Australian Journal of Telecommunications and the Digital Economy

Volume 6 Issue 4

December 2018

Published by Telecommunications Association Inc.

ISSN 2203-1693

AJTDE Volume 6, Number 4, December 2018

Table of Contents

5G Arrives

Editorial

Mark A Gregory
RMIT University

Abstract: Papers in the December 2018 issue of the *Journal* include discussion on 5G security, what's next for the National Broadband Network, a technical paper on the conflicts in routing and UAV autonomy, HTTP traffic flow load balancing and an insight into how the use of location information affects privacy. The history of Australian telecommunications paper on impressions of an overseas visit by a lines engineer provides an insight into how knowledge transfer improves with the opportunity to study telecommunications in Europe, North America and Australia. The *Journal* welcomes contributions.

In This Issue

In this issue of the *Journal* papers cover public policy, new technology solutions and historical insights. The rate of technological change is highlighted by the breadth of articles and discussion on 5G mobile cellular and the National Broadband Network.

The 4G to 5G Network Architecture Evolution in Australia presents a review of how the International Telecommunications Union has maintained the option for network operators to separate access network from core networks and systems. The paper also highlights the need for a telecommunications security assurance capability.

What Now for Australia's NBN? argues for a return to a fully privatised telecommunications market by disaggregating the National Broadband Network and selling it off. The paper also continues the discussion on the establishment of a regional telecommunications fund financed by a broad-based telecommunications levy.

Impressions of an Overseas Visit by a Lines Engineer is a fascinating paper from 1961 contrasting the technical and general differences in providing telecommunications services in Europe, North America and Australia.

Flow-level Load Balancing of HTTP Traffic using OpenFlow provides an exploration of the concept of flow-based load balancing of network traffic on multi-homed hosts.

http://doi.org/10.18080/ajtde.v6n4.173

Conflicts in Routing and UAV Autonomy examines the implications of autonomous coordination of multiple UAVs on routing techniques and network architecture stability.

Privacy versus the Use of Location Information for Law Enforcement and Security in Australia reviews existing knowledge regarding the powers of the Australian Security Intelligence Organisation and the Australian Federal Police to access and use metadata.

Mobile Cellular 5G arrives

The introduction of 5G New Radio (NR) to succeed 4G (LTE/WiMax) and 3G (UMTS) has commenced. The Australian mobile network operators have begun the 5G infrastructure rollout in anticipation of 5G-compatible handsets and devices becoming available in 2019. By October 2019, the major handset vendors should have 5G-compatible versions of their flagship products available on the market in Australia.

5G is a major step forward for mobile cellular communications and the Enhanced Mobile Broadband (eMBB) will offer improved connectivity to services and applications over greater distances and with improved reliability within built-up areas.

A key facet of 5G is the push for Ultra Reliable Low Latency Communications (URLLC) to facilitate improved access to and utilisation of applications and services that are delay sensitive and require highly reliable connectivity. The URLLC usage scenario highlights how the mobile cellular technologies are moving to create a "fibre-like" connection utilising wireless technologies.

The advent of the Internet of Things (IoT), including sensor networks, has driven the 5G Massive Machine Type Communications (mMTC) usage scenario that aims to support connections from up to 1 million devices in a square kilometre.

The ITU 3GPP IMT-2020 specifications that form the basis for what is colloquially known as 5G has set a speed target for spectrum above 6 GHz of 20 Gbps, with users experiencing a data rate of 1 Gbps and a radio network latency of 1 ms.

For spectrum below 6 GHz, the expected performance matches the still evolving 4G LTE/WiMAX technology capabilities and, over the next decade, further enhancements should be introduced to 5G NR.

The ambitious targes set by the 3GPP will culminate with the 3GPP Release 16 specification that is due to be finalised in July 2019. The work program based on the 3GPP IMT-2020 specifications should continue for several years.

The *Journal* welcomes papers on the digital economy, including, theory, public policy and case studies.

http://doi.org/10.18080/ajtde.v6n4.173

The *Journal*, Looking Forward

2019 promises to be a momentous year for Australian telecommunications with the introduction of 5G networks and devices, an increasing number of driverless vehicles and improvements to satellite and fixed wireless services.

The *Journal* is calling for papers on how new technologies will affect Australian telecommunications consumers.

The topics of *International Telecommunications Legislation and Regulations* and *International Mobile Cellular Regulation and Competition* are set to continue for some time, as the opportunity to attract papers from around the globe continues. We encourage papers that reflect on where the global telecommunications market is now, how it got to where it is, and what is going to happen next.

Papers are invited for upcoming issues. With your contributions, the *Journal* will continue to provide readers with exciting and informative papers covering a range of local and international topics. The Editorial Advisory Board also values input from our readership, so please let us know what themes you would like to see in the coming year.

All papers related to telecommunications and the digital economy are welcome and will be considered for publication after the double-blind peer-review process.

Mark A Gregory

http://doi.org/10.18080/ajtde.v6n4.173

The 4G to 5G Network Architecture Evolution in Australia

David Soldani
Huawei Technologies (Australia)

Malcolm Shore
Huawei Technologies (Australia)

Jeremy Mitchell
Huawei Technologies (Australia)

Mark Gregory
RMIT University

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.

Keywords: 5G System, 5G Architectures, 5G Technologies, 5G Security, 5G Deployment

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), thereby providing the motivation for this review of the

http://doi.org/10.18080/ajtde.v6n4.161

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), 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). 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).

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

http://doi.org/10.18080/ajtde.v6n4.161

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) and Foye (2018b).

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

The 5G service specifications for eMBB, URLLC and mMTC (ITU-T, 2018), (3GPP, 2018a) 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 "Gigabit-Speed Internet" 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/s–1 Gb/s at 26 GHz. See e.g. Soldani (2017a).
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).
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).
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), 3GPP (2018a).

http://doi.org/10.18080/ajtde.v6n4.161

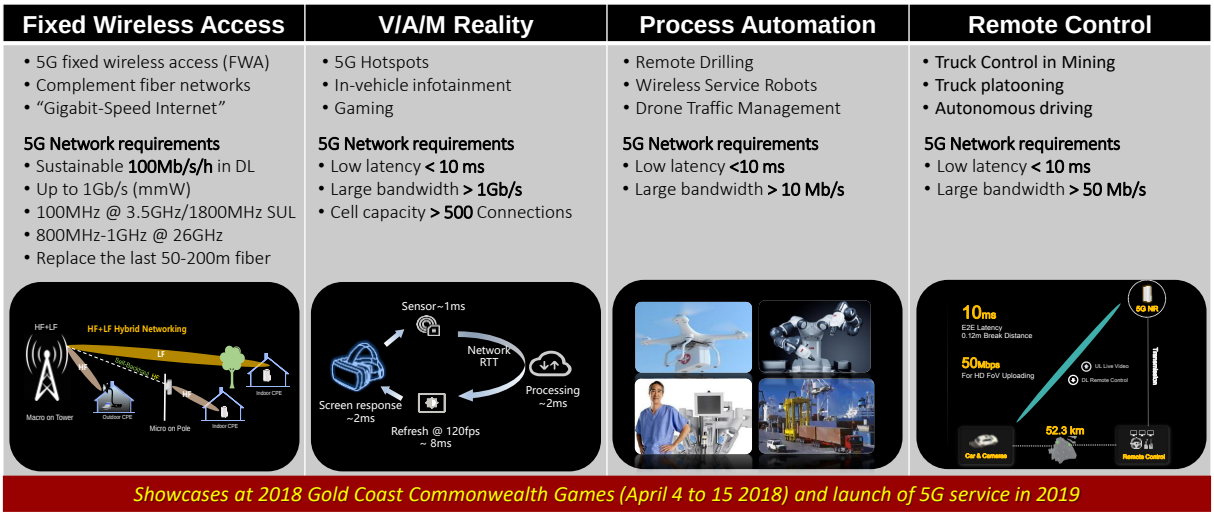


Figure 1. Examples of use cases in Australia

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).

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; 3GPP, 2018a).

5G Definitions and Standards Updates

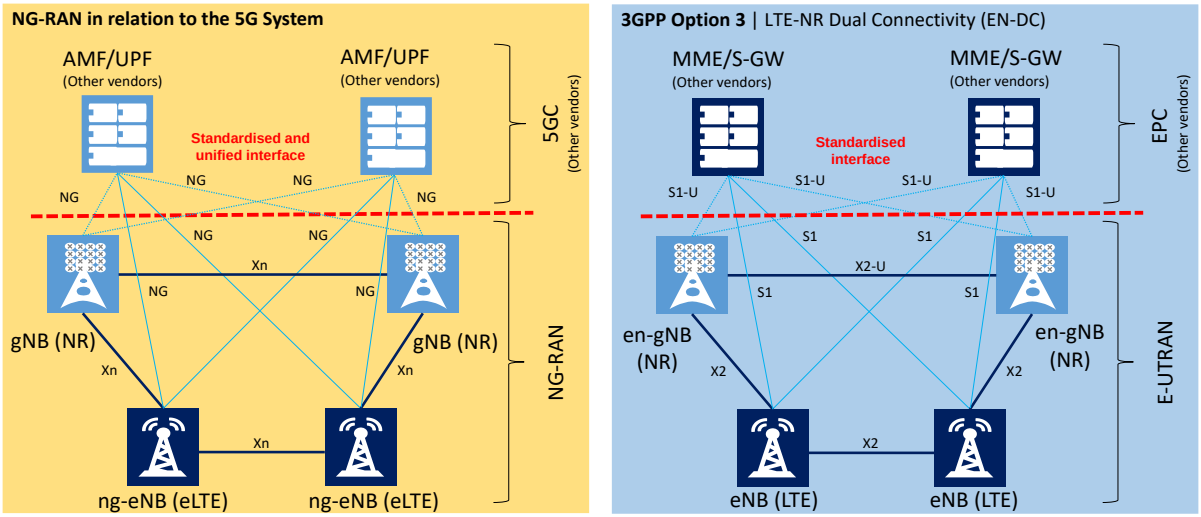
5G Wireless has been defined as the 3GPP Release 15 (R15) and later releases (R16, R17 etc.) of LTE and New Radio (NR) mobile communication systems. It is thus an *LTE advanced pro evolution and an NR technology* that adds to existing 3GPP networks.

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).

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): 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.)

http://doi.org/10.18080/ajtde.v6n4.161



a) b)

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

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.

The NG RAN operates in both so-called "Stand-Alone" (SA) operation and "Non-Stand-Alone" (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). Moreover, 3GPP has defined the following architecture configurations, see Guttman (2018), Soldani (2018a), 3GPP (2018b), 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

http://doi.org/10.18080/ajtde.v6n4.161

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).

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). 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) and Soldani (2018b).

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).

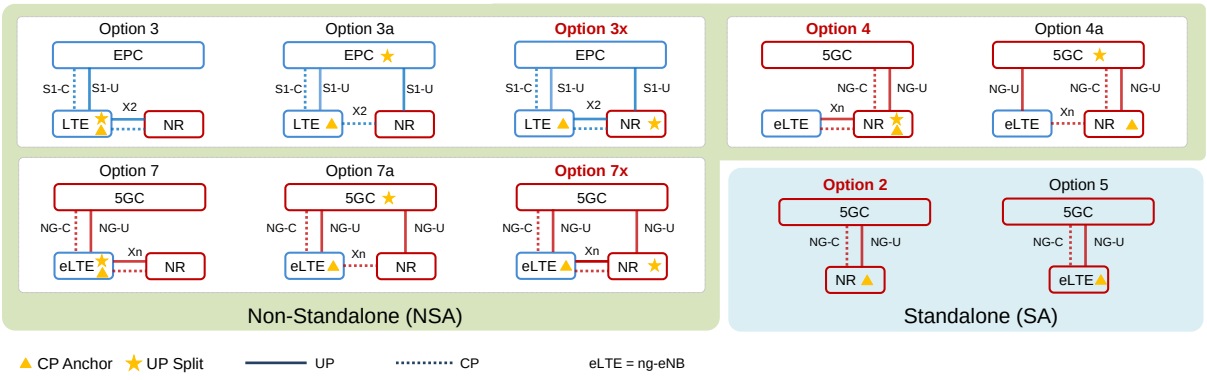


Figure 3. 3GPP architecture configurations

http://doi.org/10.18080/ajtde.v6n4.161

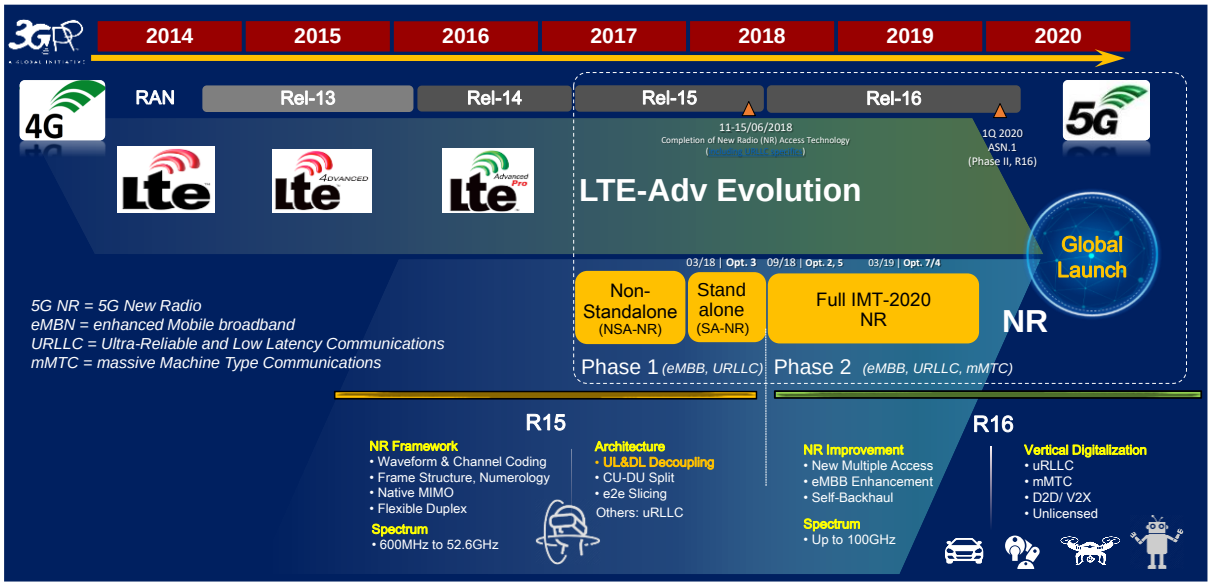


Figure 4. 3GPP definition of 5G: LTE evolution and New Radio (NR), supporting new usage scenarios

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). The standardised operating band combinations for SUL and ULS may be found in 3GPP (2018d).

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

- 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.

http://doi.org/10.18080/ajtde.v6n4.161

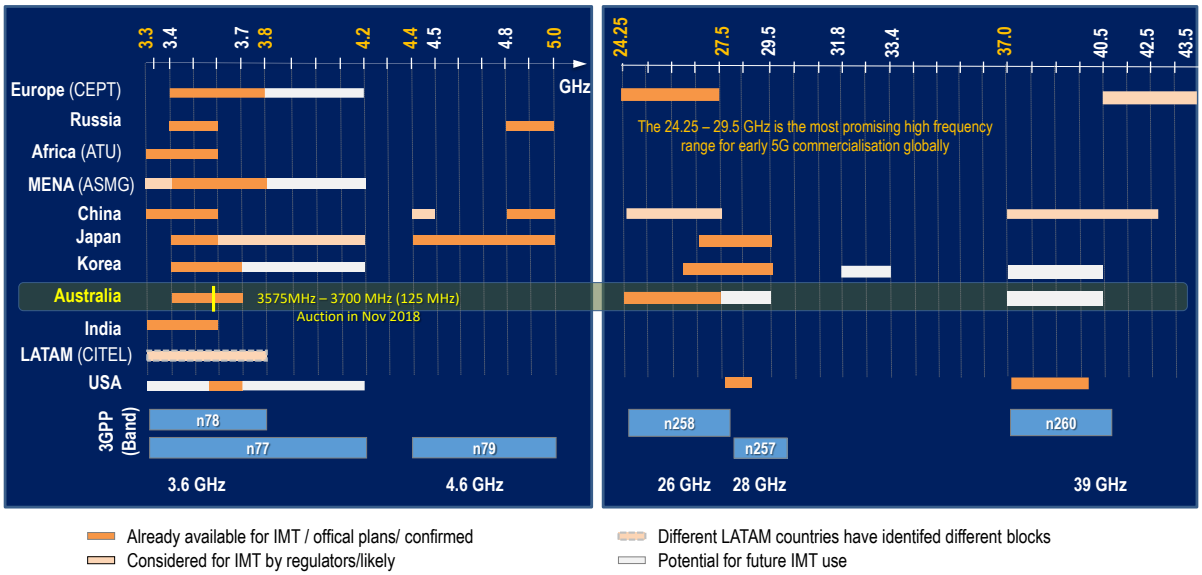


Figure 5. Global spectrum allocation and upcoming auction of 5G spectrum at 3.6 GHz in Australia

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 MHz–3700 MHz (125 MHz) in metropolitan and regional Australia by auction in October 2018 (ACMA, 2018). 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), 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) and 3GPP (2018e, 2018f, 2018g, 2018h).

- **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

http://doi.org/10.18080/ajtde.v6n4.161

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).

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).

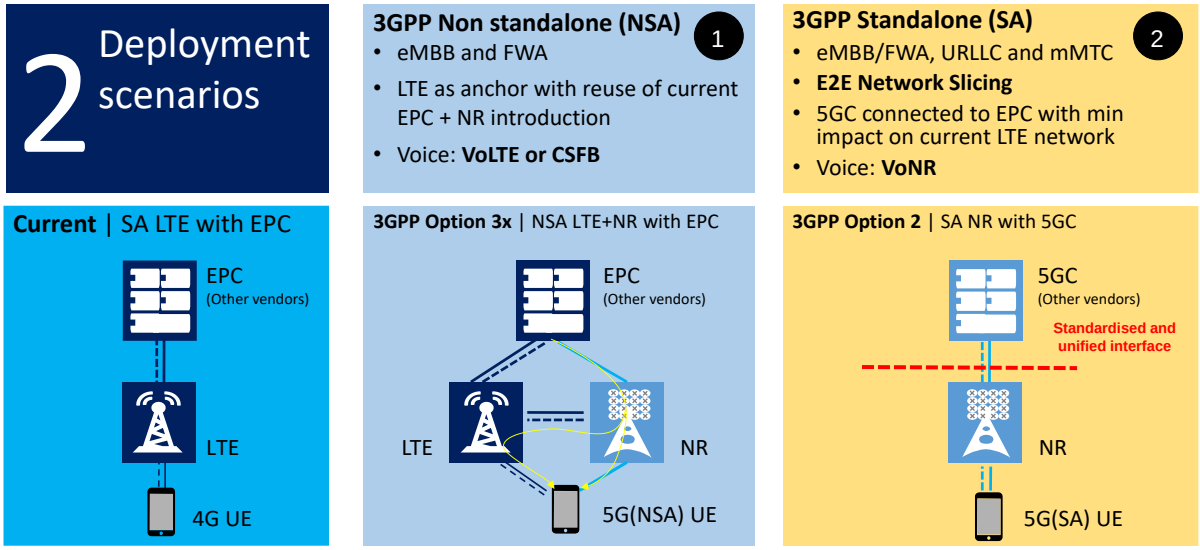


Figure 6. Main initial 5G deployment options (3GPP, 2018e, 2018f, 2018g, 2018h)

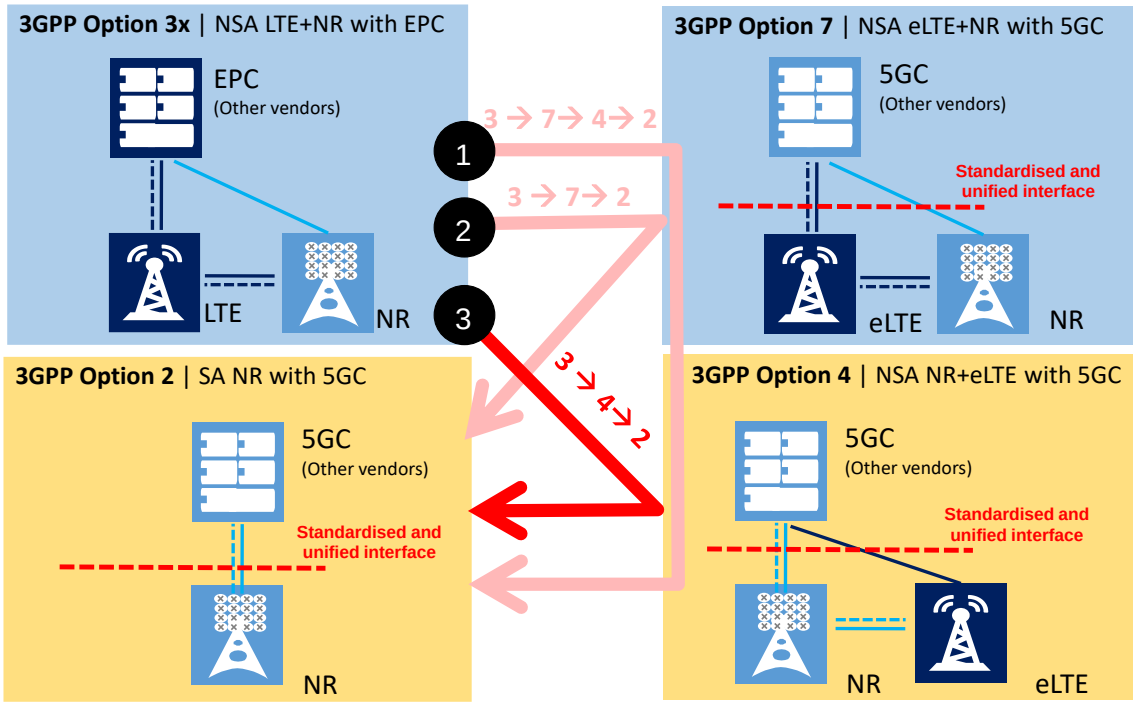


Figure 7. Long-term migration paths (Guttman, 2018)

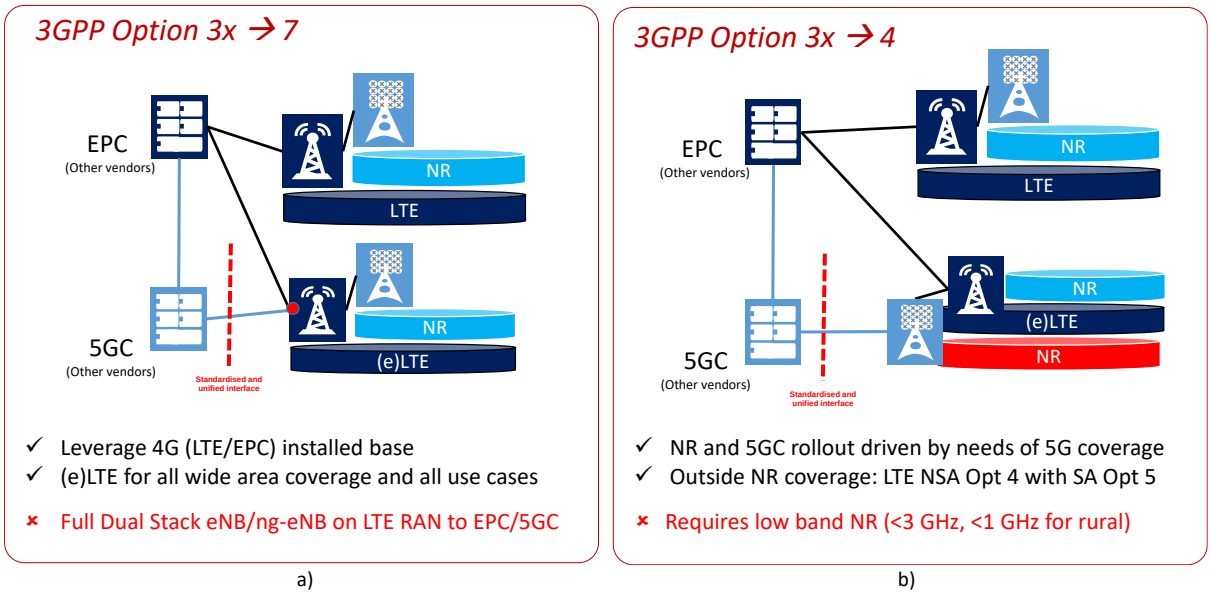
http://doi.org/10.18080/ajtde.v6n4.161

The medium-term migration strategies are basically two, depending on the carriers' spectrum availability for deploying the NR (Guttman, 2018):

- **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.

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) and a more convenient overview of the AN and CN functions in 3GPP (2018h).



a) b)

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

http://doi.org/10.18080/ajtde.v6n4.161

The two network domains are separated by a *standardised interface* (N2 and N3) defined in a set of specifications, with 3GPP (2018i) as the overarching specification which enables multi-vendor RAN–CN 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:

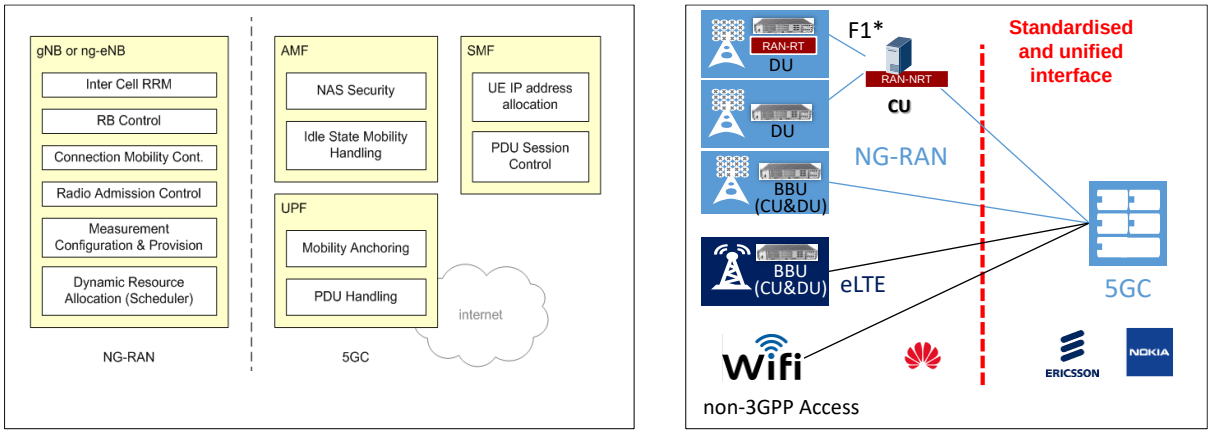
- **Central Unit (CU)-Distributed Unit (DU) split**: The RAN non-real time protocol stack is implemented in the CU and the functions more sensitive to delays in the DU close to the antennas.
- **CU-DU co-located at the Edge of the network**: All RAN baseband functionalities are running in one box placed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

http://doi.org/10.18080/ajtde.v6n4.161



AMF = Access and Mobility Function **UPF** = User Plane Function **SMF** = Session Management Function

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

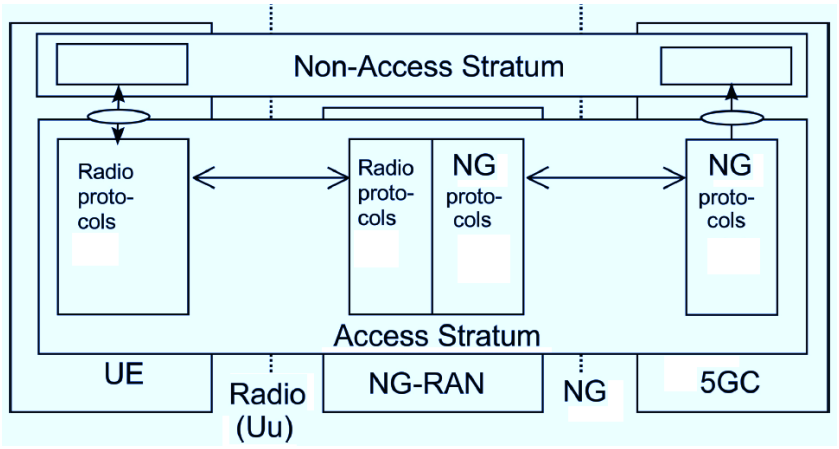


Figure 10. Overall NG-RAN architecture (Guttman, 2018; 3GPP, 2018e)

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). 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).

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.

http://doi.org/10.18080/ajtde.v6n4.161

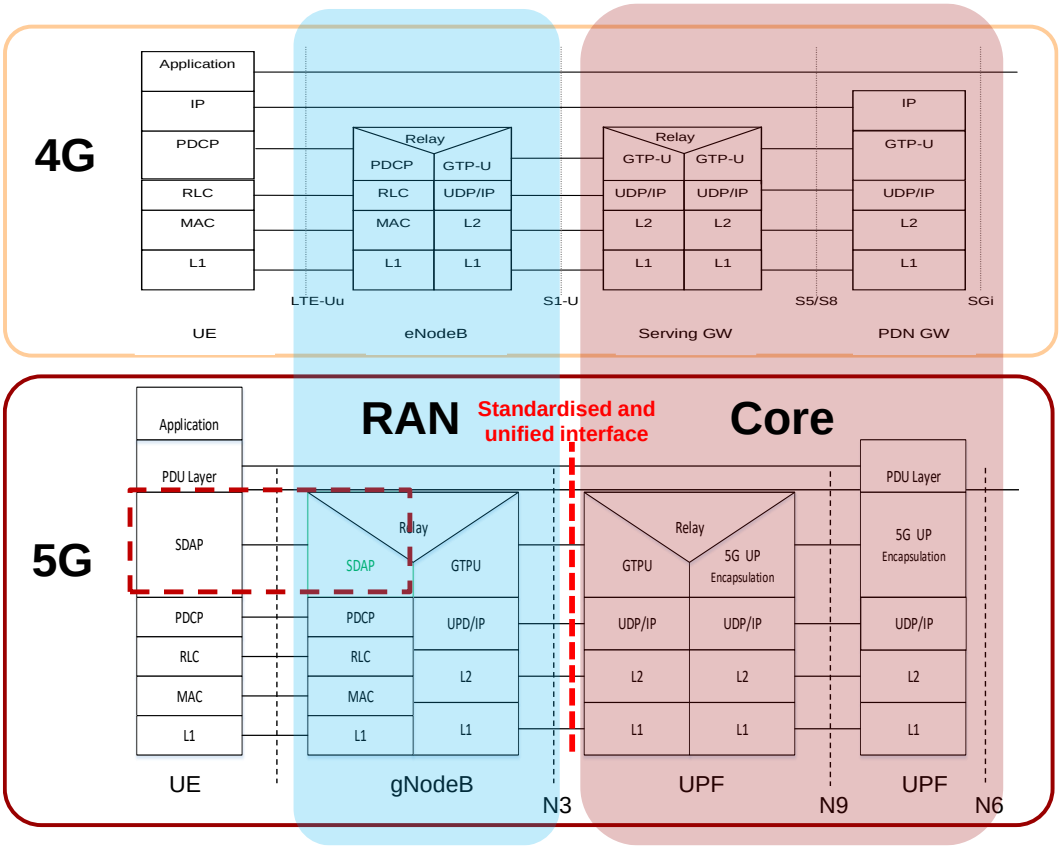


Figure 11. 4G/5G User Plane protocol stack (3GPP, 2018f; 3GPP, 2018g)

Where there is concern regarding core-RAN overlap, local breakout, e.g. to a Multi-access Edge Computing (MEC) server (ETSI, 2018), or remote break out to internal (operators' 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; 3GPP, 2018h). 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.

http://doi.org/10.18080/ajtde.v6n4.161

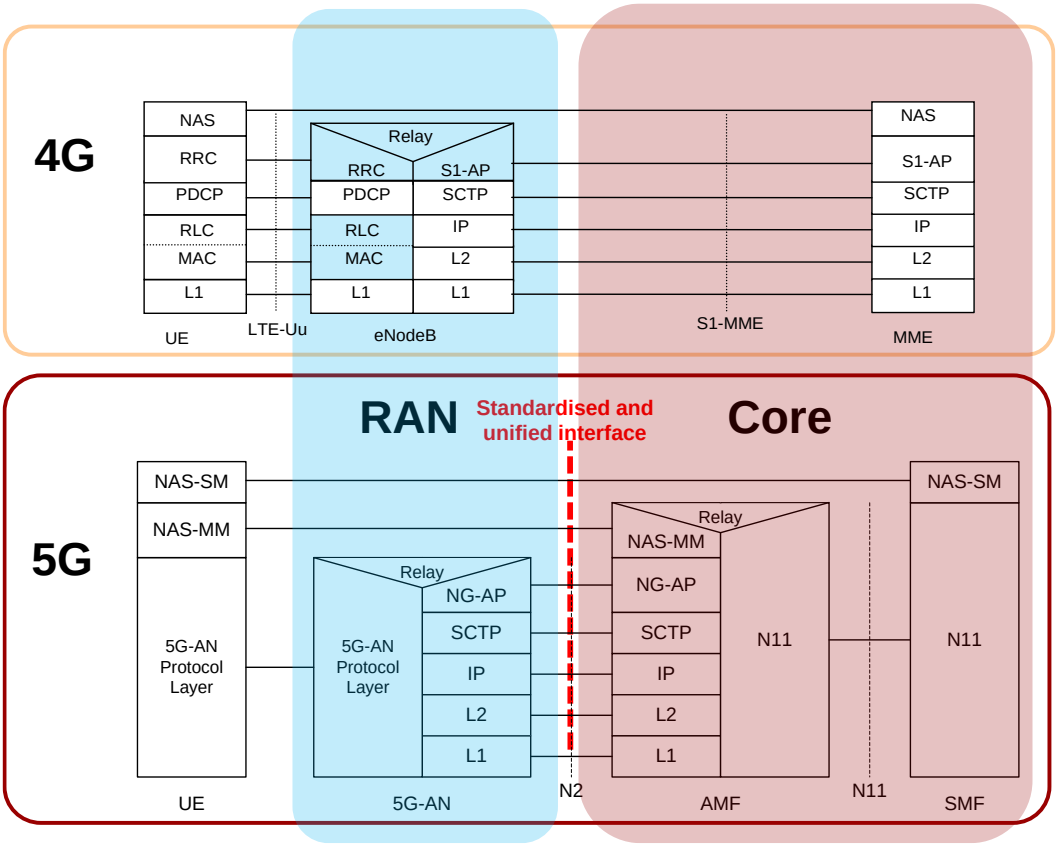


Figure 12. 4G/5G Control Plane protocol stack (3GPP, 2018f; 3GPP, 2018g)

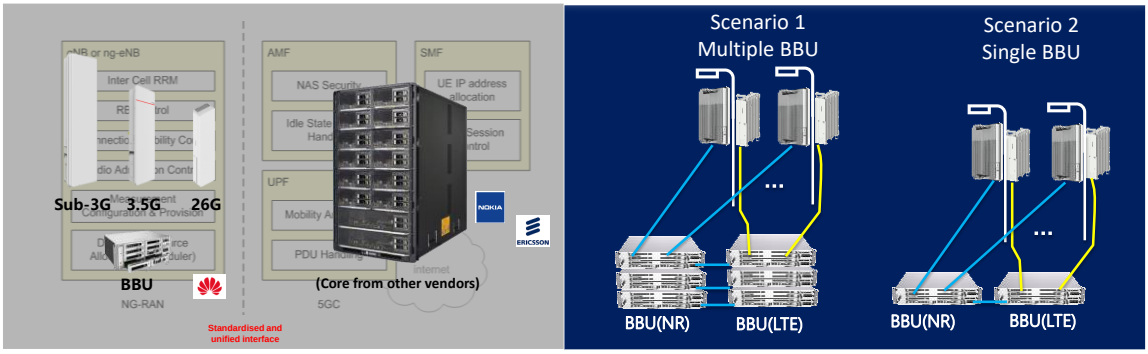


Figure 13. Huawei co-located CU-DU units running on Huawei dedicated hardware and software

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.

http://doi.org/10.18080/ajtde.v6n4.161

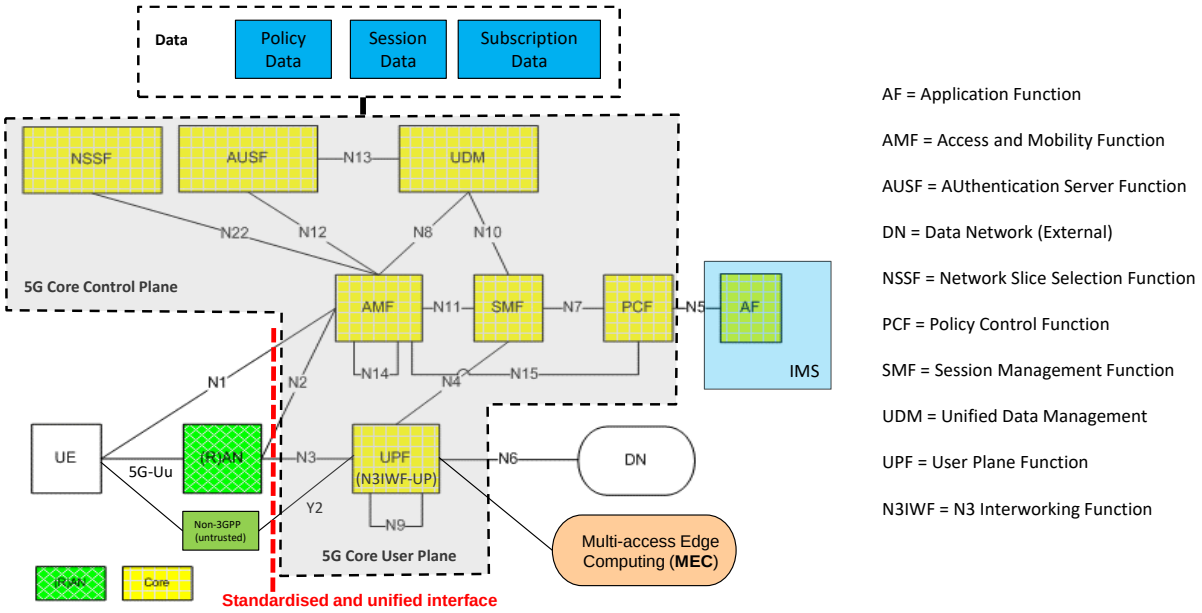


Figure 14. 5G Core (5GC) functions and interfaces (3GPP, 2018f; 3GPP, 2018h)

Other fundamental 5G enabling technologies, end-to-end, are (Soldani, 2018a): 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.

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). 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.

http://doi.org/10.18080/ajtde.v6n4.161

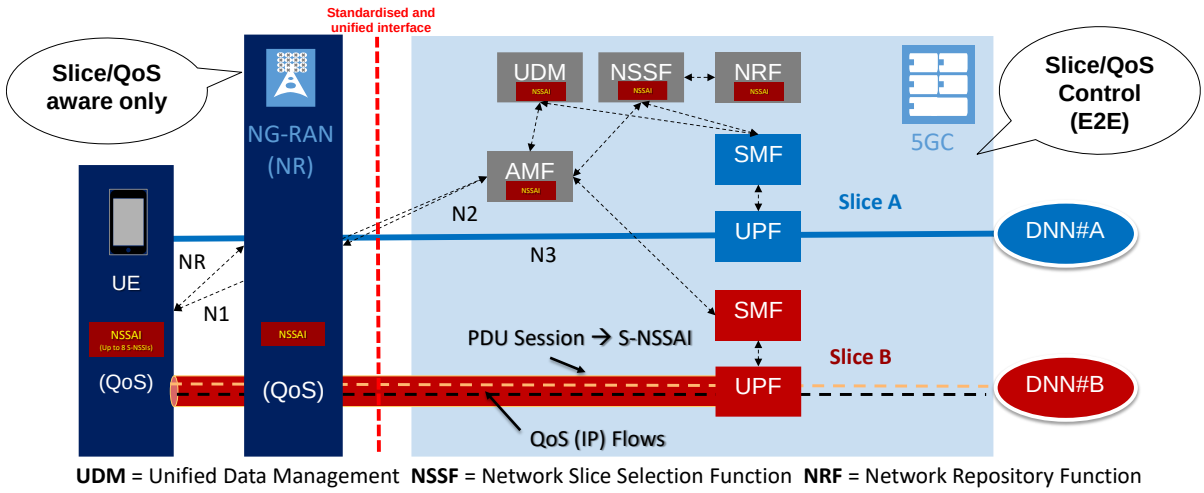


Figure 15. End-to-end QoS management and 5GC Slicing (Soldani, 2018a; 3GPP, 2018f; 3GPP, 2018h)

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).

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; 3GPP, 2018f; 3GPP, 2018h).

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). 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).

http://doi.org/10.18080/ajtde.v6n4.161

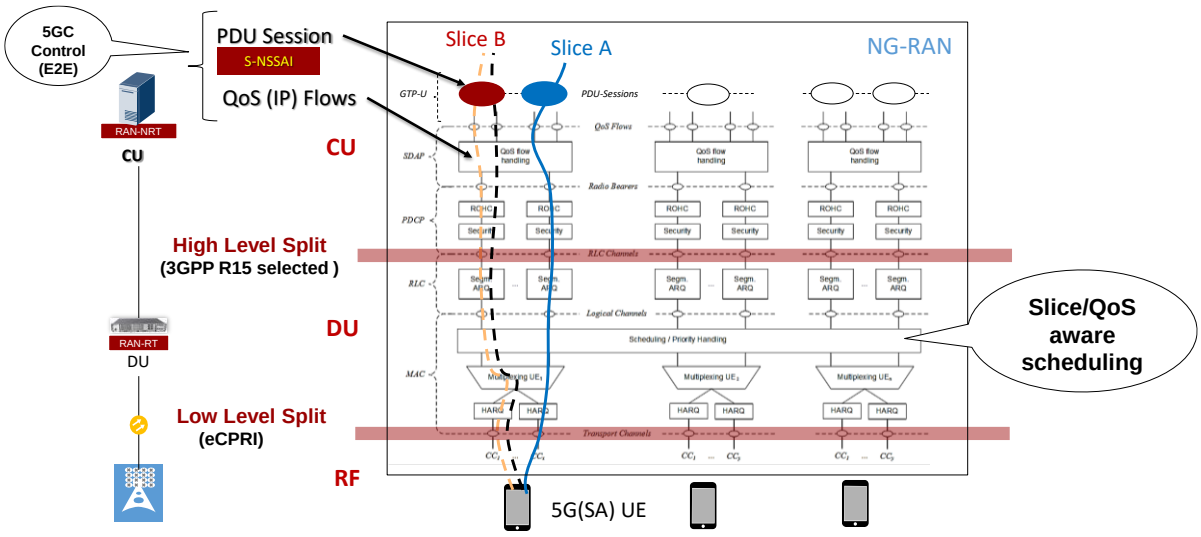


Figure 16. NG-RAN Slicing (Soldani, 2018a; 3GPP, 2018e; 3GPP, 2018f)

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).

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; 3GPP, 2018k). 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) — comparable to the IMSI of earlier system generations — 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), see Figure 18.

http://doi.org/10.18080/ajtde.v6n4.161

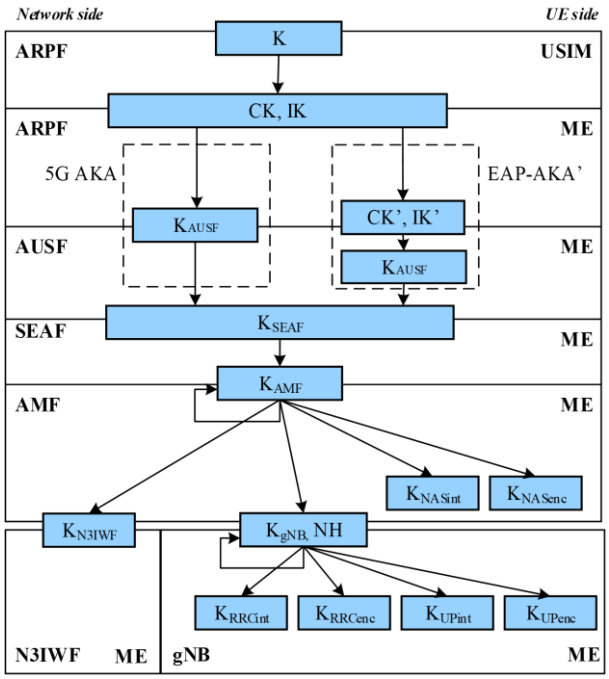


Figure 17. Key hierarchy generation in 5GS (3GPP, 2018j)

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 platform's 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.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.

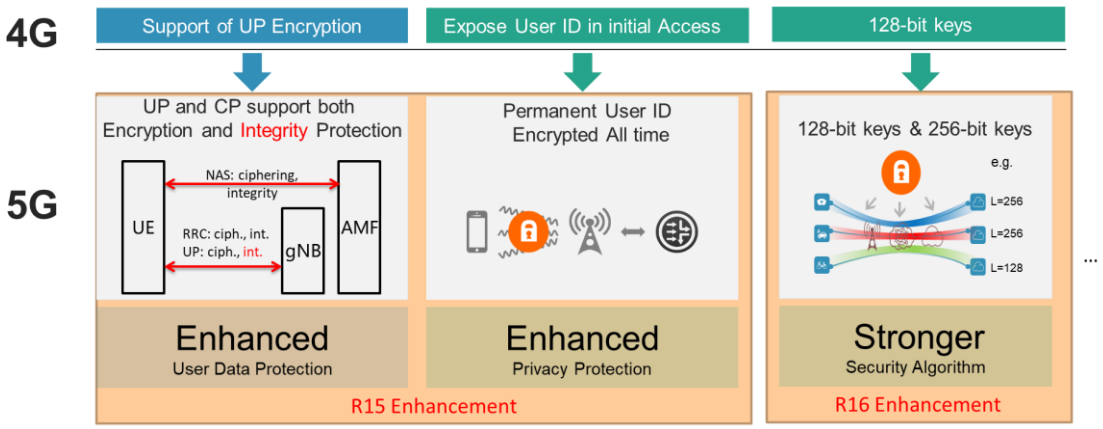


Figure 18. End-to-end security enhancement with 5G Evolution (3GPP, 2018j; 3GPP, 2018k)

http://doi.org/10.18080/ajtde.v6n4.161

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.

