Published on *Telsoc* (https://telsoc.org)

The 4G to 5G Network Architecture Evolution in Australia

David Soldani [1]

Huawei Technologies (Australia)

Malcolm Shore [2]

Huawei Technologies (Australia)

Jeremy Mitchell [3]

Huawei Technologies (Australia)

Mark Gregory [4]

RMIT University

AJTDE - Vol 6, No 4 - November 2018 [5]

[6]

☆ 119[7]

Abstract

This paper provides a review of selected design and security aspects of 5G systems and addresses key questions about the deployment scenarios of Next Generation Radio Access Networks in Australia. The paper first presents the most relevant 5G use cases for the Australian market in 2018-19, and beyond; 5G concept and definitions; 3GPP updates, in terms of system architecture and enabling technologies and corresponding timelines; and spectrum availability, linked to possible 5G deployments in Australia. Then, the paper discusses the 5G functional architecture, possible configuration options, enabling technologies and network migration strategies and related 5G security, in Australia and globally. This is followed by a description of the possible 5G deployment scenarios in a multivendor environment and includes, as a case study, the Huawei product portfolio and site solution in Australia. The paper concludes with a discussion on the potential benefits of a telecommunications security assurance centre to improve the whole-of-life security assurance of critical telecommunications infrastructure and why it is important for the Australia telecommunications sector.

Introduction

This paper reviews the most relevant technology transition options from the current 4G telecommunications network ecosystem into a 5G network ecosystem. In this paper, we set out the frameworks and roadmaps that Australian communication service providers may take to 5G. Recently the Australian Government issued security guidance on 5G systems to Australian carriers that presents a view on how 5G deployments will occur and evolve over time (Morrison and Fifield, 2018 [8]), thereby providing the motivation for this review of the relevant aspects of the 5G standards and technologies. For the purpose of explanation, the Huawei 5G solutions will be referenced in this paper to provide a case study of how the standards are applied by an international telecommunications vendor.

The 3GPP 5G System design has been based on technical requirements identified by various organisations, with the most prominent input being, perhaps, the Next Generation Mobile Networks (NGMN) 5G Whitepaper (NGMN, 2015 [9]), which provides functional design and migration considerations from a network operator perspective. 5G will be the driver of the next wave of economic productivity growth across the globe. The Asia-Pacific region is leading in the commercial delivery of 5G technology, with Japan, South Korea and China already announcing a timetable of commercial 5G rollouts. Countries like the US, Australia and the United Kingdom (UK) have also recently started trials and preliminary network rollouts.

Huawei has been chosen to be the case study for 5G system implementation because it is a recognised international telecommunications vendor that is already working closely with operators and governments in many countries. Huawei is also delivering 5G trials in the UK, Canada and New Zealand and working with the corresponding governments and operators to ensure that their citizens have access to the best 5G technologies that meet performance, security, dependability and privacy expectations.

5G is an evolutionary transition from 4G and, while there will be fundamental changes in network abilities and services delivered, the network principles remain the same (Kennedy, 2018 [10]). A key principle is that there is a clear standardised interface and separation between Core Network (CN) and Radio Access Network (RAN) across the whole transition of deployments and in a final 5G standalone environment (Guttman, 2018 [11]).

As in previous 3GPP systems, the 5G Access to CN boundary has been set out in the 3GPP global standards with a clear functional split and offers globally accepted principles. This enables the adoption of different business models, and the utilisation of RAN equipment from one vendor and core elements from other network infrastructure providers, like existing 4G network deployments in Australia. To identify how the clear functional split between the 5G Access and CN will be supported during the transition from 4G to 5G, the Huawei product portfolio and site solution for the Australian market is presented, as a case study of the potential technology solution.

The paper also provides a discussion on the potential benefits of a telecommunications security assurance capability. Whole-of-life security assurance of critical telecommunications infrastructure is a vital component of best practice for telecommunication network and system security. The transition from legacy fixed access networks to the National Broadband Network (NBN) and from 4G to 5G provides an opportunity to develop and introduce a telecommunications security assurance capability that will reduce infrastructure and system-related security risks.

5G Use Cases

5G technology is starting to be deployed. In Australia, carriers have showcased 5G networks at the 2018 Gold Coast Commonwealth Games, ahead of the announced 5G services launch in 2019: see, for example, Foye (2018a [12]) and Foye (2018b [13]).

The family of usage scenarios for International Mobile Telecommunications (IMT) for 2020 and beyond for 5G include: 1) âEnhanced mobile broadband (eMBB)â addressing human-centric use cases for access to multimedia content, services and data; 2) âUltra-reliable-low latency communications (URLLC)â with strict requirements, especially in terms of latency and reliability; and 3) âMassive machine type communications (mMTC)â for a very large number of connected devices typically transmitting a relatively low volume of non-delay-sensitive information (ITU-T, 2018 [14]).

The 5G service specifications for eMBB, URLLC and mMTC (ITU-T, 2018 [14]), (3GPP, 2018a [15]) provide the high-level performance targets for 5G. The targets described as part of the IMT 2020 development support use-case classes for various different services with similar performance requirements: e.g. industrial automation and mission critical communications both require low latency.

Examples of use cases related to the three usage scenarios are, as depicted in Figure 1:

1. **5G fixed wireless access (FWA)**: Complements fibre networks and replaces the last 50-200 m of fibre. It provides a âGigabit-Speed Internetâ experience at home. For each household, for example, the sustainable speed could be 100 Mb/s in the downlink (DL) at 3.5 GHz/1800 MHz with 5G/LTE shared uplink transmission (SUL), and even up to 800 Mb/sâ1 Gb/s at 26 GHz. See e.g. Soldani (2017a [16]).
2. **Virtual (VR), Augmented (AR) and Mixed Reality (MR)** A full immersive and interactive experience for 5G hotspots, in-vehicle infotainment, gaming etc. The most important 5G requirements are: Latency < 10 ms; Throughput > 1 Gb/s; and cell capacity of more than 500 connections. See e.g. Elbamby (2018 [17]).
3. **Industrial Processes Automation**: Remote drilling, wireless service robots, drone traffic management etc. The 5G system is expected to support latency below 10 ms, and speed above 10 Mb/s. See e.g. Soldani (2017b [18]).
4. **Remote Control of Vehicles**: Truck control in mining sector, truck platooning, autonomous driving etc. The 5G system is expected to support latency below 10 ms, and deliver a speed above 50 Mb/s. See e.g. ITU-T (2018 [14]), 3GPP (2018a [15]).

Services in use cases 3 and 4 are expected to be provided only in specific and safe areas, or by deploying dedicated networks, such as GSM-R (Railways).

[19]

1. Examples of use cases in Australia

The use cases described in this section are examples of services that require the deployment of a next generation access technology and, in some cases, a next generation core network, as none of the previous 3GPP network generations (3GPP releases), i.e. 2G, 3G and 4G, supports all of such stringent performance requirements and targets (ITU-T, 2018 [14]; 3GPP, 2018a [15]).

5G Definitions and Standards Updates

5G Wireless has been defined as the 3GPP Release 15 (R15) and later releases (R16, R17 etc.) of LTE and New Radio (NR) mobile communication systems. It is thus an *LTE advanced pro evolution and an NR technology*that adds to existing 3GPP networks.

The 3GPP proposes standards that are compliant with the IMT-2020 and beyond for adoption by the ITU. The ITU IMT 2020 expands and supports diverse usage scenarios and applications with respect to current mobile network generations, purposed primarily for voice, mobile internet and video experience (ITU-T, 2018 [14]).

