Integration of Cellular and Wi-Fi Networks

September 2013

TABLE OF CONTENTS

Executive Summary 4

1 Introduction 6

1.1 Drivers for Wi-Fi 6

1.2 Recent Wi-Fi Enablers 7

1.2.1 Evolving Standards 7

1.2.2 Evolving Device Capabilities 8

1.2.3 Evolving Models of Wi-Fi/Cellular Interworking 9

1.3 Challenges with Wi-Fi/Cellular Interworking 10

2 Current State-of-the-Art and Existing Challenges 12

2.1 Key Aspects of Wi-Fi/Cellular Integration 12

2.1.1 Seamless Service Continuity Between 3GPP and Wi-Fi 12

2.1.2 Supporting Real-Time Services & QoS Over Trusted Wi-Fi 18

2.1.3 Security & Authentication 20

2.1.4 HotSpot 2.0 and Passpoint 22

2.1.5 Intelligent Network Selection 24

2.2 Network Aspects of Intelligent Network Selection 25

2.2.1 ANDSF Information and Policy Elements 27

2.2.2 Roaming and ANDSF 29

2.2.3 What is Not Specified in ANDSF Standards Today 29

2.2.4 Analytics and ANDSF 31

2.3 Device Aspects of Intelligent Network Selection 32

2.3.1 Intelligent Network Selection and Traffic Steering 33

2.3.2 Role of Device and Key Required Information 33

2.3.3 Current State of Art 34

2.3.4 Gap Analysis 39

3 Recommended Solutions & Key Enablers of Intelligent Network Selection 41

3.1 Network Architecture Aspects 41

3.1.1 Supporting a Rich ANDSF Solution for Access Network Selection & Routing 41
3.1.2 Enabling the Sharing of Network Information with ANDSF 43
3.1.3 Bringing Venue Information to ANDSF 44
3.1.4 SIB-Based Distribution of Network conditions 46
3.2 Device Aspects 51
3.2.1 High Level Architecture and Key Functional Components 51
3.2.2 Functionality of an INS Mobile Device 52
3.2.3 INS models 57
3.2.4 Putting Things Together 59
4 Conclusions 62
5 Acknowledgements 65

EXECUTIVE SUMMARY

Mass market proliferation of mobile applications and devices has led to increased data traffic flowing across wireless broadband networks. With smartphone adoption and bandwidth-intensive services such as streaming video continuing to rise, resources of existing cellular networks are becoming increasingly constrained.

Wi-Fi is uniquely positioned to add to existing cellular network capacity, given its harmonized global spectrum allocation and widely adopted technology standard. Operators are already using Wi-Fi as an increasingly critical tool to meet capacity demands in standalone networks. To provide enhanced end user experience, improved Wi-Fi/Cellular interworking is needed for carriers to provide ubiquitous mobile broadband access.

This white paper analyzes and makes recommendations on some of the main aspects of integration between Wi-Fi and Cellular networks using Access Network Discovery and Selection Function (ANDSF) functionality:

- Section 1 of the paper describes some of the drivers for Wi-Fi in wireless networks. Enablers for technology evolution in standards, device capabilities and network models are described. End user challenges at Wi-Fi/Cellular network borders are also addressed.
- Section 2 addresses the current state-of-the-art and existing network and device challenges in three major subsections.
  - Sec. 2.1 addresses key aspects to Wi-Fi/Cellular integration, including: seamless continuity, Quality of Service (QoS), security, Hotspot 2.0, and concepts of Intelligent Network Selection (INS).
  - Sec. 2.2 describes ANDSF and sets the technical background for analysis and recommendations in the rest of the white paper. It also identifies existing network-related challenges for ANDSF-based INS.
  - Sec. 2.3 describes device aspects of the current state of network selection and traffic steering capabilities, standards, and existing solutions. Gaps in policy, network-related intelligence in devices, and device behavior are identified.
- Section 3 provides recommendations, and is structured along network and device aspects:
  - Sec. 3.1 provides recommendations on ANDSF network functionality and data structures/content to enable enhanced Wi-Fi/Cellular interworking. This also includes recommendations on network support for intelligent Wi-Fi/Cellular network selection and traffic steering with real-time load condition indication.
  - Sec. 3.2 makes recommendations on device architecture, key functionality, and enhancements to support the ANDSF-based intelligent network selection and traffic steering. Use cases are described to elaborate on device behavior regarding such intelligent network selection and traffic steering.
- Section 4 provides conclusions to the white paper. It summarizes some of the main recommendations towards standards bodies, infrastructure vendors and device vendors:

- Enhancements to ANDSF policies that include cellular network information, device mobility state
- Enhancement to LTE broadcast messages to include network load conditions
- Standardizing interfaces between subscription databases and the ANDSF
- Enhancements to ANDSF logic to allow for enhanced selection of Wi-Fi networks
- Optimizations and Application Program Interfaces (APIs) on the device and ANDSF client to improve intelligent network selection and battery consumption

The current phase of this work is focused on identifying ANDSF related requirements and recommendations on both the infrastructure and device aspects of the ecosystem. Other industry approaches, including active support from the Radio Access Network (RAN) for Wi-Fi/Cellular mobility, could be addressed at a future time as well.

1 INTRODUCTION

1.1 DRIVERS FOR WI-FI

The amount of traffic carried over wireless networks is growing rapidly and is being driven by many factors. Chief among them is the tremendous growth in multimedia applications on mobile devices – streaming music and video, two-way video conferencing and social networking to name a few. Indeed, much of today's traffic consists of low mobility, high bit rate applications (e.g., video), consuming significant air-interface resources in the process. Given the constraints on spectrum licensed for cellular use, Wi-Fi®[1] is often used to offload this type of traffic in order to free up cellular resources for the higher mobility users[2]. As users' appetite for data-intensive applications continue to outstrip cellular capacity, the more critical Wi-Fi has become in meeting this demand.

In fact, the exponential growth of data traffic on wireless cellular infrastructure over the last several years has been matched or even surpassed by a phenomenal increase in Wi-Fi traffic originating from Wi-Fi-enabled smartphones and tablets. Wi-Fi is used on many different devices every day and is on the rise. According to the Wireless Broadband Alliance, figures for 2011 put the total number of public Wi-Fi hotspots worldwide at 1.3 million. That number is forecasted to take a huge leap forward and grow 350% to 5.8 million by 2015[3].

In addition to traffic growth, subscriber expectations are also changing. They expect ubiquitous access to applications and content whether they are at home, at an enterprise, on the go or even when travelling. Increasingly, they expect the experience to be unhindered by access network inter-working constraints or incompatible technologies. For that reason, Wi-Fi can be an ideal solution for itinerant users, since it uses the same frequency bands and protocols worldwide. Indeed, this is why Wi-Fi solutions are common today in venues such as hotels and airports. While historically daily/hourly type service plans have been common in these scenarios, some service providers now offer bundles that package national Wi-Fi access with a user's fixed or mobile service subscription. And it's not just telecom operators – cable operators and multi-system operators (MSOs) have become increasingly active in deploying Wi-Fi networks within their regions.

The ability to exploit unlicensed spectrum in addition to licensed spectrum while providing a seamless subscriber experience has clear appeal for all of these service providers and network operators. Mobile service providers are starting to view Wi-Fi as another wireless technology that can augment their macro and small cell networks with affordable coverage and capacity, and with nearly universal device support. In particular, operators can leverage Wi-Fi to: offer a fast, reliable and cost-effective wireless broadband access; offload 3G/4G mobile data to relieve RAN constraints; offer a complementary wireless access as a part of a larger heterogeneous RAN or wireline access/service strategy; or offer a more complete bundled "on-load" experience and solution. In light of this, mobile operators realize that they need a combined unlicensed and licensed wireless strategy to deliver the best data services and mobile user experience at the highest margins. Additionally, fixed operators are also looking to Wi-Fi to enable new

[1] Wi-Fi® is a registered trademark of Wi-Fi Alliance.

[2] For a more detailed discussion on spectrum and capacity challenges, see the 4G America White Paper: "Meeting 1000x Challenge: The need for Spectrum, Technology and Policy Innovation," expected October 2013.

[3] Wireless Broadband Alliance Industry Report 2011 - Global Developments in Public Wi-Fi

revenues, extend service reach, offer content in more ways to more devices and improve brand loyalty. It's these trends that are driving the industry towards greater interworking with Wi-Fi networks.

1.2 RECENT WI-FI ENABLERS

1.2.1 EVOLVING STANDARDS

Recently, there have been significant developments in standards organizations that have paved the way for greater use of Wi-Fi by service providers: 1. Efforts by Institute of Electrical and Electronics Engineers (IEEE), Wi-Fi Alliance (WFA), Wireless Broadband Alliance (WBA) to standardize carrier-grade Wi-Fi features (e.g., HotSpot 2.0 and Next Generation HotSpot), and 2. Efforts by 3GPP to further standardize Wi-Fi-to-3GPP interworking capabilities.

The emergence of Hotspot 2.0 being defined by the Wi-Fi Alliance (WFA), an industry wide initiative, and Next Generation Hotspot (NGH) being defined by the WBA provides a number of standardized features for improving user experience on Wi-Fi networks and should further simplify integration with mobile networks. HotSpot 2.0 is aimed at facilitating and automating a secure and trusted Wi-Fi connection with the ability to use a variety of user- or device-based credentials. Additionally, Hotspot 2.0 promises to improve Wi-Fi network discovery and selection by providing new mechanisms for access points to broadcast information and for devices to query info from AP's without the need to associate first.

Simultaneously, the cellular industry has converged on a single mobile broadband standard which has facilitated Wi-Fi/Cellular integration work. Historically, 2G and 3G mobile access technologies were fragmented. EIA/TIA-based TDMA and CDMA access dominated in North America; whereas 3GPP based networks were the preferred option in much of the rest of the world. Today LTE is the clear 4G evolution choice of all major operators. The gravitation to 3GPP based standards for 4G facilitates integration with Wi-Fi as there is greater economy of scale for mobile devices supporting accesses, more roaming partner opportunities, and hence increased incentives for operators to invest in Wi-Fi/3GPP inter-working infrastructure. Thus, many mobile operators that are thinking strategically about investing in 4G LTE are also considering how Wi-Fi can complement and enhance their existing infrastructure deployments.

In fact, 3GPP has been working on a number of initiatives to improve Wi-Fi/Cellular interworking, including ways to improve the selection of Wi-Fi networks by cellular devices and options for integrating Wi-Fi networks into the cellular core. EAP-AKA/SIM based authentication and S2a-based Mobility over GTP (SaMOG) Trusted Access to the 3GPP core via Wi-Fi will allow end users to seamlessly roam between cellular and Wi-Fi access networks. Additionally, in order to provide optimal use of RAN resources and best end user experience, 3GPP is also working on the integration of Wi-Fi to include Radio Access Technology (RAT) selection addressed through per user and real time based decisions.

More specifically, 3GPP has spent several years standardizing the ANDSF. ANDSF provides a framework for operators to customize network steering policies and distribute those policies down to devices. There are ongoing efforts in 3GPP Release 12 to align ANDSF with the HotSpot 2.0 capabilities.

Additionally, 3GPP has recently defined a solution to allow Trusted Wireless Local Access Network (WLAN) access to the 3GPP core. While approaches such as 3GPP Interworking Wireless LAN (I-WLAN) have been considered since 2005 to allow the integration of Wi-Fi hotspots into wireless and wireline networks they have not seen widespread deployment. That is, while these approaches have been somewhat standardized; in practice, many instances of operator-owned Wi-Fi rollouts have resulted in

parallel network infrastructures with duplication of separate networks as well as subscriber/policy and traffic management systems. Indeed, until recently, standards-based approaches for carrier Wi-Fi have been based on treating Wi-Fi as untrusted access and have required the use of dedicated network elements which otherwise might not have been needed.

In Release 11, 3GPP standards work focused on non-3GPP access to the Evolved Packet Core (EPC) based on trusted WLAN access to the EPC and is based on SaMOG. This approach leverages improved WLAN and more efficient secure tunnel management (tunnels between Wi-Fi access points and the WLAN gateway). This approach results in the ability to provide Internet offload directly from the Trusted WLAN gateway or access to operator Packet Data Networks (PDN) via the packet core. There are also ongoing efforts in 3GPP Release 12 to enhance Release 11 SaMOG to provide mobility with IP address preservation and support for multiple-PDN connectivity over Wi-Fi and tighter RAN integration to provide traffic steering/mobility between 3GPP and Wi-Fi to guarantee end user experience (QoE) as well as ensure the optimal use of the network resources.

SaMOG can also be combined with ANDSF for operator controlled automatic network discovery and selection for the user. The result will be a seamless user experience that keeps devices on their "home" network, with obvious revenue and customer retention implications for operators.

Altogether, these newly standardized tools for simplified roaming, seamless handovers, and more intelligent network steering, are designed to enable users to continue using data services as they pass between cellular macro cells, small cells and Wi-Fi hotspots, with no need for further authentication or user intervention. That is, these standards seek to provide a transparent and secure user experience regardless of the radio access technology used to serve a given subscriber.

1.2.2 EVOLVING DEVICE CAPABILITIES

Most new devices coming to market feature integrated Wi-Fi radios. Smartphones, tablets, netbooks, laptops, even e-readers and games consoles all support Wi-Fi in a wide variety of variants (IEEE 802.a/b/g/n/ac). It's this rapid and widespread proliferation of Wi-Fi-enabled devices has seen data traffic across Wi-Fi hotspots increase dramatically. And due to this massive installed base of capable devices, Wi-Fi is no longer just a home networking solution, but instead represents a significant opportunity to carriers around the world.

In addition, many of the mobile devices sold today are dual radio (i.e., include both cellular and Wi-Fi radio) and are capable of using both radios simultaneously. Simultaneous access to Wi-Fi and 3GPP means that there is the opportunity to direct certain services to Wi-Fi, and others to 3GPP access. However, as more and more devices are capable of operating on multiple technology types (e.g., 3G, 4G, Wi-Fi), the more important intelligent network selection and traffic steering becomes.

To tackle this issue, many operators are interested in using ANDSF and its enhancement to provide policy driven intelligent network selection and traffic steering. A key enabler of this approach is the ability to implement an ANDSF client in devices that communicates with an ANDSF server in the network and supplies the ANDSF policy to the functionality in the device that performs network selection and traffic steering decisions. By distributing tailored policies to the ANDSF client, operators are able to steer traffic between Wi-Fi and cellular for better user experience and to allow better utilization of network and radio resources.

As mobile devices have become more intelligent, they are the entity that is most aware of actual network connectivity conditions (e.g. radio conditions, throughput over existing connectivity, etc.), and real-time

conditions in the device (e.g. type of pending traffic, active applications, status of device including battery levels, etc.). With the combination of operator policy and network/device intelligence, it is now the device that is in the unique position to make the best determination of which traffic should be transported over what access type (e.g., Wi-Fi or cellular).

1.2.3 EVOLVING MODELS OF WI-FI/CELLULAR INTERWORKING

Today's Wi-Fi hotspots operate in unlicensed spectrum, so there is no required coordination between networks. Historically, this has meant that operators lose visibility into their customers when those customers move onto Wi-Fi (i.e., insight into their connectivity and enhanced communication preferences). This is because those services that ride over Wi-Fi traverse alternative network infrastructures that do not always belong to wireless operators. However, as described above, this situation is changing with evolution of standards that support Wi-Fi and 3GPP interworking. Fundamentally, there are two models of Wi-Fi/Cellular interworking with multiple variations possible for each. These models are generally referred to as tightly coupled and loosely coupled networks. The following is an overview of the network aspects related to coupling between 3GPP and Wi-Fi:

Loosely coupled networks: In a loosely coupled network, the Wi-Fi network performance is usually not within the 3GPP operator's control, or has not been integrated by the 3GPP operator into a common converged wireless solution (e.g., when a mobile operator partners with a Wireless Internet Service Provider (WISP) or Multiple System Operator (MSO) who has deployed a Wi-Fi network). End user experience may include loss of IP session continuity, and break in data connectivity when reselection occurs between networks. Typically, this type of solution is used to provide offload of best-effort traffic to Wi-Fi while freeing up resources on constrained cellular networks. Given the potential impacts on user experience, intelligent network selection can play an important role in this model. In this case, ANDSF can be used by operators to distribute policies that guide traffic steering decisions that maximize user experience.

Tightly coupled networks: In a tightly coupled network, the Wi-Fi network performance is usually within the 3GPP operator control. This may also include integration between the 3GPP and Wi-Fi RAN networks, with common core infrastructure. Integration between the networks is designed to provide IP session continuity and seamless end user experience, so the end user is agnostic of wireless network type. As such, carriers can start making decisions based on which RAT will provide the greatest QoE for a given subscriber/service at a given time/location. In some cases, Trusted carrier Wi-Fi may provide that best experience, other times the cellular RATs might, and intelligent operator controlled network selection will play a vital role in making sure that the decision to move traffic to/from Wi-Fi is done in a way that maximizes QoE. Just as in the loosely coupled model, ANDSF gives operators a means of guiding Wi-Fi network selection within a tightly coupled network. In addition, discussions are also ongoing in 3GPP RAN standardization group on network centric solutions supporting Wi-Fi and 3GPP interoperability, whereby offloading and traffic steering decisions should consider not only the concerned user's experience but also the other active users in both the 3GPP network and Wi-Fi.

Regardless of the specific model chosen by a service provider, Wi-Fi networks present an opportunity for service innovation and revenue growth. By including both licensed and unlicensed technologies, mobile operators can begin to address network congestion and start to build true heterogeneous networks where traffic is intelligently routed according to the operator's policies.

1.3 CHALLENGES WITH WI-FI/CELLULAR INTERWORKING

From individual homes and workplaces, to coffee shops, retail stores, hotels and airports, Wi-Fi hotspots are becoming ubiquitous for semi-nomadic data connectivity. While the appeal of Wi-Fi lies primarily in its availability and relatively easy configuration, the use of Wi-Fi by mobile operator's still faces challenges. While this section has highlighted many key enablers that have evolved recently (and which are discussed in greater detail in the next chapter), there are still open problems that the industry needs to address before Wi-Fi/Cellular integration can be fully realized.

In particular, many of the challenges facing Wi-Fi/Cellular integration have to do with realizing a complete intelligent network selection solution that allows operators to steer traffic in a manner that maximizes user experience and addresses some of the challenges at the boundaries between RATs (2G, 3G, LTE and Wi-Fi).

Figure 1 below illustrates four of the key challenges at the Wi-Fi/Cellular boundary.

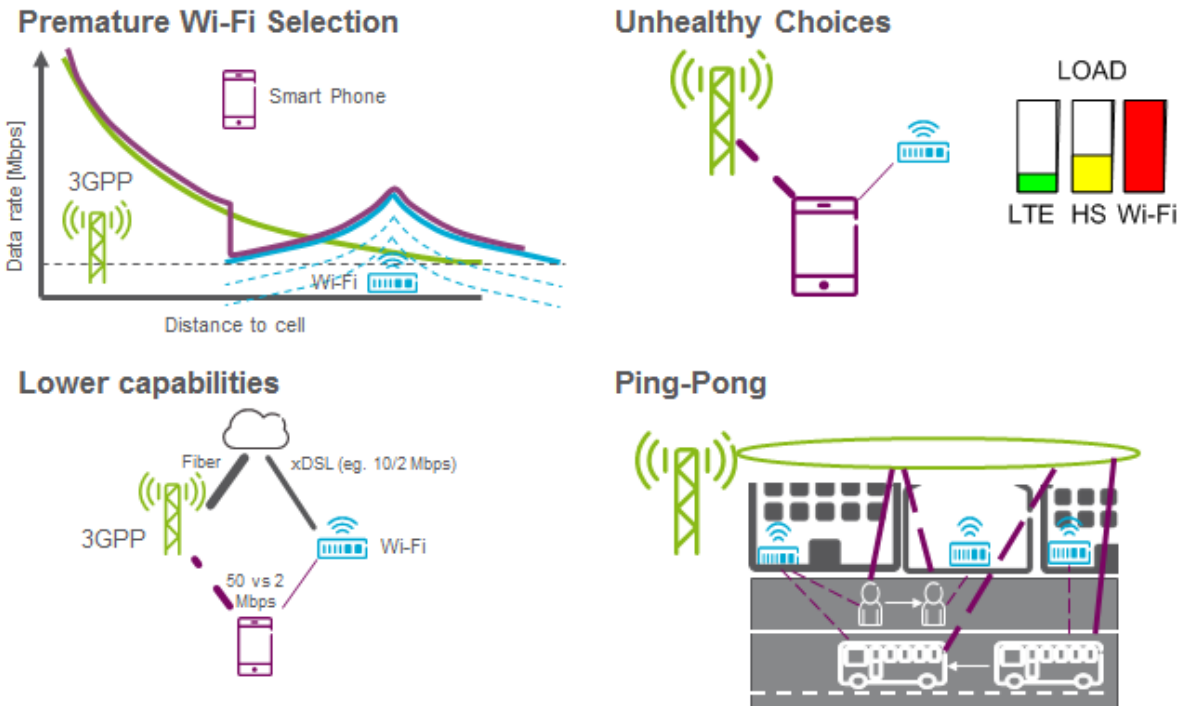

Figure 1. Four Key Challenges at the Wi-Fi/Cellular boundary.

