Unlicensed Integration with 5G Networks

WBA 5G Workgroup

Source: WBA Members
Author(s): 5G Workgroup
Issue date: October 2018
Document status: Final

ABOUT THE WIRELESS BROADBAND ALLIANCE

Founded in 2003, the mission of the Wireless Broadband Alliance (WBA) is to accelerate global leadership for enabling of wireless services that are seamless, secure and interoperable. Building on our heritage of Next Generation Hotspot (NGH) and carrier Wi-Fi, the WBA will continue to drive and support the adoption of Next Generation Wireless services across the entire public Wi-Fi ecosystem, including IoT, Converged Services, Smart Cities, 5G, etc. Today, membership includes major fixed operators such as BT, Comcast and Charter Communications; seven of the top 10 mobile operator groups (by revenue) and leading technology companies such as Cisco, Microsoft, Huawei Technologies, Google and Intel.

The WBA Board includes AT&T, Boingo Wireless, BT, Cisco Systems, Comcast, Intel, KT Corporation, Liberty Global, NTT DOCOMO and Orange. For a complete list of current WBA members, please **click here**.

Follow Wireless Broadband Alliance at:

www.twitter.com/wballiance

http://www.facebook.com/WirelessBroadbandAlliance

https://www.linkedin.com/company/wireless-broadband-alliance/

UNDERTAKINGS AND LIMITATION OF LIABILITY

This Document and all the information contained in this Document is provided on an ‘as is’ basis without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for particular purpose, or non-infringement.

In addition, the WBA (and all other organisations who may have contributed to this document) makes no representations or warranties about the accuracy, completeness, or suitability for any purpose of the information. The information may contain technical inaccuracies or typographical errors. All liabilities of the WBA (and all other organisations who may have contributed to this document) howsoever arising for any such inaccuracies, errors, incompleteness, suitability, merchantability, fitness and non-infringement are expressly excluded to the fullest extent permitted by law. None of the contributors make any representation or offer to license any of their intellectual property rights to the other, or to any third party. Nothing in this information or communication shall be relied on by any recipient.

The WBA also disclaims any responsibility for identifying the existence of or for evaluating the applicability of any claimed copyrights, patents, patent applications, or other intellectual property rights, and will take no position on the validity or scope of any such rights. The WBA takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any effort to identify any such rights.

Neither the WBA nor any of the other organisations who may have contributed to this document will be liable for loss or damage arising out of or in connection with the use of this information. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory, direct, indirect or consequential damages, loss of data, income or profit, loss of or damage to property and claims of third-parties.

CONTENTS

Executive Summary

The integration of un-licensed Wi-Fi networks with licensed cellular networks has been a topic that has been repeatedly discussed over the past 15 years or more. There has been an evolution in requirements over this extended period, moving from “switched-mode” or handover use cases where only a single access is used at any time, towards a “split-mode” use case where a device may have simultaneous access to multiple accesses over prolonged periods of time.

This paper provides an analysis of the varied approaches for integrating cellular and Wi-Fi networks, ranging from solutions where Wi-Fi is integrated into the cellular access-stratum, those that integrate Wi-Fi into the cellular non-access stratum core network, to those that integrate Wi-Fi above-the-core network using IETF defined multi-path protocols.

The paper provides detailed descriptions of the latest capabilities specified in 3GPP Release 15 and currently being studied as part of 3GPP Release 16 for integrating Wi-Fi into the 5G Core Network. The paper provides details of alternative multi-path protocol approaches which have been used to provide improved experiences when devices are simultaneously connected to cellular and Wi-Fi networks.

The findings of the working group conclude that the most likely techniques to be adopted are where Wi-Fi is either integrated into 5G using core-centric techniques, or integrated using multi-path above-the-core techniques. Moreover, the widescale deployment of multipath based solutions has led to the inclusion of such approaches into the 3GPP defined Release 16 5GCN centric integration.

In contrast to the broad alignment across the industry to focus on Wi-Fi as a peer the cellular access-network, with dual mode multi-path solutions from a user plane perspective, there is less alignment on the critical aspect of control plane and policy. The paper calls out the critical path management functionality as an area that can benefit from the use of a policy framework to facilitate efforts to deliver enhanced experiences over multi-path solutions. Such a framework needs to examine algorithms for policy combining that can support the broad range of use cases covered in this paper.

Finally, the paper provides a set of recommendations about areas of study which the WBA and other stakeholders can use to address some of the issues raised in this paper and a call to action for the industry to address these issues.

1 Introduction

The integration of un-licensed Wi-Fi networks with licensed cellular networks has been a topic that has been repeatedly discussed over the past 15 years or more. With recent reports characterizing smartphone use highlighting that over 70% of mobile data traffic is sent over Wi-Fi networks [1] there continues to be an opportunity to improve user experiences by better being able to integrate these disparate networks.

However, there has been an evolution in requirements over this extended period, moving from “switched-mode” handover use cases, where only a single access is used at any time, towards “split-mode” use cases, where a device may have simultaneous access to multiple accesses over prolonged periods of time and may be able to benefit from splitting connectivity over multiple simultaneous accesses, including being able to enhance performance by combining the connections available over these multiple access networks.

This has prompted WBA to define the different categories of integration in its early analysis of Wi-Fi and 5G [2], introducing three broad approaches of how to integrate Wi-Fi and 5G networks introduced:

- **Access Centric Integration:** these approaches were first introduced in Release 13 for LTE based access, with LTE WLAN Aggregation (LWA) for integrating trusted Wi-Fi with LTE and LWIP for integrating untrusted Wi-Fi. These approaches are described in greater detail in [3].
- **Core-Centric Integration**: these approaches were initially standardised in Release 8 for the integration of un-trusted Wi-Fi via an ePDG and in Release 11 for integrating trusted Wi-Fi into LTE’s Evolved Packet Core, as described in [4].
- **Above-the-Core integration**: using techniques such as Multi-Path TCP and Multi-Path Quick UDP Internet Connection (QUIC). More recently these new protocols have been proposed to enable integration between Wi-Fi and cellular networks.

Note, that these three alternative integration approaches can all be used support split-mode operation, with switched-mode being supported by access-centric and core-centric solutions.

Note, as described above, these definitions are well adapted to address earlier Wi-Fi integration approaches based on LTE. Moving forward, section 2 describes how the specification of 5G defines the use of the Non-3GPP Interworking Function to enable a Wi-Fi based non-3GPP access networks to present the same interfaces as exposed by the 5G New Radio (NR) Access Network. As integration is achieved via a common 5GCN, we still look to characterize this Release 15 solution as “core-centric integration”.

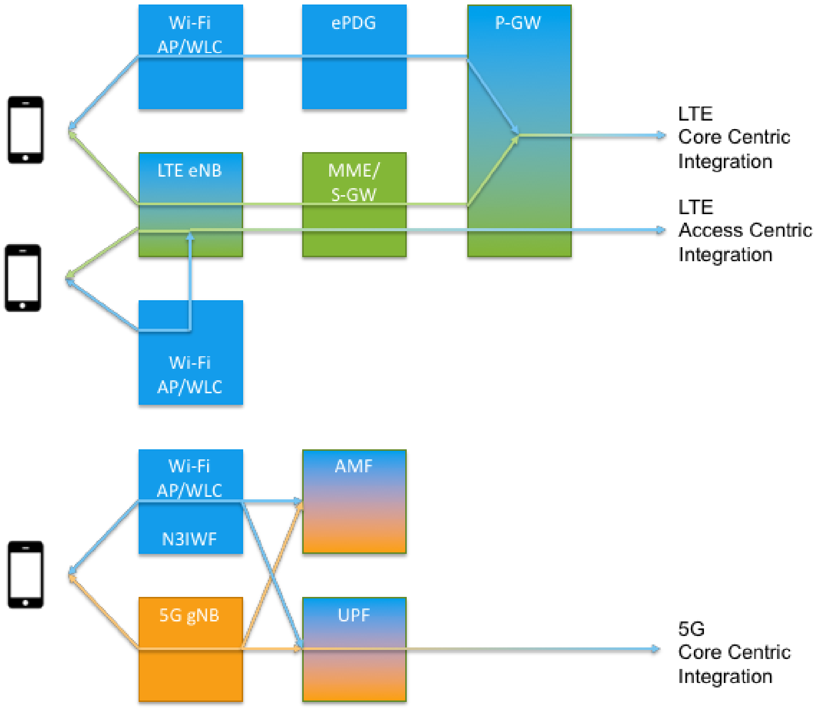
Wi-Fi AP/WLC
ePDG
P-GW
LTE eNB
MME/ S-GW
LTE Core Centric Integration
LTE Access Centric Integration
Wi-Fi AP/WLC
Wi-Fi AP/WLC
N3IWF
AMF
5G gNB
UPF
5G Core Centric Integration

Figure 1-1: Access and Core-Centric Integration – shaded functions indicate common functions that deliver functionality for supporting use Wi-Fi

The remainder of this section introduces the broad characteristics associated with these three alternative approaches to Wi-Fi integration.

1.1 Access Centric Integration

Wi-Fi integration using access-centric integration was introduced in 3GPP Release 13, with LTE WLAN Aggregation (LWA) first defining how a trusted WLAN infrastructure could be integrated into an enhanced eNB, followed by LTE WLAN integration with IPsec tunnel (LWIP) defining how an untrusted WLAN infrastructure could be integrated into an enhanced eNB.

The definition of such solutions could be viewed as a response to access centric un-licensed integration based on Licensed Assisted Access (LAA) which defines a modified LTE waveform for use as a supplemental down-link operating in un-licensed 5GHz spectrum. Proponents of LWA/LWIP argue that as LWA/LWIP solutions are based on the standard 802.11 waveform, there should be less of a concern about interference and coexistence with legacy users of the 5GHz band, as well as the ability of LWIP to leverage already installed Wi-Fi systems.

These solutions have been subsequently enhanced in 3GPP Release 14, with enhanced LWA (eLWA) defining the support for up-link data over the Wi-Fi as well as 60 GHz support, and enhanced LWIP (eLWIP) defining flow control and measurements for the untrusted Wi-Fi use case.

> Note, at the time of writing, there is no equivalent work to define an access-centric integration for Wi-Fi into the 5G Access Stratum.

1.2 Core Centric Integration

Core centric integration within a 5G deployment can either be achieved using Non-Stand Alone (NSA) or Stand Alone (SA) configuration. Significantly, there are a number of architectural options of how to deploy 5G and these are illustrated in **Figure 1-2** [5].

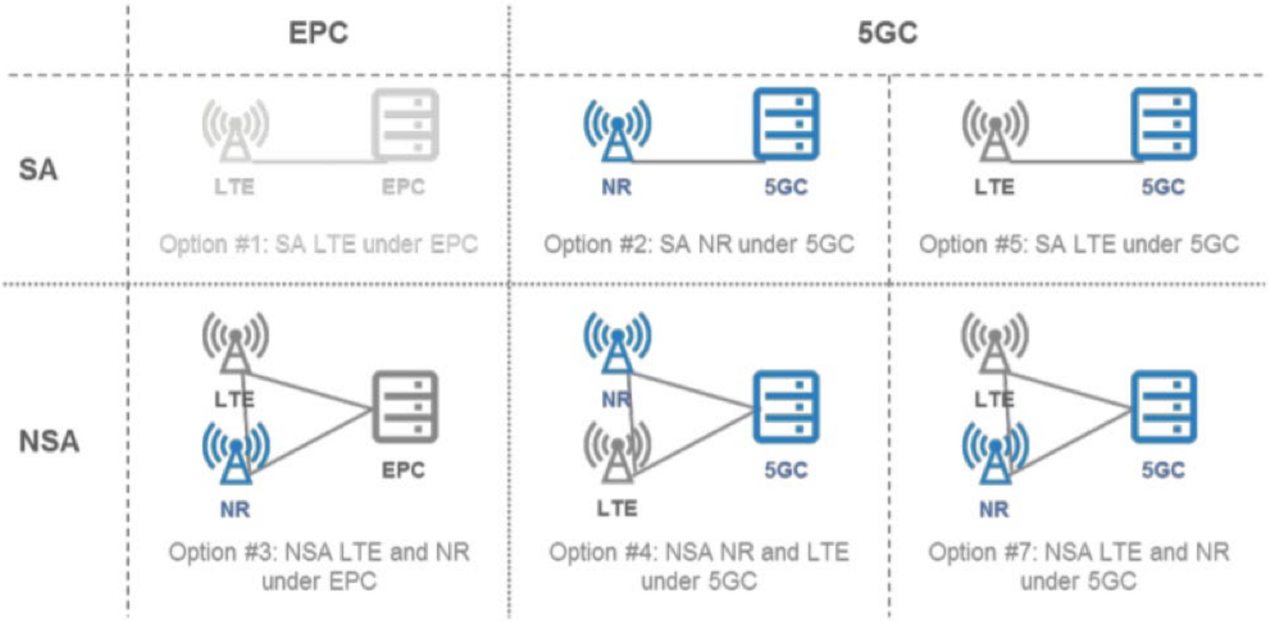
EPC
5GC
SA
NSA
LTE
EPC
Option #1: SA LTE under EPC
NR
5GC
Option #2: SA NR under 5GC
LTE
5GC
Option #5: SA LTE under 5GC
LTE
NR
EPC
Option #3: NSA LTE and NR under EPC
NR
LTE
5GC
Option #4: NSA NR and LTE under 5GC
LTE
NR
5GC
Option #7: NSA LTE and NR under 5GC

Figure 1-2: 5G Deployment Options for Stand Alone (SA) and Non Stand Alone (NSA) Configuration

In particular, NSA Option #3 enables the current EPC to be leveraged for supporting the deployment of 5G New Radio. Such an approach then facilitates the use of the traditional ePDG based approach for delivering core-centric Wi-Fi integration, even within a Release 15 New Radio deployment.

When deploying 5G New Radio using Stand Alone configuration, or NSA Options #4 or #7, core-centric Wi-Fi integration can leverage the latest Release 15 Non-3GPP Interworking Function (N3IWF) to enable Wi-Fi integration into the 5G Core Network. This 5G-based core-centric integration is the focus of Section 2. This section describes in greater detail the architectures used to support “untrusted” non-3GPP access networks in 3GPP Release 15. In addition, Section 2 summarizes the latest developments as it relates to Release 16 definitions of Trusted non-3GPP integration, as well as techniques being considered for supporting traffic splitting, steering and switching between Wi-Fi and cellular networks being specified as part of 3GPP Release 16.

> Note that the GSMA is promoting NSA Option 4 and NSA Option 7 as preferred 4G – to – 5G migration options. Their rationale is that without a 5G Core, the deployment of 5G NR will not provide compellingly different service, over 4G. If the GSMA preferred approach bears out, the non-3GPP – access to 5GC modes will be likely provide the foundation for unlicensed interoperability scenarios.

1.3 Above-the-Core Integration

In contrast to looking to solve mobility with single-path like switched/handover capabilities, above-the-core solutions recognize the increasing trend by which mobile devices have plurality of wireless interfaces simultaneously active. Instead of defining solutions that necessitate these interfaces all present a common IP address to the upper layers, multi-path approaches enable each individual interface to be independently addressable. This independent addressing then facilitates deployment scenarios where different entities can be responsible for managing the access networks associated with the different interfaces, and hence why the term “above-the-core” has been adopted by WBA to describe such approaches.

Being able to leverage independent access and connectivity networks may enable above-the-core solutions to deliver an interesting set of capabilities, including:

1. When the different access networks exhibit different delay characteristics between the device and the remote host, above-the-core solutions can selectively decide to use only the lower latency path to deliver improved user interaction
2. When the different access networks are deployed in different environments, e.g., one deployed indoors and another deployed outdoors, the above-the-core solutions can use the multi-path capability to handle the transition between the access network coverage areas.
3. When the different access networks have different probability of coverage capabilities, e.g., providing reliable wide area coverage versus un-reliable local area coverage, the above-the-core solutions can use the multi-path capability to opportunistically leverage the local area coverage whilst having an “anchor path” over the wide area network
4. When different access networks are deployed by different organizations, e.g., one deployed by a carrier Wi-Fi provider and another by a Cellular Service Provider, the above-the-core solutions can provide the ability to aggregate the connections with different IP points of attachment.

Note: recently, solutions based on multi-path protocols have been proposed to enable the steering, switching and selection of alternative paths within 3GPP’s Release 16 core-centric architecture, see sub-section 2.2.2 and 3GPP TR 29.793 [6] for more details.

2 5GC Wi-Fi Integration

2.1 R15 N3IWF

2.1.1 5GC Intro

3GPP Release 15 architecture supports access to the 5G system using both 5G NR as well as via non-3GPP access networks. In release 15, only untrusted non-3GPP access is supported. It is expected that Release 16 will provide both trusted/managed non-3GPP access (covered in the next section), as well as fixed wireline/wireless access (out of scope of this whitepaper).

The 5G Core Network (5GCN) architecture defines the clear separation of the control plane and user plane functions. In the 5GCN, one or more User Plane Function (UPF) instances can be used to anchor a single PDU session under the control of the Session Management Function (SMF). Besides the SMF and UPF, an important function is played the Access and Mobility Management Function (AMF) which replaces the MME.

A Non-3GPP Inter-Working Function (N3IWF) has been defined as part of the untrusted non-3GPP access, as illustrated in Figure 2-1. Importantly, the 5GCN has been defined to be access agnostic. Both 5G NR and non-3GPP access are interfaced to the 5G Core using the same user plane (N3) and control plane interfaces (N2), with the N3IWF terminating N2 and N3 interfaces when using non-3GPP access.

