. However, these are proprietary solutions without a detailed description of their design, and without a clear analysis of their applicability for the O-FH scenario. Therefore, this work aims to address these gaps by providing the following contributions.

A. CONTRIBUTIONS

This paper has three main contributions. First, it provides a detailed analysis of the transport network security in the O-FH interface between O-RUs and O-DUs. It identifies a number of threats for the different O-FH protocols and proposes the security features that are indispensable to protect the O-FH. Second, this paper provides a comprehensive study of the applicability of MACsec as a security protocol to protect the O-FH, including the benefits and limitations of MACsec to secure the O-FH while respecting its performance and operation. Finally, this paper proposes a MACsec hardware architecture for the O-FH that meets its security and performance requirements. It evaluates the feasibility of the architecture for its implementation on Field-Programmable Gate Array (FPGA) devices and for its impact on the network performance.

B. OUTLINE OF THE PAPER

The remaining part of this paper is organized as follows. Section II presents the O-FH including the types of data it transports, the encapsulation protocols that are involved, and their strict performance requirements. Section III analyzes each type of traffic being transported in the O-FH and identifies the different threats and vulnerabilities an attacker can exploit to impact the network. Section IV presents MACsec as a Data Link Layer security solution. Section V makes a thorough analysis of the compatibility of MACsec with the O-FH, including the challenges and limitations that MACsec faces to protect it from all the identified threats, and to respect its strict performance requirements. Section VI proposes three hardware architectures to fully secure the O-FH using MACsec taking into account the identified challenges and limitations. Sections VII and VIII evaluate these architectures under different performance metrics to demonstrate the possibility of O-FH protection while meeting its strict performance requirements. Finally, the conclusions are presented in Section IX.

II. OPEN-RAN FRONTHAUL

The RAN processing functions can be split at various points as illustrated in Fig. 2 [19]. This enables the functionality to be deployed at various points in the network. Lower layer splits enable simpler, more compact, and lower-cost RU implementations as only the RF and lower physical layer functions need to be supported. Since 5G will require an order of magnitude increase in the number of RUs to be deployed, this can lower deployment costs significantly.

The functional splits also provide flexibility when deploying functionality. This allows specific service performance

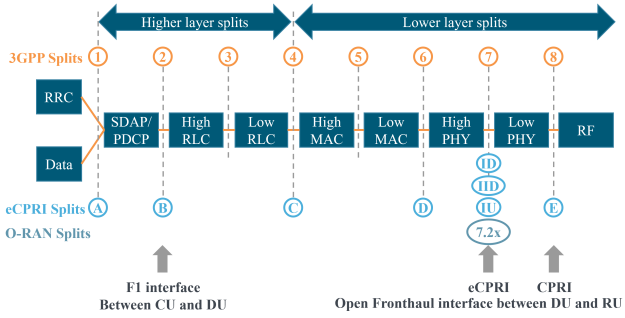


FIGURE 2. Split options of RAN processing functions. The O-RAN Alliance has defined split 7.2x based on the eCPRI interface.

requirements to be met. For example, efficient aggregation can be provided by centralizing the virtualized CU and DU functionality as close to the core as possible. On the other hand, if lower latency is required, the CU and DU functionality should be located as close to the RUs as possible.

The F1 interface between the CU and DU is defined in 3GPP specifications. However, the O-FH interface between the DU and RU is not defined. This means it has been proprietary to the vendor in previous mobile network generations. The O-RAN Alliance has defined split 7.2x of base station functionalities with O-FH interface specifications that enable multivendor operation [10]. This is based on the eCPRI interface that replaced the CPRI interface in 4G LTE between the RRU and the BBU.

A. DATA PLANES

The O-FH carries very sensitive information between O-RU and O-DU. This information is divided into four data planes as illustrated in Fig. 3:

- Control Plane (C-Plane): real-time control information to the O-RU over eCPRI to define how the User Plane traffic should be handled.
- User Plane (U-Plane): real-time uplink and downlink IQ data samples transferred over eCPRI of the traffic that goes over the air.
- Synchronization Plane (S-Plane): periodically timing and synchronization messages over IEEE 1588 Precision Time Protocol (PTP) to synchronize the O-RU to the network.
- Management Plane (M-Plane): non-real-time management and configuration NETCONF/YANG-based operations.

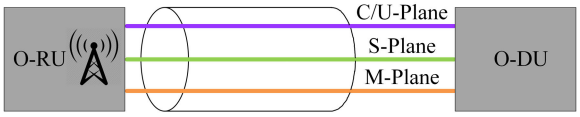


FIGURE 3. O-FH data planes between O-RU and O-DU. CU-Planes are transported over eCPRI, S-Plane over PTP, and M-Plane over NETCONF/YANG-based operations.

B. PERFORMANCE REQUIREMENTS

The full set of performance requirements according to the CUSM-Planes protocols for the transport network has been

TABLE 1. O-FH transport performance requirements for the CUSM-Planes.

Latency Transport Delay						
Latency Class	**Max one-way Frame Delay**	**Max one-way Frame Loss Ratio**	**Use case**			
High25	**25 us**	10^{-7}	Ultra-low latency performance			
High75	**75 us**	10^{-7}	For full NR performance with fiber lengths in 10km range			
High100	**100 us**	10^{-7}	For standard NR performance with fiber lengths in 10km range			
High200	**200 us**	10^{-7}	For installations with fiber lengths in 30km range			
High500	**500 us**	10^{-7}	Large latency installations > 30 km			
Medium	**1 ms**	10^{-7}	U-Plane (slow) C/M-Planes (fast)			
Low	**100 ms**	10^{-6}	C/M-Plane			
Bandwidth Transport Dimension						
Number of sectors	**Frequency Band**	**CBW (MHz)**	**MIMO Layers**	**ABW (MHz)**	**FH BW (MHz)**	**FH Interface**
1	Sub 6 C-band	100	4	400	7.5	**1 x 10Gbps**
	mmWave 39 GHz	400	2	800	14.57	**1 x 25Gbps**
3	Sub 6 C-band	100	4	1200	22.6	**3 x 10Gbps**
			16 (massive MIMO)	4800	90.4	**4 x 25Gbps**
	mmWave 39 GHz	400	4	4800	87.4	**4 x 25Gbps**
Time error budget allocation						
Timing Reference	**Transport network contribution**	**O-RU**	**Air interface target**			
At O-DU For LLS-C1: |TE|≤1.420µs	**|TE| ≤ 140 ns**	Enhanced |TE| ≤ 35 ns	Absolute |TAE| ≤ 1.5us between antennas. Category C: for Time Division Duplex, NR Inter-band carrier aggregation or NR Intra-band non contiguous carrier aggregation			
For LLS-C2: |TE|≤1.325µs	**|TE| ≤ 95 ns**	Regular |TE| ≤ 80 ns				

TE: Time Error, TAE: Air Interface Time Error, LLS-C1: point-to-point fronthaul between O-RU and O-DU, LLS-C2: network of switches fronthaul between O-RU and O-DU.

specified by the O-RAN Alliance in [10]. A summary of these requirements, presented in Table 1, consists of frame loss ratio, frame delay, bandwidth, and synchronization accuracy.

C. TRANSPORT ENCAPSULATION

Ethernet is the selected packet-based technology for the O-FH transport network because of its ubiquitous applications and the ability to mix different types of traffic [11]. The encapsulation of CUSM-Planes packets is illustrated in Fig. 4. The CUS-Planes are encapsulated directly over Ethernet, while the M-Plane is transported over TCP and IP. There are some scenarios where the CU-Planes may be transported over UDP and IP [10].

The clear-text nature of the data planes encapsulated directly over Ethernet makes the O-FH vulnerable to Layer 2 threats. Thus, each data plane requires an independent threat analysis based on its type of content.

III. THREAT ANALYSIS

This section analyzes each type of traffic being transported in the O-FH interface and identifies the different threats and vulnerabilities an attacker can exploit to impact the network. Fig. 5 illustrates the threat scenario under analysis. This study

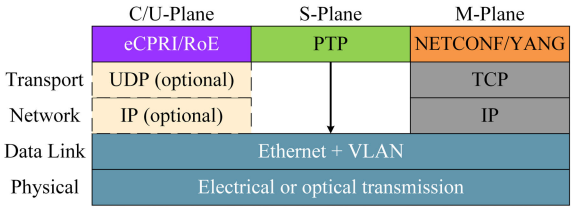


FIGURE 4. O-FH data planes encapsulation over Ethernet. CU-Planes can optionally be transported over UDP and IP for some scenarios. S-Plane PTP messages are directly encapsulated over Ethernet for full-timing support, and the M-Plane messages over TCP and IP.

focuses on the O-FH scenario where the transport of data is encapsulated directly over Ethernet. Hence, the security analysis corresponds to Layer 2 threats on Ethernet ports and frames. This occurs by the premise that an attacker has direct access to the physical port of the O-FH device, with the possibility to add its own device, either to inject its own Ethernet traffic or to perform Man-in-the-Middle attacks. An attacker can either be internal or external. An internal attacker resides within the premises of the O-RU, O-DU, or intermediate switches with access to a trusted segment or with the ability to exploit site vulnerabilities. An external attacker physically intercepts the O-FH interface link from outside the premises. These types of attacks are feasible to occur due to the available physical access to ports in the different components, especially in multi-provider networks where absolute control of the network is limited. Examples of these networks are when the O-RU, O-DU, or intermediate switches are managed by different suppliers, such as Carrier Ethernet service providers.

Layer 2 access gives an attacker the capacity to eavesdrop on all traffic in the O-FH link. This can lead to tampering of the data planes protocols and the appearance of being operational but with intentionally inaccurate information. Without any security mechanism, an attacker can access and identify hosts, types of traffic, and packet contents. This allows him to inject false messages by impersonating a legitimate node, corrupting a legitimate message, and replaying or delaying a legitimate message. All of these threats have different consequences to the RAN depending on the data plane under attack.

A. CONTROL AND USER PLANES

The CU-Planes are based on eCPRI messages [20], [21]. The eCPRI payload data contains a C-Plane or U-Plane packet based on the eCPRI message type. There are multiple types of C-Plane messages, named Section Types, each with different message content depending on what information the C-Plane describes. For this threat analysis, C-Plane Section Type 1 is chosen as it is the one used for most data. A C-Plane message contains multiple sections of control information, also named section descriptions. A U-Plane message contains the user data divided into sections, each corresponding to a specific beam or antenna.

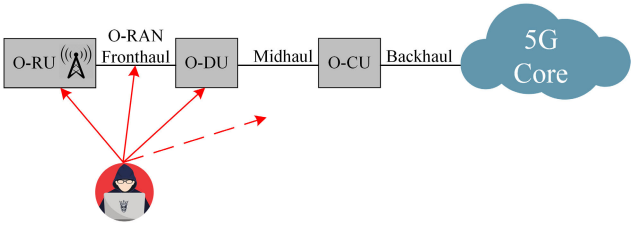


FIGURE 5. O-FH attack scenario; an attacker internal or external with legitimate access to the O-FH interface, or exploiting device vulnerabilities.

When an attacker has Layer 2 access in the O-FH, it can inject its own eCPRI messages or corrupt specific fields of legitimate eCPRI packets. Corruption may occur through the eavesdropping of all traffic and identifying eCPRI messages based on their corresponding Ethertype value of 0xAEFE. An attacker can perform these attacks by targeting different message types and packet fields. The manipulation of these fields has a diverse impact on the O-FH network.

