Securing Ethernet-based Optical Fronthaul for 5G Network

Joo Yeon Cho[1,*], Andrew Sergeev[2] and Jim Zou[3]

[1]*ADVA Optical Networking SE, Fraunhoferstrasse 9a, Martinsried, 82152, Germany*
[2]*ADVA Optical Networking Israel, 2 Hatidhar Street, Ra'anana, 4366105, Israel*
[3]*ADVA Optical Networking SE, Märzenquelle 1–3 Meiningen, 98617, Germany*
E-mail: JCho@advaoptical.com; ASergeev@advaoptical.com; JZou@advaoptical.com
[*]*Corresponding Author*

Received 29 November 2019; Accepted 04 December 2019;
Publication 23 January 2020

Abstract

In 5G networks, an optical fronthaul transports massive user data from remote radio heads (RRH) to the core network (CO) with high throughput and low latency. eCPRI is a new standard interface for the Ethernet-based optical fronthaul network to enhance the efficiency and performance. However, if fronthaul networks are deployed in an unsafe domain, an end-to-end security system should be implemented over the data flow, which requires additional overhead and processing time. This redundancy may cause unexpected latency and performance degradation in the data transport for 5G networks. According to the specification of eCPRI, vendors may optionally implement either IPsec or MACsec for the secure transmission. In this paper, we investigate security solutions suitable for the Ethernet-based optical fronthaul network. We analyse the standard security protocols such as IPsec and MACsec. Alternatively, we propose WireGuard as an replacement of IPsec for secure fronthaul networks. According to our analysis, the extended overhead for three security protocols has negligible impact on the latency. However, the encryption and decryption of transmission packets may cause additional latency on the eCPRI processing time and eventually reduce the

Journal of Cyber Security and Mobility, Vol. 9_1, 91–110.
doi: 10.13052/jcsm2245-1439.913

maximum transmission distance between RRH and CO. To verify our analysis, we simulated an eCPRI traffic on our test platform with the WireGuard protocol enabled. Our test results showed that the latency caused by encryption and decryption process could be significant. We also point out that a re-key interval should be carefully selected not to compromise the security of the high capacity transmission link such as 5G fronthaul networks. Our analysis is further extended with quantum-resistant cryptographic solutions for the long-term security of fronthaul networks.

Keywords: 5G, Ethernet, optical fronthaul, MACsec, IPsec, WireGuard, quantum-resistant cryptography.

1 Introduction

The 5G networks promise to enable a wide range of services with diverse performance requirements in order to form a fully connected society. Due to the massive connectivity and low latency, 5G can provide not only a high-speed mobile connection, but also allow new applications and services such as autonomous vehicles, massive IoT connections and eHealth.

The role of optical networks in 5G is to realize a high capacity and low latency of the data transmission that is required for a wide range of new 5G services. The optical fronthaul is an optical link between the remote radio head (RRH) at the antenna tower and the baseband unit (BBU) at the central office (CO), whereas the optical backhaul is a link between the BBU and the CO. Note that both fronthaul and backhaul are merged into X-haul that forms integrated planes which use heterogeneous switches for high optical transmissions.

The Common Public Radio Interface (CPRI) defines a core interface for fronthaul transport network. The eCPRI is an evolved interface for 5G, offering efficient and flexible data transmission via packet based fronthaul transport network such as IP or Ethernet, as it is widely used in both telecom and enterprise networks [1].

While applying Ethernet or IP in mobile fronthaul is attractive for operators who mainly offer data transport service, it also puts a new level of performance requirements, especially for delay, delay variation, packet loss, and reliability parameters [2]. Also, it brings up security issues, a heritage from the past, on Ethernet or IP based transport network.

The eCPRI specification states that “If the transport network is not safe for a particular flow, then an eCPRI network end-to-end security system should be implemented in the eREC node and eRE node for that flow.” [1].

An end-to-end security system is to ensure the confidentiality, authenticity and integrity of the data flow [3]. Usually optical networks are assumed to be a part of the trusted network, and the security of the optical network has not been well studied. However, it is possible to intercept an optical signal successfully if prevention mechanisms are not well integrated into the network, as shown in [4].

Building a proper security mechanism between RH and BBH is important for overall 5G network security. The eCPRI network security protocol includes IPsec in IP traffic and MACsec in Ethernet traffic [1]. One may expect additional latency or the performance degradation on the fronthaul network when IPsec or MACsec is activated. According to [5] and [2], a maximum one-way latency requirement of Fronthaul is about 100 μsec. Hence, one may wonder whether there is any impact on the performance of optical fronthaul when MACsec or IPsec is enabled. To the best of our knowledge, this issue has never been investigated in the literature.

In this paper, we study the security of the Ethernet-based optical fronthaul for 5G network. We investigate MACsec, IPsec and, in addition, WireGuard for the security of optical fronthaul networks. We analyse their security and feasibility in terms of latency and the bandwidth for 5G network. We derive the maximum transmission distance that meets the latency budget.