1) Premature Wi-Fi Selection: As devices with Wi-Fi enabled move into Wi-Fi coverage, they reselect to Wi-Fi without comparative evaluation of existing cellular and incoming Wi-Fi capabilities. This can result in degradation of end user experience due to premature reselection to Wi-Fi. Real time throughput based traffic steering can be used to mitigate this.

2) Unhealthy choices: In a mixed wireless network of LTE, HSPA and Wi-Fi, reselection may occur to a strong Wi-Fi network, which is under heavy load. The resulting 'unhealthy' choice results in a

degradation of end user experience as performance on the cell edge of a lightly loaded cellular network may be superior to performance close to a heavily loaded Wi-Fi AP. Real time load based traffic steering can be used to mitigate this.

3) Lower capabilities: In some cases, reselection to a strong Wi-Fi AP may result in reduced performance (e.g. if the Wi-Fi AP is served by lower bandwidth in the backhaul than the cellular base station presently serving the device). Evaluation of criteria beyond wireless capabilities prior to access selection can be used to mitigate this.

4) Ping-Pong: This is an example of reduced end user experience due to ping-ponging between Wi-Fi and cellular accesses. This could be a result of premature Wi-Fi selection and mobility in a cellular environment with signal strengths very similar in both access types. Hysteresis concepts used in access selection similar to cellular IRAT, applied between Wi-Fi and cellular accesses can be used to mitigate this.

To that end, this white paper provides an overview of the current state-of-the-art capabilities of both the network and device aspects of intelligent network selection, identifies the key gaps in existing solutions, and proposes some recommended solutions to address these gaps.

More specifically, this white paper explores how ANDSF can be enhanced on the network side to include additional information in policy decision (e.g., network-based analytics and real-time network conditions). On the device side, this white paper explores the lack of consistent network selection implementation and user experience across platforms. That is, currently there are different implementations of network selection and traffic steering from various User Equipment/Operating System/Original Equipment Manufacturer (UE/OS/OEM) vendors that result in different behaviors and inconsistency of decision making process in devices. In addition, present device based network selection solutions have limited knowledge of real-time network conditions, such as cellular network or Wi-Fi congestion. Thus, this white paper will explore solutions to provide a more full-featured and uniform intelligent network steering behavior.

2 CURRENT STATE-OF-THE-ART AND EXISTING CHALLENGES

2.1 KEY ASPECTS OF WI-FI/CELLULAR INTEGRATION

Over the past years, cellular operators have seen a tremendous increase in data traffic due to faster networks and data intensive devices with even more dramatic growth projected for the coming years. Wi-Fi is an established technology, and is becoming increasingly common in cellular handsets. Wi-Fi spectrum is unlicensed and globally available. Wi-Fi is therefore uniquely positioned to support this data expansion by augmenting, complimenting and stabilizing 3G/LTE macro coverage. Thus, this section provides an overview of the current state-of-the-art key aspects of Wi-Fi/Cellular integration.

2.1.1 SEAMLESS SERVICE CONTINUITY BETWEEN 3GPP AND WI-FI

Session mobility between Wi-Fi and cellular networks (with IP address preservation), has been a desirable vision for many years. The demand for data traffic and pressure on macro networks is accelerating and driving the need to make this possible.

It is highly desirable for both the end user and the service provider to have the ability to seamlessly move an IP session between cellular access and Wi-Fi access. This functionality also enables more sophisticated mobility scenarios such as Multi-Access PDN Connectivity (MAPCON) and IP Flow Mobility (IFOM) as defined in 3GPP. This section will discuss several protocols Proxy Mobile IPv6, Dual Stack Mobile IPv6, GPRS Tunneling Protocol (PMIP, DSMIPV6, GTP) and interfaces (S2a, S2b, S2c) that can be used to achieve this objective.

As this section discusses in detail, WLAN access may be used by mobile operators to provide mobile network access. It allows an end-user to use their mobile device's WLAN access interface and a "connection manager" client to route traffic back into the mobile network operator's packet core network and hence to both obtain access to mobile operator services and in-direct access to the public Internet via mobile operator. The mobile operator role involves both user plane routing and control plane functions including backend support for the Authentication, Authorization and Accounting (AAA) chain to provide access control and billing for WLAN service. In this case the end-user's device is assigned an IP address by the mobile operator and any requirement for legal interception of user traffic would fall on the mobile operator.

2.1.1.1 SERVICE LAYER SESSION CONTINUITY

Service layer session continuity refers to the solution where the application ensures the continuity of the service even though the IP address used to access the service has changed (due to a mobility event).

For applications (e.g. web browsing, e-mail client) where the UE is a client, when the IP address of the UE has changed, the application can issue further requests on a new Transmission Control Protocol (TCP) connection using the new IP address of the UE.

Consider an application of HTTPS services during a mobility event. If the change of TCP connection occurs while the end-user is in the middle of filling out a form (e.g. entering credit card information), this would result in the end-user having to re-enter the information to fill-in the form. A too frequent change of IP address can result in the UE continuously being interrupted. For example, in case of HTTP Adaptive Streaming (HAS), a too frequent change of IP address might mean that the UE can't get a portion of the

video file – this would be a noticeable service disruption. (This issue will be less apparent in background services, such as e-mail retrieval.)

The case where UE is a "server" (e.g., in VoIP) is more problematic as the UE's peers have to be made aware of UE's IP address change. IP Multimedia System (IMS) provides a solution, but this solution results in a lot of signaling exchanged between the UE and the network:

- The UE needs to register at IMS layer with its new IP address;
- The UE needs to issue session related signaling (to the SCC AS) when changing IP address occurs within a Voice session;
- The data related media have to be re-negotiated and restarted.

Therefore, while some services may live with a change of IP address, certain other service types are likely to be impacted. The user experience depends on the type of service, and relying on service layer session continuity is not a generic solution.

2.1.1.2 3GPP METHODS FOR MOBILITY BETWEEN 3GPP AND WI-FI NETWORKS

The Evolved Packet Core (EPC) architecture has been designed to provide support to both legacy (2G/3G) and LTE access and to provide support for access to mobility with non-3GPP access (e.g. Wi-Fi).

Support of non-3GPP access is described in 3GPP TS 23.402. Two kinds of non-3GPP access networks to EPC are defined by 3GPP TS 33.402: un-trusted and trusted[4] non-3GPP access networks.

As defined in clause 4.3.1.2 of TS 23.402, it is the home operator policy decision if a non-3GPP access network is treated as trusted non-3GPP access network. When all of the security feature groups provided by the non-3GPP access network are considered sufficiently secure by the home operator, the non-3GPP access may be identified as a trusted non-3GPP access for that operator. However, this policy decision may additionally be based on reasons not related to security feature groups. When one or more of the security feature groups is considered not sufficiently secure by the home operator, the non-3GPP access is identified as an un-trusted non-3GPP access for that operator. In this case, the UE has to establish an IPsec tunnel to the Enhanced Packet Data Gateway (ePDG) by conducting Internet Key Exchange (IKEv2) with Extensible Authentication Protocol Method-Authentication and Key Agreement (EAP-AKA) for UE authentication, (refer to the description on S2b access to EPC later in this section for additional details).

When IP address preservation during mobility between 3GPP and non-3GPP access is required, the EPC relies on the P-GW acting as an anchor point between these two kinds of accesses and hiding the mobility to the entities of the Packet Data Network.

[4] 3GPP specifications do not dictate whether a non-3GPP access technology (e.g., Wi-Fi or WIMAX) is to be considered as trusted or non-trusted. Instead, whether a non-3GPP access is to be considered trusted is determined by the Home operator of the user and is based on operational conditions.

Depending upon the nature of the interworking solution the following options may be offered:

- **Non-seamless mobility of all packet connections**: The UE gets different IP addresses (and possibly different services) over WLAN and over normal mobile network access. This feature has been defined in 3GPP Release 6 as "I-WLAN / 3GPP IP Access".

- **Seamless mobility of all packet connections**: At mobility between 3GPP and WLAN access, all PDN connections are handed-over and have their IP address preserved. This feature has been defined in 3GPP Release 8 as "Un-trusted non-3GPP access".

- **Seamless mobility of individual PDN connections**: At mobility between 3GPP and WLAN access, the UE determines which Public Data Network (PDN) connections are handed-over (with IP address preservation). For example, an Access Point Name (APN) for best effort Internet moves between cellular and WLAN access as soon as WLAN is available while a second APN for IMS service remains on the cellular access. This feature has been defined in 3GPP Release 10 as MAPCON.

- **Seamless mobility of individual IP flows on specific PDN connections**: At mobility between 3GPP and WLAN access the UE determines which IP flows of a PDN connection are handed-over (all PDN connections have their IP address preserved). For example, best effort Internet traffic on the default APN move between cellular and WLAN access as soon as WLAN is available while a dedicated video streaming flow on the same APN and a second APN for IMS service remains on the cellular access. This feature has been defined in 3GPP Release 10 as Internet Protocol Flow Mobility and seamless WLAN Offload (IFOM).

How the UE selects a network and/or steers traffic in the latter two cases is described in greater detail later in Chapter 2.

Figure 2 presents an overview of these service options and interactions between mobile and WLAN networks.

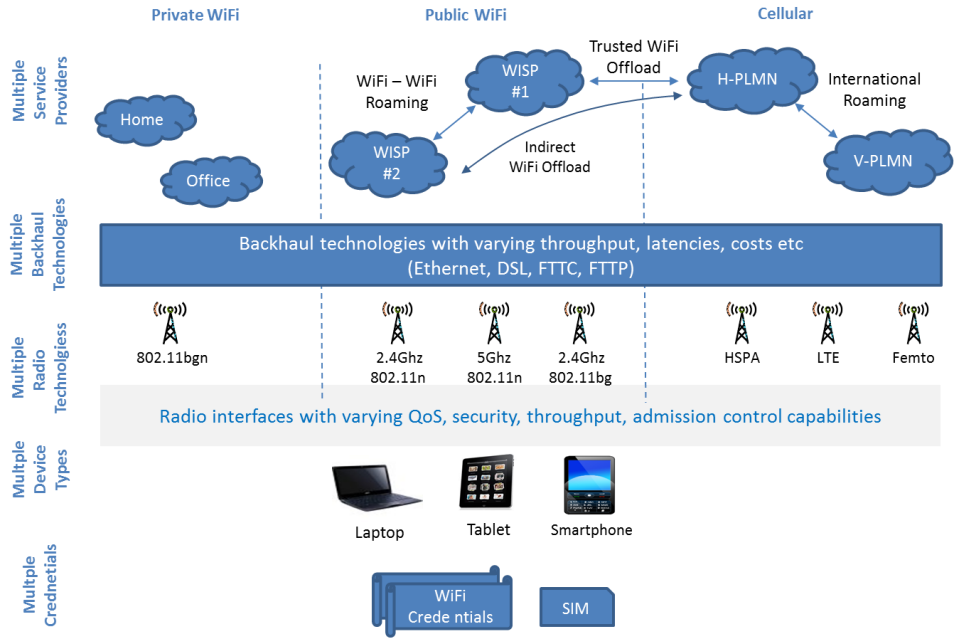

Figure 2. Overview of interworking scenarios between mobile and WLAN access.

The following section describes the 3GPP standards related aspects for each of the options and Figure 3 below illustrates the 3GPP/Non-3GPP interworking architecture.

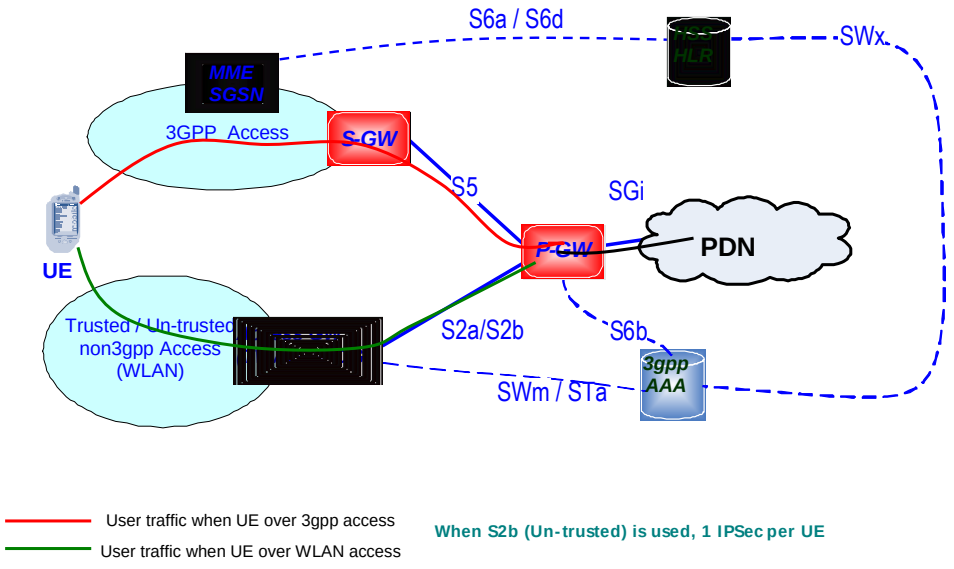

Figure 3. 3GPP/Non-3GPP interworking architecture (3GPP Rel8/9/10/11 EPC). (NOTE: Only the Network-based mobility case is shown.)

3GPP TS 23.402 allows two IP mobility management mechanisms for **non-3GPP access** (Network-based Mobility and Host-based Mobility), which are as follows:

Network Based Mobility uses S2a interface for Trusted access to EPC and S2b interface for Un-Trusted access to EPC. S2a and S2b rely on protocols such as GTP or PMIPv6 terminated in network entities managing mobility in the access network.

Client/Host-Based Mobility uses S2c interface. S2c relies on DSMIPv6 mobility signalling terminated in the UE and at the PDN Gateway (P-GW). The access network needs to allocate Care-Of-Address to the UE, and the High Availability (HA) must be reachable from the access network for the UE.

2.1.1.2.1 S2B AND S2C ACCESS TO EPC VIA NON-3GPP ACCESS

Prior to Release 11, 3GPP specifications included 2 main deployment scenarios to access to the EPC from Wi-Fi:

- **S2b scenario** - **Non-Trusted Non-3GPP Access to EPC:** To maintain trust, the UE has to establish a dedicated "Virtual Private Network (VPN) access". This comprises of establishing an IPSec tunnel(s) to a secure gateway operated by a Mobile operator (called ePDG) that provides access to the EPC. These IPSec tunnels are set-up based on 3GPP requirements. IKE parameters are used to carry 3GPP information such as the APN. For each UE, there is one such IPSec tunnel per PDN connection, the UE wants to have over Non-Trusted Non-3GPP Access to EPC. The ePDG then terminates a GTP/PMIP S2b interface to the P-GW. This S2b interface is similar to the S5/S8 interface between a SGW and a P-GW.

- **S2c scenario** - **Access to EPC with Host Based Mobility:** in this scenario, the UE establishes DSMIPv6 connectivity to the EPC mobility anchor (i.e. the P-GW) transparently over Wi-Fi. Together with DSMIPv6 support in the UE, this requires the support of an IPsec Security Association between the UE and the P-GW in order to protect the Mobile IP signalling between the UE and the P-GW.

At present, there is limited deployment of either of these two options. Therefore most UE's today are not able to utilize Wi-Fi to access operator services, and thus mobile operators are unable to offer operator-specific services that span over both 3GPP and Wi-Fi radios.

Note that requiring each UE to set up an IPSec tunnel / Security Association to access to the EPC comes at a cost for the operator as it implies the support of at least an IPsec tunnel per UE, which requires the deployment of costly nodes that terminate a large number of IPsec tunnels.

Furthermore, for the Un-trusted case, this may imply the support of nested IPSec (a corporate VPN within the 3GPP IPSec tunnel) when the UE uses the access to EPC to set up a VPN to the corporate network of the user which may not be supported by terminal operating systems.

In addition to these approaches for access to the EPC, it is also possible to have the user traffic bypass the EPC altogether, as follows:

Non seamless WLAN offload (NSWO) service: The UE may also benefit from a Non Seamless WLAN Offload service where the traffic is not sent via the EPC but instead is routed directly to the internet. This traffic cannot benefit from IP address preservation at mobility between 3GPP and Non-3GPP networks.

Mobility between 3GPP and non-3GPP accesses is always UE-initiated. As the UE moves between Wi-Fi and 3GPP coverage, it may indicate that it is a "Handover" related request. The Handover indication

ensures that the P-GW will be kept as local mobility anchor and that the IP address of the session is preserved, thereby enabling mobility without interrupting the existing session. The relative priorities between Radio Access Technology (Wi-Fi vs. 3GPP) may be controlled by ANDSF-based rules, which are discussed in greater detail later in this chapter.

2.1.1.2.2 SAMOG: S2A-BASED MOBILITY ON GTP

3GPP Release 11 introduced SaMOG, which enables access to the EPC from Trusted Wi-Fi networks and uses GTP for Network-based mobility:

- **S2a scenario -Trusted WLAN Access:** Allowing usage of Wi-Fi as a trusted non-3GPP access to EPC enables a connection to the EPC in deployments where the existing S2b and S2c solutions for untrusted non-3GPP access are not necessary. This solution is based on the observation that in many cases the Wi-Fi access is either directly owned by the mobile operator or controllable via a partnership agreement and so at least one Service Set Identifier (SSID) on the Wi-Fi access may be configured to meet the operator requirements for "trusted" non-3GPP access technologies.

As illustrated in Figure 4 below, a SaMOG deployment entails the following:

- Security per IEEE 802.11-2007 profile (based on the 802.11i amendment). As described in greater detail later in this section, this entails support of the strong EAP-AKA' based authentication and AES-based ciphering over the Wi-Fi radio;
- An AAA interface (STa) with a 3GPP AAA server to support UE authentication as well as to retrieve user Authorization data;
- An S2a interface with the P-GW where each user session is mapped to a GTP or PMIP session to a P-GW (similar mapping as enforced in a S-GW or an ePDG).

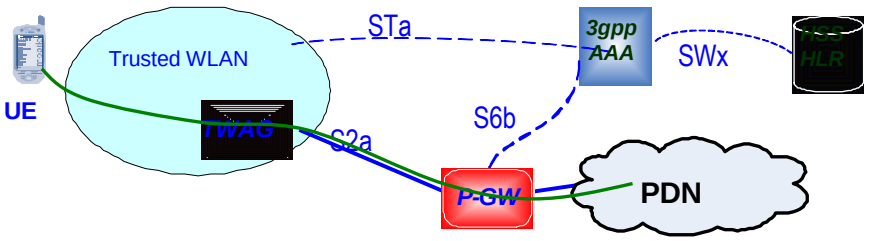

Figure 4. Architecture with Trusted Wi-Fi access to EPC.

The Authentication, Authorization and Accounting (AAA) server performs UE authentication based on USIM credentials and accesses the Home Subscriber Server (HSS) through SWx interface to get subscriber's information and security credentials. The authentication relies on EAP-AKA[5] and the authorization data may contain the P-GW serving the UE over 3GPP coverage.

[5] EAP-AKA' method is defined by IETF RFC 5448 which is required to be supported for trusted non-3GPP access

Finally, S6b interface is used to indicate to the HSS via the AAA server the P-GW that has been selected (allowing re-using the same P-GW when the UE moves to a 3GPP access).