The Next Generation Radio Access Network (NG-RAN) represents the newly defined radio access network for 5G, and provides both NR and LTE radio access (Guttman, 2018 [11]): see Figure 2.

An NG-RAN node (i.e. a base station) shown in Fig. 2a is either:

- A gNB (i.e. a NR base station), providing NR user plane (UP), i.e. user data, and control plane (CP), i.e. signalling, services; or
- An ng-eNB (i.e. an evolved LTE base station), providing LTE/E-UTRAN services towards the User Equipment (UE). (E-UTRAN means Evolved Universal Terrestrial Radio Access Network.)

The 5G System (5GS) consists of NG-RAN and 5G Core Network (5GC), as depicted in Figure 2a. The 3GPP Option 3 scenario is provided in Fig. 2b.

[20]

Figure 2. Overall 5G architecture: a) 5G system (5GS); b) 3GPP Option 3

The NG RAN operates in both so-called âStand-Aloneâ (SA) operation and âNon-Stand-Aloneâ (NSA) operation. In SA operation, the gNB is connected to the 5G Core Network (5GC); in NSA operation, NR and LTE are tightly integrated and connect to the existing 4G Core Network (EPC), leveraging Dual Connectivity (DC) towards the terminal. In a DC architecture, a Master Node (MN) and a Secondary Node (SN) concurrently provide radio resources towards the terminal for an enhanced end-user bit rate (speed or throughput) (Guttman, 2018 [11]). Moreover, 3GPP has defined the following architecture configurations, see Guttman (2018 [11]), Soldani (2018a [21]), 3GPP (2018b [22]), Figure 2 and Figure 3.

- **SA Option 2: NR gNB connected to 5GC**

In this option, the gNBs are connected to the 5GC through the NG interface. The gNBs interconnect through the Xn interface.

- **SA Option 5: LTE ng-eNB connected to 5GC**

In this option, the ng-eNBs are connected to the 5GC through the NG interface. The ng-eNBs interconnect through the Xn interface. Essentially this option allows the existing LTE radio infrastructure (through an upgrade to the eNB) to connect to the new 5G Core.

- **NSA Option 3: Multi-RAT DC with EPC**

In this option, commonly known as Multi-Radio Access Technology (Multi-RAT), LTE-NR Dual Connectivity (EN-DC), a UE is connected to an eNB that acts as a MN and to an en-gNB that acts as an SN. An en-gNB is different from a gNB in that it only implements part of the 5G base station functionality, which is required to perform SN functions for EN-DC. The eNB is connected to the EPC via the S1 interface and to the en-gNB via the X2 interface. The en-gNB may be also connected to the EPC via the S1-U interface and to other en-gNBs via the X2-U interface. Notice that the en-gNB may send user-plane packets to the EPC either directly or via the eNB (secondary bearer split).

- **NSA Option 4: Multi-RAT DC with the 5GC and NR as Master**

In this option, a UE is connected to a gNB that acts as a MN and to an ng-eNB that acts as an SN. This option requires the 5G Core to be deployed. The gNB is connected to 5GC and the ng-eNB is connected to the gNB via the Xn interface. The ng-eNB may send user-plane packets to the 5G Core either directly (Option 4a) or via the gNB (Option 4).

- **NSA Option 7: Multi-RAT DC with the 5GC and E-UTRAN as Master**

In this option, a UE is connected to an ng-eNB that acts as a MN and to a gNB that acts as an SN. The ng-eNB is connected to the 5GC, and the gNB is connected to the ng-eNB via the Xn interface. The gNB may send user-plane packets to the 5GC either directly or via the ng-eNB (Guttman, 2018 [11]).

[23]

Figure 3. 3GPP architecture configurations

3GPP 5G roadmap

As illustrated in Figure 4, the completion of the first 5G phase (Phase 1 or Release 15, R15) of the NR Access technology was in June 2018, in its NSA Option 3 configuration (3GPP, 2018b [22]). The NSA Options 4 and 7 will be finalised during the first quarter (Q1) of 2019. The SA Options 2 and 5 were completed in September 2018. The 3GPP R15 will support eMBB and some elements of URLLC, e.g. flexible numerology, packet duplication, uplink grant free, downlink pre-emption, and reduced scheduling interval (mini-slot scheduling). A more profound URLLC analysis can be found, e.g., in 3GPP (2018c [24]) and Soldani (2018b [25]).

The second 5G phase (Phase 2 or Release 16, R16), supporting usage scenarios, including URLLC and mMTC, will be frozen in Q1 of 2020 or later (3GPP, 2018b [22]).

[26]

Figure 4. 3GPP definition of 5G: LTE evolution and New Radio (NR), supporting new usage scenarios

Spectrum

5G NR is expected to increase spectrum efficiency and support contiguous, non-contiguous, and much broader channel bandwidths than available to earlier generation mobile networks. The new 5G radio will be the most flexible way to benefit from all available spectrum options from 400 MHz to 90 GHz, including licensed, shared access and licence-exempt bands, FDD and TDD modes with Supplementary Uplink (SUL), LTE/NR uplink sharing (ULS), and narrowband and wideband Carrier Components (CC) (Soldani, 2018a [21]). The standardised operating band combinations for SUL and ULS may be found in 3GPP (2018d [27]).

A multi-layer spectrum approach is required to address such a wide range of usage scenarios and requirements (Huawei, 2018 [28]):

- The "**Coverage and Capacity Layer**" relies on spectrum in the 2 to 6 GHz range (e.g. C-band) to deliver the best compromise between capacity and coverage.
- The "**Super Data Layer**" relies on spectrum above 6 GHz (e.g. 24.25-29.5 and 37-43.5 GHz) to address specific use cases requiring extremely high data rates.
- The "**Coverage Layer**" exploits spectrum below 2 GHz (e.g. 700 MHz) providing wide-area and deep indoor coverage.

[29]

Figure 5. Global spectrum allocation and upcoming auction of 5G spectrum at 3.6 GHz in Australia

5G networks will leverage the spectrum available from the three layers at the same time, and the national spectrum management agencies are expected to make available contiguous spectrum in all layers in parallel, to the greatest extent possible.

Figure 5 depicts the global availability and planning of the frequency ranges for 5G usage and the upcoming auction of 5G spectrum in the **3.6 GHz** band in Australia. The Australian Communications and Media Authority (ACMA) is preparing to allocate spectrum in the frequency range 3575 MHzâ3700 MHz (125 MHz) in metropolitan and regional Australia by auction in October 2018 (ACMA, 2018 [30]). Frequencies in the **3.4 GHz** band have been already assigned in Australia. The **700 MHz** spectrum (band 28) sold at recent auction (ACMA, 2017 [31]), which adds to the spectrum made available in 2013, will be used extensively throughout Australia to provide 4G mobile broadband or 5G coverage in the future. The allocation of mmWave spectrum, between 24.25 GHz and 27.5 GHz (**26 GHz** band), is expected in Q1 2019.

5G Deployment Scenarios and Migration Strategies

The most likely initial deployment options are illustrated in Figure 6, see e.g. Guttman (2018 [11]) and 3GPP (2018e [32], 2018f [33], 2018g [34], 2018h [35]).