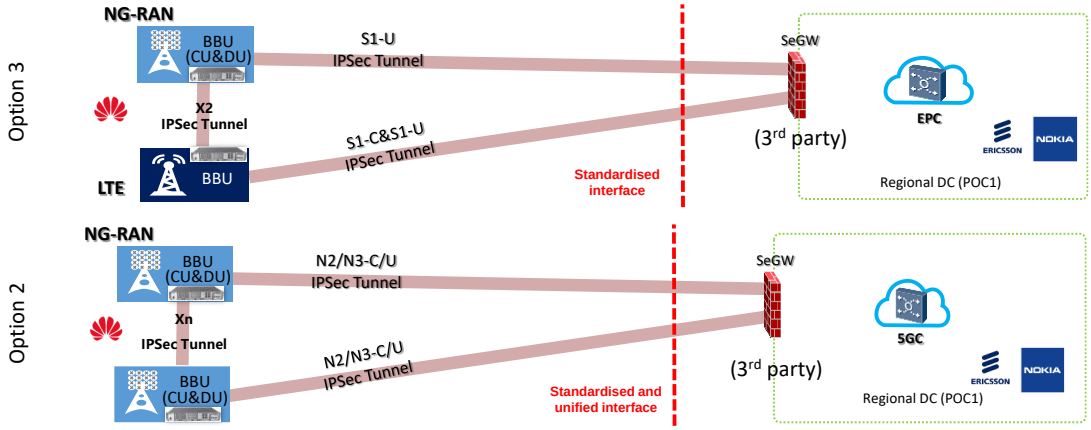


Figure 19. 3GPP NSA Option 3 and SA Option 2 security deployments

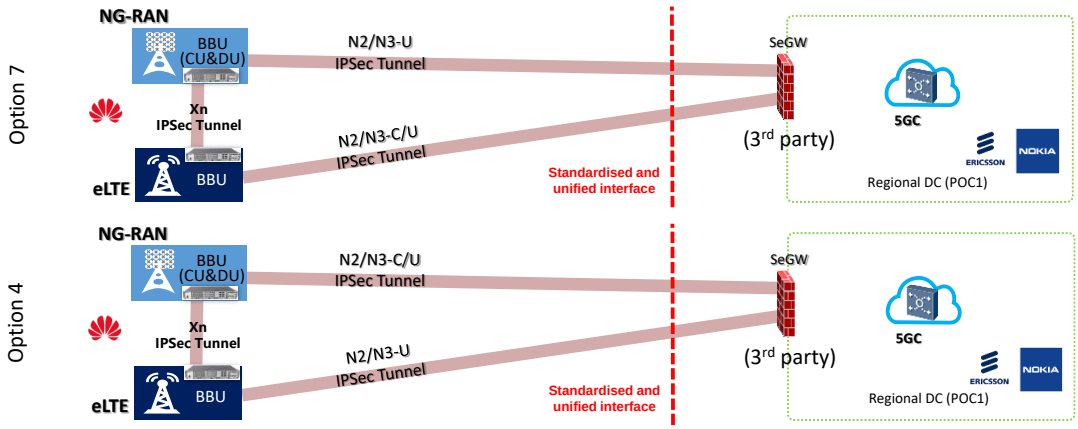


Figure 20. 3GPP NSA Option 7 and NSA Option 4 security deployments

http://doi.org/10.18080/ajtde.v6n4.161

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

http://doi.org/10.18080/ajtde.v6n4.161

hardware and software solution. The Huawei 5G RAN EMS can be installed and functions only on dedicated Huawei-provided hardware.

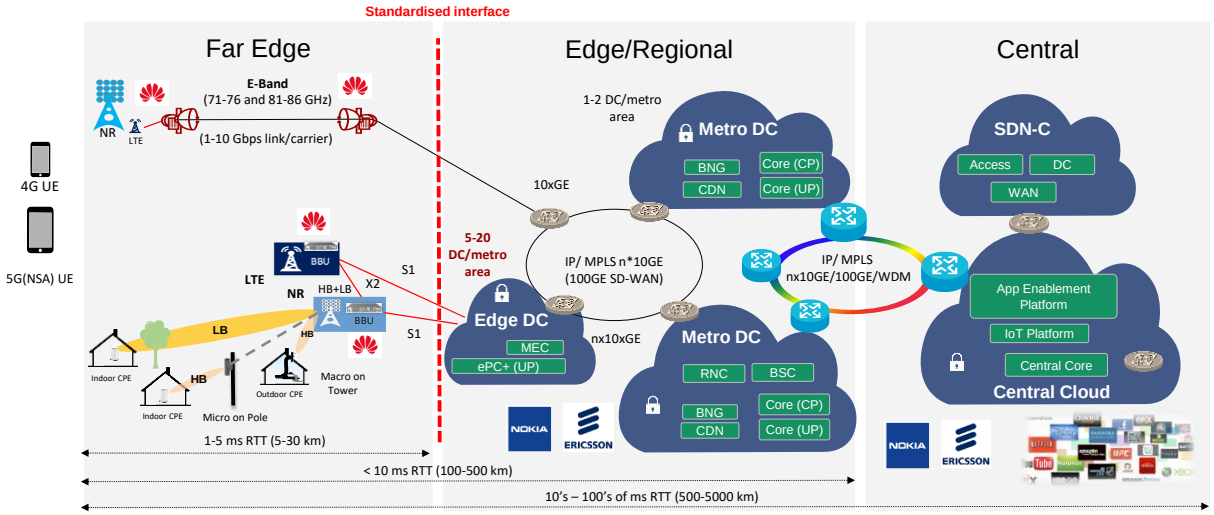


Figure 21. 5G 3GPP NSA deployment scenario with the existing Australian core network

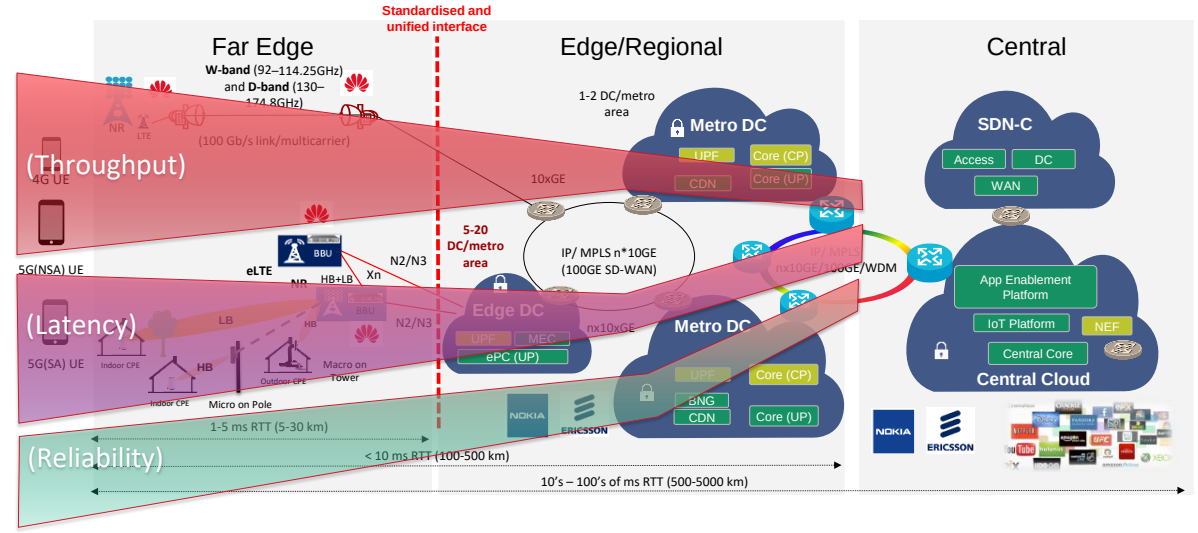


Figure 22. 5G 3GPP NSA/SA deployment scenario with 5GC in Australia, and example of network slices with different SLAs, in terms of throughput, latency and reliability parameters

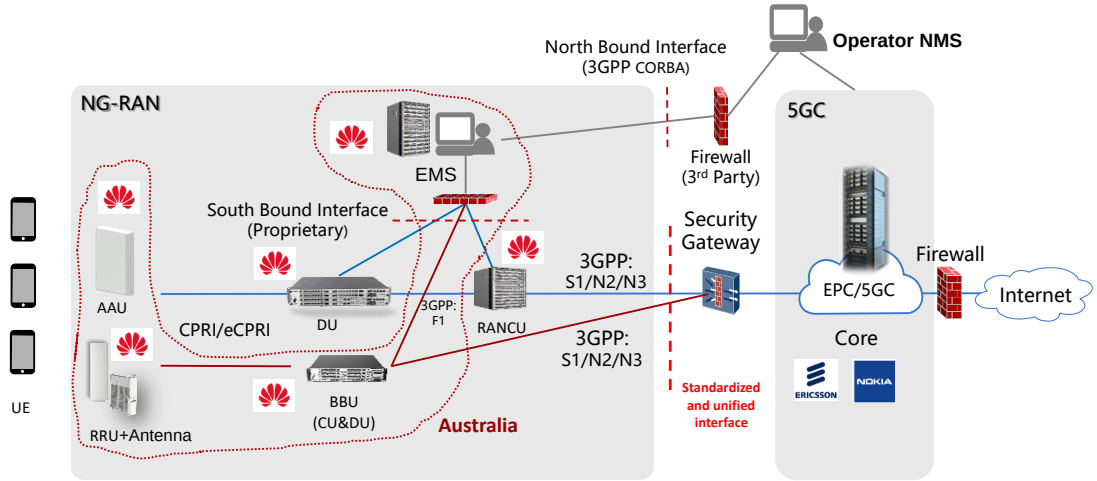


Figure 23. Example Huawei 5G RAN (NG-RAN) Element Management System deployment in Australia

http://doi.org/10.18080/ajtde.v6n4.161

The 5GS supports subscriber tracing similar to 4G in the RAN and is described in 3GPP (2018l). 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 operators' 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.

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).

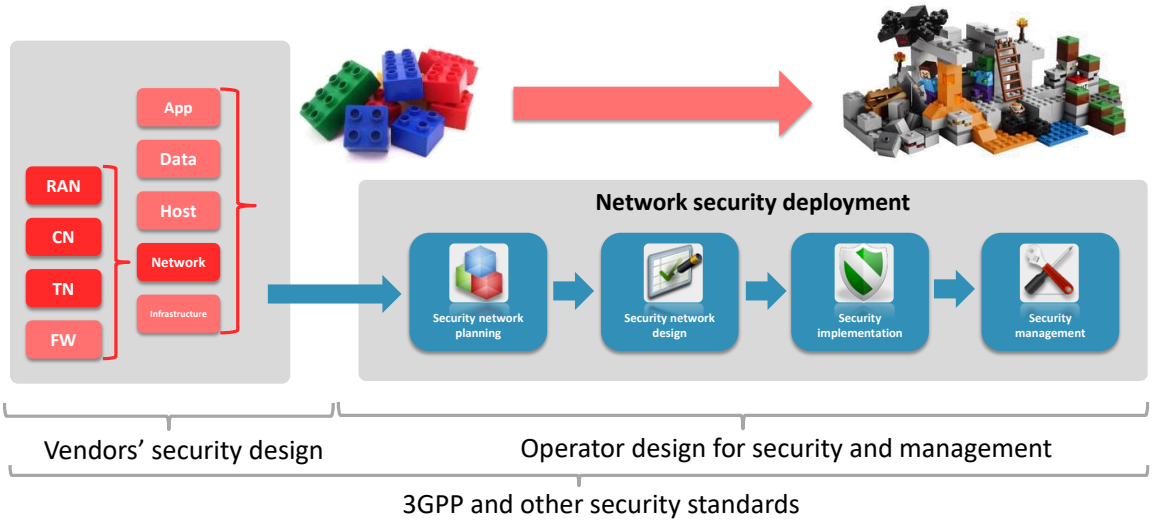


Figure 24. End-to-end security deployment and management

http://doi.org/10.18080/ajtde.v6n4.161

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.

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.

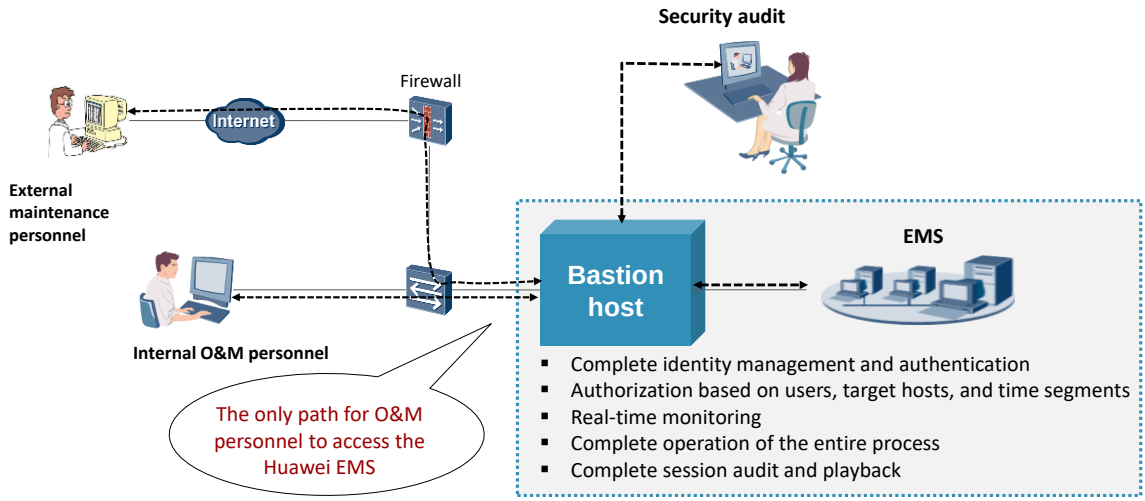


Figure 25. Example of third-party Bastion host for Huawei EMS logs

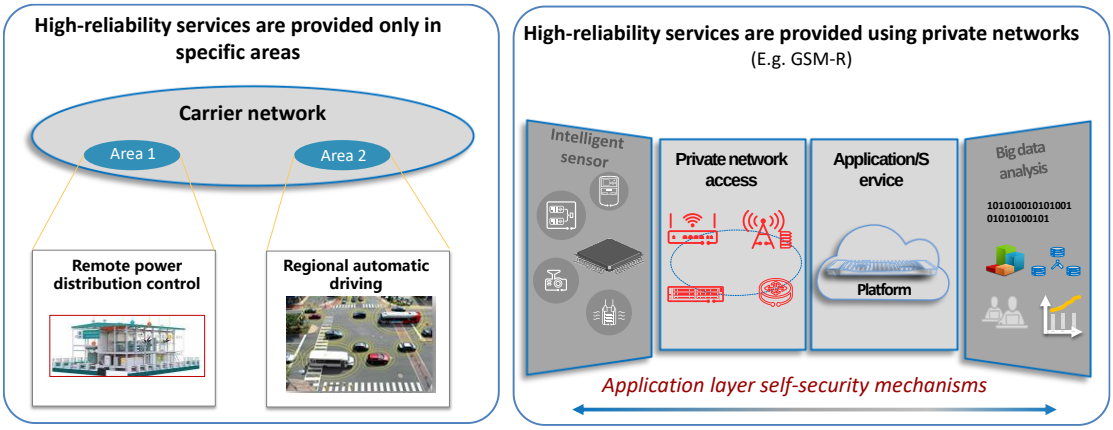


Figure 26. Examples of deployment of high-reliability and secure services

http://doi.org/10.18080/ajtde.v6n4.161

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) and, more recently, the Government introduced the Telecommunications Sector Security Reforms legislation (TSSR, 2018; TOLAA, 2017).

http://doi.org/10.18080/ajtde.v6n4.161

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 Australia's 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.

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 Huawei's 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.

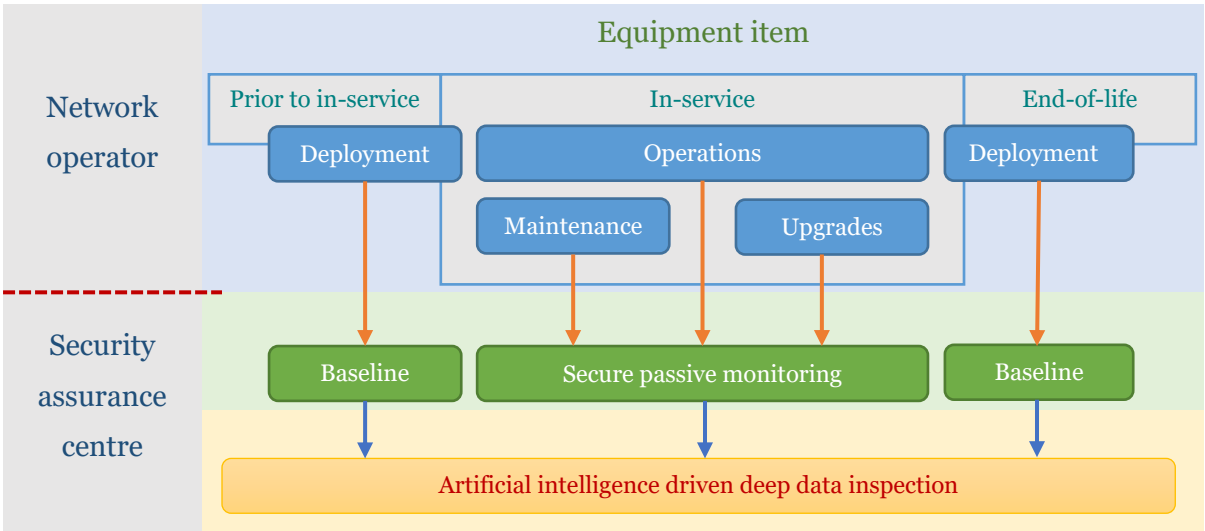


Figure 27. Passive independent security assurance system

http://doi.org/10.18080/ajtde.v6n4.161

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 “pipe” 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.

http://doi.org/10.18080/ajtde.v6n4.161

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. "Study 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

3rd Generation Partnership Project. 2018b. "3GPP", 3 July 2018, Retrieved from http://www.3gpp.org/

3rd Generation Partnership Project. 2018c. "Requirements for Further Advancements for Evolved Universal Terrestrial Radio Access", TR 38.913, v.14.0.0. 19 July 2018. Retrieved from https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2585

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

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

3rd Generation Partnership Project. 2018f. "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access",

http://doi.org/10.18080/ajtde.v6n4.161

3GPP TS 23.401 v.15.4.0. Retrieved from https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=849

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

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

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

3rd Generation Partnership Project. 2018j. "Security architecture and procedures for 5G System", 3GPP TS 33.501 v.15.0.0. Retrieved from https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

3rd Generation Partnership Project. 2018k. "Security Aspects". Retrieved from http://www.3gpp.org/DynaReport/33-series.htm

3rd Generation Partnership Project. 2018l. "Telecommunication management; Subscriber and equipment trace; Trace concepts and requirements", 3GPP TS 32.421 v.15.0.0. Retrieved from https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2008

ACMA. 2017. "Completes high-value spectrum auction at 700 MHz". 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

ACMA. 2018) "3.6 GHz band auction system". 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

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

ETSI. 2018. "MEC in 5G networks." White Paper No. 28, First edition, June 2018. Retrieved from https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf

http://doi.org/10.18080/ajtde.v6n4.161

Foye, B. 2018a. “Telstra to launch 5G services in 2019”. CRN. 5 February 2018. Retrieved from https://www.crn.com.au/news/telstra-to-launch-5g-services-in-2019-484422

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

Guttman, E; Mademann, F; Prasad, AR (Eds). 2018. "Special issue on ‘3GPP 5G Specifications’". *Journal of ICT Standardization*, May 2018. Retrieved from https://www.riverpublishers.com/journal.php?j=JICTS/6/1/jart

Huawei. 2018. “5G Spectrum”. Public policy position paper, March 2018. Retrieved from http://www-file.huawei.com/-/media/CORPORATE/PDF/public-policy/public_policy_position_5g_spectrum.pdf?la=en

ITU-T. 2018. “Requirements of the IMT-2020 network”, ITU-T Rec. Y.3101, January, 2018. Retrieved from https://www.itu.int/rec/T-REC-Y.3101-201801-I/en

Kennedy, D. 2018. “5G in Australia: Evolution not Revolution”. Ovum, TMT intelligence Informa, June 2018. Retrieved from https://www.nbnco.com.au/content/dam/nbnco2/2018/documents/media-centre/5G_report_June_2018.pdf

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

NGMN Alliance. 2015. “NGMN 5G white paper”. February 2015. Retrieved from https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf

Soldani, D; Airas, P; Hoglund. T; Rasanen, H; Debrecht, D. 2017a. “5G To The Home”, *IEEE VTC*, Spring, 2017. Retrieved from https://ieeexplore.ieee.org/document/8108603/

Soldani, D; *et al.* 2017b. “5G Mobile Systems for Healthcare”, 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, NSW, 2017, pp. 1-5. DOI: 10.1109/VTCSpring.2017.8108602

Soldani, D. 2018a. “5G beyond radio access: A flatter sliced network”, *Mondo Digitale*, AICA, March 2018. Retrieved from http://www.sipotra.it/wp-content/uploads/2018/03/5G-beyond-radio-access-a-flatter-sliced-network.pdf

http://doi.org/10.18080/ajtde.v6n4.161

Soldani, D; Guo, YJ; Barani, B; Mogensen, P; Das, CL. 2018b. "5G for Ultra-Reliable Low-Latency Communications", Special Issue of *IEEE Network Magazine*, March 2018. Retrieved from https://ieeexplore.ieee.org/document/8329617/

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

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

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

UK Government. 2018. "Huawei cyber security evaluation centre oversight board: annual report 2018". UK Government report, 19 July 2018. Retrieved from https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2018

http://doi.org/10.18080/ajtde.v6n4.161

What Now for Australia's NBN?

How Australia's politics, insular policies and preference for monopolies have made Australia a broadband backwater

Gary McLaren
Chief Technology Officer – Hong Kong Broadband Network Limited
Former Chief Technology Officer – NBN Co Limited

Abstract: Australia, like other countries, embarked on deregulation and privatisation of its telecommunications market in the late 1980s. The success of infrastructure competition in the mobile communications sector in pushing Australia to being a world leader in that sector contrasts with the failure to achieve the same in fixed telecommunications. Australia's politics, insular policies and categorisation of fixed telecommunications as a natural monopoly have made Australia a global laggard in the provision of broadband services. The return of government ownership of telecoms infrastructure in the form of the National Broadband Network and the continuing lack of investment in fibre infrastructure highlight the political and policy failures that have accumulated. A disaggregation of NBN Co into competing technology-based entities, along with the establishment of a regional telecommunications fund financed by a broad-based telecommunications levy, is recommended as the answer to fix these long-term problems.

Keywords: Telecommunications policy, NBN Co, Natural monopoly, Infrastructure competition, Universal Service Obligation.

Introduction

This paper is a contribution to a recurring debate on Australia's seemingly never-ending drama in its fixed telecommunications market, prompted by the near completion of the build phase of Australia's National Broadband Network (NBN), which is expected in 2020.

The last 30 years of market reform in Australia saw an initial push for deregulation and the introduction of competition while the government-owned monopoly, Telstra (formerly Telecom Australia), prepared for privatisation. This push faltered in the early 2000s when the issue of the full privatisation of Telstra had to be reconciled with its overwhelming market dominance in the fixed telecommunications market. Rather than push through further

http://doi.org/10.18080/ajtde.v6n4.162

reforms favouring competition by restructuring Telstra (e.g. through structural separation prior to full privatisation), the Coalition Howard Government opted in 2005 for a regulatory framework that regulated pricing and service levels for Telstra's retail and wholesale customers but maintained Telstra's overall infrastructure dominance in the fixed network. The natural consequence of this policy framework was the lack of commercial drivers for investment in fixed telecommunications infrastructure (by either Telstra or its competitors) at a time when demand for bandwidth was growing exponentially as a consequence of the growth of the Internet.

Instead of revisiting the options to restructure a fully privatised Telstra, the Labor Rudd/Gillard Government returned to the government-owned monopoly model by creating the National Broadband Network Company (NBN Co). This new company was tasked with the following objectives: (i) to build the necessary wholesale access infrastructure needed for universal high-speed broadband; and (ii) to negotiate a deal where Telstra would voluntarily relinquish its fixed telecommunications dominance, by transferring its lead-in conduits and renting space in its duct access network and exchange facilities to NBN Co. As a result the Australian government and taxpayer are responsible for the lion's share of investment in the fixed access telecommunications market, leading to the inevitable politicisation of the complex infrastructure upgrades necessary to support past, present and future growth in digital communications.

The current build phase of the NBN has now been reduced in scope by the post-2013 Coalition Government, being primarily reliant on minimal upgrades to the existing copper and HFC networks. As it nears completion (forecast for 2020), there is yet another opportunity for the failures of the policies of the last 30 years to be understood and addressed in order to ensure the necessary ongoing investment is forthcoming and Australia's lagging broadband status (Ookla, 2018) is corrected.

Further drivers for policy reform are the strong technology development roadmap and investment growth in the mobile telecommunications sector. As competition and commercial imperatives drive new technologies, such as 5G, there will be significant spillovers into the fixed telecommunications market, further complicating and possibly jeopardising the NBN investment strategies.

This paper highlights the past policy mistakes and puts forward a disaggregation of NBN Co and gradual privatisation of competing NBN operational business units as the best way to restore the commercial drivers of investment to increase investment efficiency and minimise losses to the Australian taxpayer.

http://doi.org/10.18080/ajtde.v6n4.162

Economic and Technology Drivers of Reform

The Hawke Government kicked off the last 30 years of reform when it announced in May 1988 the establishment of a new dedicated telecommunications regulator, AUSTEL, and the restructuring of the government telecommunications commissions, Telecom Australia, OTC and Aussat, as corporatised Government Business Enterprises (Australian Government, 1988).

The reasons for the reforms were numerous. Micro-economic reform of many of Australia's markets was in full swing as the Hawke Government sought to open Australia's economy and reduce protectionism and government control of key sectors. These policies were part of a global trend to reduce government controls in markets that were advanced, stimulated by new economic thinking developed during the 1960s and 1970s, now recognised as neo-liberal economics, and given political traction by the Reagan and Thatcher governments in the USA and UK in the 1980s. Commencing in the 1990s, privatisations and competitive reforms were undertaken in many Australian industries such as financial services, transport and electricity (Reserve Bank of Australia, 1997).

However, in telecommunications there was a further important driver of change beyond just economic thinking. Technology was forcing the industry to change rapidly. The use of digital integrated circuit chips from the 1970s was having a large impact on telecommunications, which would later give birth to the internet and mobile phones. The analogue telephony model that had characterised most telecommunications networks for a century was being swept away by the digital revolution. New technologies were entering the industry that would enable cheaper long-distance calling, higher speed data transmission and wireless communications. The internet and mobile phone industries were in their infancy but many could see the revolution these new digital technologies would make to the industry and to society in general.

In hindsight, it is clear that, without the corporatisation of Telecom Australia as an independent Government Business Enterprise in July 1975 and the opening up of the telecommunications market in the late 1980s, Australia would not have kept pace with this digital revolution. If bureaucratic government department budget and approval processes had continued, then investments in new technologies, such as packet switching, cellular mobile and long-distance optical fibre networks, would have likely been non-existent or delayed, to the detriment of Australia's businesses and consumers. The first steps to transform Australia's telecom operators, Telecom Australia, OTC and Aussat, into corporatised Government Business Enterprises with boards of directors making commercial decisions in response to technological and market opportunities, were not just ideological, they were a pragmatic response to the fast changing and accelerating technology landscape of the time.

http://doi.org/10.18080/ajtde.v6n4.162

Mobile communications, being a totally new industry in the late 1980s when the reforms kicked off, have been subject to open competition and minimal government regulation and ownership from the beginning. Government involvement has been mainly left to regulating and selling access to the necessary spectrum and ensuring there is sufficient competition between mobile operators to drive investment. The story has been one of huge growth. Australia has become one of the leading markets for both the penetration and quality of mobile services (OpenSignal, 2018). The industry has transitioned through the large investments necessary to go from AMPS to GSM to 3G and 4G and is now gearing up for further investments to enable 5G for the 2020s (Telegeography, 2018). At the heart of this innovation and growth has been competition between the mobile network operators. Government intervention has been limited to the amount necessary to ensure a functioning competitive market, access to scarce public resources, such as spectrum, and ensuring mobile operators have sufficient ability to deploy infrastructure effectively on public and private property.

The author is unaware of any arguments that it would have been more efficient in terms of investment and better for consumers if Telecom Australia had retained its government-owned monopoly status and been the sole operator of mobile services. The duplication in network infrastructure (antennas, towers, transmission networks, core networks) that results from having multiply mobile operators is not argued as causing inefficiencies that mean consumers are paying more or receiving less than what the mobile market is currently providing.

The contrast with the fixed telecommunication market evolution in Australia could not be greater. The established fixed market was more complex and subject to more political lobbying, given its legacy telephony structure and revenues, the diversity of new business market services being demanded, the rise of the internet and the involvement of media tycoons through the introduction of cable TV, and the historical vested interests of the telecom unions.

At the heart of the disconnect in Australia's fixed broadband policy has been the inability to create a stable policy framework for transition from the natural monopoly of the legacy telephony network of the pre-1980s to the modern competitive forms of technology that deliver broadband services.

From Monopoly to Competition and Back Again

The 30-year period between 1988 and 2018 for Australia's fixed telecommunications market is best understood in terms of three distinct phases.

The first phase, from 1988 to 2003, what I call the "Attempting Competition" phase, saw the restructuring of the government telco entities (Telecom Australia, OTC and Aussat) and the entrance of Optus in 1992 and further new entrants in 1997. An intense period of competition

http://doi.org/10.18080/ajtde.v6n4.162

between Optus and Telstra in long-distance calls and cable TV (with hybrid fibre-coax cable infrastructure) ensued between 1997 and 2001, before Telstra came out the overall victor. The first partial privatisation of Telstra occurred in 1998.

The second phase from 2003 to 2005, the "Pivot Point", was when Telstra's full privatisation and market dominance had to be resolved, with a parliamentary inquiry being scheduled into the possible structural separation of Telstra. In the end, the federal government shut down the parliamentary inquiry in early 2003 and proceeded to prepare Telstra for sale in 2005 without structural separation, in a move guaranteed to maximise shareholder returns as opposed to promoting infrastructure competition.

The third phase, from 2003 to the present, in the "Back to Government Monopoly" phase, policy makers attempted to come to grips with Telstra's dominance with various forms of regulatory and policy initiatives, culminating in the eventual creation of NBN Co and the structural separation of Telstra to return to a monopoly fixed network wholesale infrastructure model.

1988-2001: Attempting Competition

After some intense debate in the Hawke Government in 1990 between the Treasurer, Paul Keating, and the Minister for Transport & Communications, Kim Beazley, it was decided to pursue Beazley's "strong national carrier" model by combining Telecom Australia and OTC, rather than Keating's "full network competition" with OTC merging with Aussat to compete with Telecom Australia (Raiche, 1997). A phased period of duopoly involving a new entrant, Optus (who was obliged to acquire Aussat), and Telstra began in 1991, to be followed by open competition from 1997 (Productivity Commission, 2001a).

These first steps towards competition would be characteristic of future policy mistakes. Rather than reform the market in a manner that creates a semblance of balance between competitors, the Hawke/Keating Government ensured Telstra (the combined Telecom Australia and OTC) was a dominant player faced with a new entrant that was weighed down by the acquisition of Aussat but given access to Telstra's network at regulated access pricing for access to all customers.

In business markets, mainly located in CBDs and business parks, this policy was moderately successful after 1997 with new network operators building fibre networks (e.g. Optus, AAPT, PowerTel, Uecomm, Pipe Networks) that would bring many of the benefits necessary for large business customers. The unbundling of the local loop and the building of competing DSL service providers (e.g. RequestDSL and Nextep) enabled some small and medium businesses to also benefit from competition with enhanced business broadband services.

http://doi.org/10.18080/ajtde.v6n4.162

The residential telecommunications market, however, relied to a large extent on new entrants (e.g. AAPT and Primus, along with Optus) using regulated wholesale services acquired from Telstra to compete in the long-distance telephony market. The introduction of regulated wholesale ADSL and unbundling of copper access also enabled a number of strong internet retail service providers to emerge under the leadership of willing entrepreneurs (e.g. TPG Telecom, iiNet, Internode and Netspace) to take advantage of the growing demand for broadband services as the dial-up internet model declined.

There was hope that the "ladder of investment" hypothesis (Cave, 2004) would enable these service providers to transition to sustainable infrastructure-based (or facilities-based) competitors rather than relying heavily on Telstra's wholesale services. Infrastructure-based competition was seen by the ACCC as the preferred long-term structure for the fixed telecommunications industry (ACCC, 2004).

Optus, prior to the 1997 full deregulation, had commenced the rollout of a new Hybrid Fibre Coaxial (HFC) network to bring cable TV and local telephony to residential consumers and bypass Telstra's copper network altogether. Telstra, in a cable TV venture with News Corporation to be called Foxtel, responded by building its own HFC network in the same suburban areas as Optus. This early push into infrastructure competition was a bold initiative that had much to do with the introduction of pay TV and media mogul rivalries between Kerry Packer and Rupert Murdoch, rather than just pure telecommunication services (Westfield, 2000). However, the end result was large financial losses for both companies, with Optus eventually losing the cable TV wars and Foxtel becoming the dominant subscription TV service provider. Optus retained its HFC network, which it used to provide DOCSIS-based broadband, but was eventually relegated to be a reseller of the Foxtel Pay TV service in the subscription TV market.

2001-2003: The Pivot Point

By 2001, Telstra had been partially privatised through two share offerings to the Australian public, the first labelled T1 at a price of $3.30 in 1997 and the second labelled T2 at a price of $7.40 in 1999 (Telstra, 1999). A total of 49.9% of Telstra's equity was sold during these two tranches, with foreign investors restricted to just 35% of this new equity. These sales had been politically contested at the federal elections of 1996 and 1998, where the Howard Government prevailed over first the Labor Keating Government and then the Beazley Labor Opposition.

During 2000 and 2001, the Productivity Commission undertook a review of the telecommunications market and the telecommunications specific regulatory framework that had been established under Part XIB and XIC of the Trade Practices Act. However, the inquiry's terms of reference specifically did "not encompass the structural separation of

http://doi.org/10.18080/ajtde.v6n4.162

Telstra, in line with Government policy on this issue" (Productivity Commission, 2001a). The inquiry's report did highlight that the regulatory processes were "slow, uncertain and inefficient" and that "there is a risk of reduced investment in core telecommunications infrastructure – with long-run consequences for consumers and for Australia's overall economic efficiency" (Productivity Commission, 2001b, p. xxii).

The structural separation of Telstra, although not part of the Productivity Commission's inquiry, had begun to surface as a key issue, given the pending full privatisation of Telstra (to which the Howard Government had re-affirmed its commitment in its successful 2001 election campaign). The key question was whether a fully privatised vertically integrated Telstra that accounted for 95% of local access lines (via its copper and HFC network) (Productivity Commission, 2001b, p. 99) could be regulated in a manner that would still ensure ongoing investment in networks and improvement of services in the fast evolving internet and digital market that Telstra and its competitors were vying over.

Telstra's share price had hit a new post-T2 low of $3.42 in March of 2003 after the tech boom had subsided. Many Australians, now investors in Telstra, were disappointed with the share performance and the losses since the T2 peak of $7.40. Regional Australians were also dissatisfied with Telstra's performance and the government promised not to sell any further Telstra equity until "the Government … is satisfied that arrangements are in place to deliver adequate services to all Australians" (Cth, 2002a). The issue with regional telecommunications was addressed through a Regional Telecommunications Inquiry led by Mr Dick Estens, the recommendations of which the Howard Government agreed to implement in full (Cth, 2002b).

Telstra's market dominance issue was not as politically charged as the quality of regional telecommunications, but it was also addressed through two other inquiries. In March 2002, the Howard Government Minister responsible for telecommunications, Richard Alston, asked the ACCC to undertake an inquiry into the emerging market structures of the communications sector, given the dominance of Telstra in both the telephony and pay TV markets and the emerging broadband market (ACCC, 2003). In May 2002, the Labor Opposition Spokesperson on telecommunications, Lindsay Tanner, kicked off a review of possible Telstra reform options through a public discussion paper (Tanner, 2002).

The Labor discussion paper included an "option of structural separation – the idea of separating Telstra's core network from its other businesses to effectively eradicate Telstra's market dominance". This prompted the Howard Government to instigate a parliamentary inquiry into structural separation of Telstra but it was abandoned the day before the first

http://doi.org/10.18080/ajtde.v6n4.162

hearing in February 2003 after Labor announced it would pursue an "internal virtual separation" rather than full structural separation of Telstra (Ryan, 2003).

Labor had formally kicked into play the idea of "vertical" structural separation of Telstra into network and retail businesses. This reform option would live on, despite Labor's initial backtracking, to eventually dominate the thinking of reform of Australia's fixed telecommunications market and heavily influence the subsequent development of the NBN after Labor obtained government in 2007 (Gerrand, 2004; 2017).

However, the ACCC review kicked off by Alston also addressed the emerging dominance of Telstra. The ACCC's advice was clear cut and very direct: Telstra should be made to divest itself of its HFC network assets and its 50% stake in Foxtel. This "horizontal" separation of Telstra was seen by the ACCC as a "significantly more restrained policy option than the vertical separation of Telstra as a means of increasing competition in the telecommunications sector" (ACCC, 2003).

The Howard Government rejected the ACCC's advice on the grounds that the costs outweighed the perceived benefits of divestiture and the risk to taxpayers of compensation to Telstra's 1.8 million shareholders (Alston, 2003). Labor, however, supported the ACCC's horizontal separation recommendation (Ryan, 2003). Telstra's lagging share price at the time was clearly a political issue. Telstra's full privatisation was government policy and a higher share price would help the government's finances and also assuage the concerns of existing Telstra shareholders, who were a key political constituency for the Howard Government. The prospects of an HFC divestiture would not have squared with these political imperatives. The ACCC advice was publicly released on 20 June 2003. The legislation to fully privatise Telstra was formally introduced into parliament on 25 June 2003 (after the Howard Government accepted all recommendations from the Esten's Regional Telecommunications Inquiry). However, it would take the Howard Government another election victory in 2004 and significant political lobbying to get the decisive vote of a new National Party Senator, Barnaby Joyce, before the Howard Government would achieve its long-held goal of legislation authorising the full sale of Telstra in September 2005 (Sydney Morning Herald, 2005).

At the end of 2003 it was clear that Telstra's fixed network dominance in the residential market would remain. The Howard Government had rejected reforms put forward by the ACCC and the Labor Opposition to substantially reform Telstra prior to full privatisation. The ACCC stated clearly that "Telstra's market power across a range of telecommunications markets and a degree of horizontal and vertical integration remains a concern" (ACCC, 2003, p. 24).

The resolution of the conflict between Telstra's shareholders and competition had been decided in favour of the shareholders – and a much larger financial windfall to the federal

http://doi.org/10.18080/ajtde.v6n4.162

budget. Telstra would be a private regulated monopoly. The consequences of this outcome would be far reaching. It would soon become clear that a private monopoly could be regulated in terms of pricing and, to a lesser degree, service quality, but it could not be forced to invest and upgrade its infrastructure and services. To the contrary, the regulation would be a reason to not undertake the necessary upgrade of its infrastructure to keep Australia in the global race for fixed broadband.

2004-2018: Back to Government Monopoly

The early months of 2004 set the scene for the next few years of regulatory skirmishes when Telstra started to flex its muscles in the growing ADSL broadband market. Optus and Telstra had negotiated a wholesale deal in November 2003 for Optus to resell Telstra ADSL services. This would enable Optus to enter the ADSL broadband market, which was at an inflexion point as the entrepreneurial ISP sector started to find ways to satisfy the residential market's demand for a transition from dial-up to "always on" broadband (McCulloch, 2004).

A day before the launch of Optus' new ADSL services, Telstra dropped its retail ADSL price by 25% without changing its wholesale price to Optus. Optus and the other ISPs called out the price squeeze and the ACCC took formal steps to investigate if Telstra had breached special telecommunications provisions of the Trade Practices Act. A protracted process followed while Telstra grew its ADSL market share in parallel. The end result was that Telstra gained a market-leading share of over 50% in this new and growing market — a market share that it still holds nearly 15 years later.

From 2005 to 2009, Telstra was subject to various forms of political pressure to upgrade its network to the next generation of fixed residential broadband – Fibre to the Node (FTTN) using VDSL technology. The Howard and Rudd governments tried to cajole and push Telstra into a new investment program for FTTN. Meanwhile, Telstra's competitors played spoiling roles, presenting alternative upgrade options to government, but also looking for a windfall from government. However, Telstra under its American CEO, Sol Trujillo, in conflict with the Howard and Rudd Governments (advised along the way by the ACCC), was never able to come to an agreement that would satisfy the need for more investment in fast broadband while ensuring fair access to Telstra's infrastructure for its competitors (Fletcher, 2009).

Eventually, the Rudd Government, in the darkest hours of the 2007-8 Global Financial Crisis and willing to spend big on an economic stimulus program, launched the bold Fibre to the Premises (FTTP) version of the National Broadband Network (NBN), creating a new, wholly owned Government Business Enterprise (NBN Co Limited) at an anticipated cost of $A 43 billion, with the network to be completed by 2020. The newly created NBN Co would be a

http://doi.org/10.18080/ajtde.v6n4.162

stand-alone enterprise funded by government equity and private debt, operating as a wholesale only, open access broadband network (Rudd *et al.*, 2009).

The governance framework for NBN Co, with its own board of directors, mimicked the structure set up for Telstra back in 1989 by the Hawke Government and would have the political advantage of remaining out of the federal budget spotlight. The core reasons stated for the huge government intervention were: (i) Telstra, as a private monopoly, would not agree to upgrade its network on acceptable terms; (ii) separation of Telstra from its monopoly infrastructure networks could not be accomplished either legally (Australia has no judicial anti-trust mechanism), operationally (e.g. IT systems) or financially (compensation was deemed too high); and (iii) Australia was seen to be lagging the world in fixed broadband deployments and an FTTP build over a 10-year period would enable it at least to catch up, if not leap ahead, of its recognised OECD and regional peers.

However, Telstra still had to be convinced to fall into line with the new NBN policy and not become a competitor to the nascent NBN Co. To achieve this, the Rudd/Gillard Government used a carrot and stick approach. The carrot was a deal worth $ 11 billion, in net present value terms, over more than 30 years for Telstra to transfer its customers and lease its pits, ducts, exchanges and long-distance fibre to NBN Co. The stick was the threat of regulation for full functional separation (but not legal structural separation) of the Telstra copper network, along with divestiture of Telstra's HFC assets and Foxtel equity, and being excluded from the future 700 MHz spectrum auction. So, under either the deal or no-deal scenario, Telstra would effectively undergo a separation of its copper and HFC networks from its retail business. However, under the deal scenario, Telstra would be paid to lease its pits, ducts, exchange floor space and long-distance fibre to NBN Co and move its customers to the NBN, while, under the no-deal scenario, Telstra could keep it customers on its own network and force NBN to build its own infrastructure from the ground up. Effectively, both scenarios involved vertical and horizontal separation, at least at the functional level. Telstra's shareholders approved the NBN Co deal and the implicit vertical and horizontal structural separation of Telstra in October 2011 (Telstra, 2011). The ultimate goal of achieving Telstra structural separation had at long last been achieved some 8 years after it had been tentatively suggested and then withdrawn by the Labor side of politics (Havyatt, 2010). Telstra's fixed network would be both vertically and horizontally separated, with it retaining only its direct fibre connections to large enterprise customers.

However, the result was the creation of a new wholesale monopoly fixed infrastructure provider. Infrastructure competition was actively discouraged by legislation passed by the Gillard Government in 2011, with so-called "level playing field" or "anti-cherry picking" provisions introduced into the legislation to protect NBN Co's monopoly (Cth, 2010).

http://doi.org/10.18080/ajtde.v6n4.162

The Labor Rudd/Gillard Government NBN policy was controversial and far from bipartisan. In a time of turmoil for Australian politics in the form of the minority Labor Gillard Government, the federal opposition Coalition was keen to find an alternative to differentiate itself from Labor at the next election due in 2013. Despite its controversial nature, the Labor NBN policy was popular with the electorate and Malcolm Turnbull, the future Prime Minister, as Opposition Spokesperson for Communications, was keen not to be seen as an early "wrecker" of the NBN. The Coalition thus took to the 2013 election a watered-down NBN that would involve an FTTN architecture (rather than FTTP) with supposedly lower costs and faster rollout but still offering an improvement on the existing Telstra ADSL networks available to retail service providers (Coalition, 2013). The Coalition did not challenge the separation of Telstra or the creation of NBN Co as a new monopoly provider; rather, it chose to represent itself as a more responsible, economical and pragmatic owner of NBN Co to minimise the financial risks and impacts to the taxpayer.

After winning the 2013 and 2016 elections, the Coalition Abbott and Turnbull Governments proceeded to roll out a Multi Technology Mix (MTM) using FTTN, FTTB, FTTC and HFC technologies, as well as continuing Labor's use of terrestrial and satellite fixed radio technologies, after renegotiating the 2011 deal with Telstra. The rollout of the revised network was slower than originally promised by Turnbull with significantly higher costs (NBN Co, 2018) and has attracted a high level of complaints regarding its service performance and prices from both residential customers and retail service providers (ACMA, 2018). According to NBN Co's Corporate Plan released in August 2018, the peak funding had increased to $A 51 billion (NBN Co, 2018), significantly higher than the Coalition's election campaign plans and its initial projections made once in government.

On top of the cost increases and customer complaints, it is also now widely accepted that the investment in NBN Co by the Australian Government will not make a commercial return. While the August 2018 Corporate Plan is forecasting a return of 3.2% *per annum* on shareholder equity of $A 29 billion (the remaining funding to be a mixture of government and private debt), a report by Standard & Poors has forecast that a write-down of the investment is "inevitable" (AFR, 2018b).

Both Labor and Coalition Governments have sought to protect NBN Co financially by legislation and regulations that seek to dissuade competitors (who in many cases are NBN Co's own customers, such as Telstra, Optus, Vocus and TPG Telecom) from building new fibre-based networks that "cherry pick" NBN Co's more valuable customers. (McLaren, 2016).