The structure of this paper is as follows: first, we identify the major security threats in 5G fronthaul network. Then, we analyse security solutions to thwart such security threats. We describe our experiments to simulate eCPRI traffic using one of security solutions. We present our results and discussion. Finally, we conclude our paper.

2 Security Threats in 5G Fronthaul

In 5G network, the core network is normally regarded as the secure network domain. However, some network functions or some parts of the network functions of the core network could possibly be deployed in the unsafe domain. Thus, it increases the risk of communication between the radio access network (RAN) parts and the core network (CN) parts, as well as the inter-communication between the CN elements located in secure and not-secure domain. We identify the following categories for typical security threats on the optical fronthaul networks.

Eavesdropping/Packet sniffing. Eavesdropping is to attempt unauthorized access to the carried data for the purpose of stealing data or analysing the network traffic without breaking the connection. There are several ways to tap into an optical fibre, including fibre bending, splitting, evanescent coupling, scattering, and V-grooves [4]. It is not very difficult to tap the fibre; One can tap the fibre using a commercially available clip-on coupler that can detect the leaked optical signal caused by a bend in the fibre. More complex method is to observe the signal leaked due to crosstalk in optical switching and perform eavesdropping. A signal on an optical fibre can be easily captured, once the physical access to the fibre is available. At this point, the data of millions of users and billions of applications is exposed to theft and manipulation.

Denial of Service (DoS) attack. Denial of Service (DoS) attack is one of the critical cyber-attacks on 5G networks. Attackers can launch DoS attacks on the user plane by sending bogus packets to the network. In terms of optical fronthaul networks, attackers may inject bogus packets into optical fibre. The path towards the core network can be flooded by bogus packets. This would lead to denial of service or at least throughput degradation caused by congestion to networks. For instance, simulation results of DDoS attacks on optical fibre cable is presented in [6].

Network intrusion. Attackers may attempt to intrude the network via a fronthaul, access resources, and manipulate the network operation. Malicious applications and network devices may allow an attacker to introduce vulnerabilities to the core network. This type of attack is critical to optical networks that are managed by an SDN controller because the attacker may try to hijack an SDN controller and control the entire 5G networks.

Man-in-the-middle attack. A man-in-the middle attack occurs when there is no authentication of the communication endpoints. If an attacker can impersonate a legitimate network device, he can execute a man-in-the-middle attack to monitor, modify or inject control messages.

Quantum attacks. Quantum attacks are a new and critical threat on the internet, including 5G network. It is well known that most popular public-key cryptosystems, such as RSA, ECC and Diffie-Hellman key exchange will be broken using Shor's algorithm [7] when large-scale quantum computers are available. One may argue that it may be too early to discuss this threat at this stage since no one knows when quantum computers can be built. However, as long as there exists a non-negligible risk of quantum attacks such as harvest attacks, it is reasonable to consider the quantum security at the stage of 5G architecture design. In this context, the quantum attack should be considered as one of the serious threats that a framework of 5G security should consider.

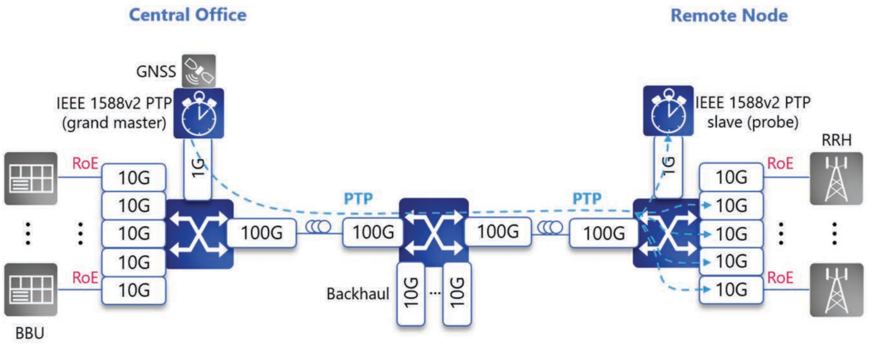

Figure 1 Fronthaul network in Ethernet-based aggregation.

3 System Model

Since Ethernet is a mature and ubiquitous technology used in vast types of networks with low cost, for 5G RAN, Ethernet becomes a converged protocol to enable connectivity between RAN functional modules, statistical multiplexing gain, multi-vendor interoperability, and prevent the protocol dependence like CPRI.

Figure 1 illustrates a typical application scenario in an Ethernet-based fronthaul network using multiple switch nodes. The radio signal from the baseband unit (BBU) is framed into Ethernet frames before entering the 10G ports for aggregation. $\mathrm{N} \times 10$ Gbps Ethernet fronthaul traffic streams are then aggregated at the central node [8].

The cell site synchronisation in most current deployments relies on the global navigation satellite system (GNSS) as the most straightforward way.