- **3GPP Option 3x** (NSA LTE plus NR with EPC) is the configuration that is most likely to be adopted by network operators globally, including those in Australia, due to minor investments for their initial 5G deployments. It supports eMBB and FWA use cases and Voice over IP (VoIP) over LTE (VoLTE) or Circuit Switch Fallback (CSFB) to earlier network releases (3G, 2G).
- **3GPP Option 2** (SA NR with 5GC) is expected initially to be adopted by only a few of the network operators globally. To take full advantage of this option, a wide coverage rollout is needed, as the interoperation with 4G Evolved Packet System (EPS) is less efficient. Initial partial coverage rollouts may be more suitable for enterprise or overlay deployments. In the long run, it will support all scenarios (eMBB, URLLC, mMTC), plus other functionalities than Option 3x, such as Network Slicing and Voice over NR (VoNR).

[36]

Figure 6. Main initial 5G deployment options (3GPP, 2018e [32], 2018f [33], 2018g [34], 2018h [35])

The medium- to long-term migration path of 5G networks is illustrated in Figure 7. Ultimately, all networks will converge to a 3GPP Option 2 architecture configuration (SA NR with 5GC).

[37]

Figure 7. Long-term migration paths (Guttman, 2018 [11])

The medium-term migration strategies are basically two, depending on the carriersâ spectrum availability for deploying the NR (Guttman, 2018 [11]):

- **From deployed 3GPP Option 3x (NSA LTE + NR with EPC) to 3GPP Option 7 (NSA eLTE + NR with 5GC)** The reasons to go for that are: Leverage 4G (LTE/EPC) installed base; NR rollout driven by better service (not coverage); and evolved LTE (eLTE) for all wide area coverage and all use cases. The drawbacks are: Full Dual Stack eNB/ng-eNB in LTE RAN to EPC/5GC; LTE RAN upgrades to eLTE; and required interworking between LTE and NR. UE availability is also, currently, questionable. The migration scenario is shown in Figure 8a.
- **From deployed 3GPP Option 3x (NSA LTE + NR with EPC) to 3GPP Option 4 (NSA NR + eLTE with 5GC)** This choice is driven by the availability of low band NR (<3 GHz, <1 GHz for rural). The 5G services are launched with LTE+NR NSA on EPC; the NR and 5GC rollouts are driven by needs of 5G coverage; outside the NR coverage, 5G services may be provided by 3GPP LTE NSA Option 4 with 3GPP Option 5 (SA eLTE with 5GC). Interworking between eLTE and NR is also required. The migration scenario is depicted in Figure 8b.

[38]

Figure 8. Medium-term migration -- Anticipated Australian migration strategy: a) From 3GPP NSA Option 3x to 3GPP NSA Option 7; b) From 3GPP NSA Option 3x to 3GPP NSA Option 4

5G Reference Architecture

As in previous mobile system generations, 3GPP defines a clear functional split between the Access Network (NG-RAN) and Core Network (5GC), with the overall 5G System architecture defined in 3GPP (2018g [34]) and a more convenient overview of the AN and CN functions in 3GPP (2018h [35]). The two network domains are separated by a *standardised interface* (N2 and N3) defined in a set of specifications, with 3GPP (2018i [39]) as the overarching specification which enables multi-vendor RANâCN deployments. Also, this interface has now been *unified*, meaning that all next generation wireless access configurations (trusted/untrusted fixed/mobile 3GPP access points) must support this interface.

The NG-RAN supports intercell radio resource management (RRM), radio bearer (RB) control, connection mobility control, radio admission control, measurements configuration and provisioning, and dynamic resources allocation.

The 5GC is responsible for non-access stratum (NAS) security and idle state mobility handling; user equipment IP address allocation and protocol data unit (PDU) control; and mobility anchoring and PDU session management.

The functional split between the NG radio and core domains is shown in Figure 9 to Figure 14, where the possible multi-vendor implementation (equipment from different vendors) of the corresponding network domain functions is also illustrated.

The 3GPP NG-RAN (NR, or gNB in 3GPP) comes with two possible configurations:

- **Central Unit (CU)-Distributed Unit (DU) split** The RAN non-real time protocol stack is implemented in the CU and the functions more sensitive to delays in the DU close to the antennas.
- **CU-DU co-located at the Edge of the network** All RAN baseband functionalities are running in one box placed close to the antenna units.

Single vendor CU-DU solutions may be deployed as a CU-DU co-located option using *dedicated hardware and software*. Huawei has demonstrated that this proprietary solution is efficient to operate, cost effective, and highlights why there will be vendor-specific solutions implemented in segments of the mobile networks. 4G and NG-RAN elements â the baseband units (BBU) â will actually be deployed on the same site, with no need to reduce the transmission capacity between sites with a centralised CU deployment. Some vendors and mainstream carriers have agreed on a CU and DU integrated deployment as illustrated in Figure 13, thereby making 4G/5G co-site deployments the likely industry trend.

Both the user plane and control plane architectures for NG-RAN follow the same high-level architecture scheme, as depicted in Figure 10.

Figure 11 and Figure 12 show the 3GPP 4G and 5G protocol stacks for user and control planes, respectively. The two systems, with similar architecture, also use the same protocols, except for the Service Data Adaptation Protocol (SDAP). The SDAP has been introduced in 5G for *flow-based QoS*, as described in the following sections. It provides a mapping between QoS flows and data radio bearers and marking QoS flow ID (QFI) in both DL and UL packets. There is a single SDAP entity for each PDU session (GTP Tunnel) (3GPP, 2018e [32]).

[40]

Figure 9. NG-RAN and core function splits in 3GPP standard (3GPP, 2018e [32])

[41]

Figure 10. Overall NG-RAN architecture (Guttman, 2018 [11]; 3GPP, 2018e [32])

In 4G, the non-access stratum (NAS) supports mobility management (MM) functionality and user-plane bearer activation, modification and deactivation; it is also responsible for ciphering and integrity protection of NAS signalling (3GPP, 2018f [33]). In 5G, NAS-MM supports registration management, connection management functionality, and user-plane connection activation and deactivation; as well as ciphering and integrity protection of NAS signalling. NAS-Session Management (SM) is responsible for user-plane PDU Session Establishment, modification and release; it is transferred via the Access and Mobility Function (AMF), and is transparent to the AMF (3GPP, 2018g [34]).

As in the previous 3GPP network releases, *the NG-RAN and 5GC have crystal-clear boundaries*, regardless of the implementation. Hence, any feasible security risk in the NG-RAN is managed in exactly the same way as in previous RAN generations. This means that network operators can be selective about the vendor equipment used in the network segments and can pursue an effective multi-vendor strategy at minimal risk in order to deliver cost-effective solutions and mitigate the risk of vendor failure.

[42]

Figure 11. 4G/5G User Plane protocol stack (3GPP, 2018f [33]; 3GPP, 2018g [34])

Where there is concern regarding core-RAN overlap, local breakout, e.g. to a Multi-access Edge Computing (MEC) server (ETSI, 2018 [43]), or remote break out to internal (operatorsâ networks, data centres) or to external data networks such as the Internet, can be provided by user-plane functions of core networks running on third party equipment, as described in the following sections.

5G Core and Slicing

The 5G core supports many new enabling network technologies (3GPP, 2018g [34]; 3GPP, 2018h [35]). Among other fundamental technology components, as depicted in Figure 14, the 5GC is characterised by a layered and service-oriented architecture, with CP and UP split, and interfaces to subscription, state and policy data. Moreover, the 5GC supports UP session continuity while a terminal moves across different access points, interworking with untrusted non-3GPP access systems, and wireless-wireline convergence. The 5GC also supports unified subscriber management, authorisation and authentication functions; and it comes along with a comprehensive policy framework for access traffic steering, switching and splitting.