A summary of all the identified threats for the CU-Planes eCPRI traffic is detailed on the left side of Table 2. The overall impact of these threats is a possible degradation or Denial-of-Service in the RAN. Therefore, there is a need for Layer 2 security mechanisms to protect the CU-Planes traffic from the aforementioned threats. These mechanisms must include the following four features: authenticity, confidentiality, integrity, and replay protection. Authenticity ensures that only legitimate O-RUs and O-DUs are communicating between them. Confidentiality keeps the eCPRI header and payload hidden. Integrity identifies if any eCPRI message has been corrupted. Finally, replay protection ensures in-order delivery of eCPRI messages.

B. SYNCHRONIZATION PLANE

The synchronization of O-FH units is based on PTP messages [22], [23]. PTP distributes very precise clock reference to O-DU and O-RU in the O-FH network. There are five types of PTP clock devices:

- Ordinary Clock: device with a single port that acts as a Master or a Slave clock.
- Boundary Clock: device with multiple ports that acts as a Master or a Slave clock.
- End-to-End Transparent Clock: device with multiple ports that acts as a bridge between Master and Slave. It forwards and corrects all PTP messages by adding the bridge residence time into a correction field.
- Peer-to-Peer Transparent Clock: device with multiple ports that acts as a bridge between Master and Slave. It forwards and corrects only Sync and Follow-up messages by adding the bridge residence time plus the peer-to-peer link delay into a correction field in the message.

Master and slave devices are kept synchronized by time-stamps generated both at the transmission and reception of PTP messages. The link delay measurement calculation, illustrated in Fig. 6, can be based on the Delay Request-Response mechanism or the Peer Delay mechanism. Ports on Ordinary or Boundary clocks can use either of these mechanisms. Ports on End-to-End Transparent Clocks are independent of these mechanisms, and ports on Peer-to-Peer Transparent Clocks can only use the Peer Delay mechanism.

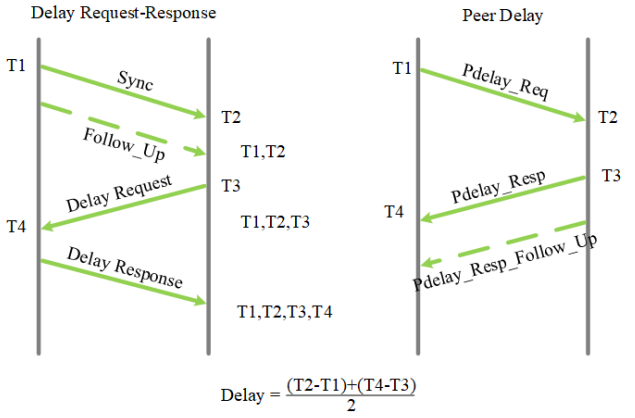


FIGURE 6. PTP delay calculation options; Delay Request-Response mechanism and Peer Delay mechanism.

The O-FH network can vary from a point-to-point topology to a network of switches as illustrated in Fig. 7. These are necessary to address different deployment market needs. With Full Timing Support the synchronization master is located at the O-DU, all Ethernet Switches function as boundary clock or transparent clock, and the O-RU operates as a slave and/or boundary or transparent clock [10].

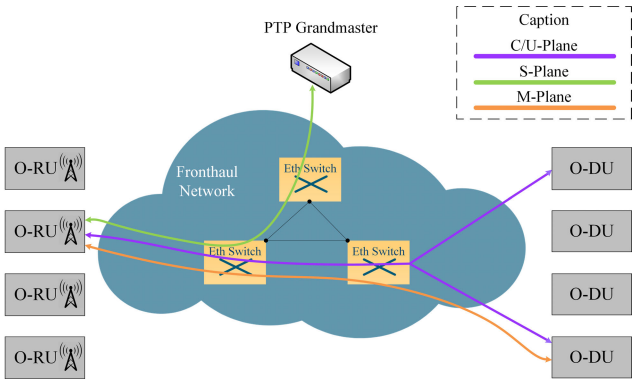


FIGURE 7. O-FH topology; it can vary from a point-to-point O-FH interface between O-RU and O-DU, to a network of switches O-FH interface.

Similar to the CU-Planes, when an attacker has Layer 2 access in the O-FH, it can inject its own PTP messages or eavesdrop on all traffic and identify all PTP messages based on its corresponding Ethertype value of 0 × 88F7. An attacker can perform these attacks by targeting different message types and packet fields. The manipulation of these fields has a diverse impact on the O-FH network.

A summary of all the identified threats for the S-Planes PTP traffic is detailed in Table 2. These threats can result in synchronization mismatching between components of the

TABLE 2. Summary of layer 2 threats in the O-RAN fronthaul.

Protocol	Data Plane	Threat	Packet Field	Impact	Security Requirement	MACsec Security Capabilities			
						Authentication	Confidentiality	Integrity	Replay Protection
eCPRI	Control and User	Eavesdropping	Ethertype, message type	Identification of eCPRI CU-Planes messages for further packet manipulation	Confidentiality		✓		
		Packet manipulation	protocol revision, message type	Packet discard or cause corrupted processing that leads to later discarding	Confidentiality and Integrity		✓	✓	
			payload size	Parser error and potential stall or corruption in the O-DU or O-RU			✓	✓	
			dataDirection	Packet drop			✓	✓	
			filterIndex	Incorrect filter applied causing erroneous processing			✓	✓	
			frameID, subframeID, slotID, startSymbolid	Timing-related content that cause packets to be received outside the reception window and be discarded			✓	✓	
		Packet drop, delay or retransmission	All	Packet is received outside reception window and discarded, leading to degradation on the air interface	Replay and delay protection				Partial
	Control	Packet injection	Section Description fields	Cell becomes unreliable. O-RU incorrectly allocates or unallocates data on the air interface causing it to glitch out for a particular slot duration or persistenly	Authentication	✓			
		Packet manipulation	udCompHdr	Incorrect or unsupported compression applied	Confidentiality and Integrity		✓	✓	
			sectionId, rb, symInc, startPrbc, numPrbc, reMask	Control messages will not be applied to the correct U-Plane data causing glitching on the air interface			✓	✓	
			ef	Parsing issue that can corrupt the O-RU			✓	✓	
			beamId	Incorrect beam is selected leading to poor performance for that particular data allocation			✓	✓	
	User	Packet injection	Section fields	Data become overwritten with the contents of the false packets, causing glitching on the air interface and requiring retransmissions to and from UEs	Authentication	✓			
		Packet manipulation	sectionId	Mismatch of U-Plane and C-Plane messages in DL causing the message to be dropped entirely	Confidentiality and Integrity		✓	✓	
			rb, startPrbu, numPrbu	U-Plane data will not be applied correctly to the air interface causing glitching and drops, or retransmissions at higher layers			✓	✓	
			udCompParam	Incorrect decompression causing errors on the air interface			✓	✓	
			iSample, qSample	Corruption of the air interface may occur requiring retransmissions at higher layers for recovery			✓	✓	
PTP	Synchronization	Packet injection	Announce message	Manipulation of the master election process, causing the switches and O-RU to believe the source is the most eligible candidate to be a clock grandmaster	Authentication	✓			
			Event and General messages	False master clock impersonating an O-DU or a BC port in a switch can distribute false timing information to legitimate slave clocks in BC switches port and O-RU		✓			
				False slave clock impersonating an O-RU or a BC port in a switch can respond to a legitimate master clock in the O-DU or BC switches port with a false clock that results in wrong delay computations		✓			
		Eavesdropping	Ethertype	Identification of PTP messages for further packet manipulation	Confidentiality		✓		
		Packet manipulation	Timing fields	Incorrect values causing wrong delay computations that impacts the synchronization accuracy	Confidentiality and Integrity		✓	✓	
		Packet drop, delay or retransmission	All	Inaccurate timing information in the fronthaul network impacting the synchronization accuracy	Replay and delay protection				Partial

O-FH network that can lead to a degradation or interruption of the clock service and a complete Denial-of-Service of the RAN. Therefore, Layer 2 security mechanisms are indispensable to protect the S-Plane. Similar to the CU-Planes, the security features of authenticity, confidentiality, integrity, and replay protection are required for the S-Plane. Here, authenticity ensures that only legitimate clock devices are communicating between them. Confidentiality keeps the PTP header and payload hidden. Integrity identifies if any PTP message has been corrupted. Finally, delay-replay protection ensures in-order on-time delivery of PTP messages.

C. MANAGEMENT PLANE

The M-Plane does not run directly over Ethernet but uses TCP/IP [24]. TLS is, thus, used to secure M-Plane messages. Nevertheless, targeted attacks at the Ethernet layer can still impact the M-Plane in similar ways to the other data planes discussed above. Ethernet frames can be corrupted, delayed, dropped or replayed and thereby disrupt the management and configuration of O-RAN components. Therefore, the same Layer 2 security mechanisms are recommended for the M-plane to complement the protection implemented with TLS. These measures can add an additional layer of protection against potential TLS vulnerabilities.

D. O-RAN ALLIANCE SECURITY SPECIFICATIONS

The O-RAN Alliance Security Focus Group (SFG) made its first announcement on October 24, 2020, introducing planned SFG activities and a roadmap [25]. In the announcement, the O-RAN Alliance recognized the need to secure important interfaces including the O-FH interface. The new and updated security specifications from October 2022 greatly progress their mission to address the security concerns of the industry. The O-RAN Security Threat Modeling and Remediation Analysis 4.0 notes that there are specific threats and vulnerabilities associated with the O-FH interface [12]. We expanded upon these threats in detail in the previous sections of this paper. The O-RAN Security Requirements Specification 4.0 defines specific requirements for the O-CU and the O-FH [26]. However, the specifications for O-RUs and O-DUs are yet to be defined. Based on the threats and vulnerabilities they identified, the requirements for the O-FH interface specifically addressed the CS-Planes. For the U-Plane, the document states that the U-Plane user data traffic is protected by higher layer security mechanisms in PDCP implemented in the O-CU protecting both C-Plane and U-Plane traffic between the O-CU and UE. However, the document also states that many of the OEMs have not implemented those security measures because of their impact on the user experience. Security of the M-Plane is addressed in the O-RAN Alliance O-RAN Management Plane Specification 10.0 from October 2022 where it is stated that ''An O-RU shall support sFTP based file transfer over SSH and FTPES based file transfer over TLS [24]. For the O-DU, the operator may use SSH, TLS, or both''. Therefore, their requirements have generally focused on authentication and less on confidentiality and integrity concerns. However, based on the threats and vulnerabilities we have identified in the preceding sections, confidentiality and integrity are equally important. This is especially true at the Data Link Layer due to the clear-text nature of the CUS-Planes protocols and its direct encapsulation over Ethernet.

A key protection method being considered for O-FH protection by the O-RAN Alliance is MACsec, a standardized Layer 2 security protocol [27]. However, the current discussion hypothesizes that MACsec would not meet split Option 7-2x requirements for stringent bandwidth, tight latency, and hard absolute and relative time error. Additionally, a full analysis of how MACsec can protect the O-FH is still necessary. The following sections of this paper contribute to the O-RAN SWG work by showing that MACsec can address the highlighted threats and vulnerabilities while respecting the strict performance required in the O-FH.