However, this may be a costly installation, and access to the GNSS satellite signal at the cell site cannot always be guaranteed. As an alternative, the IEEE 1588v2 Precision Time Protocol (PTP) provides a mechanism for end-to-end phase and time alignment as well as frequency [9]. As shown in Figure 1, the grand master clock disciplined with the GNSS generates PTP packets, which are also aggregated through a 1G port at the same node [10]. The timing information will be used to synchronize remote radio heads (RRHs). As PTP is a packet-based Layer 2/3 protocol, its performance is extremely prone to the packet delay variation (PDV) across network elements. To ensure accurate timing delivery and synchronized fronthaul traffic, the PTP packets need to be prioritized with minimum PDV, while the aggregated fronthaul traffic has a bounded delay.

Other less time-sensitive or backhaul traffic may be added at the intermediate node, dimensioned for the required upper bounded delay, without affecting the high-priority PTP packets and fronthaul services, while increasing the overall network throughput and resource utilization. At the remote node, the aggregator de-multiplexes and feeds each fronthaul traffic stream to the corresponding RRH. The PTP packets carried on the 1G stream can be terminated by the PTP slave clock, forwarding the 1PPS signal to the RRH for the radio synchronization purpose.

4 Security Solutions

For the security of 5G fronthaul, network nodes should be mutually authenticated, and traffic data between nodes should be encrypted. With 5G architectures, the traffic from RRH traverses over Ethernet or IP networks, which introduces a variety of security concerns. Security breaches can lead to severe service disruptions and financial loss. Service providers must put systems and controls in place to protect their networks against malicious attacks and ensure the integrity and confidentiality of voice and data communications [11]. In this section, we briefly describe MACsec, IPsec and WireGuard protocol that can be used for the security of 5G optical fronthaul.

4.1 MACsec

MACsec (Media Access Control Security) is an IEEE 802.1AE standards [12] to provide an point-to-point secure communication over Ethernet-based networks. When MACsec is enabled, each packet on the wire is encrypted using symmetric key cryptography such as AES-GCM-128 or AES-GCM-256 for data confidentiality and integrity.

MACsec Key Agreement (MKA) is a companion protocol defined in IEEE Std 802.1X-2010 to provide mutual authentication between the ports and derive a master session key [13]. For a point-to-point direct link, ASIC-based MACsec adds approximately 1–3 μsec of the latency and about 32 extra bytes of the overhead.

4.2 IPsec

IPsec is a widely deployed security protocol over IP networks. It enables a network entity in public domain to access a secure domain, and also enables a network entity in different domain to connect with each other in a secure way [3]. Most IPsec implementations consist of an IKE (Internet Key Exchange) daemon that processes the actual IP packets with numerous configuration options.

However, the network domain partition in 5G networks is usually complicated, therefore, a significant number of IPsec tunnels would be required. Hence, configuring IPsec tunnel will be a big challenge for a large scale of deployment. Furthermore, IPsec tunnels commonly use certificate-based authentication methods, which may cause significant cost to maintain a large scale of PKI system. A PKI system includes initial certificate application, certificate revocation and the periodical revocation list updating, which brings unnecessary risks to fronthaul networks. An online certificate status validation protocol, like OCSP [14], might solve this problem, however it is not widely used so far. In virtual infrastructure, certificate management could be much more difficult because of the virtual network functions are dynamically deployed.

4.3 WireGuard

WireGuard [15] is a modern secured tunnel that is operated over IP layer. The WireGuard Handshake protocol is based on Noise framework, which results in minimalistic and secured message exchange. Specifically, the WireGuard protocol uses a Noise Handshake pattern. The security of this pattern is formally verified in [24]. This pattern requires one-round trip of the message exchange between an initiator and a responder for session keys calculation; a static public key of initiator/responder is transmitted in an encrypted form.

WireGuard uses a point-to-point protocol for transporting IP packets that are encapsulated in UDP packets. The tunnel implements AEAD (Authenticated Encryption with Associated Data) form of data encapsulation. The data message is shown in Figure 2. The output from the AEAD is the concatenation of a ciphertext, which is of the same length as a plaintext, and a 128-bit tag, which is the output of the Poly1305 function, respectively. See [16] for details.

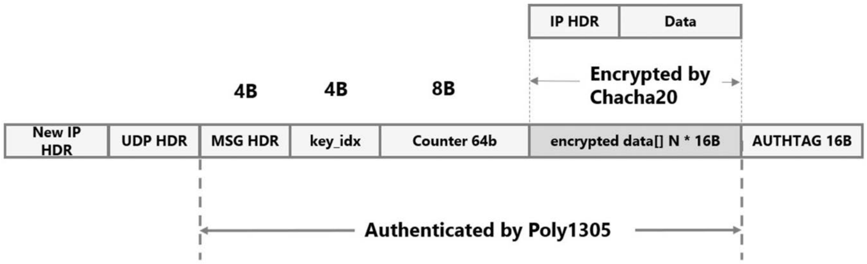

Figure 2 WireGuard data message: ChaCha20 and Poly1305 AEAD [15].