[44]

Figure 12. 4G/5G Control Plane protocol stack (3GPP, 2018f [33]; 3GPP, 2018g [34])

[45]

Figure 13. Huawei co-located CU-DU units running on Huawei dedicated hardware and software

The separation of control and user planes provides deployment flexibility and independence. The distribution of core functionality, especially user-plane functions, closer to the radio nodes, i.e. at the edge of the network, enables the placement of applications in the proximity of the end user, reducing transport network load and latency.

The service-based architecture, including the related Network Repository Function (NRF) for 5GC control plane functions, allows flexible addition and extension of network functions.

Other fundamental 5G enabling technologies, end-to-end, are (Soldani, 2018a [21]): Flow-based QoS, with a much higher level of granularity than LTE, which is limited to the bearer service concept (single pipe between terminal and core network); multi-connectivity, where the 5G device can be connected simultaneously to 5G, LTE and Wi-Fi, offering a higher user data rate and a much more reliable connection; terminal-assisted Network Slicing, and end-to-end network management and orchestration, with in-built support for cloud implementation and edge computing. Slicing and the related Network Slice Selection Function (NSSF) enable a flexible assignment of users to different network slice instances that may be tailored to different use cases.

[46]

Figure 14. 5G Core (5GC) functions and interfaces (3GPP, 2018f [33]; 3GPP, 2018h [35])

The 5G flow-based QoS and slicing concept are illustrated in Figure 15. The NG-RAN and UE are only aware of their Slice and QoS. The *NG-RAN is not aware of any subscription data*. Also, as in earlier network generations, all user-plane and signalling traffic is forwarded to the 5GC through secure tunnels and third-party security gateways, as detailed in the next section.

Slices consisting of chains of virtual network functions (VNFs) are supported by the 5GC only (Soldani, 2018a [21]). The 3GPP has defined a new parameter for terminal (UE) assisted network slicing, denoted as Single-Network Slice Selection Assistance Information (**S-NSSAI**). The S-NSSAI is to assist the network in selecting a Network Slice Instance (NSI). The S-NSSAI is composed of the following attributes:

- **Slice Service Type (SST)**: 1 (eMBB), 2 (URLLC) and 3 (massive Internet of Things) are the standardised values for roaming; operator specific settings are also possible;
- A **Slice Differentiator (SD)**: Tenant ID, for further differentiation during the NSI selection.

The Network Slice Selection Assistance Information (NSSAI) consists of a collection of S-NSSAIs. A maximum of eight S-NSSAIs may be sent in signalling messages between the UE and the Network. The NSSAI is configured in the UE per Public Land Mobile Network (PLMN) by the Home PLMN (HPLMN).

[47]

Figure 15. End-to-end QoS management and 5GC Slicing (Soldani, 2018a [21]; 3GPP, 2018f [33]; 3GPP, 2018h [35])

The terminal (UE) uses the **Requested NSSAI** during the Registration Procedure and the **Allowed NSSAI**, received from the AMF, within its Registration Area (RA). The RA allocated by the AMF to UE has homogeneous support of network slices. The 5GC supports AMF-level slicing per UE type, and SMF- and UPF-level slicing per Service or per Tenant, based on S-NSSAI and Data Network Name (DNN). An example of two network slices for one terminal type is illustrated in Figure 15.

IP Flows are mapped onto QoS flows, which are mapped onto one or more data radio bearers (DRBs). DRBs are associated with one PDU Session, which is mapped onto one S-NSSAI. The S-NSSAI is mapped onto one NSI, i.e. one Network Slice; and the NSI is mapped onto a single DNN. However, the opposite construction of mappings is not valid, as described below. This is how 5G handles the 5G flow-based QoS within a given NSI (Soldani, 2018a [21]; 3GPP, 2018f [33]; 3GPP, 2018h [35]).

The NG-RAN is aware of the slice at PDU Session level, because the S-NSSAI is included in any signalling message containing PDU Session information (3GPP, 2018e [32]). Pre-configured slice enabling, in terms of NG-RAN functions, is implementation dependent. An example of NG-RAN slicing is depicted in Figure 16. The figure shows the Medium Access Control (MAC) scheduling that is based on Radio Resource Management (RRM) policy related to the Service Level Agreement (SLA), agreed between the communication service provider and tenant. The scheduling for the supported network slices and QoS differentiation within the slice is vendor dependent (3GPP, 2018e [32]). Resources may be reserved exclusively for certain slices to fulfil SLAs, e.g. to prevent service degradation in one slice due to shortage of resources in another slice. The 5GC has full control of slice and QoS management, end-to-end. Regardless of the number of slices used simultaneously, there is only one signalling connection to the 5GC, and the 5GC directs the UE to the slice-related resources (Soldani, 2018a [21]).

[48]

Figure 16. NG-RAN Slicing (Soldani, 2018a [21]; 3GPP, 2018e [32]; 3GPP, 2018f [33])

5G Security Aspects

5G system security is based on the well-established and proven 4G EPS mechanisms, which have been further enhanced in 3GPP R15 (3GPP, 2018j [49]; 3GPP, 2018k [50]). The NAS security and keying hierarchy remain as in 4G. NAS security is established via the 3GPP Authentication and Key Agreement between NAS entities in UE and CN (AMF): see Figure 10 and Figure 12.

Figure 17 shows the 5GS keying hierarchy, which is comparable to 4G for the functionality towards the RAN, i.e. all keys for the Access Stratum (AS = RAN or AN) are derived from the NAS security parameters inside the Core Network and signalled to the RAN. *The main new model of the 5GS is on how the security functionality is decomposed and distributed inside the Core Network*. This also enables the globally unique 5G Subscription Permanent Identifier (SUPI) â comparable to the IMSI of earlier system generations â which is always signalled in an encrypted form throughout the RAN towards the CN. It is decrypted by the home PLMN and delivered from there to the serving Core Network for any user service, management or regulatory purpose. In contrast to earlier system generations, where the IMSI was used in the RAN for recovering from network failures and thereby enabled certain attacks, the 5GS neither exposes the SUPI to the RAN nor transfers it in cleartext via the radio interface. Further, 3GPP 5G R15 adds an option to perform user--plane integrity protection between UE and gNB; and, in 3GPP R16, security algorithms use up to 256-bit keys (3GPP, 2018i [39]), see Figure 18.

Since the *Huawei RAN functions run on Huawei-specific hardware*, any security assurance consideration related to installing software on a Commercial-Off-the-Shelf (COTS) platform, or interactions with the platformâs security, does not apply to the Huawei offering. Furthermore, this approach to a security implementation within network segments is reasonable, as the network operator may utilise a separate security system.

[51]

Figure 17. Key hierarchy generation in 5GS (3GPP, 2018j [49])

5G vendor equipment utilises trusted systems to ensure that unauthorised software cannot be implanted in network elements and concealed keys cannot be accessed by intruders, ensuring element management security.

The CN of the 5GS is designed to leverage software modularity and virtualisation techniques that increase the flexibility that network operators have to implement a CN design that could consist of functionality from one or more vendors.

