O-RAN Fronthaul Security using MACsec

With 5G being deployed for time-sensitive applications, security is becoming an important consideration. At the same time, Open Radio Access Networks (RAN) are gaining more interest from mobile carriers and governments. Yet, Open RAN networks have serious security challenges, especially in the RAN fronthaul where there are strict timing requirements. This paper proposes MACsec as an efficient data link layer security solution that can assist in meeting these challenges.

5G needs security

5G is now in full deployment with numerous services available across the globe. 5G provides a range of improvements over existing 4G Long-Term Evolution (LTE) mobile networks with regard to capacity, speed and latency. It also provides better security. Nevertheless, security risks still remain and these need to be addressed quickly to ensure that 5G can address all of the target applications that drove original specifications.

While 5G provides faster mobile broadband services compared to 4G LTE, the driving applications for 5G specifications are non-consumer services. 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 like industrial automation, autonomous vehicles and eHealth.

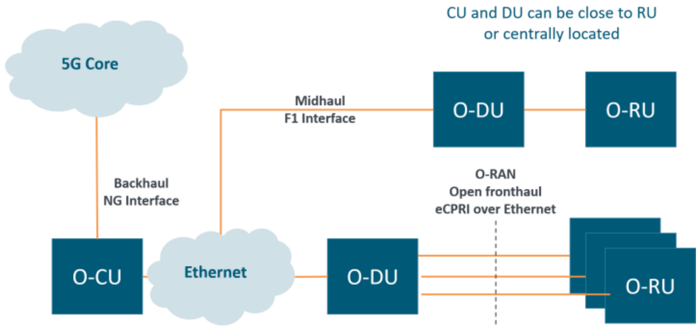

Figure 1: 5G RAN architecture

There are already numerous examples of security breaches exploiting IoT devices. But now that 5G-connected IoT devices can be used to support critical infrastructure like electricity and water supply, security becomes a concern for governments and their national security plans.

For URLLC applications, security is a pre-requisite as these are time-sensitive applications. Industrial automation applications, like Automated Guided Vehicles (AGVs) and industrial sensors, need to be secure at all times. It is also clear that applications like autonomous vehicles also need to be secure.

5G is poised to support the digital transformations happening across multiple industries, but in order to do so, security concerns must be addressed, including 5G RAN security challenges.

5G security enhancements

5G provides enhanced security measures compared to previous generation mobile networks[1], such as mutual authentication capabilities that confirm that the sender and receiver are trustworthy, enhanced subscriber identity protection and User Plane integrity checks between the Central Unit (CU) and User Equipment (UE).

[1] Source: https://www.gsma.com/security

Many of these security measures rely on upper layer security solutions, like Transport Layer Security (TLS). However, 5G networks are now based on Ethernet as the transport layer from device to 5G core. This means that attacks that target the Ethernet layer can also be used to compromise 5G networks, especially the 5G fronthaul network connecting 5G Radio Units (RUs) to Distributed Units (DUs) as shown in Figure 1.

But this also provides an opportunity. Since Ethernet is now the data link layer for 5G networks, security solutions designed for Ethernet, such as MACsec, can be used to provide security. MACsec can defend against attacks specific to the data link layer, thereby protecting upper layers.

5G fronthaul and Open RANs

As seen in Figure 1, the 5G RAN is based on a virtualized architecture where functions can be centralized close the 5G core for economy or distributed as close to the edge as possible for lower latency performance. This provides a great deal of flexibility in addressing specific service requirements, but also results in a number of new, open Ethernet-based interfaces that can pose a security risk.

While many of the interfaces between logical entities in 5G have been standardized by 3GPP, there are others, such as the interface between RUs and DUs that have not been as well defined. This is because these interfaces have typically been proprietary to the 5G RAN vendor.

In 4G LTE, the equivalent Remote Radio Unit (RRU) to BaseBand Unit (BBU) interface was based on the Common Public Radio Interface (CPRI) specification, which provided enough options for vendors to provide proprietary solutions. In 5G, this has been replaced by the Ethernet-based enhanced CPRI (eCPRI) interface, as shown in Figure 2.