5 Security Analysis

In this section, we analyze the security solutions in several aspects.

5.1 Tunnelling

IPsec is a standardized solution for network security in 3GPP. IPsec functions at Layer 3, providing an end-to-end security via tunnels. The payload encryption and decryption occur only at the end of the tunnel. A major drawback of IPsec is its complexity. Not only it entails a dedicated encryption engine, but also IPsec significantly enlarges the size of an Ethernet header, which degrades the performance of networks.

In contrast, MACsec is a relatively simple protocol. It expands only the header in a minimal way. Because MACsec is usually PHY port-based, it supports easy upgrade and high-speed connectivity up to 100 G at low power and low cost. The disadvantage of MACsec is that all traffic traversing the link requires matching and verifying secret keys at each node.

WireGuard is not a part of eCPRI Network Security Protocol suites. However, WireGuard has the potential to replace IPsec because it offers faster speeds and better reliability with new and improved encryption standards. The major strength of WireGuard is the simplicity of configuration and operation. It minimizes attack surfaces and enhances its performance. A downside of WireGuard is that peers are authenticated using pre-shared public keys that should be delivered in out-of-band. Another drawback is that WireGuard does not offer extensibility, negotiation, or cryptographic agility [17].

Nevertheless, an optical fronthaul is rather static, compared to 3GPP mobile networks. Hence, the requirements for management and agility of the security mechanisms in 3GPP would not be essential for securing optical fronthaul. Furthermore, the security of WireGuard is formally verified by several cryptanalytic groups, e.g. in [18]. WireGuard is recently released into the standard Linux kernel. Hence, it will be a de-facto VPN standard for any Linux VM/bare metal, which eliminates the need for installing extra packages.

5.2 Overhead

The overheads of MACsec, IPsec and WireGuard are depicted in Figure 3. Table 1 shows how the size of overhead is calculated in detail. An eCPRI user plane PDU consists of one or more eCPRI messages separated by eCPRI common header (4 bytes). See Figure 4. This adds at least 4 bytes eCPRI

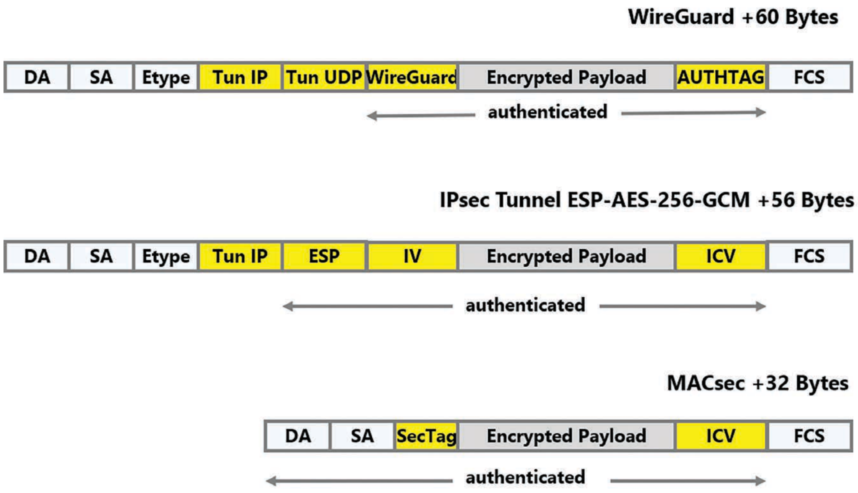

Figure 3 Comparison of MACsec, IPsec and WireGuard: AEAD data encapsulation overhead with 256-bit key length.

Table 1 Calculation of overhead in bytes

Protocol	Overhead	Description
MACsec	32	SecTag(16) + ICV(16)
IPsec ESP-AES-256-GCM	56	Tunnel IP(20) + ESP(8) + IV(12) + ICV(16)
WireGuard	60	Tunnel IP(20) + Tunnel UDP(8) + WG Header(16) + WG AUTHTAG(16)

overhead (OH) per packet (so-called for non-concatenated case, where one eCPRI message is mapped onto a transport network layer payload [1]. The eCPRI Transport overhead in total is summarized in Table 2. It shows that an extra overhead added by tunneling is negligible; for a packet size of 1500 bytes, it increases only about 3%. The calculation is based on the 3 Gbps eCPRI payload rate, which transmits 375,000,000 bytes per second. A payload size is slightly different for each tunneling protocol; for MACsec, it is 1464 bytes, and, for IPsec and WireGuard, it is 1412 and 1408 bytes, respectively.