Furthermore, as in 4G, the transport network layer within the RAN and between RAN and core network domains is protected using IPSec tunnels. Examples of security deployment scenarios for 3GPP NSA Option 3x (which is the same as with 4G) and SA Option 2, NSA Option 7 and NSA Option 4, architecture configurations are illustrated in Figure 19 and Figure 20, respectively. As shown in the figures, here with 3GPP Option 2 as an example, the 5G system RAN related transport adopts the same means as 4G and, therefore, for this aspect, it has the same level of security as 4G and as 3GPP Option 3x. For defence in depth, the Security GateWay (SeGW), Evolved Packet Core (EPC) and 5G Core Network (5GC) can all be deployed adopting solutions from different vendors.

In summary, it can be concluded that *the 5G RAN security level is at the same or higher level than for 4G, depending on deployment options, and is fully under network operator control*. The 3GPP implementation scenarios aim to ensure that the security of data transmission is robust. The Packet Data Convergence Protocol (PDCP) encryption in the RAN (downlink), see Figure 16, and UE (uplink) ensures security over the air interface. Beyond this, operators are expected to implement the security solution introduced above for intranet transmission, e.g. using IPSec tunnels, when connecting the access and core network equipment. The application layer ensures the security of services.

[52]

Figure 18. End-to-end security enhancement with 5G Evolution (3GPP, 2018j [49]; 3GPP, 2018k [50])

[53]

Figure 19. 3GPP NSA Option 3 and SA Option 2 security deployments

[54]

Figure 20. 3GPP NSA Option 7 and NSA Option 4 security deployments

5G Deployment Scenarios

For the discussion on the potential 5G deployment scenarios, a case study based on the Huawei 5G radio access products is provided.

The 5G deployment scenarios using NSA and NSA/SA architecture configurations are depicted in Figure 21 and Figure 22, respectively. All network domains, except the Huawei RAN functions, for example, may run on cloud infrastructures. The hardware at the far edge hosts the CU&DU (BBU) functions, as illustrated in Figure 16. In this case study, this is the area where the Huawei antennas, radio remote (RRU) and baseband units may be deployed.

The edge/regional cloud, hosting CN, application server and MEC functions, is separated from the far edge zone, i.e. the RAN, by the standardised NSA RAN (S1) or SA RAN (NG, i.e. N2 and N3) interfaces (see Figure 2, Figure 9, Figure 10, Figure 11, Figure 12, and Figure 14) maintaining a clear logical and physical separation between radio access equipment and core network elements.

Any wanted local breakout (e.g. for MEC) is beyond the RAN and located in the edge/regional data centres (points of presence, central part of the infrastructure, using third-party equipment), where core network functions are also embedded. There is no possibility of instantiating the latter in Huawei equipment, e.g. through an end-to-end VNF orchestration.

IoT and application enablement platforms are also placed in the central part of the network.

The introduction of the 5G core may be based on software upgrades of the core functions instantiated in the edge/regional segment, namely in the metro and edge areas, as shown in Figure 22, where an example of three network slices is also illustrated for different SLAs, in terms of throughput, latency and reliability.

Figure 23 shows the Huawei Element Management System (EMS) for the 5G RAN (NG-RAN).

The EMS connects to the RAN elements and handles Performance Management (PM), Fault Management (FM), Configuration Management (CM), Inventory Management (IM) and Software Management (SM) data of its subordinate equipment.

Network operators have full control of the access to the 5G RAN EMS, e.g. firewall and security control systems such as Citrix Systems, as currently used with 4G, which may provide port filtering and monitoring.

The 5G RAN EMS manages RAN elements through its proprietary South-bound Interface (SBI), which is not standardised by the 3GPP. Similarly, to how other vendor systems operate, a third-party EMS cannot manage the Huawei RAN, as the EMS is a vendor-specific 5G RAN hardware and software solution. The Huawei 5G RAN EMS can be installed and functions only on dedicated Huawei-provided hardware.

[55]

Figure 21. 5G 3GPP NSA deployment scenario with the existing Australian core network

[56]

Figure 22. 5G 3GPP NSA/SA deployment scenario with 5GC in Australia, and example of network slices with different SLAs, in terms of throughput, latency and reliability parameters

[57]

Figure 23. Example Huawei 5G RAN (NG-RAN) Element Management System deployment in Australia

The 5GS supports subscriber tracing similar to 4G in the RAN and is described in 3GPP (2018l [58]). As in 4G, there will not be any subscriber identities given to the RAN.

Figure 24 paints a high-level end-to-end security deployment and management process. *It is the operatorsâ responsibility to ensure network security.* For example: management plane, control plane and user plane must be isolated; in all nodes, security features, at the different interfaces, must be enabled for encrypted transmission between peer elements; unused ports shall be shut down; and EMS rights strictly controlled and restricted.

Furthermore, as depicted in Figure 25, carriers may deploy a third-party Bastion host between the Operation and Maintenance (O&M) personnel and EMS, which is the way to access the EMS. The bastion host supports, but is not limited to: complete identity management and authentication; authorisation based on users; target hosts and time segments; real-time monitoring; complete operation of the entire process; complete session audit and playback.

Ultimately, as shown in Figure 26, ultra-reliable low-latency services should be provided only in confined (specific) areas or using dedicated mobile networks, in order to comply with the related SLA parameters, e.g. five nines reliability, dependability and safety requirements. Also, for services demanding a high level of security, end-to-end security should be applied at the application layer.

[59]

Figure 24. End-to-end security deployment and management

Network operators are able to implement an independent *network managed services* solution that is provided by other vendors or handled by the network operators themselves.

Developing an Operational Assurance Paradigm

In the security guidance on 5G systems to Australian carriers, issued by the Australian Government, there was a view that the security of telecommunication networks and systems was vital for national security (Morrison and Fifield, 2018 [8]). However, the Australian Government does not have a telecommunications security assurance capability and has left this role with the telecommunications industry.

In this section, a review of global efforts to develop telecommunications security assurance is provided and a proposal on how this capability could be implemented in Australia is presented.

[60]

Figure 25. Example of third-party Bastion host for Huawei EMS logs

[61]

Figure 26. Examples of deployment of high-reliability and secure services

The transition from 4G to 5G is a timely opportunity for the Australian government, security agencies and telecommunications industry to collaboratively introduce a telecommunications security assurance capability.

Existing telecommunications security assurance measures are deficient in certain scenarios and stages of the infrastructure lifecycle. A telecommunications security assurance methodology that includes security assurance throughout the infrastructure lifecycle to provide certainty that equipment and systems are operating as expected would be a valuable addition to the existing information and systems security solutions used by the telecommunications industry.

The UK has taken the lead in network assurance with the creation of the Huawei Cyber Security Evaluation Centre (HCSEC) in Banbury, Gloucestershire. This centre has established itself as a world-class source code evaluation facility, which inspects the network products used in the UK infrastructure and ensures there is no malicious code. No malicious code or backdoors have been found on any product at this centre, providing substantial evidence that there is no latent threat of state-sponsored attack from using non-UK equipment. The centre has been instrumental in providing guidance to Huawei on continuous improvement in its products, and also in its technical development strategy. However, this is a point-in-time evaluation and does not cover the full lifecycle of the technologies.

Currently, there is a need for a unified approach to providing security evaluation of telecommunications infrastructure and systems throughout the lifecycle. Independent passive monitoring of telecommunications infrastructure and systems is required to assure that the infrastructure and systems are configured, installed, maintained and operating as expected.

The deep inspection of information that is collected utilising a passive system, which does not adversely affect nor have the potential to alter the operation of network operator infrastructure or systems, provides a new approach to assuring that telecommunications infrastructure and systems are secure and operating as expected.