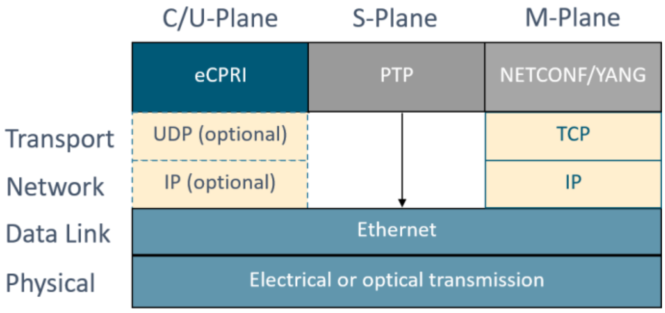

Figure 2: O-RAN Fronthaul data planes encapsulation over ethernet

eCPRI is more open and makes it possible for multiple vendors to provide either an RU or DU solution. However, additional specifications are needed to ensure interoperability. This has given rise to various Open RAN initiatives. The two most prominent Open RAN initiatives are the Telecom Infra Project (TIP) OpenRAN project and the Open-RAN (O-RAN) Alliance.

The TIP project was established to build open-source, cost-effective telecom equipment for deployment in less developed regions of the world and the TIP OpenRAN project is focused on building cost-effective RU, CU and DU solutions.

The O-RAN Alliance was established in 2018 to specify Open RAN solutions with specific emphasis on interfaces and implementation guidelines that are not detailed in 3GPP recommendations and are important for interoperability. The O-RAN Alliance specifies the Open Fronthaul interface between the RU and DU[2], which has enabled non-traditional telecom equipment vendors to deliver RU and DU solutions and increase competition. The Open Fronthaul Interface between the RU and DU is based on the 7.2x split in Figure 3 (below). As can be seen, the protocol stack can be split at various points enabling functionality to be deployed at various points in the network. This enables simpler, more compact and lower cost RU implementations as only the RF and lower PHY layer functions need to be supported. Since 5G will require an

[2] O-RAN Control, User and Synchronization Plane Specification 9.0

order of magnitude increase in the number of RUs to be deployed, this can lower deployment costs significantly.

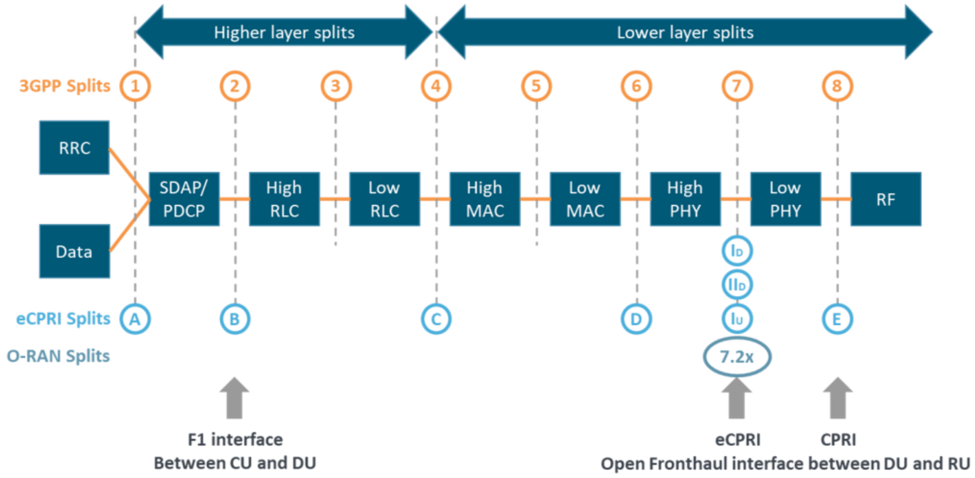

Figure 3: 5G RAN Functional Splits

The functional splits also provide flexibility when deploying functionality allowing specific service performance 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, but not the interface between the DU and RU, which was proprietary to the vendor in previous mobile network generations. The O-RAN Alliance Open Fronthaul interface specification enables multivendor operation based on the eCPRI interface.

With eCPRI, all of the functional split interfaces are now supported by Ethernet at the data link layer. As shown in Figure 2, the User (U), Control (C), Management (M) and Synchronization (S) Planes are all supported by Ethernet. However, this opens the 5G RAN to vulnerabilities at the Ethernet layer.

The first O-RAN Alliance specifications were released in 2019, but security was not an emphasis at the time. In 2020, the Security Focus Group (SFG) was formed to address this issue. This group, now known as WG11: Security Work Group, have provided new specifications in July 2022 (see Table 1) that address many security issues, but there are still vulnerabilities that need to be addressed.