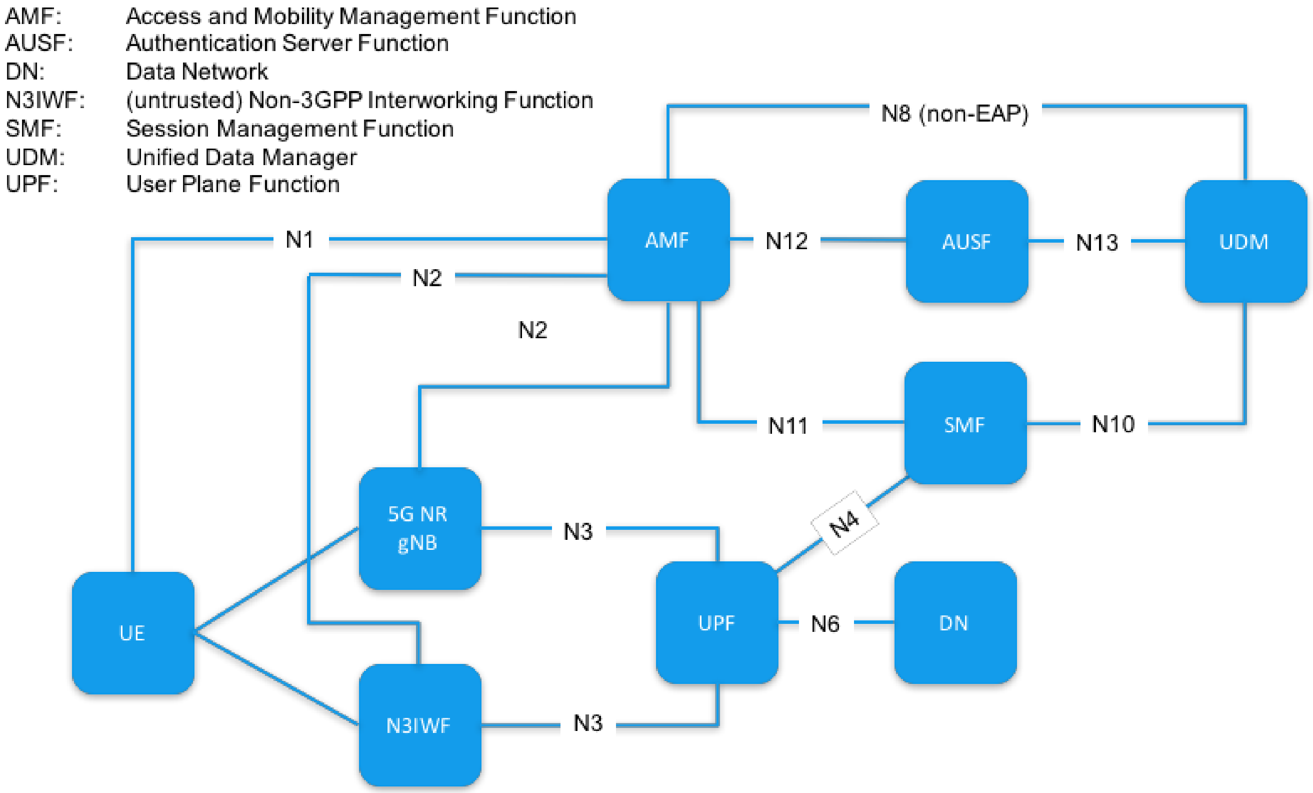
AMF: Access and Mobility Management Function
AUSF: Authentication Server Function
DN: Data Network
N3IWF: (untrusted) Non-3GPP Interworking Function
SMF: Session Management Function
UDM: Unified Data Manager
UPF: User Plane Function
N8 (non-EAP)
N1
AMF
N12
AUSF
N13
UDM
N2
N2
N11
SMF
N10
5G NR
gNB
N3
N4
UE
UPF
N6
DN
N3IWF
N3

Figure 2-1:5G Release 15 System Architecture

While the N3IWF may look functionally similar to the ePDG of earlier releases, a key difference between these approaches is that, unlike the ePDG which has been considered a core network element, the N3IWF is a peer of the 5G New Radio gNB and implements the N2 and N3 interfaces used to integrate the 5G Access Network to the 5GCN's Control Plane and User-Plane elements respectively.

> Note, 3GPP does not define the location of an N3IWF, but as it needs to terminate flows generated from devices operating on third party networks, it is likely to be located in a more centralized location, e.g., when compared to the 5G gNB.

2.1.1 5G Session Definition

Compared to LTE which defined the concept of a "default bearer" which is automatically established on registration, the 5G core defines how Protocol Data Unit (PDU) sessions are established. Additionally, whereas LTE defined "dedicated bearers" which had an associated set of packet filters to identify the corresponding IP traffic in the PGW and UE, in 5G the concept has been renamed, with "packet filter sets" being used to identify a QoS flow.

Another key enhancement delivered with 5G is that whereas in LTE only an IP and non-IP based PDU Session Types were defined (the latter used for IoT use cases), 5G has introduced the Ethernet PDU Session Type, with packet filter sets using MAC addresses to distinguish between different Ethernet frames.

2.1.2 N1/N2/N3 Interface Introduction

As illustrated in **Figure 2-1**, the UE uses the N1 connection to signal non-radio signalling between the UE and the AMF. Referred to as "Non-Access Stratum" (NAS) signalling, this is used by the 5G System for:

i) Managing the mobility between the user equipment (UE) and the AMF for both 3GPP access and non-3GPP access; and

ii) Managing the session between the user equipment (UE) and the SMF for both 3GPP access and non-3GPP access.

As described in [7], from the UE's NAS perspective, in general, common procedures and messages defined for 5G Mobility Management and 5G Session Management are used over both non-3GPP access as over 3GPP access. However, there are a few notable areas of difference:

- The registrations over 3GPP access and non-3GPP access are performed separately, using independent state machines and enabling the registered Public Land Mobile Network (PLMN) to differ between the two access networks.
- A single registration area is used over the entire non-3GPP access network, which is associated with a fixed well known Non 3GPP Tracking Area Idendtifier. As a consequence, registration updating due to movement within the same non-3GPP access network is not required and paging is not performed via non-3GPP access.
- The network-initiated servce request procedure is not supported over non-3GPP access, instead the system relies on UE-initiated service requests.

The N2 interface is used to support control plane signalling between the access network and the 5GCN [8]. In most cases the procedures defined for N2 apply equally to access via 5G Access Network and Non-3GPP Access, including:

- General N2 interface management procedures
- Non Access Stratum (NAS) transport capabilities, albeit with some differences for the signalling of access specific user location information (UE local IP addresses are used for locations over untrusted non-3GPP versus cell-ID for access over 3GPP)
- UE context management procedures
- PDU session resource management procedures

However, in Release 15, the N2 defined procedures for handover-management are only intended to be used with 3GPP access.

The N3 interface is used to support per-PDU session user plane tunnelling between the Access Network and the UPF. GTP-U is used to multiplex the different PDU sessions by tunnelling data over N3. Importantly, compared to LTE that had a direct mapping between S1 tunnel and the Radio Bearer, the 5G system transports the QoS Flow ID marking within the tunnel, enabling the mapping of flows to radio bearers to be performed in the access network.

2.1.3 Non-Access Stratum Services during network registration

When the UE decides to attach to 5GC network, the UE selects an N3IWF in a 5G network, as described in TS 23.501 clause 6.3.6.

The UE proceeds with the establishment of an IPsec Security Association (SA) with the selected N3IWF by initiating an IKE initial exchange according to RFC 7296 [9]. After the initial IKE_SA_INIT exchange all subsequent IKE messages are encrypted and integrity protected by using the IKE SA established in this step.

The UE initiates an exchange of IKE_AUTH_Req/Resp with the N3IWF to authenticate with the 5G Core. The AUTH payload is not included in the first IKE_AUTH_Req message which indicates that the IKE_AUTH exchange shall use EAP signalling (in this case EAP-5G signalling). The N3IWF in this case operates as an EAP Proxy between UE and AUSF.

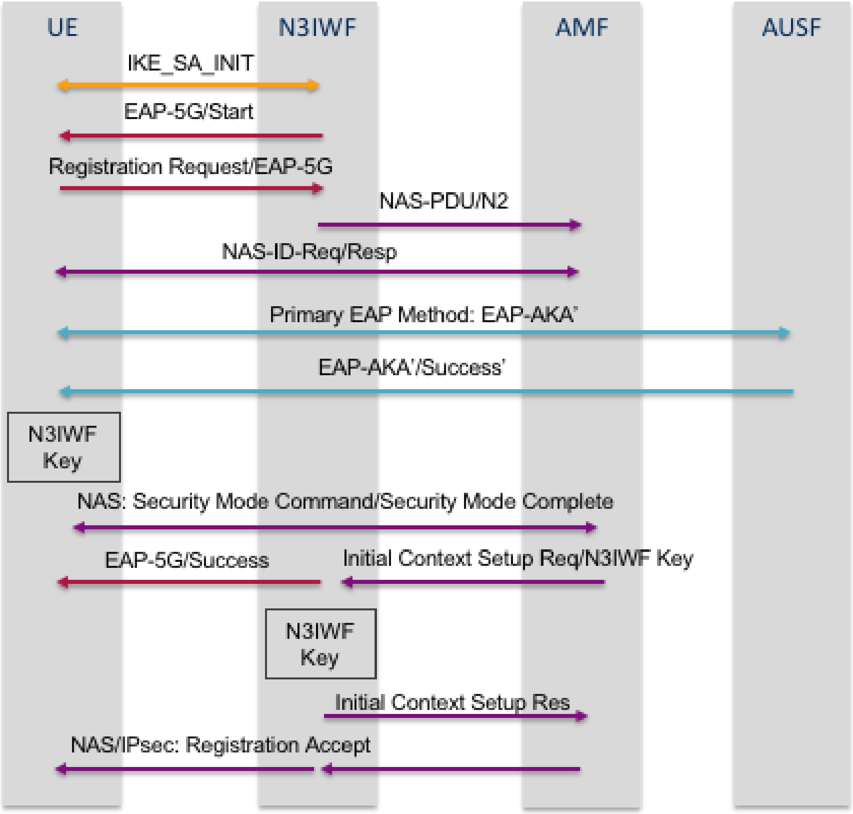
UE
N3IWF
AMF
AUSF
IKE_SA_INIT
EAP-5G/Start
Registration Request/EAP-5G
NAS-PDU/N2
NAS-ID-Req/Resp
Primary EAP Method: EAP-AKA'
EAP-AKA'/Success'
N3IWF Key
NAS: Security Mode Command/Security Mode Complete
EAP-5G/Success
Initial Context Setup Req/N3IWF Key
N3IWF Key
Initial Context Setup Res
NAS/IPsec: Registration Accept

Figure 2-2: Simplified sequence of Registration via untrusted non-3GPP access

The simplified message sequence illustrates the role of the two Extended Authentication Protocol methods: EAP-5G and EAP-AKA'.

Some text in TS 33.501 [10], covering this call-flow (modified to cater for this white paper) is as follows.

1. *The UE connects to an untrusted non-3GPP access network with procedures outside the scope of 3GPP and it is assigned an IP address.*
    a. *Any non-3GPP authentication method can be used, e.g. no authentication (in case of a free WLAN), EAP [any authentication method], etc.*
    b. *When the UE decides to attach to 5GC network, the UE selects an N3IWF. If we expect that the UE supports connectivity with N3IWF but does not support connectivity with ePDG (see Section 1.2), we expect the UE to carry out a "Stand-alone N3IWF selection" (see Section 6.3.6.2 of 3GPP TS 23.501). That is:*
        i. *A Tracking/Location Area Identifier FQDN shall be constructed by the UE based only on the Tracking Area wherein the UE is located. The N3IWF Tracking/Location Area Identifier FQDN may use the 5GS TAI when the UE is registered to the 5GS, or the EPS TAI when the UE is registered to EPS. The Location Area is not applicable on the 3GPP access.*
        ii. *The UE will use theN3IWF OI FQDN.*
        iii. *The N3IWF identifier configuration and the Non-3GPP access node selection information will be used, rather than their PDG counterparts.*
2. *The UE proceeds with the establishment of an IPsec Security Association (SA) with the selected N3IWF by initiating an IKE initial exchange. After this, all subsequent IKE messages are encrypted and integrity protected by using the IKE SA established in this step.*
3. *The UE shall initiate an IKE_AUTH exchange by sending an IKE_AUTH request message. The AUTH payload is not included in the IKE_AUTH request message, which indicates that the IKE_AUTH exchange shall use EAP signalling (in this case EAP-5G signalling). Compliant with TS 33.501, if the UE is provisioned with the N3IWF root certificate, it shall include the CERTREQ payload within the IKE_AUTH request message to request the N3IWF's certificate.*
4. *The N3IWF responds with an IKE_AUTH response message which includes an EAP-Request/5G-Start packet. The EAP-Request/5G-Start packet informs the UE to initiate an EAP-5G session, i.e. to start sending NAS messages encapsulated within EAP-5G packets. If the N3IWF has received a CERTREQ payload from the UE, the N3IWF shall include the CERT payload in the IKE_AUTH response*

> *message containing the N3IWF's certificate. How the UE uses the N3IWF's certificate is specified in TS 33.501 [10].*

As illustrated in **Figure 2-2**, when the UE completes the EAP-AKA' authentication a NAS security context and the N3IWF key are available at the UE. The N3IWF key is used to create a "signalling IPSec Security Association" between the UE and N3IWF, used to protect the exchange of further NAS messages between the UE and N3IWF. Subsequently the N3IWF has to receive the N3IWF key from AMF. If the N3IWF does not receive this key, then an EAP-Failure is signalled. Any further NAS messages exchanged between UE and AMF are carried between the UE and N3IWF using IPSec and this first security association. Further details of EAP aspects are included in sub-section 2.1.5.

2.1.4 N2 Procedures via untrusted Non-3GPPAccess

N2 procedures are used by the AMF to establish the access resources at the N3IWF for a PDU Session. As noted above, for non-3GPP access, PDU session establishment is always triggered by the UE signalling to the AMF using NAS procedures.

Based on the QoS profiles received from the AMF, the N3IWF determines the number of IPSec child SAs to establish and the QoS profiles associated with each of these IPSec child SAs. When establishing theses transport mode IPsec child SAs, the N3IWF uses a notify payload to signal the QFIs associated with child SA, the identity of the PDU session associated with the child SA and optionally a DSCP value associated with the child SA.

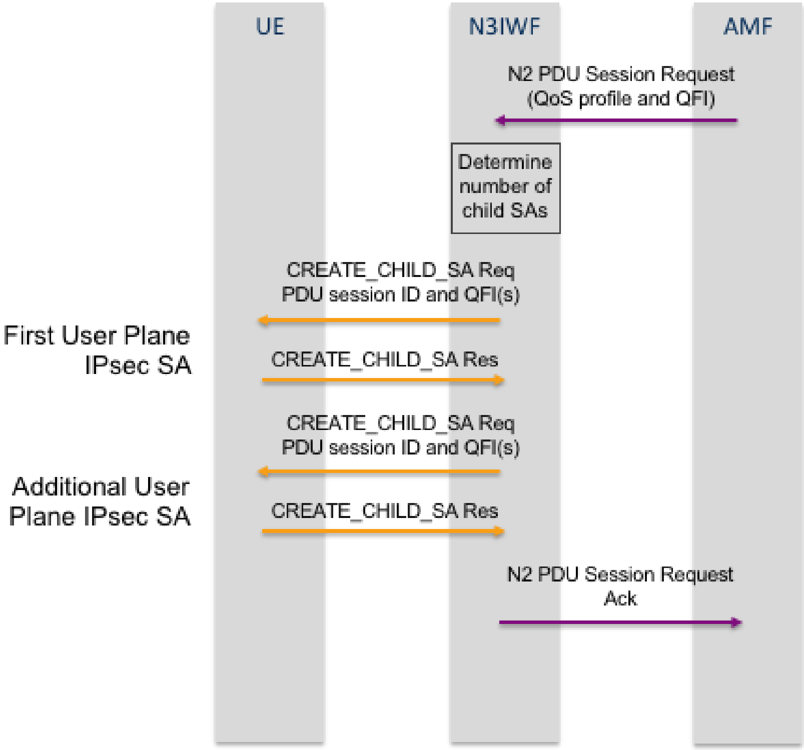
UE
N3IWF
AMF
N2 PDU Session Request
(QoS profile and QFI)
Determine number of child SAs
CREATE_CHILD_SA Req
PDU session ID and QFI(s)
First User Plane IPsec SA
CREATE_CHILD_SA Res
CREATE_CHILD_SA Req
PDU session ID and QFI(s)
Additional User Plane IPsec SA
CREATE_CHILD_SA Res
N2 PDU Session Request Ack

Figure 2-3: N2 signalling used to establish IPSec Child SAs

If the network needs to release the IKEv2 Security Association, e.g., if the UE is determined to be no-longer reachable over the non3GPP access, the network will use N2 signaling to initiate the release.

The AMF signals the context release to the N3IWF using an N2 message. The N3IWF may use an IKE Information Exchange message to signal the release reason to the UE.

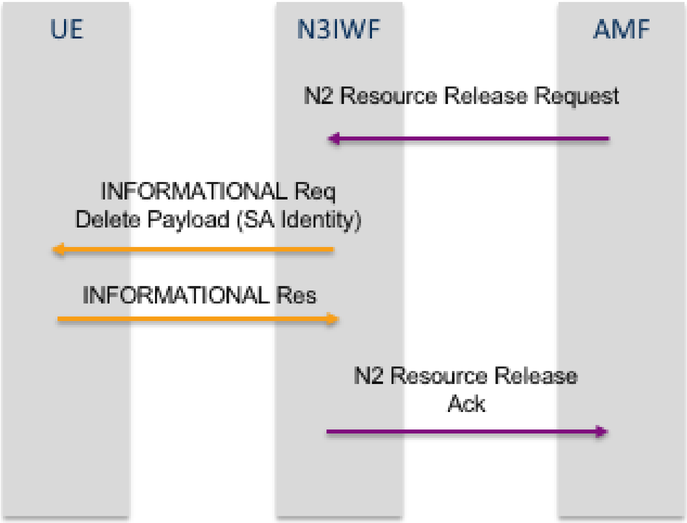

Figure 2-4: Interworking between N2 procedures and IKE information exchange

2.1.5 Use of EAP Procedures in Registration via Untrusted Non-3GPP Access

The 3GPP TS 23.502 Release 15 specification [11] describes procedures for registration via untrusted non-3GPP access. Section 4.2.8.1: states that only the support of non-3GPP access networks deployed outside the NG-RAN (referred to as "standalone" non-3GPP accesses) is described.

It also states:

> *When a UE is connected to a 3GPP access of a PLMN, if the UE selects the N3IWF and the N3IWF is located in a PLMN different from the PLMN of the 3GPP access, e.g. in a different VPLMN or in the HPLMN, the UE is served separately by the two PLMNs. The UE is registered with two separate AMFs. PDU Sessions over the 3GPP access are served by V-SMFs different from the V-SMF serving the PDU Sessions over the non-3GPP access.*
>
> *The PLMN selection for the 3GPP access does not depend on the N3IWF selection. If a UE is registered over a non-3GPP access network, the UE performs PLMN selection for the 3GPP access independently of the PLMN to which the N3IWF belongs.*

This means that, for Release 15 untrusted non-3GPP [Wi-Fi] access, the core selection is permitted to be independent of the PLMN access. Moreover, such a scenario enables the UE to combine the independent connections over 3GPP and non-3GPP access networks using an above-the-core solution, as described in section 3.

> Note, whereas Figure 2-1 shows a single AMF supporting 3GPP and non-3GPP access. the selection by the UE of a N3IWF corresponding to an independent PLMN will result two separate AMFs and SMFs being deployed. Such a scenario is illustrated in Figure 2-5 below.

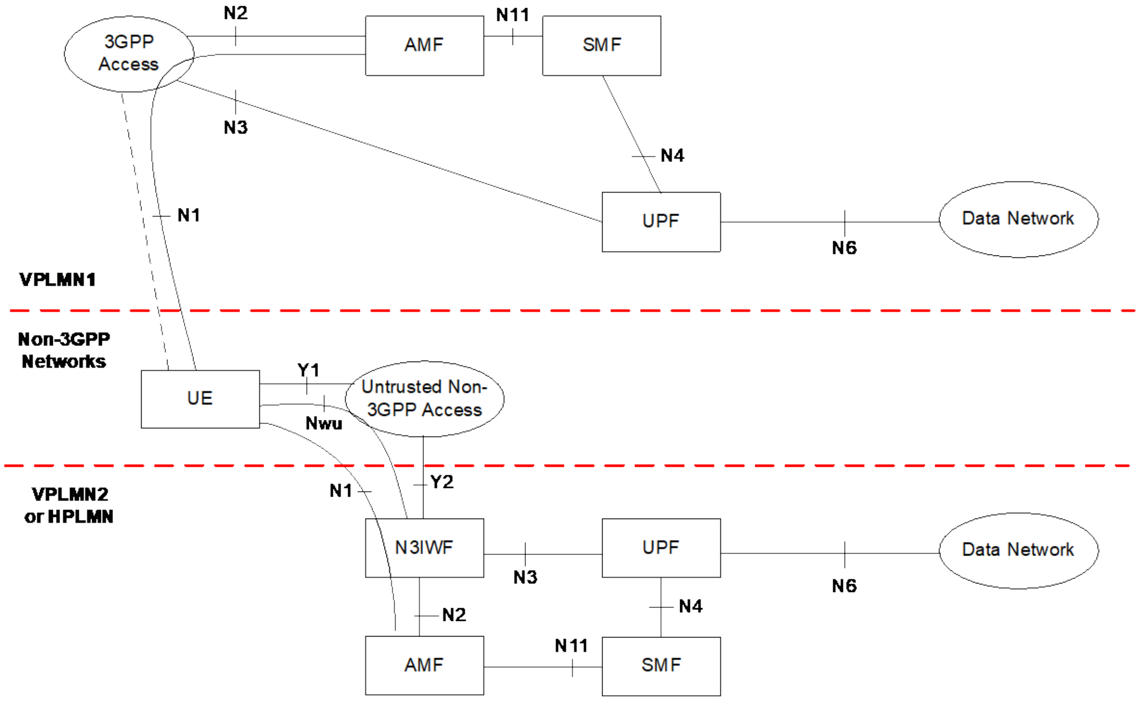

Figure 2-5: Roaming architecture for 5G Core Network with non-3GPP access – N3IWF in the different PLMN from the 3GPP access

2.1.6 PDU Sessions over non-3GPP Access networks

The user plane protocol stack for a PDU session over an untrusted non-3GPP access network is illustrated in Figure 2-6. The header of the GRE packet is used to carry the QoS information, including the QFI associated with a particular PDU and in the down-link an optional indication as to whether the UE should use reflective QoS over the non-3GPP access network.