Although not illustrated in the figure above, in case of roaming, S2a/S2b/S2c-based architectures can support both 'Home-Routed' (the P-GW is located in the HPLMN) and 'Local Break Out' (LBO: the P-GW is located in the VPLMN) with the latter being required to support VoIMS services.

While the Release 11 SaMOG work focused on supporting legacy UE's and having no device impact, as part of 3GPP Release 12, eSaMOG enhances the Release 11 trusted Wi-Fi solution by enabling:

- IP address preservation when moving between a 3GPP network and a trusted Wi-Fi network;
- Multiplexing over Trusted Wi-Fi traffic targeting different PDN connections or Multiplexing over Trusted Wi-Fi traffic targeting the EPC and traffic corresponding to non-seamless offload (NSWO);
- Capability for the UE to tell the network which APN is targeted.

2.1.1.2.3 INDUSTRY TRENDS FOR MOBILITY WITH IP ADDRESS PRESERVATION

Mobility with IP address preservation between cellular and trusted Wi-Fi accesses is an important feature to many operators. Voice and other real time applications (online gaming, video streaming, etc.) are the key services that can require session continuity with IP address preservation. The service layer cannot be expected to take care of session continuity for all services and deployment scenarios.

GTP-based solutions enjoy the highest vendor support followed by PMIP-based solutions. This is true for both trusted and untrusted Wi-Fi accesses. Recent GSMA/WBA joint activity on Wi-Fi also indicates the following industry trends:

- GTP based mobility between cellular and trusted Wi-Fi networks will be the preferred deployment solution for scenarios requiring IP address preservation and this solution is currently being worked on by 3GPP in Release 12;
- Delivery of voice and real time services over Wi-Fi will be the key drivers for such deployments;
- Most common deployment scenarios requiring Wi-Fi←→cellular mobility with IP address preservation will involve an operator that operates both Wi-Fi and cellular access networks.

Additionally, the following are also believed to be true:

- There has yet to be significant adoption of DSMIPv6-based solutions by device vendors;
- A majority of device vendors plan S2b-capable terminals;

2.1.2 SUPPORTING REAL-TIME SERVICES & QOS OVER TRUSTED WI-FI

Based on the industry trends discussed in the previous section, SaMOG is expected to be the preferred deployment option for integrating trusted Wi-Fi access to an operator's mobile core. Such a tightly integrated Wi-Fi deployment can enable services and features that may not otherwise be possible. For instance, this could include real-time services over trusted Wi-Fi or, more generally, support for end-to-end QoS over trusted Wi-Fi. This section discusses both of these topics in greater detail.

2.1.2.1 FEATURES REQUIRED TO SUPPORT REAL-TIME SERVICES

A key service requirement is to be able to carry real time services such as VoIP or two-way video over a Trusted WLAN (S2a). In such a scenario, the following features are desirable:

- The use case where an UE can simultaneously access to IMS and to Internet is important: IMS support requires a dedicated PDN connection (per GSMA IR 92) and thus over Trusted WLAN requires the multi-homing capability brought by SaMOG phase 2 (3GPP Rel12). The UE can simultaneously benefit from NSWO (for access to Internet) and from a PDN connection dedicated to IMS.

- IMS signaling: it is desirable that after mobility between 3GPP and Wi-Fi coverage, the UE does not need to re-REGISTER (or to issue re-INVITE). The preservation of UE's IP address after mobility between 3GPP and Wi-Fi coverage and the capability for the same Proxy Call Session Control Function (P-CSCF) to serve the UE over both 3GPP and Trusted Wi-Fi coverage are key pre-requisites for this goal.

- QoS: Making sure that a Trusted WLAN Access Network delivers packets carrying VoIP with the relevant QoS. Both DL and UL directions should be considered. This is discussed in greater detail in the next section.

- Charging and Location: e.g. making sure that a Trusted WLAN Access Network can at the set-up and release of a VoIP call provide to the service layer (e.g. IMS) location Information (such as Cell-Id and PLMN-Id) that is similar to the information a 3GPP access can provide. For a 3GPP access, this has been defined in 3GPP Rel11 as part of the "NetLoc" Work Item (which defines how the IMS can get the identity of the 3PP Cell serving the UE at the start and at the release of an IMS session).

    - Location at a granularity higher than that of the identity of the AP serving the UE (i.e. similar to a Cell-Id over a 3GPP access) is not required as support of emergency services over a Trusted WLAN is not intended for this white paper (corresponding to 3GPP Release 12).

- Roaming where TWAN and 3GPP are controlled by the same operator.

2.1.2.2 ENABLING END-TO-END QOS

For IP Flows requiring QoS that are sent over a Trusted WLAN access, tight Wi-Fi/Cellular integration provides an opportunity for end-to-end prioritized treatment that is not otherwise possible. This is achieved by leveraging and coordinating the QoS mechanisms available at the various network segments:

- Over the S2a interface between the P-GW and the Trusted WLAN Access Gateway (TWAG): For flows requiring QoS, 3GPP Rel11 specifications support dedicated S2a bearers associated with QoS parameters QoS Class Index, Allocation and Retention Priority, Guaranteed Bit Rate, Maximum Bit Rate, Uplink Traffic Flow Template (QCI, ARP, GBR, MBR, UL TFT, etc.). At transport level, the GSMA IR 34 describes the default mapping of these QoS parameters (QCI) onto the relevant Differentiated Services Code Point (DSCP) value to be used in the transport layer.

- Between the TWAG and the UE for DL (downlink) traffic
    - For DL traffic received over a S2a bearer, a mapping is to be enforced in the TWAG from the QCI associated with this bearer to a proper transport QoS (e.g. mapping to a proper DSCP value when an IP transport is used: in this case a default value of this mapping could also refer to GSMA IR 34).
    - For DL traffic received from the TWAG, QoS mapping in the AP (to the 802.11 QoS mechanisms) should follow the rules defined in 802.11 specifications. Hybrid coordination function HCF contention-based channel access (EDCA) defined in 802.11 may be needed to deliver proper QoS over a Trusted WLAN radio.
- Between the TWAG and the UE for UL (Uplink) traffic
    - Mapping is required in the UE to associate an Uplink IP flow with a proper QoS level. The definition of this mapping may require further study. Mapping is required in the UE to associate an Uplink IP flow with a proper QoS level. The definition of this mapping may require further study and could be based on principles in SaMOG that allow the TWAG to send a new signaling message to the UE for uplink QoS
    - Then QoS mapping in the 802.11 layer of the UE (to the 802.11 QoS mechanisms) should follow the rules defined in 802.11 specifications: the UE should use "QoS Map Set information element" received from the AP (per 802.11u and HS2.0 phase 2 specifications) to map the higher-layer priority (from the DSCP) to User Priority as defined over 802.11 radio.

Wi-Fi QoS admission control needs to be considered in the future. Currently, VoLTE will be supported through QCI=1, MBR and GBR settings at the TWAG. If the BNG and TWAG are collocated, a CAC can be performed. However, that may not apply to the WLAN AP, which will only consider the DSCP of the traffic and not any other specific CAC techniques.

2.1.3 SECURITY & AUTHENTICATION

Making secure connectivity to Wi-Fi access networks transparent for the end user is clearly a service requirement. A key obstacle to user experience of seamless connectivity over Wi-Fi has been a lack of appropriate airlink security and access authentication mechanisms. This section describes some of the recent industry trends that are helping to overcome this hurdle.

2.1.3.1 AUTHENTICATION

To provide network access to subscribers on an integrated Wi-Fi cellular network they would first have to be uniquely identified and authenticated by the network. An integrated network environment based on 3GPP Evolved Packet Core (EPC) will have dual mode devices supporting both Wi-Fi and cellular technologies. Such devices will include a UICC module with (U)SIM application having user subscription information and authentication credentials stored in a tamper proof manner. These (U)SIM based credentials are for authentication with cellular networks but their existence on dual mode devices makes it easier to reuse them for authentication over Wi-Fi accesses that are integrated with cellular networks. EAP-SIM, EAP-AKA and EAP-AKA' are Wi-Fi access authentication mechanisms that make use of (U)SIM credentials.

EAP-SIM is the EAP based mechanism defined for authentication based on SIM credentials. EAP-AKA is an improvement on EAP-SIM and is based on USIM symmetric keys allowing for mutual authentication, integrity protection and replay protection. EAP-AKA' is a minor revision to EAP-AKA method with a new key derivation function. It should be noted that while all three of these mechanisms make use of (U)SIM credentials, based on existing 3GPP specifications only the EAP-AKA and EAP-AKA' methods can provide access to the EPC via non-3GPP accesses[6]. It is therefore recommended that both EAP-AKA and EAP-AKA' be supported for authentication purposes in an integrated network environment. All of these methods require support of IEEE 802.1x. The task of using them has been made easier more recently as support of IEEE 802.11i and IEEE 802.1x is now part of HotSpot 2.0 release 1.0 and therefore is part of WFA's Passpoint certification.

Most Wi-Fi networks today still implement manual login techniques where username and password is provided over an HTTPS session. Use of such techniques like captive portal is less secure and can result in identity theft or theft of service. As indicated earlier, use of such techniques will also not allow access to the EPC and hence integration with cellular networks will not be possible. While for legacy reasons these techniques may currently need to be supported, they should be phased out in favor of more secure mechanisms as identified.

In terms of Wi-Fi security and authentication in an integrated network environment, this paper recommends the use WPA2-Enterprise along with EAP-AKA and EAP-AKA'.

2.1.3.2 AIR-LINK ENCRYPTION

Cellular networks provide a secure air interface for authentication and network access purposes. Unlike cellular networks, Wi-Fi networks can have various levels of airlink security. These range from practically no security (i.e., all traffic transmitted in the clear) to security that can be considered comparable to cellular networks. When Wi-Fi and cellular networks are integrated, there is an expectation that the combined network shall provide security on par with that of cellular networks.

To that end, HotSpot 2.0 includes the use of WPA2-Enterprise based airlink security mechanism for Wi-Fi networks. WPA2 provides AES-based airlink encryption using the IEEE 802.11i standard and the WFA (Wi-Fi Alliance) has Wi-Fi device certification for this capability. WPA2-Enteripise mode of WPA2 provides additional security by leveraging 802.1x and use of AAA server for session key distribution.

Use of such airlink security can help alleviate eavesdropping related concerns both from the end user as well as from operator community. In addition, once the airlink is adequately secured it is more likely that network operators would consider such a Wi-Fi access to be trusted as defined by the 3GPP. In particular, this will help in deployment of SaMOG type architectures for providing mobility between Wi-Fi and cellular accesses with IP address preservation. (SaMOG is currently under development in 3GPP Release 12.) In the past, GSMA and WBA joint Wi-Fi TF also recommended the use of WPA2-Enterprise and in this white paper we endorse this recommendation.

[6] According to Section 6.1 of 3GPP TS 33.402: "The UE and 3GPP AAA server shall implement both EAP-AKA and EAP-AKA'." EAP-AKA is to be used for authentication for access via Untrusted non-3GPP access networks (e.g., over the SWu in an ePDG-based model). EAP-AKA' is to be used for authentication for access via Trusted non-3GPP access networks (e.g., over the SWw in a SaMOG-based model).

2.1.4 HOTSPOT 2.0 AND PASSPOINT

Hotspot 2.0 (HS2.0) is a working group in Wi-Fi Alliance (WFA). The target of the HS2.0 work is to make Wi-Fi hotspot usage and Wi-Fi roaming as easy as it is to use a cellular network today. HS2.0 enables several Wi-Fi features, many of which are useful in Wi-Fi/cellular integration[7].

WFA work is based on certification programs, i.e., when a device has passed certain certification program test cases successfully, the vendor can market the device as WFA certified (e.g., "Wi-Fi a/b/g certified"). The HS2.0 certification program is called Passpoint.

Traditionally, WFA certification programs pick selected features from IEEE specifications (but may also add some of their own). In the case of Passpoint, HS2.0 is based primarily on IEEE 802.11u, 802.11i, and 802.1x. The Passpoint Release 1 certification program is already in progress, while Release 2 is expected to start soon. Passpoint certified devices will support both Release 1 and 2 functionality since Release 1 is only an intermediate certification "class" before completion of HS2.0 Release 2. Figure 5 below shows the main features supported in Passpoint Releases 1 and 2.

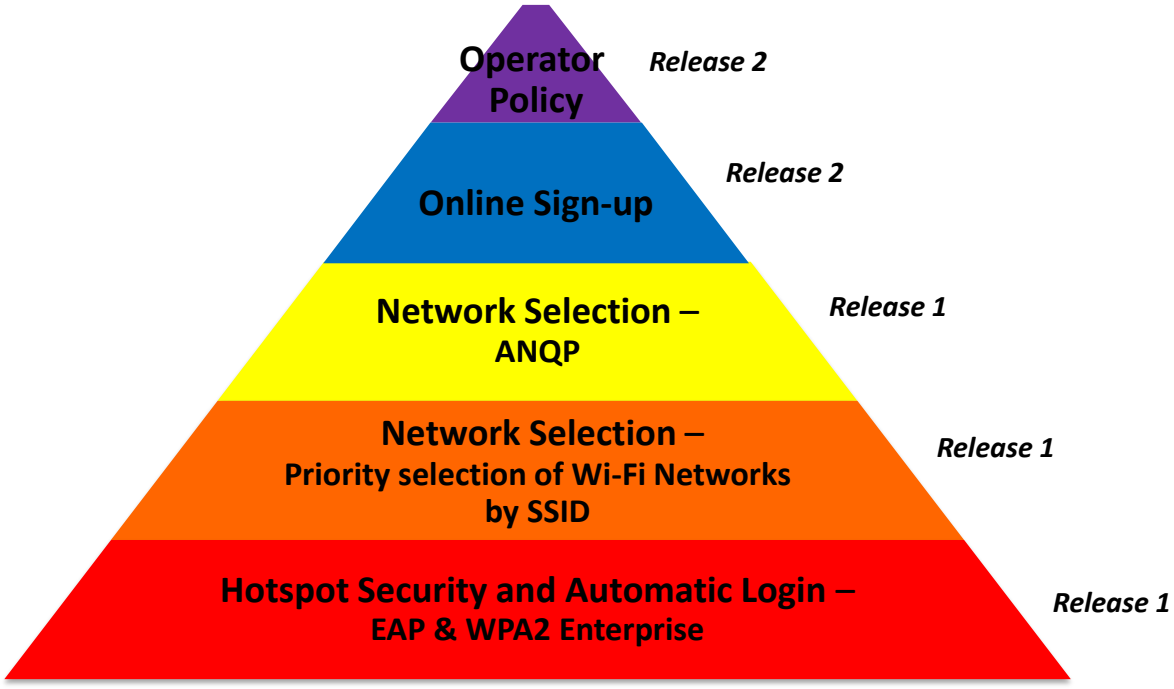

Figure 5. The main features supported in Passpoint Releases 1 and 2.

[7] **HS2.0 Definitions**:
HS2.0 Operator is an entity that deploys and operates an access network of publicly accessible Wi-Fi Access Points.
HS2.0 Service Provider is an entity that provides network services and specifically has the AAA infrastructure required to authenticate its subscribers. A subscriber has established credentials with this entity.

Beyond the security enhancements that were discussed in the previous section, the main features in HS2.0 Release 1 are based on IEEE 802.11u and include additions to the AP's beacon and the usage of ANQP (Access Network Query Protocol).

The additional information provided on the beacon indicates:

- the type of AP such as private NW, private NW with guest access, chargeable public NW, free public NW, etc.,
- venue info such as business, educational, vehicular, bank, private residence, bus, etc.,
- load information such as the total number of currently associated devices to the AP, channel utilization percentage and an estimate of remaining available admission capacity in terms of available medium time,
- Organization Identifiers to identify up to three roaming consortiums or subscriber service providers (SSP). Note: Mapping between the arbitrary OI number and the member subscriber service providers of the roaming consortium is outside the scope of HS2.0 Phase 1 and 802.11u specifications.

Overall, the beacon information assists the user during manual hotspot selection and if the UE knows its home OI and notices an AP advertising it, the UE knows it can use its home service provider's credentials to access the AP.

The ANQP allows the following capabilities to be exchanged between the client and AP provider:

- **Network Authentication Type** can be used by the AP provider to indicate the additional authentication mechanisms supported. An example would be a user having to accept the terms and conditions for Wi-Fi network access. In general, the additional step for authentication is done only if required, e.g., by the local law.
- **NAI Realm List**: the NAI Realms of the service providers whose networks or services are reachable via the AP. Also, this list may contain the supported authentication mechanisms per each service provider. The intended usage is to allow the subscriber who has received credentials (username/password or certificate credentials) from its home operator with the NAI realm is part of the credential information to match against the NAI Realm List from the AP in order to decide whether to connect to this AP or not.
- **3GPP Cellular Network Information** is mandatory only for devices having SIM credentials. It contains a list of PLMNs that are accessible via the AP. This information is only applicable for Wi-Fi access authentication: when UE finds an AP with its HPLMN in ANQP info, UE knows it can perform Wi-Fi access authentication through the AP, EAP-SIM or EAP-AKA is used.
- **Domain Name List provides** a list of one or more domain names of the entity operating the Wi-Fi access network, i.e. operator who owns the Wi-Fi radio access network. This allows the UE to compare the FQDN in its credentials against the Domain Name list retrieved from the AP to determine if it is connecting to a hotspot that is operated by its home Service Provider.

Passport Release 2 carries the following features:

- **On-Line Signup** enables automatic signup for HS2.0 Service Provider's services without prior credentials. During the on-line signup process, a new subscription and credentials are created for the UE/user. This procedure has no relationship to ANDSF network selection.

- **Policy Provisioning** allows the HS2.0 service provider to define the preferred roaming partners – i.e. HS2.0 Service Providers – in prioritized order. Basically, it allows the UE to identify HS2.0

home SPs and roaming partners that should be used when the home SP is not accessible directly. Roaming partners identify the HS2.0 SPs that do have an agreement with the home 3GPP operator to perform Wi-Fi access authentication.

While Passpoint Release 1 features are primarily complementary to ANDSF, the Passpoint Release 2 defined management object competes with ANDSF as they both provide network selection related instructions to the UE. HS2.0 MO as defined in Release 2.0 carries information (e.g. support for multiple service providers and non-SIM credentials) that GSMA WBA Joint Wi-Fi Roaming TaskForce did not consider to be acceptable for a dual mode device that supports both Wi-Fi and cellular access technologies. The TaskForce's recommendation was to use ANDSF for dual mode devices and to update it to include relevant aspects of the HS2.0 MO. Based on the TaskForce's request, 3GPP initiated work on an ANDSF Release 12 work item called WLAN_NS with the intention to update ANDSF accordingly. Currently, the WFA has no intention to start any work that would be called Passpoint Release 3.

2.1.5 INTELLIGENT NETWORK SELECTION

Wireless networks are becoming increasingly heterogeneous – often composed of different cellular layers and multiple access technologies. It's now possible for a given UE to be simultaneously in range of a variety of different networks: traditional cellular networks (i.e., 3G/LTE (e)NodeB's), integrated small cells (i.e., with 3G, LTE, and Wi-Fi), and a variety of standalone Wi-Fi AP's (i.e., ranging from private consumer-grade AP's to carrier-grade AP's that are tightly integrated with existing cellular networks). Given this reality, selecting the best network for a given user at a given time in a given location is critically important for optimizing user experience.

As depicted in Figure 6, there are several aspects to intelligent network selection. In particular, there is a variety of (1) network-based information that can be leveraged to help make network selection and traffic steering decisions, and a number of conceivable ways in which to distribute that information to devices (2).

Some examples of this information can include network-distributed selection and steering policies, real time network conditions in the cellular and Wi-Fi networks, subscriber profiles and analytics based on historical data, etc. Additionally, the device contains local intelligence about critical information such as radio conditions, relative motion, battery utilization, etc. The following sections will discuss in greater detail the current state-of-the-art and existing challenges with both the network and device aspects of intelligent network selection.