O-RAN Security Specification	Date	Description
O-RAN Security Protocols Specifications 3.0	Mar 2022	Specifies security protocols for O-RAN along with requirements for SSH, IPsec and (D)TLS where TLS1.3 is now mandatory
O-RAN Security Requirements Specification 3.0	July 2022	Updates for Open Fronthaul security, security for Near-RT RIC xAPPs and APIs, and optional support for Open Fronthaul Point to Point LAN security using 802.1x
O-RAN Security Test Specifications 2.0	July 2022	Test cases for Point-2-Point LAN Segment, SBOM, Network Protocol Fuzzing and O1 Interface Network Configuration Access Control Model (NACM) validation
O-RAN Security Threat Modeling and Remediation Analysis 3.0	July 2022	Likelihood assessment of the identified threats from the threat model and remediation analysis as well as well as updated threats and risk analysis
O-RAN Study on Security for Near Real Time RIC and xApps 1.0	July 2022	Security aspects and issues related to the Near-RT RIC platform and xApps, as well as the associated network and management interfaces (E2, A1, O1) and APIs
O-RAN Study on Security for Non-RT-RIC 1.0	July 2022	Security aspects and issues related to the Non-RT RIC Framework, rApps, R1 interface and A1 interface
O-RAN Study on Security for O-CLOUD 1.0	July 2022	Security aspects and issues related to the O-Cloud

Table 1: New O-RAN Security Specifications

Importance of O-RAN and O-RAN Security

While the O-RAN Alliance was initially driven by a mobile service provider desire to open the RAN and enable greater competition, global developments have increased the importance of Open RAN and the O-RAN Alliance in particular.

In the US and Europe, there has been growing concern over the reliance of mobile carriers on Chinese mobile network vendors, such as Huawei and ZTE. While Europe still has major mobile network vendors in Ericsson and Nokia, there are no equivalent vendors in the US.

The US has been particularly vocal in highlighting “supply chain risks” with regard to this fact[3]. As part of the national strategy to secure 5G, the US proposes specific countermeasures including “increasing diversity in 5G component manufacturers, ideally with a high proportion of US manufacturers” as well as “Leadership in the field of standardization in order to influence the development standards according to US interests”. Open RAN initiatives like the O-RAN Alliance are seen as critical to achieving these goals.

Both in the EU and US, dependence on a few vendors is seen as a major risk. This was also highlighted in the EU 5G Risk Analysis[4] published by the NIS Cooperation Group. The Federal Office for Information Security (BSI) in Germany referred to the above in its recent Open RAN Risk Analysis report[5] from February 2022.

The report went on to highlight multiple Open RAN security risks. However, it was stated in the report that many of these risks were associated with service providers not implementing optional security measures outlined in 3GPP standards or recommended in O-RAN specifications.

Latest O-RAN Alliance Security Specifications address concerns

The O-RAN Alliance SFG made its first announcement in Oct 24, 2020 introducing planned SFG activities and roadmap[6]. In the announcement, the O-RAN Alliance recognized the need to secure important interfaces including the Open Fronthaul interface.

As of July 2022, there are a number of new and updated security specifications available that go a long way towards addressing the concerns highlighted in recent analyses[7], as shown in Table 1.

In the O-RAN Security Threat Modeling and Remediation Analysis 3.0, it is noted that there are specific threats and vulnerabilities associated with the Open Fronthaul interface:

- An attacker penetrates O-DU and beyond through O-RU or the Fronthaul interface
- Unauthorized access to Open Front Haul Ethernet L1 physical layer interface(s)
- An attacker attempts to intercept the Fronthaul using a Man-in-the-Middle (MITM) attack over the Management (M) Plane
- Denial of Service (DoS) attack against a Master clock
- Impersonation of a Master clock (Spoofing) within an Ethernet Precision Time Protocol (PTP) network with a fake ANNOUNCE message
- A Rogue PTP Instance wanting to be a Grand Master
- Selective interception and removal of PTP timing packets

[3] Source: “NATIONAL STRATEGY TO SECURE 5G”, Mar. 2020 and BSI 5G RAN Risk Analysis

[4] Source: NIS Cooperation Group, “EU coordinated risk assessment of the cybersecurity of 5G Networks”, Oct. 2019 and BSI 5G RAN Risk Analysis

[5] Source: BSI 5G RAN Risk Analysis, Feb 2022

[6] Source: The O-RAN ALLIANCE Security Task Group Tackles Security Challenges on All O-RAN Interfaces and Components

[7] Source: O-RAN Downloads (orandownloadsweb.azurewebsites.net)

- Packet delay manipulation attack
- Spoofing of DL C-Plane messages
- Spoofing of UL C-Plane messages
- An attacker attempts to intercept the Fronthaul (MITM) over U-Plane
- An attacker sets up a false base station attack by attacking an O-RU masquerading as a legitimate mobile network

In the O-RAN Security Requirements Specification 3.0, specific requirements for O-CU-CP/UP, O-RUs and O-DUs are yet to be defined, but there are requirements for the Open Fronthaul interface based on the threats and vulnerabilities identified above.