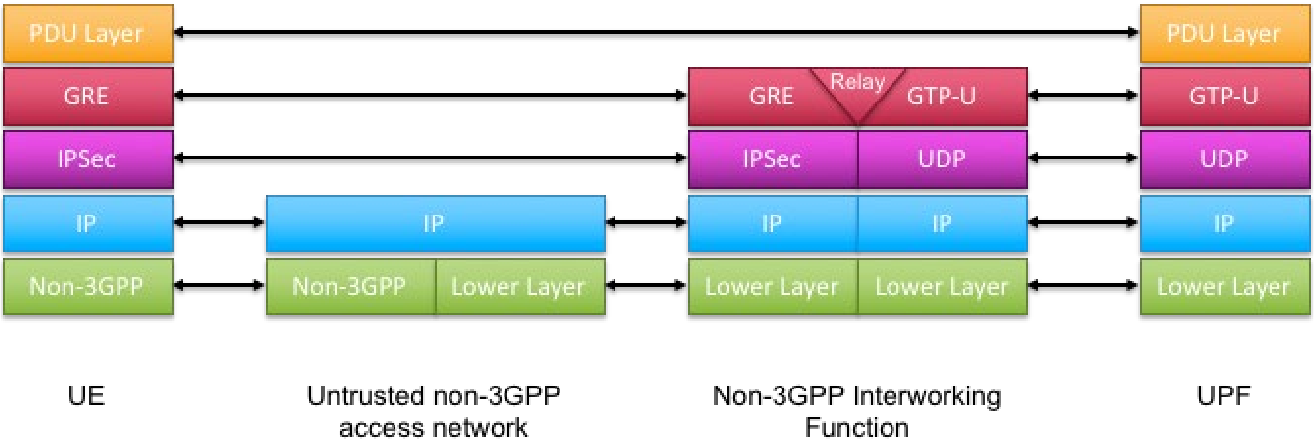

Figure 2-6: User Plane Protocol Stack for a PDU Session

The QFI is carried in an encapsulation header on N3 i.e. without any changes to the e2e packet header. QFI shall be used for all PDU Session Types. In the down-link direction, the N3IWF maps PDUs from QoS Flows to access-specific resources associated with the IPSec child SA, based on the QFI and the associated 5G QoS profile.

In the up-link, the N3IWF transmits the PDUs over N3 tunnels towards the UPF. When tunnelling up-link packets from the N3IWF to the UPF, the N3IWF includes the QFI value in the encapsulated packet towards the UPF.

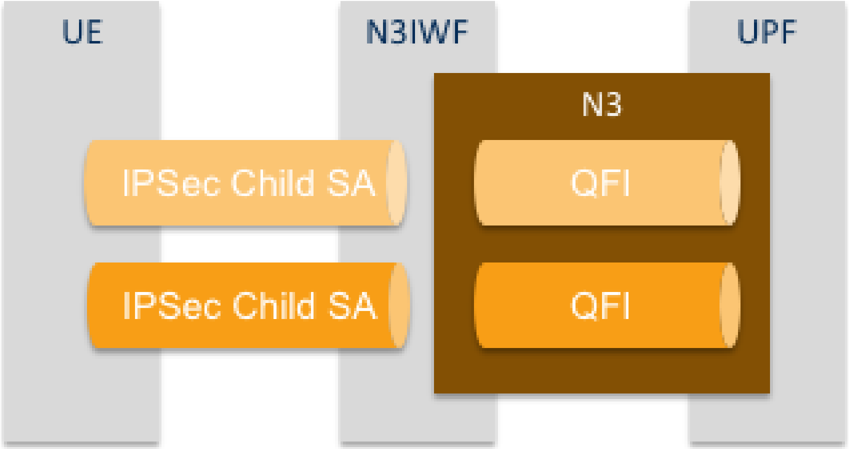

Figure 2-7: Mapping between QFI Profile(s) and IPSec Child SAs

2.1.7 Common Security Anchor/Authentication Framework/Keying Hierarchy

Previous generations of WLAN integration into 3GPP systems have largely been stand-alone from a security perspective. Independent keying hierarchies were used for 3GPP access and WLAN access, with the WLAN access hierarchy being based on an EAP generated Master Session Key.

In 5G System both control plane (N1-NAS) and user plane traffic between the terminal and the 5G Core are encrypted when the non-3GPP access(e.g. WLAN) is used. The 5G System defines a converged keying hierarchy and defines a Security Anchor Function (SEAF) that is responsible for managing the keying material generated by the primary authentication and key agreement procedure. The SEAF enables the 5G System to establish more than one security context to be derived from the key K_{SEAF}, without the need for a new authentication to be run, enabling the authentication run over the 3GPP access network to provide keys to establish the security between the UE and N3IWF used in untrusted non-3GPP access.

This is illustrated in **Figure 2.8.**, showing how K_{AMF} is used to generate the keys for the 5G Access Network (K_{gNB} NH) as well as the keys used by the N3IWF (K_{N3IWF}).

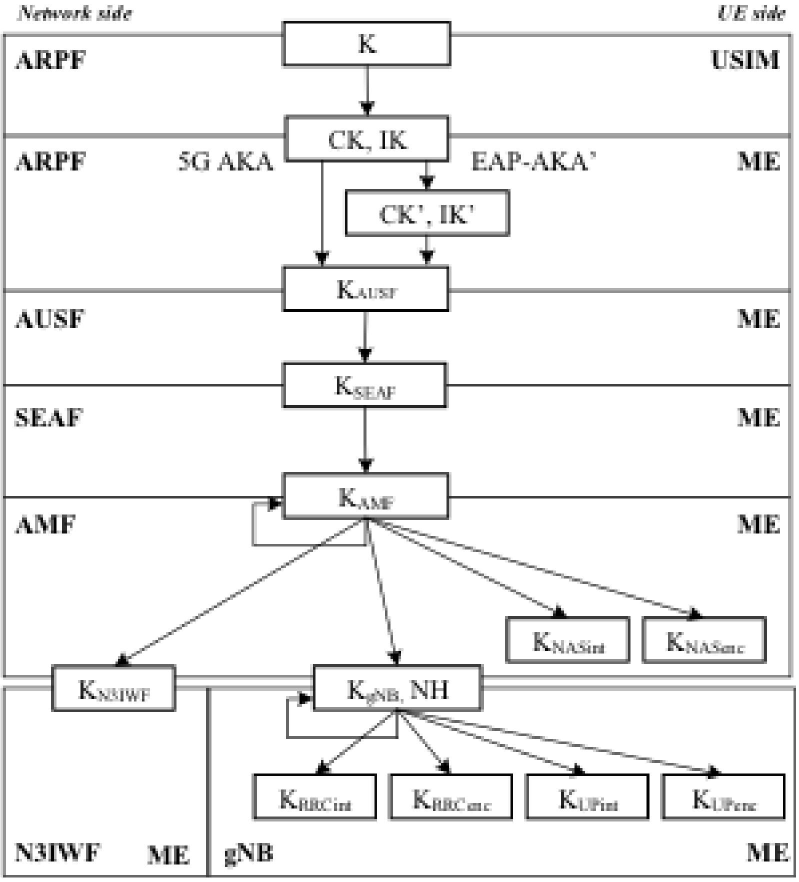

Figure 2-8: Keying Hierarchy in the 5G Systems [10]

2.2 Security Enhancements in 5G, and Implications for Wi-Fi

The 5G architecture supports a unified authentication framework, providing access-agnostic authentication. The idea is that there should be no access type limitation over 3GPP – and “non – 3GPP” – access. This means that operators using the 5G security architecture do not need to deploy two separate authentication infrastructure-sets, one for 3GPP, and another for non-3GPP access.

As illustrated in Figure 2-2, significantly 5G has moved to embrace the Extensible Authentication Protocol (EAP) that has been widely used for supporting flexible Wi-Fi authentication.

2.2.1 Primary Authentication

In their description of the 5G security framework, 3GPP describe primary authentication as: mutual (network and device) authentication, similar to 4G, but with some differences and additions. 3GPP specify a 5G primary authentication mechanism with in-built home control, allowing the home operator to know whether the device is authenticated in a given network and to take final call on authentication. In 5G Release 15 there are two mandatory authentication options: 5G Authentication and Key Agreement (5G-AKA) and Extensible Authentication Protocol (EAP)-AKA', i.e. EAP-AKA'. Optionally, other EAP based authentication mechanisms are also allowed in 5G – albeit for specific cases such as private networks.

The importance of EAP-AKA’ is that it permits the signalling of the access network name within the EAP dialogue, corresponding to an Access Network Prefix, e.g., “WLAN”, and optional strings (none defined for WLAN). The AAA infrastructure (at and behind the AUSF) can populate this information and the UE is then responsible for checking the non-3GPP network name (i.e., access technology) corresponds to that which is currently being used. This enables service-providers to bring a level of control on which type of non-3GPP networks (e.g. Wi-Fi, or HRPD) will interwork with 5G through the N3IWF.

The 3GPP 5G specifications describe a set of “primary authentication and key agreement” procedures to enable mutual authentication between the UE and the network and provide keying material that can be used between the UE and the serving network in subsequent security procedures. The keying material generated by the primary authentication and key agreement procedure results in an anchor key called the K_{SEAF} provided by the AUSF of the home network to the SEAF of the serving network, as illustrated in **Figure 2-8**.

Keys for more than one security context can be derived from the K_{SEAF} without the need of a new authentication run. A concrete example of this, mentioned in the 3GPP TS 33.501 specification [10], is that an authentication run over a 3GPP access network can also provide keys to establish security between the UE and a N3IWF used in untrusted non-3GPP access.

The anchor key K_{SEAF} is derived from an intermediate key called the K_{AUSF}. The K_{AUSF} may be securely stored in the AUSF based on the home operator's policy on using such key.

3GPP TS 33.501 notes that this is an optimisation that might be useful, for example, when a UE registers to different serving networks for 3GPP-defined access and untrusted non-3GPP access, such as Wi-Fi access. The mechanism, using the K_{AUSF} mechanism, is noted to be slightly weaker than authentication directly involving the Authentication credential Repository and Processing Function (ARPF) and the USIM. The 3GPP TS 33.501 specification likens it to fast re-authentication in EAP-AKA'.

2.2.2 New Authentication Schemes

Generally, the 3GPP specifies a new Authentication and Key Agreement scheme: 5G-AKA, giving rise to EAP-5G as a new EAP variant for transporting NAS messages.

There is an informative Annex to 3GPP TS 33.501 that describes using additional EAP methods for primary authentication. Annex B to the specification describes using EAP-TLS as the primary authentication scheme. Two points are worth noting, regarding this:

1. Informative annexes in 3GPP technical specifications can be poorly supported or withdrawn. It is wise to monitor this annex, as it progresses through the 3GPP standardization process.
2. The annex states that the additional EAP methods are only intended for private networks or with IoT devices in isolated deployment scenarios.
   a. Specifically, roaming is not considered.
   b. 3GPP TS 33.501 states that when the 5G system is deployed in private networks, the SUPI and SUCI should be encoded using the NAI format. UE always includes the realm part in the NAI for routing to the correct UDM

A Home-Service Authentication Service Function manages these.

2.2.2.1 Secondary Authentication

Secondary authentication in 5G is meant for authentication with data networks outside the mobile operator domain This is an optional possibility, between a UE and an external data network, such as an Enterprise data network. Any EAP authentication can be supported for this.

Section 11 of 3GPP TS 33.501 describes how external Data Network AAA (DN-AAA) can interoperate with the 5G Authentication and Security architecture, when a 5G subscriber uses the external network.

2.2.3 Enhanced Subscriber Identity-Hiding and Privacy

The privacy issue associated with any LTE systems being able to recover permanent user identities has been addressed with the introduction of a Subscription Concealment Identifier (SUCI). Importantly, corresponding changes to EAP-AKA' have been proposed to introduce

SUCI support [12]. This mechanism prevents malicious capturing of subscribers' identifiers, enabling Non-3GPP operators to serve 3GPP users without compromising identity privacy.

This measure is part of a wider trend that the WBA has experienced in even "pre-5G" activities: the issue of identity privacy is being addressed by device manufacturers, wireless and internet service-providers, etc., besides mobile service-providers.

2.3 R16 N3IWF

2.3.1 Trusted WLAN access to 5G Core

At the time of this writing, 3GPP is studying the integration of WLAN systems into the 5G architecture using a "trusted model". This is where a WLAN access deployed and managed by either a 5G mobile operator or by a third party who is trusted by the 5G mobile operator. In this case the WLAN access is trusted by both 5G core as well as by the 5G terminals once registered in the 5G system. How trust is established between the WLAN access and the 5G mobile operator is not considered in the 3GPP study.

2.3.1.1 Trusted WLAN Access Network (TNAN) Architecture

A **Trusted WLAN Access Network (TNAN)** is composed of two type of network functions:

1. A **Trusted WLAN Access Point (TNAP)** which terminates the UE's IEEE 802.11 over the air access link defined in IEEE Std. 802.11.
2. A **Trusted WLAN Gateway Function (TNGF)** which exposes the N2/N3 interfaces and enables the UE to connect to the 5G Core over the WLAN access technology.

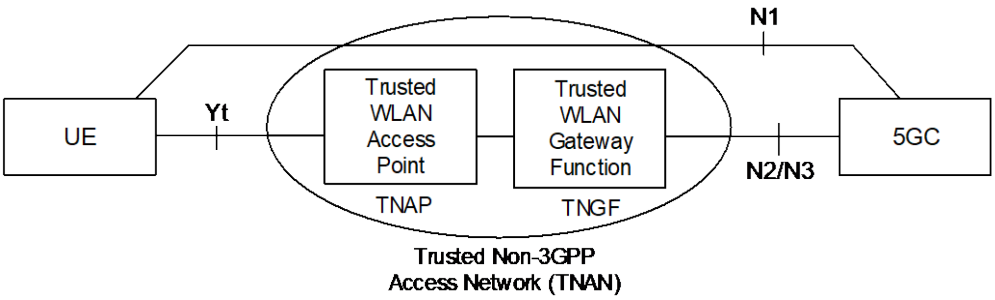
N1
UE
Yt
Trusted WLAN Access Point
TNAP
Trusted WLAN Gateway Function
TNGF
N2/N3
5GC
Trusted Non-3GPP Access Network (TNAN)

Figure 2-9: Release 16 Trusted non-3GPP Access Network

The Trusted WLAN Access Network (TNAN) may contain multiple TNAP instances and multiple TNGF instances. Each TNAP connects to one or multiple TNGFs however the details of the connections are not part of the 3GPP study. Each TNGF exposes N2/N3 interfaces that enable connection with 5G Core. Also, a TNGF may support a Tn interface for communication with other TNGFs. Such communication enables direct inter-TNGF mobility. Inter TNGF mobility may also be supported via 5G Core by using the N2/N3 interfaces. At the time of the writing, it is not clear if the Tn interfaces and inter-TNGF mobility using the Tn interface are going to be completed in the Release 16 timeframe.

2.3.1.2 User Plane and NAS Transport in TNAN

At the time of writing, there are three possible options proposed to be used for the transport of user plane data and NAS messages in the TNAN:

1. IKE v2 and IPSec with NULL encryption between UE and TNGF;
2. A new NWt protocol between the UE and TNGF;
3. IP protocol between the UE and TNGF (or IP-in-IP tunneling with no connection establishment protocol).

2.3.1.2.1 Option 1: IKEv2/IPsec protocols over NWt

This option is described in more detail, because it has been proposed to enable the solution for trusted WLAN access to use the same protocols as those used between the UE and N3IWF in Release 15 “un-trusted WLAN access”. Thus, it makes the solution for trusted WLAN access almost identical to the solution for untrusted non-3GPP specified in Rel-15 which is anticipated to increase the probability that such solutions will be adopted by the 3GPP ecosystem.

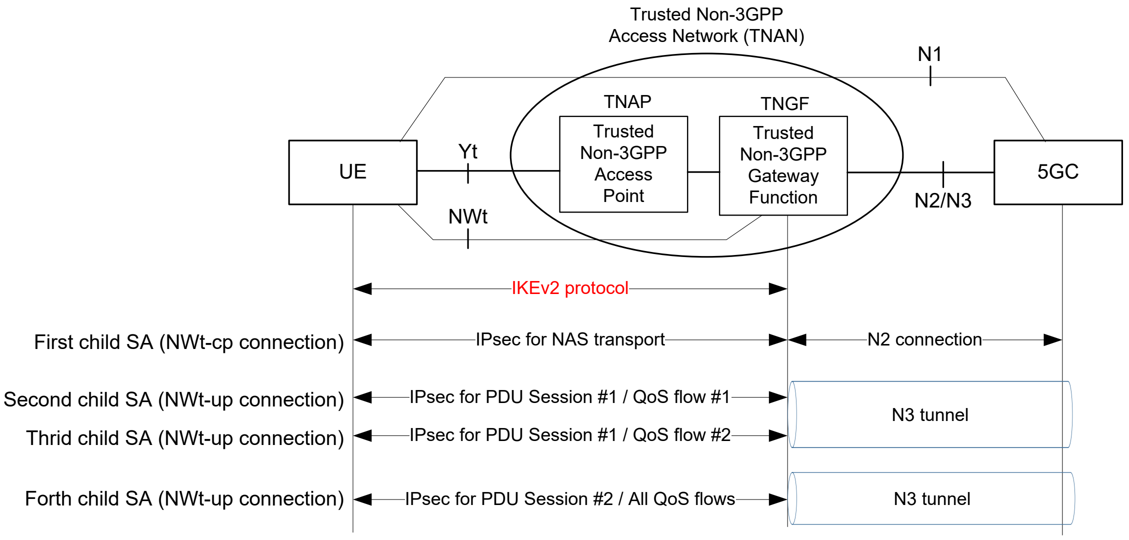
Trusted Non-3GPP
Access Network (TNAN)
N1
TNAP
TNGF
UE
Yt
Trusted Non-3GPP Access Point
Trusted Non-3GPP Gateway Function
5GC
N2/N3
NWt
IKEv2 protocol
First child SA (NWt-cp connection)
IPsec for NAS transport
N2 connection
Second child SA (NWt-up connection)
IPsec for PDU Session #1 / QoS flow #1
Thrid child SA (NWt-up connection)
IPsec for PDU Session #1 / QoS flow #2
N3 tunnel
Forth child SA (NWt-up connection)
IPsec for PDU Session #2 / All QoS flows
N3 tunnel

Figure 2-10: Option 1: IKEv2/IPsec protocols over NWt

The advantage of using “trusted” WLAN access is the elimination of encryption for data at both the UE and TNGF when the access is “trusted”. The use of Layer 3 transport also reduces the impact on the WLAN deployment by eliminating specific requirements previously needed in LTE (i.e., virtual MAC address support on the WLAN network).