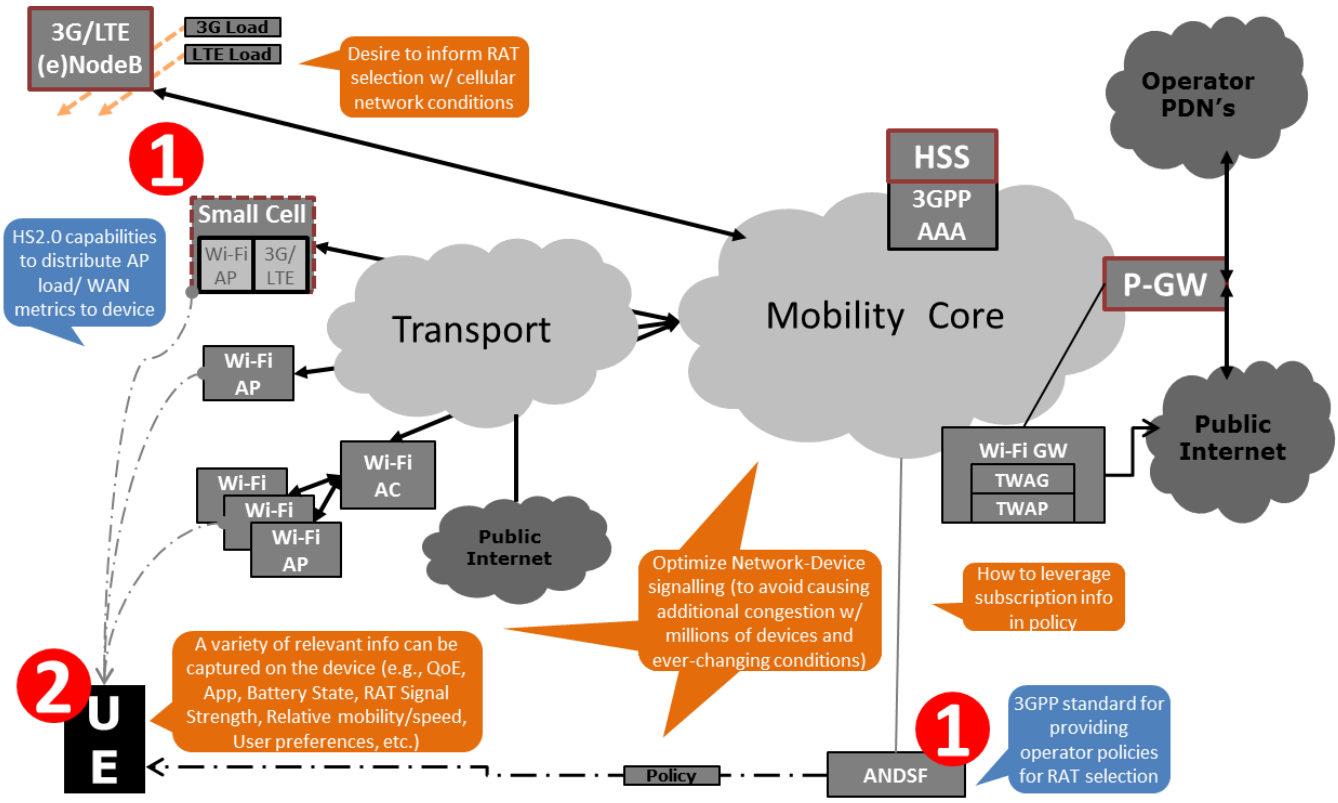

Figure 6. High-level aspects of Intelligent Network Selection.

2.2 NETWORK ASPECTS OF INTELLIGENT NETWORK SELECTION

The Access Network Discovery and Selection Function (ANDSF) is a primary enabler of intelligent network selection between 3GPP and non-3GPP access networks. ANDSF is an optional network element in the 3GPP Evolved Packet Core (EPC), the purpose of which is to provide UE's with useful information and operator-defined policies to guide network selection decisions. ANDSF was first defined in 3GPP Release 8, and continues to evolve as depicted in Figure 7. Evolution of ANDSF in 3GPP standards since Release 8. Figure 7 below:

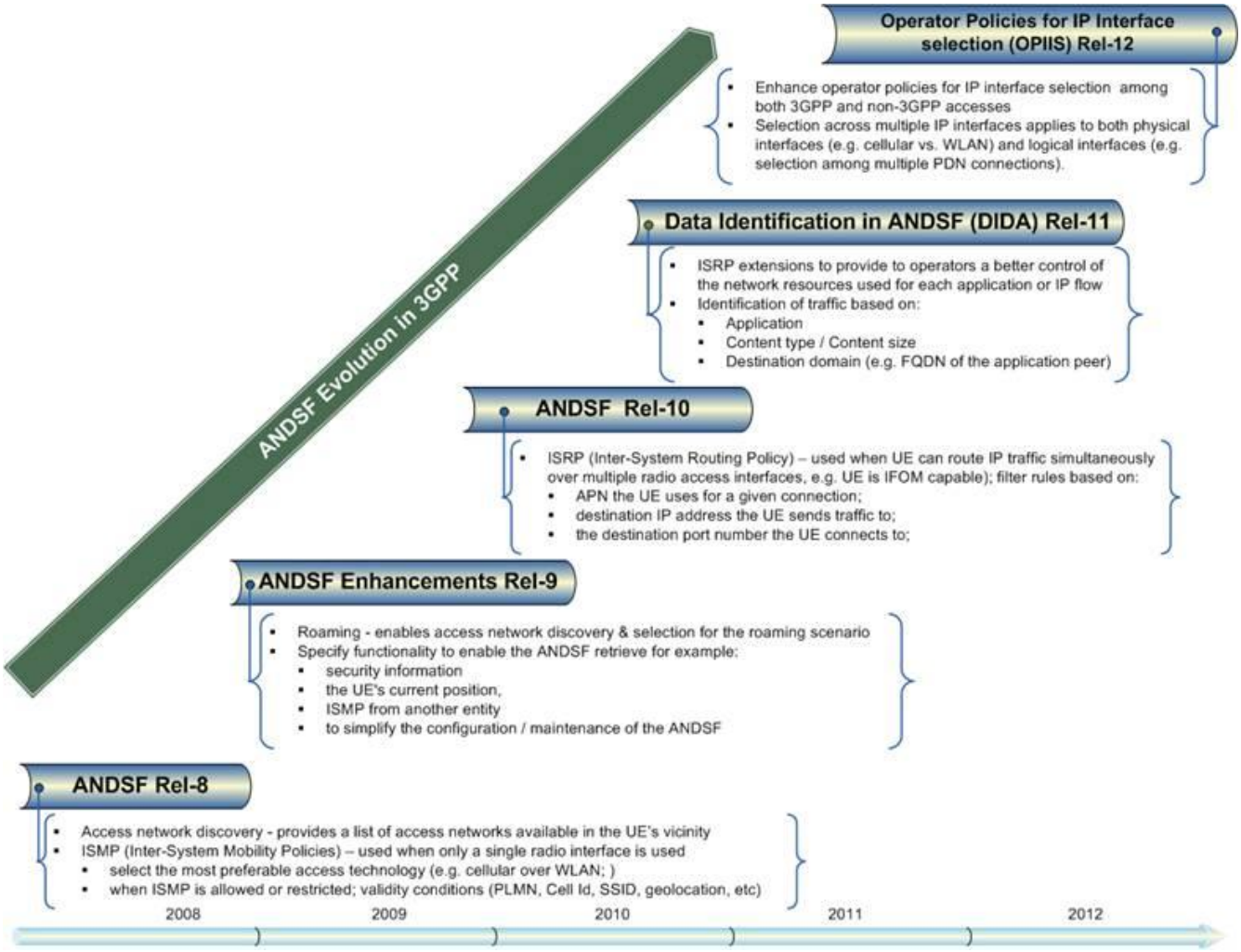

Figure 7. Evolution of ANDSF in 3GPP standards since Release 8.

The ANDSF element is a server located in the operator's network that uses a standardized interface (S14) to distribute the network selection information and policies. ANDSF is a standalone node in that the UE-to-ANDSF S14 interface is the only interface to ANDSF that has been standardized – any interaction between the ANDSF server and other network elements is outside the scope of current 3GPP standards. For disseminating the network selection information and policies, both a push and pull mode of operation are possible. A UE can query the ANDSF server to pull the desired information, or the ANDSF server can initiate a push to distribute its information to the target UEs.

The information and policies provided by ANDSF are used by the UE to help discover nearby networks that may be available (including non-3GPP networks such as Wi-Fi networks) and to help understand how those networks should be prioritized by the UE in network selection decisions (e.g., when, where, and for what traffic should a particular Wi-Fi SSID be preferred over the 3GPP network). The next section provides greater details on the various information and policy elements that can be provided by ANDSF.

2.2.1 ANDSF INFORMATION AND POLICY ELEMENTS

ANDSF communicates information and policies to the UE using the S14 interface. That interface relies on the Open Mobile Alliance – Device Management v.1.2 (OMA-DM) specification to distribute the relevant parameters to the UE. This information is organized within nodes of a Managed Object (MO), with each leaf object containing the specific parameter value. As seen in Figure 8 below, the ANDSF MO contains several major nodes, including ones for Discovery Information, Inter-system Mobility Policies and Inter-system Routing Policies. Brief descriptions of each are included below.

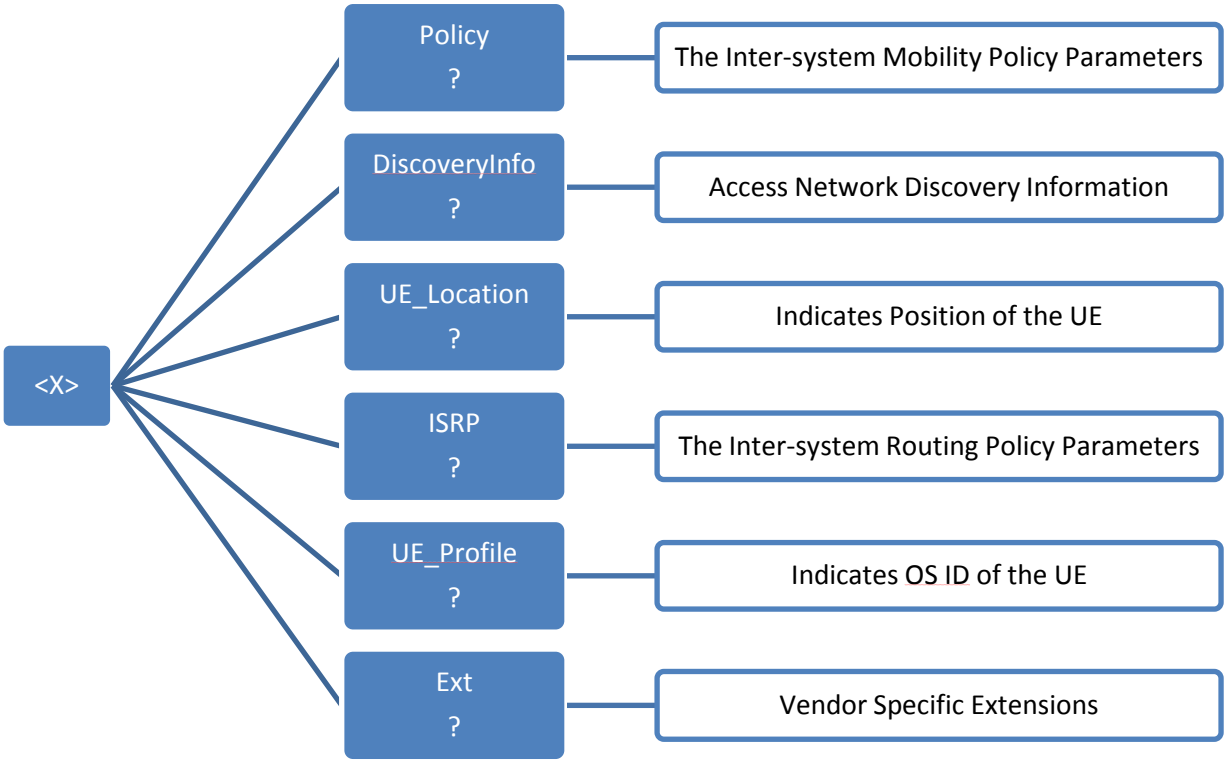

Figure 8. ANDSF MO - The high-level structure (based on 3GPP TS 24.312 Release 11.6).

The Policy Node:

This node contains the Inter-system Mobility Policies (ISMP). ISMP rules apply to UEs that can route IP traffic over only a single radio access interface at a time. Included in this node are the rules that are used to prioritize or restrict access to certain access networks.

In particular, this node includes rules for if a specific access technology type is preferable to another (e.g. Cellular is preferable to WLAN); or if a specific access network identifier is preferable to another (e.g. WLAN SSID-1 is preferable to WLAN SSID-2); or if inter-system mobility is restricted from one access type to another or when certain conditions are met (e.g. a handoff from Cellular to WLAN is restricted).

Also included in this node are the validity conditions for a given policy. These conditions include specific dates, times of day, and/or locations for which a given ISMP rule shall be applicable. For example, an ISMP rule could be crafted such that for a given UE in area A from 4pm to 8pm the cellular network should be the preferred access – while at all other times the Wi-Fi network with SSID-1 should be the preferred access.

The Discovery Information Node:

This node contains the Access Network Discovery Information (ANDI). ANDI can be used by operators to provide specific information to the UE about the access networks that are available in the UE's vicinity.

In particular, this node includes information on the access technology type (e.g., WLAN) and the relevant radio access network identifiers (e.g., the HESSID, SSID, and/or BSSID of a WLAN). This discovery information is provided to UE's based on a given UE's geolocation.

The ISRP Node:

This node contains the Inter-system Routing Policies (ISRP). ISRP rules apply to UEs that can simultaneously route IP traffic over multiple radio access interfaces at the same time. Included in this node are the rules that are used to prioritize or restrict the routing of specific IP flows to certain access networks.

More specifically, ISRP rules support 3 different types of flow distribution (each with separate MO nodes): ForFlowBased, ForServiceBased, and ForNonSeamlessOffload. The ForFlowBased node applies to IFOM-capable UE's, ForServiceBased applies to MAPCON-capable UE's and ForNonSeamlessOffload applies to Non-seamless WLAN Offload capable UE's. IFOM-capable UE's are able to seamlessly route IP flows to the same PDN over different radio access technologies (RATs). MAPCON-capable UE's are able to simultaneously route traffic for different APNs over different RATs. NSWO-capable UE's can route IP flows non-seamlessly over the WLAN radio interface.

For the ForServiceBased/MAPCON case, the traffic routing rules are based on the APN of the traffic (e.g., traffic for APN-1 is routed via the cellular RAT, while traffic for APN-2 is routed via the WLAN). As for the ForFlowBased/IFOM case and ForNonSeamlessOffload/NSWO case, each filter rule may identify traffic based on destination/source IP address and port number, transport protocol, DSCP marking or Traffic Class, destination domain name and application identity. There are also validity conditions attached to each filter rule that can indicate the specific date, time of day, and/or location for which a given ISRP rule shall be applicable.

The UE_Location Node:

This node contains the UE location descriptions.

The UE_Profile Node:

This node contains the OSid of the UE.

The Ext Node:

This node can be used to store vendor-specific information about the ANDSF MO. The contents of this node are outside the scope of the 3GPP standards.

2.2.2 ROAMING AND ANDSF

3GPP specifications allow for a visited PLMN to influence WLAN selection and traffic routing policies via Visited ANDSF (called the V-ANDSF) policies while the device is roaming. Up until Release 11, if there was a conflict between V-ANDSF and Home ANDSF (H-ANDSF) policies, V-ANDSF policies on network selection and traffic routing were allowed to prevail. This behavior however created scenarios where even for non-seamless WLAN offload, relevant home operator policies could be over ruled by the device following roaming partner's ANDSF policies.

In Release 12, this limitation is expected to be corrected so that the device would take guidance from the home operator's ANDSF on whether individual roaming partner's ANDSF policies should be followed. This approach will allow the home operator to selectively enable or disable ability of its roaming partners to influence WLAN network selection and traffic routing behavior of devices while roaming on their network.

2.2.3 WHAT IS NOT SPECIFIED IN ANDSF STANDARDS TODAY

ANDSF provides a useful framework for distributing flexible operator-defined network selection information and policies. However, there is additional information that is likely available in an operator's network and which could be used to improve network selection decisions, but that is not captured in the current iteration of ANDSF. This section provides a current snapshot of these items, with possible solutions for each item explored in greater detail in the next chapter.

Network Conditions:

One of the most important aspects of an intelligent networks selection decision is a consideration of the current network conditions of all of the relevant access networks. An example of this is the real-time load on the radio link of a cell site. Whether that load is high or low could have a dramatic impact on a given users quality of experience, and could influence a decision to select that access network relative to the other available options. Currently, this type of network condition information is not factored into ANDSF policy rules, nor are there standardized mechanisms for capturing and disseminating that information.

In order to leverage this type of information, it first must be determined what type of information is of interest (and at what timescale), how to best capture and collect this information, and finally how to best use and/or disseminate that information to aid network selection decisions. This is discussed in greater detail, and potential solutions are proposed in the next chapter.

User/Subscription Information:

The ability to tailor network selection rules based on a given user's subscription level (e.g., silver vs. gold vs. platinum), or other aspects of that user's profile (e.g., their usage history or their proximity to any usage caps/allocation thresholds, etc.) could be useful inputs for operators to factor into network selection rules. While the ANDSF standards currently allow for ANDSF policies that are user subscription dependent, there is no standardized interface between ANDSF and the user's subscription/profile information (e.g., between ANDSF and UDR or HSS).

Other types of network-based info:

There are several other pieces of information about a given access network that may be available to the network operator but which are currently not captured in ANDSF policy. For example, there are many

different types of Wi-Fi access points with a wide range of supported capabilities. In particular, a given AP may be HotSpot 2.0/Passpoint compliant or not, or it may be a trusted WLAN AP or not. A HotSpot 2.0 compliant AP may be provide a more secure connection and thus may be favored over non-HotSpot 2.0 APs. The flavor of Wi-Fi AP is not currently captured in the ANDSF policy; however, such information could be used to improve network selection decisions.

There is also venue-related information which could be used in guiding network selection decisions. For instance, the WFA HotSpot 2.0 specification includes provisions for certified APs and UEs to support the 'Interworking' information element (IE) within the IEEE 802.11 beacon and probe response frames[8]. This information element includes several venue-related attributes within the Venue Info field. This includes the Venue Group, Venue Type and the Access Network Type. These provide the following information:

Venue Group: Describes information about a venue group such as Business, Educational, Residential, Outdoor, etc.

Venue Type: Describes information about a venue type such as Arena, Stadium, Convention Center, Library, Coffee Shop, School, etc.

Access Network Type: Specifies a specific access network type such as Private network, Chargeable public network, Free public network, etc.

In addition to the Interworking IE, HotSpot 2.0 also requires that certified APs and UEs support the Venue Name ANQP element. This ANQP element provides zero or more venue names to be associated with the BSS such as "Silicon Valley Mall", "Museum of Modern Art", etc.

There are many ways in which this information could be used to improve network selection decisions. For instance, ISMP/ISRP rules could be enhanced to include venue related information. This would allow 3GPP operators to prioritize WLAN network selection based on the Venue Info field and Venue Name. For example, in a busy location such as the passenger terminal in a large airport, certain roaming partners may be preferred whereas in a small coffee shop a different set of partner networks may be preferred, so the list of WLAN networks would need to be prioritized accordingly.

However, even though this venue information may be available in HotSpot 2.0 capable networks, the 3GPP ANDSF standards currently provide no means of factoring this information into policy. Thus, section 3.1.3 will discuss recommendations for bringing this functionality into the ANDSF standards.

Network-based policy for local UE-info/intelligence:

In addition to all of the information that is available in the network, there is a considerable amount of information/intelligence that is local to the UE and which could be used to improve network selection decisions. For instance, a UE's current battery utilization level is known locally to the device and that information could be used to influence whether one or multiple radios are used at a given time. Currently, though, there is no way within the ANDSF standard to craft ISMP/ISRP policies that take this type of local information into account. This topic will be addressed in greater detail in Section 3.2 of this white paper.

[8] Based on joint contribution by Intel, AT&T, Huawei, and Broadcom Corporation for 3GPP SA WG2 Meeting #96 (S2-131168)

2.2.4 ANALYTICS AND ANDSF

With ANDSF, 3GPP established a framework for communicating to the UE operator policies for network selection and traffic routing. However, 3GPP does not specify inputs for formulating policies in the ANDSF server beyond those obtained from the UE via the S14 interface (primarily UE location and device type). A 3GPP compliant implementation of ANDSF could simply provide static, provisioned policies to the UE.