These requirements address the C- and S-Planes specifically. For the U-Plane, the document states that the Open Fronthaul U-Plane traffic is protected by security mechanisms in the Packet Data Convergence Protocol (PDCP) implemented in the CU protecting both C-Plane and U-Plane traffic between the CU and UE[8].

Security of the M-plane is addressed in the O-RAN Alliance O-RAN Management Plane Specification 9.0 from July 2022 where it is stated that "An O-RU shall support sFTP based file transfer over SSH and FTPES based file transfer over TLS. For the O-DU, the operator may use SSH, TLS, or both".

In general, the requirements are focused mainly on authentication and less on confidentiality and integrity concerns. However, based on the threats and vulnerabilities identified, confidentiality and integrity are equally important.

As can be seen above, security aspects and issues related to the Near Real Time RIC, Non-RT-RIC and O-CLOUD 1.0 have been provided where work is continuing on security aspects and issues related to the Open Fronthaul interface. We intend to contribute to this work by showing that MACsec can address the highlighted threats and vulnerabilities as well as confidentiality, integrity and authentication needs.

Proposing MACsec as a security solution for O-RAN Fronthaul

One of the concerns of implementing security for the Open Fronthaul interface is the impact on performance. The 5G fronthaul has strict latency requirements, which can be compromised when using security mechanisms like IPsec and TLS. For an in-depth description of MACsec, see our whitepaper "MACsec for Deterministic Ethernet applications.

MACsec provides authentication by ensuring that only known nodes are allowed to communicate on the network. It provides confidentiality through encryption of the data so only end-points with the correct encryption key can see the contents. Integrity is provided through a cryptographic mechanism ensuring that data has not been tampered with while in motion. Figure 4 provides an overview of the MACesc frame format.

[8] PDCP uses sequence numbering of each Service Data Unit (SDU) received from the Radio Link Control (RLC) layer to detect duplicates and re-ordering, while ciphering and deciphering is used to protect C-Plane and U-Plane data. Integrity protection and integrity verification is provided for C-Plane Data.

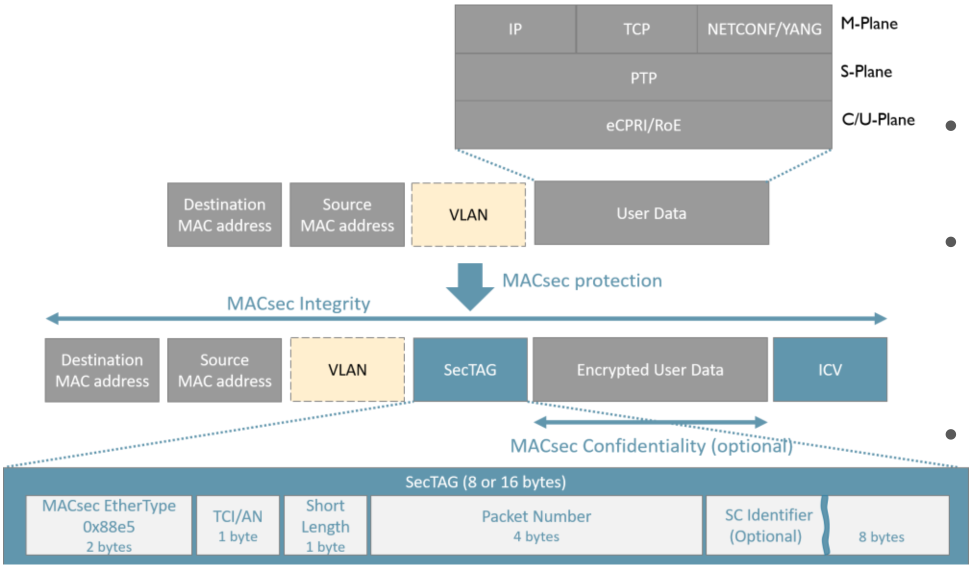

Figure 4: MACsec frame format

- The TAG Control Information/Association Number (TCI/AN) specifies if encryption is used
- The Short Length (SL) field specifies the length of the encrypted data, if it is a short frame
- The Packet Number (PN) is typically 32 bits long, but can be up to 64 bits long when eXtended Packet Number (XPN) versions are used for higher speed interfaces
- The Secure Channel Identifier (SCI) specifies the Secure Channel (SC) and is a concatenation of the 48-bit source MAC address and a 16-bit port ID

MACsec is implemented at the port level in dedicated hardware, which enables it both to scale from Mbps to Tbps and meet strict latency requirements. MACsec provides protection against attacks specific to the Ethernet data link layer, which cannot be addressed by IPsec and TLS, which operate on the network and transport layer. Since all functional split interfaces are now based on Ethernet, MACsec can be used to protect these interfaces as well as all traffic running over Ethernet.