IV. DATA LINK LAYER SECURITY: MACSEC

MACsec is a Layer 2 security protocol standardized by the IEEE in the 802.1AE standard [13]. It protects communication between components of a Local Area Network (LAN) and, thus, operates on Ethernet frames. Each port of a component that is capable of participating in a MACsec instance comprises both a control plane Key Agreement Entity (KaY) and a data plane Security Entity (SecY). Each KaY implements the MACsec Key Agreement protocol (MKA) [28]. MKA is a companion protocol that discovers or is made aware of the KaYs presence in the other stations attached to the same LAN. It ensures that those stations are mutually authenticated and authorized. Furthermore, the MKA creates and maintains secure relationships between the stations that are used by the SecYs to transmit and receive frames. The SecY operates on a frame-by-frame basis using Advanced Encryption Standard with Galois Counter Mode (AES-GCM) cryptography according to the configuration parameters set by the KaY. AES-GCM provides authenticated encryption and the ability to check the integrity and authentication of additional authenticated data that is sent in the clear. AES-GCM is specified by the NIST in [29], [30].

A. SECURITY RELATIONSHIPS

When devices that support MACsec are added to a LAN, they use the MKA protocol to create a Connectivity Association (CA). The MKA protocol is based on the IEEE 802.1X Extensible Authentication Protocol over LAN (EAPoL) that uses Ethernet-based messaging with Ethertype 0 $\times$ 888E. Before the MKA process starts, all MACsec peers' KaYs possess the same Connectivity Association Name (CAN) and Connectivity Association Key (CAK). When the MKA process starts, all MACsec peers are mutually authenticated using the CAN and the CAK, and a CA association is created. A KaY-SecY can be part of only one CA at any time. Peers present to each other their MACsec capabilities and a long-lived Secure Channel (SC) is created for each station SecY providing unidirectional point-to-multipoint communication. Each SC is identified by a Secure Channel Identifier (SCI) comprising a 48-bit MAC address concatenated with a 16-bit Port Identifier. For key rotation during MACsec operation, the SCs persist through the succession of short-lived Secure Associations (SA). A SA, identified by a two-bit Association Number (AN), consists of a unique Secure Association Key (SAK) and a Packet Number (PN) counter. Throughout the MACsec operation, each frame uses a different PN, and once the PN counter reaches its maximum value, the SC swaps to a new SA. As a result, different SAKs are used in the cryptography process. The MACsec security relationships between O-FH components are illustrated in Fig. 8.

B. SECY OPERATION

MACsec, through the SecY, provides security features of data confidentiality and integrity to Ethernet frames as illustrated in Fig. 9. It adds a header and tail to each frame. The header consists of a Security Tag (SecTAG) as illustrated in Fig. 10. The SecTAG includes a MACsec Ethertype 0 $\times$ 88E5 and frame-specific MACsec parameters, such as the TAG Control Information (TCI). The tail consists of the Integrity Check Value (ICV). When MACsec is enabled, the entire frame is always integrity protected and validated through the ICV,

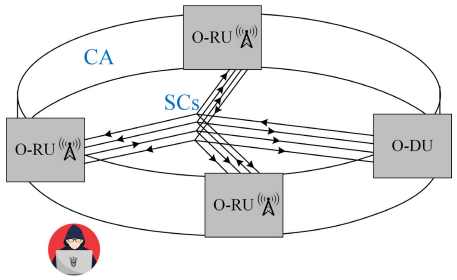


FIGURE 8. O-RAN components secured with MACsec; CA and SCs between O-RUs and O-DU. Each SC persists through the succession of short-lived SAs each with unique SAKs.

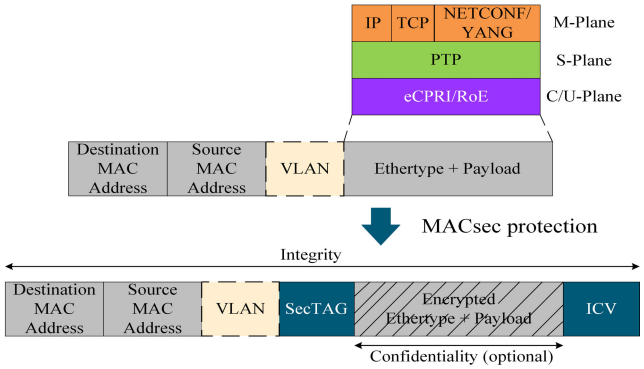


FIGURE 9. MACsec frame format; a SecTAG and an ICV are added to each frame, all frames are integrity protected while confidentiality can be optionally performed to the payload data. The VLAN field, optionally present, can be confidentiality protected as part of the payload, or in-clear before the SecTAG.

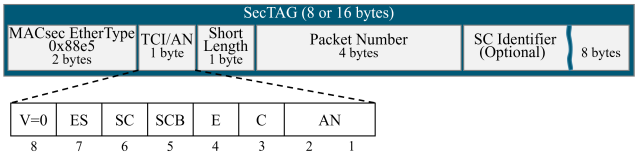


FIGURE 10. MACsec SecTAG providing frame information for MACsec peers reception. TCI/AN provides information on whether encryption is used or not, if the optional SCI is used, and the SA that is in use. The SCI specifies the SC, the SL field is only used for short frames, while the PN can be used to keep track of packet order and detect if packets are missing or delayed.

while the payload can be optionally encrypted. The ICV, unlike the Cyclic Redundancy Check (CRC) done in the MAC layer, is a cryptographic digest function dependent on the data and the SAK. This forces the attacker to know the key to tamper with the data. VLAN-in-clear is an additional feature that optionally keeps the Virtual LAN (VLAN) field without encryption before the SecTAG. This feature is used in cases that require VLAN information to be exposed to support traffic differentiation and end-to-end bridges.

In transmission, the frame is first assigned to the transmit SC and SA which will be used to protect the frame. The TCI is generated based on the configuration used, together with the SA encoded in the two-bit AN. The SecTAG is created using the MACsec Ethertype, TCI, PN, SCI, and the Short Length (SL), which is the number of octets in the frame following the SecTAG if it is less than 48. The AN is used to identify the SAK and the next PN for that SA. The frame is consequently integrity and confidentiality protected with AES-GCM cryptography using the SAK as the input key, and the SCI and PN as the initialization vector. As a result, the payload is encrypted and ICV generated.

In reception, the TCI, AN, SCI, PN, and SL field (if present) are extracted from the SecTAG. The TCI is used to identify the configuration used in the MACsec frame. The AN and SCI are used to assign the frame to a SA, and hence to identify the SAK. The frame is consequently integrity and confidentiality verified with AES-GCM cryptography using the SAK as the input key, and the SCI and PN as the initialization vector. As a result, the payload is unencrypted and the ICV is verified with the one received in the frame. If the integrity of the frame has been preserved, a valid indication and the octets of the unencrypted payload are returned. MACsec has the feature of replay protection, which allows the replay window to be set and ensures in-order delivery of frames. If the received frame is valid, replay protection (if enabled) is applied by checking that the received PN is not less than the lowest acceptable PN for the SA. If the check succeeds, the frame is presented to the MACsec client, and the lowest acceptable PN is updated. The lowest acceptable PN can lag behind the received PN values, providing a window in which out-of-order is tolerated and allowing the reception of frames that have been misordered by the network.

V. MACSEC TO SECURE THE OPEN-RAN FRONTHAUL

MACsec is a persuasive solution to secure the O-FH as it operates on Ethernet frames and, therefore, can provide protection to the CUSM-Planes encapsulated over Ethernet. However, each data plane needs to be independently analyzed to understand to what extend MACsec can protect each plane from all the identified threats and how MACsec impacts any protocol operation or performance requirements.

A. THREAT PROTECTION

When MACsec is enabled on the O-RU and O-DU, both units share the same CAN and CAK, and ports on both ends are initially mutually authenticated by the MKA protocol. A CA with SCs and SAs is created between the O-RU and O-DU with periodical SAKs generations for frame protection and verification. This ensures that only authorized O-RU and O-DU are communicating with each other using the secret keys. As a result, an attacker is not able to inject its own traffic impersonating a node in the network.

Enabling confidentiality to both units keeps all CUSM-Planes encrypted, making each protocol header and payload hidden. As a result, an attacker is not able to identify the type of traffic of the link nor the payload being transported.

Integrity protection is performed over the whole Ethernet frame by the ICV added at the end of the frame using the secret keys. If a CUSM-Plane frame is corrupted while

in-motion during the ICV verification there will be an ICV mismatch and the frame will be discarded. As a result, if an attacker changes the values of legitimate CUSM-Plane messages they will be identified and discarded before their delivery to the MACsec client.

Depending on the O-FH network operation, a replay window can be set to 0 or to a very small value in the O-RU and O-DU to ensure in-order delivery of frames. As a result, if an attacker performs a replay attack by recording a legitimate CUSM-Plane message and replaying the same message without modification multiple times at a later time, those frames will be identified and discarded before their delivery to the MACsec client.

With the use of the replay protection feature, MACsec with some limitations could also identify if an attacker has delayed a CUSM-Plane message. This can be done only for the cases where the attacker delays a single frame and lets the rest of the frames pass. In this case, the delayed frame will arrive disordered and the replay window will discard it. MACsec is not able to detect the cases where the attacker delays a desired frame together with the following frames, as they will all appear to arrive in the expected order. Additionally, MACsec is limited if an attacker drops specific frames or all the traffic in the O-FH.

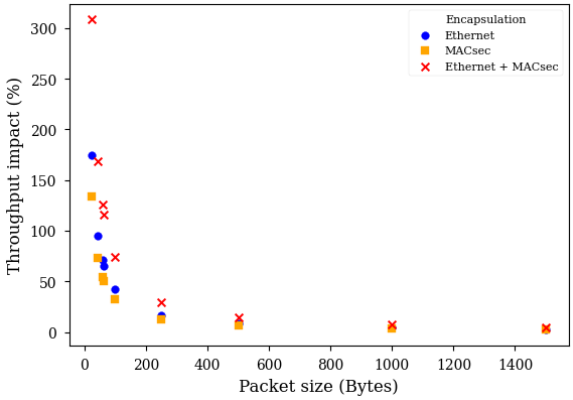
The mapping of MACsec features with the identified threats in the O-FH network is illustrated on the right side of Table 2. As can be seen, the O-RU and O-DU can be protected using MACsec from most of the identified threats, with the exception only of drop and delay attacks that MACsec is partially able to detect. These types of threats can be protected against with network architecture approaches that use redundancy links and protocols such as Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) [31], [32].

B. IMPLEMENTATION CHALLENGES

MACsec offers a compelling solution to secure the O-FH. However, implementation challenges exist that need to be addressed.

1) O-FH LINE RATE

In terms of bandwidth, MACsec introduces an overhead to each frame due to the added SecTAG of 16 Bytes and ICV of 16 Bytes. Fig. 11 illustrates the impact of Ethernet encapsulation and MACsec overhead for different frame sizes. As can be seen, frame size is inversely proportional to the line rate impact. For smaller payload sizes, there will be a higher impact caused by the overhead, while for bigger sizes the impact is minimal. The MACsec overhead to PTP frames will decrease the line rate by 50.00% - 72.73%, depending on the PTP message size, e.g. sync and follow-up messages are 44 Bytes and announce messages are 64 Bytes. The MACsec overhead to C-Plane frames will decrease the line rate by 2.13% - 133.33%, depending on the C-Plane message size, e.g. type 1 and with 1 section is 24 Bytes while multiple sections can be up to 1500 Bytes that is supported payload in a standard Ethernet frame. The MACsec overhead to U-Plane frames will decrease the line rate by 2.13% - 54.24%, depending on the U-Plane message size, e.g. with 1 section and 1 PRB per section is 59 Bytes, while with multiple sections and PRBs, it can be up to 1500 Bytes that is supported payload in a standard Ethernet frame.