Resulting number of packets must be transmitted over Ethernet line, so we are adding VLAN tag (for eCPRI over MACsec only), Ethernet MAC (14 bytes), FCS (4 bytes) and Framing OH (preamble and Start of frame 8 byte and inter-packet gap 12 byte) to original byte number. This gives us the desired line rate for transmitting eCPRI payload. The rate is 3.086 Gbps

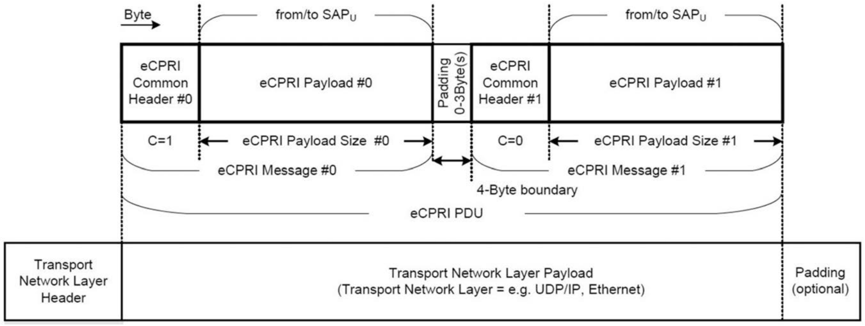

Figure 4 Two concatenated eCPRI user plan messages [1].

Table 2 The eCPRI Transport Overhead in bytes. The packet MTU is assumed to be 1500 Bytes. The size of Eth MAC + Framing is calculated by DMAC(6) + SMAC(6) + Etype(2) + FCS(4) + PRE(8) + IPG(12)

Item	MACsec	IPsec	WireGuard
eCPRI Header (minimum)	4	4	4
eCPRI UDP	0	8	8
eCPRI IPv4	0	20	20
Enc Header	16 (SecTag)	20 (ESP)	16
Enc Trailer	16	16	16
Tunnel UDP	0	0	8
Tunnel IPv4	0	20	20
Tunnel Overhead	36	88	92
eCPRI Payload	1464	1412	1408
VLAN tag	4	0	0
Eth MAC + Framing	38	38	38
Total Overhead	36 + 4 + 38 = 78	88 + 38 = 126	92 + 38 = 130

for MACsec, 3.08 Gbps for IPsec and WireGuard. Hence, Overheads are not decisive factors for the selection of the protocol. Note that an extra UDP layer in WireGuard can be ignored.

We might check forwarding pipeline difference between MACsec, IPsec and WireGuard, but eCPRI seems to be mostly P2P, so forwarding decision is almost trivial.

5.3 Re-key interval

It is important to replace an encryption key before a certain amount of data are processed with a single key in order to constrain the key exposure. This amount is called “key lifetime”. A specific value of the key lifetime should be determined in accordance with some safety margin for protocol security. In [19], it is given that low bounds on the amount of data that AES-GCM can process without needing a key change.

We note that MACsec, IPsec and WireGuard have different re-key policies. If they are used for the security of fronthaul networks, the following points should be considered.

5.3.1 MACsec

A re-key process can be occurred based on the volume of traffic or the time interval. For the high capacity links such as 5G fronthaul, a re-key interval should be carefully set in such a way that the targeted security level is ensured by encrypting a limited amount of data with a single key. Every MACsec frame contains a unique 64-bit packet number (PN) [20]. The Extended Packet Numbering (XPN) can be used to configure the re-key that is used for the GCM-AES-XPN-128 or GCM-AES-XPN-256 cipher suites under the defined MKA policy.

5.3.2 IPsec

The SA must begin a new IKEv2 SA re-key before the key lifetime expires [21]. The default key lifetime of SA is 8 hours. Assuming that 5G fronthaul uses a link of 10 Gb/s and IPsec has a 8-hour key lifetime, about 36 TB (10 Gb/sec $\times$ 8 $\times$ 3600 sec/key) data would be encrypted with a single key. Hence, according to [19], the attack success probability will be around 2^{-50}. If IPsec is used for the higher speed of link such as 100 Gb/s, then the maximum amount of data will be 360 TB and the attack success probability is lowered to around 2^{-40}. The re-authentication interval is derived by multiplying the key lifetime by the IKEv2 Authentication Multiple.

5.3.3 WireGuard

The WireGuard protocol uses short-lived sessions with ephemeral keys in order to ensure perfect forward secrecy. Each session lasts for at most 3 minutes and at most 2^{64} - 2^4 - 1 data packets transmissions. Hence, according to [19], the attack success probability is negligible since the amount of encrypted data is far below than the lower bound.

5.4 Quantum-resistance

All MACsec, IPsec and WireGuard rely on classical public key cryptosystems. Hence, they will not be secure in a quantum world. We investigate the possibility to add a quantum-resistance feature to these protocols. We note that most quantum-resistant cryptographic algorithms are relatively new and require further analysis [22].

5.4.1 MACsec

MACsec can be quantum-secure by enforcing the use of 256-bit symmetric keys for the payload encryption and quantum-resistant cryptographic algorithms for the node authentication. The MSK derived in EAP methods should be established by mandating the use of a quantum-resistant cipher suite.