This capability to reduce the risk of inadvertent, foreign or criminal interference with critical telecommunications infrastructure and systems is required, as there is an increasing dependence on telecommunications by government, business and industry.

The notion that the telecommunications industry should be an active participant in the national security obligation has been established globally and governments retain the right to require that network operators make available information about their networks and operations. The introduction of a telecommunications security assurance capability will provide independent knowledge about critical telecommunications infrastructure and systems throughout the lifecycle and be able to assure the operation of individual equipment and systems.

Telecommunications infrastructure security has become a national priority in Australia and the best way to achieve this outcome is to adopt a collaborative approach to implementing and overseeing security assurance.

The linkage between government, the security agencies and the network operators has been established and evolved as a cooperative endeavour. For example, legislation stipulating the obligations of carriers and carriage service providers for the legal interception of telecommunications in Australia was codified in Section 313 of the *Telecommunications Act 1997* (Telecommunications Act, 1997 [62]) and, more recently, the Government introduced the Telecommunications Sector Security Reforms legislation (TSSR, 2018 [63]; TOLAA, 2017 [64]).

The adoption of a unified telecommunications security assurance capability, which leverages the learnings from the UK and builds on this with passive operational assurance, would provide Australia with a new security capability based on multi-stakeholder cooperation and world-class technology assurance, and would put Australia at the front of technology assurance globally. It would provide the foundational skills and knowledge for Australiaâs aspirations to be a world-class cybersecurity nation.

The telecommunications security assurance capability would provide an opportunity for new processes and tools to be developed, introduced and evaluated by the telecommunications industry, government and security agencies. For example, the use of secure passive independent monitoring of telecommunications infrastructure and systems throughout the lifecycle provides an opportunity for new information collection approaches to be developed and for deep inspection and analysis of the data that is collected about the operation of infrastructure and systems operations utilising artificial intelligence. The design of a secure passive independent monitoring and verification system is shown in Figure 27.

[65]

Figure 27. Passive independent security assurance system

Government, industry and business would be able to gain technical advice and access to expertise as the telecommunications industry moves forward, as it is anticipated that telecommunications will further evolve and further impact upon every aspect of our daily lives.

Globally, there is a wealth of experience being gained in both private and government testing and assessment centres. The UK Government has consistently pointed to Huaweiâs Cybersecurity Evaluation Centre as providing the UK with world-class security expertise. In Australia, the Australasian Information Systems Evaluation Program (AISEP) provides a foundation, but a world-class capability for security assurance throughout the telecommunications infrastructure and beyond, into the systems lifecycle, has not been developed.

Conclusions

This paper provides a review of selected design and security aspects of 5G systems, and addresses key questions about the deployment scenarios of Next Generation Radio Access Networks in Australia. The paper also reviews and addresses the potential benefits of a telecommunications security assurance capability to improve the whole-of-life security assurance of critical telecommunications infrastructure and why it is important for the Australia telecommunications sector.

5G is defined by 3GPP Release 15 and Release 16 as an LTE advanced pro evolution and a NG-RAN/5GS developed in parallel to address different markets and migration scenario needs. 3GPP has already defined the security mechanisms for R15, which have been enhanced with respect to previous network generations, and Huawei products comply with all of them.

In 2019, the initial 5G deployment is assumed to be based on 3GPP Option 3x, which consists of a Non-Standalone (NSA) architecture configuration of LTE combined with NR and an Evolved Packet Core Network (EPC), which re-uses the same 3GPP architecture and security mechanisms as 4G. End-to-end network slicing and a range of 5G-specific services or use cases are not supported.

Looking at 2020 and beyond, the main migration strategy is to move from 3GPP Non-Standalone (NSA) architecture Option 3x to 3GPP NSA architecture Option 4, which consists of a Multi-RAT Dual Connectivity (DC) with the 5G Core Network (5GC) and New Radio (NR) as Master. The logical and physical separation between the RAN and core parts of the network (5GC and EPC) will remain as such. In 3GPP specifications, as in previous network generations, the 5GC and NG-RAN functions are separated by a standardised interface, which enables a multi-vendor deployment. The NG-RAN remains a âpipeâ between the user equipment and core network.

In Release 15 (R15), Standalone (SA) Option 2, and later releases (R16, R17, etc.), 3GPP defines additional security enhancements, such as subscription identifier encryption (SUCI) and user-plane integrity protection (R15), roaming security enhancement and 256-bit encryption (R16), and Huawei products implement and will support them.

Ultra-reliable low-latency (URLLC) communication services may be provided only in confined (specific) areas or using dedicated mobile networks, to comply with the corresponding service level agreements, dependability and safety requirements. Also, for services demanding a high level of security, such as driverless cars, service robots etc., the application system must support end-to-end security protection.

The transition to 5G follows the same approach as 4G and earlier 3GPP system generations and security risks in the NG-RAN can be managed following established procedures.

The introduction of a telecommunications security assurance capability is an important step that will reduce the risk to critical infrastructure and systems and provide assurance to key stakeholders that the infrastructure and systems are operating as expected. Careful implementation of this capability will ensure that the network operators are not affected by the passive monitoring of the operation of telecommunication infrastructure and systems. Artificial-intelligence-driven analysis of the data collected will permit a deep inspection of the operational state of infrastructure and systems that can be used to provide timely alerts to Government, security agencies and network operators about unexplained events related to the operation of telecommunication infrastructure and systems.

Finally, we want to state clearly that the assumptions and views reported herein are solely those of the authors, and do not necessarily represent those of their affiliates.

References

3rd Generation Partnership Project. 2018a. âStudy on scenarios and requirements for next generation access technologies", 3GPP TR 38.913, v.14.3.0. 19 July 2018. Retrieved from https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2996 [66]

3rd Generation Partnership Project. 2018b. â3GPPâ, 3 July 2018, Retrieved fromhttp://www.3gpp.org/ [67]

3rd Generation Partnership Project. 2018c. âRequirements for Further Advancements for Evolved Universal Terrestrial Radio Accessâ, TR 38.913, v.14.0.0. 19 July 2018. Retrieved from https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?âspecificationId=2585 [68]

3rd Generation Partnership Project. 2018d. âUser Equipment (UE) radio transmission and reception; Part 1: Range 1 Standaloneâ, 3GPP TS 38.101-1 V15.2.0. Retrieved from https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3283 [69]

3rd Generation Partnership Project. 2018e. âNR and NG-RAN overall description; Stage 2â, 3GPP TS 38.300 v.15.2.0. Retrieved from https://portal.3gpp.org/desktopmodulesâ/Specifications/SpecificationDetails.aspx?specificationId=3191 [70]

3rd Generation Partnership Project. 2018f. âGeneral Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) accessâ, 3GPP TS 23.401 v.15.4.0. Retrieved from https://portal.3gpp.org/desktopmodulesâ/Specifications/SpecificationDetails.aspx?specificationId=849 [71]

3rd Generation Partnership Project. 2018g. âSystem architecture for the 5G system; Stage 2â, 3GPP TS 23.501 v.15.2.0. Retrieved from https://portal.3gpp.org/desktopmodulesâ/Specifications/SpecificationDetails.aspx?specificationId=3144 [72]

3rd Generation Partnership Project. 2018h. âProcedures for the 5G System; Stage 2â, 3GPP TS 23.502 v.15.2.0. Retrieved from https://portal.3gpp.org/desktopmodules/Specificationsâ/SpecificationDetails.aspx?specificationId=3145 [73]