Ethernet encapsulation: DMAC(6B), SMAC(6B), ETYPE(2B), VLAN(4B), FCS(4B), PRE(8B), and IPG(12B).
MACsec header and tail: SecTAG(16B) and ICV(16B).

FIGURE 11. Ethernet and MACsec overhead impact on throughput; frame size is inversely proportional to the line rate impact, for smaller payload sizes there will be a higher impact caused by the overhead, while for bigger sizes the impact is minimal.

2) S-PLANE PTP PACKETS PROTECTION

For precise PTP timestamping, the timestamp must occur at the physical layer close to the point where the PTP message is leaving the port. The Time-Stamping Unit (TSU) timestamps PTP messages that are identified by their corresponding Ethertype. When MACsec is used to protect PTP messages, there are timestamping design considerations for transmission and reception that need to be taken into account.

In transmission, for the case of one-step PTP clock implementation, the timestamp would need to be available at the MACsec layer for PTP messages protection using MACsec. This could be possible if the TSU generating the timestamp is placed before the MACsec layer and the latency from that point to the physical layer is added as illustrated in Fig. 12. Therefore, a fixed delay is required between the MACsec layer and the physical layer where PTP timestamping is needed for time precision.

For two-step PTP clock implementation, this consideration is not required as the timestamp is sent in the consecutive follow-up message. Thus, the timestamping can be kept at the physical layer, and the timestamp is available for the MACsec layer. However, this can be possible only for the case when PTP messages are integrity protected without confidentiality because the PTP Ethertype would be visible for the TSU to identify that it is a PTP message and would be able to timestamp it. If the PTP message is confidentiality protected,

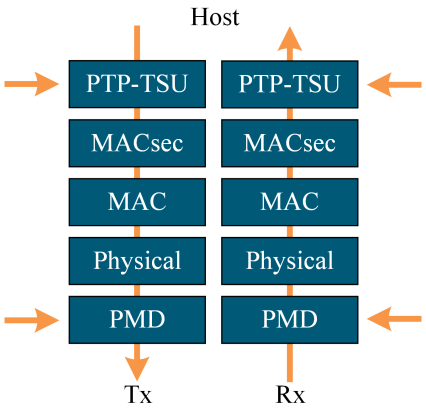


FIGURE 12. PTP TSU positioning; ideally closer to the physical layer for time accuracy, however for PTP messages protection using MACsec the TSU needs to be placed before the MACsec layer.

the TSU would not be able to identify the encrypted PTP message nor timestamp it.

In reception, similar considerations occur. If a PTP message is received with integrity protection without confidentiality, the timestamping can be kept at the physical layer with the TSU being able to identify and timestamp the visible PTP message. If a PTP message is received with confidentiality protection, the TSU needs to be placed before the MACsec layer when the PTP message is unencrypted, and, again, a fixed delay would be required between the physical layer and the MACsec layer for time precision.

As a result, with a TSU kept at the physical layer for time accuracy, only a two-step mode would be possible and PTP with messages could be MACsec protected without confidentiality. When a one-step mode or two-step mode with confidentiality is desired, the TSU needs to be placed before MACsec with a fixed delay in the MACsec and following components to the physical layer.

The O-FH can vary from a point-to-point scenario to a network of switches that may act as boundary clock or transparent clock. For the network of switches topology, MACsec can be implemented end-to-end between O-RU and O-DU, or hop-by-hop including each intermediate switch. For the end-to-end option, all Ethernet frames are integrity and confidentiality protected at the O-RU and O-DU, hence, the intermediate switches could only act as forwarding nodes without the capacity to access and make changes to the frame payload. This is a limitation for O-FH switches as they are required to timestamp and correct PTP messages. Therefore, if MACsec is used to protect PTP messages, the hop-by-hop option is required with each switch having MACsec capabilities. However, this potentially adds more latency in every hop, and adversary impacts to the end-to-end budget.

3) TRAFFIC DIFFERENTIATION

For the network of switches topology at the O-FH interface, traffic from each of the CUSM-Planes may need to be sent separately to different nodes from a single port, as shown Fig. 13. This results in multiple groups of nodes divided per data plane. For example, a group of nodes can be between an O-RU and two O-DUs based on C-Plane data, and another group between the same O-RU and a PTP grandmaster based on S-Plane data. Each group needs to be secured independently for security robustness including the need for different sets of secret keys. Thus, there is a need to support multiple security domains between a port and different destinations based on the CUSM-Planes type of traffic. If MACsec is used to protect the O-FH, a single port in O-RU, O-DU, and intermediate switches need to support multiple CAs for traffic differentiation, i.e. multiple sets of KaY-SecY per port.

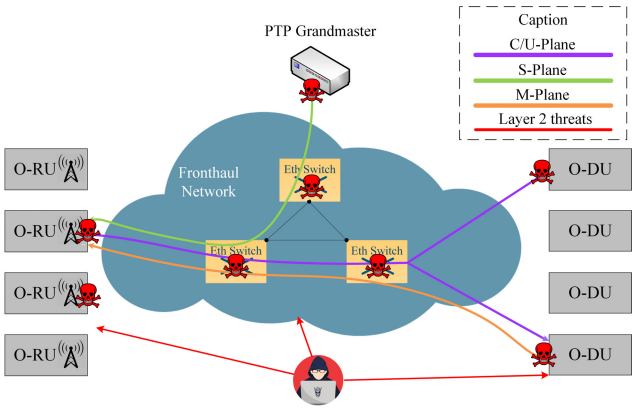


FIGURE 13. O-FH network of switches topology; traffic from each of the CUSM-Planes may need to be sent separately to different nodes from a single port. Multiple CAs per port for traffic differentiation are required to protect against threats.

VI. MACSEC HARDWARE ARCHITECTURE FOR THE OPEN-RAN FRONTHAUL

The O-RAN specifications are still under definition and will offer openness to innovation in the O-FH. This innovation requires O-RAN components to have flexibility in quickly changing or adding features for testing and upgrading functionalities. This becomes a challenge in components that are implemented in hardware (HW) chips for high-performance data operation due to the much longer development time needed compared to software (SW). Application-Specific Integrated Circuit (ASIC) chips, especially, require an extended development time because they are manufactured to execute a specific set of functions [33]. In contrast, FPGAs are pre-produced chips that can be reprogrammed after being manufactured. This offers flexibility to HW implementations that require faster time-to-market [34]. The programmability of FPGAs makes them appealing for the implementation of the continuously changing high-performance functionalities of O-FH components.

As MACsec operates at the Ethernet port level, it is constrained by the strict O-FH transport performance requirements of high throughput, low latency, and accurate time stamping. Because of this, MACsec needs to be implemented

in dedicated FPGA or ASIC, contrary to SW implementations running on general purpose Central Processing Units (CPUs) [35].

In this section, we propose a MACsec HW-based architecture for the O-FH that targets FPGA and ASIC implementations. We begin by defining a single SecY fixed-latency pipelined HW architecture compliant with IEEE 802.1AE standard for a point-to-point O-FH topology. We then analyze the requirements to expand this architecture to support multiple SecYs in the same port for traffic differentiation of CUSM-Planes using independent CAs for the network of switches O-FH topology. Following, we propose a multiple SecY architecture with the addition of a Management Domain implementing virtual SecYs. Finally, we propose a PTP buffer system that complements the previous architecture to support full PTP protection and time accuracy.

A. SINGLE SECY ARCHITECTURE

As defined by the MACsec IEEE 802.1AE standard, a SecY is the entity that operates the MACsec data processing on a network port and it can only be part of one CA at any time. The SecY operation is on a frame-by-frame basis and divided into two parts; transmit and receive. The transmit part protects the frame with encryption and integrity using the AES-GCM cryptography functions and creates and appends the SecTAG and the ICV to the frame. The receiving part verifies the frame with decryption and integrity check using the AES-GCM cryptography functions and strips the SecTAG and the ICV from the frame.

The proposed Single SecY architecture is presented in Fig. 14. It illustrates a highly abstracted hierarchy implementing Single SecY functionalities. The processing flow is divided into transmission (Tx) and reception (Rx), with the top-level architecture partitioned into three functional domains: Register Access Domain, Tx Domain, and Rx Domain.

- Register Access Domain, performing configuration and status register write and read operations.
- Tx Domain, performing MACsec transmission data plane protection functions.
- Rx Domain, performing MACsec reception data plane verification functions.

1) REGISTER ACCESS DOMAIN

The Register Access Domain maintains all SecY control information according to the standard, which includes transmitting and receiving SCs and SAs. These are stored in 32 bit configuration and status registers that are fully programmable and accessed through an AXI4-Lite Register Access Interface [36]. It runs under its 100 MHz CPU clock.

2) TX DOMAIN

The main purpose of the Tx Domain is to perform data protection of all Ethernet frames that are transmitted from the MACsec Client using input and output AXI-Stream 64 bit data interfaces [37]. It runs under a minimum Tx clock of 156.25 MHz for 10 Gbps and 390.625 MHz for 25 Gbps. At a high level, in Tx every Ethernet frame is processed as follows:

- Packet Parsing: this block extracts header and payload information of each Ethernet frame (MAC address, VLAN, Ethertype, and payload).
- Packet Classification: this block determines how to process each frame, according to the extracted header information and SecY configuration registers, and assigns a class type (bypass, drop, or protect).
- Packet Protection: this block performs frame protection to Ethernet frames with Protect class type using the Tx AES-GCM cipher suite with the corresponding security configuration parameters. The ICV is generated and the payload is encrypted if confidentiality is enabled.
- Packet Assembling: this block assembles Ethernet frames depending on the class type (Bypass, frame without alteration; Drop, the frame is assembled with error flag in Tuser signal at the end of the frame; Protect, the frame is assembled with MACsec SecTAG and ICV added and changed plaintext to ciphertext if confidentiality is enabled).

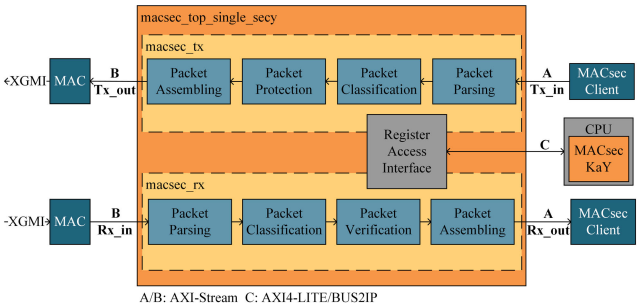


FIGURE 14. Single SecY top-level architecture partitioned into three functional domains: Register Access Domain, Tx Domain, and Rx Domain.