The result has been that Telstra, Optus and TPG Telecom (after announcing a planned merger with Vodafone) are likely to invest heavily in 4G and 5G networks as alternatives to the NBN

http://doi.org/10.18080/ajtde.v6n4.162

for providing fixed broadband services to residential consumers. This wireless NBN bypass option is currently not restricted by regulation or legislation, but will require significant investment in spectrum, fibre and other facilities to be able to offer a compelling alternative to NBN Co (Asher, 2018).

At the end of 30 years of reform, Australia's telecommunications market has ended up a more-or-less bifurcated industry, involving, on the one hand, a competitive and innovative mobile industry and, on the other, a largely monopolistic and expensive fixed network industry dominated by NBN Co.

Lessons from the Last 30 Years

As in other markets where government telecommunication incumbents were privatised, the Australian government has had to grapple with the conflict of promoting competition to benefit consumers while maximising shareholder value to the taxpayer. In Australia, the Coalition right-leaning governments have favoured the latter, with an initial focus on maximising the sale proceeds of Telstra by minimising the competitive threats to Telstra through either vertical or horizontal structural separation of Telstra. During the NBN phase the Coalition's focus has been on reducing the cost of the rollout through maximising the re-use of Telstra's assets (copper and HFC networks) rather than investing in higher quality network infrastructure (i.e. FTTP). The Labor left-leaning governments have preferred to commit to larger amounts of taxpayer's money with the goal of increasing competition, albeit competition at the retail level only, and a monopoly wholesale infrastructure provider.

The current NBN outcome is in effect the realisation of the vertical structural separation of Telstra initially proposed, and then withdrawn, by Labor in 2003. The initial NBN FTTP architecture hoped to recover lost ground and propel Australia to the forefront of broadband networks globally. The Coalition saw this goal as extravagant and sought to wind back the costs to the minimal amount, although the costs have since increased to be higher than its own initial estimates and the initial Labor estimates for FTTP. The NBN political argument today boils down to whether the government should commit more taxpayer dollars now for a high-speed broadband future (Labor) or take incremental investment steps when the demand for high-speed broadband is obvious and most likely overdue (Coalition). Both parties have seemingly agreed on the vertical structural separation model for Telstra and the national wholesale NBN monopoly – a reform first proposed by Labor back in 2003. Investment in further fibre infrastructure is a political question that will depend on reconciling the benefit in faster broadband with the demands of Australia's fiscal budgetary position.

But, while this structural monopoly outcome is effectively bipartisan policy, it is becoming clear many of the problems of Telstra's original market dominance still remain and may be in

http://doi.org/10.18080/ajtde.v6n4.162

fact worsening. The structural separation of Telstra has just seen the problems transferred to NBN Co under a new monopoly. The primary reason for structural separation was a reduction in Telstra's dominance and a more vigorous retail market enabled by a "level playing field" for retailers. "The biggest winners should be customers who will be offered a better choice of providers" (Havyatt, 2010). This has not eventuated. Complaints by retailers and end customers regarding the quality of NBN Co's service delivery (ACMA, 2018) are strikingly similar, if not worse, than those made against Telstra when it was the monopoly fixed access service provider. Complaints by retailers of a "margin squeeze" (Computerworld, 2018) are reminiscent of those made against Telstra in 2004, discussed above, when the current chairman, Ziggy Switkowski, and a director, Justin Milne, of NBN Co were, respectively, CEO of Telstra and head of Telstra's BigPond ISP business.

Furthermore, rather than resulting in a "better choice of service providers", the structural separation of Telstra and creation of NBN Co have resulted in Telstra's retail market share increasing and an overall more concentrated fixed broadband market. Consolidation of the challenger ISPs Internode, Netspace and iiNet into the TPG Telecom group has led to 95% of the fixed broadband market being supplied by just 4 independent operators (Telstra – 51%, TPG Telecom - 22%, Optus – 17% and Vocus – 6%) in 2018 (ACCC, 2018, p. 21). This compares to 2009-10 when the top four providers supplied 75% of fixed broadband services (Telstra – 41%, Optus – 16%, iiNet – 10% and TPG Telecom – 8%) (ACCC, 2011, p. 10). The Herfindahl-Hirschman Index (a metric used to estimate the level of market concentration) has risen to 3500 in 2018 (ACCC, 2018, p. 21), compared to 2554 in 2010 (ACCC, 2011, p. 10), highlighting that consumers have significantly less choice now than before the creation of NBN Co.

NBN Co is facing a future threat from wireless broadband that will undermine its business case while regional customers are demanding more investment to improve service quality. The NBN technology debate (i.e. FTTP vs MTM) is not the root cause of these issues – the real issue is the wholesale monopoly business model. The artificial, regulatory enforced, split between wholesale and retail at Layer 2 of the OSI model (also referred to as "bitstream" access) creates significant duplication and confusion regarding responsibilities for network performance between wholesaler and retailer. Retailers have very little incentive to compete on the quality of the service provided to retail customers. Retailers have been successful in shifting the "blame" to NBN Co for service quality that is effectively under their control (e.g. Connectivity Virtual Circuit (CVC) dimensioning). NBN Co, in order to protect its brand, is responding by offering plans that take CVC dimensioning away from the RSP (i.e. a fixed allocation of CVC per Access Virtual Circuit), thus making it impossible for RSPs to compete on quality. The end result is that NBN Co is effectively defining the retail product offering from

http://doi.org/10.18080/ajtde.v6n4.162

its wholesale position, leaving customers minimal choice in the normal trade-off between quality and price.

Disputes between NBN Co and its wholesale customers over pricing, products and operational performance will continue in much the same way as the industry complained about Telstra's wholesale performance during the 2000s. End customers will continue to face confusion and frustration as both NBN Co and retail service providers deflect blame over faults and provisioning foul-ups to each other. Investment in infrastructure will be limited unless political pressure can be brought to bear on NBN Co to respond to local community issues.

A more fundamental consequence of the structural monopoly is the inherent disincentive monopolies have to invest to expand supply. This stems from the well-understood profit maximising condition of monopoly firms. Monopolies, as the sole supplier of a product, maximise profits by restricting supply and selling at a price significantly above their marginal cost. This compares to a competitive market where price is more or less the same as marginal cost (Hubbard & O'Brien, 2017, chapter 15). This leads to the excessive returns or so-called "rents" that monopolies earn to the detriment of consumers and the need for price regulation. Price regulation can be successful in stable markets where demand is not changing. However, in markets where demand is increasing (e.g. demand for bandwidth in telecommunications markets as technology evolves), monopolies can simply restrict investment to restrict supply relative to the increasing demand. Regulators are not able to force monopolies to invest to increase supply and meet demand, so price regulation is insufficient to avoid effective increases in price relative to the prices a competitive market would deliver. This explains Telstra's reluctance to invest in fixed broadband when it was the monopoly infrastructure provider. The same applies now for NBN Co. Investment will not occur for commercial reasons, instead it will be solely driven by political or other non-economic drivers.

The wholesale monopoly market model pursued in Australia has not been adopted in most other markets globally. Only New Zealand and the United Kingdom have followed a similar model using a Layer 2 broadband wholesale product. Singapore has elements of the Australian model but the retail service providers are able to obtain direct fibre access in most cases and hence act more like vertically integrated operators rather than having the wholesale/retail split at Layer 2.

Telecom New Zealand underwent vertical structural separation through the demerger of its fixed telecommunications assets into a new separate company, Chorus, in 2011. The demerger was necessary to allow Chorus to participate in the New Zealand government's Ultra Fast Broadband (UFB) FTTP initiative. The New Zealand government started this initiative by entering into agreements for the rollout of wholesale-only networks with three electricity

http://doi.org/10.18080/ajtde.v6n4.162

distribution companies, which collectively covered approximately 30% of the planned UFB network. Chorus, after its demerger from Telecom New Zealand, was awarded the remaining 70% of the UFB network. Competition clearly forced Telecom New Zealand to restructure and Chorus to come to terms with the government to be able to participate in the UFB (Crown Fibre Holdings, 2018) or face loss of its entire fixed network monopoly. This was New Zealand's own version of the carrot and stick approach used in Australia to induce Telstra to voluntarily separate its fixed access network.

In the United Kingdom, British Telecom underwent functional separation into wholesale and retail units in 2006 based on undertakings given to Ofcom, the UK telecommunications regulator. However, without any government funding as in New Zealand, the wholesale company Openreach's investment in new fibre infrastructure has been limited to FTTN and found to be lagging the rest of the world (Sidak & Vassallo, 2015). The UK government, eager to see more FTTP investment, is pursuing further reform and Ofcom has put in place new regulations requiring Openreach to share ducts and poles for fibre access to enable infrastructure competition to drive further fibre investment (Ofcom, 2017).

A big issue for Australia's NBN after the completion of its rollout under the Coalition's MTM architecture is that the split into wholesale and retail networks does not, of itself, encourage sustainable long-term further investment in fibre buildouts in residential networks. In New Zealand, government grants led to investment in FTTP, but in the United Kingdom and Australia, without extra funding, there is no pathway to FTTP. As described above, the wholesale company, as a monopoly, is encouraged to restrict rather than grow supply of bandwidth from a purely commercial perspective.

The argument for a wholesale monopoly fixed network largely relies on the proposition that fixed telecommunications is a natural monopoly in much the same way that electricity, water, and sewage networks are natural monopolies. Natural monopolies are defined by large economies of scale that have constantly reducing costs per quantity of the product or service supplied. The fixed access telephony network was once such a natural monopoly (Davidson, 1982) and unfortunately this is an anchor that continues to weigh down the characterisation of fixed telecommunication networks as natural monopolies.

The digital computing and information revolution has fundamentally changed the monopoly characteristics of the fixed telephony network. This revolution has created new technologies that increase the demand for bandwidth and the means to supply such bandwidth. On the demand side, there is a huge wealth of information that is now digitised and available on demand over the internet, with the transition to online video being the most obvious and largest driver. This new wealth of information drives demand for more bandwidth. There are

http://doi.org/10.18080/ajtde.v6n4.162

many competing technologies on the supply side – e.g. DSL, G-Fast, GPON, DOCSIS, 3G, 4G, 5G. Wireless technologies not only increase the supply but also the locations where bandwidth can be consumed. The end result is that the copper fixed line telecommunication networks are no longer natural monopolies – their costs per unit of bandwidth are increasing rather than decreasing as more bandwidth is being consumed. But new entrants can build and operate networks using new technologies that can deliver the higher quantities of bandwidth demanded at cheaper per unit costs than the old copper monopoly network. The end result is competition can and does drive network investment to satisfy the higher demands being placed on the networks and new entrants can do this more efficiently than the incumbent network. The incumbent, seeing this as a threat, will invest as well, sometimes in a timely manner and hence head off the competitor or sometimes too late in which case the competitor will survive and become a viable longer-term player.

That broadband networks are not everywhere natural monopolies has been economically postulated since the very early days of broadband (Faulhaber & Hogendorn, 2000). Empirical research supports the view that access regulation of monopolies discourages investment in broadband networks and hinders infrastructure competition (Grajek & Roeller, 2012). Furthermore, separate empirical research highlights a positive correlation between infrastructure competition policies and broadband penetration (Bouckaert *et al.*, 2010). This same research, published during the critical period when the Labor NBN policy was being first bedded down, showed that markets relying on retail competition (what the research referred to as service based intra-platform competition) had a negative correlation with broadband penetration (i.e. the NBN model). A third model of facilities-based intra-platform competition, analogous to Australia's experience with the unbundled local loop and DSL investment by the service provider, had an insignificant effect on broadband penetration

The European Union identified the prospects for infrastructure competition between cable TV and telecommunications companies in 1998 when it advised regulators of the dangers of incumbent telecommunications operators owning cable TV networks (EU, 1998, para 7). The German and Portuguese markets were examples where regulators took active steps to force the incumbent monopoly to divest itself of its HFC cable businesses during the early and mid-2000s.

Australia's reluctance to embrace infrastructure competition and ongoing acceptance that fixed telecommunications is still a natural monopoly stems largely from the Telstra-Optus cable TV wars of the 1990s described above. The financial losses incurred by both companies are said to show that the market cannot support two competitors. This view only looks at the issue from a shareholder perspective and does not consider the consumer benefits. Despite the initial losses, the two networks have remained in operation with their revenues presumably

http://doi.org/10.18080/ajtde.v6n4.162

exceeding their operational and incremental capital costs. It is only under the NBN Co monopoly that the networks have come under consideration of being decommissioned, although the Telstra network is planned to be used by NBN Co. Hundreds of thousands of consumers have benefited from the higher speed broadband available on these networks. This consumer benefit far outweighs the original losses, which have been reduced by subsequent positive cashflows to both companies from these networks. In fact, David Thodey, a former CEO of Telstra, described its Foxtel investment as "the best thing we've ever done" (AFR, 2012).

Far from being proof of the natural monopoly, the Telstra-Optus cable TV wars highlight why infrastructure competition should continue to be pursued to the benefit of consumers. The horizontal, rather than vertical, separation of Telstra, as advised by the ACCC in 2003, would have fundamentally changed Australia's fixed telecommunications trajectory.

In summary, the main lessons that should be taken from the last 30 years of Australia's fixed telecommunications market development are:

1. Fixed telecommunications is no longer a natural monopoly (as it was under the century-old telephony service model until the 1980s) due to major advances in the technologies in the digital era.
2. The information economy has created a large increase in the demand for bandwidth but a monopoly provider has limited economic incentives to invest to create more supply, since profit maximisation occurs at lower supply levels than in a competitive market.
3. The structural separation of Telstra and creation of a wholesale-only NBN Co has not resulted in more aggressive retail competition, rather the intensity and scope of retail competition has reduced with a focus on price rather than quality.

To finish this section, I would like to present a hypothetical counter-factual scenario of what could have been achieved if Telstra had been forced to divest its HFC network in 2003:

1. Telstra would have sold the HFC network and its 50% stake in Foxtel to News Corporation.
2. Telstra would have commenced the build of an FTTN network in the mid-2000s and become a content aggregator using IPTV technologies to compete with Foxtel.
3. Foxtel would have launched DOCSIS 3 – 100 Mbps services in the late 2000s.
4. Telstra would have commenced upgrades from FTTN to FTTP in the early 2010s.
5. Foxtel would have increased its HFC footprint to grow its broadband market share.
6. Optus, AAPT, TPG Telecom would have still been successful in retail market on the back of Telstra's wholesale and unbundled local loop products.

http://doi.org/10.18080/ajtde.v6n4.162

7. Australian Government would have focussed government funding on regional and remote communications where competition did not encourage investment by the private sector.

The above scenario has occurred in many markets where cable TV and traditional incumbent operators have been in competition. The closest comparison to Australia is Canada where Bell Canada is now rolling out FTTP networks to compete with DOCSIS networks supplied by Rogers and Shaw Communications.

However, instead of the above, Australia's fixed telecommunications market faces similar conundrums as in 1988 when Telecom Australia was Australia's monopoly telco Government Business Enterprise, pondering how it will survive in the future as the new digital technologies unleash a range of innovation that will likely disrupt it in many unpredictable ways. The current market only has the veneer of competition as four retailers spar with NBN Co, which largely sets the parameters that determine the quality and pricing received by the end user. NBN Co, the new Telecom Australia, is restricted by politics and its wholesale remit confronts a future where its own wholesale customers can use new 5G wireless technologies to cherry pick and disrupt its business model.

Australia's Bush Telecommunications Problem

Australia's unique geographic circumstances are often raised as the reason why the fixed telecommunication market is so hard to fix. Despite Australia being one of the most urbanised populations in the OECD, the large land mass and remote populations do make provision of telecommunication services to the "outback" or "bush" costly and largely uneconomic without a subsidy of some kind.

Prior to its privatisation and deregulation, Telecom Australia was charged with managing this problem and effectively absorbing the losses in regional areas by making higher profits in urban areas – that is, via a hidden internal cross subsidy. After deregulation in the 1990s, attempts were made to expose this cross subsidy via the Universal Service Obligation (USO) levy system that applied to all operators to compensate Telstra for its losses. The funding arrangements became controversial and politicised during the period when the Howard Government was seeking full privatisation of Telstra (Fletcher, 2015). Disputes over the quantum of the subsidy led the Howard Government to simply impose a cap on the total levy. As a result, Telstra had no commercial incentive to improve regional telecommunication services and, after many regional telecommunication enquiries, there were still high levels of complaints regarding the quality of service provision in regional Australia (Coutts, 2015).

http://doi.org/10.18080/ajtde.v6n4.162

Competition can only work to drive investment in geographic areas where density is high enough to sustain more than one operator. It cannot work where telecommunications is fundamentally uneconomic or where the revenue can only support investment and operations by one operator. Hence, a subsidy arrangement of some kind is necessary to create conditions for improved telecommunications in regional and remote areas.

However, the NBN model, with its commitment to universal wholesale pricing, has simply reverted back to the old Telecom Australia model prior to the introduction of competition. There is no commercial incentive for improving Australia's regional telecommunications after the initial fixed wireless and satellite services are put in place. Regional communities must rely on raising the profile of their complaints about service levels in order to get attention and funding via publicity of these issues, as evidenced by the recent demands for upgrades to the NBN fixed wireless network (iTnews, 2018a).

A Regional Broadband Service levy has been proposed to require fixed competitors to NBN Co to contribute to some of the cross-subsidy provided by NBN Co. The proposed levy amounts to approximately 10% of the retail broadband price of $70 per month; however, because of its narrow incidence, it will raise little actual revenue ($40 million in first year) (Computerworld, 2016). Its main affect is thus to suppress competition rather than assist funding of NBN Co with its regional USO obligations.

To be effective, a levy must be broadly applied and raise substantial funds at minimal impact to competition in the industry. A 2.5% levy on the entire telecommunications industry's retail revenue (mobile and fixed) would raise approximately $1.0 billion per annum. These funds could be used to establish a regional telecommunications investment fund that is dedicated to the uneconomic parts of the Australian telecommunications industry (mobile and fixed), addressing the problems on a sustainable basis into the future. A publicly accountable and ring-fenced fund that was dedicated to improving the telecommunication services in uneconomic areas could de-politicise the issue of regional telecommunications. The funding could also be competitively disbursed in ways that promote efficient investments and operations to ensure all remote and rural Australians benefit, rather than just those in marginal electorates.

NBN Reform Options

This paper has focussed on the mistakes made during the 30 years of reform of the Australian fixed telecommunications market. The big question is: can policy makers learn from these mistakes and create a framework for investment and improved performance of this market?

http://doi.org/10.18080/ajtde.v6n4.162

As described, NBN Co is facing many challenges that will need significant changes to address them. The most pressing are as follows:

1. Revenue shortfalls due to missed forecasts of ARPU (average revenue per user) are likely to mean negative cashflows will continue indefinitely.
2. Competition from 4G and 5G wireless networks is likely to lead to customer losses and more capital expenditure to differentiate service offerings and retain customers.
3. Regional services will need to be upgraded as capacity limitations in fixed wireless and satellite continue.

The current NBN Corporate Plan assumes positive cashflows of $0.1 billion in FY22 (NBN Co, 2018). However, a more realistic scenario would assume that ARPU does not increase further (i.e. remains at $44 per month), loss of 10% of customers to 5G along with $0.3 billion extra of capex for regional networks: then, the FY22 negative cashflow is $1.5 billion per annum. This may improve after the final Subscriber Payments are made to Telstra and Optus but is likely to still involve losses of approximately $1.0 billion per annum. A write-down of the government's investment, as canvassed by Standard & Poors (see above), is in line with these more realistic financial metrics for NBN Co. Labor's Opposition Spokesperson on Communications, Michelle Rowland, has publicly stated that Labor is "keeping its options open" in respect of a write-down and "there is no way NBN Co is going to meets its average revenue per user forecast" (The Australian, 2018).

However, a write-down is also likely to trigger calls for NBN Co to lower its wholesale prices below current levels. The linkage between lower NBN Co prices and a write-down has been made by both industry participant and regulators. Bevan Slattery, founder of Pipe Networks, Superloop, NextDC and Megaport, has consistently called for a write-down in order to reduce NBN Co's wholesale prices (Slattery, 2018; AFR, 2017a). In its draft report for its Communications Sector Market Study, the ACCC called on the government to consider debt relief, asset revaluation and direct budget financing in order to allow NBN Co to lower its prices (ACCC, 2017, p. 133; AFR, 2017b). Telstra, Optus, Vocus, Macquarie Communications and Regional Development Australia (NT) all supported the ACCC's draft recommendation, although push-back from the Department of Communications resulted in the ACCC publishing a "slightly toned down" recommendation (AFR, 2018b; ACCC, 2018, p. 103-104) in its final report. Telstra's CEO, Andy Penn, has compared NBN Co's ARPU of $44 per month to the charges the ACCC has approved for Telstra's wholesale prices of approximately $20 per month. He has called for a reduction of more than $20 per month in NBN Co's charges (iTnews, 2018b).

http://doi.org/10.18080/ajtde.v6n4.162

From a financial perspective, a fall in NBN Co's ARPU of $1 equates to an approximately $100 million per annum fall in cash-flows in FY22 (Sydney Morning Herald, 2018). Hence, a reduction in NBN Co's ARPU of $10 per month (or half of the reduction called for by Telstra's CEO) would result in a further reduction of $1.0 billion per annum in NBN Co's cashflows.

A summary of the impacts described above on NBN Co's financials is presented in the following table.

Table 1: NBN Co Financials in FY2022

	FY19 Corp Plan	Realistic Scenario	Decrease in ARPU of $10 Scenario
Revenue	$ 5.6	$ 4.3	$ 3.3
Operating Expenditure	$ (2.7)	$ (2.7)	$ (2.7)
Subscriber Payments	$ (0.4)	$ (0.4)	$ (0.4)
Capital Expenditure	$ (1.2)	$ (1.5)	$ (1.5)
Interest & Working Capital	$ (1.2)	$ (1.2)	$ (1.2)
Cashflow	$ 0.1	$ (1.5)	$ (2.5)

While the focus of much of the NBN Co financial debate has been on the possibility of a write-down of the government's investment in NBN Co, a bigger concern going forward will be the weakness of its underlying cashflows, which are linked with its ARPU and take-up projections. If these projections are not realised, then NBN Co will need to cut operational and capital expenditure in addition to making purely financial adjustments. Any such reductions are likely to have significant impacts on the quality of the service provided and the investment in new technologies and deeper fibre deployments.

This financial reality will be a big factor in determining the next possible steps for NBN Co.

Gregory has outlined four possible options for reform of NBN Co as it approaches the end of its build in 2020 (Gregory, 2018). I will consider each of these options in turn.

Option A: NBN Co not sold off

Under this scenario NBN Co would continue to operate as a wholly owned Government Business Enterprise.

As discussed above, NBN Co will most likely be operating with negative cashflow and require regular government equity and/or debt to be able to continue operating. A write-down of the government's equity to less than $20 billion is likely – producing a one-off hit to the budget bottom line of approximately $30 billion. Cuts in operational expenditure will be drastically needed to avoid the need for further government funding just to keep NBN Co operating.

http://doi.org/10.18080/ajtde.v6n4.162

Further investment in new fibre infrastructure will be politically contested and subject to the fiscal constraints of the Australian Government. If the government does provide funding, it will need to be as a grant and not as an equity investment (i.e. on budget). However, fibre investment will be vital to resist competition from wireless broadband operators in key urban markets.

While NBN Co has provided mobile backhaul services in regional "mobile blackspot" areas (iTnews, 2017b), additional investment in metropolitan fibre to assist mobile operators with fibre infrastructure for 5G build-outs will raise large conflicts within NBN Co, as such investments will actually increase competition at the residential customer level. For every extra revenue dollar NBN Co gains from servicing mobile operators with 5G, it runs a significant risk of cannibalising more of its wholesale fixed access revenues. As a result, any such mobile backhaul service arrangements are likely to require substantial co-investment from mobile operators who will require exclusivity for such infrastructure. Such arrangements will be difficult to construct to avoid contradicting NBN Co's non-discrimination obligations. A mixture of policy, commercial and competitive tensions will likely mean this path will remain in the "too-hard basket" as it has been for NBN Co in its existing deliberations about providing mobile backhaul to the mobile operators in metropolitan areas.

The ability for NBN Co to invest in uneconomic areas will be heavily constrained by its weak financial position. Its ability to cross-subsidise the costs of regional telecommunications by charging higher fees in urban areas will come under pressure, given its likely ongoing financial challenges.

In short, this option is only viable if the Federal Government is prepared to commit ongoing regular funding contributions to improve NBN Co's competitive position and sustain its operational capability. After a decade of funding NBN Co, it will be difficult for any political party to request taxpayers to continue to pour money into NBN Co with no prospect of any return. Higher pricing will be both politically untenable and likely to lead to greater loss of end users to the wireless broadband market.

In the unlikely event that NBN Co is able to reach a position of positive free cashflow, then, if directed by its Minister shareholders, it could use all profits to invest in upgrading its network. These upgrades are unlikely to result in significant increases in revenues, as retailers will continue to compete on price rather than innovative and/or higher quality services as has already been seen to date given the limited retail competition.

As a result, whether NBN Co is financially viable or not, upgrades to the network will be political rather than commercial decisions. Given the normal changes of political cycles and Australian governments and the manner in which politicisation of telecommunications and

http://doi.org/10.18080/ajtde.v6n4.162

broadband has led to the current predicament, this future path is fraught with likely disappointment.

Option B: Sold off as a single entity

Private ownership in and of itself does not change the financial conditions faced by NBN Co. Regardless of the price paid, NBN Co will still have similar revenues and overall cashflows as under government ownership, with the changes likely to be mainly at the operational expenditure line as the new owner seeks to operate as a leaner, fitter outfit. This will have consequences for service quality. This option assumes that the sale would not change the regulatory settings under which NBN Co must offer uniform wholesale pricing supervised by the ACCC, and that any of the current retail service providers are not able to acquire NBN Co and seek to exploit synergies with their retail operations. Any relaxation of these rules would simply move NBN Co closer to the complaints made against the Telstra model that were the original reason for pushing structural separation of Telstra and the creation of NBN Co.

A new private owner would have only one reason to invest on its own account in more fibre infrastructure, namely to make profits by retaining revenues against competition from other operators (fixed or mobile). Some investment may be possible in partnership with mobile operators in the private ownership model, if NBN Co can strike innovative deals to share some of the revenue with the mobile operators. However, NBN Co's non-discrimination obligations would need to be relaxed considerably to enable this approach to proceed.

In essence, this path is similar to the privatisation of Telstra in the 1990s and 2000s, which, combined with its market dominance and resulting monopoly position, clearly hindered investment in the fixed broadband infrastructure market rather than the opposite.

In short, this pathway creates some opportunities for lower operational expenditure but will set up a rerun of long-lasting regulatory and policy battles that occurred during the Telstra privatisation period. Private owners will seek to remove regulation over pricing and seek to dismantle existing non-discrimination and other regulatory safeguards to find new ways to grow profitability. Investment in more fibre may occur in some areas where the economics are favourable and competition demands it to retain market share, but otherwise government funding will be necessary to push more investment.

Australia's regional telecommunications market will continue to suffer, as it has for many years, as the new private owners seek to minimise costs where there is no prospect of profits or returns.

http://doi.org/10.18080/ajtde.v6n4.162

Option C: Disaggregated technology footprints sold off separately

This model has been recommended by the Government's Panel of Experts (Vertigan, 2014) and also endorsed by the ACCC "to provide a market structure that will facilitate greater infrastructure-based competition" (ACCC, 2018, p. 5). Despite these recommendations, there has been little discussion on how this model would work in practice.

An essential element of this model would be the need to create competitive tension between companies responsible for the different technology footprints. Currently, NBN Co's technology planning assigns premises to the different technologies in a way to minimise the capital cost but still meet its Statement of Expectation goals. Under the FTTP model, this was largely pre-ordained, with FTTP going to the least expensive 93% of premises and with Fixed Wireless and Satellite to cover the rest.

Under the Multi-Technology Model, there are now options for FTTN, FTTB, FTTC (i.e. FTTx), HFC and even Fixed Wireless within the previous FTTP footprint. The FTTx options are largely dependent on copper loop lengths and the presence of multi-dwelling units. The HFC is restricted to existing Telstra HFC network coverage.

An important fact is that the Telstra HFC network is not uniform in its coverage of approximately three million homes within the more affluent suburbs of Melbourne, Sydney, Adelaide and Brisbane.-HFC is a residential service that avoided many multi-dwelling units, due to building access issues, as well as commercial business areas for which HFC was technically not suitable. As a result, the FTTx options are mostly being used to fill these "holes". It also means that the FTTx services can be easily expanded into the HFC areas by connections to the relevant copper cables that also existing in parallel with HFC to all premises.

Furthermore, NBN Co's Fixed Wireless network covers many of the outer suburban areas of Australia's metropolitan and regional cities using both 2.3 and 3.5 GHz spectrum. This coverage naturally also extends into the FTTx coverage areas. With capacity upgrades, the Fixed Wireless can compete with the FTTx coverage areas. Even the Satellite service will have spare capacity in some beams, which could be used to service customers in some larger regional towns that may currently be assigned to the FTTx technologies.

As a result, there is significant overlap between the HFC, FTTx and Fixed Wireless technology footprints that can be used as a starting point for creating competitive tension.

The end game would be to have separate ownership of firstly HFC, secondly FTTx (i.e. FTTP, FTTN, FTTB and FTTC) and a third entity owning access using Fixed Wireless and Satellite links together. I will refer to these three companies as NBN_HFC, NBN_FTTx and NBN_Wireless for simplicity.

http://doi.org/10.18080/ajtde.v6n4.162

The transition to this end game would need to be gradual to maintain operations and reduce disruptions. NBN Co could be split operationally into these three groups before the end of the build and without changing ownership structures before a Productivity Commission inquiry, both of which are currently required under existing NBN legislation (Cth, 2010). An NBN_Core operating entity could be set up to manage the Transit network and IT systems and hold the key relationships with Telstra for infrastructure leasing purposes. The key requirement is that each operating entity would start planning and augmenting its network separately and engaging separately with retail service providers.

After the build is finished and a Productivity Commission inquiry is held, these entities could commence taking private equity investment, which would involve legal separation of these entities. Ownership restrictions would need to be put in place to ensure no one company can take control of multiple entities. Subject to recommendations of the Productivity Commission and the ACCC, retail service providers would be able to invest in these entities as long as competition issues were also addressed.

Telstra's proposed InfraCo (Telstra, 2018) may have a role and could be merged with NBN_Core in a way that enabled open access to ducts and exchanges for the NBN operating entities and also for mobile operators looking to expand their fibre networks. Regulatory oversight would still be necessary to ensure equal and fair access to duct and exchanges for the NBN operating entities and new entrants. The transition would be gradual and managed with oversight and direction from policy makers and competition regulators.

Financially, the NBN entities as stand-alone operations should be encouraged to compete and stand on their own without government support. Private investment should be used to raise funds for network expansion. NBN_Wireless would need access to the regional telecommunications fund described above to subsidise its business for the uneconomic areas it is required to serve. NBN_FTTx may also need access to these funds to improve its service in areas where it lacks economic reasons to invest.

A further option may be to break NBN_FTTx into separate geographic entities to make sure this company is not too large and able to dominate the other companies, like Telstra has done in the past. An NBN_FTTx_South (covering Victoria, Tasmania, South Australia and Western Australia) and NBN_FTTx_North (New South Wales and Queensland) may be necessary to cover this eventuality.

The valuation of new equity provided by the private sector would need to be realistic and should follow a competitive bidding process wherever possible to ensure valuations are reasonable. In the early stages, it would be expected that investors would receive better valuations given the risks involved. Government's shareholding in the entities would reduce

http://doi.org/10.18080/ajtde.v6n4.162

as new equity is raised. Eventually, once the business model is proven and risks are reduced, the entities can either be listed or sold in ways that can eliminate the government shareholding altogether.

Option D: Disaggregated technology footprints (excluding satellite and fixed wireless) sold off separately

This option is essentially the same as Option C with government retaining full ownership of NBN_Wireless.

This option may be preferable to Option C given the need for ongoing annual subsidies to sustain the uneconomic operations and ongoing investments for these technology footprints. The Government would need to manage the ongoing industry levy and distribution under Option C and it may be more efficient and have greater accountability if this is continued to be held in a Government Business Enterprise. This will reduce the risk that NBN_Wireless diverts funds received from the universal service fund for use in areas where competition, rather than subsidies, should drive investment. Taxpayers may also be more comfortable having the levy-funded entity responsible via normal government expenditure scrutiny processes such as parliamentary committees and enquiries.

However, this entity should be able to compete for business, wherever possible and sustainable, to supplement its revenues and thus reduce the burden on taxpayers and the industry from the levy.

Conclusion

The Australian fixed telecommunications market has suffered through 30 years of reform that have involved significant policy mistakes and the politicisation of Telstra's privatisation and the investment needed for Australia's telecommunications infrastructure. The end result is that Australia's fixed telecommunications is in a very similar position to what it was in the 1980s at the beginning of the reform process, with a government-owned monopoly attempting to survive as consumer demands grow and new technologies are deployed by competitors.

Only a thorough reform of NBN Co can address the issues and increase infrastructure competition as the driver of investment and improving customer outcomes. A sustainably financed regional telecommunications fund is also needed to ensure all Australians have access to the necessary services and infrastructure to participate in the 21st century's network economy.

In the past, politicians and policy makers have made short-term decisions that have given preference to shareholders over consumers and resulted in taxpayers being required to support investments in metropolitan areas that could otherwise be financed by private

http://doi.org/10.18080/ajtde.v6n4.162

investment and driven by infrastructure competition. Politicians and policy makers need to recognise these mistakes and make long-term decisions that benefit consumers rather than shareholders, by bringing infrastructure competition to be the driving force for new fibre investments and by reserving government taxpayer funding for those regional areas where it is fundamentally uneconomic for infrastructure competition to be the driver of investment.

References

Alston, R. 2003. *Ministerial Press Release 20 June 2003 – ACCC Report on Pay TV Competition*. Retrieved from https://web.archive.org/web/20030623224903/http://www.dcita.gov.au:80/Article/0,,0_1-2_15-4_115441,00.html

Asher, A. 2018. *NBN faces irrelevance in cities as competitors build faster, cheaper alternatives*, 28 February. Retrieved from https://theconversation.com/nbn-faces-irrelevance-in-cities-as-competitors-build-faster-cheaper-alternatives-92275

Australian Competition and Consumer Commission. 2003. *Emerging Market Structures in the communications sector*. Australian Competition and Consumer Commission. June 2003. Retrieved from https://www.accc.gov.au/system/files/Emerging%20market%20structures%20in%20the%20communications%20sector.pdf

Australian Competition and Consumer Commission. 2004. 'Telecommunication competitive safeguards for 2002-03 financial year'. *ACCC Telecommunication Reports* 2002-03. Retrieved from https://www.accc.gov.au/system/files/ACCC%20Telecommunications%20reports%202002-03.pdf

Australian Competition and Consumer Commission. 2011. *ACCC telecommunications reports 2009-10*. Retrieved from https://www.accc.gov.au/system/files/ACCC%20Telecommunications%20reports%202009-10.pdf

Australian Competition and Consumer Commission. 2017. *Communications Market Sector Study – Draft Report – October 2017*. Retrieved from https://www.accc.gov.au/system/files/Communications%2520Sector%2520Market%2520Study%2520Draft%2520Report.pdf

Australian Competition and Consumer Commission. 2018. *Communications Market Sector – Final Report – 5 April 2018*. Retrieved from https://www.accc.gov.au/publications/communications-sector-market-study-final-report

Australian Communications and Media Authority. 2018. *NBN consumer experience. Households and businesses – the end-to-end journey*. August 2018. Retrieved from

http://doi.org/10.18080/ajtde.v6n4.162

https://www.acma.gov.au/-/media/Research-and-Analysis/Research/pdf/NBN-consumer-experience_households-and-businesses.pdf

Australian Financial Review. 2012. *Telstra media plays in ACCC's sites*, 12 April. Retrieved from http://www.mclarenwilliams.com.au/wp-content/uploads/2014/11/Telstra-media-plays-in-ACCC%E2%80%99s-sights.pdf

Australian Financial Review. 2017a. *Government rejects calls to write-down $30b investment as Bevan Slattery predicts mobile advances*, 17 April. Retrieved from https://www.afr.com/technology/web/nbn/government-rejects-calls-to-write-down-30b-nbn-investment-as-bevan-slattery-predicts-mobile-advances-20170412-gvjl5a

Australian Financial Review. 2017b. *ACCC questions NBN business model* 30 October. Retrieved from https://www.afr.com/technology/accc-questions-nbn-business-model-20171030-gzaytr

Australian Financial Review. 2018a. *ACCC recommends breaking up NBN before privatisation*, 5 April. Retrieved from https://www.afr.com/business/telecommunications/accc-recommends-breaking-up-nbn-before-privatisation-20180405-h0yd9f

Australian Financial Review. 2018b. *NBN write-down 'inevitable': Damning S&P report*, 25 July. Retrieved from https://www.afr.com/technology/web/nbn/sp-nbn-20180724-h132tf

Australian Government. 1988. *Cabinet Submission 5742 – Telecommunications regulation – Decisions 11067/SA, 11070/SA(Amended) and 11188*. National Archives of Australia A14039, 5742. Retrieved from https://recordsearch.naa.gov.au/SearchNRetrieve/NAAMedia/ShowImage.aspx?B=31429583&T=PDF

Bouckaert, J; van Dijk, T; Verboven, F. 2010. 'Access Regulation, competition, and broadband penetration: An international study'. *Telecommunications Policy,* Vol. 34, Issue 11, pp. 661-671. Retrieved from https://doi.org/10.1016/j.telpol.2010.09.001

Cave, M. 2004. 'Remedies for Broadband Services'. *Competition and Regulation in Network Industries*, Vol. 5, Issue 1, pp. 23-49.

Coalition of the Liberal and National Parties. 2013. *The Coalition's Plan for Fast Broadband and An Affordable NBN - April 2013*. Retrieved from https://www.communications.gov.au/file/315/download?token=8OjaNaNc

Commonwealth of Australia. 2002a. Parliamentary Debates, House of Representatives. 12 February 2002. Vol 1., p. 22. Retrieved from https://www.aph.gov.au/binaries/hansard/reps/dailys/dr120202.pdf

Commonwealth of Australia. 2002b. *Connecting Regional Australia*. Department of Communications, Information Technology and the Arts. Retrieved from http://pandora.nla.gov.au/pan/37886/20031218-0000/www.telinquiry.gov.au/rti-report/rti%20report%20text%20f-a%2018.pdf

Commonwealth of Australia. 2010. *Explanatory Memorandum – National Broadband Network Companies Bill 2010, Telecommunications Legislation Amendment (National Broadband Network Measures – Access Arrangements) Bill 2010*. Retrieved from http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r4495_ems_b1f1627d-69f3-40d8-80e0-abfe11389b91/upload_pdf/349799.pdf;fileType=application%2Fpdf

Computerworld. 2016. *Broadband levy to subsidise regional NBN services*, 12 December. Retrieved from https://www.computerworld.com.au/article/611443/broadband-levy-subsidise-regional-nbn-services/

Computerworld. 2018. *Telstra CEO attacks 'unsustainable' NBN pricing*, 9 April. Retrieved from *https://www.computerworld.com.au/article/635877/telstra-ceo-attacks-unsustainable-nbn-pricing/*

Coutts, R. 2015. 'Better telecommunications services for all Australians – Further Thoughts on the Universal Service Obligation'. *Australian Journal of Telecommunications and the Digital Economy*, Vol. 3, No. 4, pp. 89-107.

Crown Fibre Holdings. 2018. Retrieved from https://www.crowninfrastructure.govt.nz/about/

Davidson, J. 1982. *Report of the Committee of Inquiry into telecommunications services in Australia* [known as the Davidson Inquiry], AGPS Canberra 1982, 3 vols.

European Union. 1998. European Union Directive 98/C 71/04, 'Commission communication concerning the review under competition rules of the joint provision of telecommunications and cable TV networks by a single operator and the abolition of restrictions on the provider of cable TV capacity over telecommunications networks'. *Official Journal of the European Communities*, C 071. 7 March 1998, pp. 0004-0017. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31998Y0307(01)&from=EN

Faulhaber, GR; Hogendorn, C. 2000. 'The Market Structure of Broadband Telecommunications'. *Journal of Industrial Economics*, Vol. 48, No. 3, pp. 305-329.

Fletcher, P. 2009. *Wired brown land: Telstra's battle for broadband*. Sydney: UNSW Press

Fletcher, P. 2015. *Speech to the ACCAN USO Forum*. Retrieved from https://www.paulfletcher.com.au/portfolio-speeches/speech-to-the-accan-uso-forum

http://doi.org/10.18080/ajtde.v6n4.162

Gerrand, P. 2004. 'Revisiting the Structural Separation of Telstra', *Telecommunications Journal of Australia*, Vol. 54, No.3, 2004, pp.15-28; republished online as an attachment in Gerrand (2017).

Gerrand, P. 2017. 'Historical paper: The 2004 Proposal for the Structural Separation of Telstra', *Australian Journal of Telecommunications and the Digital Economy*, 5(4), December 2017, at https://doi.org/https://doi.org/10.18080/ajtde.v5n4.134

Gregory, M. 2018. 'Australian Wholesale Telecommunications Reforms'. *Australian Journal of Telecommunications and the Digital Economy*, Vol. 6, No. 2, Article 155. http://doi.org/10.18080/ajtde.v6n2.155

Grajek, M; Roeller, LH. 2012. 'Regulation and Investment in Network Industries: Evidence from European Telecoms'. *Journal of Law & Economics*. Vol. 55, No. 1, pp. 189-216.

Havyatt, D. 2010. *Analysis: The long, hard slog to split Telstra*. iTnews.com.au, 10 December 2010. Retrieved from https://www.itnews.com.au/news/analysis-the-long-hard-slog-to-split-telstra-240517

Hubbard, RG; O'Brien, AP. 2017. *Microeconomics, 6th Edition*. Boston, Massachusetts: Pearson

iTnews. 2017a. *Vodafone first to sign up for NBN mobile backhaul*, 3 February. Retrieved from https://www.itnews.com.au/news/vodafone-first-to-sign-up-for-nbn-mobile-backhaul-449762

iTnews. 2017b. *NBN Co boss declares war with internet providers*, 31 July. Retrieved from https://www.itnews.com.au/news/nbn-co-boss-declares-war-with-internet-providers-469724

iTnews. 2018a. *NBN Co fixes wireless when users go below 6Mbps peak*, 16 February. Retrieved from https://www.itnews.com.au/news/nbn-co-fixes-wireless-when-users-go-below-6mbps-peak-485295

iTnews. 2018b. *Telstra CEO demands $20 a month NBN price cut*, 16 October. Retrieved from https://www.itnews.com.au/news/telstra-ceo-demands-20-a-month-nbn-price-cut-514013

McCulloch, D. 2004. 'Broadband Wars'. *Communications Law Bulletin*, Vol. 23, No. 1, pp. 4-6. Retrieved from http://www5.austlii.edu.au/au/journals/CommsLawB/2004/2.pdf

McLaren, G. 2016. *Is the NBN Co Monopoly Now Safe?*, 2 August. Blog post on mclarenwilliams.com.au. Retrieved from http://www.mclarenwilliams.com.au/2016/08/02/is-the-nbn-co-monopoly-now-safe/

NBN Co Limited. 2018. *Corporate Plan 2019-22*. August 2018. Retrieved from https://www.nbnco.com.au/content/dam/nbnco2/2018/documents/media-centre/corporate-plan-report-2019-2022.pdf

Ofcom. 2017. *Wholesale Local Access Market Review*. Published 20 April 2017. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0008/101051/duct-pole-access-remedies-consultation.pdf

Ookla. 2018. *Speedtest Global Index – September 2018*. Retrieved from http://www.speedtest.net/global-index

Open Signal. 2018. *The State of LTE (February 2018)*. Retrieved from https://opensignal.com/reports/2018/02/state-of-lte

Productivity Commission. 2001a. *Telecommunications Competition Regulation – Inquiry Report No. 16, 20 September 2001*. Retrieved from https://www.pc.gov.au/inquiries/completed/telecommunications-competition/report/telecommunications1.pdf

Productivity Commission. 2001b. 'Telecommunications Competition Regulation'. *Report No. 16. Appendix – Regulatory Background*. Retrieved from https://www.pc.gov.au/inquiries/completed/telecommunications-competition/report/telecommunications3.pdf

Raiche, H. 1997. *A History of Australian Telecommunications Policy*. Australian Legal Information Institute. Retrieved from http://www2.austlii.edu.au/itlaw/articles/raiche_history/telco_history-5.html

Reserve Bank of Australia. 1997. 'Privatisation in Australia'. *Reserve Bank of Australia Bulletin*, December 1997. Retrieved from https://www.rba.gov.au/publications/bulletin/1997/dec/pdf/bu-1297-2.pdf

Rudd, K; Swan, W; Tanner, L; Conroy, S. 2009. *New National Broadband Network – Joint media release of Prime Minister, Treasurer, Minister for Finance and Minister for Broadband*. Retrieved from http://ministers.treasury.gov.au/DisplayDocs.aspx?doc=pressreleases/2009/036.htm&pageID=003&min=wms&Year=&DocType

Ryan, M. 2003. *Developing the alternative communications policy framework*. Queensland University of Technology. Retrieved from https://eprints.qut.edu.au/4473/1/4473_1.pdf

Sidak, JG; Vassallo, AP. 2015. 'Did Separating Openreach from British Telecom benefit Consumers?', *World Competition*, Vol. 38, No. 1, pp. 31-76. Retrieved from https://www.criterioneconomics.com/docs/did-separating-openreach-from-british-telecom-benefit-consumers.pdf

Slattery, B. 2018. *Bevan Slattery Commsday Summit Predictions 2015-2018*. Retrieved from https://www.slideshare.net/BevanSlattery/slattery-commsday-prediction-superdeck-20152018

Sydney Morning Herald. 2005. *Senate votes in favour of Telstra sale*, 15 September. Retrieved from https://www.smh.com.au/business/senate-votes-in-favour-of-telstra-sale-20050915-gdm2gy.html

Sydney Morning Herald. 2018. *Telstra is preparing to buy NBN – but not before huge hit to taxpayers*, 17 October. Retrieved from https://www.smh.com.au/business/companies/telstra-is-preparing-to-buy-nbn-but-not-before-huge-hit-to-taxpayers-20181017-p50a5t.html

Tanner, L. 2002. *Reforming Telstra*. Retrieved from http://www.digecon.info/docs/0119.pdf

Telegeography. 2018. *Optus and Telstra outline 5G intentions*. Retrieved from https://www.telegeography.com/products/commsupdate/articles/2018/02/05/optus-and-telstra-outline-5g-intentions/

Telstra Corporation Limited. 1999. *Telstra 2 Share Offer*, 6 September. Retrieved from https://www.telstra.com.au/content/dam/tcom/about-us/investors/pdf%20A/t2-share-offer.pdf

Telstra Corporation Limited. 2011. *Explanatory Memorandum – Telstra's Participation in the Rollout of the National Broadband Network*. Telstra Annual General Meeting, 18 October 2011. Retrieved from https://www.telstra.com.au/content/dam/tcom/about-us/investors/pdf A/Explanatory-Memorandum.pdf

Telstra Corporation Limited. 2018. *T22 – our plan to lead*, 20 July. Retrieved from https://exchange.telstra.com.au/telstra2022-our-plan-to-lead/

The Australian. 2018. *Writedown an option as Labor vows to repair NBN*, 14 October. Retrieved from https://www.theaustralian.com.au/business/technology/writedown-an-option-as-labor-vows-to-repair-nbn/news-story/4e093d7cf652efca8bebc1a715c3dec0

Vertigan, M. 2014. *Volume I – National Broadband Network Market and Regulatory Report. Independent cost-benefit analysis of broadband and review of regulation*, 14 August. Retrieved from https://www.communications.gov.au/sites/g/files/net301/f/NBN-Market-and-Regulatory-Report.pdf

Westfield, M. 2000. *The Gatekeepers: The Global Media Battle to Control Australia's Pay TV*. Pluto Press Australia.

http://doi.org/10.18080/ajtde.v6n4.162

Impressions of an Overseas Visit by a Lines Engineer

Simon Moorhead
Ericsson Australia and New Zealand

Abstract: A fascinating paper from 1961 contrasting the technical and general differences in providing telecommunications services in Europe, North America and Australia.