With regard to the specific threats and vulnerabilities identified by the O-RAN Alliance, MACsec provides a compelling solution that can also meet performance requirements.

O-RAN Fronthaul vulnerabilities addressed by MACsec

MACsec can be used to provide protection of Ethernet frames transporting CUS and M-Plane data against attacks targeting Ethernet.

Control and User Plane vulnerabilities

If an attacker gains access to a DU or RU, either using a MITM attack or through access to the device directly, he can use the C-Plane or U-Plane to perform a variety of attacks at the Ethernet layer and eCPRI interface.

First, the attacker can claim to be either an RU or DU and inject malicious control messages. These can be used to manipulate U-Plane traffic, degrade performance or cause a DoS attack. Intercepted control messages can be stored and then delayed or re-transmitted repeatedly affecting the operation of upper layer protocols.

With MACsec, each end-point of the Open Fronthaul interface is part of a MACsec Connectivity Association (CA) and authenticated using a Connectivity Association Key (CAK). Only nodes that are part of the same CA are allowed to transmit or receive Ethernet frames. In addition, each Ethernet port will have at least one Secure Association (SA) for transmit and one SA for reception of traffic from each connected end-point. The SA is protected by a short-lived Secure Association Key (SAK), which is derived from the long-lived CAK.

MACsec can thus authenticate each RU and DU and ensure that only trusted end-points with valid CAKs and SAKs can exchange information. The SAKs are used as input to the AES-GCM cipher algorithms for encrypting Ethernet frames ensuring that attackers cannot see any payload contents. They are also used for integrity generating a unique ICV that ensures that any manipulation of the frames is detected immediately.

In addition, MACsec uses incremental Packet Numbers (PN) in each SA to keep track of Packets exchanged between end-points. This ensures that re-ordering, replaying or delaying of Ethernet frames is detected.

While PDCP protects U-Plane user data at a higher network layer, eCPRI packets are normally sent in plaintext in both the C- and U-Planes. Thus, attacks at the Ethernet layer could impact C/U-Planes by manipulating eCPRI user and control packets.

Management Plane vulnerabilities

As can be seen in Figure 2, the M-Plane does not run directly over Ethernet, but uses TCP/IP. TLS can thus be 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 planes discussed above. Ethernet frames can be corrupted, delayed, dropped or replayed and thereby disrupt management of the Open Fronthaul.

MACsec can offer the same protection for the M-Plane as other data planes and thereby complement the protection implemented with TLS.

Synchronization Plane vulnerabilities

As 5G needs to meet very strict performance requirements in relation to latency, synchronization based on ITU-T G.8275.1 PTP and Synchronous Ethernet needs to be protected. As both rely on Ethernet, they can be exposed to targeted attacks that could cause the disfunction of 5G networks and total DoS.

In ITU-T G.8273.2, requirements for timing accuracy are defined for different classes of boundary clocks in PTP nodes:

- Class A: 100ns
- Class B: 70ns
- Class C: 30ns
- Class D: 5ns

For 5G Open Fronthaul, there are use cases that can require PTP nodes to support Class C performance, as outlined in IEEE 802.1CM Ethernet TSN profile for Time-Sensitive Networking for Mobile Fronthaul, where the relative timing error needs to be lower than 65 ns between co-located RUs, 130ns for RUs sharing a clock in the same building and 260 ns for RUs sharing a clock, but situated in different buildings.

If an attacker can delay PTP packets for just a microsecond, services can be seriously disrupted. In addition, attackers can impersonate grand master clocks, boundary clocks or slaves and send malicious synchronization frames or just false frames to disrupt synchronization. This would have immediate impact on delivered services. They can also delay or repeat sync messages or adjust offsets to cause synchronization misalignments and disruption that can be hard to troubleshoot.