For each PDU session, it supports one or many IPsec child SAs. As described in sub-section 2.1, each IPsec child SA can carry the traffic of one QoS flow, or can multiplex the traffic of several QoS flows (as in the solution for untrusted non-3GPP access).

This solution supports well-known and widely deployed layer-3 mechanisms to establish security protection between the UE and TNGF. Note that the layer-2 (access-specific) security mechanisms between the UE and the TNAP may not be sufficient when the UE communicates with the TNGF over IP. For example, when the UE sends an IP packet to TNGF, the TNGF needs to verify the origin of this IP packet (i.e. to determine which UE generated this packet) and to confirm its integrity (that it has not been modified en-route to TNGF). In addition, if the communication path between the TNAP and the TNGF does not provide confidentiality, and where it may be subject to eavesdropping, the IP packet sent by the UE may also need to be encrypted in order to support confidentiality protection from the UE to TNGF (not only between the UE and the TNAP). All these layer-3 security protection mechanisms can be supported by IKEv2/IPsec.

2.3.1.3 Registration for 5G Services over TNAN

For terminals that connect to the 5G System via the TNAN and can use 5G NAS signaling, the EAP-5G method should be selected, which enables the transport of NAS signaling between the UE and the 5G Core (5GC) during Registration and Service Request procedures. In order to do so, the UE provides a special NAI in the EAP-Request/Identity message. This triggers the TNAN to select the EAP-5G method for authentication toward the 5GC.

The UE registers to 5GC and, at the same time, it authenticates with the TNAN by using the EAP-based procedure. This procedure is essentially the same with the registration procedure for untrusted non-3GPP access introduced in sub-section 2.1. The interface between the TNAP and TNGF-CP is an AAA interface.

The registration procedure and the authentication mechanism over TNAN are detailed in TR 23.716, clause 7.1.3.3 .[6]

2.3.2 Access Traffic Steering, Switching and Splitting Support in 5G System Architecture (ATSSS)

The release 16 ATSSS Study Item investigates solutions that allow a terminal device to use one or more access networks when they are simultaneously available. In Release 16 only “untrusted WLAN access” is considered; “trusted WLAN access as well as hybrid access for fixed network deployments are expected to be covered in the next Release.

Release 16, introduces a new PDU session type, the Multi Access PDU (MA-PDU) Session type. A MA-PDU is a PDU whose traffic may be sent over one or more accesses simultaneously. All the procedures associated with an ATSSS solution are applied after a

MA-PDU session is established. The establishment of the MA-PDU session is done using the Separate Establishment procedure detailed in TR 23.793 clause 6.2.3.1.

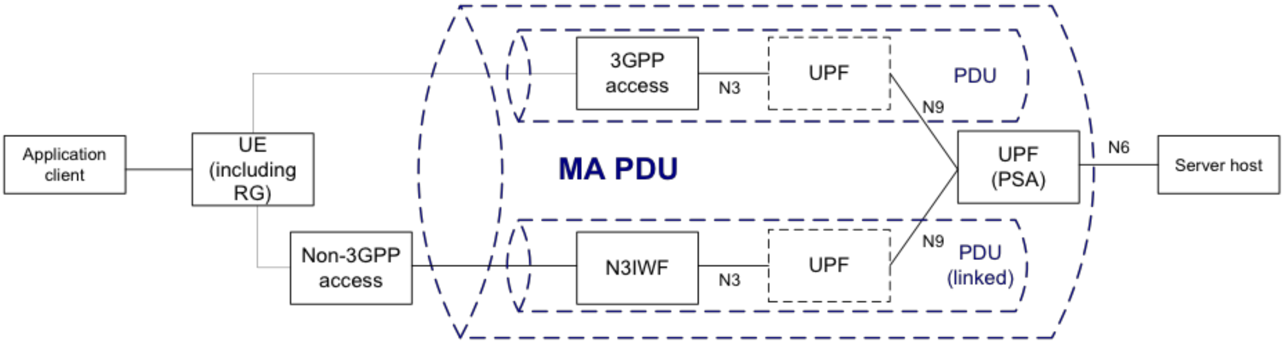

Figure 2-11: Combining 3GPP and non-=3GPP Access into a Multi-Access PDU

The establishment of the MA-PDU session may be done by the network if the terminal device signals the support of MA-PDU. This indication is signalled by the UE setting the MA-PDU capability indication in a NAS message request for a single access PDU session. This indication may be used by the network to establish a multi-access PDU session instead of the requested single access PDU session.

2.3.2.1 ATSSS Architecture Description

The architecture definition for ATSSS has not been finalized at the time of this writing this paper. A possible architecture is shown in the **Figure 2-12** below detailing the interactions between AT3SF's of UE, UPF, SMF and PCF. 5GS can implement ATSSS for MA PDU session according to PCF policy, user preference settings and link performance of 3GPP & non-3GPP access networks as shown in **Figure 2-12**.

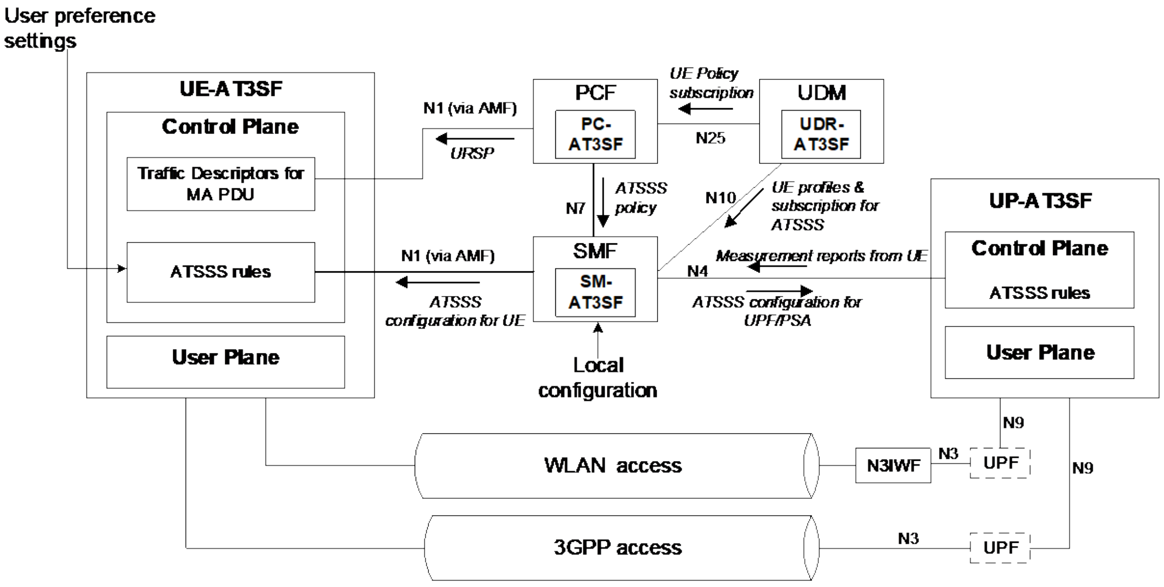

Figure 2-12: Interaction between AT3SF's of UE, SMF, PCF & UPF

During the establishment of a MA-PDU session, the PCF may create PCC rules for the MA-PDU session. These rules specify how specific service data flows (SDFs) should be routed across the 3GPP and WLAN accesses.

The SMF maps the PCC rules into (a) ATSSS rules which are sent to UE via the AMF, and (b) Packet Detection Rules which are sent to UPF. The ATSSS rules are used by the UE for up-link traffic steering and the Packet Detection Rules are used by the UPF for down-link traffic steering.

The ATSSS rules are sent to UE with a NAS message when the MA-PDU session is created or when they are updated by SMF/PCF. Similarly, the Packet Detection Rules are sent to UPF when the MA-PDU session is created or when they are updated by SMF/PCF.

Measurements can be done via the user plane between the UE and the UPF implementing the AT3SF and can be also made available to SMF if needed. At the time of this writing, Round Trip Time (RTT) evaluation has been identified as a metric to be used for ATSSS rules implementing “Smallest Delay”.

2.3.2.2 ATSSS Rules

An ATSSS rule includes the following:

1. **A Precedence value**, which identifies the priority of this ATSSS rule with respect to other ATSSS rules.
2. **A Traffic Descriptor**, which identifies a service data flow (SDF). It may include e.g. an Application ID, IP descriptors, non-IP descriptors, etc.
3. **A Steering Function ,** which identifies which function (e.g. MPTCP or AT3SF) should be used to steer the traffic of the matching SDF. This is useful in case the terminal device supports multiple functions for traffic steering.
4. **A Steering Mode**, which identifies how the matching SDF should be steered across 3GPP and WLAN accesses. The following Steering Modes will be supported:
   a. **Active-Standby**: It is used to steer a SDF on one access (the Active access), when this access is available, and to switch the SDF to the other access (the Standby access), when Active access becomes unavailable. When the Active access becomes available again, the SDF is switched back to this access. If the Standby access is not defined, then the SDF is only allowed on the Active access and cannot be transferred on another access.
   b. **Priority-based steering**: The two accesses are assigned a priority, e.g. during the establishment of the MA-PDU session. All traffic (or some) of the MA-PDU session is sent to the high priority access. When congestion arises on the high priority access, new data flows (the "overflow" traffic) are sent to the low priority access. In addition, when the high priority access becomes unavailable, all traffic is switched to the low priority access.
   c. **Smallest Delay**: It is used to steer a SDF to the access that is determined to have the smallest Round-Trip Time (RTT). Measurements may be conducted to determine the RTT over 3GPP access and over WLAN access.
   d. Load-Balancing: It is used to split a SDF across both accesses. With a 50/50 load-balancing, the SDF traffic is equally split across the two accesses. With an 80/20 load-balancing, about 80% of the SDF traffic is sent on one access and 20% on the other access.

2.3.2.3 MPTCP support in ATSSS

In Release 16, MPTCP proxy support is an integral part of the ATSSS solution. The same MA-PDU Session may support both steering the MPTCP flows by using the MPTCP protocol and simultaneously steering all other flows using another steering function called the AT3SF. The same set of rules is applied for steering decisions by both MP-TCP function and by the AT3SF.

The solution supports MPTCP proxy functionality as follows:

1. The terminal device indicates to the network in MA-PDU Session establishment the request for MP-TCP proxy support.
2. If the network agrees to provide MP-TCP proxy functionality for the specified MA-PDU session then the network will allocate two IP addresses for the MA-PDU. At the time of this writing, it has not been decided if the addresses are to be allocated to either the terminal or the MP-TCP proxy.
3. The network may also send the MP-TCP proxy information to the UE e.g. IP address(es), port(s), type (SOCKS5, or TCP Convert Protocol), etc. Also, the network may indicate the terminal the type of application for which the MP-TCP proxy should be applied.

2.4 Slicing requirements and impact on Wi-Fi 5G integration

Slicing is seen as foundational to 5G networks and is perceived by some as being unique to 3GPP. However, many of the concepts behind slicing have already been implemented by the Wi-Fi community, delivering solutions that enable multiple use cases to be simultaneously supported on a common Wi-Fi infrastructure. As an early deliverable associated with this project looking at unlicensed integration into 5G, WBA has published a whitepaper describing in detail how Wi-Fi networks can support slicing use cases [13].

3 Above NGCN Wi-Fi Integration

3.1 MP-TCP and SOCKS/Converters

TCP, which is used by the vast majority of applications, is essentially a “single-path” protocol. In particular, when a TCP session is established, the connection is bound to the IP address of the two communicating hosts [14]. This has motivated the definition of mobility solutions that deliver mobility “below” the IP layer, including the definition of GTP and Proxy Mobile IP that deliver a stable IP address to the TCP layer, even when “handing over” a user between different layer 2 points of attachment to the network.

3.1.1 Introduction to MP-TCP

Multipath TCP (MPTCP) is a major modification to TCP that allows multiple paths to be used simultaneously by a single transport connection. The Multipath TCP protocol has been standardized by the IETF in RFC 6824 [15]. Multipath TCP allows multiple sub flows to be set up for a single MPTCP session. An MPTCP session starts with an initial sub flow. Then, after the first MPTCP sub flow is set up, additional sub flows can be established which are bound to the existing MPTCP session. Data for the connection can then be sent over any of the active sub flows that have the capacity to take it.

Figure 3-1 illustrates the sub-flow establishment in a scenario where a user device has simultaneous coverage of Wi-Fi and cellular based access networks. The figure shows the device establishing a first sub-flow over the cellular network and then subsequently adding a second sub-flow over the Wi-Fi network. The MP-TCP stack in the client device is responsible for combining these two sub-flows and providing a single socket link to the application.

> Note: The MP-TCP protocol does not place restrictions on the ordering of sub-flow establishment, although particular device implementations may integrate concepts of "anchor sub-flows" that are preferentially transported over wide-area radio systems.

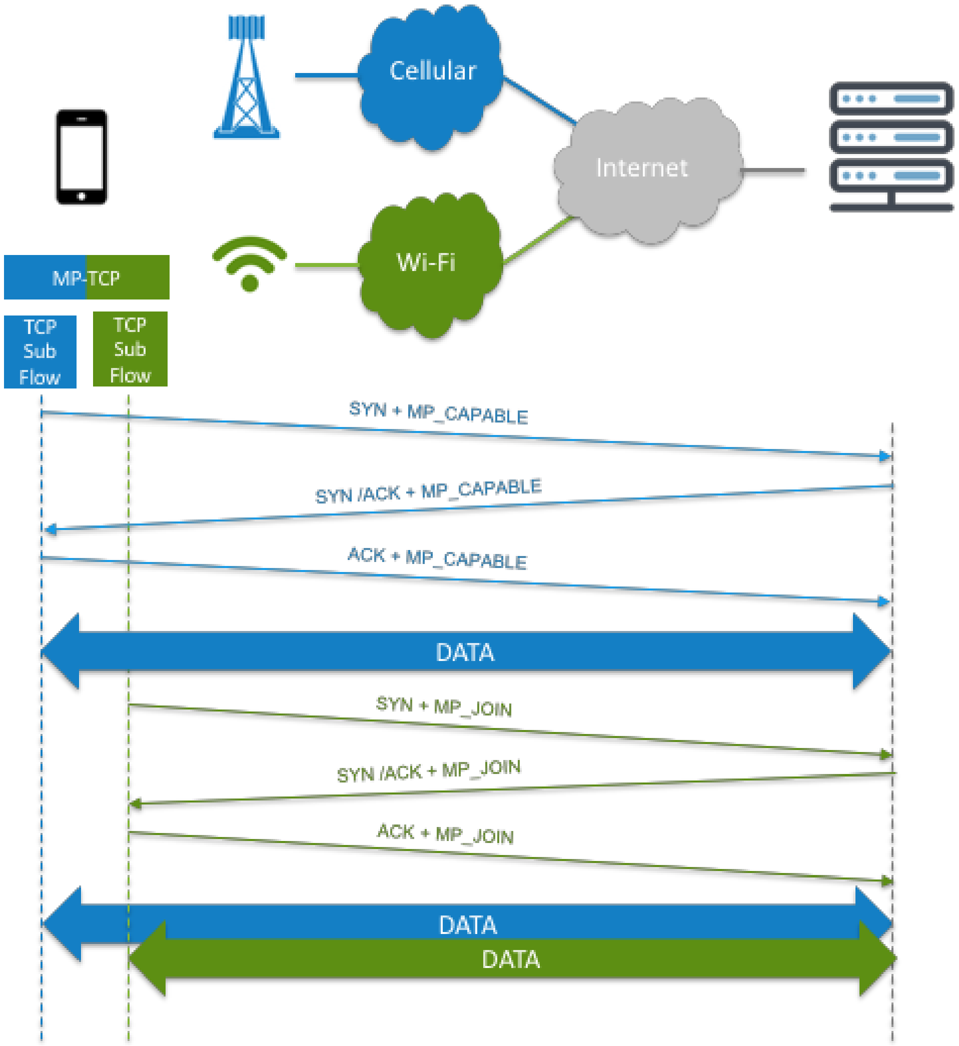

Figure 3-1: MP-TCP Sub-Flow establishment

3.1.2 Converters/Proxies

There are significant barriers to MP-TCP adoption. Most significantly, almost all servers on the Internet are traditional TCP servers and experience shows that it could take many years to migrate these to integrate MP-TCP capabilities. As a consequence, the use of converters and/or proxies has been defined in order to support MP-TCP sessions between an MP-TCP enabled host and a conventional TCP server.

Conventional approaches to realizing MP-TCP proxy functionality leverage the SOCKS protocol [16]. Using such an approach, the device first establishes a connection to the SOCKS proxy, exchanging authentication information and signaling the address and port of the intended destination server.

The SOCKS proxy then establishes a connection to the destination server and relays data between the two proxied connections, as illustrated in **Figure 3-2**.

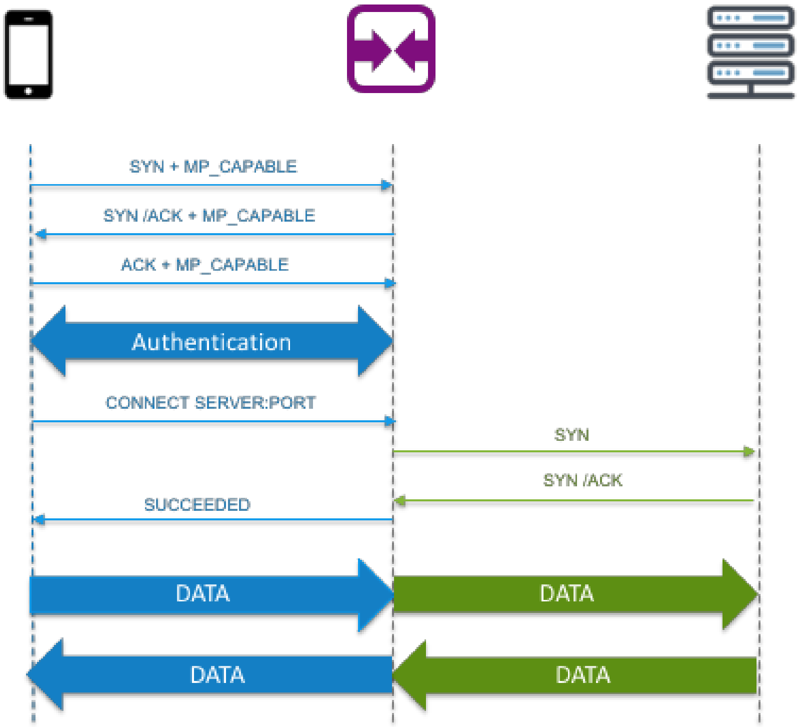

Figure 3-2: SOCKS based MP-TCP Proxy

In contrast to this approach, the IETF is currently defining a “TCP Converter” functionality that is an application proxy aimed at facilitating the deployment of TCP extensions [17]. One of the immediate use cases driving the definition of such a converter relates to extensions associated with MP-TCP, enabling MP-TCP to be leveraged by wireless devices without requiring end-to-end support of MP-TCP.