Keywords: Telecommunications, History

Introduction

This historic paper was published in June 1961 at a time when overseas fact-finding assignments were a privilege for the recipient. A detailed report was required by management upon return (around 12,000 words in this example) which was widely circulated within the Postmaster-General's Department and ultimately published in the *Telecommunications Journal of Australia* (Volume 13, Number 1).

The actual overseas visit took place in late 1959 and was primarily to deal with technical matters in connection with the contract for the Sydney-Melbourne coaxial cable. The opportunity was also taken to investigate various aspects of external plant practices.

The paper is particularly interesting as it details the influence of non-technical factors on technical procedures. Relative wage and price levels are discussed and their influence on telecommunications manufacturing. For example, wages were higher in North America and the cost of materials handling equipment was lower, which encouraged a greater level of mechanisation in cable manufacture, compared to Europe.

The paper boldly examines various political factors which influence telecommunications infrastructure. For example, import restrictions on manufactured goods and raw materials in support of local industry are discussed. The report analyses the ownership of the telecommunications manufacturing industry in each country. It also contrasts the advantages and disadvantages of government or private ownership of telecommunications assets, and the flow-on effects to site acquisition, standardisation and interworking.

This is 1959 and well before the break up of Bell in 1984; however, the paper states the Bell System in Canada has a "taint of American capitalism about it and is therefore unpopular on National grounds". It also cautions the reader on one hand about the dangers of uncritical

http://doi.org/10.18080/ajtde.v6n4.164

acceptance of overseas matters, while, however, it cannot help but be impressed by the North American techniques.

The second half of the paper provides a detailed comparison between Australian and North American telecommunications infrastructure. This is a fascinating insight into the industry at the time and covers topics such as skilled tradesmen, exchange areas, subscriber services, buildings, installation and material supply.

The paper finishes with a short appraisal of the Bell System and the service provided to the public, namely: "A strong impression is gained of the Bell System to serve the public in every possible way". How this had changed by the breakup in 1984.

Reference

Bradley, D. P. 1961. "Impressions of an Overseas Visit by a Lines Engineer", *Telecommunication Journal of Australia*, Vol. 13, No. 1, June 1961, pp. 19-28.

The Historic Paper

http://doi.org/10.18080/ajtde.v6n4.164

IMPRESSIONS OF AN OVERSEAS VISIT BY A LINES ENGINEER

*D. P. BRADLEY, B.Sc., B.Com., A.M.I.E.Aust.**

FOREWORD

This article consists of a number of impressions of a technical and general nature gained on a visit to Europe and North America in late 1959. The visit was made primarily to deal with a number of technical matters in connection with the contract for the Sydney-Melbourne coaxial cable awarded to Felten & Guilleaume Carlswerk A/G, Cologne, (F & G), but the opportunity was taken to investigate various aspects of external plant practices, particularly cable design and application. This article deals with general topics only, and a second one dealing specifically with cable design and application will appear in a subsequent issue of the Journal.

INFLUENCE OF NON-TECHNICAL FACTORS ON TECHNICAL PRACTICES

General

Probably the most interesting and most important observation to be made from an overseas visit is the important influence which non-technical factors can have on technical designs and practices. While it is fairly obvious, looking from Australia, that differing geopraphical conditions and other factors must have an influence on designs and practices, nevertheless, first-hand observation overseas is necessary to appreciate how important these factors are. In fact, it is a reasonable first assumption that, whenever some overseas practice does not seem soundly or logically based in the view of Australian knowledge and experience, non-technical factors are the reason. Considerable caution must therefore be exercised in adopting overseas practices, particularly if it means departure from accepted and apparently satisfactory Australian practices.

Some of these factors are discussed in the following paragraphs. The list is not exhaustive and many chance and transitory factors influence technical decisions. As an example of the latter an enquiry was made why lead sheathed and not Stalpeth sheathed coaxial cable was to be used for the large trunk installation programme now commencing in the U.S.A. An explanation given was that the Western Electric Company's coaxial cable works had lead sheathing facilities only.

A word on the organisation of the telephone services overseas may be of interest. In the U.S.A. the telephone system is privately owned; about two-thirds of the facilities belong to the Bell System; the remainder to a large number of companies called the Independents. The Bell System has over 60 million subscribers and it is by far the largest telephone organisation in the world. It consists of four separate sections; the Bell Telephone Laboratories, the Western Electric Co., the American Telephone and Telegraph Co. (the A.T. & T.) and nineteen Bell operating companies. The operating companies provide telephone services in the different geographic areas of the U.S.A. and in Quebec and Ontario Canada. The A.T. & T. corresponds to Central Office in Australia, and is the central co-ordinating and policy-making body. It also provides the long distance trunk line services. The Western Electric Co. is the manufacturing and supply organisation. It is the largest telephone apparatus and the largest cable manufacturer in the world. The Laboratories, as well as engaging in the scientific and technical research which has made them world famous, prepare the manufacturing specifications and technical standards for the whole System in association with Western Electric and the A.T. & T.

The scene in England and Germany is much more familiar. Telephone services are provided respectively by the British Post Office (B.P.O.) and the Deutsche Bundespost (Bundespost). These are Central Government Departments and provide a similar wide range of postal and telecommunication services as we are accustomed to in Australia. Unlike the Bell System, neither of these organisations are extensive designers and manufacturers of telephone plant and apparatus, but buy most of their requirements from private manufacturers. Both England and Germany are large exporters of telephone equipment and engineering services, but the Post Office in each country is the major customer for the home industry.

Price Levels

Relative wage and price levels are a most important factor. As an example, this factor has an important bearing on the way construction and production jobs are done. The question here is the proportion of manual labour to machine time. In U.S.A., with a very high wage rate, as much labour as possible must be eliminated from every operation. On the other hand, the need is less pressing in the United Kingdom and Germany. And, in fact, it is evident to a visitor to those countries that every endeavour is made to substitute machines for men in the U.S.A., whereas in England and Germany manpower tends to be regarded as the basic commodity. Australia, by comparison, appears a well mechanised country, more so than the relative wage rates would indicate; possibly this is because the acute shortage of labour in Australia over the past 15 years has forced the pace of mechanisation beyond the economic level. There is also, perhaps, some uncritical acceptance of American methods in Australian industry generally without fully appreciating their economic limitations outside of the American economic environment.

An obvious operation for comparing the degree of mechanisation in countries is material handling. It is very striking to see numbers of men manually handling material, loading trucks and so on in English and German cable factories, whereas in U.S.A. work is extensively mechanised and little labour is employed. Australia appears to be well mechanised. To give an example of the care that must be taken, however, in assessing the degree of mechanisation justified and the risks involved in accepting overseas standards, the following example in regard to warehouse operation compares the use of manpower with the use of a fork-lift truck:

	Australia	U.S.A.
Price of fork-lift truck	£2,500	£1,000
Weekly wage of warehouseman	£15	£40

Obviously the Australian factory for best economy would employ more warehousemen and fewer fork-lift trucks than a comparable factory in the U.S.A., provided, of course, that the labour was available.

In each country visited, an enquiry was made about wage levels, taking as the criterion the wage paid to an operator in the cable industry (i.e. a non-skilled man with a certain amount of knowledge acquired on the job and paid a margin above unskilled work.) Typical figures were as follows:—

U.S.A. (New York area) £A45 per week plus; 40-hour week.
Canada £A32; 40-hour week.
Australia £15; 40-hour week.
U.K. £A12; 44-hour week (now 42-hours).
Germany £A11; 44-hour week (now 42 hours).

These figures are not exact because of the influence of overtime and bonus payments which vary from factory to factory in the same country. Also in England and Germany heavy social service payments are made by the factories on a per capita basis. Nevertheless, the figures are satisfactory for comparative purposes and show, contrary to the general opinion in Australia, that our wage levels are not high by overseas standards.

These wage levels, however, are no indication of relative price levels for raw materials or manufactured goods; for instance copper, the basic raw material of the telephone industry, has a world standard price. Plastics are cheaper in the U.S.A. than in Europe and U.K. and, as a general rule, are more expensive in Australia than elsewhere. Manufactured goods tend to be dearer in Australia than in other countries. While it proved impossible to find any item of plant or material to draw a price comparison similar to the wages comparison some trends are:—

1. The only price levels which seem clearly lower in Australia than overseas are some items of foodstuffs.

* See page 79.

http://doi.org/10.18080/ajtde.v6n4.164

2. Volume produced manufactured goods seen on retail sale such as domestic electrical apparatus and household utensils are, as a rule, more expensive in Australia. As a general rule, price and quality are best in the U.S.A.
3. Mechanised tools, construction plant and similar are low in price in the U.S.A.
4. The tax free retail prices of the Volkswagen is £450 in Germany, the Chevrolet £1,000 in U.S.A. (basic model) and the Holden £885 in Australia.

Regarding telephone material, cable and indoor apparatus made in U.K. and Europe is cheaper than when made in Australia. The position in regard to U.S.A. manufacture is less certain. Catalogue prices available are for supply to the Independent Telephone industry and most items are very highly priced by Australian standards, except cable which is a little dearer than in Australia. However, the Independent companies are small buyers and the prices listed are probably not representative of those paid by the Bell Companies. These should be low as manufacture by the Western Electric Co. is on an enormous scale, items are highly standardised and specifications are only changed if proved uneconomical on a balance of manufacturing, installation and maintenance costs; from the makers point of view, specifications are not subject to the whims of the customer. As an example, at the Kearny cable works of the Western Electric Company in October, 1959, 670 workers were employed and output was at the rate of 4,300,000 pair miles of cable per year. The output of Austral Standard Cables Pty. Ltd., with a comparable staff is some 500,000 pair miles per year and their productive operations compare very favourably with any cable plant seen in England and Germany. The result was achieved by a degree of mechanisation only made possible by the enormous demands for cable, and the positive planning made possible when the one organisation is both maker and user of the material.

While conclusions must be drawn with caution, Australia appears to be a country where manhours are comparatively cheap and manufactured goods and plant items are expensive. The lesson to be drawn, of course, is that a particular technique may be economically best in one country because of its labour/material costs ratio, but quite uneconomic in a country with a different relation between the costs of manhours, machines and materials.

Geographical and Economic Factors

These have an obvious bearing on telecommunication practices. For instance, subscribers distribution methods used in Australian and American cities where most people live in suburban houses will be quite different to those in German cities where people live in large apartment buildings. Again, if the terrain is rocky and mountainous, broadband radio is likely to be preferred to trunk cables. Economic factors will determine, for instance, the proportion of residential and business telephone services; the proportion of local trunk traffic and the volume and direction of trunk telephone services. These factors were observed fairly closely in Germany and England, and to a lesser extent in Holland and in North America.

The United Kingdom and West Germany are both similar in size to Victoria (U.K. 93,000, West Germany 95,000 and Victoria 88,000 sq. miles) but the populations are U.K. 50 million, West Germany 55 million and Victoria 2.5 million. Holland has 11 million people and is 13,500 sq. miles in area. The terrain in each country is largely flat and there are few apparent natural obstacles to transport and communication.

In contrast to these small, densely populated countries, the U.S.A. and Canada resemble Australia in their size and spaciousness. As a result trade and commerce carried out on an international basis between European countries corresponds geographically to interstate or even intrastate trade and commerce in Australia and North America. There is much greater freedom of intercourse and consequently a much greater volume. Hence the pattern of trunk telephone traffic is quite different. Long distance traffic such as Sydney-Melbourne, New York-Chicago, is vitally important in their countries, whereas short distance trunk traffic within the nations border is more important, both administratively and in volume in the compact European nations than the long haul international circuits.

London is the social, economic and administrative centre of the U.K. It is also one of the largest cities in the world. In consequence it is the focal point for trunk telephone traffic and the B.P.O. trunk network is laid out in star formation with London at the centre. Large blocks of circuits are required to connect London with cities such as Birmingham, Manchester and Sheffield and to provide for centres beyond. Traffic is densest at the London end and tapers with distance from London. The consequent heavy demands for trunk circuits were probably the reason why the B.P.O. pioneered the use of coaxial cable and is the largest user in the world on an area basis. London itself is the centre of an enormous urban area with a large residential and industrial telephone service and all the problems encountered in Melbourne and Sydney could be expected to exist in a worse form in London.

A feature of West Germany is the comparatively large number of medium-sized cities and the absence of one single large city comparable to London or Paris. Berlin, of course, is a large city, but it is effectively outside the normal range of telephone communication in the country. Hamburg has 1.7 million people, Munich 1.1 million, and there are six other cities over half a million. There are many cities of the population of Newcastle, Wollongong and Geelong. The cities are very compact and cover a small area. Most people live in several storey apartment buildings and there are few private houses. There is "no suburban sprawl" as we know it and there is a clear demarcation between urban and rural areas. As an example, travelling by train from Cologne (population 670,000) to Dortmund (580,000), the train passes through Leverkusen (72,500), Dusseldorf (595,000), Mulheim (151,000), Essen (661,000) and Bochum (325,000). The distance overall is about 60 miles—less than the rail distance from Dandenong to Geelong. This is one of the most heavily industrialised areas in the world, yet it is most surprising to an Australian that more than half the distance is through farming country devoid of any sign of industry or urbanisation.

Because of the compact self-contained cities the problem of providing subscribers services is comparatively simple. There are few transmission difficulties with local calls and there are few problems of the type experienced in Australia with residents on the outskirts of the city.

The proportion of residential telephone services is relatively low and the proportion of business services high. Hence there is a heavy demand for trunk line service, particularly short distance services, say 20 to 40 miles; there is proportionally less longer distance traffic. Technical development has, accordingly placed emphasis on meeting demands for heavy blocks of circuits over distances of 20 to 50 miles rather than over longer distances. For instance, Cologne has heavy traffic to the cities in the Ruhr mentioned above, but has lighter demands for trunk traffic to such cities as Frankfurt 100 miles away and Munich 200 miles away. As there is no focal city in West Germany the trunk network is not laid out in star formation but in a figure 8 with Frankfurt at the middle, Hamburg at the top and Munich at the bottom. The traffic density would not be comparable at any point with that in the vicinity of London and broadband facilities were not required until at a much later stage than in England.

Holland is similar to Germany although there is a greater degree of centralisation with the large cities of Amsterdam and Rotterdam. Distances between cities are small and their trunk problems look more like a junction problem to Australian eyes.

Cities in North America are similar in general layout and appearance to Australian cities of the same size and type. For instance, seen from an aircraft the suburban development of New York, Denver, St. Paul, and Salt Lake City resemble similar suburban development in Sydney, Melbourne, Adelaide or Brisbane; and, in fact, the telephone problem is much the same. Touring new housing estates in Toronto, Chicago and San Francisco, the comparison with residential areas in Sydney and Melbourne was striking. The cities consist of what is called the "down town" section which corresponds to the business section of the city proper, as known in Australia. An interesting feature here, is that in spite of the presence of a number of large multi-story buildings, the average area density of office workers in the

http://doi.org/10.18080/ajtde.v6n4.164

"down town" section is probably comparable with that in Sydney and Melbourne, because the sky-scrapers are usually few in number compared to the total number of buildings in the area. Outside the "down town" section there is, just as in Australia, an industrial area and an inner rather poor type of residential area where the houses are either of the apartment type or small houses close together; then further out, large areas of residential suburbs interposed with new industrial areas. This is the "suburban sprawl" just as in Australia except that the residential building blocks seem smaller than here. The comparison must not be taken too far of course; the U.S.A. has 18 times the population in the same area and consequently the urban territories in the East and in California are much greater in area and population than any in Australia.

It is apparent that the urban telephone problems have many points of similarity in each country. One difference however, is the higher telephone density in the U.S.A. with the result the residential telephone services penetrate into a lower income earner group than in Australia. Hence there is a heavy demand for telephone services in the tenement residential sectors where the population density is high and the telephone density per unit area is correspondingly high.

Climatic Conditions

This is an obvious point of difference between different countries, but its effects may be more far-reaching than would be expected. Two examples are quoted for the U.S.A.

The Isoceraunic Level: This is the average number of days per year on which thunder is heard and is the accepted measure of the intensity of lightning in an area. Obviously more elaborate and more expensive protection of external plant is required where the isoceraunic level is high. There is a great difference between the isoceraunic level in Australia and U.S.A. Nearly all of Australia is under the 30 days per year limit which is exceeded only in the mountainous areas of the Eastern States and in parts of the tropical north; nearly all of the U.S.A. is over the same limit, including most of the heavily populated part of the country. Much greater care must obviously be paid in the U.S.A. to lightning protection.

The Harsh Winter in North America: In all except the Pacific coast area and the south-east of the U.S.A. outdoor construction work ceases during the cold months. This necessarily adds heavily to costs as construction plant and organisations are idle for a considerable portion of the year. It also explains the much publicised high speed of construction work in U.S.A. because the short construction season necessitates high working speed to complete projects in a reasonable span of time and also, construction organisations have a compulsory and lengthy period to refit and to plan for the next season's work. Both the high construction speeds and the elaborate and expensive pre-planning are necessitated by the short construction period. High speed construction work is inherently expensive as it requires large-scale provision of men and plant and thus any hold up on the job such as shortage of material or breakdown of machines or any poor organisation of work will result in an elaborate construction organisation working in an expensive condition of inefficiency. A proportionally large and experienced engineering organisation is required to back-up the construction force. It is well to be aware of the background to the high speed construction work in the U.S.A. and to realise that the construction season in Australia is 12 months of the year and that projects can be completed in the same calendar period as in North America but at half the working speed and at lower cost.

Political Factors

The one that occurs to mind immediately is import restrictions and the encouragement of local industry in economically young countries such as Australia. This results in high internal price levels for many manufactured goods and, if the policy is extended to basic materials, may restrict the possible range of manufacture. For instance, all commonly used plastics are made in Australia under protected conditions and the industries using plastics must firstly pay more for them than overseas factories and, secondly, do not have access to the same variety of type and grades of these plastics. The local manufacturer is placed at a disadvantage on both accounts.

By contrast, in England and Germany traditional exporting nations, attention is paid to assisting the export industry; hence, this Department has access to the engineering data of the British and German Post Offices. As a specific example, all research work done by the German Telecommunication Industry is charged as overhead on local orders only. Export orders are not charged overhead for research. This is an agreement between the Bundespost and the industry for the express purpose of helping the industry in the export market.

A most interesting case in regard to political influence is the development of styroflex type carrier cable in Germany after the war. This happened because the Armistice forbade T.V. in occupied Germany. The ban extended to T.V. frequency amplifiers and hence coaxial cable installations were not permitted. The rising demands for trunk line facilities, therefore, led to the development of the 120-channel per pair styroflex insulated cable. This cable is unique to Germany and may never have been developed had technical issues only been involved. Further, when the T.V. ban was relaxed, an extensive Broadband Radio Programme was put in hand partly because this was the fastest way of providing large blocks of telephone circuits and T.V. relay facilities at short notice; secondly, at the time (about 1951) current technical opinion was that radio systems had made trunk cable systems obsolescent—a view which has since changed completely.

An important political factor is whether the telephone service is publicly or privately owned. Where it is under Government ownership it is traditionally a Department of the Central Government. As such it enjoys considerable legal privilege and its operating charter and regulations (i.e. the Act and Regulations under the Act) have legal precedence over those of other public utilities, the order of priority being Federal or Central Departments, Federal or Central Instrumentalities, State or Regional Departments, State or Regional Instrumentalities, Local Government organisations and privately owned enterprises. This legal privilege gives the Post Office telephone service substantial advantage over the privately owned system, which reflects in technical practices but it also makes them directly subject to the Central Government financial policy.

To quote some aspects where the privately owned Bell System suffers in comparison with the Post Office telephone systems:—

1. The acquisition of sites, properties wayleaves, etc. is strictly a private business transaction between the System and the property owner and the System can be held to an exhorbitant price for an essential site.
2. Local Governments place restrictions on such matters as the routing and alignment of duct systems, the siting of public telephone cabinets, etc.
3. Interference to telephone circuits by power circuits is a chronic problem everywhere. In Australia and the U.K. however, the operations of Power Authorities are governed by Regulations designed to reduce interference to a minimum and the Power Authority must build and operate its plant to conform to the requirements of the Telephone Authority. By contrast in the U.S.A., Power Authorities are under no obligation and the Telephone Authority may have to take elaborate and expensive precautions to protect its plant from power interference..
4. Telephone charges and conditions of service are determined in the U.S.A. by a large number of Regulatory Commissions. The Bell System is put to considerable expense in dealing with Regulatory Bodies. There are substantially more Regulatory Bodies than Bell Operating Companies, they are not obliged to follow the same principle and one Company may find itself dealing with several Regulatory Bodies each with its own individual rules. Government telephone systems are subject to parliamentary control but appear to enjoy considerable autonomy in detail matters. In the U.S.A., however, the Bell System is regulated in detail—for instance, in some Regulatory areas they are obliged to furnish party line service on demand even though this may militate against economical plant design.
5. The Bell System does not enjoy a legal monopoly of communications. This can be a matter of serious conse-

http://doi.org/10.18080/ajtde.v6n4.164

quences; for instance, the System is attempting to legally restrain long distance road hauliers from installing their own point to point fixed radio telephone service which they will use in place of the trunk line service.

The Bell System is a highly profitable organisation, and is regarded by investors in the U.S.A. as a stable and ably managed enterprise. A.T. & T. shares are regarded as a first-class investment. Consequently, the System can always raise funds on the money market. Further, due to the profitable nature of telephone business, the System is always looking for means to employ more funds. Hence, Bell System policy is to provide plant in advance of demand. The effectiveness of this policy is illustrated by the fact that orders for new residential services are normally issued immediately on application without checking first that plant is available. There is a certain degree of "calculated risk" in this policy, but difficulties rarely occur. For instance, in travelling through widely separated areas, in the U.S.A. and Canada, aerial line plant can be seen installed and ready for service in new housing estates, well in anticipation of occupation of the houses. Quoting actual figures for the Illinois Bell Company (State area), in 1952 the Company had 900,000 main stations, and 9,000 "Held" orders (deferred applications in our phraseology). In 1959 it had 1,270,000 main stations and only 1,900 held orders.

In England and Germany funds for telephone service are restricted as in Australia under a general anti-inflationary policy of restricting public works expenditure. This consideration, of course, does not apply with the privately owned Bell System, and it might appear that private ownership does provide funds for telephone service if the service is profitable, and if the money-market is prepared to respond to call on it for such funds; whereas a Government telephone authority under similar circumstances is restricted in funds by reason of general Government policy. However, this conclusion may not be true. The telephone service in North America is excellent and is always available, and this possibly is primarily due to the great economic strength of that country. Briefly, the country can afford the luxury of a first-class telephone service, whereas other countries cannot. Their first-class telephone service, is probably a reflection of economic strength, and is not a question of Government versus private ownership. This point is mentioned because the Americans make a feature of private ownership. Other public utilities in the U.S.A. owned by private capital, particularly transport services, compare unfavourably with Government-owned services in Europe and Australia.

A result of the ready availability of funds in the Bell System is that works are planned in the most economic possible way balancing immediate capital expenditure against operating and maintenance costs of the facility over its life. In the well-managed Bell System it can be safely assumed that the method of providing a facility where several alternative methods are available is determined strictly on the basis of Economic Comparison. By contrast Government telephone authorities, restricted for capital funds, must tend to do works in a way which makes least call on their capital resources. An amusing sidelight on the funds position in the Bell System is that individual engineers tend to charge as much expenditure as possible to Capital Account, which is freely available and to charge as little as possible to the Maintenance Account (which forms part of the Profit and Loss Account). The latter account is strictly policed and a field engineer is judged by comparison between his plant fault record and the expenditure on maintenance.

A positive factor in Bell System policy appears to be fear of Government ownership. To quote an example, the Telephone Division of the Rural Electrification Administration, which has a specific task to upgrade telephone service in rural areas has had the effect that the Bell System apparently no longer seeks to make a profit on its rural operations. Further, the System feels obliged to provide a good class of rural service because its view is that if the Bell System does not, then the Government will, and this will be "the thin end of the wedge" for Government ownership generally. Their views are influenced by the difficulties of the privately owned power industry in the U.S.A.

The situation is even more marked in Canada, where the Bell System has the 'taint' of American capitalism about it and is, therefore, unpopular on National grounds; and, secondly, because in Canada there are some first-class Government-owned utilities such as the Ontario Hydro-Electric Power Commission, whereas in the U.S.A. Government services have the reputation of being poorly operated. For instance, the U.S. Post Office, from the point of view of a superficial customer, appears to be poorly run and the Bell System points to such examples as the fate that could overtake the American Telephone Service if it were Government run. However, the Canadian Bell cannot point to any such example. Some years ago in Toronto in new housing developments the Government-owned electricity, water supply and sewerage utilities were able to provide service in new housing developments ahead of occupation, whereas at the time there was a lag of up to two years in the provision of telephone service. Canadian Bell, therefore, exerted all its resources to overcome the situation because of this fear of Government ownership.

The System is very sensitive to public opinion and goes to considerable lengths to forestall criticism. Surprisingly a great deal of criticism of the System is to be heard in North America; most of it is ill-informed and unfair as the System provides a first-class service at, by American income levels, low rates. The type of criticism was much as would be expected in Australia but more intensified.

Ownership of the Telephone Manufacturing Industry

Three separate cases must be considered:

(i) The operating authority designs and manufactures the bulk of its own plant and equipment. The Bell System is probably the only case.

(ii) The operating authority buys equipment designed and manufactured by a national telephone equipment manufacturing industry. This is the position in England, Germany and Sweden and other parts of Europe.

(iii) The operating authority either imports its material or else buys it from local factories which make to overseas design. This is substantially the position in Australia.

The fact that the Bell System also designs and makes its own plant has some important influences on costs and design, for instance, the optimum balance in design can be struck between manufacturing costs and user costs (that is installation and maintenance costs). Where the telephone authority buys from a separate manufacturing industry there must be a tendency for the authority's specifications to be drawn up largely with installation and maintenance requirements to the forefront and manufacturing considerations overlooked to some extent; and where the operating authority buys from an overseas manufacturer there must be tendency for ease of manufacture or the requirements of the manufacturer's major customers to take precedence over the buyer's operating and maintenance costs. Whether manufacturing or user considerations take precedence will depend on the cussomer's strength as a buyer as well as his ability to specify his own requirements correctly. The Bell System is in a position to strike the best compromise between these conflicting requirements.

Another aspect is that since there is no competition in supply the manufacturing plant can be run until it reaches the end of its economic life. At this point new plant is installed using the most modern techniques and the product design is suitably altered to take best advantage of the new manufacturing techniques. New developments are only introduced when proved economic on the basis of all manufacturing costs including investment in manufacturing plant which will be rendered obsolete by the change as well as all conditions relating to use in the field. Sound designs are not prematurely scrapped to meet a competitive situation.

As both maker and user the Bell System obtains its apparatus under probably the most favourable possible economic conditions. However, there must be a tendency to defer the latest developments for the time being until the appropriate interval in economic overall planning. Furthermore, a lack of competition exists which must to some extent tend to make design less progressive.

The telephone authority which buys from outside, buys on a competitive market and enjoys all the advantages

http://doi.org/10.18080/ajtde.v6n4.164

of competition including the ability to buy the latest development at the earliest stage. Even if the telephone authority must buy from its national industry and there is no internal competition, there is intensive competition with other countries for the export market which ensures that the industry remains technically progressive even if there is no price competition in the home market.

A reasonable conclusion to be drawn is that the Bell System practice in regard to plant design may be somewhat conservative but that it preserves the best balance between manufacturing and user costs. It should always be kept in mind, however, in examining any Bell System practice that the association of the Western Electric Coy. and the Bell System will result in a different approach to the design of items of plant in which manufacturing aspects of the design are given more weight than when the item is designed by an authority whose main interest is in operation and maintenance.

Australia and Canada differ from the U.K., European countries and the U.S.A. in that there is no national telephone manufacturing industry—while most requirements are made in Australia they are to overseas designs and patents and the industry is partly overseas owned. One result is that there is more freedom of choice of design than in the case of overseas administrations. For instance, it would hardly be conceivable for the B.P.O. or Bundespost to adopt the Swedish cross-bar technique and ignore the technical developments and the patent pools of the national telephone industry; the freedom of technical choice of a Government telephone authority must be limited by the manufacturing and research capacity of its home industry and their current investment in manufacturing plant and ownership of patents.

One conclusion reached overseas is that this Department is one of the largest uncommitted customers in the world and that its business is eagerly sought by the British and European industry both for its volume and also because its technical prestige is sufficiently high that its choice of design influences other customers.

Technical and Administrative Complexity

Recent technical development such as the Broadband Programme, the E.L.S.A. and A.N.S.O. schemes and the crossbar project are regarded by engineers as heralding a new era of "technical sophistication". By comparison with the Bell System, B.P.O. and Bundespost, however, Australia is "technically unsophisticated". One result is that developments and modification to existing plant and equipment can be effected simply and without undue complexity whereas small technical changes in the more complex overseas telephone systems must be closely and cautiously examined for side effects. Another probably consequential result is that these three authorities have proportionally much larger technical headquarters staffs.

Another factor is the comparatively small scale of organisation in Australia. The Bell System and the Department are organised along similar lines except that there are three tiers of authority in the Bell System—the Operating Company regional organisation, the Operating Company headquarters, and the System headquarters (A.T. & T.) — compared with two—State Administration and Central Administration. Further, the scale of magnitude is perhaps in the ratio of thirty to one. Consequently there is much more opportunity in Australia to collect information, make decisions and put them into practice quickly and accurately. This is the advantage of a small organisation. By reason of the complexities due to sheer size the Bell System must be slow moving and cautious and give the appearance of being conservative. Similar remarks apply to the B.P.O. and the Bundespost except that they are smaller in volume and territory than the Bell System and consequently can operate with somewhat more speed and flexibility.

The conclusion is that the large overseas authorities must be more cautious and slow moving than we are in technical matters and the fact that the Bell System or B.P.O. has not adopted a new practice is not necessarily a good reason why we should wait—it may merely be that administrative difficulties are delaying its investigation and introduction.

AUSTRALIA & NORTH AMERICA

General Conditions

In spite of being aware of the dangers of uncritical acceptance of overseas matters it is difficult for an Australian visiting U.S.A. and Canada for the first time to avoid being so impressed by the general similarity of the three countries to such an extent as to unduly influence him towards North American techniques. This is particularly so if he is returning to Australia after a visit to the U.K. and Europe where customs, ideas and conditions are obviously very different from those at home. The Australian landing in the U.S.A. after a period in Europe feels so much at home that he is bound to be biassed towards American ways. These are the views not only of the writer but of every experienced person with whom he has discussed the matter. Since Australia has so much in common with U.S.A. and Canada their methods and techniques must often be eminently suited for use here. But there are sufficient important points of difference to make the uncritical acceptance of American ideas a dangerous procedure.

The first important aspect of similarity between Australia, Canada and the U.S.A. is the large physical area of these countries compared to European countries.

Secondly, these three countries are new countries. For instance the modern development of U.S.A. commenced with the opening of the West and the inauguration of large scale migration, after the end of the Civil War in 1865. Australia's growth commenced about the same time with the discovery of gold. Thus both countries grew in the age following the Industrial Revolution and the previous era has left little mark—this, for instance, is probably the reason why Australian cities appear so similar in character to American cities and both seem so different to English and European cities. As a result there is little tradition in either country and people are probably more open to new ideas and new techniques.

Neither country has suffered modern war on its own soil, a factor which, particularly after seeing the results of war damage in Europe and England, must have a profound effect both on the economy and the outlook of the people.

Another factor is that the economy has been consistently expanding for a century in both countries and there has always been scope for application of new techniques and practices.

While an Australian feels at home in the U.S.A. and life in both countries is similar in many ways it is not correct to say that Australia is "Americanised" —it is rather that both are New World countries and the customs, manners and problems in each are those of the New World. There are, however, some very important differences between the two countries which must be taken into account.

The first point is the great economic strength of the U.S.A. The wealth of the U.S.A. is well known and much publicised in terms of statistical data but first hand observation is necessary to really appreciate the position and to quell any scepticism that may be felt about the statistics. Quoting some diverse examples:—

1. High incomes combined with low costs of living. For instance, engineers at A.T. & T. Headquarters, New York equivalent to Sectional and Divisional rank, are paid $18,000-$21,000 and $15,000 (£A6,700) per year respectively. These are good, but not exceptional salaries. Their living expenses, for equal standards, would not be much higher than ours.

2. A flight from St. Paul to Denver, a distance of about 700 miles across the heart of inland U.S.A. was over fertile farm country for its full distance. A similarly placed flight in Australia would be from Alice Springs to Kalgoorlie across barren desert country. The U.S.A. is endowed with a rich soil, adequate rainfall, a temperate climate, as well as with great mineral and other resources —it is a country richly endowed by nature.

3. It is most impressive in the Bell System to see the number of Engineers who can be directed to work at a single task. Proportionally more Engineers are employed in England, or Germany than in Australia, but, it is clear that the Americans can and do put far more professionally trained men on to a given task, then either England or Germany or Australia.

However, there is a wide disparity between the economic strength of the different parts of the U.S.A. and while the

http://doi.org/10.18080/ajtde.v6n4.164

Northern and Pacific coast States are undoubtedly the most prosperous areas in the world the Southern States are comparatively weak economically. These comments apply to the North.

Another factor is the comparatively small population and relatively immature economy of Australia. This has many effects, one being that there is not the weight of demand for service that there is in the U.S.A. and another being that Australia's resources have not been developed to the extent required to meet the demand.

Conclusions to be drawn are that needs for service in the two countries may differ in both type and intensity, the economic way of meeting them may be different and finally types of services which can be provided in the U.S.A. may not be feasible in Australia due to our inferior economic position.

Availability of Skilled Tradesmen

There appear to be few facilities for training skilled tradesmen in the U.S.A. such as the apprentice scheme familiar in Australia. For instance, the Bell System does not operate anything equivalent to our 5-year training course for technicians or even the shorter course for training linemen. Craftsmen are recruited directly from school and are trained almost entirely on the job with short classroom sessions from time to time. This is typical of American methods as a whole and has the repercussion that trade skills are highly valued in the U.S.A. In fact, when enquiring as to how such skills as toolmaking are acquired a satisfactory answer could not be given, but it was suggested that most of such tradesmen are migrants from England and Europe.

This lack of a force of skilled tradesmen has an important repercussion on plant design in that every effort is made to "deskill" field operations in the U.S.A. As much of the installation complexity as possible is taken out of the task by designing the item so that most of the skilled work is done in the factory and installation becomes largely a simple attachment task. This approach also explains the high degree of specialisation by workmen in the U.S.A. Under the apprentice training scheme the tradesman is trained in every branch of his craft particularly in the first principles whereas under the American scheme tradesmen are trained to be skilled for the task in hand and nothing more.

Side by side with this absence of a large body of skilled workmen is a relative abundance of engineers so that technical practices and designs can be carefully and elaborately engineered and made suitable for use by a relatively unskilled body of workmen.

Hence it follows that many American designs and practices are unsuited for Australian usage because of the difference in the proportion of engineers to skilled workmen here.

SIZES OF EXCHANGE AREAS IN NORTH AMERICA

It is generally known in Australia that the sizes of telephone exchanges and exchange areas in North America are substantially larger than we are accustomed to. Nevertheless, it is surprising to find in suburban areas similar in appearance to Australian suburbs, how few exchanges there are in the area and that these are mainly very large exchanges. For instance, the Evanston district of Chicago is an urban area very similar in social, commercial and residential development to the eastern suburbs of Melbourne. A comparison of the exchange sizes is illuminating.

Melbourne

W Group (Note 1)

Box Hill	9,354
Camberwell	4,685
Canterbury	7,004
Deepdene	3,521
East Kew	5,097
Hawthorn	4,852
Kew	3,442
Mitcham	2,749
Nth. Balwyn	1,780
Ringwood	3,268
4 small exchanges	1,338
	47,090

Chicago

Evanston District (Note 2)

Evanston	29,662
Wilmette	9,334
Winnetka	10,050
	49,046

Note 1.—Subscribers connected at 30/6/59.

Note 2.—Subscribers Pairs Terminated at M.D.F., December, 1958. The term "Subscriber Pairs Terminated" means the number of working subscribers' lines appearing on the line side of the M.D.F. Because of the widespread use of party lines the actual number of working cable pairs terminated may be substantially less than this figure.

The three Chicago exchanges serve an area about 10-12 miles long and 4 miles wide with a population of about 105,000. The W group in Melbourne is somewhat larger in area and population. Evanston is part of a Bell System administrative area (the North Shore Division) where there are 10 exchanges (including the 3 quoted above) with 193,950 subs. pairs terminated.

Another example is Chicago Heights exchange with 15,830 working subscribers' pairs terminated. The exchange area is roughly triangular in shape the base being about 13 miles and the height about 7 miles. It is a newly developed residential area with a large amount of still undeveloped land. The developed area is scattered amongst the undeveloped areas. Ultimately, it is expected that the whole area will become one large suburban residential development. As a matter of interest, it includes the suburb of Park Forest, described in William H. Whyte's book, *The Organisation Man*. The exchange is approximately in the geographical centre of the area, but not the copper centre and is about 15 miles from the centre of "down town" Chicago.

Another example was an exchange area in a country district which the Bell system had recently taken over from an independent Company. The plant was in run-down condition and the Illinois Bell had virtually started from new in rebuilding it. The area consisted of a country village, and surrounding farming population. One exchange only was established in the village to serve the exchange area which was over 200 sq. miles in size. Farm houses up to 12 miles from the exchange were served by loaded 20 lb. cable. Under Australian practices cable would be used for three or four miles, then aerial construction to meet transmission requirements or alternatively several R.A.X.'s would be established to serve the area in addition to an exchange in the town.

The following data is an analysis of exchange capacity for the State Area of the Illinois Bell Telephone Company at December, 1958:—

Number of subscriber's lines: 1,245,000

Number of subscribers' pairs terminated on exchange M.D.F.'s 1,066,000

(The difference between the two figures is due to the use of party lines. If there were no party lines, the two figures would be equal.)

Number of Exchanges:

Subscribers' Pairs Terminated	Number
Under 100	13
100- 1,000	87
1,000- 5,000	58
5,000-10,000	23
10,000-20,000	21
20,000-30,000	10
30,000-40,000	5
	217

Largest Exchange, 38,570 Subs. Pairs Terminated.

Smallest Exchange, 22 Subs. Pairs Terminated.

There are 36 exchanges with over 10,000 Subscribers' Pairs Terminated each and totalling 869,500 Subscribers' Pairs Terminated.

Some comparative figures for Australia at 30/6/59 are:—

Subscribers connected to automatic exchanges 1,054,517

Exchanges—

Standard auto	435
Rural auto	1,213

Thus, for approximately the same number of subscribers there were 1,648 exchanges compared to their 217. The population density of the Illinois Bell area is very much greater than in Australia, being that of the urban areas surrounding the City of Chicago together with well settled farming country; nevertheless, a fundamental difference is revealed in the approach to the problem in the two countries.

http://doi.org/10.18080/ajtde.v6n4.164

Exchange Loops. It is evident that these must be longer than in Australia. Recent statistical surveys by the Illinois Bell in an inner area Chicago exchange showed that the average length of subscribers' loop was 7,700 pair feet and in two large country towns 11,000 pair feet and 9,500 pair feet. A similar investigation made in 1957 in Australia gave the average at 5,280 pair feet (Metropolitan Areas).

Thus there are two aspects of the difference in approach:—

1. The number of subscribers connected to an exchange is greater in the U.S.A.
2. The size of the exchange area is also greater.

The two aspects are, of course, compatible.

Although statistical data is quoted only for the Illinois Bell, from observations in other cities and from discussion, the figures are typical of Bell practice. There are no particular technical reasons for the difference between exchange sizes in the two countries. It is true that extensive loading of subscribers' cable is practised in the United States compared to Australia and also that the dialling loop resistance limits are higher than in Australia, but these factors only affect the fringe areas of exchanges and are not important reasons for the difference.

In discussion appropriate engineers in the Illinois Bell Company could not give any explicit reasons for the large size of exchanges beyond saying that it had always been so and that this was the most economic way of providing service.

Possibly an important factor is that the Bell System is privately owned and lacks any special legal privileges. By comparison the Australian, British and German Post Offices enjoy considerable legal privilege by virtue of the fact that they are central Government Departments; further, they are not subject to the rules of local and regional administrations. This effects the relative economic positions as follows:—

1. The Bell System cannot compulsorily acquire exchange sites but must buy them on the open market at the vendor's price.
2. The Bell System has to pay rates on its buildings. Apart from the fact that Government systems do not pay rates at all, these are higher in the United States because of the wide functions of local Government there (in particular law and order and education).
3. The Bell System is restricted in the location and route of its duct runs by municipal authorities.

Furthermore, the need to build Post Offices in every main business centre means that space is incidentally available for telephone exchange purposes.

These restrictions have the effect that the Bell System will be reluctant to own more exchange property than absolutely necessary. Thus fewer and larger exchanges are indicated. This has the advantage then that, as the copper centre of a large exchange area is less precisely defined than that of a small exchange area, there is a larger choice of suitable exchange sites and therefore more chance of acquiring a suitable site at the market price and less chance of being charged an exhorbitant price for the desired block.

Another factor is the high wage rates combined with low costs of factory made goods in the U.S.A. which make large exchanges more favourable in America. In regard to exchange equipment, one large exchange in lieu of several smaller ones centralises maintenance and reduces the size of maintenance staff. Furthermore, fewer manhours are required to build one large exchange than several small ones and a greater proportion of unskilled labour can be employed. Centralising exchange construction increases the scope for mechanisation and the use of labour-saving devices at which the Americans are so adept.

As regards external plant, conduit costs in the U.S.A. probably favour large exchanges. Conduit construction is restricted by our standards due to wide use of aerial cable, and is mainly confined to the areas in the immediate vicinity of the exchanges. Construction costs are high as the work is mainly in congested areas where hand labour must be used. Further, due to Local Government rules, the cheapest route cannot always be followed and the conduits must be laid deeply in the roadway.

This favours large exchanges, firstly because maximum size cables are used and therefore maximum utilization is made of the ducts and secondly they require very large duct runs which are the cheapest to construct per duct since the cost of digging the trench and refilling it and reinstating the roadway increases much less than proportionally to the increase in the number of ducts.

On the other hand cable costs favour small exchange areas. Labour costs of cable installation are probably similar irrespective of whether an area is served by one large or several small cables. However, heavier gauge of cable is used in the case of one big exchange and total cable costs are much greater as a result. In fact, under transmission conditions common to all local exchange areas, doubling the radius of the exchange area will quadruple the costs—costs increase as the square of the increase in the radius.

To assess the relative importance of costs the following is the latest data available for Australia:—

1958-59 Cost of Subscribers' Services.

Metro. Auto	Providing			Maintenance		
Exchange Equipment	68	2	2	5	14	6
Subs. Equipment	15	4	1	1	8	0
Cables and Conduits	138	16	0	3	6	7
Aerial Wires	18	0	11	1	1	0
	£240	3	2	£11	10	1

It will be noted that Cables and Conduits make up the bulk of the providing costs, but Exchange Equipment makes up the bulk of the maintenance costs.

From the discussion above it is plain that both the ratio and magnitude of the different items listed above would be altered if assessed in terms of American costs and price levels. The ratio of internal and external plant costs in Australia arises largely from the sizes of particular exchange areas which are determined in metropolitan areas by economic comparisons in every case. The usual process is that a demand for telephone service arises on the outskirts of existing exchange areas due to the development of previously unoccupied land. This demand is initially met by providing more cable back to the existing exchanges. This cable must be heavier gauge than existing cables to provide standard grade of transmission for these more distant services. Eventually, as the demands for service in the new area increases the costs of extra cable and conduit become so high that it is cheaper to establish an exchange to serve the area. The decision to establish the new exchange is based on an economic comparison of capital and annual charges for internal and external plant of serving the area from existing exchanges compared to establishing the new exchange. It is the rising cost of line plant to serve the new area which first shows the need to investigate the economics of establishing a new exchange.

Thus there is a logical economic basis for the ratio of internal and external plant costs in Australia although the correctness of the ratio is effected by the difficulties inherent in economic comparisons which are necessarily spread over a number of years due to changes in the value of money, to changes in the relative price levels of different items of plant and labour and to changes in technique.