O-RAN Identified Threats	MACsec solution	O-RAN Requirements	Additional MACsec security capabilities relevant to Open Fronthaul Interface		
		Authentication	Encryption	Integrity	Replay Protection
An attacker penetrates O-DU and beyond through O-RU or the Fronthaul interface	MACsec authentication ensures that only authorized nodes can communicate with other peers	X			
Unauthorized access to Open Front Haul Ethernet L1 physical layer interface(s)	MACsec authorization based on SAKs that are short-lived and derived from CAKs that are not accessible at the interface.	X			
An attacker attempts to intercept the Fronthaul using a Man-in-the-Middle (MITM) attack over the Management (M) Plane	MACsec encryption ensures that the transported headers and payload are not visible while integrity capabilities ensure that any manipulation of frames will be detected.		X	X	
An attacker attempts to intercept the Fronthaul (MITM) over U-Plane					
Denial of Service (DoS) attack against a Master clock	MACsec authentication ensures that PTP nodes can only communicate if they are authenticated while encryption protects PTP messages. Integrity mechanisms detect any changes to frames as well as injection or deletion of PTP messages.	X	X	X	
Impersonation of a Master clock (Spoofing) within an Ethernet Precision Time Protocol (PTP) network with a fake ANNOUNCE message					
A Rogue PTP Instance wanting to be a Grand Master					
Selective interception and removal of PTP timing packets	MACsec encryption ensures that the content of the frame cannot be decoded so the attacker cannot see if the frame holds a PTP message or not. The attacker needs the encryption key to create a valid PTP message for injection.		X		
Packet delay manipulation attack	MACsec can detect out-of-order, replayed and delayed frames using the PN. But the attacker needs the encryption key to manipulate the frame.		X	X	X
Spoofing of DL C-Plane messages	MACsec authentication and confidentiality ensure that unauthorized nodes cannot communicate and that messages need to use the correct CAKs for encryption.	X	X		
Spoofing of UL C-Plane messages					
An attacker sets up a false base station attack by attacking an O-RU masquerading as a legitimate mobile network					

Table 2: How MACsec addresses 5G Fronthaul vulnerabilities

Again, MACsec authentication, encryption and integrity checks make it very difficult for attackers to succeed with these attacks. However, MACsec implementations need to respect the timing requirements and ensure that they are not a source of synchronization errors.

MACsec features thus protect the Open Fronthaul from the identified threats and vulnerabilities by the O-RAN Alliance as illustrated in Table 2.

Implementation challenges

Implementing security at the Open Fronthaul interface introduces new challenges that need to be addressed. Meeting latency requirements is a challenge, but can be addressed with careful planning. However, there are other implementation challenges that need to be considered with regard to the need for ensuring accurate timestamps and supporting multiple security domains. With careful implementation using MACsec, these challenges can be overcome.

Timestamp challenges

One of the challenges in implementing a high precision Ethernet port is when to time-stamp Ethernet frames. Ideally, the time-stamp should be added as close to the physical line as possible as the last action to ensure the most accurate outgoing time-stamp. Time-stamping can be done in one or two steps. In the case of a one-step PTP clock implementation, the time-stamp would need to be available at the MACsec layer in order to protect PTP messages using MACsec. This could be possible if the time-stamp is generated before the MACsec layer and the latency from that point to the physical layer is added. But for this to work, a fixed and predictable delay is required, which is a challenge in Ethernet.

The solution proposed by Comcores is to use a two-step PTP clock implementation. With a two-step solution the time-stamp is not sent with the frame, but in a separate “follow-up” message. This means that the accurate timestamp in the new “follow-up” message can be made available at the MACsec layer for protection.

The Comcores solution is depicted in Figure 5. A sideband tag is added to the PTP message. The message is then MACsec protected with confidentiality and integrity. The Time-Stamping Unit (TSU) is kept close to the physical layer. During transmission, it timestamps the frame with the PTP message and sideband tag. A Transmit buffer (TX buffer) is used to store the timestamp that can then be used to set the timestamp in the PTP follow-up message, which can then be MACsec protected with confidentiality and integrity.

During reception, the TSU timestamps all MACsec protected frames and tags each frame with a sideband tag. It stores the tag in a Receive buffer (RX buffer), and after MACsec verification, it maps the timestamp to the corresponding PTP message.