Similar to the SOCKS based proxy, the converter is responsible for relaying data exchanged between the host-to-converter and converter-to-server connections. Moreover, the converter can be operated by a network operator or a third party and may be realised using a stand-alone device or delivered as service integrated into the routing infrastructure.

In contrast to the SOCKS-based proxy, the TCP converter enables the device to indicate the address and port of the intended destination server in the payload of the TCP SYN packet, as shown in Figure 3-3. This enables the TCP Converter to immediately initiate the connection towards the destination server, avoiding the additional delay experienced by SOCKS based solutions. In the illustrated example, the destination server does not signal that it is MP-Capable, whereas MP-TCP can be used between the device and the converter.

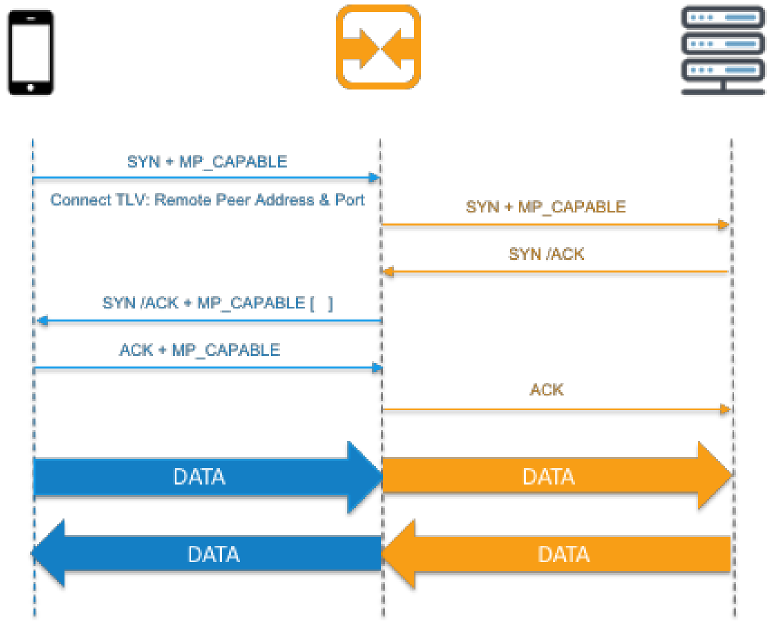

Figure 3-3: TCP Converter based MP-TCP Proxy

3.2 Multi-Access Management Service (MAMS)

Multi Access Management Services(MAMS) framework [18] enables a flexible and dynamic selection of access and core network paths between a multi connectivity capable device and the network, as well as the kind of user plane treatment (e.g. switching or aggregation), based on application needs, device, network capabilities and network conditions.

The MAMS framework is illustrated in Figure 3-4. The framework enables negotiation and configuration of the user plane protocols (and network proxies) based on needs of deployment (e.g. IPsec where network level security is needed), application needs (e.g. packet/flow switching or aggregation using protocols like MPTCP), network conditions (e.g., Switching or Aggregation modes based on differential link delay), transport type, etc. and including client/network capabilities.

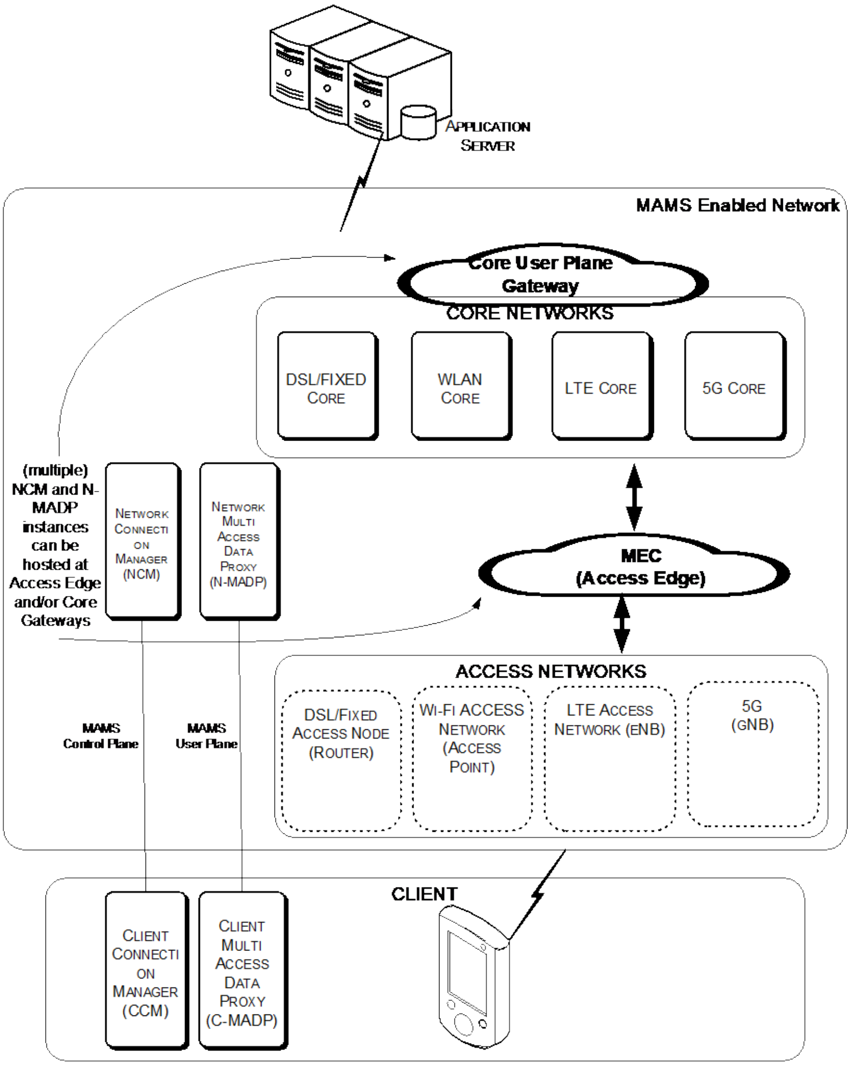
APPLICATION SERVER
MAMS Enabled Network
Core User Plane Gateway
CORE NETWORKS
DSL/FIXED CORE
WLAN CORE
LTE CORE
5G CORE
(multiple) NCM and N-MADP instances can be hosted at Access Edge and/or Core Gateways
NETWORK CONNECTION MANAGER (NCM)
NETWORK MULTI ACCESS DATA PROXY (N-MADP)
MEC (Access Edge)
ACCESS NETWORKS
DSL/FIXED ACCESS NODE (ROUTER)
WI-FI ACCESS NETWORK (ACCESS POINT)
LTE ACCESS NETWORK (ENB)
5G (GNB)
MAMS Control Plane
MAMS User Plane
CLIENT
CLIENT CONNECTION MANAGER (CCM)
CLIENT MULTI ACCESS DATA PROXY (C-MADP)

Figure 3-4: MAMS Functional Architecture

The MAMS control plane consists of the Network Connection Manager (NCM) and the Client Connection Manager (CCM). Network Multi Access Data Proxy (N-MADP) and Client Multi Access Data Proxy (C-MADP) are the user plane functional elements. NCM and CCM exchange the MAMS control plane messages, and configure the user plane protocols and traffic distribution at C-MADP and N-MADP.

The functional elements can be flexibly located as long as they have user plane connectivity with the device, either in the RAN/RAN-Edge or Core depending on the deployment needs. Due to a clear separation between the control and user plane, MAMS control plane can co-exist with and complement any of the existing IETF protocols like MPTCP, GRE, MP-QUIC or new ones. NCM and N-MADP can either be collocated or hosted on separate network elements.

3.2.1.1 MAMS Control Plane

MAMS control plane messages use WebSocket/TLS as transport and are carried as user plane data transparent to the underlying network.

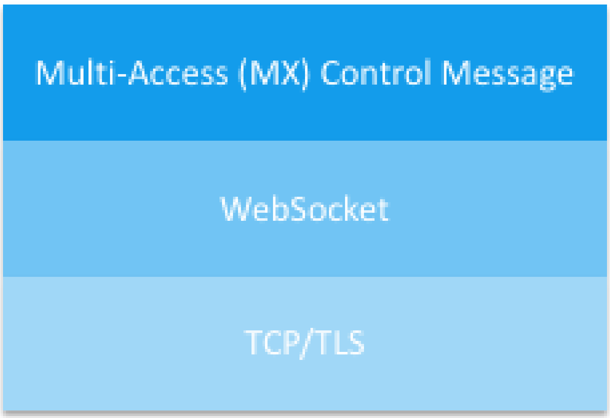

Figure 3-5: MAMS Control Plane Protocol Layering

MAMS control plane is used for negotiation of access links and user plane protocols, including discovery and configuration of network user plane proxies. It also supports dynamic access and link status estimation and reporting to adapt the selected link and user plane configurations to ensure best performance. MAMS control plane procedures provide the following services to enable efficient management of the user plane traffic:

- User Plane Access and Core Selection
  - Selection of combination of accesses in up-link and down-link, with appropriate core network (IP Anchor).
- User Plane Protocols and Proxy setup
  - Discovery and selection of user plane protocols and proxy in the network.
- Link status monitoring

The client reports on link performance for dynamic adaptation of traffic steering rules and user plane proxy configuration

3.2.1.2 MAMS User plane

MAMS control plane allows any user plane protocol to be incorporated into the framework, including negotiation and configuration of existing user plane protocols, e.g. GRE, MPTCP, for user plane traffic distribution and aggregation. Figure 3-6 shows the MAMS user plane protocol stack, which consists of the following two sublayers:

- Multi-Access (MX) Convergence Sublayer: this layer performs multi-access specific tasks, e.g., access (path) selection, multi-link (path) aggregation, splitting/reordering, lossless switching, fragmentation, concatenation, keep-alive, and probing etc.
- Multi-Access (MX) Adaptation Sublayer: this layer performs functions to handle tunnelling, network layer security, and NAT (network address translation).

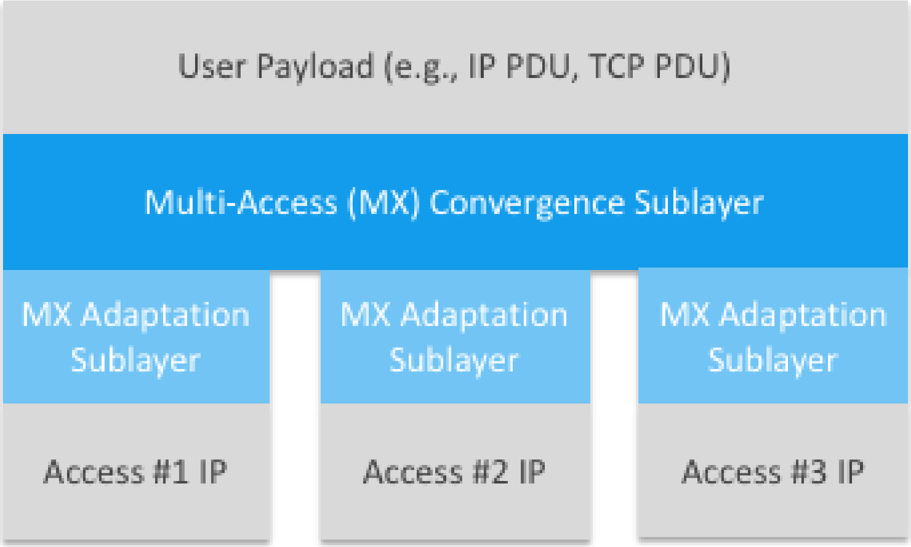

Figure 3-6: MAMS User Plane Protocol Layering

An N-MADP/C-MADP pair instance is defined by the combination of Convergence an Adaptation layer protocols and parameters configured based on NCM-CCM control plane exchange. There can be multiple N-MADP/C-MADP pair instances configured using the MAMS control plane procedures depending on the types of applications and traffic needs.

There are two types of connections defined in the MAMS user-plane:

- **Anchor Connection:** refers to the e2e network path between the client and the Application Server. This corresponds to an instance of convergence layer at N-MADP/C-MADP.
- **Delivery Connection:** refers to the network path between the client and the MAMS network data proxy for delivering data traffic. This corresponds to an instance of convergence layer at N-MADP/C-MADP. Multiple delivery connections can be configured to distribute user traffic, which are combined and managed at the convergence layer.

The MAMS convergence sublayer allows to use existing protocols, e.g. GRE, MPTCP etc Figure 3-7 shows the MP-TCP-based MAMS user plane protocol stack.

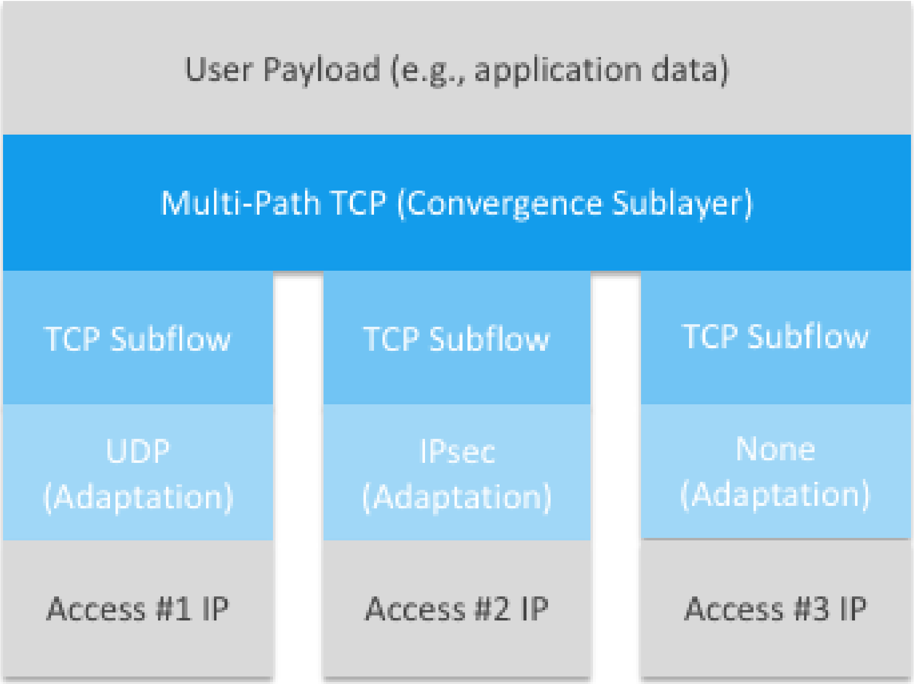

Figure 3-7: MP-TCP based MAMS User Plane Protocol Layering

On the other hand, Figure 3-8 illustrates a new trailer-based protocol for more flexible multi-access management.

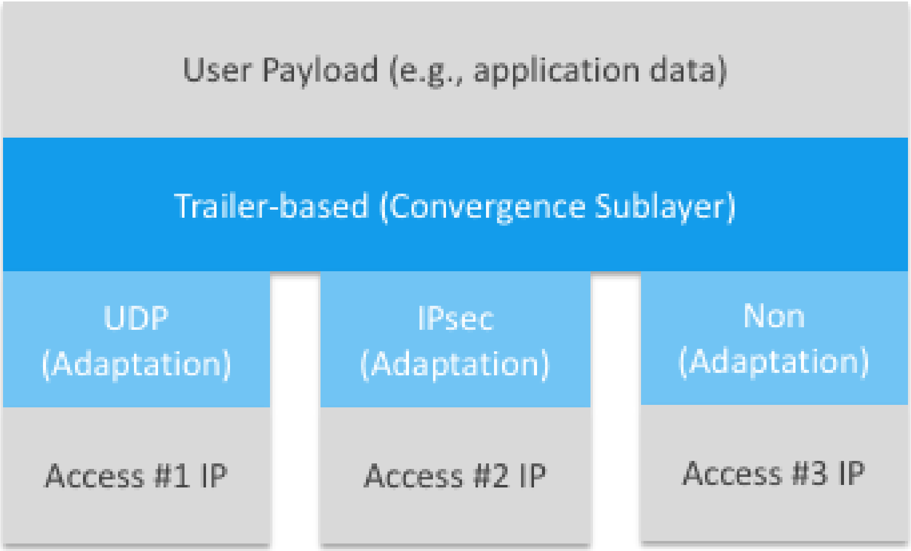

Figure 3-8: Trailer-based MAMS User Plane Protocol Layering

3.3 MP-QUIC

3.3.1 Introduction to QUIC

Quick UDP Internet Connection (QUIC) is a multiplexed and secure transport protocol that runs on top of UDP that combines functions of HTTP/2, TLS, and TCP [19]. QUIC is targeted at reducing the latency of client-server communication, providing an alternative to conventional layered HTTP/TLS/TCP protocol stack used by the web. One of the rationales for the development of QUIC has been the constraints experienced by TCP that is implemented in operating system kernels, and middlebox firmware, making significant changes to TCP (e.g., Multi-Path capability) very challenging to deploy [20]. Being based on UDP, QUIC doesn't suffer from such limitations and hence is able to incorporate new features without having to upgrade legacy systems.

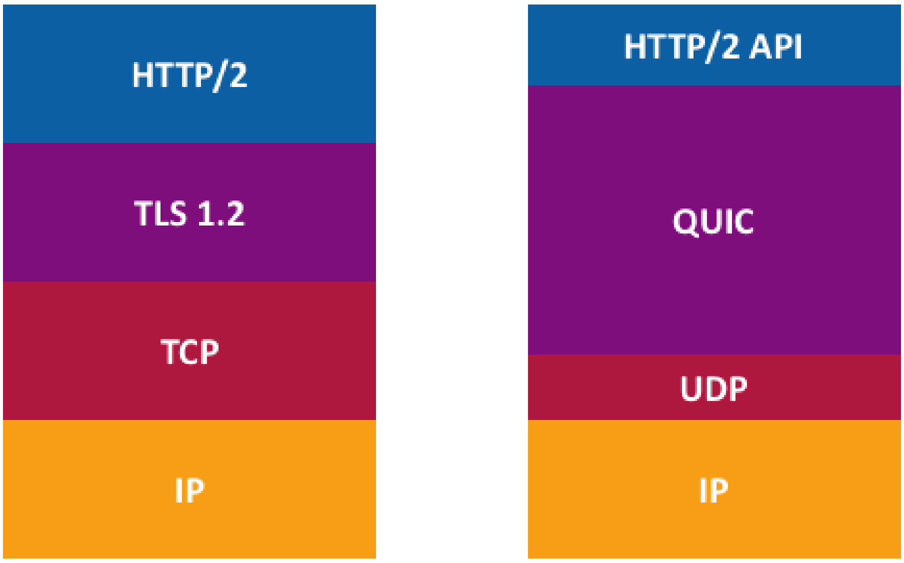

Figure 3-9 : Comparing QUIC with Conventional HPPT/TLS/TCP

QUIC has been championed by Google and, even though IETF QUIC is not yet fully standardized, it has been widely deployed. Analysis in November 2017 indicated that QUIC comprised 20% of all mobile traffic [21] and one anecdotal report from Vodafone put the figure at between 40-50% [22].

One of the key motivations for defining QUIC is to improve the responsiveness of the web, minimizing the number of round-trip times required to establish a secured connection, as illustrated in **Figure 3-10**.