5.4.2 IPsec

In the IPsec tunnel, the peer authentication and session key establishment are performed by the IKE protocol [21]. This means that IPsec can achieve quantum-resistance by enforcing the use of a quantum-resistant cipher suite during the IKE protocol. For this, new key exchange identifiers need to be defined in the Secure Association. A negotiation process is done in the same way as classic key exchange such as Diffie-Hellman key exchange.

5.4.3 WireGuard

WireGuard uses Curve25519 [23] for an ECDH key exchange. It can be replaced by a quantum-resistant key exchange algorithm. Alternatively, WireGuard allows to use a pre-shared key (PSK) that is a pairwise-unique static symmetric key. This optional PSK is mixed with session keys using the key derivation function (KDF). As shown in [25], a quantum adversary could break ephemeral ECDH, which reveals static public keys. This means that an adversary can compute a long-term static key pair of the initiator or responder. However, this attack would not reveal session keys thanks to the presence of the PSK.

The main operational challenge of using WireGuard with PSK is the requirement of secured out-of-band channel for distribution of PSK and public keys. For 5G transport network it is translated to the presence of technician on the site, which may increase operational cost.

6 Experiment

We performed a simulation of eCPRI traffic with IP tunneling. We measured a one-way latency for three cases: a single IP forwarding, a paired IP forwarding without tunneling, and a paired IP forwarding using WireGuard tunneling.

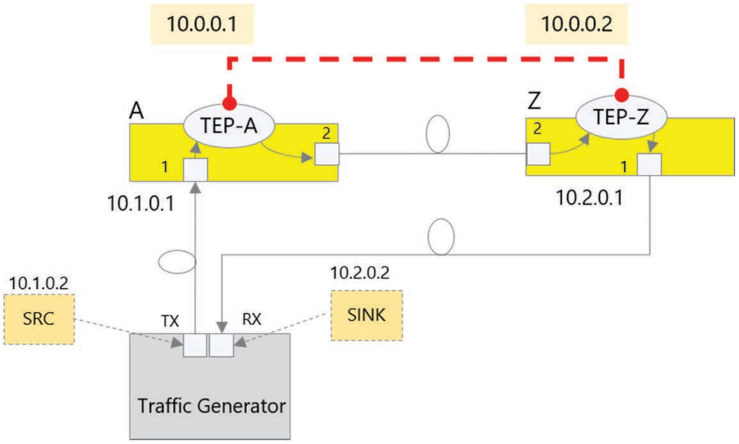

Figure 5 A test system with ECPA (Etherjack Connection Performance Analysis) over 10 GbE fiber.

6.1 Testbed Setup

A block diagram of the test system is depicted in Figure 5. The eCPRI traffic between a source node (IP: 10.1.0.2) and a sink node (IP: 10.2.0.2) is simulated by Traffic Generator (ADVA FSP 150 XG116Pro embedded with a traffic generator and an analyzer, allowing the latency measurement with resolution of 50 ns). Network elements A and Z are connected via a 10 GbE fiber link and an IP tunnel is established between A and Z.

The source node generates a specific size of IP packets with different rates; each packet has a sequence ID which is encoded in the IP payload. The traffic is forwarded by A and Z towards the traffic analyzer where the latency of the packet is measured. In order to avoid IPv4 fragmentation and re-assembly of the tunneled traffic, each packet is generated in the length of 1420 bytes.

Network elements A and Z are based on x86 platforms (Xeon-D SoC D-2166NT@2.0 GHz and D-1559@1.5 GHz), running Ubuntu 18.04 with kernel version of 4.15.0. The BIOS and Linux OS are configured in such a way that the maximum CPU frequency is kept.

6.2 Analysis

The purpose of experiments is to estimate the latency added by an encryption/decryption process. Hence, we do not perform an exhaustive performance evaluation of state-of-the-art IP forwarding. Instead, we use the

Table 3 Experimental results – throughput and latency

Case	Throughput (Gbps)	Latency avg. (μs)	Latency min. (μs)
Baseline 1	5	30	12
Baseline 2	5	74	20
Baseline 3	2	108	32

regular Linux kernel stack as a simple performance baseline and benchmark an impact of the encrypted tunnel.

We tested the following cases:

(1) Baseline 1: single D-2166NT IP forwarding;
(2) Baseline 2: two routers D-2166NT and D-1559 IP forwarding; and
(3) Baseline 3: Baseline 2 + WireGuard tunnel.

For each case, we measured throughput, average latency, and the minimum latency. We generated a single stream of IP packets with a payload of 1420-byte length.

The average latency of the single node IP forwarding is 30 μs. Comparing Baseline 1 with Baseline 2, we can see that the second IP router adds $74 - 30 = 44$ μs latency on average, which is explained by lower CPU frequency of D-1559: the frequency ratio is 2 GHz/1.5 GHz $= 1.33$, the latency ratio is 44 μs/30 μs $= 1.47$. For the case 3 that WireGuard tunneling is used in Baseline 2, WireGuard tunnel processing adds $108 - 74 = 34$ μs to overall latency on average. We assume that individual router latency contribution follows the CPU frequency ratio, i.e. D-2166 takes 15 μs and D-1559 takes 19 μs, respectively.