However, as indicated in the previous section, the ANDSF server can factor into policy definition additional information from the network (e.g., subscriber profile repository (SPR) or User Data Repository (UDR), and information available from the mobile). Leveraging this information is neither restricted nor standardized in ANDSF today. This is discussed in greater detail in section 3.1.2.

The selection of OMA-DM as the S14 (UE←→ANDSF Server) interface protocol restricts the reasonable use of external information in ANDSF policy to factors that may change on the order of 30 minutes, to hours or days, or longer. This divides control over access selection into two complementary time-based components:

- Fast changing (e.g., less than ~30 minutes) factors known to the network and universal to all UEs within a cell can be best managed by broadcasting relevant information to UEs, or by other proposed mechanisms where the 3GPP RAN takes an active role in directing UEs to Wi-Fi. The primary application for this is real-time load balancing between access options, and hence the mechanism requires a feedback loop to assess the efficacy of load balancing efforts. Whether implemented via broadcast or other means, real-time signaling to shift UEs currently on 3GPP to Wi-Fi should be executed in the context of expanded ANDSF provided policy rules.

- Slower changing (e.g., 30 minutes or greater) factors with a granularity as fine as per-subscriber can be accounted for in the ANDSF server policy and sent individually to UEs via S14. This enables analytics tailored policies that reflect longer term factors known by elements both inside and outside the scope of 3GPP. Examples include subscriber affinity level from a loyalty management system, or cell-level congestion based on historical analysis of weekly or daily trends.

Access selection based on available a-priori information and delivered in more slowly changing ANDSF policies provides a baseline for faster load balancing between available Wi-Fi and 3GPP access options. This makes subsequent real-time, closed-loop load balancing based on fast changing factors simpler to control and more stable.

Note that supporting per-UE or per-cell level policies that reflect analytics does not mean that the ANDSF server must push new policies to the UE whenever it changes location, or that separate, unique policies need be maintained for 1000s of cells. The ANDSF managed object allows policies to be specified for a designated validity area and time-of-day. Hence a different policy may be specified, for example, for the 5% most congested cells during busy-hours based on historical data and predictive analysis. The simplest implementation of this could have just two policies, one for when cells are congested and a second for when cells are not. Both would be sent to the UE for use when in a validity area at the designated time-of-day, and would be updated by the ANDSF server only when long-term busy hour trends changed.

Network Congestion is but one of one of many considerations in a comprehensive solution to determine the best access option for a UE. Other examples are shown in Figure 9, divided into Dynamic Subscriber Analytics and Dynamic Network Analytics. As the name implies, Dynamic Per-subscriber analytics consists of factors that may influence access selection based on subscriber intelligence, resulting in personalized policies. For example, a mobile operator may wish to establish policies that more aggressively steer to Wi-Fi subscribers that stream large amounts of video, while preferentially keeping on the 3GPP network subscribers that have recently complained to customer care about Wi-Fi performance.

Dynamic network analytics can include other factors beyond congestion trending. As indicated in Figure 9, examples include security threats, network element outages, and hardware loading. The ANDSF server can account for factors such as these via a policy engine that accepts analytics information as input to the policy decision process.

Dynamic Subscriber Analytics	
Quality of Experience	Video stalled during last operator PPV video session on Wi-Fi
	Subscriber has been complaining on Twitter about operator Wi-Fi service & has >10K followers
Subscriber Analysis	Recent Google searches for Alternate Mobile Carrier?
	Using Operator Applications?
	Chronically searches for on-line coupons / discounts
	Big Purchaser of operator sponsored content?
	Subscriber Loyalty analysis?
	Application tendencies (video?)
Wireless Service	Usage / Quota
	Calls to Customer Care?
	Data rates experienced?

Dynamic Network Analytics	
Network Analytics	Cell HW load
	Signatures on known issues e.g. APN configuration, virus, bad hardware
	3GPP air Interface bearer plane loading
	DoS Attack
	Adjacent cell air-interface bearer plane loading
	Unexplained performance degradation
	Per-cell video / audio quality metrics
	Core Network Signaling load surge
	Major event occurring in area
	Network element outage
	Wi-Fi Loading & QoE

Figure 9. A wide range of Subscriber and Network Analytics may be used to drive the ANDSF and Tailor Access Selection Policies.

2.3 DEVICE ASPECTS OF INTELLIGENT NETWORK SELECTION

Mobile traffic has been growing at a very fast pace and the trend is continuing. Service providers are actively looking for solutions to cost effectively leverage all available radio technologies, including cellular and Wi-Fi technologies to meet the increased mobile traffic demand and achieve consistent policy-based end user experience.

Currently, there are different implementations of network selection from various UE/OS/OEM vendors that result in different behaviors and an inconsistent decision making process in devices; therefore, today there is no consistent user experience across various device platforms. Furthermore, no standardized

solutions exist today to leverage any knowledge of real-time network conditions, such as cellular network or Wi-Fi congestion.

A key aspect addressed by this paper is the definition of the UE and network functionality needed to support intelligent selection of the optimal radio access technologies (Wi-Fi vs. cellular) and to route user traffic on a per application basis. Specifically, we intend to address functionality that enhances present mechanisms for offloading, and considers intelligent network selection based on the combination of operator policies, network intelligence and the device intelligence, in order to achieve improved and consistent user experience.

2.3.1 INTELLIGENT NETWORK SELECTION AND TRAFFIC STEERING

A multimode device performs two steps in order to enable traffic offloading from cellular to WLAN and routing of traffic over the two available interfaces.

In the first step, the device performs network selection. This paper does not discuss network selection for the 3GPP access link, since such mechanisms are well defined already in standards. The focus of this paper is on WLAN network selection. The device needs to select the most appropriate WLAN network available based on a series of conditions, which are better described in the rest of the paper.

In a second step, the device performs traffic steering between multiple access technologies. If the device is capable of transmitting data only over a single radio interface, the device needs to select which interface should be used based on a series of conditions. If the device can simultaneously transmit data over multiple interfaces, the device determines which data traffic should be routed over which access.

2.3.2 ROLE OF DEVICE AND KEY REQUIRED INFORMATION

The role of the device is two-fold: provide a better user experience and enable the operator to move traffic from the cellular network. The device enables operators to steer traffic and offload it to WLAN for better user experience and to allow better utilization of network and radio resources.

The device is the only entity aware of actual connectivity conditions (e.g. radio conditions, throughput over existing connectivity, etc.), and real-time conditions in the device (e.g. type of pending traffic, active applications, status of device including battery levels, etc.).

The device is in the unique position to make the best final determination of when traffic can be transported over WLAN (e.g. based on real-time radio conditions, type of pending traffic, device conditions such as mobility and battery status, etc.). The device can make decisions based on policies from the operator and knowledge of the LOE (Local Operating Environment). The LOE is a set of information that the device can use along with other information (e.g. knowledge about network load, operator policies and user preferences) as inputs to operator INS to select the most suitable access for routing the traffic, and has been left unspecified since it is based on specific implementations and the information available inside the device.

Current devices rely heavily on the use of SSID when configured by the user or an operator to identify preferred networks. Though standards solutions such as 802.11u have been defined for a while and would allow the mobile device to discover a set of features supported by the WLAN network, such solutions have not been deployed widely and devices do not usually make use of such mechanisms.

2.3.3 CURRENT STATE OF ART

When analyzing the current state of the art, device solutions that have already been implemented and deployed need to be looked at separately from the current solutions available in standards.

2.3.3.1 DEVICE SOLUTIONS

Current devices deploy a variety of proprietary solutions for the selection of WLAN and the selection of traffic routing. Most devices today do not connect to the operator core network, and therefore the discussion in this section relates to Internet traffic and IP address preservation is not considered.

Most devices tend to connect to WLAN whenever WLAN is available. The selection of the WLAN network to use is at present based on user preferences and in some cases on operator-configured lists of preferred WLAN networks. As an example, some operators deploy client-based solutions where the operator downloads to the device applications that enable discovery of a list of preferred WLAN networks in the location where the device is currently roaming. In some cases, such client-based solutions select a WLAN network based on popularity/quality of the APs that the network collected from UE feedback. Most of these solutions then rely on manual user selection among the networks indicated by the application. Also, existing application-level solutions may have conflicts between the decision made by such applications and the connectivity decisions made by the lower layers in the device, typically due to the application layer not having access to all the information required to make an educated decision.

Current devices implement proprietary algorithms to select a suitable AP before attempting connectivity. Such algorithms consider a variety of parameters, such as RSSI value, MAC statistics, etc. Current devices can also implement algorithm to measure the throughput on the cellular/Wi-Fi link, based on a variety of parameters, even with current networks that do not provide specific load indications.

Basic devices, especially those not using any applications that require a specific throughput, tend to move all the IP traffic not corresponding to operator-provided voice services to WLAN any time WLAN is available. More advanced devices implement algorithms to determine for what traffic WLAN is appropriate and route traffic appropriately.

Some operating systems use proprietary algorithms to implement clientless solutions to aid in WLAN selection, where the algorithm is built in the operating system.

All these solutions are implemented with vendor specific solutions across different operating systems and hardware platforms, often leading to inconsistent behavior.

In summary, there are different UE/OS/OEM behaviors and inconsistency of decision making process in device in the existing implementations. Figure 10 below provides a high-level illustration of the current state-of-the-art of UE functionality.

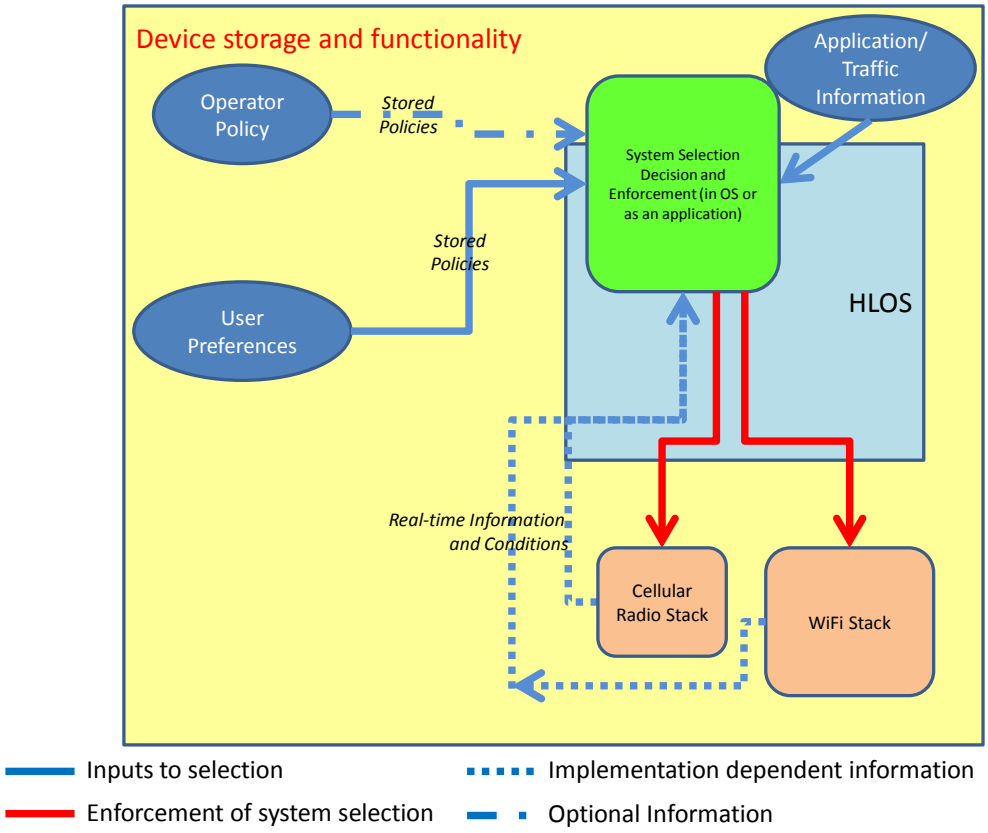

Figure 10. Current State-of-the-Art of UE functionality.

2.3.3.2 STANDARDS SOLUTIONS

3GPP I-WLAN

First specified in 2006 as part of 3GPP Release 6, the 3GPP I-WLAN standard ([TS23.234], [TS24.234]) defines a mechanism to enable interworking between 3GPP systems and Wireless Local Area Networks (WLANs) and providing bearer services allowing a 3GPP subscriber to use a WLAN to access 3GPP PS based services. I-WLAN defines authentication and authorization to devices with 3GPP credentials to connect to the Internet or to the operator core network using WLAN.

As part of the I-WLAN standard, network selection for WLAN has been defined. Specifically, I-WLAN defines a mechanism for the mobile device to select a preferred AP and then perform PLMN selection in order to authenticate with the most preferred PLMN. I-WLAN defines a mechanism to provide configurations to the UE by using a management object or USIM files. With I-WLAN, the operator can provide the UE with a list of preferred APs (e.g. using SSIDs) and ordered lists of PLMNs. The PLMN selection part of the I-WLAN mechanism has been defined in line with the 3GPP PLMN selection mechanism defined for the cellular link ([TS23.122]). It allows the home network to indicate which networks have priority, and how to use prioritized lists of network either defined by the user or the home operator.

3GPP ANDSF

As discussed in section 2.2, ANDSF has been defined in 3GPP from Release 8 to Release 11 as a framework for policy provisioning to a device in order to enable a device to perform appropriate traffic routing decisions between a 3GPP link and WLAN. ANDSF has not been designed as a mechanism for WLAN selection in terms of selecting a service provider/PLMN. However, ANDSF may impact the selection of the SSID used by the device.

ANDSF enables an operator to provision a device, via OMA-DM, with an MO containing a set of rules for traffic routing. The device periodically re-evaluates the validity conditions of the rules and selects the active rule with the highest priority. Validity can include date, time of day, location (e.g. defined as specific geographic location, cellular cell, etc.). The device uses the active rule traffic routing information (e.g. preferred RAT, specific WLAN that is preferable, forbidden WLAN, specific IP traffic) to decide whether existing traffic should be routed over 3GPP or WLAN.

The ANDSF MO contains the following optional information:

- Access Network Discovery Information (ANDI): ANDI provides a list of access networks that may be available in the vicinity of the UE, including radio access network identifiers, technology specific information, validity conditions for the information provided (e.g. location).
- Inter-System Mobility Policies (ISMP): ISMP provides devices that can only route traffic over on one RAT at a time (as defined from release 8 and onward) with policies for the selection of what RAT should be used for routing all the data traffic.
- Inter-System Routing Policies (ISRP): ISRP provides devices that can simultaneously route traffic over different RATs at the same time (i.e. IFOM-capable devices as defined from Release 10 and onward) with policies indicating what traffic should be routed over what RAT, and whether EPC connectivity or NSWO should be used. The traffic is identified either as an IP flow descriptor, the destination domain used by an application, or the identifier of the application that generates the traffic.

ISMP and ISRP in Release 8 to Release 11 have not been defined for WLAN selection, and only provide policies for a device to perform traffic steering decisions. Once the device has gained connectivity to WLAN, e.g. using I-WLAN mechanisms or other currently implemented solutions, the device configured with the ANDSF MO can use the operator policies, together with user preferences and information on the Local Operating Environment (LOE) to select how traffic should be routed. Figure 11 below illustrates UE functionality based on current ANDSF standards.

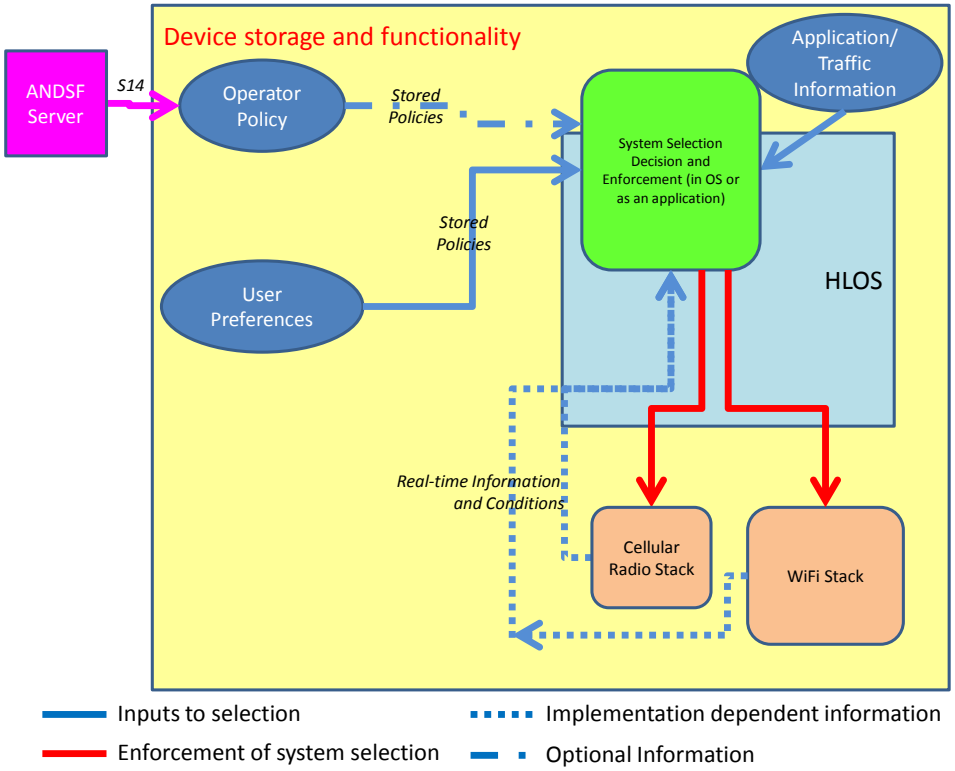

Figure 11. UE functionality based on current ANDSF standard.

HotSpot 2.0

WFA HotSpot 2.0, also known as Wi-Fi Certified Passpoint or HS2.0, is a set of mechanisms defined by WFA in order to enable mobile devices to automatically join a Wi-Fi network based on a subscription whenever the user enters a Hotspot 2.0 area. Hotspot 2.0 aims at providing better bandwidth and services-on-demand to end-users, and better selection of Wi-Fi networks, whilst also alleviating mobile carrier infrastructure of traffic overhead. Hotspot 2.0 is based on the IEEE 802.11u standard, which was designed to enable cellular-like roaming.

HotSpot 2.0 defines mechanism to configure devices with operator policies/preferences and for the device to discover the characteristic of the available networks. Currently SSID is used as the main identifier for any WLAN hotspot; with the introduction of HotSpot 2.0, the role of WLAN identifiers such as SSID decreases since the device will be selecting WLAN networks based on a variety of parameters and identifiers (e.g. Organizational Identifier, in addition to SSID), thus enabling operators to deploy WLAN AP with more flexibility and to simplify roaming.

In HotSpot 2.0, after scanning for WLANs and discovering which APs support HotSpot 2.0, the mobile device can use the 802.11u ANQP to learn more about the characteristics of the network, including which networks support available credential(s), 3GPP-specific information for devices authenticating through SIM/USIM credentials, roaming consortium identifiers, WAN Metrics and IPv4/IPv6 connectivity information, etc.

HotSpot 2.0 allows an operator to provide the device with a set of policies defined in a Management Object. The device uses the information in the HotSpot 2.0 MO (e.g. preferred roaming partners list) to select the most appropriate WLAN network based on the operator preferences.

A comparison between current I-WLAN, Release 11 ANDSF and HotSpot 2.0 is provided in Figure 12 below.