A comparison between the economics of Australian and American practice would require a breakdown of American costs between labour and material. An accurate knowledge of building and equipment costs and of manhours required for plant installation would also be necessary. It might be possible then to draw a comparison between the economics of the practices in the two countries and it is likely that the comparison would prove our practices correct under the Australian cost structure and the Bell System correct under U.S.A. costs. The required data is not available but it should be obvious that any proposed changes in present practice to bring it more in line with American practices must be approached with great caution and all the relevant cost factors in the U.S.A. ascertained and their importance assessed.

Apart from the reasons given above it is possible that the large exchange areas in the U.S.A. are based on practices developed in pre-war years. It is stated that the move to the suburbs is a relatively recent one and that the bulk of the urban population formerly lived in apartment house areas of high population density. (King's Cross, Sydney is the only area in Australia similar to the types of such areas to be seen in the inner parts of New York, Chicago and San Francisco). The area density of

http://doi.org/10.18080/ajtde.v6n4.164

telephones in these localities was very high and very large exchanges serving relatively compact areas were required to serve them.

Furthermore, the present suburbs grew from a nucleus of small towns spaced some miles apart on the periphery of the metropolitan areas. The suburbs grew by filling up the open space surrounding these towns until the developments met to form one continuous urban area. The suburban development in Australia has not been of this type; rather the boundaries of existing suburbs have moved further outward in a continuous development although the American pattern can be seen in the way that Dandenong is becoming part of the Melbourne urban area and Gosford appears likely to become a dormitory suburb of Sydney. A result is that the areas served by existing exchanges in these U.S.A. towns grew out as the suburbs grew just as the areas served by country towns in Australia tend to grow. This is the case in the Evanston exchange area quoted above.

Summarising this discussion, in both U.S.A. and Canada the service areas and the number of subscribers connected are substantially larger than in Australia. The reasons probably include the factors which make it desirable for the Bell System to own as little exchange property as possible, the relative scale of wages and material costs in North America, and some historical factors which do not exist in Australia.

The effect of large exchanges and exchange areas is almost certain to reduce equipment providing and maintenance costs, but line plant costs will increase substantially because heavier gauge cable is required to meet transmission limits and the average length of subscribers' lines is longer.

The relevant factors in the two countries are so difficult to assess and compare that great caution must be exercised and a careful assessment of the economics made before changing our present scale of exchange sizes. As exchange areas in Australia have been determined primarily on the basis of economic comparison it is very likely that they are the correct size for Australian economic conditions. It is to be expected, however, that wages will continue to rise relative to material cost and this may tend to make the preferred size of the exchange area larger.

EXCHANGE BUILDINGS

Exchange buildings in the U.S.A. are similar in general design and appearance to Australian exchanges, particularly suburban exchanges. The ground floor contains the M.D.F. test desk, staff amenities, etc., and the equipment is housed on the floor above. In visiting crossbar, panel type and Strowger exchanges the general layout in each case was a familiar one.

There is however, one important point of difference—all these buildings have large basements. This is normal building practice in the U.S.A. because of climatic conditions. This basement housed the power and battery equipment. The power equipment appeared familiar, but in every case enclosed type cells were used and the batteries were not partitioned off from the rest of the basement which was, in fact, one large room. In some cases there was a brick partition along one wall to form a separate cable chamber but in other cases the cable racking was erected along one wall of the basement and was not partitioned off from the plant in the basement. An important point to mention is that cable entry is by ducts and all the ducts are carefully sealed off so there is no question of water or gas entering the basement through the duct.

One exchange building only was visited in Germany. It was a combined exchange, carrier station and district office. The exchange equipment was E.M.D. type and the interesting point was that the switches were in a separate sealed room served by a packaged air-conditioner; staff enter this room only for specific purposes such as routines and attention to faults. The M.D.F. and the test desk were side by side in a room in another part of the building. The exchange itself was of about 2,000 lines capacity. This approach seemed a reasonable one in that the switches are confined to a small air-conditioned space from which the staff are excluded as far as possible.

PARTY LINES IN THE U.S.A.

The Bell System provides 2 party and 4 party line service with harmonic ringing in urban areas in addition to rural party line service with code ringing. The party line service is a non-secret type and there is nothing similar to duplex in use. The party line system which has been widely used in urban areas appears to be a trouble to the Bell System, which is forced in some areas by the Regulatory Commission to provide party line service on demand by applicants; a steady demand exists because party line rent is lower than exclusive service rent. Nevertheless, as would be expected, there are a diminishing number of party line services in the urban areas and the operating Companies are put to some trouble to insure that a 4-party line service, say, has 4 parties on it and not a lesser number; obviously they are faced with a difficult commercial situation if people paying rent for a 4-party service are only sharing a line with one or two other subscribers. The result is that the subscribers to a party line may be widely separated in the exchange area and a difficult problem in cable design arises, particularly in resording and re-arranging cable pairs. In discussion with American engineers, it appeared that the Bell System would prefer not to have party line service in urban areas.

PROCEDURE FOR INSTALLATION OF SUBSCRIBER'S TELEPHONE SERVICE

These are generally similar in Australia, Germany, U.K. and U.S.A. In each country application for a private subscriber's service is made at a Commercial Office where a multi-copy Telephone Order form is prepared listing particulars of the subscribers's requirements. Exchange number and cable pair allocations are made by appropriate plant offices and copies of the Telephone Order complete with installation data go to the Installation and Exchange staffs. On completion of the works, costs and statistical details are added and copies of the Order are distributed to Accounts, Directory, etc. Both the B.P.O. and Bundespost forms are similar in appearance to the Australian Telephone Order.

One difference to Australian organisation in these countries is that the one staff completes the work at the subscriber's premises; separate line and substation installation staffs are not employed. An exception to this rule is made by the Bell System when installing large numbers of services in the one area such as new house developments—in this case the Task Force principle is used and separate teams are employed for inside and outside work.

In the Bell System preparing and moving copies of the Order quickly to the destinations is a problem which has been closely studied by the Bell System and the latest procedure used is for the Business Office, Plant Service Centre, Revenue Accounting, Directory and Traffic Intercept to be connected to the one teletype circuit. The Order is prepared in the Business Office, the exchange number and pair allocation being passed over the teletype circuit from the Plant Service Centre, and is then distributed to the field staff. The aim in Metropolitan areas is to provide a "one day service" which means that if a subscriber applies say on Monday P.M. the Order is in transit on Tuesday and copies are in the hands of the M.D.F. and Installation Foremen by the close of business Tuesday. The M.D.F. jumper is run on Tuesday night and the Installer is given his copy of the Order when he reports for duty on Wednesday morning. He will report to the applicant's premises at any time on Wednesday that the applicant cared to nominate to the Business Office; he completes the installation at the one visit. Note that the designation "one day service" is a slight exaggeration. Had the applicant applied on Monday A.M. the service could have been installed on Tuesday P.M.

The Bell System, as part of its service to customers, puts great store on completing the service by the time promised and statistics on the subject at A.T. & T. Headquarters showed that 98% or better were completed by the promised date which means, in most metropolitan cases, "same day" or "one day" — a very impressive performance. About 60% of Orders, taking the System as a whole, are said to be completed on the "same day" or "one day", basis. One factor that helps is that the Business Office assumes that a cable pair and an exchange number are available and accordingly quotes the application on the spot. The Office has a list of barred

http://doi.org/10.18080/ajtde.v6n4.164

areas where service cannot be quoted on demand, but everywhere else it is assumed that line plant is in situ to provide the applicant's service. Experience is that this policy involved only a slight risk. As there are now few barred areas it is evident that many applicants are connected one or two days after they apply.

Other reasons for this promptness, apart from the ready availability of capital and hence of plant, are:—

1. The one Supervisor controls the work at both the exchange and subscriber's end.
2. The use of a lineman installer associated with a form of outside plant construction which allows one man, by running a length of drop wire, to complete the line work. I.T.P. construction used in many parts of Australia is similar.
3. Pre-jumpering at the M.D.F. is done the night before.
4. All testing of the installation is done by the installer using a simple battery operated tester and an exchange ringback type test. If any component is faulty he faults the whole installation and leaves the premises. The new service is then treated as a faulty line and handled through the fault procedure.
5. Paper work is kept to a minimum by the installer reading his completion data to a female clerk or into a tape recorder at the Plant Service Centre. He does not submit a written completion Order.

The exchange Test Desk does not check any new private subscriber's service. It is employed for maintenance and fault testing only. This procedure was introduced some years ago as a stop gap due to shortage of staff and equipment, but testing by the Installer proved satisfactory and the saving in staff, equipment and exchange space is such that the previous procedure, the same as present Australian procedure, was not re-introduced.

Another important factor is the positive drive to ensure that all work is completed on time. The efforts of all persons involved in these operations is measured and examined by their superior on the basis that every person must complete a certain proportion of his work on the day it is received and is only permitted a certain carry-over to the next day, e.g. the Business Office must clear say 90% of its orders on the day the application is made and a continuous critical record is kept of its performance.

The procedure in Germany is that the Commercial Office contacts the Cable Recorder by telephone while the applicant waits at the counter and, if a line is available, the Order, complete with installation data, is prepared immediately and posted to the installation staff. The Bundespost claim that 40% of all applicants have service within five working days.

In England the average time for completion of order work in London is three weeks in the Sales Division and four weeks in the Engineering Division. In the Provinces 60% of Orders are completed within one month, the majority being within 2-3 weeks.

Corresponding data is not available for Australia, but it seems unlikely that the performance would be as good as any of these, even for areas where both exchange numbers and cable pairs are available. One reason is probably the use of two separate staffs to complete work at the subscriber's end. In the other systems time is lost at two stages—one is in the paper-work which is unavoidably complex resulting in a delay before the Order is in the hands of the Installation Staff. The other is the staffing delay before the work force arrive at the subscriber's premises. In the Australian system a third delay is involved while notification is passed to the Internal Staff that linework is completed and finally there is the delay before the Internal Installer arrives at the subscriber's premises.

Particularly by comparison with the Bell System there seem a lack of positive drive to expedite this phase of work which is probably the most important of all in regard to good public relations. Apart from the use of two separate staffs to complete work at the subscriber's end, control of the work, except in Country Divisions, is spread between three different Divisions—Metro. Service for the M.D.F. jumpering and the Test Desk work, District Works for the line work and Subscribers' Installation for the instrument. The lowest common level of authority is the Superintending Eigineer, Metropolitan.

A better arrangement for management would be the one Divisional Engineer in charge of all work external to the exchange and also of work on the M.D.F. This is the arrangement in New Zealand, where the M.D.F. is partitioned off from the exchange and is the responsibility of the External Plant Engineer. If testing is carried out by the installer then all work directly associated with the subscriber's installation would be controlled by one Divisional Engineer.

MATERIAL SUPPLY ORGANISATION

The scale of the problem in Australia is larger than might be expected. England and Germany are territorially small and the material distribution and control problem is simplified thereby. The volume of the material handled in Australia is surprisingly high. Taking subscribers' cable, which is a basic item, our annual requirement is 500,000 pair miles per year and increasing by about 50,000 pair miles per year. The consumption in the U.K. is 700,000-800,000 pair miles per year. Bell System requirements of cable were estimated at 125 B.C.F. (billion conductor feet) for 1959 and 131 B.C.C. for 1960—11.8m. pair miles and 12.4m. pair miles respectively. The relative quantities of cable used in Australia, U.K. and U.S.A. are not proportional to the number of subscribers in the three countries and this suggests that the length of subscriber's loop in the U.K. is less than in Australia and is substantially larger in the U.S.A. than in either —this is undoubtedly due to the large size of exchange areas in the U.S.A.

Figures were not obtained for Germany but the output of the F. & G. P.I.L.C. plant at Cologne is about 350,000 pair miles per year. This is not the total output of F. & G. as they have plants in other parts of Germany. A factory producing 350,000 pair miles is a large one by English and European cable industry standards but Australian factories have a comparable volume of output.

In both the U.S.A. and U.K. the estimating of material requirements is a major difficulty and no completely satisfactory means of doing so have yet been developed. Shortly before I was in the U.S.A. the President of the American Telephone & Telegraph Co. had become so concerned with inaccuracies in forecasts, particularly under-estimates and subsequent shortages, that he had written a personal instruction that material forecasts were to be scrutinised at the highest levels in the Operating Companies (i.e. our State Administrations).

Both the B.P.O. and Bundespost work on negotiated contracts and the administrative machinery for placing orders is simpler than with the public tender system used in Australia. In the Bell System, the Western Electric Co. fulfils the role of Supplies organisation, Stores Branch and major manufacturer and public tender as we know it is not used. There are no administrative or funds difficulties in ordering material quickly. Material is manufactured in Western Electric Co. factories or bought by the Company from outside suppliers to W.E. specifications. Stocks are held at warehouses located at suitable points throughout the country from which the Operating Companies draw as required. Although Western Electric Co. is part of the Bell organisation, it is required to show a profit in its own right and consequently seeks to maintain minimum stock holdings consistent with the ability to supply any item on demand. The inability to supply an item means loss of profit on its sale to the Operating Company as well as the administrative penalties which the System will enforce if the Operating Company is unable to provide service for this reason.

The Bell System uses "long-term estimates" and "short-term estimates" of material requirements. These estimates originate in the Operating Company. "Long-term estimates" cover major works material such as switching plant and large cables which are normally supplied from the factory direct to the job. "Short-term estimates" cover day-to-day requirements of plant items, telephones, pole hardware and the like which are carried in the Western Electric Co. warehouses to meet demands from the Operating Company in the same way as the Stores Branch carries stocks to meet Engineering Division demands.

http://doi.org/10.18080/ajtde.v6n4.164

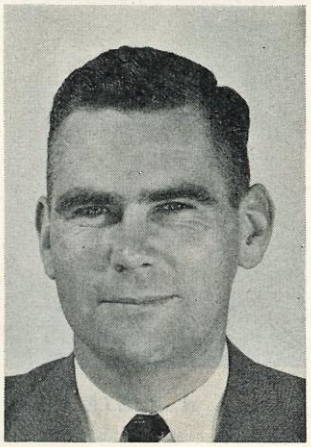
The short-term estimates are prepared at 3 monthly intervals covering a period 6 months ahead and they cover about 80 "key items" from which are computed the requirements for all items of this type. Statistics of past usage of all items of plant are held by the Western Electric Co. and from them have been prepared tables of usage showing the quantities of all general items required to match the forecasted requirement of key items. However, should the Operating Company expect that for some reason the usage of certain general items will be out of balance with the associated key items then the Western Electric Co. must be notified. The estimate, together with details of stock on hand and estimate recoveries, is forwarded by the warehouse to the W.E. headquarters in New York where it is analysed and a proposed delivery schedule prepared for all items required in the period. This delivery schedule is referred to the region where it is available for examination and approval by both the warehouse and the Telephone Company. It will be noted that the arrangement is similar to the Australian one, except for the accumulation and analysis of data over a lengthy period, which has enabled a few key items to be confidently adopted as a basis for computing material requirements.

THE BELL SYSTEM AND SERVICE TO THE PUBLIC

A strong impression is gained of the desire of the Bell System to serve the public in every possible way. This appears to be typical of American business in such public services as restaurants, shops, etc., where there appears to be a genuine desire to provide good service and it is, undoubtedly, part of the American business philosophy. But the emphasis on service appeared to run deeper in the case of Bell than the normal desire to provide good service for good profit. In fact, the Bell System impresses as having a deep sense of responsibility to the public quite apart from any question of profit.

An impressive example is the efforts just discussed to provide subscribers' telephone service at short notice. Two other items that impressed were the bell on their standard subscribers' telephone and their public telephone set. The bell has a deep melodious ring which can be adjusted for volume from almost silent to a loud clamour. As anyone with a young family knows, this is a valuable feature in a telephone which is also of assistance to the Administration as the subscriber is not tempted to leave the handset off to prevent the bell ringing and disturbing the household. The public telephone had 3 coin slots and no buttons and was simple and easy for the customer to use. By comparison, the 4d. tariff creates an inconvenience because the weight of four pennies is such that an average person may not have four of them in his possession when he wants to make a call from a public telephone and is less likely still to have a further four available if the first call is ineffective. This trouble particularly arises due to the large size of Australian coins compared to American; it is the type of problem which the Bell System would give serious attention to.

It could be stated that the Bell System is "customer orientated" and their whole organisation and outlook is developed so that customers' needs are met speedily and promptly. Although there is an awareness in Australia of this need, the organisation is not geared to meet the customers' requirements so much as to provide administrative efficiency and it could well be re-examined from this point of view.



D. P. BRADLEY

D. P. BRADLEY, author of the article "Impressions of an Overseas Visit by a Lines Engineer", has been a Sectional Engineer in the Lines Section, Central Office, for the last six years, initially in the Works Programme and Material Design Group and currently in Works Methods and Practices. His present duties include preparing the Linemen's magazine, "On the Line". He was trained as a Cadet Engineer in Victoria and worked in that State and Western Australia, where he was Divisional Engineer, Northern Division, before coming to Central Office.

Mr. Bradley holds the degrees of Bachelor of Science and Bachelor of Commerce from the University of Melbourne and is an Associate Member of the Institution of Engineers, Australia, and an Editor of this Journal. This article is his third contribution to the Journal.

http://doi.org/10.18080/ajtde.v6n4.164

Flow-level Load Balancing of HTTP Traffic using OpenFlow

Anees Al-Najjar
School of ITEE, The University of Queensland, Brisbane, Australia

Siamak Layeghy
School of ITEE, The University of Queensland, Brisbane, Australia

Marius Portmann
School of ITEE, The University of Queensland, Brisbane, Australia

Jadwiga Indulska
School of ITEE, The University of Queensland, Brisbane, Australia

Abstract: In this paper, we explore the concept of flow-based load balancing of network traffic on multi-homed hosts. In contrast to existing approaches such as MultipathTCP, our approach is a client-side-only solution, and can therefore easily be deployed. We specifically explore flow-based load balancing for web and video traffic use cases. Experimental evaluations of our OpenFlow-based load balancer demonstrate the potential of flow-based load balancing.

Keywords: Software Defined Networking, Load Balancing, Multi-homed Devices, Web Traffic Optimisation, Video Streaming Traffic

1. Introduction

Computing devices are increasingly equipped with multiple network interfaces, e.g. LTE and WiFi in the case of smartphones. Efficiently using multiple network interfaces on such multi-homed hosts is a challenging problem. Approaches such as Multipath TCP (MPTCP) (Ford, Raiciu, Handley & Bonaventure,2015) allow load balancing of traffic across multiple links and paths on a per-packet granularity. The problem with MPTCP is that it requires both ends, i.e. client and server, of the end-to-end path to support the protocol. Despite the many years since the introduction of MPTCP, its deployment and use are minimal with a few notable exceptions, such as Apple's Siri, as stated in https://support.apple.com/en-au/HT201373.

In contrast, we consider a client-side only approach to load balancing across multiple network interfaces, which does not require any special support from the server. In this approach, load

http://doi.org/10.18080/ajtde.v6n4.166

balancing at the level of granularity of packets is not possible, due to the fact that TCP connections are bound to IP addresses and hence host interfaces. Thus, we do not consider approaches such as Mobile IP (Perkins, 2002), Host Identity Protocol (HIP) (Moskowitz, Nikander, Jokela & Henderson, 2010) or Site Multihoming by IPv6 Intermediation (Shim6) (Abley, Black & Gill, 2003) here, due to their limited adoption. Instead, we consider a practical, flow-based load balancing approach, where the level of granularity for distributing network traffic is network flows, e.g. TCP connections. We discussed the basic idea of this approach and its preliminary implementation using Software Defined Networking and OpenFlow in Al-Najjar, Layeghy & Portmann (2016). Our initial evaluations in Al-Najjar, Layeghy & Portmann (2016) showed the potential and practicality of this approach. However, it was limited in regard to the considered network traffic (download of identical, fixed size files) as well as the considered network links with static link capacity.

In this paper, we investigate the potential of flow-based load balancing on multi-homed hosts in a realistic setting. We specifically focus on Web and video traffic, due to their predominance and relevance for overall quality of user experience.

The potential of flow-based load balancing depends on the characteristics of the network traffic, e.g. the number, size distribution, and level of concurrence of flows. In the extreme case, we could have a web page that is downloaded via a single TCP connection. In our approach, this flow would be allocated to a single interface, and there would be no potential gain for load balancing and using the other available network interface and corresponding path.

It is therefore important to understand the characteristic of Web traffic in regards to network flows. We have performed extensive measurements and analysis of the web traffic for HTTP(s)/TCP connections, based on the Alexa top 100 web pages (Alexa, n.d.). Our analysis shows that typical websites require a large number of flows (typically TCP connections), which shows there is a potential for flow-based load balancing to improve the download performance and user experience.

We also investigated controlling the HTTP traffic in SDN-based multi-homed devices over the QUIC (Quick UDP Internet Connection) protocol. QUIC is a relatively new transport-layer protocol specifically designed for web traffic (Roskind, 2013). Like TCP, QUIC is also connection-oriented. QUIC carries about 7% of the global Internet traffic and 30% of Google traffic (Langley *et al.*, 2017), and is becoming increasingly relevant.

In addition to web traffic, this paper also considers controlling the flow of video traffic. Dynamic Adaptive Streaming over HTTP (DASH) (ISO, 2014) traffic running over the QUIC protocol will be considered in our use case. Because DASH traffic is considered as a single TCP

http://doi.org/10.18080/ajtde.v6n4.166

or UDP flow and that flow is only allocated to a single network interface, it is not as amenable to flow-based load balancing as is web traffic. However, we consider the scenario of having video streams as background traffic, and investigate how this impacts on the efficiency of our SDN-based traffic load balancing approach for web traffic in multi-homed devices.

Our experimental evaluation of flow-based load balancing is based on an implementation using an OpenFlow Software Switch, Open vSwitch (OVS), and the Ryu SDN controller. For our experiments, we consider the realistic and practical scenario of a dual-home host, with both an LTE and a WiFi interface. We performed extensive measurements where we established the simultaneous and co-located link capacity of LTE and WiFi interfaces at our university campus. We then used these realistic link capacity measurements for our experiments, using link emulation.

Our results show that flow-based load balancing can significantly reduce the page load time, for the realistic and practical traffic and link scenario that we considered. Somewhat surprisingly, it even outperforms MPTCP.

The rest of this paper is organised as follows. Section 2 gives a brief background on the concept of SDN and OpenFlow, MPTCP and QUIC. Section 3 explains the idea of flow-based load balancing as well as our implementation. In Section 4, we present our analysis of web traffic and its potential for flow-based load balancing. Sections 5 and 6 present our experimental evaluation of flow-based load balancing, for two different link capacity scenarios. Finally, Section 7 discusses related works, and Section 8 concludes the paper.

2. Background

2.1. OpenFlow

Since our flow-based load balancer is implemented in SDN using OpenFlow, we provide a brief introduction to the relevant key concepts.

In Software Defined Networks (SDN), a key idea is the separation of control and data plane. The SDN architecture with its three layers (infrastructure, control and application) is shown in Figure 1. The logically centralised SDN controller configures the forwarding behaviour of forwarding elements (SDN switches) via a *southbound interface*.

http://doi.org/10.18080/ajtde.v6n4.166

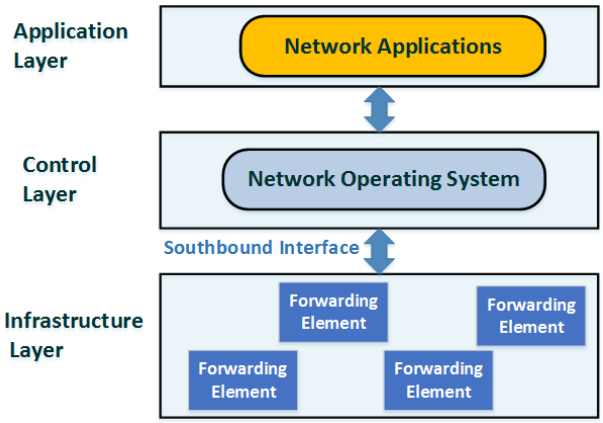


Figure 1. SDN Architecture

The OpenFlow protocol (McKeown *et al.*, 2008) proposed by Open Networking Foundation (available on https://www.opennetworking.org/) is the dominant SDN southbound interface. It allows the controller to install forwarding rules using a *match-action* paradigm. The rules can match on various L2-L4 header fields, including MAC and IP addresses, as well as the ingress port via which the packet was received.

OpenFlow supports different types of actions. The *output* action allows the switch to forward packets via a specific port. OpenFlow also supports a *set-field* action which allows rewriting of packet header fields. This is typically used for functions such as Network Address Translation (NAT).

The interaction between the SDN controller and switches occurs via OpenFlow messages. A switch can encapsulate and send a data packet to the controller via an OpenFlow *Packet-in* message. The controller can send a packet to the switch via a *Packet-out*, with instructions (a set of actions) on how to handle the packet. The controller also can install forwarding or flow rules on switches via OpenFlow *Flow-Mod* messages.

The OpenFlow protocol provides messages that allow querying statistics from switches in regard to links, ports and flows. *Port Stats* is one of these message groups. The controller requests statistics of active ports by sending a *PortStatsRequest* message. The switch replies with a *PortStatsReply* message, carrying a set of statistics related to each port, such as the cumulative number of sent and received packets and bytes, as well as the number of packets that have been dropped or had errors.

Flow Stats is another type of OpenFlow probing message type. It allows collecting statistics of the active flow entries (forwarding rules) in the switch. The controller requests this information via sending a *FlowStatsRequest* message, upon which the switch replies with a *FlowStatsReply* message. The message contains information related to each installed rule, for instance table_id, priority, number of bytes/packets that matched the rule, the active duration of the flow, and the match/action fields.

http://doi.org/10.18080/ajtde.v6n4.166

Our flow-based load balancer, which will be discussed in detail in this paper, was implemented using these basic OpenFlow primitives.

2.2. MPTCP

Multi-Path TCP (MPTCP) is one of the current approaches for sending traffic across multiple network interfaces and paths on multi-homed hosts (Ford *et al.*, 2015). We briefly explain MPTCP, since we will use it as a benchmark against our proposed approach. However, this is a somewhat unfair comparison, since MPTCP requires support on both ends of the communication path, which is a key reason for the very slow and minimal adoption of MPTCP. In contrast, our proposal is a client-side only solution, which makes deployment very easy.

MPTCP adds a layer between the Application and Transport layers in the TCP/IP protocol stack, as shown in Figure 2. It creates multiple TCP subflows that can be sent via multiple different network paths. As mentioned, MPTCP requires support from both connection sides (the client and the server). If the server does not support MPTCP, the protocol will fall back to basic TCP.

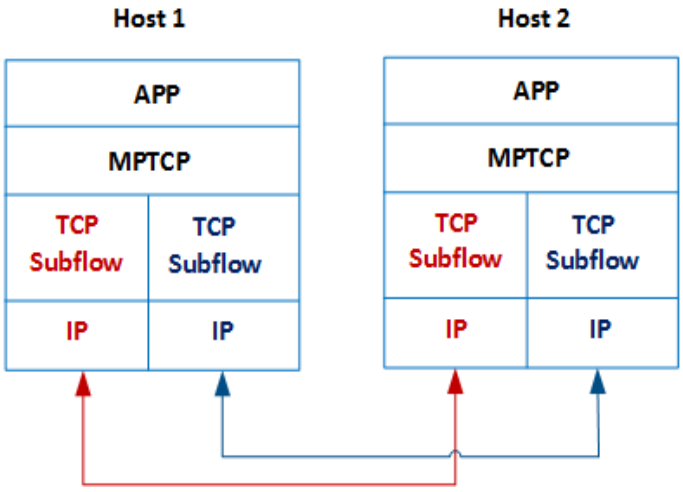


Figure 2. MPTCP Protocol

To establish an MPTCP connection, a host uses the normal TCP handshaking packets represented by SYN, SYN/ACK, and ACK with an additional option. This **MP_CAPABLE** option allows checking if both ends support MPTCP and, if not, the connection falls back to a normal TCP connection. In the case where MPTCP is supported by both client and server, a 64-bit authentication key is generated and exchanged. The keys are required in the next stages for creating and authenticating TCP subflows. Once both ends confirm supporting MPTCP, and authentication keys have been exchanged, a new TCP subflow can be initiated. Each MPTCP subflow also uses the same TCP handshaking packets with an MP_JOIN option. The option contains a number of flags and the address ID of the corresponding host.

http://doi.org/10.18080/ajtde.v6n4.166

MPTCP allocates network traffic among multiple network interfaces at the level of granularity of TCP segments. This is in contrast to our approach, where the level of granularity is limited to flows. As a result, one would expect MPTCP to outperform our flow-based approach. Based on our experiments, this is not the case. This can be explained by limitations of MPTCP that have been identified in previous work (Chen *et al.*, 2013).

2.3. QUIC Protocol

The QUIC protocol has been proposed by Google in order to overcome some of the limitations of TCP, specifically when used in conjunction with HTTP traffic (Langley *et al.*, 2017).

QUIC runs on top of UDP, making it easy to be deployed and updated. Figure 3 shows the architecture of HTTP2 over QUIC compared with HTTP2 over a TCP connection (Langley *et al.*, 2017; Cui *et al.*, 2017).

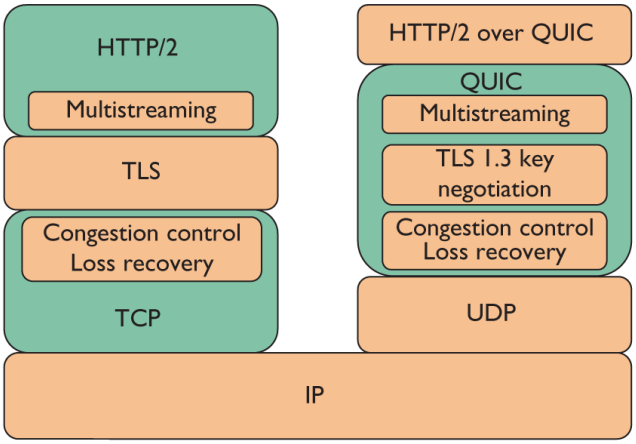


Figure 3. HTTP2 over QUIC vs HTTP2 over TCP (Cui *et al.*, 2017).

The QUIC protocol not just supports multi-stream multiplexing for HTTP traffic, like HTTP/2 over TCP, but also overcomes data delivery issues related with this type of multi-streaming. The HTTP/2 over TCP protocol multiplexes the data units related to a certain server into multiple streams carried via one connection. Delivering those streams is done in a sequential manner and, when loss happens, this stream will block the others, causing "head-of-line blocking". In contrast, the QUIC packets consist of multiple frames. Each frame encompasses stream frames resulting from multiplexing data units. If loss happens in a stream frame, the other frames will not be affected by that loss. This type of concurrent delivery can mitigate the aforementioned problem with TCP. QUIC also supports security, such as provided via TLS in HTTP. The simpler and more efficient connection establishment of QUIC, in contrast to TCP/TLS, is shown in Figure 4 (Cui *et al.*, 2017).We will consider the QUIC protocol in the experimental evaluation of our flow-based load balancing approach.

http://doi.org/10.18080/ajtde.v6n4.166

3. Flow-based Load Balancing

In this section, we briefly discuss the architecture of our flow-based load balancing system, and its implementation using OpenFlow. The overall idea is that, for each new flow (e.g. TCP or QUIC/UDP connection) initiated by the client, the SDN controller will decide to which network interface it will be allocated. Once a flow is allocated to an interface, all the corresponding packets will be sent via that interface. Changing the interface mid-flow is very difficult, and requires approaches such as Mobile IP, Shim6, HIP, etc. that are avoided in this work for the sake of simplicity and ease of deployment.

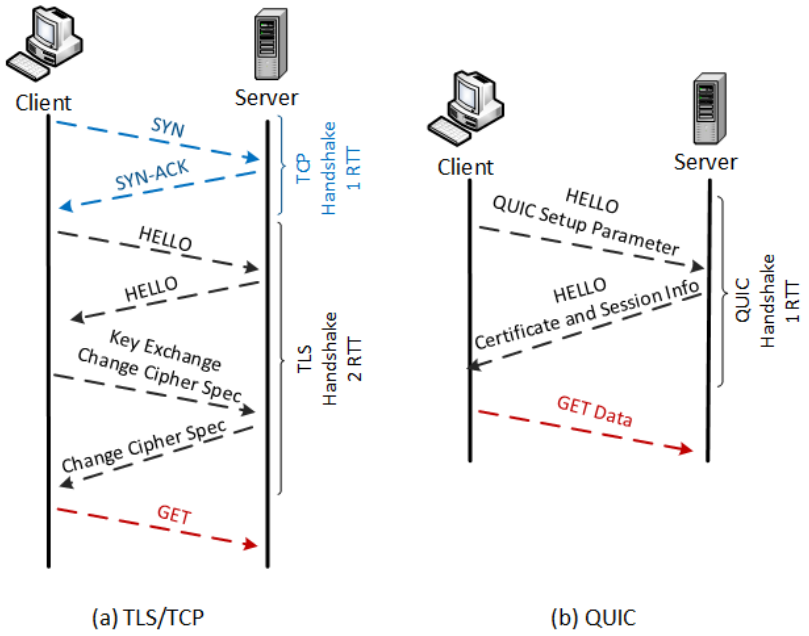


Figure 4. Handshaking of HTTP2 over TCP and QUIC protocols

The architecture of our system is shown in Figure 5. While we consider the scenario of two network interfaces, the approach works for any number of interfaces. The OpenFlow switch is bound to the two physical network interfaces, *eth0* and *eth1*. To provide it with the ability to switch network traffic across those interfaces in a way that is transparent to the application, we need to add a layer of indirection. We do this by adding a virtual interface pair (*veth0* and *veth1*). All application traffic is sent to *veth1*, via configuring the routing table. The OpenFlow switch can then control the forwarding of traffic from the application (entering the switch via *veth0*), via OpenFlow forwarding rules. In our implementation, these rules are installed by the SDN controller, which runs locally on the host.

http://doi.org/10.18080/ajtde.v6n4.166

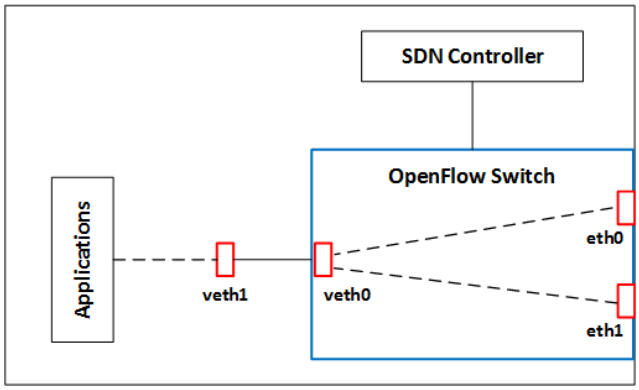


Figure 5. System Architecture

To enable transparent switching across different interfaces, we need to perform Network Address Translation (NAT), as well as ARP handling, discussed in more detail in Al-Najjar, Layeghy & Portmann (2016).

In our implementation, we used Open vSwitch (available on http://open-vswitch.org/download/) version 2.4 as our switch, and Ryu (available on http://osrg.github.io/ryu/) as our SDN controller.

3.1. Detecting and Controlling Flows

Web traffic can be transmitted over TCP or QUIC/UDP. This section discusses how new flows are detected and allocated to a particular network interface.

In the case of TCP, new flows are detected as follows. When the first packet of a new flow (i.e. TCP SYN packet) arrives at the OpenFlow switch, it will not match an existing forwarding rule, and hence it is forwarded to the controller via an OpenFlow *Packet-In* message. At this point, the controller can check that this is indeed the first packet of a new TCP connection, i.e. that the SYN flag is set. In OpenFlow version 1.3, which is used for our implementation, matching cannot be made on TCP flags, so this check can only be done at the controller. From OpenFlow version 1.5, matching on TCP flags is supported, and this can be done at the switch.

At this point, the controller decides which interface to allocate this flow to, based on the particular load balancing algorithm that is used, which will be discussed in the following section. The same basic approach is used to detect new QUIC/UDP flows, but with the additional filtering for UDP destination port 443, which is the port number allocated for QUIC servers.

Once the decision of allocating the flow (TCP or QUIC) to the specific network interface has been made, the controller installs a corresponding forwarding rule on the switch, which then sends all the packets belonging to this flow via the chosen interface, and performs the corresponding address rewriting operations. The OpenFlow match fields consist of the 5-tuple

http://doi.org/10.18080/ajtde.v6n4.166

of IP source and destination address, source and destination port number, as well as type of transport layer protocol.

3.2. Load Balancing Algorithm

To allocate network flows across multiple network interfaces, we use a *Weighted Round Robin (WRR)* load balancing algorithm, which allocates the number of flows to interfaces in proportion to their respective link capacity. To estimate the capacity of the different links in the context of SDN and OpenFlow, we utilise an active probing methodology that we have introduced in one of our previous works (Al-Najjar *et al.*, 2016). Unfortunately, this allocation can only be based on the number of flows, and does not consider the size of different flows. This is due to the fact that the flow allocation decision needs to be made when the first packet of a flow, e.g. a TCP SYN packet, is seen by the controller. Future work could potentially consider flow size estimation, to further improve the efficiency of the algorithm. However, as we will see, our flow based Weighted Round Robin algorithm considering the number of flows performs very well, due to the relatively large number of flows and their reasonably well-behaved size distribution, as discussed in the following section.

4. Web Traffic Flow Analysis

Since our load balancing approach is limited to the granularity of flows, its potential for performance improvement depends on the characteristics of the traffic in regard to flow availability and distribution. As mentioned before, in the extreme case of an application using a single large flow, flow-based load balancing cannot provide any benefit.

Since our focus is on web traffic, we performed an experimental analysis of typical websites with regard to their flow characteristics. Our methodology and results are discussed in the following.

For our analysis, we considered the top 100 Alexa websites. We downloaded the content of each website (main page) via a Python script using the Selenium WebDriver API (described on https://github.com/SeleniumHQ/selenium/), using HTTP/1.1. We disabled cookies as well as caching. All the traffic was captured as a pcap file, and the Tshark tool (Combs, 2012) (version 1.12.1) was used to analyse the data.

As a first result, Figure 6 shows the distribution of the number of flows for the 100 websites. We see a relatively long-tailed distribution, with a significant number of websites using more than 30 flows.

http://doi.org/10.18080/ajtde.v6n4.166

Based on our analysis, news sites tend to have a particularly large number of flows. Examples include *msn.com*, *theguardian.com*, *sohu.com*, and *sina.com*, with 151, 169, 207, and 281 flows, respectively. The average number of flows is around 42.

Overall, these results are encouraging for the potential of flow-based load balancing.

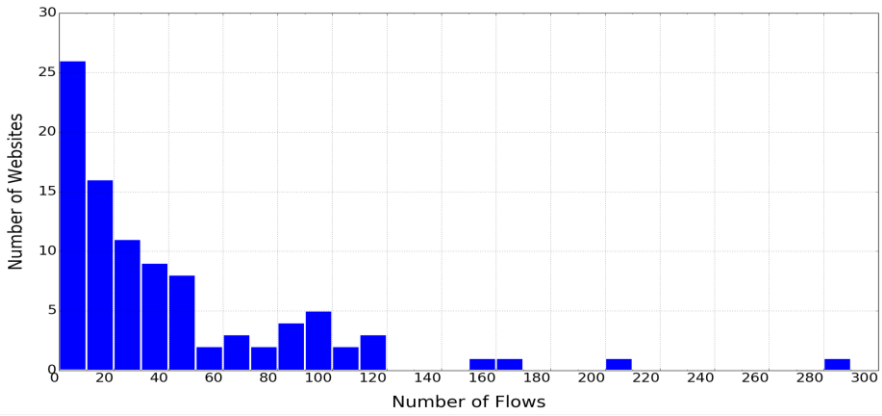


Figure 6. Alexa Top 100 Websites Flows Histogram

We also considered the size of the flows, and Figure 7 shows the distribution of flow sizes in kilobytes, using a log scale on the y-axis. We can see that, while the majority of flows are a few hundred KB or less, there are a small number of outliers, with the largest flow size close to 5MB.

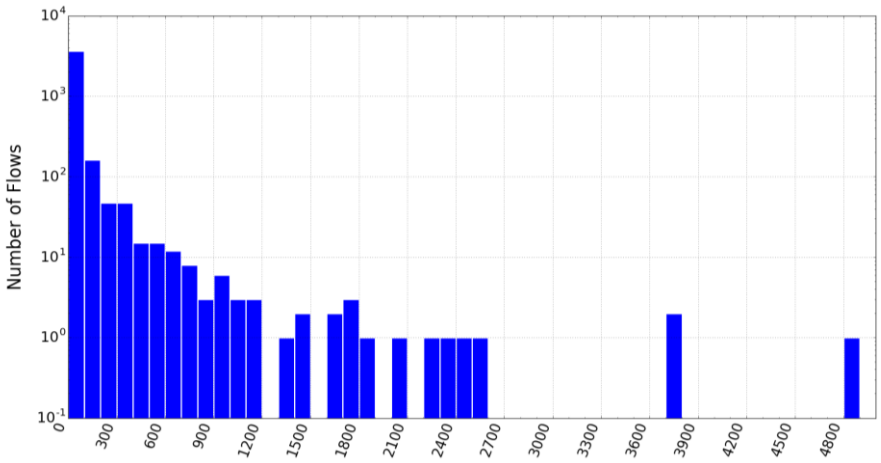


Figure 7. Alexa Flows Sizes

In summary, the distribution of flow numbers and sizes per website indicates that flow-based load balancing has the potential to deliver a performance gain, i.e. achieve a reduced page load time. We will further explore this via experiments in the following sections.

5. Load Balancing Experiment — Static Link Capacity

To evaluate the potential of flow-based load balancing for the web browsing use case, we initially performed an experiment using a scenario with a static link capacity.

http://doi.org/10.18080/ajtde.v6n4.166

Figure 8 shows the topology of our test-bed. The end-host is dual-homed and is connected to two gateways, *GW1* and *GW2*, that are connected to a physical gateway (GW) which provides connectivity to the Internet and provides access to the Alexa top 100 websites. The nodes were implemented as virtual machines (with Ubuntu Linux version 3.13.0-24 OS) and the whole topology was emulated using GNS3, a network emulation software available on https://www.gns3.com/. This will make sure that the last hop link presents the bottleneck in the end-to-end path, and should allow our load balancing approach to perform well.

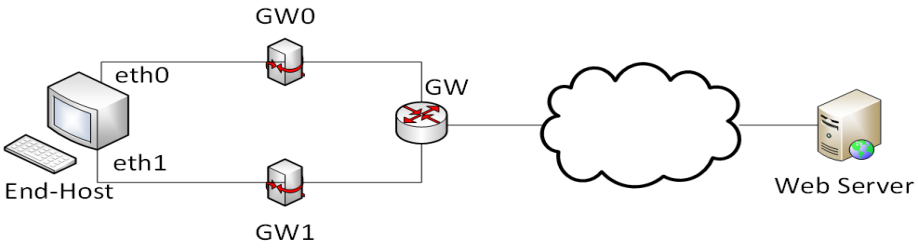


Figure 8. The Proposed Load Balancing Topology

As a performance metric, we use the page load time (PLT) (Wang & Jain, 2012), i.e. the time from when the first HTTP GET Request is sent, until the page is completely loaded. We again used the Selenium Webdriver API, along with Chromium (v58.0.3029.110), to measure the PLT for all the Alexa top 100 websites.

The static link capacity scenario is evaluated with HTTP traffic over TCP and QUIC/UDP.

5.1 Web Traffic over TCP

In this experiment, we measured the page load time (PLT) for each of the Alexa top 100 webpages 10 times, and took the average as our performance metric. We used the weighted round robin (WRR) load balancing algorithm, as discussed above, to allocate flows to the two interfaces considered in our experimental scenario. As a reference, we also measured the PLT for the single-interface case as well.

Figure 9 shows the cumulative density function (CDF) of the PLT parameter for all 100 websites. The figure clearly shows the advantage of the flow-based load balancing method. For example, in the single interface case, 50% of all page downloads are completed in under 12 seconds. In contrast, using both interfaces via flow-based load balancing, 50% of all downloads are completed in under 7.5 seconds. Overall, using both interfaces via flow-based load balancing achieves a reduction of the average page load time by almost 37%. This is a respectable improvement, considering the theoretical maximum is a reduction of 50%, and that we are working with a very coarse grained level of granularity, i.e. flows rather than packets.

http://doi.org/10.18080/ajtde.v6n4.166

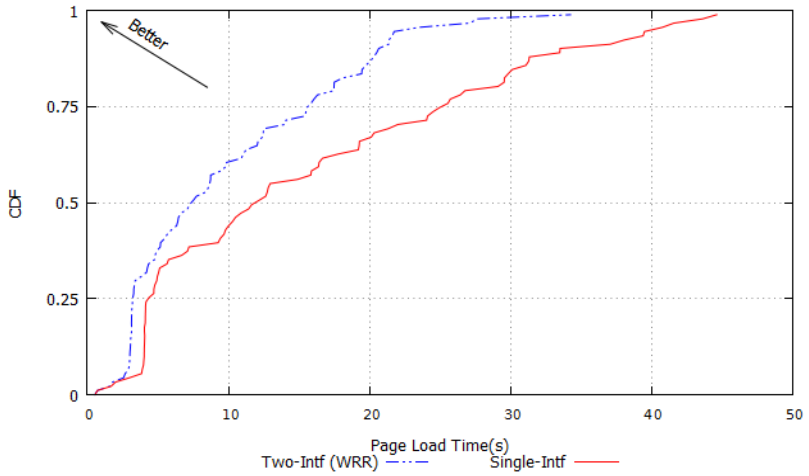


Figure 9. CDF of PLT for Static Link Capacity Scenario

We wanted to compare our flow-based load balancing approach with MPTCP, even though this is a somewhat unfair comparison. We expect MPTCP to perform significantly better, since it is able to perform load balancing on a packet-by-packet basis. On the flip side, it requires both ends to the communication path to be upgraded to support the mechanism. In contrast, our approach is a purely client-side approach, and therefore easy to deploy.

Unfortunately, none of the Alexa top 100 websites that we considered supported MPTCP. The only website that we were able to find that supports MPTCP was, somewhat ironically, mptcp.org (Paasch, *et al.*, 2013). For this measurement, we used the Linux kernel implementation of MPTCP (v.090), with the default parameter settings, as in (Paasch *et al.*, 2013).