6.3 Discussion

In [5], the BBU processing time is found to be 2754 μs, leaving a maximum of 246 μs to the fronthaul path's round-trip time, a one-way delay of 123 μs. Hence, a one-way fronthaul latency should be 100 μs for the best performance [2].

However, one may not expect that software-based tunneling protocols could satisfy strict latency requirements even the packet processing is accelerated by DPDK [26] or XDP [27]. An average latency of software-based packet forwarding (1500 Bytes) is 7 μs (XDP) and 3 μs (DPDK) [28]. Adding encryption/decryption processing in software will cost an extra latency which might exceed 100 μs.

Let D denote the maximum transmission distance of an optical fronthaul. The sum of transmission delays and baseband processing time at BBU must be less than 3 ms. Note that the round-trip transmission latency of an optical fiber is 10 µs/km. According to [5], the round-trip delay components are

- Typical processing time: RF (40 µs), eCPRI (10 µs) and BBU (2700 µs)
- Fronthaul equipment processing delay: 4 µs [1]

Suppose that the encryption/decryption processing time takes T µs. Then, the distance D (in kilometers) is determined as follows:

$$\begin{aligned} \mathrm{D} &= (3\,\mathrm{ms} - 40\,\mu\mathrm{s} - 10\,\mu\mathrm{s} - 2700\,\mu\mathrm{s} - 4\,\mu\mathrm{s} - T)/10\,\mu\mathrm{s/km} \\ &= 24.6 - 0.1 \times T\,(\mathrm{km}) \end{aligned}$$

As our experimental results show, the one-way encryption/decryption processing in software adds about 34 µs to the "regular" IPv4 packet forwarding time. Hence, for a round-trip processing, the distance

$$\mathrm{D} = 24.6 - 0.1 \times 2 \times 34 = 17.8\,\mathrm{km},$$

i.e. the maximum transmission distance of a fronthaul link needs to be reduced by around 28%.

Note that we put the results of non-optimized software implementation as a base line. It might be improved by using a hardware crypto accelerator. Hence, the next step would be to evaluate an FPGA based implementation of (selected) secured tunneling protocols, which accelerate the encryption/decryption processing speed, allowing a longer transmission distance for the secure optical fronthaul.

7 Conclusion and Future Plan

It is of importance to ensure the security of fronthaul network while maintaining low latency for 5G services. The eCPRI specification puts the use of security protocols such as MACsec and IPsec as an option for the security of the fronthaul transport network. We found out that WireGuard has potential to replace IPsec due to its speed and simplicity. According to our analysis, the extended eCPRI transport overhead induced by security protocols has negligible impact on the latency. However, the processing time of cryptographic operations may cause a non-negligible latency, which results in a significant reduction on the maximum transmission distance between RRH and BBU. Even quantum-resistant MACsec, IPsec and WireGuard would be more challengeable due to their enlarged key size and increased computational complexity. It would be interesting to see whether hardware assisted cryptographic computation could minimize the latency of security protocols. We also pointed out that a re-key interval should be carefully configured for a high-speed link of the fronthaul since the security level can be bounded by the maximum amount of data that are encrypted with a single key.

Acknowledgments

This research is co-funded by the Federal Ministry of Education and Research of Germany Project QuaSiModO under grant agreement No. 16KIS1051.

References

[1] CPRI, "Common Public Radio Interface eCPRI Interface Specification V1.2," 2018. [Online].

[2] S. Bjørnstad, D. Chen and R. Veisllari, "Handling Delay in 5G Ethernet Mobile Fronthaul Networks," in *European Conference on Networks and Communications (EuCNC)*, 2018.

[3] 3GPP, "3G security; Network Domain Security (NDS); IP network layer security (Release 16). TS 33.210 V16.1.0," 2019.

[4] K. Shaneman and S. Gray, "Optical network security: technical analysis of fiber tapping mechanisms and methods for detection amp; prevention," *IEEE MILCOM 2004. Military Communications Conference*, vol. 2, p. 711–716, 2004.

[5] H. J. Son and S. Shin, "Fronthaul Size: Calculation of maximum distance between RRH and BBU," [Online]. Available: https://www.netmanias.com/en/post/blog/6276/c-ranfronthaul-lte/fronthaul-size-calculation-of-maximum-distance-between-rrhand-bbu.

[6] S. Kumar, "Simulating DDoS Attacks on the US Fiber-Optics Internet Infrastructure," in *Proceedings of the 2017 Winter Simulation Conference*, 2017.

[7] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring.," *35th annual IEEE symposium on the foundations of computer science*, 1994.