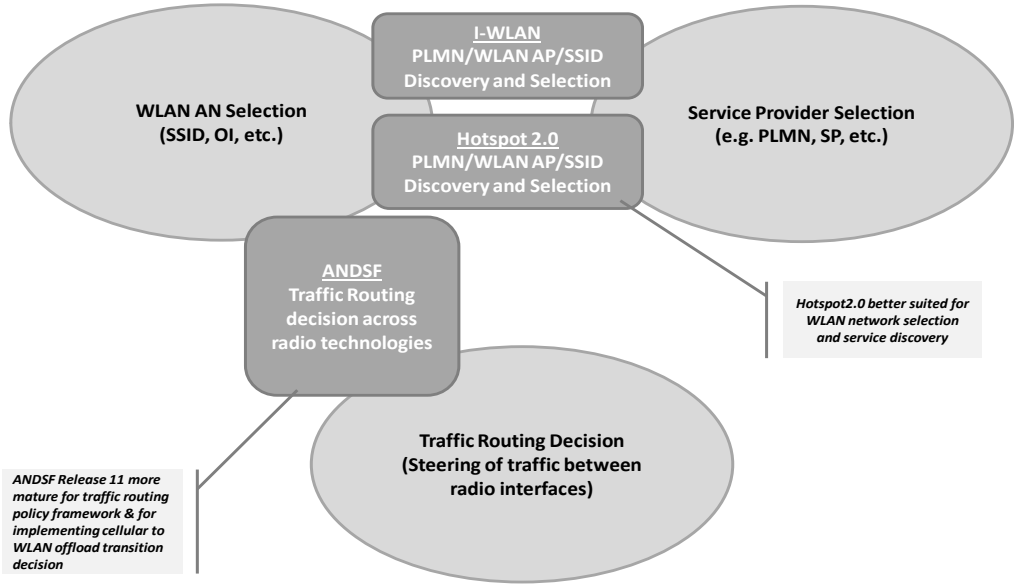

Figure 12. Functionality comparison of I-WLAN, ANDSF and HotSpot 2.0.

2.3.3.3 MARKET ADOPTION OF CURRENT STANDARDS SOLUTIONS

HotSpot 2.0 is still being developed, but many AP products have already been announced and deployment of HS2.0 APs is expected to take place soon, before release 12 3GPP standards are completed. Even with the completion of HS2.0 specifications, it is unclear how fast HS2.0 capable access points will enter the market and therefore how much an operator and mobile devices can rely on HS2.0.

Though the standard has been available for years, at present there seem to be no wide-scale deployments of I-WLAN, though some networks in the past have been running trials. Therefore, there is no market experience on the performance and usefulness of I-WLAN, and there are no market indications that I-WLAN will be adopted by operators. At present, considering that ANDSF is a recent standard (Release 11 was completed in 2012), no commercial deployments of ANDSF exist, though trials are undergoing to understand the feasibility of ANDSF-based solutions. However, operators have expressed high interest in the use of ANDSF to control network selection and traffic steering for mobile devices. Investigations on the ANDSF adoption and applicability are ongoing, therefore further enhancements and extensions of ANDSF are to be expected in future 3GPP releases.

2.3.4 GAP ANALYSIS

This section identifies the gaps present in the solutions currently available for network selection and traffic steering. In particular, this section identifies gaps in existing ANDSF and HotSpot 2.0 policy frameworks, gaps in existing UE behavior, and lack of network-related intelligence in the device intelligence. Section 3.2 will then address the gaps that are identified in this section.

2.3.4.1 POLICY

Considering the current standardized mechanisms:

- ANDSF enables an operator to define a rich set of rules and criteria to guide a device to select the most appropriate access, among those available, to route the device traffic. However, at present ANDSF focuses mostly on defining policies for the routing of traffic between different accesses and does not allow the definition of rich policies for the selection of WLAN networks.
- Existing ANDSF policies are limited in terms of considering knowledge of the network status (e.g. load on the cellular or WLAN side), UE conditions (e.g. velocity of the UE, etc.).
- Selection of optimal WLANs outside of registered PLMN is not possible.
- The I-WLAN solution is based on a semi-static management object provisioned to the device through OMA-DM. Specifically, though the operator can refresh the MO in the device when needed, the information in the MO is used statically (e.g. prioritized list compared to networks available), without considering any real time conditions such as location, time, type of connectivity, type of traffic, etc. Moreover, I-WLAN relies heavily on the use of SSIDs to identify the preferred WLAN networks, but maintaining an up-to-date list of all SSIDs used by hotspot providers may become very cumbersome and inconvenient, especially since roaming agreements may change and since the hotspot providers may modify or extend their SSIDs.
- The combination of pre-release 12 ANDSF (and specifically ANDI) and I-WLAN may lead to the selection of sub-optimal networks, and does not enable the re-selection of a different PLMN, thus leading to results that are contrary to the operator needs.
- HotSpot 2.0 defines mechanism for the device to discover the characteristics supported by the AP and minimizes the reliance on SSIDs. However, the HotSpot 2.0 MO does not contain any information specific to the type of traffic that should be transported over WLAN and does not allow selection of WLAN based on dynamic conditions.

When considering these existing solutions, the WLAN network selection in a dual mode handset may be based on information provided to the handset by the operator in e.g., an ANDSF Management Object or a WFA Hotspot 2.0 MO or both, or it can be pre-configured in the device. In this way, inconsistent sets of information from different sources can be present in the device, thus leading to conflicting set of rules for the UE. Solutions are needed to ensure that such conflict do not arise, while avoiding complex information management by the operator (e.g. maintenance of coordinated management objects repositories) and avoiding complex device implementation to resolve conflicts.

2.3.4.2 UE BEHAVIOR

The following aspects of the UE behavior (including the type of information available to the UE) need to be considered:

- The role of IP address preservation (not considered in the current selection of WLAN). Selecting a WLAN network that does not provide IP address preservation defies the purpose of the offloading when the device requires it for the services that would benefit from offloading.
- Devices should be enabled to verify/measure key factors of connectivity over WLAN contributing to a better user experience: channel quality (local link characteristics), Internet connectivity (e.g. firewall that prevent access to the Internet, captive portals that prevent applications from connecting) and congestion (e.g. public Wi-Fi speed is too low). Enabling WLAN selection using local link and end-to-end path characteristics (e.g. available bandwidth, latency, Internet reachability, etc.) as a single input will allow for better selection from the point of view of user experience and successful offloading based on the operator needs.
- Devices should be enabled to obtain/measure key factors regarding cellular network conditions, such as load or downlink/uplink performance. In particular, it is important that devices are enabled to receive cellular network congestion related parameters that can be used for intelligent network selection to achieve a better user experience.
- Standard or common practices should be developed on how operator policies are implemented and enforced in the device.

2.3.4.3 NETWORK-RELATED INTELLIGENCE IN THE DEVICE

When performing INS decisions, both for network selection and traffic steering, the mobile device can benefit from knowledge about real time network conditions and quality parameters. The following aspects of the device's knowledge about network condition need to be considered:

- Wi-Fi AP load conditions, including radio and backhaul, and other HS2.0 attributes, such as venue specific information, etc. This enables the device to perform INS decisions as to whether to select a specific Wi-Fi network and whether the Wi-Fi network is suitable to support newly generated IP traffic or traffic already existing over the 3GPP access. The device can use such information to make a decision based on policies from the operators, using specific values such as the load obtained by the network and benchmarked against threshold values in the policies, and device specific algorithms.
- Cellular network congestion condition: this allows the device to perform decisions not based only on the viability of a Wi-Fi network, but also based on the conditions on the 3GPP access to determine the "need" to move traffic to Wi-Fi and when such traffic can indeed be moved back to 3GPP.
- Potential distinction between different 3GPP technologies, e.g. UMTS, LTE, etc. In several situations, the specific technology used by a 3GPP cell impacts the INS decision of whether Wi-Fi or 3GPP should be used. Specifically, if the 3GPP technology available is LTE, the device may be configured to prefer LTE to Wi-Fi, whereas if the available technology is HSPA the device may be configured to prefer Wi-Fi. Using the information available in the mobile device about the cell features and policies that consider such parameters enables the mobile device to perform more intelligent decisions. It has to be noted that the differentiation between 3GPP technologies in the mobile device and ANDSF policies is not meant to influence cell selection and re-selection algorithms, but to apply after regular 3GPP algorithms have performed cell selection.

- ANDSF pre-configuration of preference on NSWO, SaMOG, etc. and what device behaviour corresponds to the flavours mentioned. With the development in 3GPP of new connectivity models over Wi-Fi, e.g., SaMOG connectivity to the EPC over Wi-Fi, awareness of whether a Wi-Fi network provides SaMOG connectivity to the VPLMN and/or the HPLMN becomes an essential input for the device INS decisions. In fact, it is expected that some services will be available only over the walled garden connectivity of an operator, e.g. IMS services. Therefore, SaMOG connectivity for devices using IMS is important. Moreover, some of these services may require connectivity to the HPLMN EPC, e.g. Internet traffic with parental control, whereas other services require connectivity to the VPLMN EPC, e.g. IMS services, since for IMS local breakout connectivity is requested.

3 RECOMMENDED SOLUTIONS & KEY ENABLERS OF INTELLIGENT NETWORK SELECTION

3.1 NETWORK ARCHITECTURE ASPECTS

ANDSF provides a standardized framework for distributing (from the network down to devices) operator-defined policies for network selection and traffic steering. While section 2.2 discussed the current-state-of-the-art of ANDSF and its role as a critical enabler of INS, that section also identified several existing challenges. This section explores several ways an ANDSF-based INS solution could be enhanced, and makes several specific recommendations. In particular, this section explores how to enable a rich, analytics-based ANDSF solution, how to enable the sharing of network information with ANDSF, how to bring available HS2.0 venue type information into ANSDF, and how to leverage System Information Block (SIB) messages to distribute real-time network conditions to devices.

3.1.1 SUPPORTING A RICH ANDSF SOLUTION FOR ACCESS NETWORK SELECTION & ROUTING

Figure 13 below shows how a rich, analytics-based ANDSF solution can be implemented in harmony with fast adaptation for load balancing and in a manner consistent with the architecture currently being considered by 3GPP for Release 12. There are four key components:

1. HotSpot 2.0 compliant access points supply to the UE metrics and information (including enhancements discussed in section 3.1.3) to be used for access decisions.
2. The 3GPP network supplies real-time loading to the UE. Network loading can be supplied from a variety of sources within the 3GPP network (and section 3.1.4 provides a recommendation).
3. The ANDSF server supplies policies to the UE. Included in those policies are thresholds and parameters that the UE can use to assess additional information beyond validity area and time-of-day. That information includes the Hotspot 2.0 metrics and 3GPP loading mentioned above.
4. The UE uses this set of information to select the appropriate Wi-Fi and to perform traffic routing decisions (as described in greater detail in section 3.2).

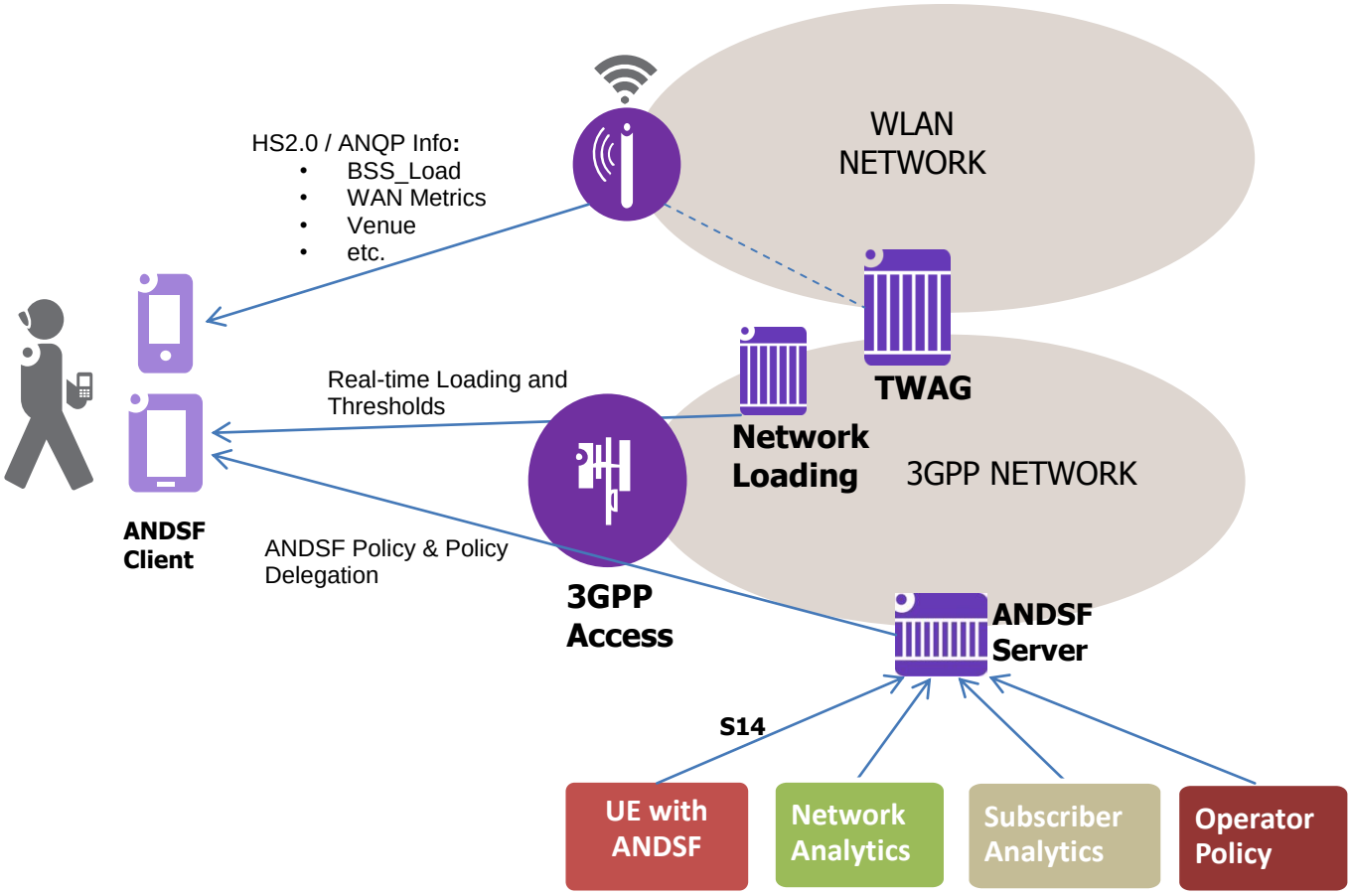

Figure 13. Dynamic ANDSF Policies with Real-time Access Control.

In 3GPP Release 11, the result from considering relevant inputs to the ANDSF Server is a ranked list of access options. This is sent to the UE in the managed object via the S14 interface. The complexity associated with analytics based policy decisions made in the ANDSF server is not visible to the UE. This means that subsequent considerations that affect the access selection must be reflected in the policy rules. Without this, the nuances applied in the ANDSF server to differentiate access selection are lost.

For example, in the case cited in section 2.2.4 where analytics indicates some subscribers have historically been heavy video users and others have complained to customer care about poor experiences on Wi-Fi, the operator may wish to establish the following policies in the ANDSF server:

- Serve all users on 3GPP when real-time cell loading is low
- Push heavy video users to Wi-Fi when real-time cell loading increases while preferentially keeping Wi-Fi-complainers on 3GPP
- Push Wi-Fi complainers to Wi-Fi only if real-time loading gets heavy

With the Release 11 ANDSF managed object, support for this is not possible if the criteria for dealing with the loading information are conveyed to the UE outside of S14. The UE does not have sufficient information to treat the two subscriber types differently.

To solve this problem, policy criteria provided by the ANDSF server must specify how information sent to the UE or available locally (such as battery status) will affect access selection. Fortunately, this is easily

implemented with additional ANDSF policy evaluation in the UE. For example, currently the UE receives Validity Area parameters from the ANDSF server, and then evaluates its current location to determine whether to apply a policy. This model can be extended for other important sources of information such as 3GPP loading, Wi-Fi loading, WAN Metrics, etc. if suitable thresholds and parameters are included in the ANDSF policy.

If broadcast 3GPP loading is one such source of information, as in the example above, then the ANDSF policy could contain a threshold value (3GPP_Load_Max) against which the UE can compare the broadcast 3GPP loading. The ANDSF server can provide different values of 3GPP_Load_Max for our two categories of subscribers (heavy video users vs. Wi-Fi complainers). Hence the mobile operator can achieve the desired policy outcome: moving heavy video users to Wi-Fi before moving the Wi-Fi complainers when congestion starts to increase. Further randomization in the UE may be applied to ensure that large numbers of subscribers that share a common policy are not simultaneously moved to Wi-Fi because of this triggering mechanism.

There are several benefits to this approach:

- The UE has a single source for policy: the ANDSF server. This prevents potential conflicts that arise with the use of HS2.0 Passpoint Release 2 policies.
- Operators have the flexibility to define policies based on a rich set of network and subscriber analytics available to the ANDSF server.
- ANDSF policy update frequency is consistent with OMA-DM capabilities and 3GPP intentions.
- Real-time load balancing based on network conditions is supported.
- It supports roaming and home network UEs.
- The methodology is flexible and expandable to include additional parameters of interest to operators.

More generally, this methodology can be applied for any local UE parameter, HS2.0 obtained information or 3GPP network information conveyed to the UE. Rather than an ANDSF policy that is applicable based only on evaluation of the Validity Area and Time-of-Day, policy could also be valid for specific network congestion levels, HS2.0 Venue-type, HS2.0 Wi-Fi loading (BSS_Load) and other factors included in a policy in a similar manner. To implement this requires only a straight forward expansion of the 3GPP Release 11 ANDSF Managed Object.

3.1.2 ENABLING THE SHARING OF NETWORK INFORMATION WITH ANDSF

Section 2.2.4 described some of the advantages of leveraging analytics based on network information in an ANDSF-based INS solution. And as discussed in that section, in 3GPP Release 11, nothing restricts the ANDSF server from obtaining this type of information for use in policy formulation even though interfaces to network information sources have not been defined. Currently, this may be accomplished in two ways:

1. Via reuse of standardized interfaces on existing network functions and elements, such as Ud on the UDR.
2. Via vendor-specific interfaces to sources of network congestion, subscriber analytics and mobile clients that report analytics to the network.

A well designed ANDSF solution for the creation of policies for mobile devices will take into account a rich set of analytics and other information based on both mechanisms. Vendor-specific interfaces expand the

available sources of information to non-3GPP network elements, and allow for quicker advancement in functionality, particularly when information is provided to the ANDSF server from fast developing areas largely outside the realm of 3GPP (such as analytics). However, standardized interfaces better facilitate inter-vendor interoperability, particularly to other 3GPP network elements.

Thus, this white paper recommends that 3GPP standardize additional network interfaces to the ANDSF server so that additional information can be used in network selection and routing policy (e.g., the Ud interface between ANDSF server and UDR to enhance subscriber-related policy, as illustrated in Figure 14 below).

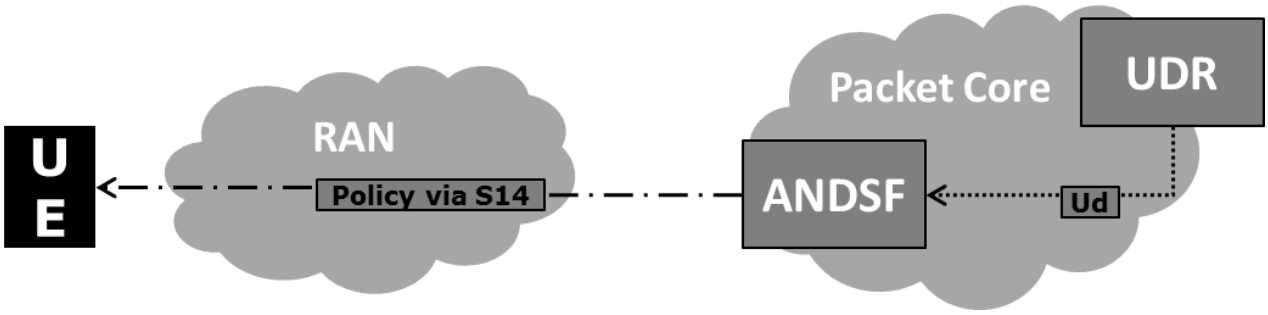

Figure 14. Illustration of an enhanced ANDSF solution that leverages a standardized Ud interface to share subscriber-related information between the UDR and ANDSF server.

3.1.3 BRINGING VENUE INFORMATION TO ANDSF

As discussed in Chapter 2, venue-related information can be an important factor in making intelligent network selection decisions. In the existing solutions described in section 2.2.3, there is no standardized means of factoring venue-related information into ANDSF policy. This section describes how HotSpot 2.0 venue-related information can be added to ANDSF policy to improve network selection decisions[9].

The use of venue-specific information (e.g., HS2.0 Venue Type, which can indicate whether a Wi-Fi AP belongs to a stadium vs. a hospital vs. a train station), enables the operator to define different priorities between different Wi-Fi APs of the same service provider, and define different selection and traffic steering policies for different venue types. If the ANDSF ISMP/ISRP rules are enhanced to include venue related information, then 3GPP operators can prioritize WLAN network selection based on Venue Type and Venue Name. There are many ways this could be useful in practice.