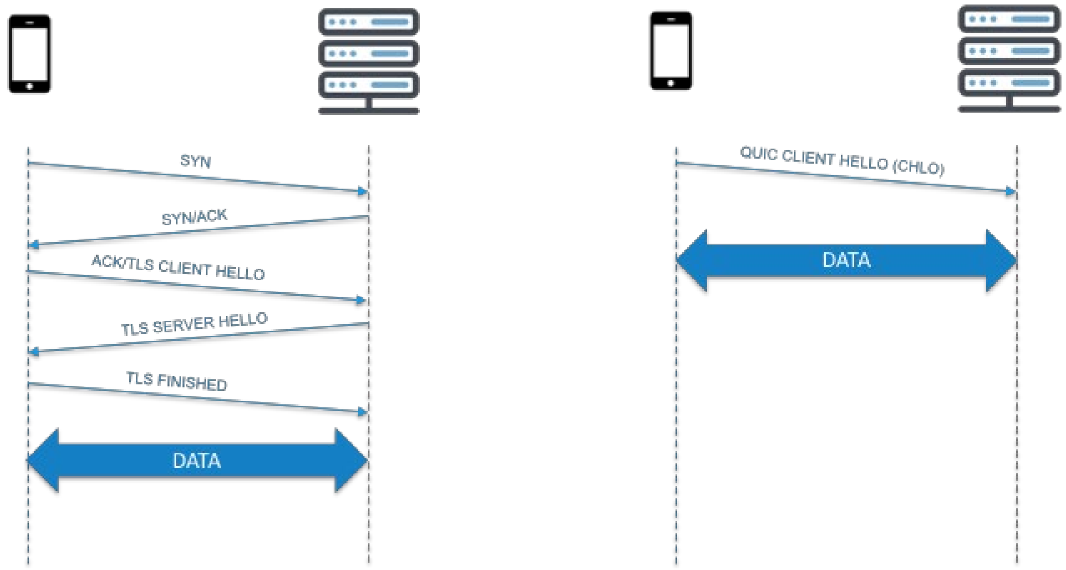

Figure 3-10: Comparing Round Trip Times for TLS and QUIC Resume

Another key benefit of QUIC is that it does not use the conventional 5-tuple as an implicit connection identifier, instead defining the exchange of explicit connection IDs. This decoupling of connections from 5-tuples allows QUIC endpoints to migrate connections between different IP addresses and network paths. A QUIC enabled device supporting both Wi-Fi and cellular is able to migrate the QUIC connection between the cellular data network and the Wi-Fi network, e.g., if the user moves into range of the Wi-Fi network.

Figure 3-11 illustrates this operation. The client first establishes a QUIC connection over a cellular network. Then, perhaps in response to becoming aware of the availability of a Wi-Fi connection, the client starts probing the new path by sending a PATH_CHALLENGE messages to the server over the Wi-Fi connection. The reception of the PATH_RESPONSE from the server over the Wi-Fi connection confirms that the path can be used, allowing the client to trigger the connection migration procedure. This is initiated by the client sending a packet other than a PATH_CHALLENGE/RESPONSE message to the server over the new path. When the client receives a packet over the Wi-Fi network containing a packet other than a PATH_CHALLENGE/RESPONSE, this confirms that the server has migrated the connection from the cellular to the Wi-Fi network.

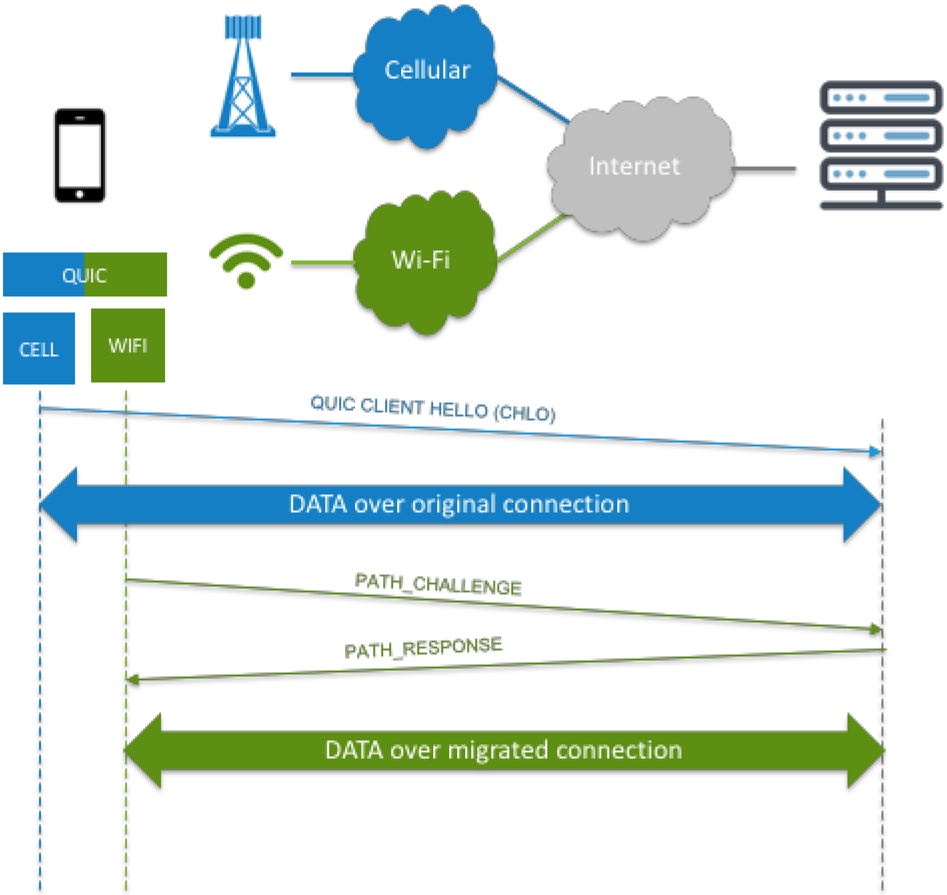

Figure 3-11: QUIC based connection migration

3.3.2 Multi-Path QUIC

Compared with the baseline QUIC capability that supports a single connection over a single, migratable path, there are proposals to define extensions to the QUIC protocol to enhance the migration capabilities to enable support of a single connection over multiple paths [23].

More specifically, during the initial exchange, both client and server advertise the maximum number of additional paths they can simultaneously support. The MPQUIC enabled host then uses the ADD_ADDRESS frame to advertise its current addresses. The existing PATH_CHALLENGE and PATH RESPONSE messages are then used to verify whether the additional addresses are available to be used by the separate paths.

An example of MP-QUIC operation is described in [24]. A path manager is defined to control the creation and deletion of paths. In one implementation, after the initial handshake is completed, the path manager in the client opens one path over each available interface.

Importantly, MPQUIC enables hosts to use the newly defined PATHS message to communicate the path state of the sending peer. The message contains the path IDs of active paths together with statistics such as estimated round-trip time. Hence, this message can be used to detect broken paths and thus speed up the handover process associated with mobility events as the client moves in and out of coverage of individual wireless networks.

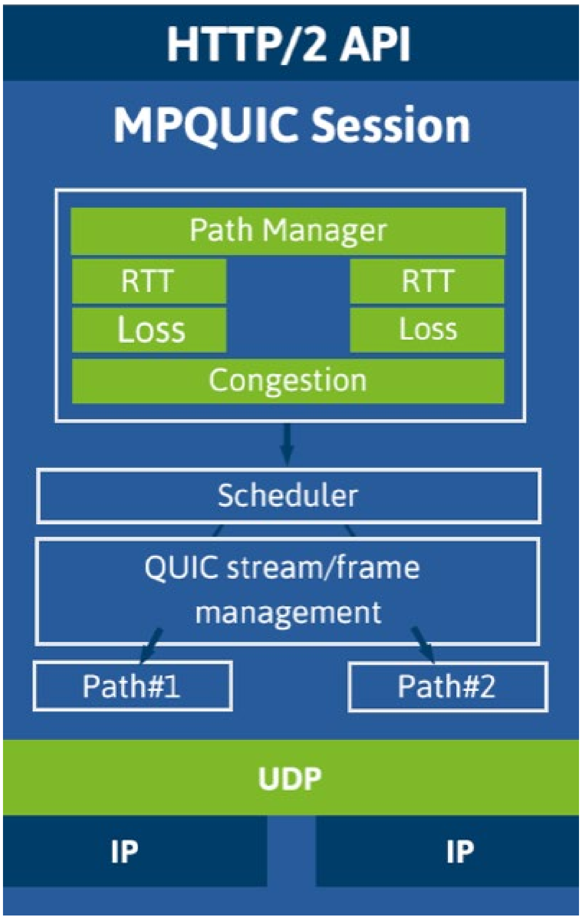

Figure 3-12:MPQUIC Path Management [25]

4 Control plane aspects of integrated Wi-Fi and cellular solutions

A key characteristic of all multi-path solutions is the policy functionality related to path management, e.g., PC-AT3SF in the case of 3GPP Release 16, Path Manager functionality for MP-TCP and MP-QUIC, or Network Connection Manager (NCM) in the case of MAMS. This path management functionality controls the utilization of the different paths. The logic embedded in the path manager needs to accommodate a wide range of multi-path use cases. The remainder of this section examines aspects of path management.

4.1 Policy definition

As described in [26] there is a wide variety of scenarios that can be conceived related to multi-path policy definition, e.g.,

- Prefer sub-flow sent using interface A over interface B if interface C is down
- Application ABC can only be sent using sub-flows over interface B
- Always initiate connections using sub-flows over interface C and then establish additional sub-flows over interface A if the socket lifetime exceeds a specific threshold.

More generically, we introduce the concept of a *Policy Outcome*. This represents the desired outcome of the policy. There are a wide range of desirable policy outcomes, some of which have been described in the 3GPP Study on ATSSS [6]:

- **Performance based:** a policy may focus on improving the user's perception of performance which may be because of lower RTT and improved interactivity, or due to improved peak throughput.
- **Load based:** a policy may focus on balancing the load between different access networks. The policy may be a simple load balancing or more elaborate load-based decisions which look to steer traffic to the least loaded access.
- **Financial cost based:** a "top up" policy may be used to steer traffic to the least cost access, either optimizing the retail cost to the user, or a wholesale cost to the service provider.
- **Improved resilience**: a "hot standby" policy may be focused on enhancing the coverage proposition to the user, which may include enhanced resilience or being able to support service continuity as the user moves in and out of Wi-Fi coverage.

The path manager is responsible for realizing how a particular policy outcome should be handled. In particular, a policy may be defined to apply homogenously across the device for all applications or services. Alternatively, a policy may be defined in a heterogeneous fashion, where the integration policy deals with only specific applications and/or services.

> Note, because the path manager deals with policies associated with sub-flows over different interfaces, there is overlap with earlier concepts used in 3GPP's Inter System Routing Policy (ISRP), described in [27]. In the ANDSF scenario, the ISRP rule is used to detect, control, and route traffic over 2 concurrent connections. The UE uses ISRP rules to select the most preferable access network which should be used to route IP traffic that matches specific criteria such as traffic for a specific APN, or all traffic for a specific IP flow ,or all traffic for a specific application. ISRP rules identify a prioritised list of access networks based on the selected criteria.

4.2 Application Experience

When multiple access networks are available for a device to access applications, the end user experience varies depending on the type of access network used to transport application data. e.g. heavy throughput demanding applications may perform better on a Wi-Fi network which offers large capacity whereas Voice applications may perform better over an LTE network which offers controlled Quality of Service.

The application experience also varies dynamically with changing conditions like user population, coverage changes with mobility. For example, when only a few users are connected to the access point, Wi-Fi offers good application experience, but due to current contention-based access mechanism, the experience may degrade with increasing user populations, resulting in decreased throughputs, and increased and unpredictable delays. In contrast, the LTE network, due to its network controlled scheduled resource allocation, provides consistent user experience even when number of users increase.

> Note, as reported in [28]. enhancements defined in 802.11ax are targeted at addressing such deficiencies.

Then there is the case, where different applications are accessible only via specific core networks, e.g., enterprise applications are typically accessible via enterprise Wi-Fi networks, and not via the public internet. The best application experience therefore, is dependent on the optimal choice of access and core network paths, depending on application needs and the network characteristics, and with the flexibility that the combination of network paths can be dynamically adapting based on changing network conditions.

4.3 Per Application Control

Instead of embedding complex policy logic in a path manager, an alternative approach is to provide the granular control of the different paths on a per application basis.

> Note, effectively this approach is being used with commercial ePDG deployments that limit themselves to IMS-APN support and hence limit their multi-path applicability to IMS-based base VoLTE services.

One way to formalize such an approach is to define an enhanced socket API, e.g., [29]. This enables the application to control the creation and deletion of different paths according to its own application logic.

In particular, Section 5 describes the results of MP-QUIC tests that examine the performance of multi-path solutions, indicating that for some transfers using short-lived sockets the use of multi-path capabilities is not desirable. Moreover, testing of MP-TCP indicate the same characteristic, that for small transfers, e.g., less than 30 Kbytes, the additional overhead of establishing multiple paths results in MP-TCP actually having a decrease in performance compared to regular TCP [30]. As it is only the application which has visibility regarding the longevity of particular flows, then this would seem to re-enforce the involvement of the application in path section policies.

4.4 Instrumentation used for control/policy

The optimum operation of the path management functionality requires instrumentation to be available to assist in policy implementation.

Policy outcomes that relate to performance require those associated metrics to be exposed to the path manager functionality. Some solutions inherently expose key functionality. For example, sub-section 3.3.2 describes how QUIC keeps RTT and loss statistics for each individual path, ensuring the path manager has an accurate estimate of such to use in implementing path selection policies.

Policy outcomes that relate to load require those associated metrics to be exposed. In particular, for Wi-Fi systems, the WLAN channel utilization (BSS load) is signaled to Wi-Fi devices, enabling them to use such information in their decisions. Moreover, as part of its ATSSS study, 3GPP is considering being able to signal measurement information, including the Wi-Fi load information, to the enhanced core network. In contrast to Wi-Fi systems, cellular systems do not typically signal their load to attached devices, instead relying on network control to implement load balancing.

Policy outcomes that relate to financial cost require those associated metrics to be exposed. From a Wi-Fi perspective, a device can use ANQP to query a HS2.0 network's "Access Network Type". This may enable the HS2.0 WLAN network to signal to the device whether it is a "Free Public Network" or a "Chargeable Public Network". The device can then use this information when implementing policies associated with financial metrics. In contrast, from a cellular perspective, "advice of charge" has largely focused on support for circuit and IMS-based voice calls and so a cellular client has little or no information related to financial costs associated with connections that use a cellular path.

4.5 Combinational issues with coexistence of alternative multi-path solutions

One of the key challenges with the multi-path approaches described in previous sections of this report is the number of alternative approaches available for combing Wi-Fi-based and cellular-based access networks, with the definition of access-centric, core-centric and above-the-core centric solutions. In particular, this may result in coexistence issues as multiple alternative approaches are deployed in parallel.

Whereas there are established core-centric solutions deployed today, e.g., for supporting Wi-Fi calling, and section 5 describes the deployment of above-the-core solutions by a number of service providers, the GSM Suppliers Association (GSA) only lists a single deployment of access-centric solutions, available using a single handset [31].

Moreover, the GSA has identified no additional announcements of trials of LWA over the last 12 months. Hence this section focuses on the possible interactions between core-centric and above-the-core solutions, both of which treat the Wi-Fi access network as a peer of the 3GPP defined cellular network.

4.5.1 Interactions between core-based and above-the-core-based solutions

Section 2 has introduced the 5G core-centric solutions being define by 3GPP as part of Release 15 and 16. This section has highlighted that the 3GPP architecture enables the UE to select an N3IWF independently of the network it is using for 3GPP access. Importantly, this delivers the independent IP addressing on the WLAN and 3GPP interfaces that can then be subsequently used by above-the-core solutions. However, if the UE instead always selects an N3IWF corresponding to its 3GPP access network, then the UE will be supported by a common 5G core network which may be configured to only present a common IP address over both WLAN and 3GPP interfaces, thus precluding operation of above-the-core multi-path based capabilities in such a Release 15 configuration.

4.5.2 Policy Interactions

The previous section has highlighted the breadth of elements that can be involved in path management decisions, ranging from application logic which may take into account flow longevity in making decisions, through to platform policies that may be configured by users to preferentially use particular access networks, to core network policies that may be configured by operators to balance load amongst a range of different networks, to a proxy/converter policy that may define policies based on round-trip times and packet loss ratios. This environment highlights the need for a mechanism to combine disparate policies.

Application Policy
Platform Policy
Core Network Policy
Proxy/ Converter Network Policy

Figure 4-1: Range of Policy Enforcement Options

An example of defining an approach to policy combining is eXtensible Access Control Markup Language (XACL) [32]. XACML is an OASIS standard that describes both a policy language and an access control decision request/response language (both written in XML). Although focused on access based policy, a framework has been defined to enable different policies to be combined, even supporting scenarios where some policies contradict each other. In this approach, the policy-combining algorithm defines a procedure for arriving at an access decision given the individual results of evaluation of a set of policies.

5 Deployment of Above the Core Solutions

Whereas there have been a number of deployments of core-centric solutions, including widescale adoption of conventional LTE based ePDG based Wi-Fi calling, this section describes the deployments and trials of various above-the-core solutions.

5.1 MP-TCP

5.1.1 Siri

As described in [33], Apple's Siri digital voice assistant has been using MP-TCP since iOS 7 (September 2013). The primary use case for MP-TCP with Siri is to address the common experience of users engaging with Siri as they are leaving a building, e.g., to ask for travel directions. Hence, it is common for there to be *connectivity events* during a Siri "transaction". Because Siri streams the user's audio to the server, a change in networks would typically mean that a new TCP connection would need to be established and the voice resent to the server. Using MP-TCP, the Siri connection can be seamlessly moved from the indoor Wi-Fi to the outdoor cellular network avoiding any need to resend the audio to the server. This has resulted in a 5-fold decrease in Siri failures because of network connectivity failures.

Since iOS9, Apple has enhanced the MP-TCP capabilities to additionally address the "time to first word" metric. This is the time it takes from a user saying a word to when the device displays the word on the device's screen. From iOS9, the Siri application monitors the round-trip delay experienced on Wi-Fi and when this rises above a threshold, the Siri application will automatically start to use the LTE/cellular connection. This has resulted in a 20% reduction in the time to first word metric, at the 95th percentile, and 30% faster at the 99th percentile [34].

5.1.2 iOS11

iOS11 introduced support for multi-path TCP for application developers, enabling applications on iPhones and iPads to establish multiple sub-flows to a destination host over cellular data and Wi-Fi connections [35]. This capability leverages the URLSession class which is used to support interactions with URLs and communications with servers using standard Internet protocols. The URLSessionConfiguration object controls the behaviour of the session, for example, setting cookie policies, HTTP proxy settings and whether to allow connections on a cellular network.

In iOS11, the URLSessionConfiguration object was enhanced to enable configuration of multi-path TCP. The integrated MP TCP path capability can be used to schedule traffic across Wi-Fi and cellular interfaces.

Apple has defined 4 different service types for controlling the behaviour of MP-TCP operations [36]:

- **None**: The default service type indicating that Multipath TCP should not be used.
- **Handover**: A Multipath TCP service that provides seamless handover between Wi-Fi and cellular in order to preserve the connection.
- **Interactive:** A service whereby Multipath TCP attempts to use the lowest-latency interface.
- **Aggregate**: A service that aggregates the capacities of other Multipath in an attempt to increase throughput and minimize latency.

Note, at the time of writing, the aggregate service is only available for experimentation, requiring an iOS device operating in Developer mode.

5.1.3 MP-TCP Proxy based

5.1.3.1 KT

At the WBA's Wireless Global Congress in November 2017, KT presented their "GiGA LTE" service that uses MP-TCP to combine LTE and Wi-Fi access networks [37]. Using existing smartphones, the GiGA LTE service is able to combine 3 Carrier Aggregated LTE and 802.11ac MIMO networks to deliver a peak 1.17 Gbps service to its users. Claimed benefits when using the service include a 74% increase in download speeds and 66% less LTE usage. This has allowed KT to use their GiGA LTE service to optimize their CAPEX spend whilst attracting higher ARPU customers with the differentiated proposition.