3) RX DOMAIN

The main purpose of the Rx Domain is to perform data verification of all Ethernet frames that are received from the MAC using input and output AXI-Stream 64 bit data interfaces [37]. It runs under a minimum Rx clock of 156.25 MHz for 10 Gbps and 390.625 MHz for 25 Gbps. At a high level, in Rx every Ethernet frame is processed as follows:

- Packet Parsing: this block extracts header and payload information of each Ethernet frame (MAC address, VLAN, Ethertype, SecTAG, payload, and ICV).
- Packet Classification: this block determines how to process each frame according to the extracted header information and SecY configuration registers and assigns a class type (bypass, drop, or verify).
- Packet Verification: this block performs frame verification to Ethernet frames with Verify class type using the Rx AES-GCM cipher suite with the corresponding security configuration parameters. The frame integrity is checked using the ICV and the payload is decrypted if confidentiality is enabled.

- Packet Assembling: this block assembles Ethernet frames depending on the class type (Bypass, frame without alteration; Drop, the frame is assembled with error flag in Tuser signal at the end of the frame; Verify, the frame is assembled with stripped MACsec SecTAG and ICV, and changed ciphertext to plaintext if confidentiality is enabled).

This architecture is, therefore, suitable for a point-to-point scenario as it consists of a single SecY that is required to form a single CA between two O-FH nodes.

B. MULTIPLE SECY ARCHITECTURE

As was presented in Section V-B, there is a need to support multiple SecYs per port for the network of switches O-FH topology. To support multiple SecYs in the same port for traffic differentiation of CUSM-Planes using independent CAs, one option is to have four instances of the Single SecY architecture, each serving an independent data plane. However, this option is very expensive as it increases by four the whole resource utilization, especially the packet protection and verification blocks implementing the AES-GCM cryptography operations.

We identified that it is possible to have multiple SecYs while keeping a single instance of the Tx and Rx processing flow, including the AES-GCM cryptography operations. This can be done by taking advantage of the frame-by-frame transmission and reception operation in the Ethernet port. We propose to abstract the SecY control parameters from Tx and Rx Domains to a new Management Domain and only keep frame data processing operations in Tx and Rx domains. The Management Domain can then store and maintain control information of multiple SecYs and interface with Tx and Rx Domains, instructing them to perform data processing using specific configuration parameters according to a desired SecY. As a result, a configurable number of virtual SecYs can be instantiated in the Management Domain, all sharing the same Tx and Rx data processing flow. The proposed Multiple SecY architecture is presented in Fig. 15.

As there is a single physical transmission interface, CUSM-Planes need to be mapped to its corresponding SecY. To achieve this, we introduce in the Management Domain a traffic mapping table at the input interface. Here, rules can be configured to govern which SecY is used for a given transmit frame and to bypass a specific frame if necessary, as illustrated in Fig. 16. The rules can be based on MAC Address, VLAN ID, or Ethertype, offering flexibility depending on the O-FH topology. For example, the rules can be used in the following three O-FH scenarios:

- If a specific type of traffic is sent between concrete physical nodes in the O-FH network, MAC addresses can be used to associate traffic to a specific SecY.
- Different VLAN IDs can be used for each CUSM-Plane to differentiate them, thus, four rules based on VLAN IDs can be used to associate each data plane to a SecY.
- Each CUSM-Plane uses a specific protocol, hence, the corresponding protocol Ethertype can be used as a rule criterion to associate each data plane to a specific SecY.

The processing flow of the Management Domain is as follows:

- Packet Assignment: this block uses the parsed header information in Tx and Rx Domains to check a match in the traffic mapping table to either bypass MACsec or to assign the frame to a SecY.
- SecY Access: this block accesses all control information associated with the selected SecY, determines how the frame should be processed, and updates its state.
- Packet Instruction: this block instructs Tx and Rx Domains how to continue processing the frame and provides the corresponding configuration parameters.

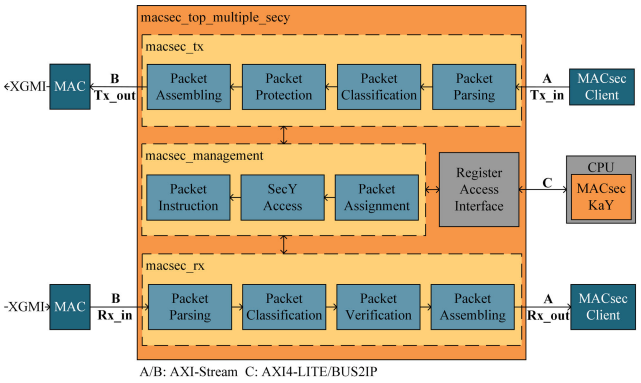


FIGURE 15. Multiple SecY top-level architecture partitioned into four functional domains: Register Access Domain, Tx Domain, Rx Domain, and Management Domain.

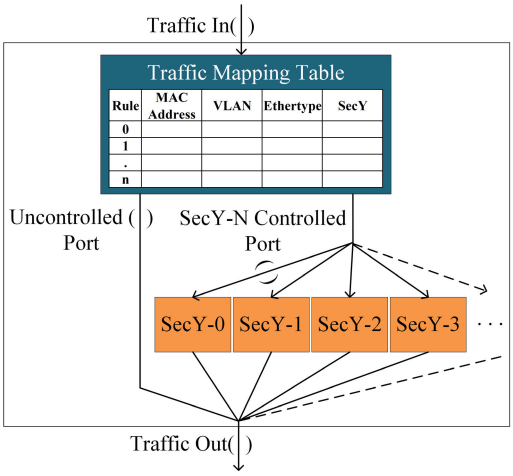


FIGURE 16. Traffic mapping to multiple SecYs with rules based on MAC Address, VLAN ID, or Ethertype, offering flexibility depending on the O-FH topology.

This architecture avoids the need of increasing by four the whole resource utilization by having four instances of the Single SecY architecture for each data plane. Instead, it only increases by four the SecY control information handled by

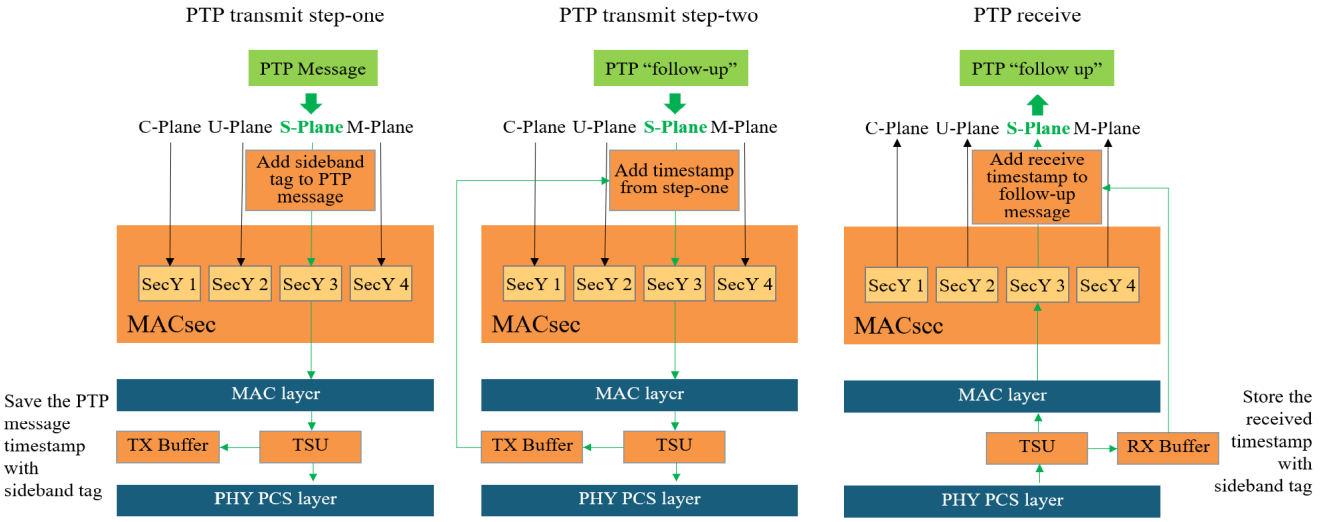


FIGURE 17. Complement Secure PTP top-level architecture for two-step PTP clock implementation with a TSU at the physical layer for time accuracy.

the Management Domain. Furthermore, the number of virtual SecYs is fully configurable making it flexible depending on the use case scenario. Therefore, this architecture provides the support of multiple CAs in a single port for traffic differentiation targeting different destinations in a network of switches O-FH topology.

C. COMPLEMENT SECURE PTP ARCHITECTURE

To address the PTP challenges described in Section V-B2, we propose a Complement Secure PTP Architecture for two-step PTP clock implementation with a TSU at the physical layer for time accuracy. The architecture is presented in Fig. 17.

For transmission, a sideband tag is added to the PTP sync message before MACsec layer. The PTP message is then MACsec protected with confidentiality and integrity using its independent SecY. At the physical layer, the TSU identifies the PTP message by the sideband tag instead of using the Ethertype as this will be encrypted. It timestamps the PTP message and stores the PTP message-specific sideband tag with the timestamp in a Transmit Buffer (TX Buffer) that is used to prepare the PTP follow-up message, which can then be MACsec protected with confidentiality and integrity.

During the reception, because all MACsec frames arrive encrypted and the TSU is not able to identify PTP messages, it timestamps all protected frames, assigns a tag to each timestamp, and the tag is added as a sideband to each frame. The tags and timestamp are stored in a Receive Buffer (RX buffer) and, after MACsec verification, the unencrypted PTP message is mapped to its corresponding timestamp with the use of the sideband tag.

As a result, S-Plane PTP messages can be MACsec protected and verified with confidentiality and integrity while keeping accurate timestamping at the physical layer where the message leaves and arrives at the port.

VII. HARDWARE SCALABILITY AND PERFORMANCE EVALUATION

The architectures proposed in this paper were implemented as Register Transfer Level (RTL) Silicon Intellectual Property (IP) Cores, whose source code was written in SystemVerilog Hardware Description Language (HDL) [38]. This section aims to explore the feasibility boundaries of the architectures implemented in FPGA devices.

At a high level, an FPGA device consists of Logic Blocks, Programmable Interconnect, and I/O pins [38]. In Xilinx devices, the main resources used to implement circuits are Configurable Logic Blocks (CLBs). These blocks contain Look-Up Tables (LUTs) and CLB Registers. LUTs are n-input truth tables for combinatorial logic, and CLB Registers are storage elements for sequential logic. The CLBs also contain carry logic for arithmetic operations (CARRY8) and Multiplexers (FnMUX) to maximize resource utilization [39]. Some FPGAs also contain specialized blocks with non-programmable modules performing a specific function, e.g. Block Random Access Memories (BRAM) and Digital Signal Processing (DSP) blocks.

The results presented in this section are the output of the logic synthesis process executed by Xilinx Vivado 2020.2 SW. Specifically, the timing reports and resource utilization reports [40].

The synthesis runs were executed under three explanatory variables:

- Compile time parameters with variable settings for number of SecYs (1, 2, 3, 4, 8, 12, and 16) and number of Peers (1, 8, 16, 32, and 64).
- Target operating frequency of 156.25 MHz for 10 Gbps and 390.625 MHz for 25 Gbps.
- Target devices of different Xilinx FPGA base architectures (7 Series, Ultrascale, and Ultrascale+) and families (Virtex and Zynq) [41].

The response variables from the logic synthesis process that were analyzed consist of:

- Fmax, Maximum operational frequency.
- Total LUTs, Number of Look-up Tables used for implementation.
- Total FFs, Number of Flip-Flops used for implementation.
- RAMB36, 36 kbit Block RAM.
- RAMB18, 18 kbit Block RAM.