For instance, a 3GPP operator may have different relative priorities of WLAN roaming partners in different types of venues. That is, in a busy venue a certain roaming partner may be preferred, whereas in less busy venue another roaming partner may be preferred. Given this difference in relative preference based on venue, the list of WLAN networks that a UE should attach to would need to be prioritized accordingly. Below are some additional examples of enhanced ISMP/ISRP rules that factor in venue-related information:

[9] Based on joint contribution by Intel, AT&T, Huawei, and Broadcom Corporation for 3GPP SA WG2 Meeting #96 (S2-131168)

1. Prioritization based on SSIDs at different venue names.

   Rule Priority 1: Flow distribution rule for NSWO: Route all traffic based the following prioritized accesses:

   Access Priority 1:
   WLAN, SSID = “roamingPartner1”, Venue_Type=”Stadium”, Venue_Name=”Gymnastics Olympic Stadium”

   Access Priority 2:
   WLAN, SSID = “roamingPartner2”, Venue_Type=”Stadium”, Venue_Name=”Athletics Olympic Stadium”

2. Prioritization based on differences in time of day at the same venue.

   Rule Priority 2: Route all traffic based on the following prioritized accesses at a passenger terminal.

   Access Priority 1:
   WLAN, any SSID, realm = “example1.com”, Venue Type=”Passenger Terminal”, Venue Name=”Heathrow Airport”, TimeStart=”8:00 AM”, TimeStop=”8:00 PM”

   Access Priority 2:
   WLAN, any SSID, realm = “example2.com”, Venue Type=”Passenger Terminal”, Venue Name=”Heathrow Airport”, TimeStart=”8:00 PM”, TimeStop=”8:00 AM”

Furthermore, in addition to Venue Group, Venue Type, and Venue Name, with ANDSF enhancement the operator could specify rules/policies based on the Access Network Type of WLAN network. For example, the public WLAN networks managed by the 3GPP operator may offer better QoS and other services as compared to “free”, “personal” or “private” WLAN networks operating in “Residential” locations. Thus, the Access Network Type field can be used to prioritize operator-preferred WLAN networks over the potentially less desirable access network types.

Finally, as discussed in section 2.2.3, the ISMP/ISRP rules have a number of validity conditions. Currently, the ANDSF server includes at least one of the leaves (i.e. HESSID, SSID or BSSID) to be present in a single instance of WLAN_Location interior node of the ValidityArea of the Policy node. However, if ANDSF is enhanced to include venue-related info, the Validity Area could also be specified in terms of Venue Info and Venue Name for a WLAN network.

It should be noted that since this HS2.0 information is sent unprotected over the radio link, it is important that no access control policies are defined based on this information. As an example, indicating that a hospital AP is less preferred than any other venue type for one device, whereas a hospital AP is the most preferred for a different device, can allow the operator to define meaningful selection policies. However, defining policies that restrict certain devices from accessing an AP advertising a Venue Type “hospital” may lead to denial of service since the value can be spoofed by devices impersonating an AP. Therefore, strict policies that restrict access based on Venue Info should be avoided.

From these examples, it is easy to see the many ways in which including venue-related information could be used to improve network selection decisions. Thus, this white paper recommends the following enhancements be adopted in INS and in 3GPP ANDSF:

- ANDSF MO should be enhanced to allow ISMP/ISRP policy rules based on the Venue Group, Venue Type and Venue Name of WLAN networks.
- ANDSF policy rules should be enhanced to allow selection of preferred WLAN networks based on Venue Group, Venue Type and Venue Name.
- The policy should also include information about Access Network Type to distinguish between the different types of operator managed and other WLAN networks in conjunction with the venue information.
- This venue-related information should not be used in ANDSF policy to restrict access to specific WLAN networks.

With these updated policies from ANDSF, the mobile device would be able to intelligently use Venue Type, Venue Group, Venue Name and Access Network Type information available from the HotSpot 2.0 APs when making network selection decisions.

3.1.4 SIB-BASED DISTRIBUTION OF NETWORK CONDITIONS

As discussed earlier in this section, network conditions can be an important factor in making intelligent network selection decisions. In the existing solutions described in Chapter 2, there is no standardized means of capturing these conditions and distributing them to UE's to influence selection decisions. This section describes how SIB messages can be used to convey the necessary network conditions to a UE, enabling factors such as real-time load and radio conditions to be used as inputs to network selection decisions (as illustrated in Figure 15 below).[10]

[10] Anna Cui, Don Zelmer, Vince Spatafora of AT&T and Cisco, "WLAN/Cellular Intelligent Network Selection" R2-131052, 3GPP TSG-RAN WG2 #81bis, Chicago, Illinois, April 15-19, 2013

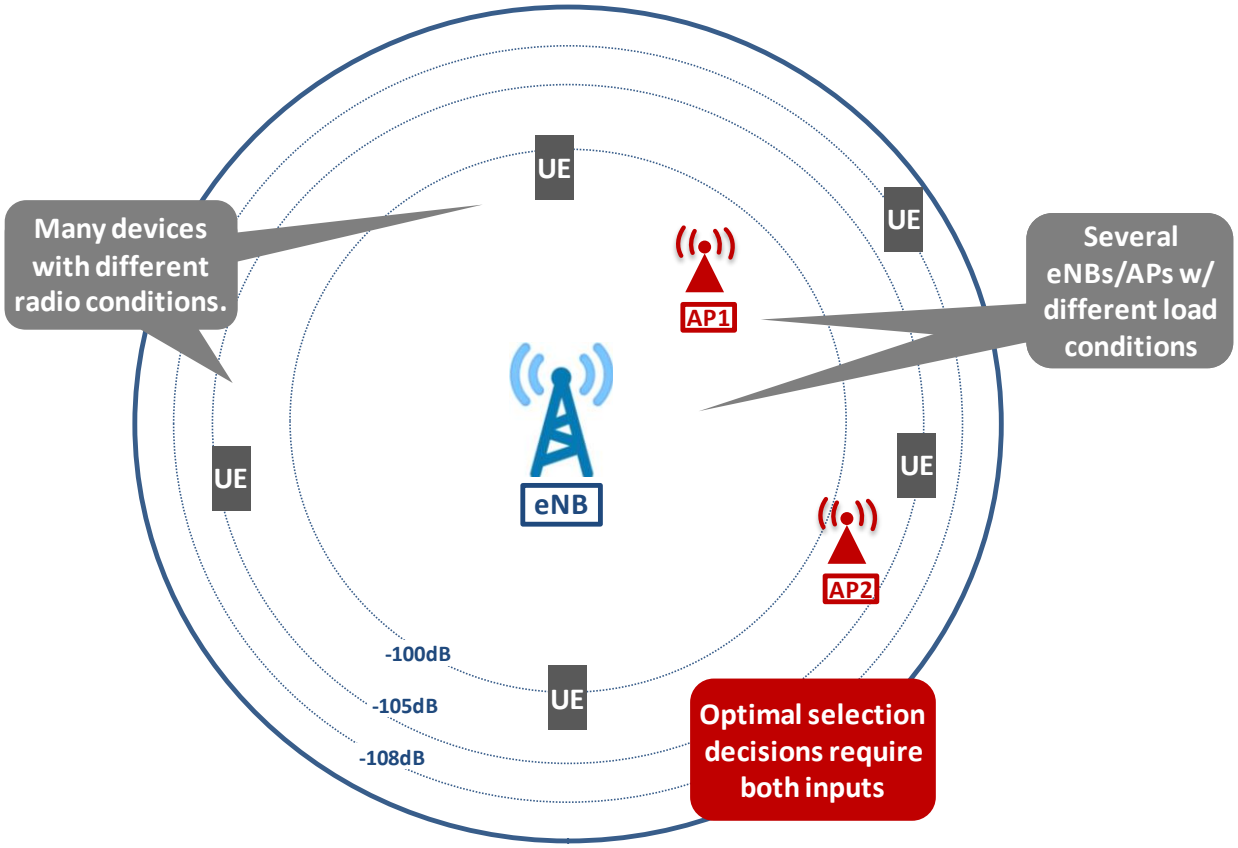

Figure 15. Both real-time network load and radio conditions can be important factors in making optimal network selection decisions.

Given that SIB messages are currently used in LTE to broadcast system information to UE's, SIB messaging is well-suited to distribute the network condition information required to make intelligent network selection decisions. Thus, it is recommended that a new SIB message be defined or that new attributes are added to an existing SIB message that convey the following 3 types of information (which are discussed in greater detail in the next sections):

1. Cellular network load level (for both the LTE and UMTS networks)
2. A signal strength threshold parameter
3. A calculated value used to steer a random subset of UE's

Using this information, UE's can make access network selection and traffic routing decisions based on the combination of operator policy, network load conditions, and RF signal strength conditions. (This is discussed in greater detail in section 3.2.).

3.1.4.1 DISTRIBUTING NETWORK LOAD

Consider a network operator who controls both a cellular (UMTS or LTE) network and a WLAN network in a given area. When the cellular network is not congested (Load = Low), that network operator may prefer to serve their customers via the cellular network. As the load on that cellular network increases (Load = Med) and potentially begins impacting customer experience, that operator may want to start steering some of the user traffic towards the WLAN network. As the cellular network becomes even more

congested (Load = High), that same operator may want to steer even more users towards the WLAN network. (This is depicted in the Figure 16 below.)

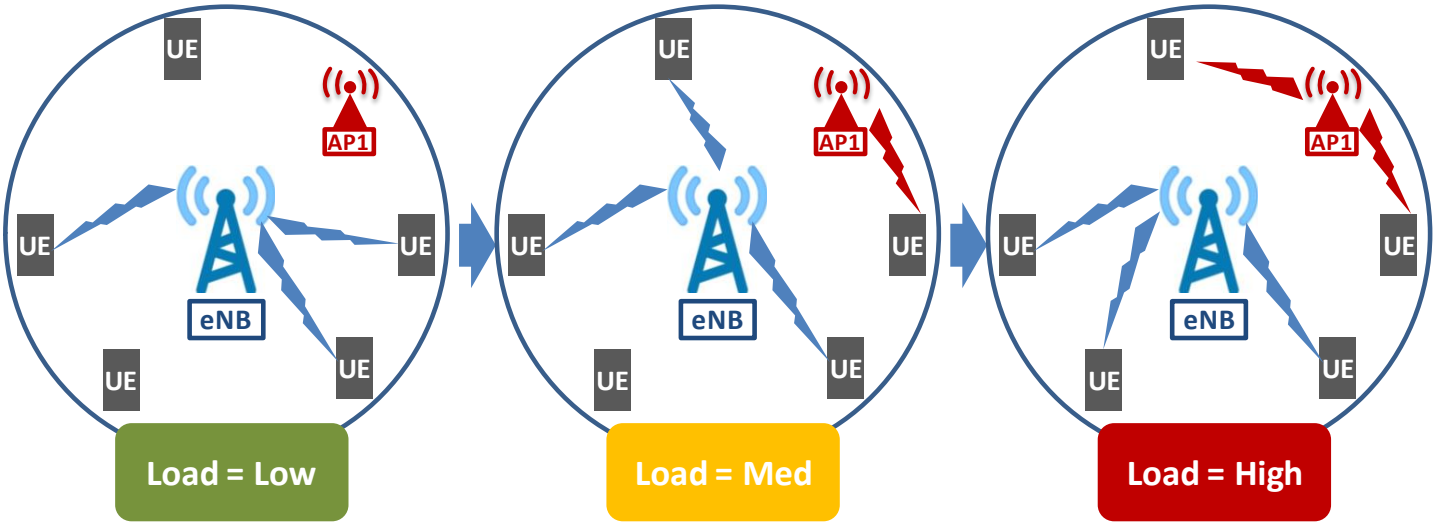

Figure 16. Illustrative example of steering users to WLAN network as load on cellular network increases.

In order to effectively steer users towards the most appropriate access network, SIB messages can be used to convey the real-time load conditions (e.g., Low, Med, High) to UE's in the vicinity. When the UE has access to real-time load conditions, policies can be conveyed to the UE (e.g., via ANDSF as discussed in Chapter 2), that guide a UE's selection decision while factoring in current network conditions.

3.1.4.2 DISTRIBUTING SIGNAL STRENGTH THRESHOLD

In the example above, the operator used cellular network load to steer traffic towards their WLAN network. This practice is even more effective if those users with the worst radio conditions on the cellular network (e.g., poor Reference Signal Receive Power (RSRP) for LTE or RSCP for Universal Mobile Telecommunication System (UMTS)) are steered towards the WLAN network first.

For example, when the cellular network is somewhat congested (Load = Med), the operator who controls both the cellular and WLAN networks may want to steer the devices that have poor cellular RF conditions from cellular to WLAN (assuming WLAN APs are available and are suitable based on various criteria, such as WLAN AP quality/load/signal strength, UE's relative motion, UE's application/service, etc.).

As the cellular network becomes more heavily congested (Load = High), the operator may want to steer more users towards WLAN. Figure 17 below shows that as the cell site becomes congested, the UE's with the worst radio conditions (i.e., the outer red ring) are steered to WLAN first, then UE's with better radio conditions are steered to WLAN after that (i.e., the inner yellow ring).

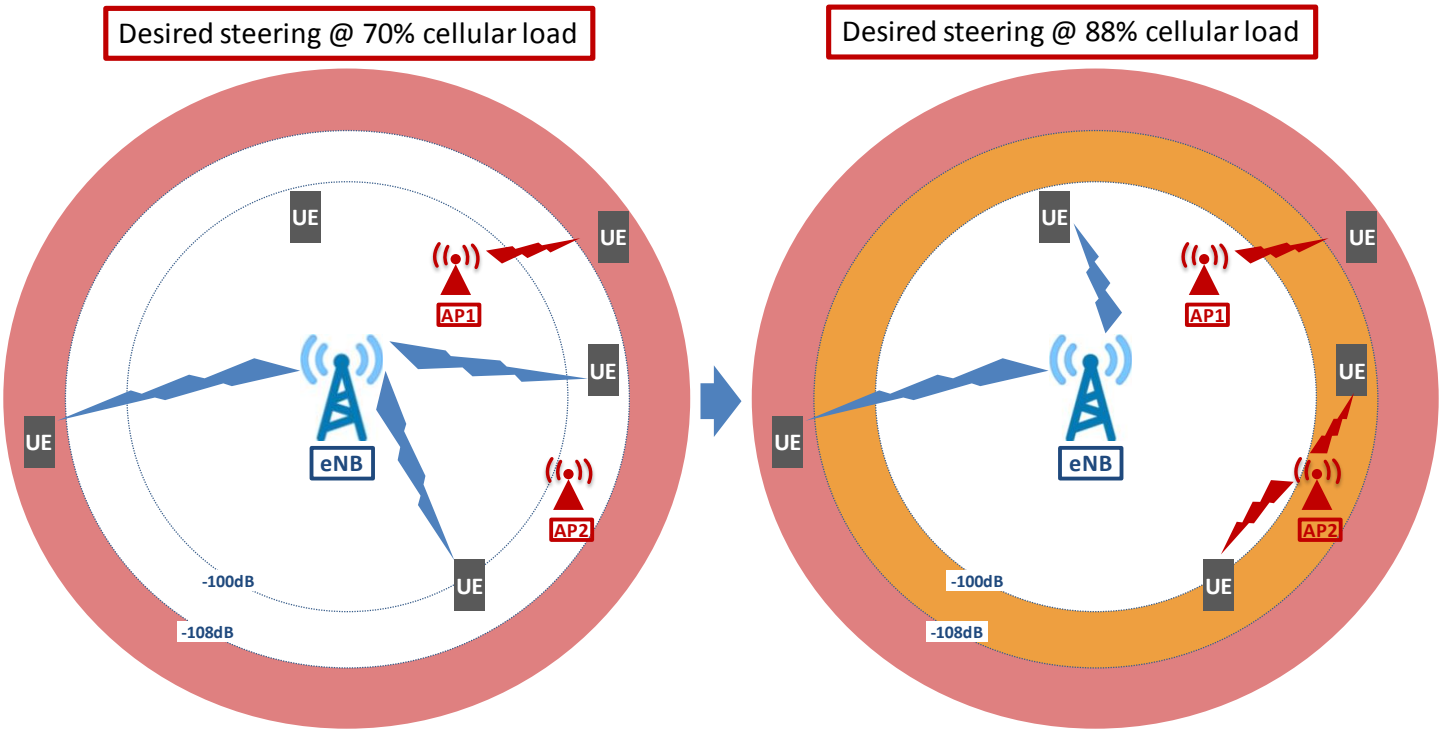

Figure 17. Example illustration of desired steering to WLAN based on cellular load and UE radio conditions.

Even when the cellular network is not congested, some users may experience poor RF quality on the cellular network but have access to a WLAN AP with acceptable quality and load and, in this case, the operator may want to serve that user's traffic via WLAN instead of the cellular network. Additionally, the exact thresholds at which certain users are steered to WLAN vs. cellular depend on the distribution of eNB's and AP's in the network as well as the instantaneous distribution of UE's in the vicinity. Thus, the mapping between load level and signal strength level at which a user is steered to WLAN may not be static.

To ensure that the correct users (i.e., those with poor received signal level) are steered to WLAN while keeping other users' traffic on cellular, a signal strength threshold can be distributed to UE's via a SIB message. For instance, when cellular load is 70%, the signal strength threshold may be -108dBm, but when cellular load is 88% then the signal strength threshold may be -105dBm.

This signal strength threshold indicates a minimum received signal strength, below which UE's should attach to available and acceptable WLAN APs. More specifically, the UE compares their experienced signal strength to the SIB-distributed signal strength threshold, and then makes a network selection decision based on that SIB information plus their operator distributed policy (e.g., via ANDSF). In this way, an operator can first move UEs with poor cellular radio quality to WLAN APs, but in an intelligent way that factors in cellular network load.

Furthermore, the signal strength threshold may be combined with thresholds provided in ANDSF policy so that distinctions made in ANDSF policy are not lost when load balancing using the SIB provided thresholds. In section 3.1.1, a methodology was described whereby, based on analytics, different policies

are provided to different user types. In that example, the operator wished to preferentially steer heavy video users to Wi-Fi while preferentially keeping subscribers that complain about Wi-Fi service on 3GPP. Alternatively, the operator might simply want to introduce different tiers of service. To accomplish either, the ANDSF server can specify separate signal strength thresholds TA1 and TA2 for the two types of subscribers.

The ANDSF policy sent to the Wi-Fi Complainer (or higher service tier) UE would then been be:

- Prefer Wi-Fi if Signal Strength < TA1 + TB

And for the heavy video or lower service tier user:

- Prefer Wi-Fi if Signal Strength < TA2 + TB

Where TA1 < TA2, and TB is the threshold sent via cell broadcast.

This methodology allows for both dynamic load control via changes in the broadcast threshold TB, and analytics based subscriber differentiation using the relatively static TA1 and TA2 thresholds.

3.1.4.3 DISTRIBUTING A CALCULATED VALUE

When steering large numbers of UE's between cellular and WLAN AP's, it is possible to dramatically affect the instantaneous network conditions. For instance, if a large number of users are steered towards WLAN (e.g., due to high cellular network load), the load on the cellular network would be dramatically reduced. This reduction in load could cause those same UE's to try and re-select the cellular network as it is now a much more desirable access network than it was before. As all the users move back to the cellular network, the load increases and causes users to be steered back towards WLAN. Thus, there is a ping-pong effect of UE's bouncing between the cellular and WLAN networks as long as this process continues.

To avoid this ping-pong effect, a calculated integer can be sent in the SIB message along with the load level and signal strength threshold. This calculated integer is used to steer a subset of targeted UE's at a time, instead of all targeted UE's at once. It works as follows: There is a calculated integer "A" (e.g., in the range of 0-10) that is distributed in the SIB. Furthermore, each UE generates a random number *x*, which is also in the range of 0-10. If x<A (and the other conditions are met), then a given UE is steered towards the WLAN AP. Otherwise, the UE stays on the cellular network.

In this way, a given fraction of the targeted population is steered towards WLAN at any given time. This fraction is tunable by the network operator (based on the calculated value distributed). Additionally, more than one calculated value can be distributed, with each value targeted at a specific class of users with similar service characteristics (for those cases where the operator wants to steer different types of users in different ways).