The architecture supporting the GiGA LTE service is based on a combination of MP-TCP together with Socket Secure (SOCKS) [16] functionality, as illustrated in **Figure 5-1**. The use of SOCKS enables the service to be used when accessing servers that are not natively MP-TCP capable. This enables the MP-TCP service to be deployed with minimal impact to existing cellular core and Wi-Fi infrastructure.

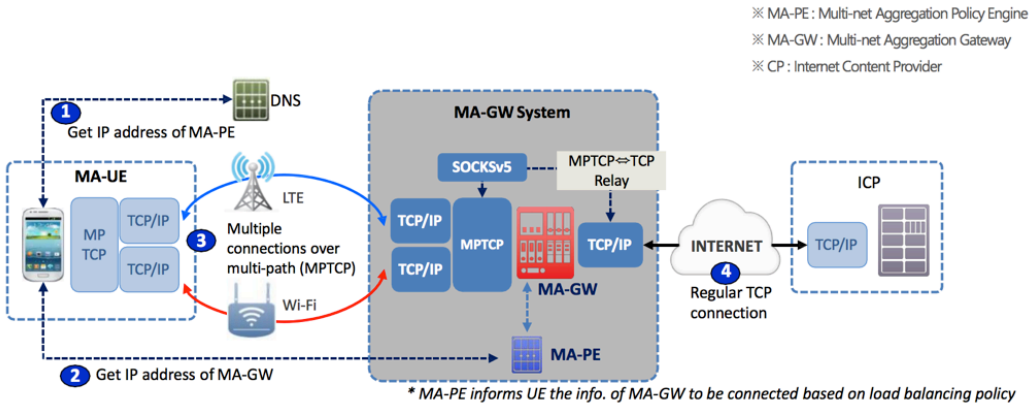
※ MA-PE : Multi-net Aggregation Policy Engine
※ MA-GW : Multi-net Aggregation Gateway
※ CP : Internet Content Provider
1
Get IP address of MA-PE
DNS
MA-GW System
MA-UE
SOCKSv5
MPTCP⇔TCP Relay
ICP
LTE
MP TCP
TCP/IP
TCP/IP
3
Multiple connections over multi-path (MPTCP)
TCP/IP
TCP/IP
MPTCP
TCP/IP
INTERNET
TCP/IP
4
Regular TCP connection
MA-GW
Wi-Fi
MA-PE
2
Get IP address of MA-GW
* MA-PE informs UE the info. of MA-GW to be connected based on load balancing policy

Figure 5-1: GiGA LTE Service Architecture

The client includes functionality to first recover the address of the Multi-net Aggregation Policy Engine (MA-PE). This delivers the IP address of the Multi-net Aggregation Gateway (MA-GW) to the client. This gateway includes SOCKSv5 and MP-TCP capability.

The SOCKS client on the end user device intercepts any TCP connection attempts and triggers the creation of a TCP connection to the SOCKS server/Multi-net Aggregation Gateway. The SOCKS server checks that the subscriber is authorized to use the service and then creates a conventional TCP connection towards the remote server the client is wanting to communicate with.

The end user device will signal that it is MP CAPABLE when establishing the TCP connection to the SOCKs server. This allows the client to send an MP-JOIN over the alternative network to enable the Multi-net Aggregation Network to aggregate the flows over both access network. The SOCKS server relays all data sent over the multipath TCP connections over the conventional TCP connection to the remote server.

With the GiGA LTE implementation, the initial TCP connection to the SOCKs server is always sent over LTE and the MP-JOIN is sent over the Wi-Fi Network.

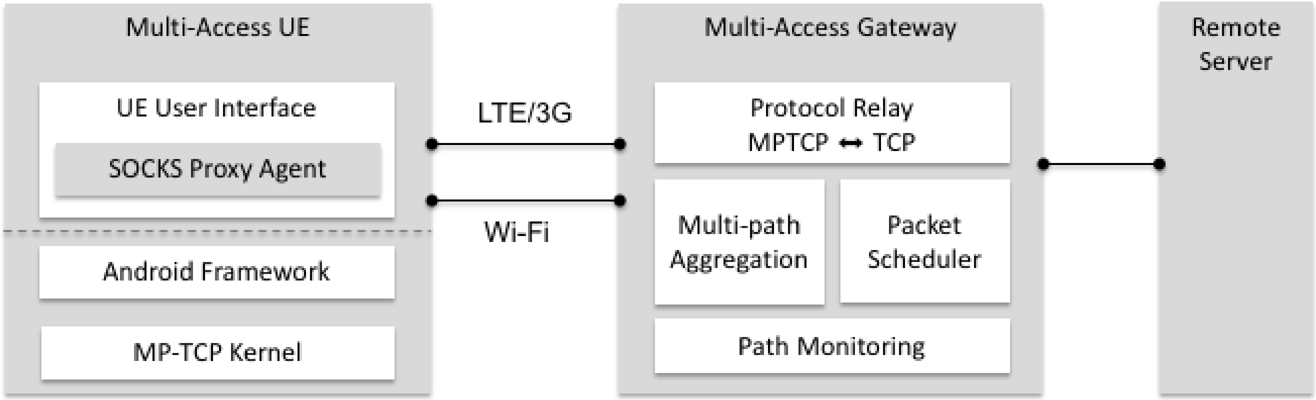

Figure 5-2: GiGA LTE Protocol Functionalities [38]

The MA-UE includes the MP-TCP implementation in the Linux kernel and a SOCKS proxy client in user space, as illustrated in Figure 5-2. An additional user interface is defined to enable subscribers to activate and deactivate the service.

The Multi-Net Aggregation gateway includes the protocol relay between MP-TCP and TCP, Multi-Path aggregation capability based on MP-TCP, a path monitoring capability that can detect network events, e.g., when a previously available Wi-Fi connection is no longer available, and a packet scheduler that can scheduler down-link packets according to policy and the instrumentation provided by the path monitoring functionality.

Following the initial launch of its GiGA-LTE service, in 2016, KT upgraded the service to support 802.11ac wave 2. Branded as “GIGA Wi-Fi 2.0”, this service is claimed to be able to deliver peak speeds of 1.73 Gbps, [39].

5.1.3.2 SKT and LG U+

After the launch of its GiGA-LTE service, both KT’s national competitors, SK Telecom and LG U+, introduced MP-TCP proxy-based LTE-Wi-Fi aggregation services [40]. SK Telecom has branded their service “band LTE Wi-Fi” and LG U+ has branded theirs “Giga Multi-Path”.

5.1.3.3 Other

Netvision, a company that supplies MP-TCP proxy- based LTE/Wi-Fi Data Traffic aggregation solutions for mobile networks, has announced that its technology has been trialled by AIS in Thailand, Vodafone and Turkcell in Turkey and RJIL in India [41].

5.1.4 MP-TCP Hackathon

At the recent IETF 101, the results from the MP-TCP Hackathon which took place in February 2018 have been discussed [42]. The focus of the three-day MP-TCP hackathon was to leverage the native support for MP-TCP in iOS11, to modify applications so as to enable support for MP-TCP, as well as setting up corresponding server capability necessary to demonstrate the end-to-end MP-TCP support. The developers selected a few iOS applications and modified those to enable them to leverage MP-TCP, including a web browser, an internet radio streaming application, and network measuring tools.

When looking at the browser application, unfortunately analysis indicated that it used the WebKit library for its main browser feature, and this library had not been enhanced for multi-path support [43]. Because iOS 11’s MP-TCP is based on URLSessionConfigruration, the only services in the browser that were suitable for MP-TCP were the search suggestion service and the icon service associated with a particular web search.

The radio application did make native use of the URLSessionConfiguration capability and so could be modified for MP-TCP support [44]. As the original streaming service broke on a change of network interface, the addition on MP-TCP added the necessary handover capability to be able to continue the radio session as the user moved between networks.

One of the key takeaways from the Hackathon was the number of parties involved in delivering different applications. In particular, the application developer, who may be motivated to add MP-TCP to their application, is often different and distinct from the organization responsible for delivering the back-end server functionality. Moreover, the browser example showed at least 3 different back end server systems involved in delivering an application, the search service, the search suggestion service and the icon service, all being delivered by different organizations.

The other key takeaway from the Hackathon was the number of 3rd party libraries being leveraged by typical application developers. These do not expose the same set of MP-TCP APIs used by Apple in its URLSessionConfiguration. Moreover, application developers are using other Apple APIs, most notably WebKit, which currently is not multi-path TCP enabled.

5.2 MAMS Deployment Example

Figure 5-3 shows an example of MAMS deployment. The MAMS network data proxy is intercepts the user-plane interface (e.g. N3) between Radio Access Network (RAN) and Core Network function (e.g. UPF), in the way similar to the S1-based MEC (Multi-Access Edge Computing) deployment [45]. Alternatively, MAMS network data proxy may be deployed over the interface (e.g. N6) between Core Network and Internet in the way similar to MPTCP proxy.

In this example, 5G connection is the anchor, and Wi-Fi connection is for delivery. A UDP tunnel is established to deliver user's (5G) IP traffic over the Wi-Fi connection. The UDP tunnel may be further protected by DTLS (Datagram Transport Layer Security) [46] for enhanced security. Alternatively, IPsec can be used to secure the Wi-Fi connection.

The MX Convergence layer can be configured to be an MPTCP proxy or to be trailer-based depending on device/network capabilities and needs. Trailer-based multi-access (MX) convergence sublayer allows MAMS to support MPTCP like aggregation for *any* IP traffic, e.g. TCP, UDP, etc.

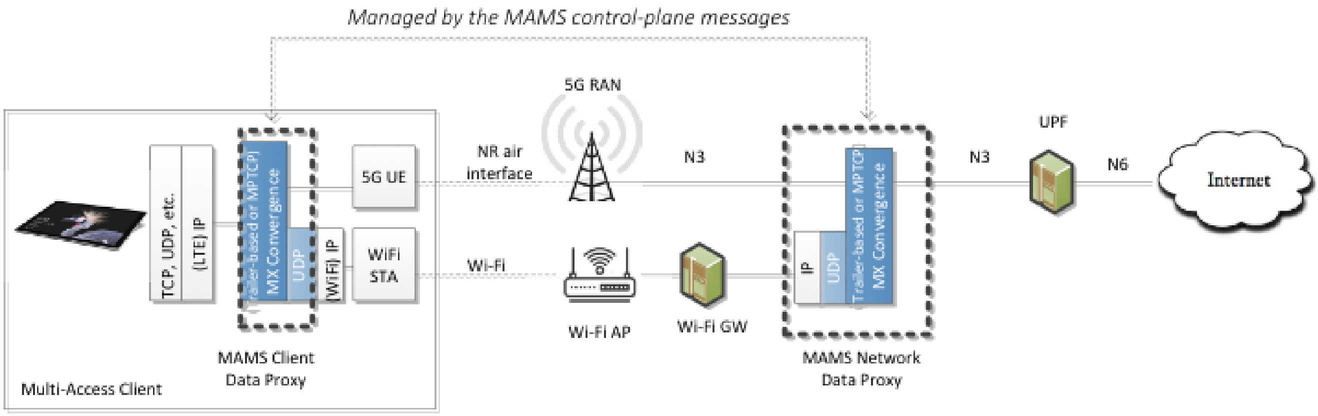

Figure 5-3: MAMS Deployment Example

5.3 MP-QUIC

The performance of MP-QUIC has been compared with MP-TCP in a recent testbed [24]. The MP-QUIC implementation only uses client-initiated paths. In terms of the path manager implementation, the client implementation uses a scheduler that will first send data on sub flows with the lowest RTT until their congestion-window is full. Importantly, when a new path is initialized, the scheduler duplicates traffic over this new path until an estimate of round-trip time is available.

The performance of MP-QUIC has been compared with that of MP-TCP using three different scenarios:

- Large file downloads
- Small file downloads
- Network handover

For large file downloads, a range of different bandwidth-delay profiles and loss ratios were used and, it is reported that the time necessary to deliver the file was lower in 89% of the scenarios when MP-QUIC was used compared with MP-TCP.

Significantly, in high bandwidth-delay tests that may be characteristic of cellular networks, the experiments indicated that MP-TCP only provided aggregation throughput advantage in 20% of the scenarios, versus 58% of the scenarios for MP-QUIC.

For short downloads, the experimental results reported that using multi-path protocols is not desirable. Of course, when operating in single path mode, the 0 RTT operation of QUIC results in performance gains compared with conventional TLS1.2.

For network handover, the ability of a client to use MP-QUIC to signal that a packet has been retransmitted because the initial path has failed, ensures that the server does not use the initial path for sending its response and so leading to improved handover performance.

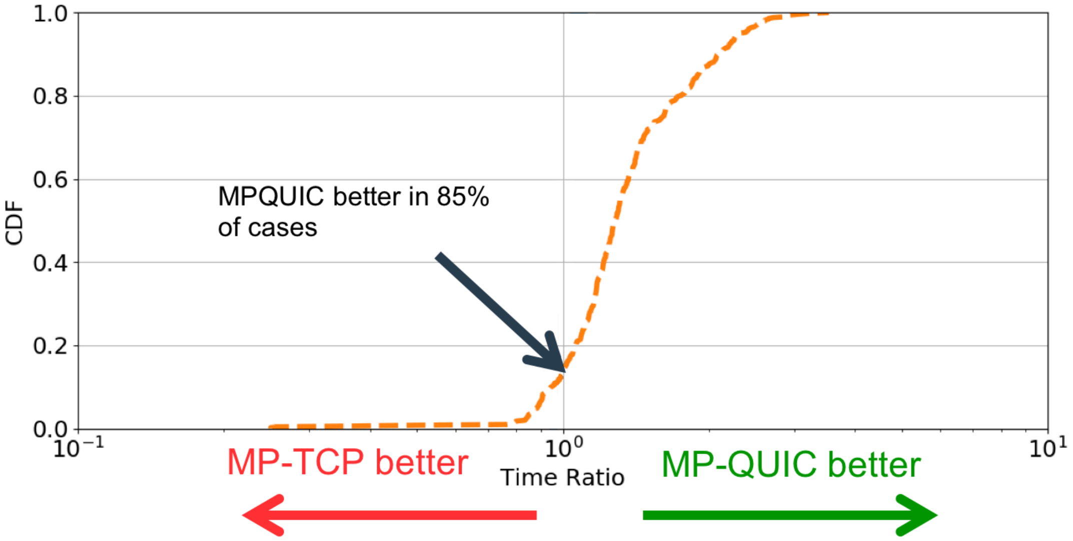

Figure 5-4: Ratio of median download time for large file over MP-QUIC and MP-TCP using a Low Bandwidth-Delay product [47]

Figure 5-4 shows the Cumulative Distribution Function (CDF) for the ratio of MP-TCP download times to MP-QUIC download times, where a value of 1.0 represents equivalent performance for MP-QUIC and MP-TCP, values >1.0 representing shorter download times over MP-QUIC and values of <1.0 representing shorter download times over MP-TCP. As illustrated, in 85% of these experiments, the performance of MP-QUIC outperformed that of MP-TCP. More recently, the same team have developed a multipath tester application for iOS [48]. This application can be used to test the performance of QUIC and MP-QUIC over various Wi-Fi and cellular networks.

6 Challenges

6.1 Fragmentation of Approaches

One of the key challenges with the approaches described in previous sections of this report is the number of alternative approaches available for combing access over Wi-Fi-based and cellular-based access networks.

In order to characterize these alternative approaches, we can use the segmentation introduced earlier to describe some of the drivers that have led to the definition of these alternative solutions.

- **Access Centric Solutions:** These approaches look to opportunistically use the Wi-Fi access network to enhance the core 3GPP access proposition. Current solutions restrict access via the Wi-Fi access network to situations when the device has a signaling connection over the 3GPP access network. As a consequence, Wi-Fi is limited to providing additional capacity to be leveraged by the integrated system. [49]

- **Core Centric Solutions**: These approaches look to define the Wi-Fi access network as a peer of the 3GPP access network and enable them to be integrated into 3GPP core systems. This enables the Wi-Fi networks to provide both additional coverage and capacity while being able to manage the transition between primarily indoor Wi-Fi access networks and primarily outdoor 3GPP access networks.

- **Above -the-core Centric Solutions:** These approaches look to leverage the Wi-Fi access network as a peer of the 3GPP core network, but without the limitations of requiring integration into a 3GPP core system. The multi-path capability may be delivered by 3GPP core system provider, or an application service provider.

Examining the drivers that have led to the definition of access-centric solutions, it is evident that today it could be argued that there are benefits from being able to leverage a Wi-Fi based 802.11ac access network operating in up to 160 MHz of unlicensed spectrum compared with an LAA access network operating in 20 MHz of unlicensed spectrum. However, the differences in bandwidths is being addressed with the definition of 100 MHz 5G systems in sub-6GHz and 400 MHz 5G systems in mm-wave spectrum. These developments may reduce the motivation to integrate Wi-Fi into an access network proposition for pure capacity reasons. Furthermore, the future definition of 3GPP access networks to enable them to operate in the unlicensed 6 GHz band may address earlier drivers that motivated the definition of LWA and LWIP to address co-existence concerns.

As a consequence, the remainder of this section focuses on the challenges associated with solutions that treat the Wi-Fi access network as a peer of the 3GPP defined cellular network.

6.2 Dealing with Device Dependencies

One of the dependencies on delivering effective integration of Wi-Fi and cellular systems is device support. For example, the original core-centric Wi-Fi integration proposition was defined in 2005 as part of 3GPP's interworking WLAN capability [50]. The architecture was subsequently enhanced in 2008 with the LTE Evolved Packet System (EPS) defining integration of non-3GPP access networks. However, it took the release of iOS8 in 2014 to see native support of ePDG based access introduced into the device ecosystem,

Compared to the un-trusted core integration approaches that are now widely available, the integration of Wi-Fi as a trusted access network [51] has currently seen little adoption across the device ecosystem. However, the move by 3GPP to define trusted Wi-Fi access networks as being tightly integrated into the 5G keying hierarchy may lead to increasing levels of adoption of such core-centric approaches. Moreover, sub-section 2.2 has reported on the on-going definition of trusted WLAN integration in Release 16, with one candidate option using an architecture that is common with that used for un-trusted WLAN integration, an approach which is intended to lower barriers to adoption.

Finally, in contrast to core-centric and access-centric propositions what have been defined by 3GPP, it is interesting to characterize the above-the core centric solutions as being driven by software platforms, with QUIC being originally championed by the Chromium project before migrating to the IETF, and MP-TCP being leveraged by Apple native applications since 2013, followed by the availability to all application developers with the launch of iOS11 in 2017.

6.3 Defining Multi-Path Policy

Another key challenge to defining a single approach to integrating Wi-Fi and cellular based networks is the breadth of policy approaches that can be used. There at least three key aspects that impact the policy:

- **Policy Outcome:** As described in Section 4, defines the desired outcome of the policy which may be focused on for example, enhancing the coverage proposition to the user, improving the overall user's perception of performance or targeted at optimizing the costs.
- **Policy Definition:** The entity which defines a particular policy can also differ. This may be a service provider, the user or device provider, or an application provider. In those

scenarios where an enterprise provides a particular service to its employees, it may even be the enterprise itself that defines a particular policy.

- **Policy Applicability:** A policy may be defined to apply homogenously across the device for all applications or services. Alternatively, a policy may be defined in a heterogeneous fashion, where the integration policy deals with only specific applications and/or services.