A. SINGLE SECY ARCHITECTURE

The resource utilization for the Single SecY Architecture targeting different devices is illustrated in Fig. 18. As shown, the resource utilization increases linearly with an increasing number of SecYs and peers. This was expected as the Single SecY Architecture needs to be instantiated for the number of SecYs and peers required. With this architecture, one to eight SecYs can be supported according to the maximum available resources in the different devices. Devices using UltraScale+ architecture provide higher resources compared to 7 Series architectures. This is without taking into account additional IP blocks that would need to fit in the FPGA as part of the communication subsystem, e.g. Ethernet Switch, MAC, and PCS. For example, a MAC/PCS IP in a Zynq Ultrascale+ device consumes 13,000 LUTs, giving a MACsec impact of 12,400% with a 16 SecY configuration. Thus, the Single SecY Architecture is only feasible for point-to-point O-FH topologies where a minimum number of CAs is required.

Fig. 19 illustrates the Fmax for different devices and supported number of SecYs and peers. As can be seen, the number of SecYs and Peers does not influence the Fmax. The Fmax remains constant when the number of SecYs and peers increase. However, it was observed that the limiting critical path was in the packet classification block due to the combinatorial logic required for processing each frame and assigning class types, which can be improved with further design optimizations. Devices using UltraScale+ architecture provide higher Fmax compared to 7 Series architectures. The target frequency of 390.625 MHz required for 25 Gbps was achieved by UltraScale+ devices. However, the target frequency of 156.25 MHz required for 10 Gbps was reached by all devices.

B. MULTIPLE SECY ARCHITECTURE

The resource utilization for the Multiple SecY Architecture targeting different devices is illustrated in Fig. 20. It can be seen that the resource utilization is significantly reduced compared to the Single SecY Architecture. This was achieved by the addition of a Management Domain that stores and maintains only the control information of the number of SecYs defined, all sharing the same Tx and Rx data processing flow. This architecture more than doubles the number of SecYs that can be supported compared to the Single SecY Architecture. Over 16 SecYs can be supported according to the maximum available resources in the different devices. Devices using UltraScale+ architecture provide higher resources compared

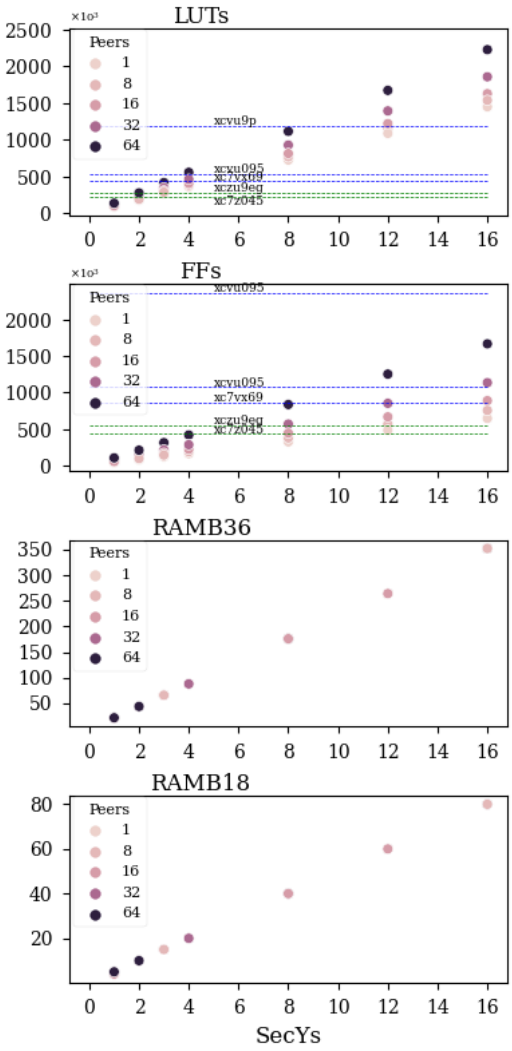


FIGURE 18. Resource utilization of the Single SecY Architecture. One to eight SecYs can be supported on UltraScale+ devices which provide higher resources compared to 7 Series architectures.

to 7 Series architectures. Compared to the MAC IP utilization, this architecture with a 16 SecY configuration gives a MACsec impact of 6,100%, offering a decrease in utilization of more than half compared to the Single SecY architecture. As a result of the reduced resource utilization, additional IP blocks as part of the communication subsystem can be included. This makes the architecture feasible for O-FH components that require multiple CAs for traffic differentiation, especially for the network of switches O-FH topology.

Fig. 21 illustrates the Fmax for different devices and supported number of SecYs and peers. Similar to the Single SecY Architecture, the number of SecYs and Peers does not influence the Fmax, meaning that the limiting critical path remains in the packet classification block. The Fmax remains constant when the number of SecYs and peers increase. Devices using UltraScale+ architecture provide higher Fmax compared to 7 Series architectures. The

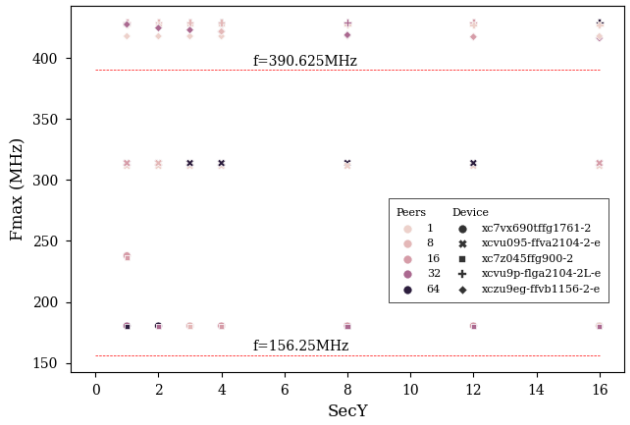


FIGURE 19. Fmax of the Single SecY Architecture. Fmax remains constant when the number of SecYs and peers increase with higher Fmax in UltraScale+ devices compared to 7 Series architectures.

target frequency of 390.625 MHz required for 25 Gbps was achieved by UltraScale+ devices. However, the target frequency of 156.25 MHz required for 10 Gbps was reached by all devices.

VIII. EXPERIMENTAL PERFORMANCE EVALUATION

To analyze the impact of the proposed MACsec HW architecture on the link performance, we have deployed two experimental setups with Xilinx ZCU102 development boards. The first setup is used to evaluate the CPU gain of the MACsec HW offloading. The second setup is used to measure the throughput and latency provided by the MACsec HW architecture. The first setup is illustrated in Fig. 22. The Zynq chip on the ZCU102 consists of a Programmable Logic (PL), which is the FPGA fabric where the digital design is implemented, and a Processor System (PS) running the Linux Operating System on a Quad-core ARM Cortex-A53 processor [42]. On the two Xilinx boards, the PL implements a 10G Ethernet port transport subsystem that includes DMA, MACsec, MAC, and PCS IPs. In the PS, the Linux kernel network stack implements an Ethernet network device driver that enables the transmission and reception of Ethernet frames to and from the PL 10G Ethernet port transport subsystem. The MACsec IP implements the proposed Multiple SecY Architecture with a 156.25 MHz clock for 10G which is supported by the Xilinx ZCU102 board.

With the two boards connected to each other via 10G Small Form-factor Pluggables (SFPs) and fiber port to port, it is possible to send traffic between them and determine the throughput offered to Ethernet frames of different sizes. The traffic is protected first using the SW-based MACsec Linux implementation deployed in the Linux kernel [43], and then using the MACsec HW-based implementation proposed in this paper.

The second setup is illustrated in Fig. 23. It emulates a 10G O-FH interface between O-RU and O-DU with CUSM-Planes traffic. The setup consists of two O-FH interfaces; one

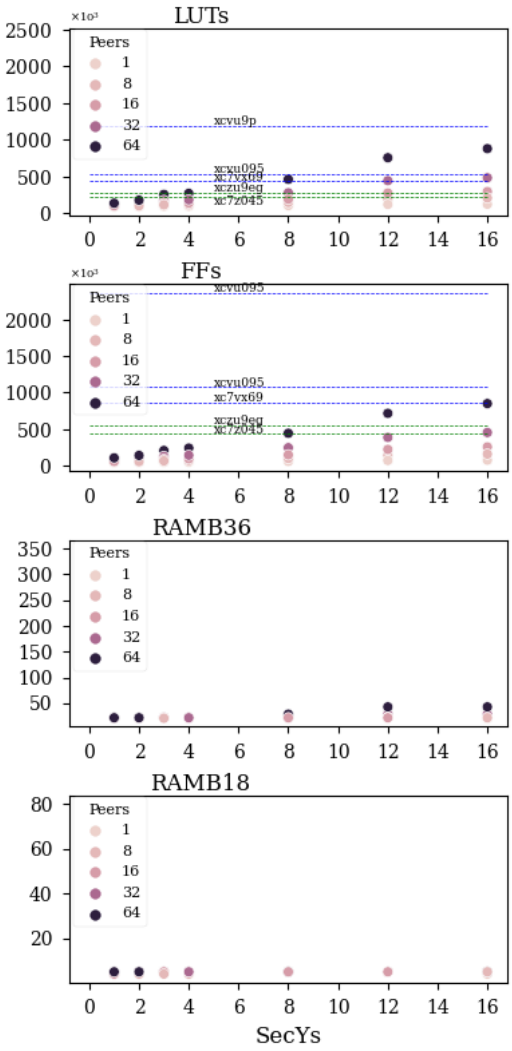


FIGURE 20. Resource utilization of the Multiple SecY Architecture. More than 16 SecYs can be supported on UltraScale+ devices which provide higher resources compared to 7 Series architectures.

with a point-to-point connection between O-RU and O-DU, and the other interface with one Xilinx board in the middle implementing two 10G Ethernet port transport subsystems for MACsec protection. In both interfaces the throughput and latency are measured for different CUSM-Planes frame sizes evaluating the performance provided by the MACsec IP.

The ZCU102 development board contains features to measure voltage and current for various components of the board [44]. These features are used to analyze the dynamic power consumption of the proposed MACsec architecture.

A. CPU OFFLOAD

Fig. 24 illustrates the CPU gain by offloading MACsec to dedicated HW in Test setup 1. Results show that the throughput achieved with the HW-based MACsec implementation increases up to 42.38% compared to the SW-based implementation, especially with larger frame sizes. The limitation of

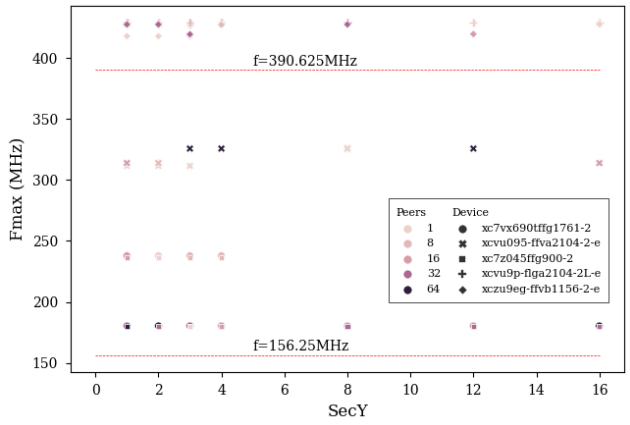


FIGURE 21. Fmax of the Multiple SecY Architecture. Fmax remains constant when the number of SecYs and peers increase with higher Fmax in UltraScale+ devices compared to 7 Series architectures.