3rd Generation Partnership Project. 2018i. âNG-RAN; NG general aspects and principlesâ, 3GPP TS 38.410 v.15.0.0. Retrieved from https://portal.3gpp.org/desktopmodulesâ/Specifications/SpecificationDetails.aspx?specificationId=3220 [74]

3rd Generation Partnership Project. 2018j. âSecurity architecture and procedures for 5G Systemâ, 3GPP TS 33.501 v.15.0.0. Retrieved from https://portal.3gpp.org/desktopmodulesâ/Specifications/SpecificationDetails.aspx?specificationId=3169 [75]

3rd Generation Partnership Project. 2018k. âSecurity Aspectsâ. Retrieved fromhttp://www.3gpp.org/DynaReport/33-series.htm [76]

3rd Generation Partnership Project. 2018l. âTelecommunication management; Subscriber and equipment trace; Trace concepts and requirementsâ, 3GPP TS 32.421 v.15.0.0. Retrieved from https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspxâ?specificationId=2008 [77]

ACMA. 2017. âCompletes high-value spectrum auction at 700 MHzâ. Australian Communications and Media Authority, 12 April 2017. Retrieved from https://www.acma.gov.au/theACMA/Newsroom/Newsroom/Media-releases/sold-acma-completes-high-value-spectrum-auction [78]

ACMA. 2018) â3.6 GHz band auction systemâ. Australian Communications and Media Authority, 10 April 2018. Retrieved from https://www.acma.gov.au/theACMA/spectrum-tune-up-3-6-ghz-band-auction-system [79]

Elbamby, MS; Perfecto, C; Bennis, M; Doppler, K. 2018. âToward Low-Latency and Ultra-Reliable Virtual Realityâ,*IEEE Network Magazine*, March 2018.

ETSI. 2018. âMEC in 5G networks.â White Paper No. 28, First edition, June 2018. Retrieved from https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINALâ.pdf [80]

Foye, B. 2018a. âTelstra to launch 5G services in 2019â. CRN. 5 February 2018. Retrieved fromhttps://www.crn.com.au/news/telstra-to-launch-5g-services-in-2019-484422 [81]

Foye, B. 2018b. âOptus to showcase 5G network at 2018 Gold Coast Commonwealth Games ahead of 2019 launchâ. CRN. 2 February 2018. Retrieved from https://www.crn.com.auâ/news/optus-to-showcase-5g-network-at-2018-gold-coast-commonwealth-games-ahead-of-2019-launch-484251 [82]

Guttman, E; Mademann, F; Prasad, AR (Eds). 2018. "Special issue on â3GPP 5G Specificationsâ"*Journal of ICT Standardization*, May 2018. Retrieved from https://wwwâ.riverpublishers.com/journal.php?j=JICTS/6/1/jart [83]

Huawei. 2018. â5G Spectrumâ. Public policy position paper, March 2018. Retrieved fromhttp://www-file.huawei.com/-/media/CORPORATE/PDF/public-policy/public_policy_âposition_5g_spectrum.pdf?la=en [84]

ITU-T. 2018. âRequirements of the IMT-2020 network [85]â, ITU-T Rec. Y.3101, January, 2018. Retrieved fromhttps://www.itu.int/rec/T-REC-Y.3101-201801-I/en [86]

Kennedy, D. 2018. â5G in Australia: Evolution not Revolutionâ. Ovum, TMT intelligence Informa, June 2018. Retrieved from https://www.nbnco.com.au/content/dam/nbnco2â/2018/documents/media-centre/5G_report_June_2018.pdf [87]

Morrison, S; Fifield, M. 2018. âGovernment Provides 5G Security Guidance to Australian Carriersâ. Joint Media Release, 23 August 2018. Retrieved from https://www.minister [88]â.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers

NGMN Alliance. 2015. âNGMN 5G white paperâ. February 2015. Retrieved from https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf [89]

Soldani, D; Airas, P; Hoglund. T; Rasanen, H; Debrecht, D. 2017a. â5G To The Homeâ,*IEEE VTC*, Spring, 2017. Retrieved from https://ieeexplore.ieee.org/document/8108603/ [90]

Soldani, D; *et al.* 2017b. â5G Mobile Systems for Healthcare [91]â, 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, NSW, 2017, pp. 1-5. DOI: 10.1109/VTCSpringâ.2017.8108602

Soldani, D. 2018a. â5G beyond radio access: A flatter sliced networkâ,*Mondo Digitale*, AICA, March 2018. Retrieved fromhttp://www.sipotra.it/wp-content/uploads/2018/03/5G-beyond-radio-access-a-flatter-sliced-network.pdf [92]

Soldani, D; Guo, YJ; Barani, B; Mogensen, P; Das, CL. 2018b. â5G for Ultra-Reliable Low-Latency Communicationsâ, Special Issue of*IEEE Network Magazine*, March 2018. Retrieved fromhttps://ieeexplore.ieee.org/document/8329617/ [93]

Telecommunications Act. 1997. Section 313. Australian Government, 1997. Retrieved from http://www5.austlii.edu.au/au/legis/cth/consol_act/ta1997214/s313.html [94]

TOLAA. 2017. Telecommunications and Other Legislation Amendment Act 2017, Australian Government. Retrieved from https://www.legislation.gov.au/Details/C2017A00111 [95]

TSSR. 2018. Telecommunications Sector Security Reforms. Australian Government. 20 August 2018, Retrieved from https://www.homeaffairs.gov.au/about/consultationsâ/telecommunications-sector-security-reforms [96]

UK Government. 2018. âHuawei cyber security evaluation centre oversight board: annual report 2018â. UK Government report, 19 July 2018. Retrieved from https://www.gov.ukâ/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2018 [97]

Article PDF:
161-article_text-1678-1-10-20181105.pdf [98]

Cite this article as:

David Soldani, Malcolm Shore, Jeremy Mitchell, Mark Gregory. 2018. *The 4G to 5G Network Architecture Evolution in Australia* ajtde, Vol 6, No 4, Article 161. http://doi.org/10.18080/ajtde.v6n4.161 [100]. Published by Telecommunications Association Inc. ABN 34 732 327 053.https://telsoc.org [101]