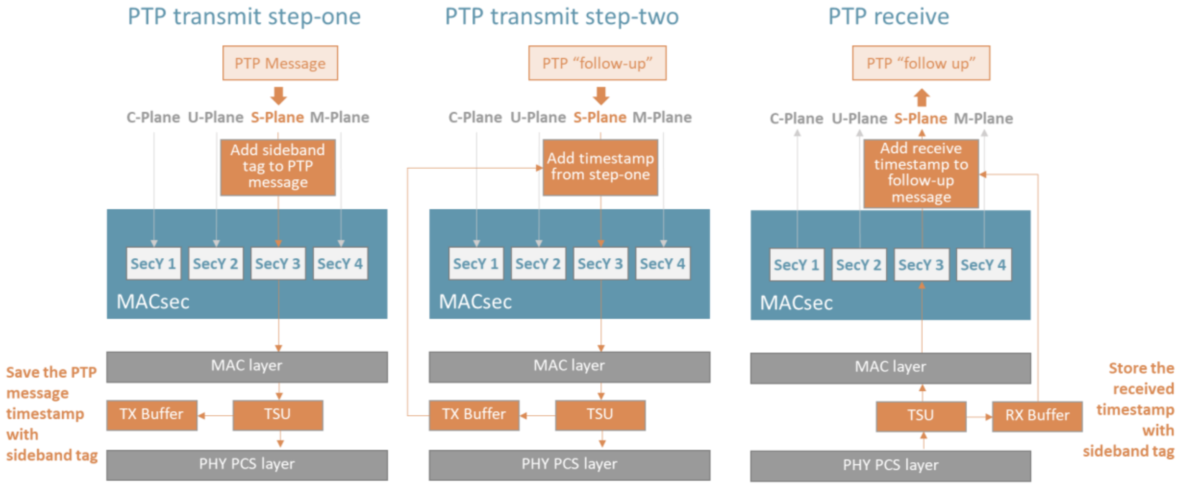
PTP transmit step-one
PTP transmit step-two
PTP receive
PTP Message
PTP “follow-up”
PTP “follow up”
C-Plane U-Plane S-Plane M-Plane
C-Plane U-Plane S-Plane M-Plane
C-Plane U-Plane S-Plane M-Plane
Add sideband tag to PTP message
Add timestamp from step-one
Add receive timestamp to follow-up message
SecY 1
SecY 2
SecY 3
SecY 4
MACsec
MAC layer
TX Buffer
TSU
RX Buffer
PHY PCS layer
Save the PTP message timestamp with sideband tag
Store the received timestamp with sideband tag

Figure 5: Precise time-stamping for MACsec

Multiple security domain challenges

At the Open Fronthaul interface, traffic from each of the CUSM planes may need to be sent separately to different nodes from a single port, sometimes over a fronthaul network, as shown in Figure 6. This results in different groups of nodes supporting each plane. For example, one group of nodes supports the C/U-Planes, while another group supports the S-Plane. Each group needs to be secured independently for security robustness including the need for different sets of keys. Thus, there is a need to support multiple security domains between a port and different destinations based on the type of traffic.

Comcores proposes a solution based on separate MACsec SecYs. As defined by the 802.1AE standard, a “SecY “is the entity that operates the MACsec protocol on an Ethernet port. Each SecY is associated to one port and can be part of only one Connectivity Association (CA) at a time, meaning that a port can send all its traffic to all peers that are part of the CA.

For a fronthaul unit, in order to support multiple security domains on a single physical port, multiple virtual ports and SecYs can be instantiated. This allows a port to support multiple CAs, and each CUSM Plane traffic can use an independent SecY for multiple destinations with different sets of keys.

In addition, for a fronthaul switched network, MACsec provides a “VLAN in clear” option” to allow VLAN bridging of MACsec frames. With this option, the VLAN tag is not encrypted and is therefore visible and available to VLAN bridges. This option can be complemented with the MACsec “confidentiality offset” feature where IP packet, TCP and UDP header information can also be exposed.