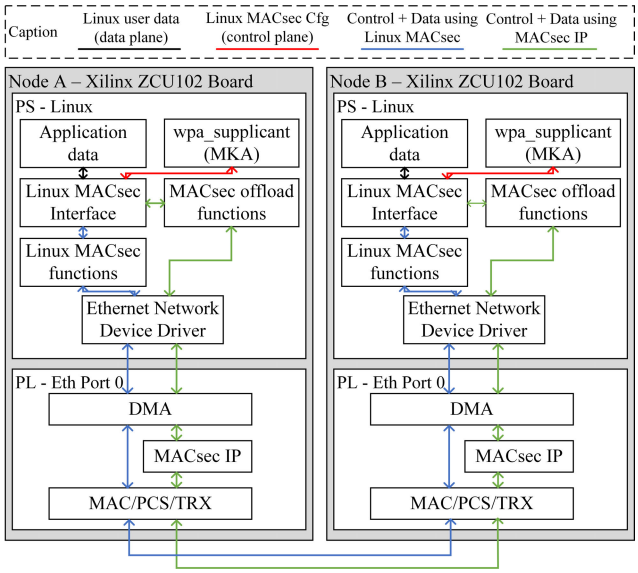


FIGURE 22. Test setup 1: Two Xilinx ZCU102 development boards with PL implementing the digital design, and a PS running Linux Operating System.

the SW-based implementation is due to the CPU processing workload for MACsec. Acceleration mechanisms, such as Data Plane Development Kit (DPDK), can be used to improve the CPU processing workload. In this scenario, DPDK will accelerate the CPU processing for packet injection and MACsec processing, and thus scale the achieved throughput to both, the SW and HW-based MACsec implementations. As a result, the maximum achieved throughput of 430 Mbps will increase. However, the relative offload difference between SW and HW-based implementations will remain at 42.38%, since the encryption processing by the CPU will also scale proportionally.

B. THROUGHPUT AND LATENCY

Fig. 25 illustrates the O-FH throughput in Test setup 2 with and without the MACsec IP. It can be seen that the throughput

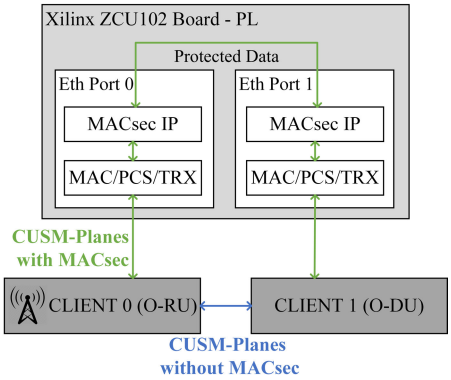


FIGURE 23. Test setup 2: O-FH interface emulation. Point-to-point connection between O-RU and O-DU with Xilinx ZCU102 board for MACsec protection.

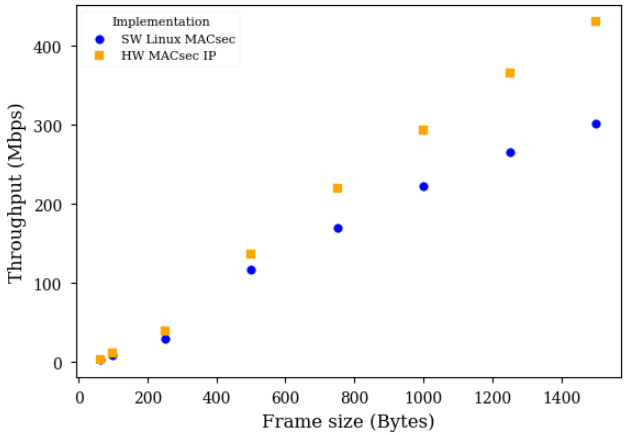


FIGURE 24. CPU gain by offloading MACsec to dedicated HW. Throughput increases up to 42.38% in larger frames with the MACsec IP.

is proportional to the frame size with an exponential increase. This is due to the impact of the overhead introduced by the network protocols encapsulation as described in Section V-B1. Without MACsec the maximum throughput was 9.25 Gbps. When the MACsec IP was used for O-FH protection the maximum throughput was 8.25 Gbps. Hence, the proposed MACsec architecture follows the O-FH line rate with a maximum cost of 10% reduction. Based on the throughput requirements defined in Table 1, this cost can be added to dimension the required O-FH bandwidth. Furthermore, the proposed MACsec architecture can be integrated into 10 Gbps and 25 Gbps interfaces as it supports target frequencies of 156.25 MHz and 390.625 MHz.

Fig. 26 illustrates the latency of the proposed MACsec IP for different frame sizes. The number of clock cycles (cc) was measured for the following reference points:

- sof_i to sof_o: from the first 64b input word start of frame (sof_i) to the first 64b output word start of frame (sof_o).
- eof_i to eof_o: from the last 64b input word end of frame (eof_i) to the last 64b output word end of frame (eof_o).

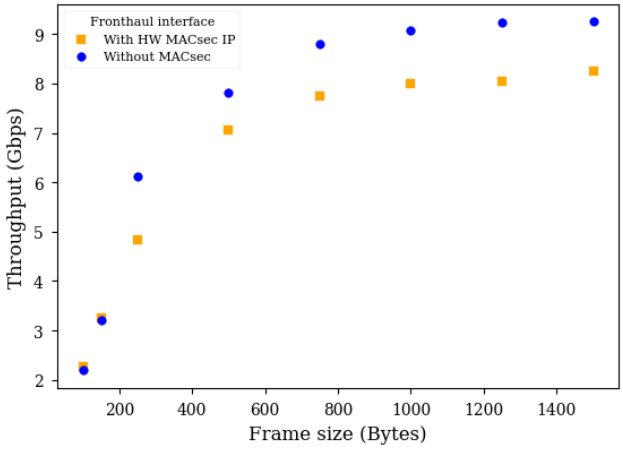


FIGURE 25. O-FH throughput with and without the MACsec IP. The throughput is proportional to the frame size with a maximum value of 8.25 Gbps provided by MACsec.

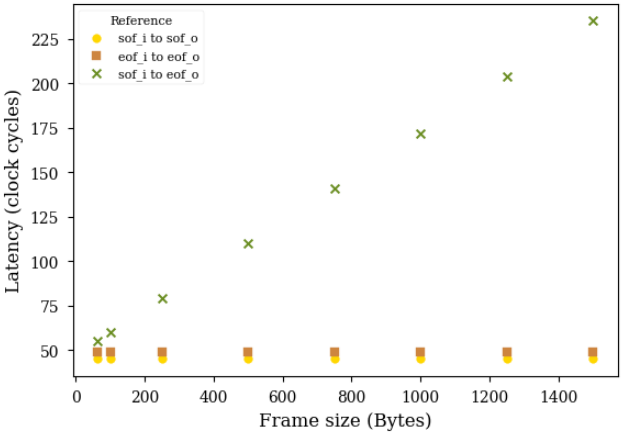


FIGURE 26. Latency of the MACsec IP for different frame sizes. It has a fixed latency from sof_i to sof_o and from eof_i to eof_o supporting the placement of the TSU before the MACsec layer for one-step PTP clock implementation.

- sof_i to eof_o: from the first 64b input word start of frame (sof_i) to the last 64b output word end of frame (eof_o).

It can be seen that the MACsec IP has a fixed latency of 45 cc from sof_i to sof_o and 49 cc from eof_i to eof_o. The number of clock cycles increases linearly from sof_i to eof_o depending on the frame size. This fixed latency results from a pipelined MACsec implementation that also keeps a constant throughput. The 45 cc at a target frequency of 156.25 MHz for 10 Gbps corresponds to a delay of 0.288 us. The strictest latency requirement from Table 1 defines a maximum one-way frame delay of 25 us for Ultra-low latency use cases. Thus, the delay contribution of the proposed MACsec architecture to the O-FH interface is minimal.

The Complement Secure PTP Architecture proposed in this paper keeps the TSU placed at the physical layer. This means that by design the MACsec IP doesn't have any impact on the time-stamping done at a lower layer. Therefore, the proposed MACsec architecture respects the O-FH time requirements defined in Table 1. Furthermore, the fact that the MACsec IP provides a fixed latency indicates that it also supports the placement of the TSU before the MACsec layer for one-step PTP clock implementation, if required.

C. POWER CONSUMPTION

Fig. 27 illustrates the measured power in the PL when frames are protected using the SW-based MACsec Linux, and when using the proposed HW-based MACsec IP. It can be seen that the power contribution of the MACsec IP to the design is 3 mW. Furthermore, the power in the PL remains constant for all frame sizes in both cases. Therefore, the addition of MACsec to the 10G Ethernet port transport subsystem in this implementation increases the power consumption by 150%. It can be observed that the impact of MACsec on power consumption doesn't follow the same behavior as the resource utilization impact of 6,100%.

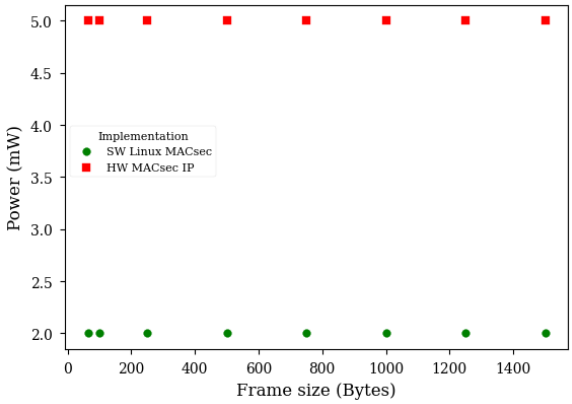


FIGURE 27. Power contribution of the MACsec IP to the design for different frame sizes.

IX. CONCLUSION

The O-RAN Fronthaul is exposed to Layer 2 threats and vulnerabilities that can significantly risk the operation of the RAN. An attacker with access to the fronthaul interface has the capacity to eavesdrop on all traffic in the link. Without any security mechanism, an attacker can access and identify hosts, types of traffic, and packet contents. This allows him to inject false messages by impersonating a legitimate node, corrupting a legitimate message, and replaying or delaying a legitimate message. These threats can be performed especially to CUS-Planes protocols due to their clear-text nature and direct encapsulation over Ethernet. The overall impact of these threats is a possible degradation or Denial-of-Service in the RAN. Therefore, there is an urgent need for Layer 2 security mechanisms to protect the O-RAN Fronthaul with features of authenticity, confidentiality, integrity, and replay protection.

MACsec is a persuasive solution to secure the O-RAN Fronthaul as it operates on Ethernet frames and, hence, can

provide protection to the CUSM-Planes encapsulated over Ethernet. However, implementation challenges exist that need to be addressed. These include fronthaul line rate dimensioning with MACsec overhead taken into account, accurate timestamping for S-Plane PTP protection with a fixed latency MACsec design, and multiple MACsec CAs support per port for traffic differentiation protection or for MACsec bypass in the multiple fronthaul topologies.

This article proposed a MACsec HW-based IP core architecture for the O-RAN Fronthaul that targets FPGA and ASIC implementations. It provides traffic bypass and multiple SecY selections per port according to CUSM-Planes data traffic. It also includes accurate S-Plane PTP timestamping for two-step PTP clock implementation with the TSU at the physical layer for time accuracy.