Links
[1] https://telsoc.org/journal/author/david-soldani [2] https://telsoc.org/journal/author/malcolm-shore [3] https://telsoc.org/journal/author/jeremy-mitchell [4] https://telsoc.org/journal/author/mark-gregory [5] https://telsoc.org/journal/ajtde-v6-n4 [6] https://www.addtoany.com/share#url=https%3A%2F%2Ftelsoc.org%2Fjournal%2Fajtde-v6-n4%2Fa161&title=The%204G%20to%205G%20Network%20Architecture%20Evolution%20in%20Australia [7] https://telsoc.org/printpdf/2272?rate=0Lx4mm_RSvZNNDuqarML51woK-cE64rZnxF6_f8ZDNA [8] https://telsoc.org/journal/ajtde-v6-n4/a161#Morrison [9] https://telsoc.org/journal/ajtde-v6-n4/a161#NGMN2015 [10] https://telsoc.org/journal/ajtde-v6-n4/a161#kennedy2018 [11] https://telsoc.org/journal/ajtde-v6-n4/a161#Guttman2018 [12] https://telsoc.org/journal/ajtde-v6-n4/a161#Foye2018a [13] https://telsoc.org/journal/ajtde-v6-n4/a161#Foye2018b [14] https://telsoc.org/journal/ajtde-v6-n4/a161#ITUT2018 [15] https://telsoc.org/journal/ajtde-v6-n4/a161#threegpp2018a [16] https://telsoc.org/journal/ajtde-v6-n4/a161#Soldani2017a [17] https://telsoc.org/journal/ajtde-v6-n4/a161#Elbamby2018 [18] https://telsoc.org/journal/ajtde-v6-n4/a161#Soldani2017b [19] https://telsoc.org/sites/default/files/images/tja/166fig1.jpg [20] https://telsoc.org/sites/default/files/images/tja/166fig2.jpg [21] https://telsoc.org/journal/ajtde-v6-n4/a161#Soldani2018a [22] https://telsoc.org/journal/ajtde-v6-n4/a161#threegpp2018b [23] https://telsoc.org/sites/default/files/images/tja/166fig3.jpg [24] https://telsoc.org/journal/ajtde-v6-n4/a161#threegpp2018c [25] https://telsoc.org/journal/ajtde-v6-n4/a161#Soldani2018b [26] https://telsoc.org/sites/default/files/images/tja/166fig4.jpg [27] https://telsoc.org/journal/ajtde-v6-n4/a161#threegpp2018d [28] https://telsoc.org/journal/ajtde-v6-n4/a161#Huawei2018 [29] https://telsoc.org/sites/default/files/images/tja/166fig5.jpg [30] https://telsoc.org/journal/ajtde-v6-n4/a161#ACMA2018 [31] https://telsoc.org/journal/ajtde-v6-n4/a161#ACMA2017 [32] https://telsoc.org/journal/ajtde-v6-n4/a161#threegpp2018e [33] https://telsoc.org/journal/ajtde-v6-n4/a161#threegpp2018f [34] https://telsoc.org/journal/ajtde-v6-n4/a161#threegpp2018g [35] https://telsoc.org/journal/ajtde-v6-n4/a161#threegpp2018h [36] https://telsoc.org/sites/default/files/images/tja/166fig6.jpg [37] https://telsoc.org/sites/default/files/images/tja/166fig7.jpg [38] https://telsoc.org/sites/default/files/images/tja/166fig8.jpg [39] https://telsoc.org/journal/ajtde-v6-n4/a161#threegpp2018i [40] https://telsoc.org/sites/default/files/images/tja/166fig9.jpg [41] https://telsoc.org/sites/default/files/images/tja/166fig10.jpg [42] https://telsoc.org/sites/default/files/images/tja/166fig11.jpg [43] https://telsoc.org/journal/ajtde-v6-n4/a161#ETSI2018 [44] https://telsoc.org/sites/default/files/images/tja/166fig12.jpg [45] https://telsoc.org/sites/default/files/images/tja/166fig13.jpg [46] https://telsoc.org/sites/default/files/images/tja/166fig14.jpg [47] https://telsoc.org/sites/default/files/images/tja/166fig15.jpg [48] https://telsoc.org/sites/default/files/images/tja/166fig16.jpg [49] https://telsoc.org/journal/ajtde-v6-n4/a161#threegpp2018j [50] https://telsoc.org/journal/ajtde-v6-n4/a161#threegpp2018k [51] https://telsoc.org/sites/default/files/images/tja/166fig17.jpg [52] https://telsoc.org/sites/default/files/images/tja/166fig18.jpg [53] https://telsoc.org/sites/default/files/images/tja/166fig19.jpg [54] https://telsoc.org/sites/default/files/images/tja/166fig20.jpg [55] https://telsoc.org/sites/default/files/images/tja/166fig21.jpg [56] https://telsoc.org/sites/default/files/images/tja/166fig22.jpg [57] https://telsoc.org/sites/default/files/images/tja/166fig23.jpg [58] https://telsoc.org/journal/ajtde-v6-n4/a161#threegpp2018l [59] https://telsoc.org/sites/default/files/images/tja/166fig24.jpg [60] https://telsoc.org/sites/default/files/images/tja/166fig25.jpg [61] https://telsoc.org/sites/default/files/images/tja/166fig26.jpg [62] https://telsoc.org/journal/ajtde-v6-n4/a161#TelAct1997 [63] https://telsoc.org/journal/ajtde-v6-n4/a161#TSSR2018 [64] https://telsoc.org/journal/ajtde-v6-n4/a161#TOLAA2017 [65] https://telsoc.org/sites/default/files/images/tja/fig27.jpg [66] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2996 [67] http://www.3gpp.org/ [68] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?%E2%80%8CspecificationId=2585 [69] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3283 [70] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3191 [71] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=849 [72] https://portal.3gpp.org/desktopmodules%E2%80%8C/Specifications/SpecificationDetails.aspx?specificationId=3144 [73] https://portal.3gpp.org/desktopmodules/Specifications%E2%80%8C/SpecificationDetails.aspx?specificationId=3145 [74] https://portal.3gpp.org/desktopmodules%E2%80%8C/Specifications/SpecificationDetails.aspx?specificationId=3220 [75] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169 [76] http://www.3gpp.org/DynaReport/33-series.htm [77] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2008 [78] https://www.acma.gov.au/theACMA/Newsroom/Newsroom/Media-releases/sold-acma-completes-high-value-spectrum-auction [79] https://www.acma.gov.au/theACMA/spectrum-tune-up-3-6-ghz-band-auction-system [80] https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL%E2%80%8C.pdf [81] https://www.crn.com.au/news/telstra-to-launch-5g-services-in-2019-484422 [82] https://www.crn.com.au/news/optus-to-showcase-5g-network-at-2018-gold-coast-commonwealth-games-ahead-of-2019-launch-484251 [83] https://www.riverpublishers.com/journal.php?j=JICTS/6/1/jart [84] http://www-file.huawei.com/-/media/CORPORATE/PDF/public-policy/public_policy_%E2%80%8Cposition_5g_spectrum.pdf?la=en [85] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi0_vzDm6XcAhULjZQKHcBGDpcQFggoMAA&url=https%3A%2F%2Fwww
REC-Y.3101-201801-I!!PDF-E%26type%3Ditems&usg=AOvVaw27SYxyzVrSXCeEORKhMp8o [86] https://www.itu.int/rec/T-REC-Y.3101-201801-I/en [87] https://www.nbnco.com.au/content/dam/nbnco2%E2%80%8C/2018/documents/media-centre/5G_report_June_2018.pdf [88] https://www.minister [89] https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf [90] https://ieeexplore.ieee.org/document/8108603/ [91] http://ieeexplore.ieee.org/document/8108602/ [92] http://www.sipotra.it/wp-content/uploads/2018/03/5G-beyond-radio-access-a-flatter-sliced-network.pdf [93] https://ieeexplore.ieee.org/document/8329617/ [94] http://www5.austlii.edu.au/au/legis/cth/consol_act/ta1997214/s313.html [95] https://www.legislation.gov.au/Details/C2017A00111 [96] https://www.homeaffairs.gov.au/about/consultations%E2%80%8C/telecommunications-sector-security-reforms [97] https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2018 [98] https://telsoc.org/sites/default/files/tja/pdf/161-article_text-1678-1-10-20181105.pdf [99] https://telsoc.org/copyright [100] http://doi.org/10.18080/ajtde.v6n4.161 [101] https://telsoc.org [102] https://telsoc.org/topics/5g-technologies [103] https://telsoc.org/topics/5g-network-architecture [104] https://telsoc.org/topics/5g-security [105] https://telsoc.org/topics/5g-system [106] https://telsoc.org/topics/5g-architectures [107] https://telsoc.org/topics/5g-deployment