[8] N. J. Gomes et al., "Boosting 5G Through Ethernet: How Evolved Fronthaul Can Take Next-Generation Mobile to the Next Level," *IEEE Veh. Technol. Mag.*, vol. 13, p. 74–84, 2018.

[9] IEEE, "Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," IEEE Std. 1588–2008.

[10] IEEE, "Precision clock synchronization protocol for networked measurement," IEEE Std. 1588–2008.

[11] 3GPP, "Study on the security aspects of the next generation system (Release 14), TR 33.899 V1.3.0," 2017.

[12] IEEE, "Local and metropolitan area networks–Media Access Control (MAC) Security," IEEE Std 802.1AE.

[13] IEEE, "Standard for local and metropolitan area network – port-based network access control. IEEE 802.1X-2010."

[14] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP," 2013. [Online]. Available: https://tools.ietf.org/html/rfc2560.

[15] J. Donenfeld, "WireGuard: Next Generation Kernel Network Tunnel," [Online]. Available: https://www.wireguard.com/papers/wireguard.pdf.

[16] Y. Nir and A. Langley, "ChaCha20 and Poly1305 for IETF Protocols," 2018. [Online]. Available: https://tools.ietf.org/html/rfc8439.

[17] C. Wood, T. Enghardt, T. Pauly, C. Perkins and K. Rose, "A Survey of Transport Security Protocols," 2019. [Online]. Available: draft-ietf-tap s-transport-security.

[18] B. Lipp, B. Blanchet and K. Bhargavan, "A Mechanised Cryptographic Proof of the WireGuard Virtual Private Network Protocol," in *IEEE European Symposium on Security and Privacy (EuroS&P'19)*, 2019.

[19] A. Luykx and K. Paterson, "Limits on Authenticated Encryption Use in TLS – Information Security," 2017. [Online]. Available: http://www.isg.rhul.ac.uk/k̃p/TLS-AEbounds.pdf.

[20] IEEE, "MAC Security (MACsec) – Extended Packet Numbering," IEEE 802.1AEbw-2013.

[21] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen and T. Kivinen, "The Internet Key Exchange Protocol Version 2 (IKEv2). IETF RFC 7296," 2014.

[22] L. Chen, S. Jordan, Y. Liu, D. Moody, R. Peralta, R. Perlner and D. Smith-Tone, "Report on Post-Quantum Cryptography, NISTIR 8105," 2016.

[23] A. Langley, M. Hamburg and S. Turner, "Elliptic Curves for Security," IETF RFC 7748, 2016.

[24] B. B. K. B. Benjamin Lipp, "A Mechanised Cryptographic Proof of the WireGuard Virtual Private Network Protocol," June 2019. [Online]. Available: https://hal.inria.fr/hal-02100345v2/document.

[25] J. Appelbaum, C. Martindale and P. Wu,, "Tiny WireGuard Tweak," Cryptology ePrint Archive, Report 2019/482, 2019.

[26] DPDK, “Data Plane Development Kit,” [Online]. Available: https://www.dpdk.org.

[27] “XDP: eXpress Data Path,” IO Visor Project, [Online]. Available: https://www.iovisor.org/technology/xdp.

[28] T. Høiland-Jørgensen, J. Brouer, D. Borkmann, J. Fastabend, T. Herbert, D. Ahern and D. Miller, “The eXpress Data Path: Fast Programmable Packet Processing in the Operating System Kernel,” [Online]. Available: https://github.com/xdp-project/xdp-paper/blob/master/xdp-the-express-data-path.pdf.

Biographies

Joo Yeon Cho received the Ph.D. degree in cryptography from the Macquarie University, Australia, in 2007. He has worked on the research and development of cryptography and data security for more than 10 years. He is currently a Principal Engineer in the Advanced Technology group at ADVA Optical Networking in Munich, Germany. His expertise comprises cryptography, network security, cryptanalysis and cybersecurity.

Andrew Sergeev is currently a senior principal engineer in the Advanced Technology department at ADVA Optical Networking, actively participating in various projects in the field of Network Function Virtualization (NFV) and of modern cryptography. Andrew has broad hands-on experience in software development, system engineering and design for data communications and wireless data services. He is the author of more than twenty inventions in the networking area. Andrew graduated from the Saint Petersburg State Electrotechnical University with a M.Sc. in electrical engineering.

Shihuan (Jim) Zou is currently a senior engineer in the Advanced Technology department at ADVA Optical Networking SE, Germany, participating in various EU FP7 and Horizon-2020 research projects. He is also a core member of PLM Access Solution team, responsible for product roadmap, prototyping, and business development support related to the next generation optical access technologies. He received his B.Eng. in communication and information engineering and M.Sc. in electrical circuits and systems from Shanghai University, China, in 2008 and 2011, respectively. In 2015, he received the PhD degree from the Eindhoven University of Technology, The Netherlands, where he conducted the research work with Electro-Optical Communication (ECO) group of COBRA research institute in the area of broadband indoor fiber-wireless networks.