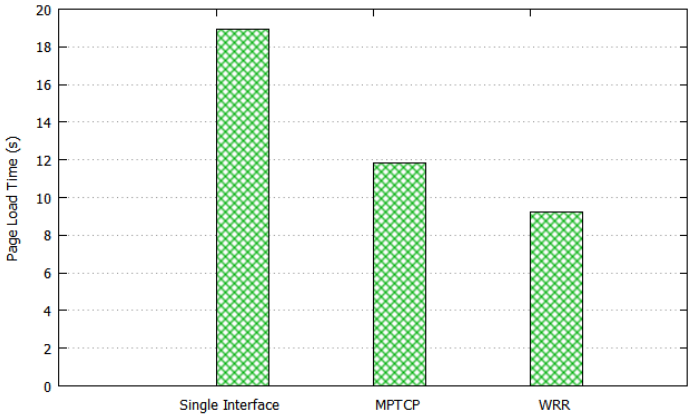


Figure 10. Mean PLT for Web Traffic over TCP (Static Link Capacity Scenario)

Figure 10 shows the page load time of mptcp.org, for three different cases: single-interface, MPTCP and flow-based weighted round robin (WRR) load balancing. Compared with the single-interface case, MPTCP reduces the page load time by 37%. Surprisingly, flow-based load balancing (WRR) clearly outperforms MPTCP and achieves a PLT reduction of 51%. Our investigations showed that MPTCP achieves a very uneven allocation of traffic across the two equal-capacity paths, with 1.3 MB of traffic sent across *etho* (see Figure 8) and only 130KB

http://doi.org/10.18080/ajtde.v6n4.166

sent across *eth1*. Another potential reason for MTPCP's relatively poor performance is its limitations in dealing with small flows, as reported in (Nikravesh *et al.*, 2016).

5.2 Web Traffic over QUIC/UDP

As previously mentioned, QUIC is a protocol developed by Google and is hence supported mostly by Google products (e.g. Chrome and Chromium browsers), as well as Google services (Google search engine and YouTube servers). In order to run QUIC, both communication end-points, i.e. the client and the server, need to support the protocol. In our experiments, we activated QUIC by enabling the "-enable-quic" option on the Chromium browser, using the Selenium API. The evaluation was done via two scenarios, with only web (HTTP) traffic, and another one with simultaneous web and video traffic.5.2.1 Web Traffic Only.

This scenario is about evaluating the control and load balancing of web traffic over the QUIC protocol. Given the limited support of QUIC on web servers, we used the YouTube main page. We loaded the page 10 times, and recorded the average page load time (PLT). We compared the results of our WRR-based load balancing approach with the scenario with a single interface only.

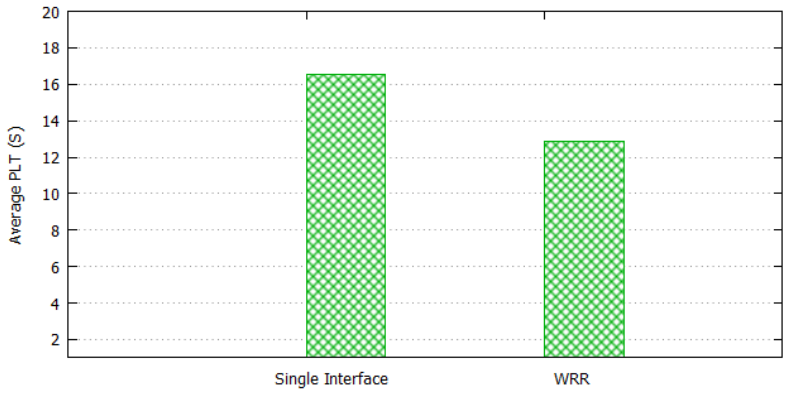


Figure 11. Mean PLT for Web Traffic over QUIC/UDP (Static Link Capacity Scenario)

Figure 11 shows the results. We can see that our WRR-based algorithm decreases the average page load time by around 30% compared to the benchmark scenario with a single interface only. While the benefits of our SDN-based load balancing approach are not quite as big as in the case of MPTCP, this experiment shows that it can still achieve a significant improvement when using the QUIC/UDP protocol.

5.2.2 Simultaneous Web and Video Traffic

Recently, multi-homed devices have allowed users to utilise multiple applications simultaneously. For instance, gadgets with decent operating systems, such as Android, offer a feature of having multi-window usage to their users. It is common to surf a website via a window while streaming a video through another window. Therefore, we adopt that scenario

http://doi.org/10.18080/ajtde.v6n4.166

to evaluate different application traffic types using our proposed system. The traffic to be evaluated is not only short-lived flows (such as webpage traffic), but also long-lived flows (e.g. DASH video traffic).

In this scenario, we consider the simultaneous flow of web and video traffic. This is an increasingly realistic and common scenario, with recent versions of Android supporting a multi-window feature, which allows users to watch a video in one browser window, while browsing a range of web pages in another window. To consider this scenario in our experiments, we used two Chromium browser windows. In the first one, we loaded the landing pages of the Alexa top 100 web sites and measured the page load time (PLT). In the other browser window, we continuously streamed a short video loaded from YouTube using the DASH (Dynamic Adaptive Streaming over HTTP) protocol, running over QUIC. The Big Buck Bunny video (available on https://www.youtube.com/watch?v=03-17GUAfNU) used in the experiment is 3 minutes long and encoded at a rate of 1 Mbps.

Our analysis using Wireshark showed the video traffic is transmitted as a single QUIC/UDP flow, as expected. This does not allow any load balancing of the video traffic across multiple interfaces. Instead, we can consider the video stream as background traffic for the simultaneously occurring web flows. Our experiments aimed to investigate the interaction between the two types of flows, and the overall performance of our flow-based traffic control and load balancing approach. Since DASH uses adaptive video encoding depending on the available bandwidth (Huang *et al.*, 2012 Akhshabi, Begen & Dovrolis, 2011), we also monitored the transmission rate of the video streams, by regularly polling the SDN switch via OpenFlow Flow Stats messages. The measured video transmission rate, or throughput, can be used as an indicator of the quality of the video, as viewed by the user. Figure 12 shows the average page load time (PLT) for the top 100 Alexa webpages for our weighted round robin (WRR) based load balancing approach, as well as the single interface scenario as a reference. We can see that, even with the video traffic in the background competing with the web traffic, our load balancing approach achieves a reduction in PLT of around 22% compared to the case where we only use a single interface.

We also considered the throughput of video traffic streamed concurrently with loading the webpages. Figure 13 shows the achieved throughput of video traffic, which is an indicator of the video QoS experienced by the end user. The figure shows three results: the video throughput achieved if we only use a single interface; the throughput achieved when using our WRR-based load balancing approach; and the *Reference* case, where there is no web traffic and video traffic has exclusive access to the available link capacity.

http://doi.org/10.18080/ajtde.v6n4.166

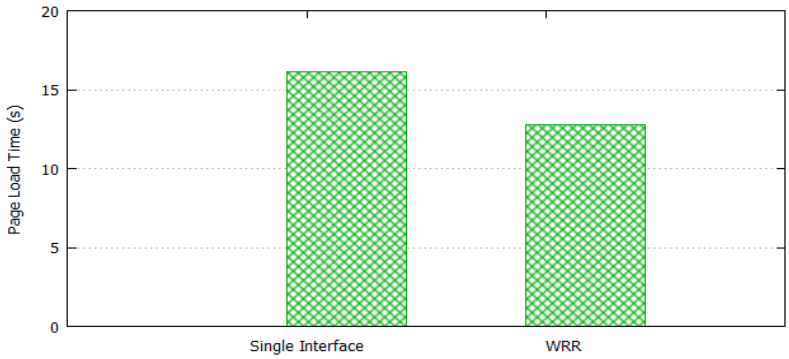


Figure 12. Mean PLT for Web and Video Traffic over QUIC/UDP (Static Link Capacity Scenario)

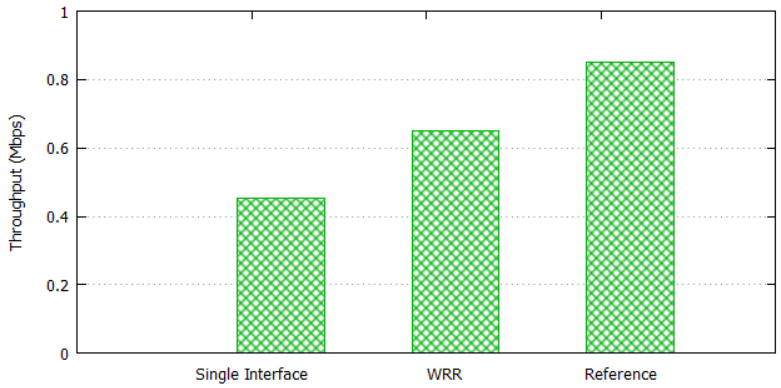


Figure 13. Throughput of Video Flows over QUIC/UDP (Static Link Capacity Scenario)

In summary, we can see that our load balancing mechanism strikes a good balance of handling competing web and video flows, and can achieve a significant reduction in page load time for web traffic, while increasing the video quality compared to the single interface case.

6. Load Balancing Experiment — Dynamic Link Capacity

In the previous section, we evaluated the concept of flow-based load balancing using a realistic traffic scenario of web-browsing. However, we considered the somewhat unrealistic scenario of static link capacities, which we used as a baseline case. In this section, we will consider a more realistic link bandwidth scenario. For this, we aim to use traffic traces from real wireless networks (WiFi and 4G) and then use these to emulate realistic links in our experiment.

While we were able to find a number of published papers and corresponding traffic traces for either WiFi or 3G/4G networks, such as in Netravali *et al.* (2015), we were not able to find any dataset which provides link bandwidth measurements for both WiFi and 3G/4G at the same time and location. However, this is exactly what we need, if we want to evaluate the potential of load balancing traffic across these types of networks.

To address this gap, we performed our own measurements. Our approach and the gathered data are discussed in the following section.

http://doi.org/10.18080/ajtde.v6n4.166

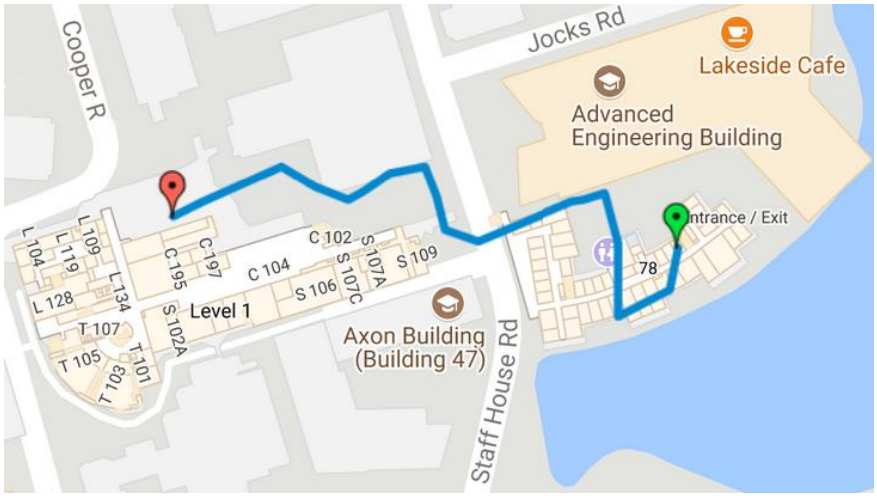


Figure 14. Bandwidth Measurement Path

6.1 WiFi and 4G/LTE Bandwidth Measurement

We performed our bandwidth measurements on the St Lucia campus of the University of Queensland (UQ). For this measurement, we walked across the campus while recording the link capacity of both the UQ WiFi network, as well as the Telstra 4G/LTE network, in 1 second intervals. The location of each measurement point was recorded using GPS. Figure 14 shows the path that was taken for our measurement. The path includes both indoor segments (starting inside building 78), as well as outdoor segments, giving a broad range of wireless link conditions. The duration of the measurement experiment is 400 seconds.

The bandwidth measurements were performed using iperf (available on https://iperf.fr/), with an iperf server running in our networking lab. located on campus. Given the high-speed campus network, it is safe to assume that our bandwidth measurement corresponds to the last-hop wireless link, since it is the path bottleneck.

For the experiment, we used two identical laptops (Dell Latitude E5470, Intel Core i5-2.3GHz, 8GB RAM, Ubuntu Linux 14.04), carried by the experimenter in a backpack. One laptop was equipped with a USB-based 4G/LTE modem (MF823). For the WiFi measurement, we used the laptop's built-in WiFi interface (Intel AC8260, 802.11a/g/n/ac).

For the iperf server, we used a Dell PowerEdge R320, Intel Xeon 2.2GHz, 32GB RAM, running the same version of Ubuntu Linux as on the laptops.

The measured bandwidth dataset is shown in Figure 15. We can see that, for the first 2 minutes of the measurements, network throughput is highly dynamic, with WiFi having a higher capacity up 160 Mbps, while LTE/4G has a capacity of well below 10 Mbps. This is as expected, since it corresponds to the indoor segment of the measurement path. For the rest of the measurement, taken outdoors, we see that 4G/LTE provides a relatively steady capacity of around 30 Mbps. In contrast, WiFi fluctuates highly and with mostly a lower capacity, and

http://doi.org/10.18080/ajtde.v6n4.166

with some sections that have no throughput at all. We will use this data set for link emulation in our flow-based load balancing experiments discussed below.

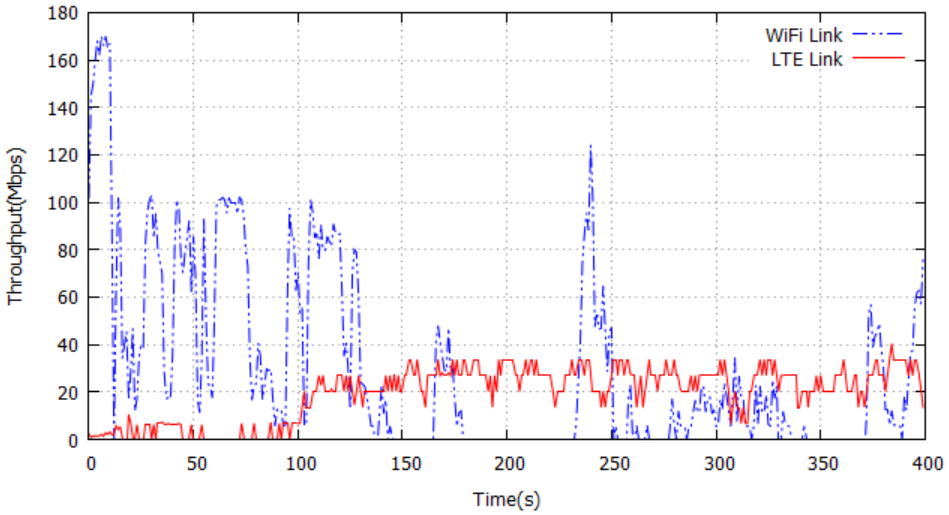


Figure 15. UQ Measured Bandwidth

6.2 Results

The testbed and scenario for this experiment are the same as discussed in Section 5 and shown in Figure 8. The only difference is that, instead of using a static link capacity for the two links (*eth0-GW0*, *eth1-GW1*), we now emulate the dynamic capacities of these links based on our measured data set (Figure 15). As before, we use the Linux *tc* tool for link emulation. Every second, *tc* is called with the corresponding link emulation parameter, i.e. bandwidth. In our scenario, link *eth0-GW0* corresponds to the WiFi link, and link *eth1-GW1* to the 4G/LTE link.

We again measure the page load time (PLT) for the Alexa top 100 websites.

In this experiment, we do this by continuously loading the same page for the entire 400 s duration of the experiments, and we record the average PLT for the period.

We considered three scenarios: using WiFi only; using 4G/LTE only; and using flow-based load balancing across both links. As in our initial experiment, we used a Weighted Round Robin (WRR) approach to load balancing. The difference in the dynamic case is that the weights are updated every second, based on the bandwidth data of the different links.

Figure 16 shows the CDF graph of the average page load time across all the 100 websites. The figure shows the results for the load balancing case (WRR) as well as for the two single-interface scenarios (LTE and WiFi). We can see that the load balancing (WRR) approach provides a significant reduction in page load time compared to both single-interface cases. For WRR, 50% of downloads are completed in under 3.9 s. The corresponding numbers for WiFi and LTE are 6.3 s and 4.8 s, respectively. Figure 17 further shows the mean PLT values for the three cases. We see that, for the single-link case, LTE achieves an average of 6.7 s, compared

http://doi.org/10.18080/ajtde.v6n4.166

to 8.6 s for WiFi. This is consistent with Figure 15, which shows that LTE has a consistently high bandwidth most of the time, compared to the more patchy performance of WiFi. Most importantly, we see that flow-based load balancing using simple weighted round robin (WRR) achieves a further reduction in PLT, with an average of 5.8 s. This represents an almost 33% reduction compared to WiFi, and a more than 13% improvement over LTE.

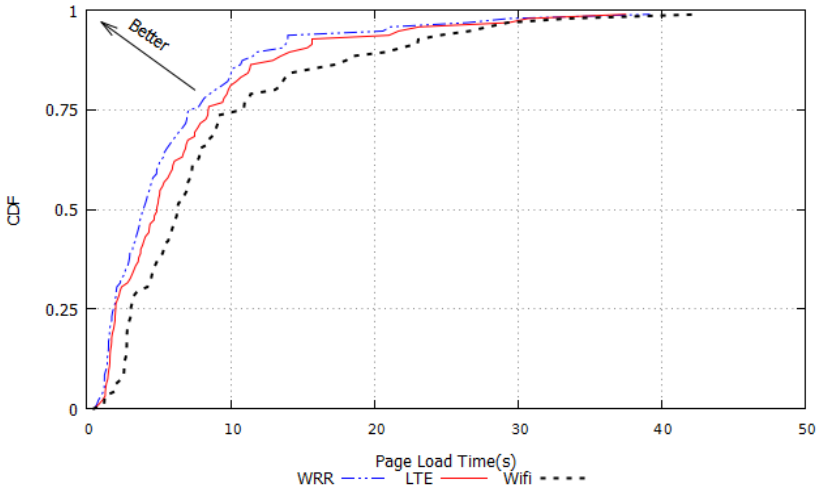


Figure 16. CDF of PLT for Web Traffic over TCP (Dynamic Link Capacity Scenario)

In summary, we have demonstrated that flow-based load balancing using simple weighted round robin has the potential to make efficient use of multiple network interfaces on end-hosts. Our experiments have shown this for the important use case of web traffic.

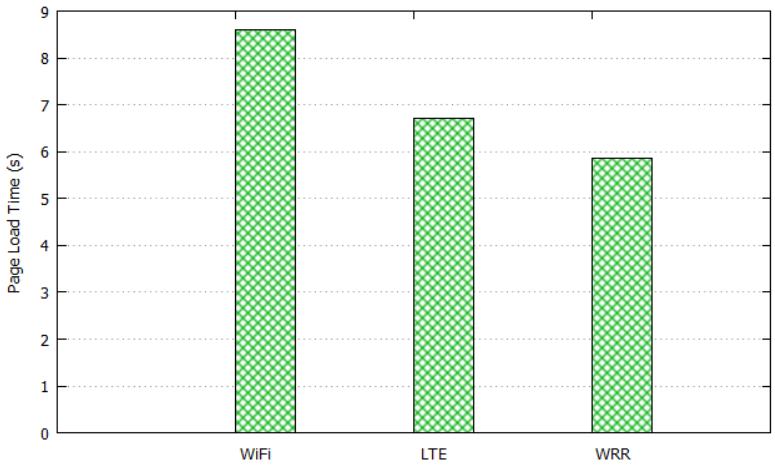


Figure 17. Mean PLT for Web Traffic over TCP (Dynamic Link Capacity Scenario)

7. Related Work

Probably the most well-known traditional approach to load balance traffic on multi-home hosts is MPTCP (Ford *et al.*, 2015). The protocol distributes TCP traffic over multiple network interfaces and end-to-end paths, and it can do this on a packet-by-packet basis. MPTCP requires deployment at both the client and server end, since it is not compatible with legacy TCP. As a result, MPTCP has achieved only limited adoption and deployment so far. Stream

http://doi.org/10.18080/ajtde.v6n4.166

Control Transmission Protocol (SCTP) (Stewart, 2007) is another transport layer protocol that supports multi-homing. Similar to MPTCP, SCTP requires support from both the client and server ends, and hence has found only very limited use. The key benefit of our flow-based load balancing approach is that it is a client-side only approach, which can easily be deployed. As a trade-off, the level of granularity is reduced (flow *vs* packet). Despite this, we demonstrated that our approach can outperform MPTCP for the web traffic use case.

A number of papers have proposed to use the SDN paradigm and OpenFlow to load balance network traffic. These works have mainly focused on load balancing in the network infrastructure and the server side (R. Wang *et al.*, 2011; Handigol *et al.*, 2009), which is in contrast to our approach.

The authors in Yap *et al.* (2012) use OpenFlow to control the network traffic in multi-homed Android hosts. The approach discusses different network functionalities, such as network hand-off, dynamic interface selection, and interface aggregation. However, the work does not address the specific problem of load balancing. Another point of difference is that the implementation of these functionalities requires support from both ends of the network path.

Another technology that allows using multiple network interfaces on end-hosts is Apple's Wi-Fi Assist, described on https://support.apple.com/en-au/HT205296, which switches to the cellular connection in case of a poor WiFi connection. This approach essentially does a vertical hand-off between the two networks, and does not allow for dynamically load balancing traffic and using both interfaces simultaneously. This is in contrast to the approach discussed in this paper.

8. Conclusions

In this paper, we have explored the concept of flow-based load balancing of network traffic across multiple interfaces on multi-homed hosts. The key benefit of this approach, compared to alternative solutions such as MPTCP, is that it is a client-side-only solution. Our approach demonstrates the capability to efficiently control and load balance HTTP flows over both TCP and QUIC/UDP. Our evaluation specifically focuses on the important use cases of web traffic, as well as simultaneous web and video traffic. Our analysis of the Alexa top 100 websites in regards to their flow distribution showed the potential for the concept of flow-based load balancing. We experimentally evaluated the concept via our OpenFlow-based implementation, considering static and realistic dynamic link capacity scenarios. Our results showed a significant performance improvement in terms of reduction in page load time, as well as increased throughput and quality of video traffic.

http://doi.org/10.18080/ajtde.v6n4.166

References

Abley, J; Black, B; Gill, V. 2003. 'Goals for IPv6 Site-Multihoming Architectures'. RFC 3582. Retrieved from https://tools.ietf.org/html/rfc3582

Akhshabi, S; Begen, AC; Dovrolis, C. 2011. 'An experimental evaluation of rate-adaptation algorithms in adaptive streaming over HTTP'. *Proceedings of the second annual ACM conference on multimedia systems*, pp. 157-168.

Alexa. n.d. 'The top 500 sites on the web'. Retrieved from, http://www.alexa.com/topsites/global/. Accessed 25 Jan 2017.

Al-Najjar, A; Layeghy, S; Portmann, M. 2016. 'Pushing SDN to the end-host, network load balancing using Openflow'. *2016 IEEE international conference on pervasive computing and communication workshops (percom workshops)*, pp. 1-6.

Al-Najjar, A; Pakzad, F; Layeghy, S; Portmann, M. 2016. 'Link capacity estimation in SDN-based end-hosts'. *Signal processing and communication systems (icspcs), 2016 10th international conference on*, pp. 1-8.

Chen, Y-C; Lim, Y.-S; Gibbens, RJ; Nahum, EM; Khalili, R; Towsley, D. 2013. 'A measurement-based study of multipath TCP performance over wireless networks'. *Proceedings of the 2013 conference on internet measurement conference*, pp. 455-468.

Combs, G. 2012. 'Tshark Dump and analyze network traffic'. Retrieved from https://www.wireshark.org/docs/man-pages/tshark.html

Cui, Y; Li, T; Liu, C; Wang, X; Kiihlewind, M. 2017. 'Innovating transport with QUIC: Design approaches and research challenges'. *IEEE Internet Computing*, *21* (2), pp. 72-76.

Ford, A; Raiciu, C; Handley, MJ; Bonaventure, O. 2015, October 14). 'TCP Extensions for Multipath Operation with Multiple Addresses'. RFC 6824. RFC Editor. Retrieved from https://www.rfc-editor.org/rfc/rfc6824.txt

Handigol, N; Seetharaman, S; Flajslik, M; McKeown, N; Johari, R. 2009. 'Plug-n-serve: Load-balancing web traffic using Openflow'. *ACM SIG-COMM Demo, 4* (5), p. 6.

Huang, T-Y; Handigol, N; Heller, B; McKeown, N; Johari, R. 2012. 'Confused, timid, and unstable: picking a video streaming rate is hard'. *Proceedings of the 2012 internet measurement conference*, pp. 225-238.

ISO. 2014. 'Information technology — Dynamic adaptive streaming over HTTP (DASH). Part 1: Media presentation description and segment formats' ISO/IEC 23009-1:2014, May. Retrieved from https://www.iso.org/standard/65274.html

http://doi.org/10.18080/ajtde.v6n4.166

Langley, A; Riddoch, A; Wilk, A; Vicente, A; Krasic, C; Zhang, D; *et al.* 2017. 'The QUIC transport protocol: Design and internet-scale deployment'. *Proceedings of the conference of the ACM special interest group on data communication*. pp. 183-196.

McKeown, N; Anderson, T; Balakrishnan, H; Parulkar, G; Peterson, L; Rexford, J; ... Turner, J. 2008. 'Openflow: enabling innovation in campus networks'. *ACM SIGCOMM Computer Communication Review*, *38*(2), pp. 69-74. doi: 10.1145/1355734.1355746

Moskowitz, R; Nikander, P; Jokela, P; Henderson, T; Heer, T. 2010. 'Host identity protocol', RFC 5201-bis. Retrieved from https://tools.ietf.org/html/draft-moskowitz-hip-rfc5201-bis-01

Netravali, R; Sivaraman, A; Das, S; Goyal, A; Winstein, K; Mickens, J; Balakrishnan, H. 2015. 'Mahimahi: Accurate record-and-replay for HTTP'. *Usenix annual technical conference*, pp. 417-429.

Nikravesh, A; Guo, Y; Qian, F; Mao, Z. M; Sen, S.(2016. 'An in-depth understanding of multipath TCP on mobile devices: Measurement and system design'. *Proceedings of the 22nd annual international conference on mobile computing and networking*, pp. 189-201.

Paasch, C; Barre, S; *et al.* 2013. 'Multipath TCP in the Linux kernel'. Available from https://www.multipath-tcp.org/

Perkins, C. 2002. 'IP mobility support for IPv4'. RFC 3344.

Roskind, J. 2013. 'QUIC (Quick UDP Internet Connections): Multiplexed stream transport over UDP'. *IETF-88 TSV Area Presentation*. Retrieved from https://www.ietf.org/proceedings/88/slides/slides-88-tsvarea-10.pdf

Stewart, R. 2007. 'Stream control transmission protocol', RFC 4960. Retrieved from https://tools.ietf.org/html/rfc4960

Wang, R; Butnariu, D; Rexford, J. 2011. 'Openflow-based server load balancing gone wild'. *Hot-ICE'11: Proceedings of the 11th USENIX conference on Hot topics in management of internet, cloud, and enterprise networks and services*, p. 12.

Wang, Z; Jain, A. 2012. 'Navigation timing', W3C Recommendation 13 December 2012. Retrieved from http://www.w3.org/TR/2012/REC-navigation-timing-20121213/

Yap, K-K; Huang, T.-Y; Kobayashi, M; Yiakoumis, Y; McKeown, N; Katti, S; Parulkar, G. 2012. 'Making use of all the networks around us: a case study in android'. *Proceedings of the 2012 ACM SIGCOMM workshop on cellular networks: operations, challenges, and future design*, pp. 19-24.

http://doi.org/10.18080/ajtde.v6n4.166

Conflicts in Routing and UAV Autonomy Algorithms for Ad-hoc & Infrastructure-based UAV Networks

Ogbonnaya Anicho
Liverpool Hope University (United Kingdom)

Philip B Charlesworth
Liverpool Hope University

Gurvinder S Baicher
Liverpool Hope University

Atulya Nagar
Liverpool Hope University

Abstract: Routing is very fundamental to the implementation of any networking or communications infrastructure. This paper, therefore, examines the conflicts and relevant considerations for implementing autonomous or self-organising unmanned aerial vehicles (UAVs) for communications area coverage, with particular emphasis on the impact of aerial vehicle autonomy algorithms on routing techniques for such networks. UAV networks can be deployed either as ad-hoc or infrastructure-based solutions. The mobility of UAVs introduces periodic topology changes, impacting link availability and routing paths. This work examines the implications of autonomous coordination of multiple UAVs on routing techniques and network architecture stability. The paper proposes a solution where routing techniques and UAV autonomy algorithms are integrated for improved global network efficiency for both ad-hoc and infrastructure-based scenarios. Integrating UAV autonomy algorithms with routing schemes may be an efficient method to mitigate link/topology stability issues and improve inter-UAV communication and network throughput, a key requirement for UAV networks. The implementation of inter-UAV links using optical, microwave or mmWave transmission is examined in the context of this work. The proposed integration may be crucial for communications coverage, where UAVs provide communications area coverage of a community of mobile or fixed users in either ad-hoc or infrastructure-based modes.

Keywords: Routing, UAV, High Altitude Platforms, Autonomy Algorithm

http://doi.org/10.18080/ajtde.v6n4.169

Introduction

Unmanned Aerial Vehicle Communications Network

The use of unmanned aerial vehicles (UAVs) as a communication infrastructure is covered in the literature and continues to be considered an active area of research (Aadil *et al.*, 2018; Jiang & Han, 2018; Rosati *et al.*, 2016; Zhao & Braun, 2012; Zheng, Sangaiah & Wang, 2018). These aerial vehicles or platforms can be lighter than air (e.g. airships, balloons) or heavier than air (e.g. aircraft, high altitude platform stations (HAPS) capable of operating in the upper atmosphere). Regardless of taxonomical differences, all aerial platforms considered within this category are unmanned aerial vehicles with different aeronautical profiles. Depending on the network architecture, aerial networks can be infrastructure-based (Gupta, Jain & Vaszkun, 2015) or ad-hoc, also known as flying ad-hoc, networks (FANETs), a type of mobile ad-hoc network (MANET) (Jiang & Han, 2018; Rosati *et al.*, 2016). When the aerial vehicles are comprised of UAVs specifically, the network can be described as a UAV Ad-hoc Network (UANET) or Unmanned Aeronautical Ad-hoc Network (UAANET) (Jiang & Han, 2018; Maxa, Mahmoud & Larrieu, 2015), as shown in Figure 1. This work will describe all forms of aerial ad-hoc networks as UANETs regardless of platform type. UANETs are significantly different from MANETs due to mobility, dynamic topology, changing link quality and 3D environmental scenarios. These characteristics pose challenges for designers and applications (Aadil *et al.*, 2018; Gupta *et al.*, 2015). This work considers both infrastructure-based and ad-hoc network implementation scenarios for routing and aerial platform coordination requirements. In most literature, UAV networks are readily assumed or treated as ad-hoc networks (Gupta *et al.*, 2015) but this limits capability, applications and research scope of UAV communication networks in general. Ad-hoc networks by definition do not have any central infrastructure and therefore no fixed topology, unlike infrastructure-based systems (Zhao & Braun, 2012). However, in MANETs and VANETs (Vehicle Ad-hoc Networks), the distinction is clearer and easily applicable but with UAV networks the definitions become less strict, especially when inter-UAV links are implemented. An infrastructure-based UAV network that uses inter-UAV links and comprises of more than one UAV will likely encounter similar challenges common to ad-hoc networks in some parts of its implementation, as shown in Figure 1. Considering design similarities for both ad-hoc and infrastructure-based systems at the lower network layers (2 and 3) is critical for implementing efficient routing and platform coordination schemes. This approach will provide design-level proof against scenarios where UAV infrastructure-based systems have some ad-hoc traits in parts of the network due to reliance on inter-UAV links for multi-UAV communications.

http://doi.org/10.18080/ajtde.v6n4.169

The remainder of this section introduces the concept of UAV networks in both ad-hoc and infrastructure-based modes. Section II examines routing schemes proposed for UAV networks. Section III highlights design considerations for routing schemes especially for UAV network implementation. Section IV examines the requirements of autonomous UAV algorithms. Section V outlines an integration proposal for routing and autonomous UAV algorithms. Section VI describes the impact of implementing inter-UAV links with optical, microwave or millimetre wave technology. Finally, section VII draws conclusions on the work and considers future work.

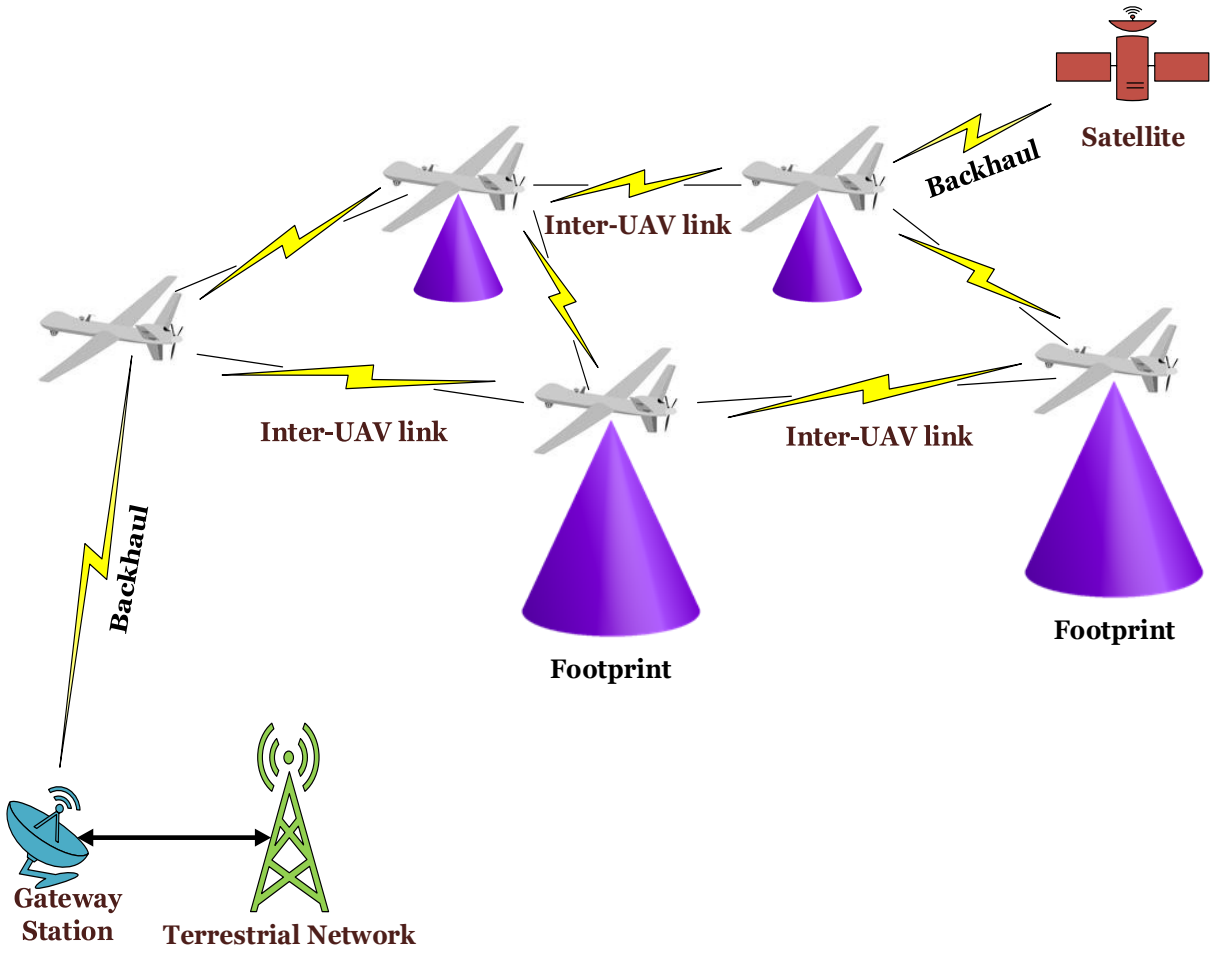


Figure 1. UAV-based network showing both infrastructure-based and ad-hoc traits

Autonomous and Cooperative Multi-UAV Networks

This work is considered within the context of implementing swarms of semi- or fully autonomous aerial vehicles with self-organising capabilities. Autonomy is defined within the context of the capability of the UAV for decision-making or self-governance; however, levels of autonomy exist and may depend on design, functions and specifics of the mission (Chen, Wang & Li, 2009). It is expected that the movement of aerial vehicles of the future will be managed by fully autonomous algorithms maintaining network connectivity, data rate and coverage as mission objectives (Zhao & Braun, 2012). Autonomy in this regard can also refer to the ability

http://doi.org/10.18080/ajtde.v6n4.169

of the UAVs to make local decisions with limited or no global knowledge and still achieve network-wide objectives cooperatively. For a swarm of flying UAVs with the mission of providing communications coverage, either as a standalone network (ad-hoc) or part of a larger infrastructure, self-organisation and swarm coordination is very crucial. Maintaining stable inter-UAV communications is very critical to any form of autonomous and efficient coordination scheme for communications area coverage or similar applications (Gupta *et al.*, 2015). As demands for the deployment of UAVs for various communications infrastructure scenarios are considered, the challenge of developing autonomous aerial vehicles with a capability to cooperate or coordinate as a swarm, providing service with very minimal human input, is essential. Reviewed literature on UAV networks has focused on topology changes and impact on routing without considering autonomy algorithms and requirements. In this work an attempt is made to integrate routing techniques with aerial vehicle autonomy, with a view to achieving stable network link availability and quality. That mobility of aerial vehicles introduces a higher dimension of topology change is an established issue but how much vehicle autonomy algorithm decisions affect link and network stability is not sufficiently addressed in the literature (Anicho *et al.*, 2018b). In designing aerial vehicle autonomy algorithms, the main consideration is always to develop agents with intelligence for learning and decision making. In this work, a proposal to integrate routing decisions with autonomy decision outputs is made. For instance, current routing techniques use different routing metrics to make routing decisions: integrating another layer of logic that interfaces more proactively with the aerial vehicle autonomy algorithm will be desirable.

Routing Schemes in UAV Networks

Routing is a critical concept in UAV networks and has received attention from the research community. This work is not about how routing schemes work but how routing may be affected by higher decisions of the autonomous UAV logic layer. The link disruptions for aerial networks are significant due to mobility and related issues; however, to provide service, the network must be able to route control and data traffic from source to destination reliably (Maxa *et al.*, 2015). How to achieve this will depend on the performance of the routing schemes adopted. It is accepted that routing techniques employed in other mobile systems cannot be implemented for UAV ad-hoc or infrastructure-based networks (Zheng *et al.*, 2018; Gupta *et al.*, 2015).

Zheng *et al.* (2018) proposed an adaptive hybrid reinforcement learning, self-learning routing protocol (RLSRP) to address the network-layer routing requirements and position-prediction-based directional (PPMAC) protocol for the FANET MAC layer. The protocol implements two cooperative transceivers operating concurrently, with one processing position and control packets while the other handles data traffic. This scheme depends on position prediction and estimation, which may be problematic if predictions become significantly inaccurate. The

http://doi.org/10.18080/ajtde.v6n4.169

protocol relies heavily on the assumption that GPS coordinate vectors will be shared amongst all participating UAV nodes, which is also subject to link availability. From the perspective of an autonomous platform algorithm, it is important to clarify how such a routing scheme will be affected by flight control systems, which are not integrated with routing algorithms.

Rosati *et al.* (2016) compared the performance of optimised link-state routing (OLSR) and predictive-OLSR (P-OLSR) and discovered that P-OLSR performed significantly better than OLSR. P-OLSR essentially predicts the evolution of quality of the wireless links using GPS information from the autopilot system. In this approach, the routing algorithm predicts link quality evolution, which is a proactive routing approach. It is also evident that there is no integration of the flight system decisions with the routing algorithm.

Biomo, Kunz & St-Hilaire (2014) proposed a strategy to mitigate the failure of Geographic Greedy Forwarding (GGF), a routing scheme that relies on greedy forwarding (GF) to route packets to the neighbour whose location is closest to the destination. However, the scheme fails when there is no node that meets the GF metrics: i.e., no neighbour is closer to the destination. The void node in this circumstance drops the packet, a scenario that is very undesirable for reliable communications. The strategy proposed by the authors relied on implementing some kind of holding scheme to prevent the node from dropping the packets too soon while trying various remedial strategies. One remedial strategy focused on retrying the GGF process and dropping the packet after the second attempt, which also does not assure success. Another strategy was to forward the packet to the furthest neighbour regardless of distance, which may be a problem if there is no node within transmission range. Finally, the last strategy relied on forwarding the packet to the best moving node, which may be the forwarding node itself, in which case a loop is formed and may lead to the packet being dropped. The above strategies are reactive in nature and do not coordinate action between the routing algorithm and the vehicle autonomy or flight system algorithm, as proposed by this paper.

There are several routing schemes proposed for aerial networks but none explicitly addresses the impact autonomous system decisions may have on the inter-UAV links and, by extension, the routing algorithm. The purpose of this work is not to review all proposed routing techniques for UAV networks but to address the impact of designing routing schemes without considering UAV autonomy or flight system algorithms; or *vice versa*.

Routing Algorithm Design Considerations

Routing generally is made up of two basic activities: determining optimal routes or paths; and the switching or transport of data packets through the network. However, in order to achieve the above goals, the network architecture must maintain reliable links for routing data from source to destination. In applications where link stability or topology is fixed, routing is more

http://doi.org/10.18080/ajtde.v6n4.169

straight-forward and less complicated, e.g., in low mobility or fixed topology networks. For instance, in MANETs, the mobility of the nodes is quite slow and predictable and can be approximated with synthetic mobility models. This makes routing algorithm design less complicated. Routing algorithms that have shown reliable performance in MANETs or low mobility networks have been found to be unsuitable for UAV networks, as noted earlier. Current routing techniques proposed for UAV networks have tried to use position-vector, link-state or other reactive and hybrid approaches to mitigate the impact of topology instability. Since the mobility factor is very high in UAV networks and routing algorithms have to determine and route packets through these highly dynamic links, then the solution cannot lie with the routing algorithm alone (Anicho *et al.*, 2018b). The approach being explored will have to link the vehicle autonomy algorithm to the routing algorithm, with the aim of stabilising the links and also avoiding dropped packets due to relocation decisions. The process in Figure 2 is a conceptual flow process and does not reflect all the technical details expected in a full routing algorithm but describes a typical routing process, agnostic to any particular routing protocol or metrics.

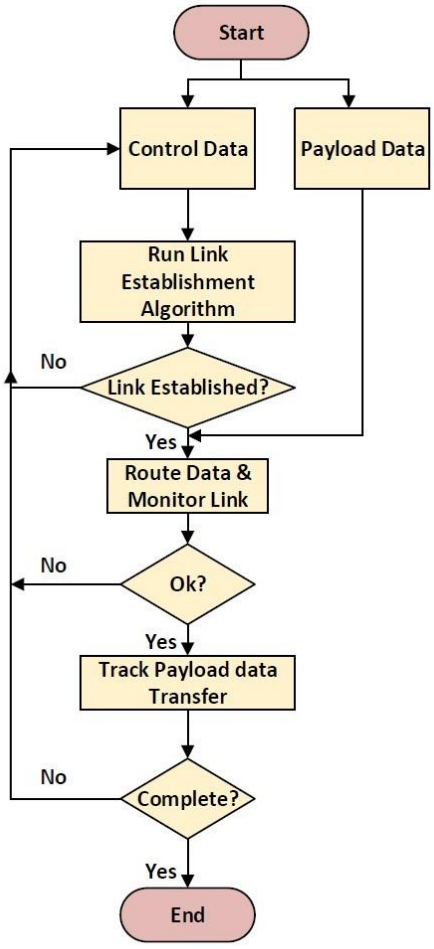


Figure 2. Conceptual Routing Flow Process

http://doi.org/10.18080/ajtde.v6n4.169

Autonomous Algorithms for UAVs

The concept of semi- or full autonomy in UAV implementation is accepted as the next generation of UAV system capability. However, autonomy is mission specific and has to be defined within the context of the application and what is essential for the mission objective. For instance, in the case of a solar-powered fixed wing UAV used for area coverage, autonomy encompasses the capability of the aerial platform to make decisions on how best to position itself to maximise coverage and maintain inter-UAV links for reliable communications while rationing stored energy through night/non-solar periods (Anicho *et al.*, 2018a). It is also expected that the autonomous algorithm will coordinate path planning tasks while balancing the constraints of energy and power management for flight control and payload/mission requirements. Autonomous capability for such a solar electric aerial vehicle also involves the management of the three-dimensional aerodynamic environment where pitch, roll and yaw vectors are relevant. This picture does elevate autonomy in such aerial vehicles to a complex set of requirements that involve mission-critical decisions. For instance, how will the algorithm manage situations of insufficient stored energy to sustain flight in the midst of data exchange, where the option is either to cut off energy supply to the payload or risk a crash? The scenario of a crash may be extreme but not impossible and highlights the kind of decisions that may arise during implementation. However, applying a proactive and predictive design concept for the routing and flight control algorithm interface may help mitigate conflicts and improve performance.

Overview of a Typical UAV Platform Autonomy Algorithm

An algorithm to manage the flight, power and communications segment of a solar-powered fixed wing UAV or HAPS (which operates in the stratosphere at about 17-25 Km) is under development in the present research. The coordination algorithm has largely depended on using metrics like power and coverage parameters to control flight, platform positioning and communications. In the conceptual solar-powered fixed HAPS or UAV referenced in this research, the autonomy algorithm consists of the energy management and platform coordination algorithms. These two key subsystems define the level of autonomy applicable to the platform and are explained further below.

1) Energy Management Algorithm:

The energy management algorithm that is relevant in solar applications manages the UAV power and energy requirements in order to assure platform persistence. It should apply smart decisions on power dimensioning and allocation to all units of the system. The objective is to ensure accurate conservation, prioritisation, and management of both primary and secondary energy sources for successful missions. The energy management logic achieves the mentioned objectives by tracking solar power availability and

http://doi.org/10.18080/ajtde.v6n4.169

switching to back-up batteries when inevitable and to further trigger a gliding manoeuvre if energy resources reach critical minimum thresholds. Under such critical conditions, the logic shuts off power for propulsion and payload while the HAPS glides freely subject to glide dynamics consistent with the vehicle's configuration (Anicho *et al.*, 2018a). The algorithm initiates UAV platform ascent when solar energy is restored and the back-up batteries go into the recharge cycle.