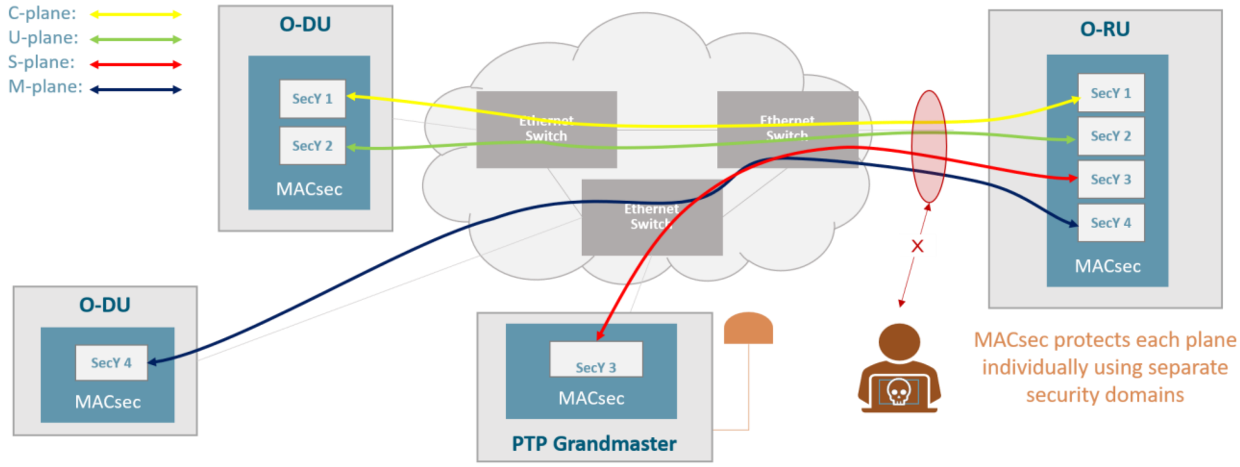

Figure 6: Multiple security domains

Comcores Packaged MACsec solutions for 5G

Comcores is planning to provide a range of Ethernet-based Packaged IP Solutions for 5G fronthaul applications that include MACsec. The Packaged IP Solutions combine various IP cores to provide a complete, pre-tested and validated solution that can be customized to meet individual design requirements.

This provides Comcores customers with a solid foundation for secure 5G fronthaul implementations. With Packaged IP Solutions, it is possible for customers to significantly accelerate their development efforts safe in the knowledge that the Packaged IP Solution has been tested and verified. Comcores experts are available to assist with adapting and customizing the Packaged IP solutions to meet specific needs and requirements.

Comcores MACsec IP

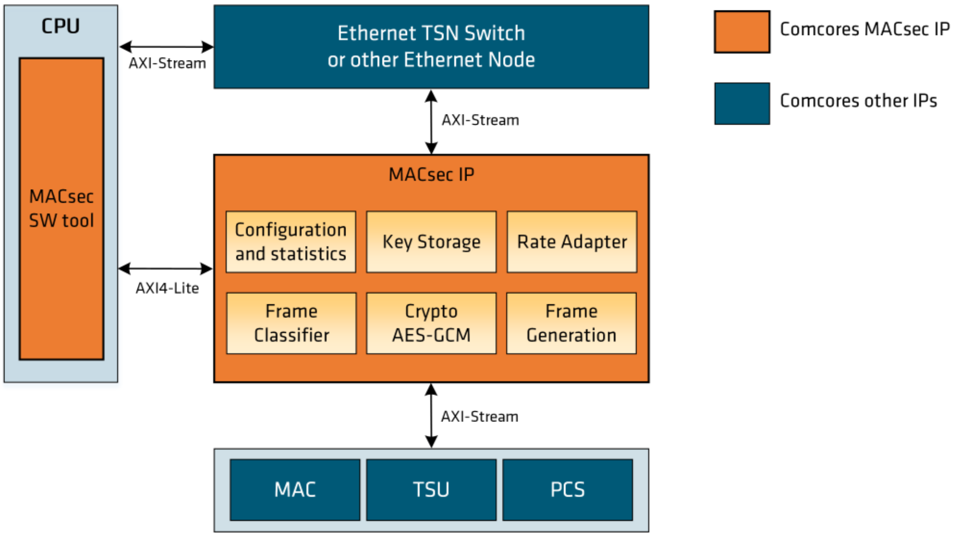

Figure 7: Comcores MACsec IP core integrated with other IP to form Packaged IP Solution

The Comcores MACsec implementation is also available as an individual IP core. The Comcores MACsec IP core is designed to be silicon agnostic and can thus be used in any FPGA, SoC or ASIC chip design. This enables a smooth migration from FPGA to ASIC.

The MACsec IP core provides full support for the IEEE 802.1AE-2018 MACsec specification including important features, such as both AES-GCM-128 and AES-GCM-256 Cipher Suites, VLAN-in-Clear and Confidentiality Offset.

The solution is highly configurable[9] and allows multiple SecY's and Connectivity Associations (CA) per port with traffic mapping rules. The solution supports a configurable number of peers. This allows traffic differentiation per port with an independent CA for multiple traffic types and MACsec bypass for a desired traffic type. For each CA, up to 4 Secure Associations (SA) can be supported for each transmit and receive Secure Channel (SC).

Software is also provided for integration of the IEEE 802.1X MACsec Key Agreement Protocol.

Secure 5G fronthaul implementations using Comcores MACsec IP

MACsec provides a compact, yet powerful security solution that meets O-RAN Alliance security requirements for 5G Open Fronthaul as well as addressing security concerns raised about Open Fronthaul. As Open Fronthaul becomes a strategic priority for service providers and national security strategies, the time is right to implement MACsec.

With Comcores MACsec IP core integrated in Packaged IP solutions for 5G fronthaul, chip developers can accelerate their time to market with a solid, reliable and flexible design foundation that minimizes development effort. This enables Comcores customers to deliver even more secure 5G fronthaul implementations quickly and reliably.

For more information on Comcores Packaged IP solutions and access to Comcores MACsec IP core visit: www.comcores.com