The MACsec IP was implemented and evaluated for its feasibility in FPGA devices and its impact on the link performance. Results show that over 16 SecYs can be supported using Xilinx UltraScale+ devices that provide higher resources compared to 7 Series architectures. The target frequency of 390.625 MHz required for 25 Gbps was achieved only by UltraScale+ devices. However, the target frequency of 156.25 MHz required for 10 Gbps was reached by UltraScale and 7 Series devices.

It was observed that a CPU gain of 42.38% was achieved using the MACsec IP compared to the SW-based Linux MACsec implementation. However, adding the MACsec IP to the Ethernet port under evaluation increases the power consumption by 150%. The proposed MACsec architecture follows the 10 Gbps fronthaul line rate under evaluation with a maximum cost of 10% reduction. This cost can be added to dimension the fronthaul bandwidth when using MACsec. Finally, the MACsec IP offers a fixed latency of 0.288 us from the frame ingress to the frame egress regardless of the frame size which represents a minimal delay contribution to the fronthaul interface. This also supports the placement of the PTP TSU before the MACsec layer for S-Plane PTP one-step clock implementation if required. Therefore, the proposed MACsec hardware architecture satisfies the security and performance required in the O-RAN Fronthaul interface.

REFERENCES

[1] L. Bariah, L. Mohjazi, S. Muhaidat, P. C. Sofotasios, G. K. Kurt, H. Yanikomeroglu, and O. A. Dobre, "A prospective look: Key enabling technologies, applications and open research topics in 6G networks," *IEEE Access*, vol. 8, pp. 174792–174820, 2020.

[2] M. Polese, M. Giordani, M. Mezzavilla, S. Rangan, and M. Zorzi, "6G enabling technologies," in *6G Mobile Wireless Networks* (Computer Communications and Networks). Cham, Switzerland: Springer, 2021.

[3] I. F. Akyildiz, S. Nie, S.-C. Lin, and M. Chandrasekaran, "5G roadmap: 10 key enabling technologies," *Comput. Netw.*, vol. 106, pp. 17–48, Sep. 2016.

[4] Q. Li, Z. Ding, X. Tong, G. Wu, S. Stojanovski, T. Luetzenkirchen, A. Kolekar, S. Bangolae, and S. Palat, "6G cloud-native system: Vision, challenges, architecture framework and enabling technologies," *IEEE Access*, vol. 10, pp. 96602–96625, 2022.

[5] A. Dutta and E. Hammad, "5G security challenges and opportunities: A system approach," in *Proc. IEEE 3rd 5G World Forum (5GWF)*, Bangalore, India, Mar. 2020, pp. 109–114.

[6] S. A. A. Hakeem, H. H. Hussein, and H. Kim, "Security requirements and challenges of 6G technologies and applications," *Sensors*, vol. 22, no. 5, p. 1969, Mar. 2022.

[7] M. A. Habibi, B. Han, M. Nasimi, N. P. Kuruvatti, A. Fellan, and H. D. Schotten, "Towards a fully virtualized, cloudified, and slicing-aware RAN for 6G mobile networks," in *6G Mobile Wireless Networks* (Computer Communications and Networks). Cham, Switzerland: Springer, 2021.

[8] *O-RAN Alliance*. Accessed: Jan. 17, 2023. [Online]. Available: https://www.o-ran.org/

[9] *Xhaul Transport Requirements 1.0*, O-RAN Open Xhaul Transport Workgroup, O-RAN Alliance, Germany, Feb. 2021.

[10] *O-RAN Control, User and Synchronization Plane Specification 10.0*, O-RAN Open Fronthaul Interfaces Workgroup, O-RAN Alliance, Germany, Oct. 2022.

[11] *IEEE Standard for Packet-Based Fronthaul Transport Networks*, IEEE Standard 1914.1-2019, Apr. 2020, pp. 1–94.

[12] *O-RAN Security Threat Modeling and Remediation Analysis 4.0*, O-RAN Security Work Group, O-RAN Alliance, Germany, Oct. 2022.

[13] *IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security*, IEEE Standard 802.1AE-2018, Dec. 2018, pp. 1–239.

[14] D. Dik and M. S. Berger, "Transport security considerations for the open-RAN Fronthaul," in *Proc. IEEE 4th 5G World Forum (5GWF)*, Oct. 2021, pp. 253–258.

[15] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, "Open RAN security: Challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 214, May 2023, Art. no. 103621.

[16] J. Y. Cho and A. Sergeev, "Secure open fronthaul interface for 5G networks," in *Proc. 16th Int. Conf. Availability, Rel. Secur.*, New York, NY, USA, Aug. 2021, pp. 1–6.

[17] Rambus. *Rambus Announces Complete 800G MACsec Solution for Enhanced Data Center and 5G Infrastructure Security*. Accessed: Mar. 30, 2023. [Online]. Available: https://www.rambus.com/rambus-announces-complete-800g-macsec-solution-for-enhanced-data-center-and-5g-infrastructure-security/

[18] Marvell. *Marvell Announces Dual 400GbE MACsec PHY With Class C PTP Timestamping For Data Center and 5G Infrastructure*. Accessed: Mar. 30, 2023. [Online]. Available: https://investor.marvell.com/2020-02-04-Marvell-Announces-Dual-400GbE-MACsec-PHY-with-Class-C-PTP-Timestamping-for-Data-Center-and-5G-Infrastructure/

[19] L. M. P. Larsen, "A survey of the functional splits proposed for 5G mobile crosshaul networks," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 146–172, 1st Quart, 2019.

[20] *eCPRI Specification V2.0, Common Public Radio Interface: ECPRI Interface Specification*. Accessed: Jan. 17, 2023. [Online]. Available: http://www.cpri.info/

[21] *eCPRI Transport Network V1.2, Common Public Radio Interface: Requirements for the eCPRI Transport Network*. Accessed: Jan. 17, 2023. [Online]. Available: http://www.cpri.info/

[22] *IEC/IEEE International Standard—Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*, document IEC/IEEE 61588-2021, Jun. 2021, pp. 1–504.

[23] *Precision Time Protocol Telecom Profile for Phase/Time Synchronization With Full Timing Support From the Network*, ITU, document ITU-T Recommendation G.8275.1/Y.1369.1 Mar. 2020.

[24] *O-RAN Management Plane Specification 10.0*, O-RAN Open Fronthaul Interfaces Workgroup, O-RAN Alliance, Germany, Oct. 2022.

[25] O-RAN Alliance. *The O-RAN ALLIANCE Security Task Group Tackles Security Challenges on All O-RAN Interfaces and Components, O-RAN SWG Announcement of MACsec Future Study*. Accessed: Jan. 17, 2023. [Online]. Available: https://www.o-ran.org/blog/the-o-ran-alliance-security-task-group-tackles-security-challenges-on-all-o-ran-interfaces-and-components

[26] *O-RAN Security Requirements Specification 4.0*, O-RAN Security Work Group, O-RAN Alliance, Germany, Oct. 2022.

[27] O-RAN Alliance. *The O-RAN ALLIANCE Security Work Group Continues Defining O-RAN Security Solutions*. Accessed: Jan. 17, 2023. [Online]. Available: https://www.o-ran.org/blog/the-o-ran-alliance-security-work-group-continues-defining-o-ran-security-solutions

[28] *IEEE Standard for Local and Metropolitan Area Networks–Port-Based Network Access Control*, IEEE Standard 802.1X-2020, Standard 802.1X-2010, IEEE Standard 802.1Xbx-2014, and IEEE Standard 802.1Xck-2018, pp. 1–289, Feb. 2020.

[29] *NIST Advanced Encryption Standard (AES)*, Federal Inf. Process. Stds. (FIPS), Nat. Inst. Standards Technol., USA, Nov. 2001.
[30] M. Dworkin, "Recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC," Special Publication, NIST, Gaithersburg, MD, USA, Tech. Rep. 800-38D, Nov. 2007.
[31] W. Alghamdi and M. Schukat, "Precision time protocol attack strategies and their resistance to existing security extensions," *Cybersecurity*, vol. 4, no. 1, p. 12, Dec. 2021.
[32] J. Neyer, L. Gassner, and C. Marinescu, "Redundant schemes or how to counter the delay attack on time synchronization protocols," in *Proc. IEEE Int. Symp. Precis. Clock Synchronization Meas., Control, Commun. (ISPCS)*, Sep. 2019, pp. 1–6.
[33] H. N. Weste and D. Harris, *CMOS VLSI Design A Circuits and Systems Perspective*, 3rd Ed. London, U.K.: Pearson Addison Wesley, 2005.
[34] V. Taraate, "FPGA architecture and design flow," in *Digital Logic Design Using Verilog*. Cham, Switzerland: Springer, 2022.
[35] M. Vestias and H. Neto, "Trends of CPU, GPU and FPGA for high-performance computing," in *Proc. 24th Int. Conf. Field Program. Log. Appl. (FPL)*, Sep. 2014, pp. 1–6.
[36] *AMBA AXI and ACE Protocol Specification*, ARM Corp., Cambridge, U.K., 2003.
[37] *AMBA 4 AXI4-Stream Protocol Specification*, ARM Corp., Cambridge, U.K., 2019.
[38] S. D. Brown and Z. G. Vranesic, "Fundamentals of digital logic with VHDL design," in *McGraw-Hill Series in Electrical and Computer Engineering*, 3rd ed. New York, NY, USA: McGraw-Hill, 2009.
[39] *UltraScale Architecture Configurable Logic Block User Guide (UG574)*, Xilinx, San Jose, CA, USA, 2017.
[40] *Vivado Design Suite User Guide: Design Flows Overview (UG892)*, Xilinx, San Jose, CA, USA,2022.
[41] *UltraScale Architecture and Product Data Sheet: Overview (DS890)*, Xilinx, San Jose, CA, USA, 2020.
[42] *ZCU102 Board User Guide (UG1182)*, Xilinx, San Jose, CA, USA, 2019.
[43] *Linux WPA/WPA2/IEEE 802.1X Supplicant*. Accessed: Jan. 17, 2023. [Online]. Available: https://w1.fi/wpa_supplicant/
[44] D. Matson and L. Bielich. (2019). *Accurate Design Power Measurement Made Easier*. [Online]. Available: https://www.xilinx.com/developer/articles/accurate-design-power-measurement.html

DANIEL DIK (Graduate Student Member, IEEE) received the B.Sc. degree in electronics and telecommunications engineering from ESPOL University, Ecuador, in 2015, and the M.Sc. degree in telecommunications engineering from the Technical University of Denmark, in 2019, where he is currently pursuing the Ph.D. degree. His research is in collaboration with Danish Company Comcores ApS, where he leads projects related to security in next-generation radio access networks and time sensitive networking.

MICHAEL STÜBERT BERGER (Member, IEEE) was born in 1972. He received the M.Sc. (E.E.) and Ph.D. degrees from the Technical University of Denmark (DTU), in 1998 and 2004, respectively. He was the Project Leader of the National Project Ethernet for RAN (ERAN), where TSN was explored in the Fronthaul network. Furthermore, he coordinated the participation from DTU in a Eurostars Project on TSN (Fronthaul for CRAN). He is currently an Associate Professor with DTU in the areas of switching and network node design. He has been participating in several projects in relation to TSN. He is also responsible for the department's participation with Nordic University HUB project on the Industrial IoT, fog computing, and TSN. At the moment, he is a mentor of two postdoctoral and two Ph.D. students in the areas of TSN and deterministic networks.