It is important to highlight the workings of the energy management algorithm as part of the autonomous capability of the UAV, which does not currently have any routing awareness or considerations.

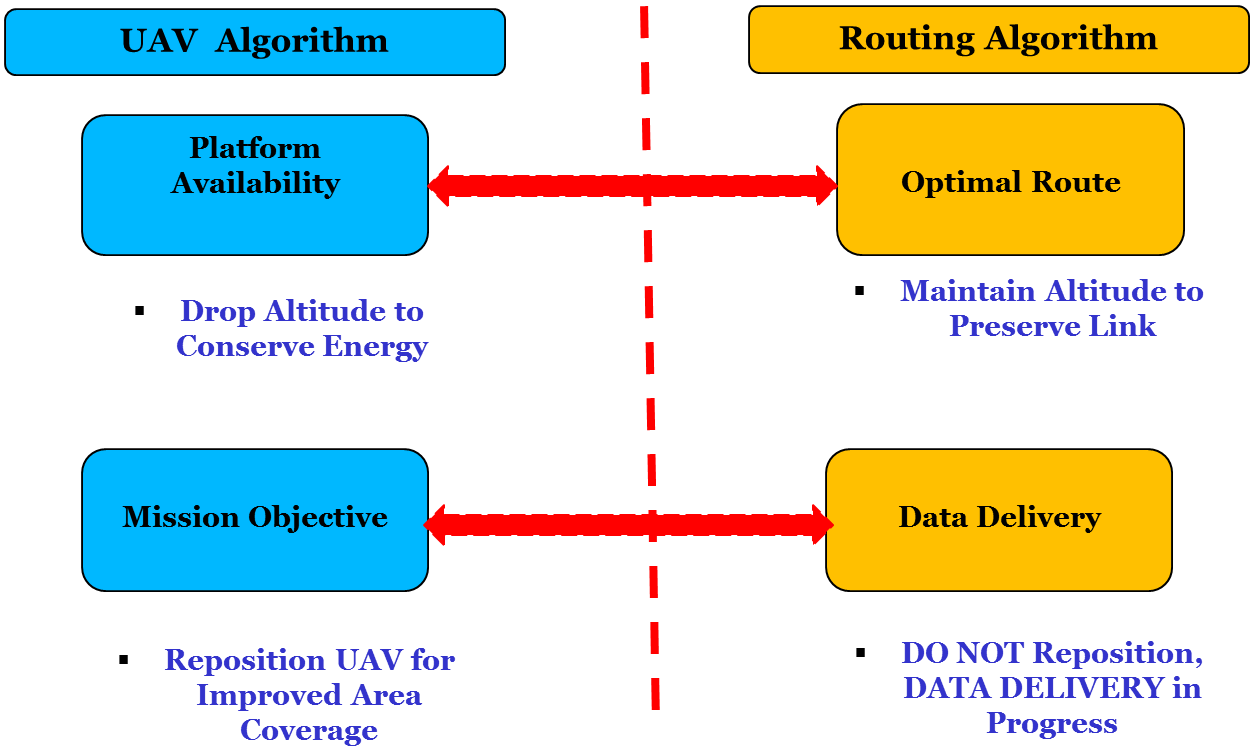


Figure 3. Conceptual Conflicts in UAV Platform Algorithms and Routing Schemes

2) Coordination Algorithm: The coordination algorithm enables the UAV to function in a multiple UAV network scenario by being able to dynamically coordinate within a swarm of UAVs. In this scenario, the UAV platforms are able to self-organise autonomously to meet global objectives. The coordination algorithm is designed to help each UAV navigate and function within a swarm in ways that the network can guarantee service to users. Deploying UAVs in this manner involves rigorous technical and engineering considerations as the mobility of the UAVs impact link stability, as earlier mentioned. For instance, providing communications coverage to mobile ground users using multiple UAVs with coordination-enabled capability requires that the UAVs can relocate dynamically to maximise coverage. The coordination algorithm ensures that all UAVs in the swarm can find improved locations to meet a predefined mission objective, which is to maximise ground user coverage. A conceptual

http://doi.org/10.18080/ajtde.v6n4.169

coordination algorithm is designed to improve the UAV platform's participation in the swarm network and to ensure improved relocation and positioning capabilities to meet mission objectives. However, the flaw with this approach is that such autonomous algorithms may conflict with the performance of any selected routing technique, as shown in Figure 3. The challenge of finding suitable routing technique may be linked to the non-integration approach to autonomous systems and routing protocol design.

In the case of the current autonomous solutions being developed for multiple coordination of aerial platforms, it is essential to provide the flight control system and coordination algorithm with an interface to interact with the routing algorithm and determine flight patterns or manoeuvres that will improve link stability for improved network performance. Designing autonomous vehicle control and coordination algorithms should involve adding interfaces which will enable the flight systems and routing algorithms to interrogate each other to improve platform position and management for link quality performance. It is important to mention that this interface requires critical infrastructure level security against attack vectors, e.g. uplink subscriber-initiated attack on the flight control system. In the design hierarchy, the flight system algorithm will have higher priority in terms of decision-making and will be able to override suggestions from the routing algorithm if it will impact safety or vehicle/platform endurance.

Proposed Integration Interface for Routing and Autonomous Algorithms

As described in Figure 4, the proposed interface will be implemented using mostly layer 2 and 3 protocols. The control data will include some information bits exchanged between the routing and autonomous algorithms. The information load will incur minimal overhead, as the bulk of the exchange is within the same vehicle. There are three main messages that will be exchanged; more could be added depending on application specifics, protocol frame requirements and bandwidth. One of the messages will control the positioning of the UAV platform for maximum link quality, which will improve routing performance. The aerial platform operates in a 3D environment and is capable of station-keeping, a capability that can be explored to improve inter-UAV link performance. The routing algorithm shares link status parameters with the flight control system, which in turn carries out computations on how to improve link status if below certain thresholds. The second information exchange informs the routing algorithm that the UAV plans a manoeuvre that may interrupt or degrade the link. This will enable the routing algorithm to make decisions on routing and may even broadcast this for other UAVs to adjust altitude to maintain link performance. This kind of message may be a warning message for extreme platform manoeuvres, for example gliding during critical phases of the mission,

http://doi.org/10.18080/ajtde.v6n4.169

especially in a solar powered vehicle. A third message may be the routing algorithm requesting information from the UAV for likely delay in any sort of manoeuvre due to critical data transmission operation or related QoS provisioning. The integration of these two important algorithms, especially at design phase, may improve how aerial vehicles are implemented for communication networks. This aspect of the integration considers inter-UAV link stability for quality network performance.

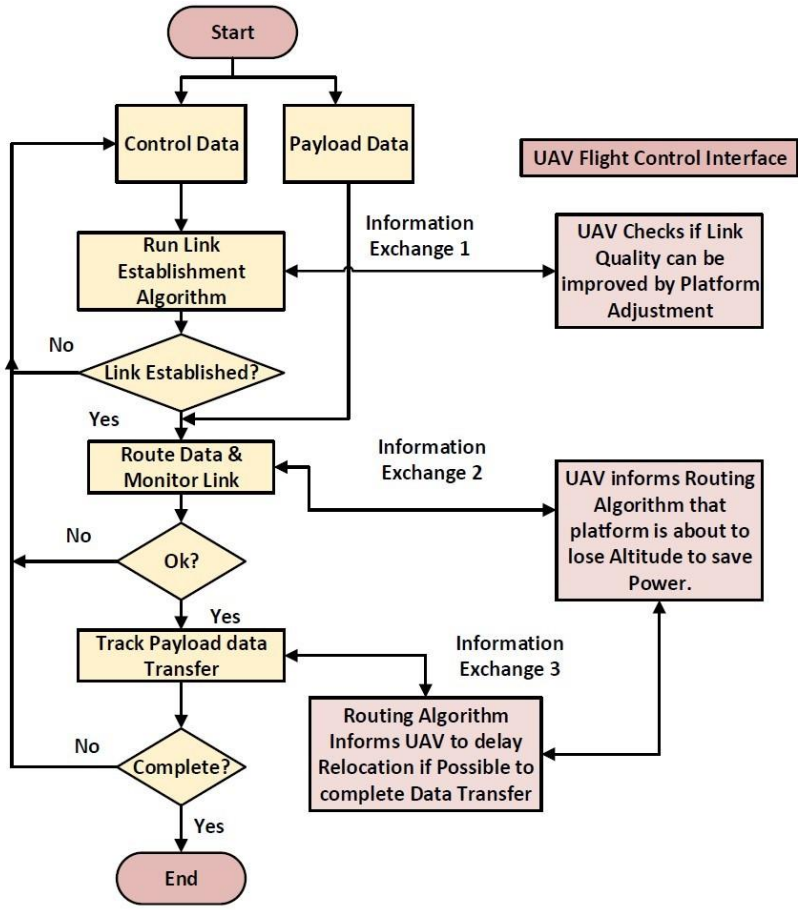


Figure 4. Integrated Autonomous Flight System and Routing Algorithm

Implementation of Inter-UAV Links

Inter-UAV links are significant in the design and implementation of UAV-based networks, either as ad-hoc or infrastructure-based systems. The ability to sustain the quality of inter-UAV links will be crucial in the application of UAV-based networks for high-speed internet access. Future 5G networks will rely heavily on cloud-native architecture (e.g. CloudRAN), which will require very reliable links for maintaining connectivity, especially for enhanced mobile broadband (eMBB) (Huawei, 2016).

Microwave, mmWave & Optical Transmission for Inter-UAV Links

Free space optical systems use collimated laser beams with wavelengths in the range of 0.48-0.78 μm to transmit data at multigigabit rates with narrow beamwidth, compact and light

http://doi.org/10.18080/ajtde.v6n4.169

weight terminals (Aviv, 2006; Fidler *et al.*, 2010). Consequently, optical links have low power, are highly secure, are immune to interference or jamming (tap-proof) and, further, prevent exhaustion of scarce spectrum resources (Aviv, 2006; Henniger & Wilfert, 2010). However, optical or laser systems are susceptible to cloud coverage, weather conditions and atmospheric turbulence with stringent pointing, acquisition and tracking requirements (Zettl *et al.*, 2007; Truyens, 2017). Optical links may be problematic or impractical for any propagation environment where unfavourable cloud and weather conditions are significant.

Microwave links, on the other hand, have better weather penetration characteristics and consequently lower propagation losses (Aviv, 2006; Fidler *et al.*, 2010). In terms of ground-to-air and air-to-ground links, microwave systems prove more reliable and may be suitable for inter-UAV links within the troposphere. However, microwave systems need bulkier antennas or surface-mounted phased arrays, which require more computing power for steering beams and may significantly increase overall size, weight and power (SWaP) parameters (Aviv, 2006). The broader beamwidth of microwave radiation causing interference and security susceptibility are significant issues with this system as well (Aviv, 2006; Fidler *et al.*, 2010).

Implementing mmWave will free up spectrum resources and harness the larger bandwidths and higher data rates possible within this frequency band (Huo *et al.*, 2018). Smaller antennas improve SWaP configuration of mmWave systems, with better pointing profiles than microwave. However, mmWave is susceptible to gaseous attenuation due to water vapour, aggravated by atmospheric humidity, which degrades link quality (Huo *et al.*, 2018). Wider application of mmWave systems will likely increase, as mmWave is proposed for use in future 5G network implementations.

Regardless of transmission technology, inherent characteristics of the technology must be considered for improved link performance. UAV platform autonomy algorithms must be able to manage aerial vehicle, antenna orientation and pointing computations to support routing decisions; this requirement sums up design considerations for routing, platform autonomy and transmission link technology for implementing UAV networks, either as ad-hoc or infrastructure-based.

Conclusion and Future Work

This paper has identified conflicts between routing and UAV autonomy algorithms and provides some context to the impact of autonomous platform algorithms on routing schemes. The work proposes a design approach that will integrate the routing and autonomous platform algorithms for improved network reliability. However, the implementation of inter-UAV links has significant impact on the network links regardless of the efficiency of the interfaces.

http://doi.org/10.18080/ajtde.v6n4.169

Therefore, designing links using appropriate transmission technology may enhance the performance of integrating routing schemes and autonomous platform algorithms.

Future work will focus on developing simulation models to investigate routing-aware platform autonomy algorithms for mitigating topology/link issues. Another area of consideration will be the extent to which current advances in software defined networking can aid in the resolution of the conflicts between routing and UAV platform control. It will be interesting to research this problem within the context of next generation networking capabilities; this may redefine the impact of earlier defined conflicts. Moreover, this may lead to settling the open research question of the most suitable routing technique for UAV-based networks.

References

Aadil, F; Raza, A; Khan, MF; Maqsood, M; Mehmood, I; Rho, S. 2018. 'Energy Aware Cluster-Based Routing in Flying Ad-Hoc Networks'. *Sensors*, *18*, 1413. MDPI. http://dx.doi.org/10.3390/s18051413.

Anicho, O; Charlesworth, PB; Baicher, GS; Nagar, A. 2018a. 'Autonomous Unmanned Solar Powered HAPS: Impact of Latitudes and Seasons on Power and Communications Coverage'. *IEEE COMNETSAT*, Medan, Indonesia, November.

Anicho, O; Charlesworth, PB; Baicher, GS; Nagar, A. 2018b. 'Integrating Routing Schemes and Platform Autonomy Algorithms for UAV Ad-hoc & Infrastructure Based Networks'. *28th International Telecommunications Networks and Applications Conference* (ITNAC), Sydney, Australia, November.

Aviv, DG. 2006. *Laser Space Communications*. Artech House Inc.

Biomo, JDMM; Kunz, T; St-Hilaire, M. 2014. 'Routing in Unmanned Aerial Ad hoc Networks: A Recovery Strategy for Greedy Geographic Forwarding Failure'. 2014 *IEEE Wireless Communications and Networking Conference*, April, pp. 2236-2241. http://dx.doi.org/10.1109/WCNC.2014.6952677

Chen, H; Wang, X; Li, Y. 2009. 'A Survey of Autonomous Control for UAV', *2009 International Conference on Artificial Intelligence and Computational Intelligence*, Shanghai. IEEE, Nov. https://ieeexplore.ieee.org/document/5375937

Fidler, F; Knapek, M; Horwath, J; Leeb, WR. 2010. Optical Communications for High-Altitude Platforms. *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 16, issue 5, Sep-Oct, pp. 1058-1070. https://ieeexplore.ieee.org/abstract/document/5464268 .

Gupta, L; Jain, R; Vaszkun, G. 2015. 'Survey of Important Issues in UAV Communication Networks'. *IEEE Communications Surveys & Tutorials*, vol. 18, issue 2, pp. 1123-1152. https://ieeexplore.ieee.org/document/7317490

Henniger, H; Wilfert, O. 2010. 'An Introduction to Free-space Optical Communications'. *RadioEngineering*, vol. 19, no. 2, pp. 203-212.

Huawei. 2016. '5G Network Architecture: A High-level Perspective'. *Huawei White Paper*. Available at https://www.huawei.com/minisite/5g/img/5G_Network_Architecture_A_High-Level_Perspective_en.pdf

Huo, Y; Lu, T; Xu, W; Yuen, M. 2018. 'Distributed and Multi-layer UAV Network for the Next-Generation Wireless Communication'. Cornell University. arXiv:1805.01534

Jiang, J; Han, G. 2018. 'Routing Protocols for Unmanned Aerial Vehicles'. *IEEE Communications Magazine*, vol. 56, issue 1, pp. 58-63.

Maxa, J-A; Mahmoud, M; Larrieu, N. 2015. 'Secure routing protocol design for UAV ad hoc networks'. *2015 IEEE/AIAA 34th Digital Avionics Systems Conference*. http://dx.doi.org/10.1109/DASC.2015.7311415

Rosati, S; Kruzelecki, K; Heitz, G; Floreano, D; Rimoldi, B. 2016. 'Dynamic Routing for Flying Ad Hoc Networks'. *IEEE Transactions on Vehicular Technology*, vol. 65, issue 3, pp. 1690-1700. http://dx.doi.org/doi: 10.1109/TVT.2015.2414819

Truyens, N. 2017. 'Complementing and Enhancing Satellite Infrastructure by HAPS and optical communication'. *2017 HAPS4ESA Conference*. https://atpi.eventsair.com/QuickEventWebsitePortal/haps4esa/website/ExtraContent/ContentPage?page=8

Zettl, K; Muhammad, SS; Chlestil, C; Leitgeb, E; Friedl, A; Schmitt, NP; Rehm, W. 2007. 'High bit rate optical wireless systems for swarm unmanned aerial vehicles: a feasibility study'. *The Mediterranean Journal of Computers and Networks*, vol. 3, no. 4, pp. 142-150.

Zhao, Z; Braun, T. 2012. 'Topology control and Mobility Strategy for UAV Ad-hoc Networks: A Survey'. *Joint ERCIM eMobility and MobiSense Workshop*. Available at https://pdfs.semanticscholar.org/2cbc/2c96cd19630c6d2097aef3d9450ab9665bea.pdf?_ga=2.20979835.1960318396.1546752601-1305157130.1546752601

Zheng, Z; Sangaiah, AK; Wang, T. 2018. 'Adaptive Communication Protocols in Flying Ad Hoc Network'. *IEEE Communications Magazine*, vol. 56, issue 1, pp. 136-142.

Privacy versus the Use of Location Information for Law Enforcement and Security in Australia

Stanley Shanapinda
La Trobe University

Abstract: This article reviews existing knowledge regarding the powers of the Australian Security Intelligence Organisation and the Australian Federal Police to access and use metadata. The review is primarily based on published research on the privacy impact of the revised metadata retention and collection framework introduced in 2015. The review reveals that, after 2015, no comprehensive study was undertaken in the following areas: how location information is generated and exchanged in the IP-mediated long-term evolution telecommunications network, and how mobile devices are tracked and create more precise location estimates, in the legal and policy context of the exceptions and privacy safeguards introduced after 2015; the discretionary powers of the agencies to use personal and sensitive information to identify inquiries and investigations to pursue, to enforce the law and perform their functions, and to carry out activities related to their functions and purposes; and the flexible oversight principles contained in the guidelines that create conflicts between law enforcement and privacy interests. The review proposes future multidisciplinary research.

Keywords: location information, privacy, metadata retention and disclosure, LTE, law enforcement and national security

Introduction

The retention and disclosure of metadata to law enforcement agencies has been met with criticism worldwide and has been invalidated by the courts. The broad range of investigatory powers are not regarded as being consistent with the protection of privacy (*the Watson case*, 70; *Digital Rights Ireland Ltd, 2014*, [60]; *USA FREEDOM Act*; *Carpenter case*, 2018).[i] This review highlights arguments that state privacy is not adequately protected, given the investigatory powers of the Australian Security Intelligence Organisation (ASIO) and the Australian Federal Police (AFP) (the Agencies) that appear broad and based on how Location Information (LI) is personal and precise, given the use of modern telecommunications technologies. The review raises complex issues that at times appear to be at odds with one another. This complexity highlights the need for in-depth studies, in the interest of a nuanced privacy debate. This review highlights these arguments in relation to existing literature and

http://doi.org/10.18080/ajtde.v6n4.167

states that existing literature did not adequately study the contemporary powers of the Agencies to collect retained data in relation to how modern communications technology generates and shares LI and the personal nature of LI. As such, an empirical study must still be undertaken. The proposed study is likely to confirm that privacy is poorly protected, but the benefit of such a study would be the relevant findings that are based on current contexts about how the powers of the Agencies are designed and operate.

The issues raised by other authors included: understanding how modern mobile phone location services work to balance the powers of the Agencies; the privacy characteristics of telephone metadata in America; inadequate protection of privacy; the lack of transparency in the exercise of the powers of the Agencies; the broad powers of the Agencies and whether telecommunications data is considered 'personal information'; and the impact on privacy by the use of Big Location Data (BLD) analytics software by the Agencies for investigations. Criticism of the powers of the Agencies were made through the privacy lens – i.e. the focus was largely on the impact of the powers on privacy. Whereas the impact of the powers of the Agencies on privacy is not a new issue, this review also approaches privacy from the perspective of privacy being a tool that is used to restrict the powers of the Agencies. There is a difference between how privacy was protected in 1988 when the *Privacy Act* was introduced, and how privacy is protected since 2015, when the *Data Retention Act 2015* (Cth) introduced the two-year mandatory retention of LI. There is no comprehensive study of the privacy safeguards revised in 2015, both as principles to be protected and as limits to the powers of the Agencies and how privacy is impacted by the very powers it aims to restrict. This review recommends empirical studies based on how privacy can be used to exercise oversight over the powers of the Agencies. Studies must look at this dynamic interaction to understand how privacy is impacted but also how privacy plays the role of gatekeeper. Privacy is not a static standard, it evolves with time, and has a dual nature – as a target and as an oversight tool. The LI generated by new communications technologies such as LTE (the mobile fourth-generation long-term evolution standard) is more revealing of Personal Information (PI) and Sensitive Information (SI), and so the definition of what is considered 'personal information' changes with time. This review raises relevant and modern issues that provide the context needed to try to understand the modern privacy debate. The review makes a preliminary conclusion that the use of modern communications technologies leaves privacy more vulnerable than before, when earlier authors wrote about the impact on privacy. To strike a fair balance between privacy as a right to be protected and simultaneously using privacy as a tool to limit the powers of the Agencies, privacy may require greater protection than before. The requirement to retain the information for a minimum period of two years, or longer, creates an incentive for the Telco to collect and store more LI than the Telco ordinarily stored, and for use in new

http://doi.org/10.18080/ajtde.v6n4.167

commerce developing digital products and digital services (AGD, Submission 2015, 16–17 [2.3]; Telstra, Submission 2015, 5 [8]). The same LI may in practice be retained for longer than the two-year minimum and remain available to the Agencies without a judicial warrant throughout its lifespan (*TIA Act 1979* ss 5(1) (definition of 'retained data'), 187C, 175–184; *TA 1997* ss 275A, 276, 313(3), 313(4), 3131(7)). This weakens the position of privacy as a principle to be protected and as a safeguard for the accountable exercise of power, in the context of BLD.

Existing common law precedents must be analysed in detail in the context of the 2015 data retention scheme. These include:

- The 2015 *Telstra Corporation Limited* case ([2015] AATA 991 (18 December 2015)) and the 2017 *Privacy Commissioner* case ([2017] FCAFC 4 (19 January 2017)), where the meaning of PI was argued – whether the data in question can be about multiple things, including being about the individual or not;
- The *Farrell* ([2017] AATA 409 (31 March 2017)) case and the *Jaffarie* case, where the broad meaning of national 'security' was contested but accepted by the courts;
- The *Day* ([2000] FCA 1272 (11 September 2000)) case where the court decided that the word 'investigation' is taken to mean 'the act or process of searching or enquiring in order to ascertain facts'. This case was not critically analysed in relation to the use of BLD analytics and the resulting impact on privacy; and
- The *Samsonidis* case ([2007] FCAFC 159 (5 October 2007)) that effectively makes the point: if the information collected for the purpose of investigation A was shared within one organisation to perform investigation B, the organisation would be allowed to do so, without having to apply the privacy tests in respect of investigation B before sharing the data. The *Samsonidis* case needs to be critically analysed in relation to the privacy impact of its interpretation when it comes to the use of BLD analytics, that reveal more SI and PI, about people's behaviour that may not be related to the investigation in question and in relation to third parties that may not be primary targets of investigations.

The sections below review key issues raised in existing literature related to the collection and the use of metadata, in relation to its impact on privacy.

Understanding How Modern Mobile Phone Location Services Work to Balance the Powers of the Agencies

Leonard (2015c, p. 7) suggested that an understanding of the types of data that will be collected, and the entity collecting the data, could help assess the effectiveness of any limits that are placed on receiving the telecommunications data. Location Information is identified

http://doi.org/10.18080/ajtde.v6n4.167

as one such data type and is the focus of this review, in order to try and assess the effectiveness of any limits on collecting and using LI. The review distinguishes between the two Agencies, assessing their powers individually. Leonard (2015c, p. 7) also stated Australian telecommunications law that deals with the disclosure of information regarding communications is vague and does not address modern issues. An LTE mobile telecommunications network (ETSI 2017a), with its more precise location functionality, is one such modern technological issue and is raised as the focus of this review.

Taking a historical look, Leonard (2015c, p. 7) made the point that the ambiguity in the law can be traced back to the reason why telecommunications interception was developed. The reason was to protect privacy of voice telephone calls. The calls were mediated by copper wires (Leonard, 2015c, p. 7). The information about communications using copper wires was deemed less sensitive than the contents of the phone call (Leonard, 2015c, p. 7). This distinction between the voice call (as the contents of the communication) versus the time and duration of the call (as the information related to the voice phone call) is now the basis of Australian telecommunications interception law (Leonard, 2015c, p. 7). American electronic surveillance legislation has also drawn distinctions in protection between the content of a communication and information that is related to the content of a communication. This was at a time when content and metadata were more distinct (Bellovin 2016, pp. 2, 3, 8, 17).

Information about communications is accessed by the Agencies under the less stringent *CAC Determination 2015* because the metadata is considered less sensitive than the content of SMS or voice messages (*TIA Act 1979* ss 174 – 84; *TA Act 1997* s 275A). Bloch and Wark (2015) cited the recommendation of the Parliamentary Joint Committee on Human Rights (PJCHR) that 'content' be defined, in order to better protect privacy (Bloch & Wark, 2015, pp. 23-27). The report, however, did not go to the extent of recommending an actual definition for the type of information that should be considered 'content'. The critical question to be examined is how the distinction between content and metadata is relevant to the discussion regarding the protection of privacy, given the modern Internet-Protocol (IP)-mediated LTE network. In an advanced IP-mediated, LTE mobile network, from a technological perspective, the lines between metadata and content are blurred, as discussed below. In the IP-mediated LTE network, LI is created, exchanged, and stored in a Stream Control Transmission Protocol/Internet Protocol (SCTP/IP) packet over the Internet, which is technologically speaking, a communication (IETF, 2007, 6 [1.2], 15 [3]; ETSI, 2017a, 22 [6.4.1-1]). The network architecture is illustrated in Figures 1 and 2. Figure 1 is best read from left to right to understand how the various pieces of equipment in the IP-mediated LTE network operate. Location Information is carried as the LTE Positioning Protocol Annex (LPPa) message inside the S1 Application Protocol (S1AP) message, as its content, between the two devices, such as

http://doi.org/10.18080/ajtde.v6n4.167

the Evolved Universal Terrestrial Access Network (E-UTRAN) Node B (eNB) in the EUTRAN and the Mobility Management Entity (MME) (ETSI, 2017d, 7 [1], 10 [6]; ETSI, 2017e, 91 [8.17.1], 92 [8.17.2.1-1]). These messages include Assistance Data, Measurements and LI forwarded from the User Equipment (UE), which is the mobile device, and the MME by using the LTE Positioning Protocol (LPP) (ETSI, 2017a, 21 [6.2.1]). These Network Elements work together by exchanging radio signals and the identity of the UE, to help locate the position of the UE and to store the location of the UE (ETSI, 2016a, 145). The connections between these Network Elements are made over the Internet (ETSI, 2017a, 91 [8.17.1]). The Network Elements use various interfaces and Internet-based protocols to exchange these messages (ETSI, 2017f, 24 [4.1.1.1]).

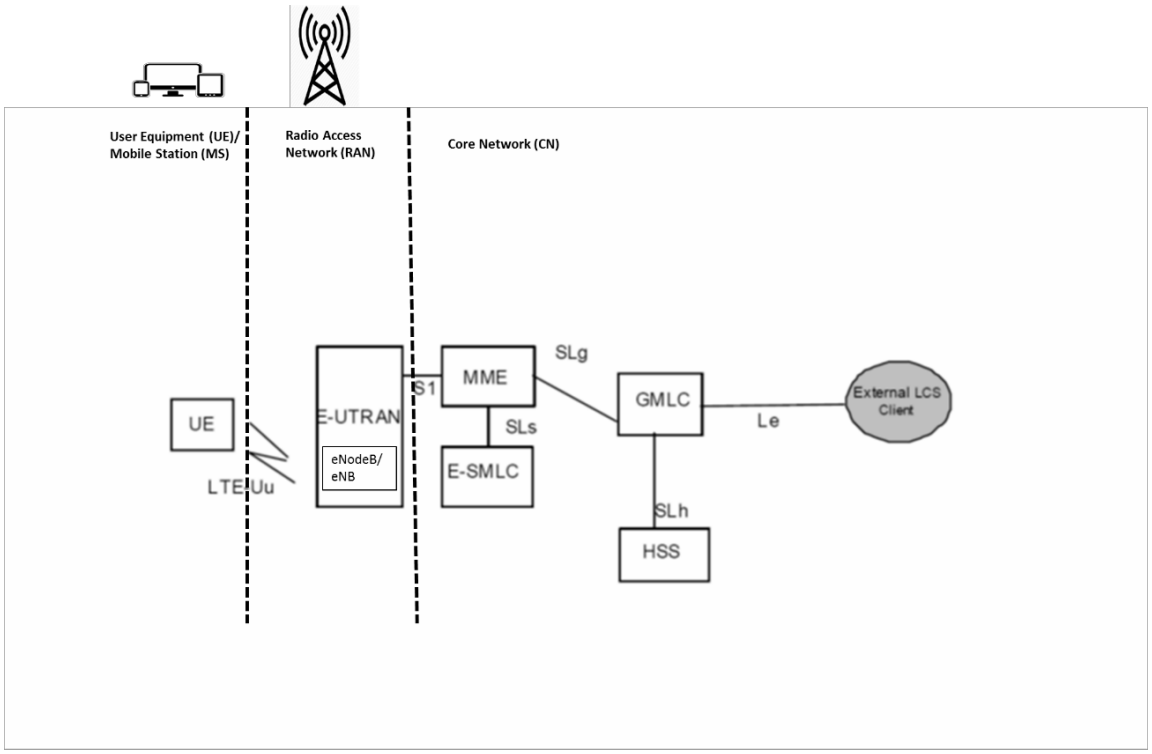


Figure 1. The IP-mediated LTE Network (ETSI, 2017f, 58 [5.2.3])[ii]

Location Information is technologically, from the perspective of the IP-mediated LTE network, carried inside an Internet Protocol (IP) packet, as the contents of the IP packet. The LPPa signal messages are communication(s) carried over the Internet by means of these various protocols, such as the SCTP/IP (ETSI, 2017a, 21 [6.2.1]; Kozierok, 2005; IETF, 1981a, 1981b; IETF, 2007). This is illustrated by Figure 2. However, Location Information is not the contents of a voice or SMS communication (IETF, 2007, 15 [3.]). Legally, LI is considered to be information about a customer, and as 'telecommunications data'. This is evident from the legal phrase: 'the affairs or personal particulars (including any unlisted telephone number or any address) of another person' (TIA Act, 1979, s 276). Location Information is not legally regarded as the content of a communication in Australia, unfairly denying this aspect of LI, whereas LI may be both content in itself and information related to voice content. Instead,

http://doi.org/10.18080/ajtde.v6n4.167

location information is regarded as subscriber related data, as metadata, as telecommunications data, as information related to the contents of a communication (Parliamentary Debates, 2016; TA 1997 ss 275A, 276, 280, 313(3)(4)(7); TIA Act 1979 ss 187A (1), 187AA (1) items 1– 6, Chapter 4 Part 1 Division 3-4; LCARC, 2015, 27).

From a technological perspective, the traditional metadata versus content distinction is difficult to apply to the IP-mediated LTE network when it comes to the retention and disclosure of LI, in American law (Bellovin *et al.*, 2016, pp. 2, 3, 8, 17) and in terms of Australian electronic surveillance law and policy, as contained in *TIA Act 1979* and the *TA 1997*.

The *CAC Determination 2015* sets out the metadata collection procedure to be used. This allows the Agencies to access the information about the voice call or SMS. The Agencies issue authorisations and notifications requesting access to the LI (*CAC Determination 2015*). Leonard (2015c, p. 7) referred to this process as self-certification. The *TIA Act 1979* addresses how the content of the call is to be accessed, given the sensitivity and personal nature of the call (Leonard, 2015c, p. 7). A domestic preservation notice and a stored communications warrant or an interception warrant are required to access the contents of the call (Leonard, 2015c, pp. 8-9; TIA Act, 1979 ss 39, 109, 110, 110A, 115). Leonard (2015c, p. 10) stated, given the popularity of smart phones with built in geo-located cellular abilities, information about communications over those phones reveal details of people's lives, and the value of this cannot be underestimated. This trend has led Australia to adopt the data retention scheme requiring the Telco to retain the data about a phone call or SMS (Leonard, 2015c, p. 10). This smart phone use trend is enabled by the geo-located cellular abilities of telecommunications networks, such as the IP-mediated LTE network. Unlike the copper wire system, an IP-mediated LTE network uses the Internet to carry both the contents of the voice call and the information about the communications (IETF, 2007, p. 6 [1.2]). The telecommunications data retention scheme requires LI be retained and disclosed to the Agencies, in the same way it was done for copper wires (Leonard, 2015c, pp. 7, 10). The Australian telecommunications law, which allows for access to LI, with the newly introduced privacy safeguards as per the *CAC Determination 2015*, must therefore be assessed for vagueness and broadness, as to whether it sufficiently protects privacy. This is needed given the popular use of smart phones, which track the location of the device and reveal personal habits and traits, coupled with the discretion granted to the Agencies and the Telco, even though LI may not be voice content. The more fundamental question is: if LI is carried inside an IP packet, as a message, would this not make the LI the content of a communication in itself, even though it may be related to the voice call because the LI is generated at the time the voice call is made? If so, should LI be protected as the content of a communication exchanged within the network, as illustrated in

http://doi.org/10.18080/ajtde.v6n4.167

Figures 1 and 2, given it reveals SI and PI about the individual, equally sensitive as the contents of a voice call message? This would require an analysis of the legal definitions of terms such as 'communication(s)' and 'information related to the contents of a communication' (TIA Act, 1979 s 276). This analysis must be done in relation to how LI is legally classified as subscriber data, but is, as a matter of fact, technologically carried as the content of an IP packet and simultaneously reveals SI and PI. The potential dual nature of LI, both as a content and as information related to the voice call needs to be legally and technologically deciphered. Disregarding the content nature of LI and legally classifying LI simply as metadata, not only has the effect of denying the true nature of LI, but is not rooted in how the modern Internet-based communication network operates. This policy position may be entrenching the existing powers of the Agencies, despite being based on how an outdated analogue fixed-line copper-based network was designed and operated.

Packet Neutrality

As discussed above, the *TIA Act 1979* and the *TA 1997* are not technology neutral in that they do not treat all types of PI with the same privacy protection standards. The Attorney-General's Department (AGD), however, stated that the *TIA* must remain technology neutral (Department of Parliamentary Services, 2007, 7-8 14). Section 187AA (1) items 1–6 of the *TIA Act 1979* and section 275A of the *TA 1997* treat signal messages carrying LI inside SCTP/IP packets (*see Figure 2 below*) differently from the Transmission Control Protocol (TCP)/IP packets carrying voice or SMS communications. Voice content is also able to be carried in SCTP/IP packets (IETF 2007).

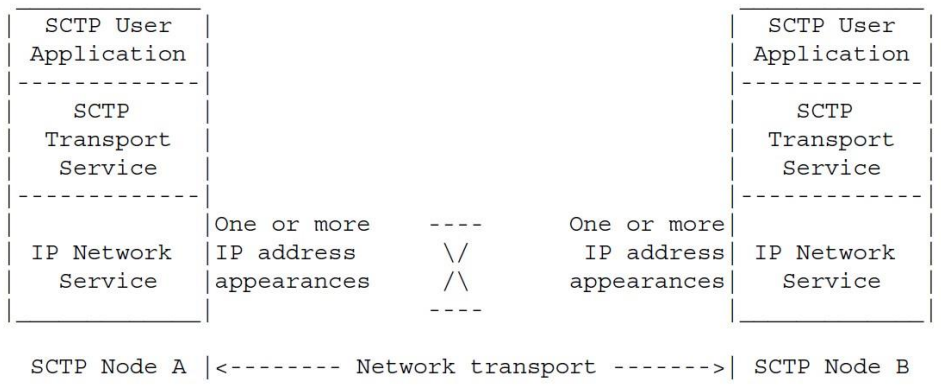


Figure 2. The structure of the SCTP, demonstrating the connection between two connected devices to carry SCTP messages (IETF, 2007, 6 [1.2]).

The IP packets carrying voice or SMS communications must only be stored with a domestic preservation notice and be disclosed and accessed only with a stored communications warrant (TIA Act, 1979 ss 39, 109, 110, 110A, 115). The SCTP/IP packets carrying LI are instead subject to mandatory data retention, without the need for similar protection to be disclosed and

http://doi.org/10.18080/ajtde.v6n4.167

accessed only with a stored communications warrant (TIA Act, 1979 ss 39, 109, 110, 110A, 115). Instead, it may be accessed with a self-certification authorisation and notification under the *CAC Determination 2015*.

The *TIA Act 1979* and the *TA 1997* should be packet neutral to both types of IP packets, so as not discriminate against LI by granting it less privacy protections under the *CAC Determination 2015* because LI is not the contents of a voice or SMS communication and is not carried in TCP/IP packets. The contents of TCP/IP packets and SCTP/IP packets both reveal PI and SI about the individual, and this may need to be the standard under which privacy must be better protected. The research questions raised in the section above are equally relevant to this discussion.

Greater Location Precision

The Agencies are granted access to coarse LI (Evidence to PJCIS, 2015), but the coarse LI from a modern IP-mediated LTE network generates and reveals more precise locations than earlier networks (Nohrborg, 2017). The coarse LI are the radio measurements or positioning measurements. The radio measurements or positioning measurements are the location estimates of the mobile device as generated by the IP-mediated LTE network itself, without the Telco analysing the location estimate to, for example, narrow down the location estimate from 100 m from the cell tower, to 50 m. The Telco is not required to analyse the location estimate to narrow the location of the mobile device from 100 m to 50 m. The Telco is simply required to disclose the 100 m location estimate to the Agencies. However, given that E-UTRAN is a new Radio Access technology, and is not reliant on older technologies, this enables the UE to be located with greater accuracy. E-UTRAN is planned to be technology neutral and robust for the future as 5G LTE networks are rolled out, in providing more precise geographic locations by using the Global Navigation Satellite System (GNSS): 'the E-UTRAN positioning capabilities are intended to be forward compatible to other access types and other position methods, in an effort to reduce the amount of additional positioning support needed in the future' (ETSI, 2017g, 12 [4.1]).

To better protect privacy, it needs to be recognised that the LI carried in a modern IP-mediated LTE network reveals more precise locations of the mobile device and of the individual user. This is also made possible by the use of femtocells that reveal more precise LI than traditional analogue and fixed-line telecommunications (Germano, 2010; ETSI, 2017a, 43 [8.1.3.2.1]; ETSI, 2017b, 20 [3.1]; ETSI, 2017c).

http://doi.org/10.18080/ajtde.v6n4.167

Privacy is Not Adequately Protected

Selvadurai, Gillies and Islam (2009) stated the operation of the *TIA 1979* threatened fundamental privacy interests. Privacy is not adequately protected (Michael & Clarke, 2012). In the view of Michael and Clarke (2012), privacy laws are eroded by exceptions and location privacy is not specifically addressed in any Australian law. Fernandes and Sivaraman (2015) also argued the Australian data retention law passed in 2015 strengthened protections for privacy. This claim was made without adequate analysis of the powers of the Agencies, the role of the Telco and the oversight limitations and exceptions placed on the Agencies in relation to LI. Reference was made to Internet of Things (IoT) devices, claiming that the retention laws may negatively impact privacy due to the deployment of IoT devices, but no specific mention was made of the significance of the LI of IoT devices. Zwolenski and Weatherill (2014) warned of the security and data protection pitfalls of IoT devices, but not in relation to the duties of the Telco to retain and disclose GPS data, and how mobile devices use the IP-mediated LTE network to create and exchange LI. Carona, Bosua Maynard and Ahmad (2016) examined the individual privacy risks posed by IoT, in relation to the Australian Privacy Principles (APP). Two risks identified related to the collection of data by means of unauthorised surveillance and uncontrolled data generation and use. Unauthorised surveillance was defined as the collection of mass data, which inferred the extensive tracking of individuals. The tracking is done without prior or informed consent. This definition did not make it clear whether access and use by the Agencies was considered unauthorised surveillance, seeing that the prior consent of the individual is not required for the Telco to retain and disclose LI (Carona *et al.*, 2016). Carona *et al.* (2016), however, admit that law enforcement bodies and the government comprise those parties that are involved with IoT data protection. The conclusion reached was that individual privacy is insufficiently guarded (Carona *et al.*, 2016). The data considered included LI, call history, movement and software applications collected from smartphones as the type of sensor, and its use for criminal investigations and fraud (Carona *et al.*, 2016). Carona *et al.* (2016) did not consider the APPs from the perspective of Australia's mandatory metadata retention and disclosure perspective, nor did they conduct a legal analysis.

Statutory 'privacy' jurisdiction is reliant on the existence of PI as per the *Privacy Act 1988* (Cth). Australian common law is said not to recognise the general right to privacy (Taylor, 2000: 238, 241; Human & Constitutional Rights Resource Page, 2018; the *Victoria Park case*, 1937; the *Lenah Game case*, 2001). Privacy is protected as a by-product of other interests that are already protected, such as confidentiality clauses from contracts with banks (Taylor, 2000: 240-241).[iii] Customers of Telcos are protected by privacy policies and standard terms and conditions that contain clauses to protect the privacy of the customers, and also under the *Privacy Act 1988* (Cth) (Vodafone Hutchinson Australia, 2017). Lachmayer and Witzleb (2014;

http://doi.org/10.18080/ajtde.v6n4.167

768) wrote that the powers of the Agencies were extended in 'hyper-legislation' because of the 9/11 attacks, with significant negative impacts on privacy, due to Australia's lack of a constitutional right to privacy (Roach, 2011). Bloch and Wark (2015) suggested that the increased data collection and access powers are unjustified as they intrude into the private lives of individuals. The authors Davies (2001), Williams (2005), Golder and Williams (2006), Bramwell (2012), Nicholson and Redlich (2015), Leonard (2015a, 2015b), Fair (2015) and Leonard (2015c) generally focussed on writing about the negative impact on privacy as a human right, because of the power to access retained telecommunications data without a judicial warrant. Rodrick (2009) wrote about the negative impact on privacy of mobile phone data location access and use. Rodrick (2009) discussed GPS and cell identification as methods of cellular device location approximation. The studies of these authors predate the introduction of the data retention scheme in 2015. In 2009, less detail was publicly revealed about the types of information to be retained. Privacy must now be studied in the context of PI in terms of the revised *Privacy Act*. After 2015, Shanapinda (2017) argued the collection of LI from social network websites also aims to complement the LI collected by the Agencies and undermines privacy safeguards such as those contained in section 180F of the TIA Act, 1979.

The Privacy Test

In terms of section 180F of the TIA Act 1979, the AFP, but not ASIO, must be satisfied on reasonable grounds that any interference with the privacy of any person that may result from the disclosure or use of the 'information or document' is justifiable and proportionate. This is the privacy test to be applied. Section 180F of the TIA Act 1979 refers to the proportionality principle, which lays the basis of using privacy itself as a tool to limit the powers of the Agencies. In other words, only LI, that is PI that is proportionate and justifiable, must be collected and used – nothing more. Selvadurai (2017) concluded that the post-2015 Australian framework that allows for access to telecommunications data was drafted in a manner that sought to overcome the privacy challenges the European Union (EU) faced. Selvadurai (2017, pp. 35-41, 36) referred to the EU Data Retention Directive (Directive 2006/24/EC) that was invalidated by the European Court of Justice (ECJ), stating that, given this legal precedent, it is interesting that Australia requires the retention of specific kinds of telecommunications data. Selvadurai (2017) questioned whether the retention of telecommunications metadata was a necessary national security initiative or a disproportionate interference with personal privacy, by analysing the Australian framework in relation to the ECJ's decision, given the similarities. Selvadurai (2017, pp. 35-41, 36) described the data as valuable to the Agencies, referring to the benefit of identification of associations between communicators, providing a precise digital profile and matching the data with data obtained from social media, to identify persons of interest. Selvadurai (2017, pp. 35-

http://doi.org/10.18080/ajtde.v6n4.167

41, 37) described the scope of the statute to analyse the effectiveness in calibrating the privacy and national security interests. This review proposes an assessment about whether the Australian framework can really be said to have overcome the privacy challenges, based on the functionality of the IP-mediated LTE network, as discussed in previous sections, critically analysing in detail the privacy safeguards introduced in 2015, based on BLD analytics. In other words, given the use of automatic data processing of the LI, as discussed in the section titled 'The Use of Big Data Analytics Software and Governance', is the retention and collection of LI for two years justifiable and proportionate?

The questions that future research may study include:

- given the broad inquiry and investigatory powers;
- the less stringent access rules; and
- given the broad meaning of national security as discussed in existing court cases, such as the *Jaffarie*, the *Farrel*, the *Day* and the *Samsonidis* court cases;
- the use of BLD analytics; and
- coupled with the lack of transparency,

what volume of LI retained and disclosed is proportionate and justifiable to ensure public safety, based on the risks posed?

Given the circumstances above, is privacy adequately protected? Is privacy a strong enough tool to effectively limit the powers of the Agencies or is privacy placed in a conflicting position, making it almost impossible to effectively restrict the powers of the Agencies?

The Privacy Protection Principles versus the Broad Investigatory Powers versus Public Safety

Clarke (2015, 2016) proposed the 'Meta-Principles for Privacy Protection' framework. Clarke (2016) proposed a privacy impact analysis in respect of data retention implementation. The principles include: evaluation, consultation, transparency, justification, proportionality, mitigation, controls and audit (Clarke, 2016). Clarke (2015) described the 2014 data retention proposal before the law was passed in 2015. After the *Data Retention Act 2015* was passed, the principles of transparency, justification and proportionality were incorporated into the privacy safeguards, and now require an empirical analysis.