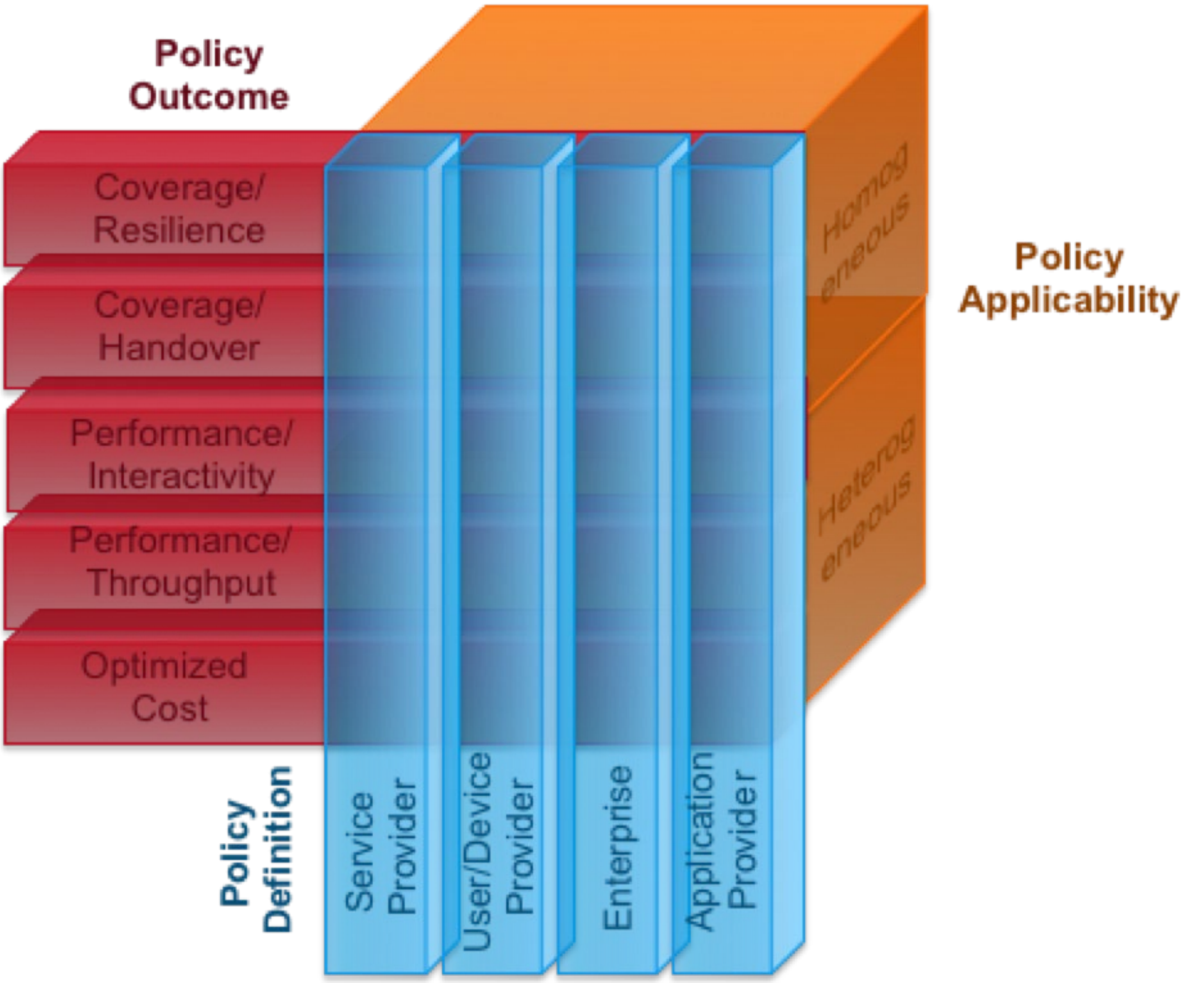

Figure 6-1: Key aspects that impact Wi-Fi Cellular integration policies

Sub section 4.5.2 has introduced the use of policy combining algorithms in other policy use cases focused on access control, even supporting scenarios where some polices contradict each other. It would seem evident that there is an opportunity for the various stakeholders to analyse whether a similar policy combining framework could be used to enhance the integration of Wi-Fi and Cellular networks.

7 Summary

The integration of un-licensed Wi-Fi networks with licensed cellular networks has been a topic that has been repeatedly discussed over the past 15 years or more. There has been an evolution in requirements over this extended period, moving from “switched-mode” or handover use cases where only a single access is used at any time towards a “split-mode” use case where a device may have simultaneous access to multiple accesses over prolonged periods of time.

Moreover, there are multiple different specifications that define the integration between Wi-Fi and cellular, ranging from those where Wi-Fi is integrated into the cellular access-stratum, those that integrate Wi-Fi into the cellular non-access stratum core network, to those that integrate Wi-Fi above-the-core network using IETF defined multi-path protocols.

Clearly this variety of integration approaches can lead to fragmentation of the market and/or delays in deployment as alternative approaches are evaluated. However, from a market adoption perspective, it is evident that to date, compared with widescale adoption of core-centric (focused on VoWi-Fi use cases) and above-the-core centric solutions (focused on multi-path enabling specific applications), there is reportedly only a single deployment of access-centric Wi-Fi integration, with the Global mobile Suppliers Association (GSA) reporting no additional trials of such solutions over the last 12 months.

At least this can motivate a focussing on those core-centric and above-the-core centric solutions where Wi-Fi is treated as a peer of the cellular network (either as a peer access network, for core-centric solutions, or as a peer connectivity network, for above-the-core solutions).

Also, although this document has focused on 5G integration, it is interesting to observe that compared to the widescale deployment of IKEv2 based un-trusted core based integration for LTE, there have not been corresponding deployments of the WLAN Control Protocol (WLCP) for trusted integration in LTE. This has motivated the definition of a solution for trusted WLAN solution into the 5GC that re-uses the same IKEv2 approach for both trusted and un-trusted, making the solutions almost identical. Using such a common approach is then hoped to increase the likelihood of trusted integration of WLAN into the 5GCN. However, it remains unclear whether this is the only barrier for deploying such solutions, e.g., compared with the ease by which untrusted solutions can be incrementally deployed leveraging legacy infrastructure.

The widescale deployment of multi-path based solutions has also led to the inclusion of such approaches into candidate solutions for the 3GPP defined 5GCN-centric integration. However, with the multi-path solutions largely being currently driven by platform ecosystems (iOS and Chromium), it is less clear whether the success of above-the-core centric multi-path solutions will translate into successful adoption of such techniques for delivering core-centric solutions, especially if the architectures define path management as being the sole responsibility of the core network operator.

Finally, if there is broad alignment moving forward to focus on Wi-Fi as a peer network with split-mode multi-path solutions from a user plane perspective, there looks to be less alignment on the critical aspects of control plane and policy. Instead of defining siloed policy solutions that are built on the assumption that a single entity is responsible for policy definition, there is an opportunity to investigate how the definition of a common policy framework could facilitate efforts to deliver enhanced experiences over multi-path solutions. Such a framework will need to examine algorithms for policy combining that can support the broad range of use cases covered in this paper.

8 Recommendations

The WBA 5G work group have put together a series of recommended next steps based on this white paper in order to align the industry players and avoid fragmentation and delays. Subject to agreement:

1. The WBA recommends and advocates integration solutions which treat Wi-Fi as a peer of the cellular network, i.e. core-centric solutions where Wi-Fi is treated as a peer of the cellular access network, or above-the core solutions, where Wi-Fi is treated as a peer connectivity network.

2. The WBA recommends next steps in the program to analyze the instrumentation capabilities of Wi-Fi networks that can support various policy outcomes (performance-based, load-based, financial-base, improved-resilience).This should include instrumentation that relates to financial cost of the Wi-Fi service, analyzing the benefits of using of HS2.0 network's "Access Network Type" query to determine whether the Wi-Fi network corresponds to a "Free Public Network" or a "Chargeable Public Network".

3. WBA, will liaise with the GSMA, to analyze the benefits of better instrumentation of the non-Wi-Fi (cellular) experience, to enable a more holistic view of the performance over the plurality of networks able to be leveraged by a particular device.

4. WBA, in co-operation with other stakeholders, will investigate how the definition of a common policy framework could facilitate efforts to deliver enhanced experiences over multi-path solutions. Such a framework will need to examine algorithms for policy combining that can support the broad range of use cases covered in this paper.

5. WBA will survey its membership on the key barriers to deployment of various solutions, for example, including trusted WLAN integration, visited N3IWF deployment, integration with fixed networks, SMF/UPF integration with sliced Wi-Fi networks.

6. WBA will liaise with the GSMA regarding clarifications regarding support for non EAP-AKA’ methods, in particular being able to leverage earlier WLAN integration approaches that supported non-SIM based roaming.

7. WBA will continue to liaise with IEEE and 3GPP to understand the potential benefits of defining a secondary identifier in the Access Network ID for use in trusted WLAN deployments.

WBA invites the broader industry to join it in addressing these recommendations - for more information and to learn how to engage please contact WBA PMO (pmo@wballiance.com).

REFERENCES

[1] https://www.fiercewireless.com/wireless/how-much-cellular-and-wi-fi-data-are-smartphone-users-consuming-and-which-apps-verizon-0

[2] https://www.wballiance.com/resource/5g-networks-the-role-of-wi-fi-and-unlicensed-technologies/

[3] "WBA Unlicensed Spectrum LTE - Market Drivers and Roadmap", http://www.wballiance.com/resource/unlicensed-spectrum-lte-market-drivers-and-roadmap/

[4] “WBA Industry perspectives, trusted WLAN architectures and deployment considerations”, http://www.wballiance.com/resource/industry-perspectives-trusted-wlan-architectures-and-deployment-considerations/

[5] GSMA Paper: Road to 5G: Introduction and Migration: April 2018, https://www.gsma.com/futurenetworks/wp-content/uploads/2018/04/Road-to-5G-Introduction-and-Migration_FINAL.pdf

[6] 3GPP TS23.793, “Study on access traffic steering, switch and splitting support in the 5G system architecture”, http://www.3gpp.org/ftp//Specs/archive/23_series/23.793/23793-100.zip

[7] 3GPP TS 24.501, “Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3” http://www.3gpp.org/ftp//Specs/archive/24_series/24.501/24501-f10.zip

[8] TS23.501, “System Architecture for the 5G System” http://www.3gpp.org/ftp//Specs/archive/23_series/23.501/23501-f30.zip

[9] RFC 7296, “Internet Key Exchange Protocol Version 2 (IKEv2)”, https://trac.tools.ietf.org/html/rfc7296

[10] 3GPP TS33.501, “Security architecture and procedures for 5G System”, http://www.3gpp.org/ftp//Specs/archive/33_series/33.501/33501-f20.zip

[11] 3GPP TS 23.502, “Procedures for the 5G System” http://www.3gpp.org/ftp//Specs/archive/23_series/23.502/23502-f30.zip

[12] “Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')” https://tools.ietf.org/html/draft-ietf-emu-rfc5448bis

[13] https://www.wballiance.com/resource/network-slicing-understanding-wi-fi-capabilities-2/

[14] “An Overview of Multipath TCP”. http://www0.cs.ucl.ac.uk/staff/M.Handley/papers/9346-login1210_bonaventure.pdf

[15] RFC 6824, “TCP Extensions for Multipath Operation with Multiple Addresses”, IETF https://tools.ietf.org/html/rfc6824

[16] RFC 1928, “SOCKS Protocol Version 5”, IETF, https://tools.ietf.org/html/rfc1928

[17] “0-RTT TCP Converter”, draft-bonaventure-mptcp-converters

[18] “Multiple Access Management Services”, https://www.ietf.org/id/draft-kanugovi-intarea-mams-framework-01.txt

[19] “QUIC: A UDP-Based Multiplexed and Secure Transport”, https://datatracker.ietf.org/doc/draft-ietf-quic-transport/

[20] “QUIC, a multiplexed stream transport over UDP”, https://www.chromium.org/quic

[21] “Why the Meteoric Rise of Google QUIC is Worrying Mobile Operators”, https://owmobility.com/blog/meteoric-rise-google-quic-worrying-mobile-operators/

[22] “QUIC Working Group”, https://www.youtube.com/watch?v=fcPb_x2PXsQ

[23] “Multipath Extension for QUIC”, draft-deconinck-quic-multipath

[24] “Multipath QUIC: Design and Evaluation”, https://multipath-quic.org/conext17-deconinck.pdf

[25] “Reliability enhancement for LTE using MPQUIC in a mixed traffic scenario”, https://projekter.aau.dk/projekter/files/281252124/MasterThesisFinal.pdf

[26] “A socket API to control Multipath TCP”, https://datatracker.ietf.org/meeting/96/materials/slides-96-mptcp-4.pptx

[27] WBA Convergence of Cellular and Next Gen Wi-Fi Networks – ANDSF and HS2.0 Policies: Policy Interworking, https://www.wballiance.com/resource/convergence-of-cellular-and-next-gen-wi-fi-networks-andsf-and-hs2-0/

[28] “Enhanced Wi-Fi – 802.11ax Decoded”, WBA, https://www.wballiance.com/resource/enhanced-wi-fi-802-11ax-decoded

[29] “A socket API to control Multipath TCP”, draft-hesmans-mptcp-socket

[30] “How Hard Can It Be? Designing and Implementing a Deployable Multipath TCP”, https://inl.info.ucl.ac.be/system/files/nsdi12-final125.pdf

[31] “LTE Unlicensed - LTE in Unlicensed Spectrum: Trials, Deployments and Devices”, https://gsacom.com/paper/lte-in-unlicensed-spectrum-trials-deployments-and-devices/

[32] https://en.wikipedia.org/wiki/XACML

[33] “iOS & Linux: Implementation Updates”, https://datatracker.ietf.org/meeting/99/materials/slides-99-mptcp-sessa-ios-linux-implementation-updates

[34] “Multipath TCP Deployments”, https://www.ietfjournal.org/multipath-tcp-deployments/

[35] “Improving Network Reliability Using Multipath TCP”, https://developer.apple.com/documentation/foundation/urlsessionconfiguration/improving_network_reliability_using_multipath_tcp

[36] “URLSessionConfiguration.MultipathServiceType”, https://developer.apple.com/documentation/foundation/urlsessionconfiguration.multipathservicetype

[37] “WiFi and Mobile Best Connected :GiGA LTE”, https://www.wballiance.com/wp-content/uploads/2017/11/WBA_NYC2017_SUNGHOON_SEO__KT_THURSDAY_MAIN_PLENARY.pdf

[38] “KT’s GiGa LTE: - Commercial Mobile MPTCP Proxy service launch - Collaboration with handset manufacturers”https://www.ietf.org/proceedings/93/slides/slides-93-mptcp-3.pdf

[39] “Korea Communications Review”, https://www.slideshare.net/Netmanias/netmanias20160801kcragust2016

[40] “Analysis of LTE – WiFi Aggregation Solutions”, https://www.netmanias.com/en/post/reports/8532/laa-lte-lte-u-lwa-mptcp-wi-fi/analysis-of-lte-wifi-aggregation-solutions

[41] http://www.netvisiontel.com/nv/work/index.html

[42] “MP-TCP Implementation Update”, https://datatracker.ietf.org/meeting/101/materials/slides-101-mptcp-mptcp-implementation-update-00

[43] https://github.com/multipath-tcp/hackathon_2018/tree/master/brave_ios_mptcp

[44] https://github.com/multipath-tcp/hackathon_2018/tree/master/Radio_ios_mptcp

[45] “MEC Deployments in 4G and Evolution Towards 5G”, http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp24_MEC_deployment_in_4G_5G_FINAL.pdf

[46] “Datagram Transport Layer Security Version 1.2”, RFC 6347, https://tools.ietf.org/html/rfc6347

[47] “Multipath QUIC: Design and Evaluation”, https://conferences2.sigcomm.org/co-next/2017/presentation/S4_2.pdf

[48] https://itunes.apple.com/us/app/multipathtester/id1351286809

[49] WBA “Unlicensed Spectrum LTE**”,** https://www.wballiance.com/unlicensed-spectrum-lte/

[50] 3GPP TS23.234, “3GPP system to Wireless Local Area Network (WLAN) interworking; System description”, http://www.3gpp.org/ftp//Specs/archive/23_series/23.234/23234-d10.zip

[51] WBA “Industry perspectives, trusted WLAN architectures and deployment considerations for integrated Small-Cell Wi-Fi (ISW) networks”,https://www.wballiance.com/wp-content/uploads/2016/04/SCF_WBA_industryperspectives_wi-fi_isw_networks.pdf

ACRONYMS AND ABBREVIATIONS

ACRONYM / ABBREVIATION	DEFINITION
AMF	Access and Mobility Function
ARPF	Authentication credential Repository and Processing Function
ATSSS	Access Traffic Steering, Switching and Splitting
AUSF	Authentication Server Function
BSSID	Basic Service Set Identifier
C-MADP	Client Multi Access Data Proxy
DSCP	Differentiated Service Code Point
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
ePDG	Evolved Packet Data Gateway
GRE	Generic Routing Encapsulation
GSA	GSM Suppliers Association
GTP	GPRS Tunneling Protocol
LAA	Licenses Assisted Access
LWA	LTE WLAN Aggregation
LWIP	LTE WLAN Radio Level Integration with IPsec Tunnel
MAMS	Multi Access Management Services
MEC	Multi-Access Edge Compute
MP-QUIC	Multipath QUIC
MP-TCP	Multipath TCP
MX	Multi-Access
N3IWF	Non-3GPP Inter-Working Function
NAT	Network Address Translation

N-MADP	Network Multi Access Data Proxy
NAS	Non-Access Stratum
NCM	Network Connection Manager
NR	New Radio
NSA	Non-Stand Alone
PDU	Protocol Data Unit
PLMN	Public Land Mobile Network
QFI	QoS Flow Information
QoS	Quality of Service
QUIC	Quick UDP Internet Connection
RTT	Round Trip Time
SA	Security Association
SEAF	Security Anchor Function
SMF	Session Management Function
SOCKS	Socket Secure
SSID	Service Set Identifier
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
UDM	Unified Data Management
UPF	User Plane Function
WBA	Wireless Broadband Alliance
WGC	Wireless Global Congress
WWD	World Wi-Fi Day™
XACL	eXtensible Access Control Markup Language

PARTICIPANT LIST

COMPANY	NAME	ROLE
Orange	Nigel Bird	Project Leader
Cisco	Mark Grayson	Chief Editor & Project Co-Leader
Broadcom	Florin Baboescu	Project Co-Leader
Intel	Necati Canpolat	Project Co-Leader
Accuris Networks	Finbarr Coghlan	Editorial team member
BT	Simon Ringland	Editorial team member
Huawei	Lei Wang	Editorial team member
Intel	Jing Zhu	Editorial team member
Nokia	Thierry Van de Velde	Editorial team member
Aruba, an HPE company	Stuart Strickland	Project Participant
Aruba, an HPE company	Peter Thornycroft	Project Participant
BSG Wireless	Betty Cockrell	Project Participant
BSG Wireless	Michael Sym	Project Participant
BT	Steve Dyett	Project Participant
BT	Tim Twell	Project Participant
C-DOT	Sandeep Agrawal	Project Participant
Charter Communications	Mohammad Said	Project Participant
Smith Micro Inc.	Dzung Tran	Project Participant
Starry Internet	Nick Ilyadis	Project Participant
ViaSat	Peter Flynn	Project Participant

For other publications please visit:
wballiance.com/resources/wba-white-papers

To participate in future projects, please contact:
pmo@wballiance.com

READ MORE