Selvadurai, Kisswani, and Khalaileh (2016, p. 229) simply described the Australian interception law reform process in relation to the proportionality principle. The reforms were justified on the basis of enhancing legislative longevity, due to the persistent changes of telecommunications technologies (Selvadurai *et al.*, 2016, p. 230). However, as illustrated by the digital and mobile transformation of communications, from analogue and fixed-line

http://doi.org/10.18080/ajtde.v6n4.167

communications, laws may lose touch with reality and continue to grant more powers to the Agencies due to the advancements in communications technology. Keeping the laws unchanged does not allow for a check-in to assess the impact of these technological advances, as discussed in previous sections. Selvadurai, Kisswani, and Khalaileh (2016) assessed the application of the proportionality principle. This was done specifically with regard to conducting interceptions, and not access to LI in relation to technological convergence and 'heightened national security' (Selvadurai *et al.*, 2016, pp. 230, 239). In the context of telecommunications law, the proportionality principle was described as weighing up potential threats to 'public security against possibly breaking the rights of the person – the aim is to ensure that collecting the content is reasonably proportionate to the desired goal….' (Australian AGD, 2012, p. 26). The concept of 'public safety' refers to the safety of the public (Australian AGD, 2012, p. 26; Selvadurai *et al.*, 2016, p. 232). Selvadurai *et al.* (2016, pp. 231-232) noted that the concept of security is broad and open to interpretation, but did not analyse the *Jaffarie*, the *Farrel*, the *Day* and the *Samsonidis* court cases.

Selvadurai *et al.* (2016, p. 229) placed emphasis on the 'likely threat'. However, the powers of the Agencies involve investigating persons, to determine if they may pose a security threat: '(a) … undertake inquiries to determine whether a particular subject or activity is relevant to security' (Attorney-General's Guidelines, s 6.1.). In regard to description by Selvadurai *et al.* (2016, p. 229) of the 'proportionality principle', it appears that the powers of the Agencies are defined, insofar as the Agencies seek to investigate or conduct an inquiry in circumstances where there is no 'likely threat'. However, the LI is collected to assess if a person may pose a threat in the future, and the collection of the LI is not always legally required to be based on reasonable suspicion or on goodwill, to determine if a person is relevant to security. There is a requirement for the AFP to have an 'investigation' in order to collect prospective location information (TIA Act, 1979 s 180(4)). If the AFP is requesting access to prospective location information for a serious offence or an offence against the law of the Commonwealth that is punishable by imprisonment for at least 3 years, the AFP needs to have suspicion of a past, present or future serious offence, based on reasonable grounds, to collect prospective location information (CAC Determination 2015 Part 3 s 3.01 (1) Item 3(c) (viii), (ix)). It is, however, only when it comes to serious offences that the AFP is required to conduct an 'investigation' and have suspicion of a past, present or future serious offence, based on reasonable grounds (TIA Act, 1979 s 180(4)*; CAC Determination 2015* Part 3 section 3.01 (1) Item 3(c) (viii) and (ix)). It follows that, for minor offences, historical location information may be collected without a suspicion of a past, present or future serious offence, based on reasonable grounds.

It is only in respect of prospective location information for serious offences that the short description of offences is required to be stated in the authorisation under the *CAC*

http://doi.org/10.18080/ajtde.v6n4.167

Determination 2015, and only in respect of the AFP. It is only in respect of prospective location information for serious offences that an 'investigation' of offences is required, and only in respect of the AFP (*CAC Determination 2015*, Schedule 1 Part 2 s 2.02 (1) Item 8). It also follows that, for serious offences, historical location information may be collected without the suspicion of a past, present or future offence, based on 'reasonable grounds'. In other words, no reasonable grounds are required to collect the historical location information under the *CAC Determination 2015* for serious offences (TIA Act, 1979 s 178(2); *CAC Determination 2015* Part 3 section 3.01 (1) Items 1- 6). The AFP does not need to have an investigation as a requirement before collecting the historical location information for a serious offence (TIA Act, 1979 ss 6A, 6B). There seems to be no requirement for the AFP to have an active 'investigation', as defined in the *Day court case*, as a requirement to collect historical location information. It means the AFP does not need to have a suspicion of a past, present or future offence, based on reasonable grounds, to collect the location information when it is putting the facts together about the actions of the individual in order to allege that the person has committed a crime. Given these broad investigatory powers, the Agencies may collect and use LI under the less stringent requirements of the *CAC Determination 2015*. The two conflicting interests can be still better balanced than they are at present by requiring reasonable suspicion and a judicial warrant. Without the latter more stringent requirements but pending a rigorous study, it may be said that privacy appears to be unfairly compromised in favour of 'public safety'.

It may be said that it appears that the privacy safeguards introduced after 2015 continue to be threatened by the fact that the Agencies continue to self-certify the authorisations, as they have always done when copper-wire landline telecommunications was in use (Evidence to PJCIS, 2015, 31). This is despite the revealing nature of the modern IP-mediated LI. A detailed study, based on the legal powers, contrasted against the oversight mechanisms and the functionality of LI may potentially support the above argument. The proportionality test can then be critically analysed in this relevant context of self-certification and 'public safety'.

Lack of Transparency

Williams and Hardy (2014) stated metadata access is not transparent - disclosing that ASIO collecting data for special intelligence operations is a criminal offence. This poses risks to media freedom. Rix (2013) studied ASIO investigations about the questioning and detention of suspects and the power to keep the information about this secret. Rix (2013, p. 240) objected to the claims for secrecy, arguing 'there can be little dispute with the assertion that some level of secrecy is required by ASIO to enable it to deal effectively with the terrorist threat. It is far more difficult to accept that complete secrecy, and no accountability, equates to watertight

http://doi.org/10.18080/ajtde.v6n4.167

security'. Rix (2013) went on to state that the public is not able to scrutinise the powers of the Agencies due to the level of secrecy. Sarre (2017, p. 176) states it is still too early to determine whether the telecommunications data retention laws are effective, given the confidential nature of the investigations. In respect of ASIO's confidential access to LI, the lack of transparency makes it difficult to assess whether the Agencies are complying effectively with the privacy safeguards at the time of collecting the LI, and whether the actions of the Agencies are reviewed in a sufficiently open administrative and judicial systems afterwards. The lack of transparency contributes to the self-serving character of the LI retention and disclosure framework. The Telco is prohibited from informing the person of the LI collected about them (TIA Act, 1979 ss 181A (1), (2), (4), (5); 181(B1), (2), (4), (5); 182A (1), (2)). The collection of the LI is a confidential process (*CAC Determination 2015* Schedule 1, Part 3; TIA Act, 1979 s 108(1)). The individual is not informed of the LI requests and disclosures. In replying to the PJCIS' comment that the Journalist is not informed about the application for a Journalist Information Warrant (JIW), the Attorney-General replied that a person under investigation may destroy evidence if informed and frustrate the investigation (Letter from the Attorney General, 9 February 2016). However, the lack of transparency has a profound impact on the ability of the individual to try and assert their privacy. There is little or no opportunity for an individual to become aware that the LI may have been misused. There is little or no opportunity for an individual to know that only LI that was reasonably necessary and proportionate was collected. For the person to lodge a complaint they would need to be aware of the privacy breach of section 180F. The affected individual would find it challenging to collect copies of the authorisations and notifications to challenge the Agencies and whether and how they met the post-2015 privacy tests. It is significant that the oversight bodies such as the Office of the Inspector-General of Intelligence and Security (OIGIS) and the Commonwealth Ombudsman conduct their investigations based on complaints (IGIS Act 1986 (Cth) ss 10, 11, 12*;* *Data Retention Act* Schedule 3). However, obtaining the information necessary to identify a possible privacy breach and to make a credible and specific complaint is practically almost impossible. Can privacy be said to be adequately protected under these circumstances? The workings of the oversight bodies may require further scrutiny.

Less Stringent Oversight Measures and the Broad Powers

Leonard (2015c) did not address how the broad investigatory and discretionary powers of the Agencies to collect LI, and the discretion of the Telco to voluntarily retain and voluntarily disclose LI (TIA Act, 1979 ss 177(1), 178(3)), interacts to create an environment that subjects the privacy of the individual to the commercial and law enforcement interests, and without providing sufficient privacy safeguards. Enhanced accountability was introduced in the form of greater legislative oversight, with the granting of additional supervisory powers to the

http://doi.org/10.18080/ajtde.v6n4.167

Commonwealth Ombudsman (TIA Act, 1979 Schedule 3). This included the complaint procedures. As stated in the section above, the lack of transparency makes lodging complaints difficult, potentially weakening the oversight and protecting privacy poorly.

The powers of the Agencies are also broad because LI is not classified as 'contents of a communication'. LI is classified as 'metadata', and less stringent requirements are applied to access and use LI (TIA Act, 1979 s 275A; LCARC, 2015, p. 77 [71.182]). The *CAC Determination 2015* is the less stringent procedure that is used to access LI. Burgess (2015, pp. 16-17) argues new 'metadata' laws are vital for the police. There is no doubt about the value of the LI. The Agencies can still perform their functions effectively using valuable LI, but privacy can still be better protected than it is currently protected under the *CAC Determination 2015*, by amending the self-certification process and introducing a judicial warrant to access and use LI.

In 2012, Svantesson (2012, pp. 268, 275) described how private data could be accessed in Australia for specified purposes, as opposed to bulk data collection. Accessing data for a specific purpose appears to be a myth. The LI can be collected for broad purposes if they are related to undefined police activities and functions. As stated in the paragraph titled 'The Privacy Protection Principles versus the Broad Investigatory Powers versus Public Safety', this may pose unfair risks to privacy. Svantesson (2012, pp. 270–271) referred to the Attorney-General's Guidelines to be followed regarding access to the data, distinguishing between requests for data and voluntary disclosure, and stated the Agencies were generally compliant with the laws when accessing and using telecommunications data. However, an oversight tool, such as the *CAC Determination 2015* that is used to protect privacy, may be more permissive than it is restrictive, and have such a low threshold that the Agencies are able to easily comply. Sarre (2017) argues that the Agencies are generally compliant with the laws, and states the Agencies use their powers for the purposes of security and law enforcement. The powers are broad and therefore compliance is easier due to the low access threshold. The oversight test used only inspects the 'extent' of compliance, which may send the message that non-compliance is accepted and condoned (*Data Retention Act* (Cth), s 186B).

Jones (2016) argued Australian intelligence is imprecise because it is subject to political distortion. The expanding legal powers, in Jones' view, have evolved into a national security state that exacerbates domestic accountability issues. Jones (2016) did not explicitly analyse the powers of the Agencies in relation to the IP-mediated LTE network, in terms of how the network locates the mobile phone with greater precision and reveals PI and SI. Jones (2016) did not contrast the revealing nature of the network against the Attorney-General's Guidelines and the *CAC Determination 2015*. These two documents do not contain clear restrictions about inquiries and investigations that have political and racial angles, to ensure good faith.

http://doi.org/10.18080/ajtde.v6n4.167

The two documents also do not clearly address how the Agencies can prevent bias and prejudice to avoid potential misuse. In the *Jaffarie case* (16 [17]), the court relied on section 20 of the *ASIO Act* 1979 as preventing undue influence from the outside but did not question whether any internal processes exist and are applied to address biases of officers themselves and undue influence from the outside.

Telecommunications Data as Personal Information

Telephone metadata is valuable in making inferences that are of a sensitive nature (Mayer, Mutchler and Mitchell, 2016). Mayer *et al.* (2016) assessed the privacy characteristics of telephone metadata, using a crowdsourcing methodology. The study concluded that telephone metadata was 'densely interconnected' and re-identifiable – this even though the privacy protections of telephone metadata are not significant, and the bulk telephone metadata collection program of the National Security Agency (NSA) relied on data that is not considered 'Personally Identifiable Information' (PII) (Mayer *et al.*, 2016). Using the location histories of the participants, re-identification of the participants was performed using location data from social networking sites.[iv] The researchers could often make inferences regarding the geo-location of the participants' residences from call and SMS data. The location data did not disclose exact locations (Mayer *et al.*, 2016). Locations could, however, be inferred by re-identifying the business the participants called, supported by location addresses from the websites, and using this information to guess their residential premises. The final step was to use the Google Geocoding API[v] to assess the longitude and latitude of the businesses and homes (Mayer *et al.*, 2016). If privacy is to be appropriately protected, the law must recognise that LI is generated and exchanged as a communication that reveals more precise location estimates, and PI and SI about the individual. If the voice or SMS communication is made via a femtocell, the location estimate of the eNB selected to handle the communication can be just as precise as if signal strengths from various towers were used. The Telco is practically made to retain LI that was selected by the femtocells deployed inside and outside homes to boost the cell phone coverage (Germano, 2010). If the femtocell's signal is the strongest, the cell phone will connect to the femtocell (Battersby, 2012). The precision of these base stations can be within a range of 100 meters, such as the Vodafone site at the University of New South Wales (UNSW) (ACMA 2017a). Electronic Frontiers Australia (EFA) argued mobile phone location accuracy approximates 200 to 100 meters in metropolitan and urban areas. Electronic Frontiers Australia (EFA) argued Assisted-GPS would greatly improve mobile phone LI (Department of Parliamentary Services, 2007, 14). The LI is disclosed raw and unprocessed, but that means a 100 m coverage radius for finding a person. It is no longer like looking for a needle in a haystack, but more like using a microscope. Given the development of modern IP-mediated communications technologies, with base stations that are nearer to each other and

http://doi.org/10.18080/ajtde.v6n4.167

the coverage radius smaller in urban areas, the licensing and use of femtocells with a proximity radius of 100 m, and the popularity of smart phones with satellite positioning ability, the reliance on this traditional content versus metadata distinction may be working to the benefit of the Agencies and compromise privacy protections. The scales are thereby subtly skewed in favour of the powers of the Agencies rather than adequately balancing the more revealing nature of modern-day mobile communications. To gain access to use LI is more flexible than under the traditional rules prescribed for warrants and domestic preservation notices. As a result, LI may need to be protected in the same way as the contents of a communication, under the legal system, given that all these types of communications reveal PI and SI.

The Dual Nature of Telecommunications Data

Johnston (2017, pp. 82-83) advanced the argument that LI cannot be about just one thing but can also be about the individual and therefore be PI. In the *Telstra Corporation Limited case*, the Deputy President decided telecommunications data not used for billing purposes, and from which the identity of the person is not obvious, is not 'about' the individual and is therefore not PI. Johnston (2017) argued that this was a narrow and binary formulation. The information need not be about only one phenomenon or aspect. Johnston (2017) argued that this decision might result in entities denying their privacy obligations by arguing that the information is strictly 'about' the service, such as banking transactions or medical procedures, to the exclusion of the privacy rights of the individual. This review agrees with Johnston (2017). The Administrative Appeals Tribunal (AAT) dissected how the technology operates, but then took a very technology-driven and narrow interpretation. LI is inherently designed to track the mobile device in the IP-mediated LTE network in order to deliver the communication to the device, as illustrated by Figure 1. However, LI can be applied for a myriad of other purposes, especially when aggregated using BLD analytics technologies, to reveal PI and SI. The later decision of the Federal Court: the *Privacy Commissioner case*, that stated information can be about a myriad of things, requires greater scrutiny in the BLD and IP-mediated LTE network contexts, in relation to the Attorney-General's Guidelines and the *CAC Determination 2015*, as governance tools. According to the *Telstra Corporation Limited case*, any other application of the telecommunications data generated does not alter the primary purpose and functioning of the technology, even if the telecommunications data is matched with other external information and reveals habits about the person, the residence of the person or details about the work-related activities of the person. The information cannot be just about one thing. The *Privacy Commissioner case* planted the seed for the idea that the LI may not just be about the primary purpose of delivering communications. If the facts can demonstrate that the LI was matched, and the identity of the person was revealed or is reasonably ascertainable, by the LI that tracked the mobile device, whether it delivered the

http://doi.org/10.18080/ajtde.v6n4.167

voice call or whether there was no voice communication to deliver, the LI can also at the same time be about the individual (Privacy Commissioner case 16 [63]). Unlike the AAT, the Federal Court accepted that the information can be about various things: 'Information and opinions can have multiple subject matters' (Privacy Commissioner case 16 [63]).

A single piece of information that starts out by not being about a person may end up being about a person when it is combined with other separate pieces of information (Privacy Commissioner case 16 [63]). If the pool of LI is combined with extra information, the LI may end up being PI. The Federal Court stated, based on the facts of every case, at first, it must be determined whether every single item of information or the combined pieces of information requested from the Telco are about the individual (Privacy Commissioner case 16 [63]). Secondly, once having determined that the information is about an individual, in order to determine whether the identity of the person is reasonably ascertainable, one must then make an evaluative conclusion. The Federal Court stated that aggregated information may be about an individual, even if a single piece may not be about an individual (Privacy Commissioner case 16 [63]). The Federal Court differentiated between a case of an identity that is obvious from the information, and a case where the identity may not be apparent. As illustrated by Figures 1 and 2, LI is inherently designed to be about tracking the mobile device in the IP-mediated LTE network, with the view of delivering the communication (the location information contained in a message) to the mobile device or the Location Server or the SEDNode web portal from where the LI is downloaded and given to the Agencies (iiNet, 2015). However, LI may be applied to a myriad of other purposes and, as such, the LI forms various relationships that end up being about the individual. The primary design and purpose of LI remains, but that does not exclude other relationships. The LI may start out being about the delivery of the voice and SMS communication to the recipient, as it is exchanged via the Network Elements, such as the Location Server, as illustrated in Figure 1, but a new relationship is formed with the individual at the secondary level, when the LI reveals the physical location of the mobile device and in turn that of the individual, leading to opinions being formed about the character of the person. The LI now serves a secondary purpose, but still an important purpose that may require greater privacy protection, under more stringent requirements than what the *CAC Determination 2015* provides.

The Use of Big Data Analytics Software and Governance

To Moses and Chan (2014, p. 645) Australia was starting to recognise the potential of Big Data (BD) analytics for the enhancement of national security. In BLD analytics, various pieces of information are aggregated to reveal new information that can be used in investigations by the Agencies. Chan and Moses (2017) explored the likely impact of BD technology in relation to

http://doi.org/10.18080/ajtde.v6n4.167

the Australian law enforcement and national security landscape. Chan and Moses (2017, p. 300), and Smith, Moses and Chan (2017) made the clarion call for a better understanding of BD analytics technology, its challenges, its uses and influence, and its proper governance and regulation. BD analytics is about establishing connections by using new software and hardware technologies to analyse huge sets of diverse data (Maurushat, 2016, p. 2). Maurushat (2016) described the perceived advantages, risk and challenges around BD and its uses by the Agencies. The uses related to being able to 'predict' and investigate criminal and intelligence incidents (Maurushat, 2016, p. 1). The risks associated with such use included the threat to privacy and the erosion of trust (Maurushat, 2016, pp. 9-10). Selvadurai (2017) described BD as valuable to the Agencies, referring to the benefits of identification of associations between communicators, providing a precise digital profile, and matching the data with data obtained from social media to identify persons who are relevant to security or suspected of having committed an offence. Selvadurai (2017) argued this undermined privacy protections. Shanapinda (2017) argued the public has a legitimate expectation not to be tracked online by the Agencies, when describing the application of BD analytics over retained data, and then merged with open source intelligence (OSINT), for investigations. Privacy is impacted at the time the LI is retained – the PI about the individual is stored. Privacy is again impacted at the time the LI is disclosed to the Agencies – the PI about the individual is shared. Privacy is impacted again at the time the LI is analysed using BLD analytics, to reveal PI about individuals. The BD analysis is automated processing of the LI, and with greater efficiency than previous manual operations. There is no telling what treasures two years' worth of LI may reveal about the individual. There is no telling how relevant the PI that has been revealed is to the investigation or inquiry in question. The *CAC Determination 2015* does not regulate how the data collected and PI revealed may be treated and applied to the investigation at hand. The extra PI revealed is open to the risk of misuse, to aid the investigation. The newly revealed PI may broaden the scope of the investigation that can potentially incentivise Agencies to continue indefinitely to use the PI to find something criminal against all odds, whether minor or serious, instead of dropping the inquiry or investigation. Under a judicial warrant, the scope of the inquiry or investigation would be clearly defined and authorised. Under the *CAC Determination 2015*, however, the Agencies can bypass such a narrowed scope – leading to scope creep. Throughout all this, the PI is retained indefinitely by the Agencies, and this too impacts the privacy of the individual. The ease with which LI is available to the Agencies for two years, that the LI can be collected from the Telco, and that the LI can be processed by automated means to disclose PI and SI are the sorts of circumstances that may impact privacy heavily. The safeguards adopted in 2015 may therefore be inadequate to protect privacy. It may be justifiable and proportionate that a two-year history of the person be revealed, in order

http://doi.org/10.18080/ajtde.v6n4.167

to keep the public safe, but could a week's or a month's history do? The *CAC Determination 2015* is silent on these sorts of governance issues, and does not offer such guidance.

Unfair Limits to Civil and Property Rights

To better protect privacy, the Telco is not required to retain LI when the individual is not making a call. As an exception, the Telco may only retain LI at the start and at the end of a communication. This is commendable, but the Telco may, however, legally retain this LI voluntarily (TIA Act 1979 ss 187A (1), 187AA (1) item 6). To the AGD, this reduces the level of detail because the Telco is not required to retain the regular continuous records of the location information:

> [T]he nature and volume of location information that service providers will be required to keep has been strictly limited to ensure that service providers are not required to keep continuous records about the location of a device, or anything approaching that level of detail (PJCIS 2015, 93 [3.79]).

The detail of LI to be retained is therefore dependent on whether the person uses the mobile device to make calls or to send an SMS. This position sends the message that, if a person wants less LI about their communications to be retained and want less PI about them retained and disclosed, then the person should reduce their level of communication with their friends, families and other associates. Mobile devices are popular and people are dependent on these devices (ACMA, 2017, 17). Not using the device or reducing its use would be a form of self-censorship and create a chilling effect on civil and political rights. This impacts the affected person's privacy and free speech, to communicate at will, when and how they like, and not to be concerned that, if they speak too often, the Telco would retain more LI than they would be comfortable to disclose to the Agencies.

The individual must also be wary about the location from which to communicate. The person seeking to protect their privacy may limit their movements or choose not to carry their mobile device with them for fear of being tracked. The freedom of movement of the person is indirectly curtailed. The person would also be unfairly restricted from enjoying and exercising full ownership over his or her private property. The psychological impact is another factor to consider: the fear that is created and the mental health effects of being under constant surveillance with every communication made and every location entered. These are the negative impacts of the LI retention and disclosure framework that may be studied further.

Analysis and Recommendations for Future Research

The traditional argument from the authors cited has been to criticise the powers of the Agencies to access and use information collected from the Telco, in relation to privacy. As

http://doi.org/10.18080/ajtde.v6n4.167

stated above, this information includes LI, which reveals PI and SI about the individual user. It is therefore known that the powers of the Agencies impact the privacy of the individual. However, privacy is rarely studied from the perspective of being a tool used to help limit the powers of the Agencies. Many authors have written about the impact on privacy of the powers of the Agencies, but not about the powers and the limits on those powers in the period from 2015 to date, and not in enough detail about how modern technologies operate. This was a period where the powers of the Agencies came under the public spotlight as the Agencies renewed their commitment to better protect privacy, while simultaneously seeking new powers to collect retained LI (TIA Act 1979 s 180F; *CAC Determination 2015*). The duties imposed on the Telco to retain LI for two years, coupled with the discretion to also retain more LI for commercial purposes, are an essential component of the changes made since 2015 and they require empirical investigation, in order to confirm what reasonably appears to be, from the discussions above, a negative impact on privacy.

As legal and policy positions change, the context and status of these frameworks evolve. For a better contemporary understanding, the recent changes require investigation to assess their modern impact on privacy in the new environment, as opposed to continuing to rely on outdated concepts that may be decreasingly relevant to emerging practices. At the same time, privacy is also a check on the powers of the Agencies (TIA Act 1979 s 180F; *CAC Determination 2015*). The Agencies are entrusted with safeguarding privacy interests as well as pursuing law enforcement interests to obtain, access and use LI (TIA Act 1979 s 180F; *CAC Determination 2015*). The *TIA Act 1979* classifies LI as subscriber data and as metadata,[vi] despite the revealing and sensitive characteristics of LI (APC, 2015, 42 Appendix B [8]). This means the Agencies can access LI under less stringent requirements than the contents of a voice or SMS communication (*CAC Determination 2015*; TIA Act 1979 ss 107H, 108(1)). The proposed research can investigate how the powers of the Agencies and the revised privacy safeguards are aligned. The research can confirm the fact that privacy is the most vulnerable value to be protected, but, at the same time, privacy is the target of investigations – the Agencies must protect privacy but are allowed broad powers to access and use PI intrusively. The research can theorise on the dynamic interaction of these opposing interests and the resulting impact on privacy.

After having studied the oversight tools the Agencies must comply with and given that the Agencies have as their primary consideration the greater interest of law enforcement and national security, solely entrusting the Agencies with safeguarding privacy may be creating a clear conflict of interest. It is difficult to balance the powers of the Agencies and protect privacy under these circumstances. The studies by the authors did not sufficiently dissect how LI generated and exchanged in modern telecommunications networks is accessed under

http://doi.org/10.18080/ajtde.v6n4.167

authorisations issued by the Agencies themselves instead of a judge, and how privacy is used as a limit to those very powers, and the clear conflict that arises. The studies proposed can describe the weaknesses of the legal privacy protections for LI, in contrast to the stronger protections for voice and SMS contents, which are as sensitive and as personal as LI (*CAC Determination 2015*; TIA Act 1979 ss 107H, 108(1)).

The review reveals a lack of detailed research in the following areas:

- How LI is generated and exchanged in the IP-mediated LTE network, and how mobile devices are tracked and create precise location estimates, in the context of the exceptions and privacy safeguards introduced after 2015;
- The discretionary powers of the Agencies to use PI and SI to identify inquiries and investigations to pursue, to enforce the law and perform their functions, and to carry out activities related to their functions and purposes (Revised Explanatory Memorandum, 2015, p. 5 [22] – [23]; *CAC Determination 2015*);
- The flexible oversight principles contained in the guidelines that create conflicts between law enforcement and privacy interests for the Agencies (Attorney-General's Guidelines s 13; *CAC Determination 2015*);
- Court precedents about security, investigations, the transparency and review opportunities of the powers of the Agencies, interpreting the discretionary powers of the Agencies to inquire into, pursue and enforce the law; and
- A critical analysis of what is content, and how content is treated under the law versus how LI is treated as metadata, based on how equally sensitive LI and metadata are, given how modern LTE networks and BLD operate.

The Agencies are required to comply with various privacy standards, but these standards are as vague as the broad powers of the Agencies (Attorney-General's Guidelines s 13; Privacy Act Schedule 1 Part 2 3.1.). This creates a framework that makes it difficult to challenge the powers of the Agencies at the time of collecting the LI from the Telco. Unlike warrants, where Judges oversee privacy as independent third parties, the Agencies play the role of the judge (Telecommunications (Interception and Access) Regulations, 2017 (Cth) Schedule 1, Form 6). The moment when LI is collected from the Telco is the moment when privacy is at its most vulnerable, and the moment external oversight is appropriately required but clearly lacking.

Subject to a detailed study, the framework appears to be designed in the following manner:

- The inquiry and investigative powers are broad;
- the restrictions are more enabling than restrictive (Attorney-General's Guidelines);
- the collection procedures are not transparent (*CAC Determination 2015* Part 3; TIA Act 1979 ss 107H, 108(1));

http://doi.org/10.18080/ajtde.v6n4.167

- the standards to collect and use LI are high and based on the 'reasonable man' test but at the same time are subject to the sole discretion of the Agencies, with no avenue to challenge whether the test was complied with objectively (*CAC Determination 2015* Part 3; TIA Act 1979 ss 107H, 108(1), Parts 1–3);
- the Telco is not required to follow the privacy standards of reasonable, necessary, justifiable and proportional when disclosing LI to the Agencies, whereas the Agencies are required to do so when requesting the LI (TIA Act 1979 ss 175-184; TA 1997 ss 275A, 276, 313(3), 313(4), 3131(7); *CAC Determination 2015*); and
- the Agencies are not required to follow the privacy standards of reasonable, necessary, justifiable and proportional when collecting LI from the Telco in respect of all individuals (*CAC Determination 2015;* the *Samsonidis* case). As a result, the privacy tests are selectively applied, resulting in potential discriminatory treatment.

The commercial and network maintenance interests of the Telco need to be examined, as well as the indefinite retention period and continued use of the LI, which leaves the LI at the discretion of the Agencies for longer than two years. The Telco's discretion to disclose LI voluntarily to the Agencies and the discretion of the Agencies and the Telco to retain LI for any length of time jointly appear to outweigh the privacy interests of the individual in an unfair manner that appears to lead to poor privacy safeguards. This, however, needs to be examined thoroughly. The privacy of the individual is left to the discretion of the Agencies and the Telco. This framework appears to lead to the inadequate protection of privacy, and leaves privacy vulnerable as a check on the powers of the Agencies. Access to LI should be implemented fairly. It may be reasonable to agree that LI should be granted similar legislative privacy protections as voice and SMS communications.

Conclusion

This article was a review of existing literature with comments about the adequacy of the body of work that has been undertaken to date. The paper reviewed the inadequacy of existing literature to holistically analyse the impact on privacy after the 2015 introduction of the telecommunications data retention and disclosure framework, based on how the IP-mediated LTE network generates, stores and shares LI and how this LI is analysed to reveal SI and PI, using BLD analytics, and in relation to existing governance tools. The paper highlighted how the powers of the Agencies to access and use telecommunications data appear not to adequately protect privacy before 2015 and do not do so after 2015, but one must accept that this conclusion requires a contemporary and detailed study to confirm the preliminary arguments.

http://doi.org/10.18080/ajtde.v6n4.167

Acknowledgements

Thanks to UNSW, SEIT (ACCS, UNSW Law); and the D2D CRC LTD, whose financial support made this research possible.

References

ACMA. 2017a. Site Location Map <https://web.acma.gov.au/rrl/site_proximity.main_page>

ACMA. 2017b. *Communications report 2016–17*

Australian Security Intelligence Organization (ASIO) Act 1979 (Cth)

Attorney-General's Department. 2015. Submission No 27 to the Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, 16 January 2015

Attorney-General's Department. 2016. 'Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)', June (Attorney-General's Guidelines). http://www.asio.gov.au/About-ASIO/Oversight-and-Accountability/Attorney-General-Guidelines.html

Australian Privacy Commissioner. 2015. Submission No 92 to the Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, January 2015

Australian Attorney-General's Department. 2012. 'Equipping Australia against Emerging and Evolving Threats', *Discussion Paper*, July 2012

Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd. 2001. HCA 63 (the Lenah Game case)

Australia & New Zealand Bank v Ryan. 1968. 88 WN (Pt l) (NSW) 368

Barclays Bank Plc. (Trading as Barclaycard) v Taylor [l989] 1 1 WLR 1066

Battersby, L. 2012. 'Telstra offers signal boost – at a price', *Sydney Morning Herald* (online), 6 July 2012 http://www.smh.com.au/business/telstra-offers-signal-boost--at-a-price-20120706-21l5f.html

Bellovin, SM; Blaze, M; Landau, S; Pell, SK. 2016. 'It's Too Complicated: The Technological Implications of IP-Based Communications on Content/Non-Content Distinctions and the Third Party Doctrine'. *Harvard Journal of Law & Technology,* 30(1), 1-101

Bloch V; Wark V (eds). 2015. 'Australian Internet Data Collection – Are We Fighting to Protect Privacy Which Is Already Lost'. *Communications Law Bulletin,* 34(2), 23-27

Bramwell, O. 2012. *A delicate balancing act: data protection, individual privacy & the right to be forgotten: tackling data retention in the digital age* (LLB Thesis). Melbourne, Monash University

Burgess, M. 2015. 'Why new "metadata" laws are vital for police'. *Police Association (Victoria) Journal,* 81(5), May 2015, pp 16–17. https://search.informit.com.au/documentSummary;dn=340074488849139;res=IELAPA

Carona, X; Bosua, R; Maynard, SB; Ahmad, A. 2016. 'The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective'. *Computer Law & Security Review,* 32(1), 4–15. http://dx.doi.org/10.1016/j.clsr.2015.12.001

Carpenter v. United States (Supreme Court of the United States of America, No. 16-402, 22 June 2018) IV 18. https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

Christoj v Barclays Bank. 2000. 1 WLR 937

Chan, J; Moses, LB. 2017. 'Making Sense of Big Data for Security', *The British Journal of Criminology,* 57(2), 299-319

Clarke, R. 2015. 'Data retention as mass surveillance: The need for an evaluative framework'. *International Data Privacy Law,* 5(2), pp 121–132. http://dx.doi.org/10.1093/idpl/ipu036

Clarke, R. 2016. 'Privacy Impact Assessments as a Control Mechanism for Australian National Security Initiatives'. *Computer Law & Security Review,* 32, pp 403–418.

Commonwealth, Parliamentary Debates, Senate, 25 March 2016, 2294 (George Brandis MP)

Communications Access Coordinator's (CAC) *Telecommunications (Interception and Access) (Requirements for Authorisations, Notifications and Revocations) Determination 2015 (Cth) (at 9 October 2015) [CAC Determination 2015]*

Davies, D. 2001. 'Unprincipled privacy: Why the foundations of data protection are failing us', *UNSW Law Journal,* 24(1), 284-289

Day v Commissioner, Australian Federal Police. 2000. FCA 1272 (11 September 2000) (the *Day* case)

Department of Parliamentary Services (Cth), Bills Digest, No. 10 of 2007-08, 3 August 2007

D*igital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (C-293/12 and C-594/12) [2014] ECJ

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006

ETSI. 2016a. 'Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Functional stage 2 description of Location Services (LCS)', (3GPP TS 23.271 version 13.0.0 Release 13)

ETSI. 2017a. 'LTE; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Stage 2 functional specification of User Equipment (UE) positioning in E-UTRAN', 2017, (3GPP TS 36.305 version 14.2.0 Release 14)

ETSI. 2017b. 'Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data', 2014, TS 102 657 V1.15.1 (2014-08)

ETSI. 2017c. 'LTE; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2', 2017

ETSI. 2017d. 'LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); LTE Positioning Protocol A (LPPa)'

ETSI. 2017e. 'LTE; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)'

ETSI. 2017f. 'Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Network architecture', 2017, (3GPP TS 23.002 version 14.1.0 Release 14) ETSI TS 123 002 V14.1.0 (2017-05)

ETSI. 2017g. 'Universal Mobile Telecommunications System (UMTS); LTE; Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol'

Evidence to PJCIS, 30 January 2015, 48 (Malcolm Lanyon, Assistant Commissioner Commander, Special Services Group, New South Wales Police Force)

Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 30 January 2015, 31 (Peter Leonard Guildford, Chairperson of the Media and Communications Committee, Business Law Section of the Law Council of Australia)

Farrell; Secretary, Department of Immigration and Border Protection (Freedom of information) [2017] AATA 409 (31 March 2017) (the *Farrel* case)

Fair, P. 2015) 'Mandatory Data Retention: Overview and Issues Citation'. *Inhouse Counsel*, 19(8), 110

http://doi.org/10.18080/ajtde.v6n4.167

Fernandes, F; Sivaraman, V. 2015. 'It's only the beginning: Metadata Retention laws and the Internet of Things'. *Australian Journal of Telecommunications and the Digital Economy*, 3(3), 47–57. http://dx.doi.org/10.18080/ajtde.v3n3.21

Federal Commissioner of Taxation v Australia & New Zealand Banking Group (1979) 143 CLR 499

Germano, A. 2010. 'The Impact of Femtocells on Next Generation LTE Mobile Networks', (PowerPoint Presentation at the FemtoForum) 1–30. ftp://www.3gpp.org/Information/presentations/presentations_2010/2010_05_Moscow/Femto_Forum_Germano.pdf

Golder, B; Williams, G. 2006. 'Balancing national security and human rights: Assessing the legal response of common law nations to the threat of terrorism'. *Journal of Comparative Policy Analysis: Research and Practice*, 8(1), 43-62.

Human & Constitutional Rights Resource Page. 2018 http://www.hrcr.org/safrica/privacy/austr_law.html

iiNet. 2015. Law enforcement agencies contact https://www.iinet.net.au/about/legal/law.html

IETF. 2007. 'Request for Comments: 4960 Stream Control Transmission Protocol'.

IETF. 1981a. 'RFC. Transmission Control Protocol DARPA Internet Program Protocol Specification'

IETF. 1981b. 'RFC 791. Internet Protocol DARPA Internet Program Protocol Specification'

Inspector-General of Intelligence and Security Act 1986 (Cth) (IGIS Act)

Jaffarie v Director General of Security [2014] FCAFC 102 (18 August 2014)

Johnston, A. 2017. 'Privacy law: Data, metadata and personal information: A landmark ruling from the federal court'. *Law Society of NSW Journal,* 31 (March), 82-83.

Jones, DM. 2016. 'Intelligence and the management of national security: the post 9/11 evolution of an Australian National Security Community'. *Intelligence and National Security*, 33(1), 1–20.

Kozierok, C. 2005. The TCP/IP Guide in the TCP/IP Guide. http://www.tcpipguide.com/free/t_MessagesPacketsFramesDatagramsandCells-2.htm

Lachmayer, K; Witzleb, N. 2014. 'The Challenge to Privacy from Ever Increasing State Surveillance: A Comparative Perspective'. *UNSW Law Journal,* 37(2), 748-783

Laster, D. 1989. 'Breaches of Confidence and of Privacy by Misuse of Confidential Information'. *Otago Law Review* 31, 424

Legal and Constitutional Affairs References Committee (LCARC), Parliament of Australia, *Comprehensive revision of the Telecommunications (Interception and Access) Act 1979*, (2015)

Leonard, P. 2015a. 'The Metadata Retention Debate Rages On'. *Internet Law Bulletin,* 18(1) 17. https://www.gtlaw.com.au/sites/default/files/The-Metadata-Retention-Debate-rages-on.pdf

Leonard, P. 2015b. 'Internet Data Retention in Australia: New Controversies and Complexities'. *Privacy Law Bulletin* 2, 12(1) (Lexis Nexis, online)

Leonard, P. 2015c. 'Mandatory Internet Data Retention in Australia – Looking the horse in the mouth after it has bolted'. https://www.gtlaw.com.au/sites/default/files/Mandatory-Internet-Data-Retention-in-Australia_0.pdf

Loyd v Freshjeld (1826) 2 Car & P 325; 172 ER 147

Letter from the Attorney General, George Brandis to Hon Philip Ruddock MP, Chair of the PJCIS, 9 February 2016 cited in PJCHR, 25 February 2016

Maurushat, A. 2016. 'BD use by law enforcement and intelligence in the national security space: Perceived benefits, risks and challenges'. *Media and Arts Law Review,* 21(3), 1–27.

Mayer, J; Mutchler P; Mitchell, JC. 2016. 'Evaluating the privacy properties of telephone metadata'. *Proceedings of the National Academy of Sciences of the United States of America*, 113(20), pp. 5536–5541

Michael, K; Clarke, R. 2012. 'Location privacy under dire threat as uberveillance stalks the streets'. *Precedent,* 108, 24–29.

Moses, LB; Chan, J. 2014. 'Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools'. *UNSW Law Journal,* 37(2), 643-678

Nicholson, N; Redlich, H. 2015. 'Big Data, Metadata and Personal Data - How Does the Privacy Act Regulate Metadata?' *Privacy Law Bulletin,* 12(8), 215 (online)

Nohrborg, M. 2017. LTE, 3GPP. http://www.3gpp.org/technologies/keywords-acronyms/98-lte

Office of Australian Information Commissioner (OAIC, January 2015, Submission No 92 to the Parliamentary Joint Committee on Intelligence and Security, Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, January 2015

Parliamentary Joint Committee on Human Rights (PJCHR). 2014. Parliament of Australia, Fifteenth Report of the 44thParliament

Parliamentary Joint Committee on Intelligence and Security (PJCIS). 2015. Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth)

Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 (19 January 2017)

Privacy Act 1988 (Cth)

Revised Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (Cth)

Rodrick, S. 2009) 'Accessing telecommunications data for national security and law enforcement purposes'. *Federal Law Review,* 37, 391.

Rix, M. 2013. 'Security without secrecy? Counter-terrorism, ASIO and access to information', pp. 240-263 in Baldino, D. (Ed), *Spooked: the truth about intelligence in Australia*. Sydney, Australia: NewSouth Publishing.

Rix, M. 2014. 'What is the meaning and what is the use of 'metadata retention'?' *The Conversation* (online) 26 August 2014. https://theconversation.com/what-is-the-meaning-and-what-is-the-use-of-metadata-retention-30350

Robertson v Canadian Imperial Bank of Commerce [l9941 1 WLR 1493

Roach, K. 2011. *The 9/11 Effect: Comparative Counter-Terrorism*. Cambridge: Cambridge University Press.

Samsonidis v Commissioner, Australian Federal Police [2007] FCAFC 159 (5 October 2007)

Sarre, R. 2017. 'Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia'. *Asian Journal of Criminology,* 12(3) pp. 167–179

Selvadurai, N; Gillies, P; Islam, R. 2009. 'Maintaining an effective legislative framework for telecommunications interception in Australia'. *Criminal Law Journal*, 33(1), 34–44

Selvadurai, N; Kisswani, N; Khalaileh, Y. 2016. 'The proportionality principle in telecommunications interception and access law in an environment of heightened security and technological convergence'. *Information & Communications Technology Law*, 25(3), 229-246. doi:10.1080/13600834.2016.1230925

Selvadurai, N. 2017. 'The retention of telecommunications metadata: A necessary national security initiative or a disproportionate interference with personal privacy?' *Computer and Telecommunications Law Review*, 23(2), pp 35–41.

Senate Legal and Constitutional Affairs References Committee (SLCARC), Parliament of Australia, *Comprehensive revision of the Telecommunications (Interception and Access) Act 1979* (2015)

Shanapinda, S. 2017. 'Retention and disclosure of location information and location identifiers OTT content and communication services'. *Australian Journal of Telecommunications and the Digital Economy*, 4(4), 251-279. https://doi.org/10.18080/ajtde.v4n4.68

Shanapinda, S. 2018. *Advance metadata fair: The retention and disclosure of location information as metadata for law enforcement and national security, and the impact on privacy – An Australian story*, (PhD Thesis). UNSW Canberra University (unpublished)

Smith, GJD; Moses, B; and Chan, J. 2017. 'The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approach'. *The British Journal of Criminology,* 57(2), pp 259–274.

SSHD v Watson & Others Secretary of State for The Home Department and Tom Watson MP and others [2018] EWCA Civ 70 (the *Watson case)*

Svantesson, DJB. 2012. 'Systematic government access to private-sector data in Australia'. *International Data Privacy Law*, 2(4), 268–276.

Taylor, G. 2000. 'Why is there no Common Law Right of Privacy?' *Monash University Law Review*, 10, 26(2) 235.

Telstra Corporation Limited and Privacy Commissioner [2015] AATA 991 (18 December 2015)

Telecommunications (Interception and Access) (Data Retention) Amendment Act 2015 (Cth) (*Data Retention Act*)

Telecommunications Interception Legislation Amendment (TILA) Act 2002 (Cth)

Telecommunications (Interception and Access) Regulations 2017 (Cth)

Telstra. 2015. Submission No 112 to the Parliamentary Joint Committee on Intelligence and Security, (PJCIS) *Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, January

Telecommunications (Interception and Access) Act 1979 (Cth)

Telecommunications Act 1997 (Cth)

Tournier v National Provincial & Union Bank of England [l9241 1 KB 461

USA FREEDOM Act 2015, 114–23 H.R.2048

Victoria Park Racing and Recreation Grounds Co Ltd v Taylor (1937) 58 CLR 479 (the Victoria Park case)

Vodafone Hutchinson Australia. 2017. 'Privacy, 2017'. https://www.vodafone.com.au/about/legal/privacy

Williams, G and Hardy, K. 2014. 'National security reforms stage one: Intelligence gathering and secrecy' [online]. LSJ: *Law Society of NSW Journal*, No. 6, Nov 2014: 68-69. Availability: https://search.informit.com.au/documentSummary;dn=785911277868564;res=IELAPA

Williams, G. 2016. 'The Legal Assault on Australian Democracy'. *QUT Law Review*, 16(2), 19-41.

Williams, G. 2005. 'Balancing National Security and Human Rights: Lessons from Australia'. *Borderlands e-Journal*, 4(1) http://www.borderlands.net.au/vol4no1_2005/williams_balancing.htm

Winterton Constructions v Hambros (1992) 39 FCR 97, 114-15

Zwolenski, M; Weatherill, L. 2014. 'The digital universe: Rich data and the increasing value of the internet of things'. *Australian Journal of Telecommunications and the Digital Economy,* 2(3), 41–49. http://doi.org/10.7790/ajtde.v2n2.47

Endnotes

[i] The *USA FREEDOM Act* 2015 was passed to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes. Sec. 101 defines "call detail record" as session identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call. Excludes from such definition: (1) the contents of any communication; (2) the name, address, or financial information of a subscriber or customer; or (3) cell site location or global positioning system information.

[ii] © 2017.3GPP™ TSs and TRs are the property of ARIB, ATIS, CCSA, ETSI, TSDSI, TTA and TTC who jointly own the copyright in them. They are subject to further modifications and are therefore provided to you "as is" for information purposes only. Further use is strictly prohibited.

[iii] Loyd v Freshjeld (1826) 2 Car & P 325; 172 ER 147; Tournier v National Provincial & Union Bank of England [l9241 1 KB 461; *Australia & New Zealand Bank v Ryan* (1968) 88 WN (Pt l) (NSW) 368;

Federal Commissioner of Taxation v Australia & New Zealand Banking Group (1979) 143 CLR 499; *Barclays Bank v Taylor* [l9891 1 WLR 1066; *Winterton Constructions v Hambros* (1992) 39 FCR 97, 114-15; *Robertson v Canadian Imperial Bank of Commerce* [l9941 1 WLR 1493; *Christoj v Barclays Bank* [2000] 1 WLR 937; Laster, 'Breaches of Confidence and of Privacy by Misuse of Confidential Information' (1989) 7 Otago Law Review 31,424.

[iv] Yelp, Google Places and Facebook.

[v] Application Programming Interface.

[vi] Section 275A was added by the *Communications Legislation Amendment (Content Services) Act 2007* (Cth). Date of Assent: 20 Jul 2007 https://www.legislation.gov.au/Details/C2007A00124.

http://doi.org/10.18080/ajtde.v6n4.167