3.2 DEVICE ASPECTS

Section 2.3.4 identified the key gaps of network selection and traffic steering. In this section, we focus on the enhancements and recommendations especially on the key device functional components which enable intelligent network selection and traffic steering. Further, various INS models are described and examples are used to illustrate how an INS device performs intelligent network selection and traffic routing based on the combination of operator policy, network condition and UE intelligence.

3.2.1 HIGH LEVEL ARCHITECTURE AND KEY FUNCTIONAL COMPONENTS

This section describes the device high-level architecture and key functional components.

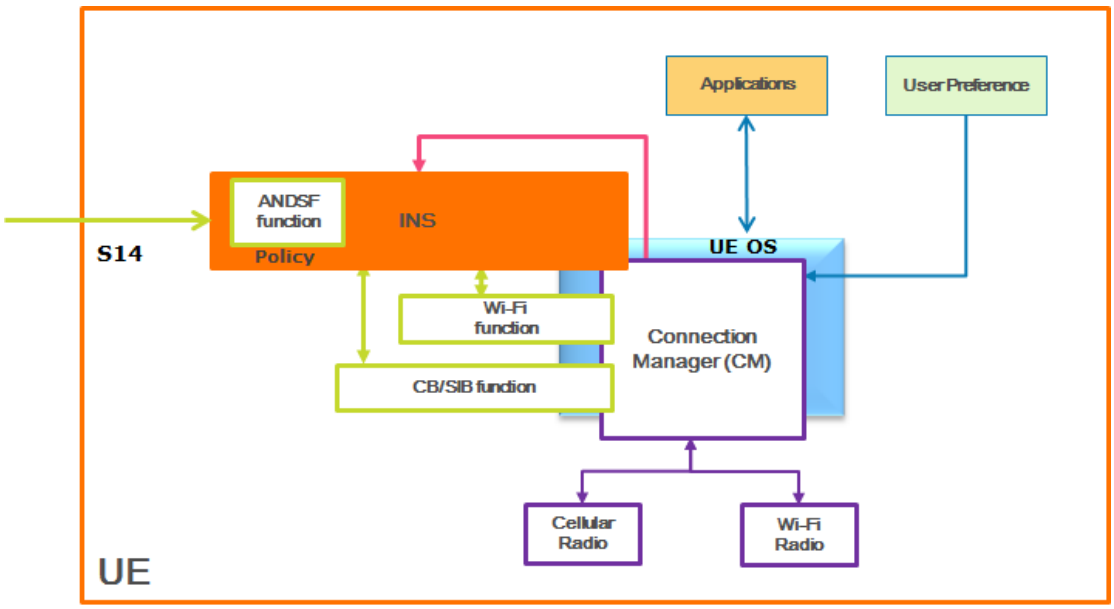

Figure 18. Device High-Level Architecture.

Figure 18 depicts a high level functional view of Intelligent Network Selection (INS) on the UE that enables service provider policy driven dynamic intelligent network selection of the best radio technology (incl. cellular and Wi-Fi) for user traffic delivery on a per application basis.

The intelligent network selection is based on operator policy, application/IP-flow, user subscription profile, radio network conditions, device intelligence (e.g., local operational environment such as mobility state, battery usage, data usage, etc.) to provide consistent optimal user experience across customers and improve network efficiency.

The key functional components of the architecture (that can be implemented in the client or OS/CM as described in section 3.2.3) include:

- **INS Function for network selection and traffic steering**– a service provider policy driven intelligent network selection (INS) function. It performs the following functions:

  1. Make INS decision regarding which radio needs to be used under a specific set of conditions, what Wi-Fi network the device should connect to when Wi-Fi is selected, and what traffic

should be steered over Wi-Fi vs. cellular. The following network and device inputs are considered:

a. Service provider ANDSF policy via S14 interface. The ANDSF policy includes the 3GPP ANDSF existing capabilities, such as access network discovery information (ANDI), Inter System Mobility Policy (ISMP), Inter System Routing Policy (ISRP) and any enhancements needed to enable network condition and UE intelligence based policies. Note, in addition to ANDI, ISMP, and ISRP, standard S14 also supports the security features such as Generic Bootstrap Architecture (GBA) for device and server mutual authentication as defined in 3GPP specification.
b. Cellular network congestion condition and parameters via Cell Broadcast (CB) / System Information Block (SIB) function (defined below).
c. Wi-Fi network congestion condition via Wi-Fi function (defined below).
d. Mobile device intelligence (defined below).

2. Provide input to Connection Manager (CM) (defined below) on how to route user traffic to the proper radio (e.g. Wi-Fi or cellular) on a per application basis.

- **CB/SIB** function - Cellular Network condition function on the device. It performs the following function (as discussed in section 3.1.4):
  - Receives/extracts the following dynamic cellular network conditions and parameters from the cellular network via CB or SIB using a new message or new attributes on an existing message**:**
    a. load information in the format of load flag (e.g. Red, Yellow, Green, etc.),
    b. signal strength thresholds, e.g. RSRP/RSCP, RSSI, etc., and
    c. percentage, that can be used to move portion of the users between cellular and Wi-Fi networks.
- **Wi-Fi** function – Wi-Fi network condition function on the device that receives/extracts Wi-Fi AP conditions such as BSS load condition, RSSI, and WAN metrics via HotSpot2.0. In addition, performance measurement over the Wi-Fi network including RTT delay, jitter, packet loss, etc. might also be used for leaving WLAN or for future session reference.
- **UE intelligence** function– UE local intelligence, including battery usage, UE mobility state, e.g., motion relative to the Wi-Fi AP (speed, vibration patterns, etc.), data usage, etc.

CM function- the CM is a generic term in this document. It refers to a functional component that takes as input user preference, input from INS function, performs connectivity management and the traffic steering, i.e., binding user application/flow to a radio. It is expected the device has one CM function.

3.2.2 FUNCTIONALITY OF AN INS MOBILE DEVICE

Mobile devices destined for 3GPP cellular networks and Wi-Fi interworking are expected to implement a set of key functions in order to optimize the steering of traffic between 3GPP and Wi-Fi and to select the appropriate Wi-Fi network under the appropriate conditions. In order to achieve this goal, a functionality called Intelligent Network Selection (INS) is expected to be implemented in the device. This section describes the INS functionality and the technologies it uses.

The target for INS is to enable the mobile device to select a Wi-Fi and/or cellular network for its service delivery, based on subscriber preferences, network operator policies, and network/device conditions. Specifically, INS enables both WLAN network selection (i.e., which Wi-Fi the device should connect to) and traffic steering (i.e., whether cellular radio or Wi-Fi should be used) decisions.

One of the key assumptions regarding the INS functionality is that it leverages a set of existing technologies, including the existing ANDSF Standard as specified in 3GPP TS 24.302 and TS 24.312 documents, the IEEE 802.11u standards and/or its Wi-Fi certified version known as Hotspot2.0/Passpoint. In addition, it is expected that INS will leverage the technical solutions being developed in 3GPP for release 12 WLAN network selection, and necessary enhancements of ANDSF and HS2.0 that allows intelligent network selection and traffic steering which takes into account network and device intelligence.

The following sections describe the INS functionality in greater detail.

3.2.2.1 INS GENERAL DEVICE REQUIREMENTS

Mobile devices are expected to implement an INS platform to allow network selection and traffic routing decisions between various Wi-Fi and operator cellular networks and that can be applied to multiple OSs and devices. Moreover, INS is expected to be expandable to meet future operator needs, mobile device capabilities and network features.

The INS functionality in the mobile device allows:

- WLAN network selection based on user preferences as well as operator policies and network requirements.
- Traffic steering, by influencing the routing of IP traffic flows to Wi-Fi or cellular networks. The routing decisions in the mobile device are expected to be performed based on a variety of inputs, including operator-defined policies, user preferences, real-time conditions (e.g. specific applications running in the device and with pending data, RAN and transport conditions such as load and RF condition), and the local operating environment, such as user mobility state, etc. INS supports the ANDSF policy framework in order to meet network selection and traffic steering requirements defined by operators.

3.2.2.2 ANDSF POLICIES AND ENHANCEMENTS

An INS capable mobile device receives operator ANDSF policies from a network-based ANDSF server by means of an ANDSF client, according to the mechanisms defined in 3GPP for ANDSF. Such device applies the operator ANDSF policies according to the ANDSF functionality defined in 3GPP standards at least up to Release 11.

The INS mobile device implements an ANDSF client based on the latest 3GPP specification TS 24.302 and TS 24.312.

The mobile device uses the S14 interface to the network for policy delivery, and implements both policy pull and push modes for communication with the ANDSF server. The mobile device can initiate the policy pull from the ANDSF server over any access (e.g. 3G, 4G Network or when connected on a WLAN), but it is expected that the policy push can happen only over a cellular access, as defined in current ANDSF specifications.

When using the pull model to retrieve policies from the ANDSF server, the device can use different triggers to initiate the retrieval and can be configured according to operator requirements to consider one or more of the following triggers:

- At power up after location update and network registering;

- At Location Area or Traffic Area (LAC/TAC) update;
- At expiration of a dedicated S14 trigger timer;
- At expiration of a previously received policy;
- Other triggers are for further study.

When initiating the push of new policies to the device, the network considers as triggers at least changes to the user subscription and changes to ANDSF policies.

It is expected that the ANDSF policy will be transferred between the UE and the ANDSF server using OMA DM as defined in OMA-ERELD-DM-V1_2 and 3GPP TS 24.302 with the management objects as specified in 3GPP TS 24.312. The push model supported by the device for S14 is in accordance with the latest version of OMA-ERELD-DM-V1_2 [8] and 3GPP TS 24.302 using WAP Push.

ANDSF can deliver both ISMP and ISRP policies to the mobile device. Depending on the device capabilities, the device uses ISMP or ISRP as defined in 3GPP TS 24.302. As an example, for dual mode devices capable of simultaneous connectivity to the cellular and Wi-Fi networks, if ISRP policy is received from ANDSF server, then the device uses ISRP for network selection policy.

In terms of how the device differentiates application traffic, the device supports the application formats (e.g. IP traffic descriptor in terms of source and destination addresses and port numbers, etc.; application identifier; , etc.) specified in 3GPP TS 24.312 for all traffic routing decisions (e.g. including IFOM and NSWO). It is also expected MAPCON capabilities will be supported in the future.

The mobile device implementing INS needs to support additional enhancements to provide an extensible and configurable platform that allows intelligent network selection and traffic steering based on a variety of parameters, including but not restricted to the type of application that requires data to be transmitted (in order to differentiate per multiple applications), operator policies, cellular network conditions, Wi-Fi AP conditions as defined in HS2.0 mechanisms, the available quality of the Wi-Fi connection (referred to as Quality of Experience - QoE, typically defined in terms of a set of parameters including packet loss, RTT, and throughput), applicable cellular, local operational environment and device intelligence.

For WLAN network selection, the device uses the following parameters as input to the selection algorithm:

- User subscription profile
- Cellular network load (e.g. cellular condition)
- Wi-Fi conditions (e.g. BSS/WAN load) based on information that the device can obtain through HS2.0, and Wi-Fi RSSI (RCPI)
- Time of Day (ToD)
- Device location

For traffic steering decisions, the device uses additional parameters including:

- Application type for the applications generating data traffic
- Cellular network load
- RSRP/RSCP threshold
- Overall quality of the Wi-Fi connectivity, defined in terms of Wi-Fi load, radio conditions, and backhaul conditions (either provided to the mobile device by the network or calculated/estimated by the mobile device)

In general, the mobile device uses other parameters when performing network selection and traffic steering, such as:

- Motion of the mobile device relative to one or more APs (e.g., mobile device speed with respect to one or more Wi-Fi APs, that can be calculated in the device based on a variety of mechanisms, e.g., can be extrapolated via AP rate of changing signal strength as measured by the UE), estimated by the device according to implementation dependent mechanisms
- Power conditions in the mobile device (e.g., battery usage)
- Application specific requirements (e.g., encryption, service continuity, etc.)

Mobile devices supporting INS are expected to function both in deployments where the Wi-Fi access points are HS2.0 capable and in older deployments where access points have not been upgraded to HS2.0. When HS2.0 information is not available (e.g., the AP the device is currently connected to is not HS2.0 compliant), the device estimates the Wi-Fi AP quality of experience using implementation specific means (e.g., using RTT delay, packet loss, throughput, etc.). It is expected that the device is capable of using the estimated Wi-Fi network quality of the connection with the current AP to trigger the reselection to a different Wi-Fi network if the quality is below a threshold defined by the ANDSF policies, user preferences and implementation dependent values in the device.

In scenarios where the AP is not HS2.0 compliant, the device may be capable of storing the QoE estimate related to such AP. The device may then use such stored estimate at a later time, together with real-time information such as the radio conditions, to perform network selection decision regarding this specific AP.

Once the mobile device has selected the target access to be used (e.g., a specific WLAN network), INS influences the traffic routing over the selected access for traffic corresponding to the policies, e.g., on a per-application or a per-APN basis.

The INS mobile device leverages HS2.0 functionality and integrate ANDSF solutions with HS2.0 solutions. Specifically, ANDSF policies defined by the operator will contain relevant HS2.0 policies defined by HS2.0 and whose corresponding values can be obtained by the device from an HS2.0 compliant AP. Network selection decisions based on ANDSF policies will use the HS2.0 policies embedded in ANDSF policies.

Enhanced ANDSF Policies and MOs

In order to support INS functionality, a set of enhancements is being designed in 3GPP release 12 work related to HS2.0 and, further, this white paper recommends the following enhancements to the ANDSF policies and ANDSF Management Objects.

- Cellular network parameters, including cellular network load conditions and cellular signal strength threshold. Note, the dynamic real-time or near real-time values of the load and cellular signal strength threshold will directly come from cellular access network.
- User subscription class offset (e.g. silver user offset = 2 dB, gold user offset =1dB, and Platinum user offset = 0dB).
- Wi-Fi specific parameters, such as Wi-Fi signal strength threshold (e.g. RSSI) and information related to HS2.0 capable APs (e.g. network discovery and selection capabilities and MOs, e.g., Wi-Fi BSS and WAN load thresholds), along other HS2.0 related information, such as Venue related information as described in section 3.1.

- Other device-related attributes such as motion of UE relative to AP (e.g. device speed), device battery usage information, device data usage.

In addition, to address the limitation of Wi-Fi access network selection identified in section 2.3.4, and maximize the flexibility of Wi-Fi selection, this white paper recommends ANDSF enhancement of Wi-Fi network selection to allow for selection of Wi-Fi networks that belong to the registered PLMN as well as Wi-Fi access network that not belong to the registered PLMN.

3.2.2.3 WI-FI DEVICE REQUIREMENTS

A mobile device supporting interworking between cellular and Wi-Fi, implementing INS and capable of leveraging carrier-deployed Wi-Fi networks implements a variety of technical solutions defined by IEEE 802.11.

An ideal INS mobile device will be WFA HS2.0 Passpoint certified. Regarding the use of HS2.0, this paper assumes the support of the HS2.0 architecture for the Wi-Fi AP. In HS2.0, the AP can implement one of two models with respect to how ANQP information can be obtained. In a first model, the AP is configured with or can derive the information required to respond to ANQP queries available from mobile devices. In a second model, the AP relies on an ANQP server in the network and relays the ANQP queries from the mobile devices to such server. In this paper, we do not promote any specific AP model, with the expectations that the AP model has no impact on the mobile device, and that both models can be deployed in the market in different networks.

The INS mobile device also supports and is certified for IEEE 802.11e – EDCA, as certified by WFA Wi-Fi Multimedia (WMM®). The support of 802.11e enables the broadcasting and use of load information in the beacons.

In terms of wireless network measurement capabilities and wireless network management, the INS device supports the set of functionality defined in IEEE 802.11k (e.g. radio measurements and neighbor reports) and 802.11v required for WFA Voice Enterprise certification. WFA is also starting the Network Power Save certification, and the INS mobile device supports the features defined in such certification program.

Among the technical features defined by IEEE 802.11v (Wireless Network Management), the Multiple BSSID capability is considered future enhancement for the INS mobile device since it enables the advertisement of information for BSSIDs using a single Beacon or Probe Response frame, instead of multiple Beacon and Probe Response frames, each corresponding to a single BSSID. The Multiple BSSID capability also enables the indication of buffered frames for multiple BSSIDs using a single TIM element in a single beacon. However, at present no WFA certification program includes such capability, and therefore INS mobile devices cannot be certified for such feature.

3.2.2.4 CELLULAR RADIO NETWORK CONDITIONS

An INS mobile device will leverage information related to the cellular network, e.g., as described in section 3.1.3, in order to perform intelligent decisions regarding when to steer traffic between cellular and Wi-Fi. The device is expected to receive cellular network condition information, including RSCP/RSRP thresholds and cellular network load conditions, from the RAN via cell broadcast /SIB messages.

3.2.2.5 UE INTELLIGENCE

A relative amount of intelligence is expected to be implemented in an INS mobile device, specifically regarding device real-time conditions that influence the network selection and traffic routing decisions for INS. This applies specifically to some of the conditions that in current 3GPP standards are referred to as Local Operational Environment.

Conditions that the device uses for INS decisions include the detection of its motion relative to the AP and information about the device battery usage.

In addition, the INS device performs estimation of the quality of connectivity with a specific Wi-Fi network based on parameters specific to the traffic that is being transmitted, including the requirement of applications for the quality of the connections, e.g., in terms of RTT and packet loss.

Optionally, an INS mobile device may estimate data usage information in terms of the volume of data that the device has transmitted over the cellular interface, e.g., in order to make network selection and traffic routing decisions based on the amount of data already used with respect to the data subscription budget associated to the device subscription.

3.2.3 INS MODELS

Two types of solutions can be considered – a client-based solution and a clientless solution.

CLIENT-BASED SOLUTION:

Client-based solutions are characterized by a preloaded or downloaded client which the subscriber must activate/install and generally register (for client updates and to establish a control link to some network entity if needed). Examples of existing client-based solutions are AT&T Smart WiFi, Netwise SmartSpot, Airplug and Airsense. Client-based solutions can have the benefit of fast deployment and greater flexibility (by allowing for regular updates). Client-based solutions in theory can provide consistent user experience across all OSs/OEMs if the client has access to the same APIs and information across all platforms. Further, the client can be implemented by a 3rd party, thus eliminating the need for OS vendor intervention. Client-based solutions also must address distribution challenges (how to get users to download, install and activate).

In the case of client-based solution, INS is a function distributed between an INS client running in the device and connectivity management in the OS/CM. The INS functionality spreads across the application layer and lower layer with functional split between INS client and lower layer that can vary. In this model, the availability of relevant information about network and mobile device to the INS client is essential. In addition to operator policy (ANDSF-based), the following information needs to be available to INS functionality:

- Wi-Fi conditions can be used by the INS functionality and should be provided by the Wi-Fi function element. Such condition information can be provided by the network via HS2.0, or inferred by the UE (based on performance measurements, e.g. RTT, throughput, etc.) in case HS2.0 is not supported. For the support of legacy APs that cannot be upgraded to support HS2.0 capabilities such information can be inferred by the UE in an implementation specific manner.
- Cellular network conditions can be used by the INS functionality and should be provided by the CB/SIB function element to provide cellular load information and RSRP threshold conditions.

Such information can be provided by the network for instance via SIB or cell broadcast messages.

- The INS functionality can use conditions of the mobile device, such as mobility state, battery usage, etc., and need to be available to the INS functionality.

Based on such information, the INS decision influences the CM to route IP flows to the proper radio. Specifically, a set of APIs is expected to exist between the INS client component and the OS/CM.

The INS function uses as input operator policies, that are downloaded into the device in the ANDSF function, user preferences and operator configuration information provided by the client. Operator policy and user preference information is used by the client to control performance, e.g. battery life, mobility state, provide radio or throughput thresholds to the INS function, thus determining –- the performance and aggressiveness of Wi-Fi selection and traffic steering.

Client-based solutions can be divided into a full-client solution and a lightweight-client solution (where OS/CM provides the necessary capabilities and INS functionality, with a separate lightweight client downloaded in the device to implement the ANDSF functionality and to provide policies, configuration, and input to the INS function).

In the case of full-client solution, all this information is exchanged via a set of APIs to gather network and device conditions and enable operator intelligent network selection decisions to be communicated to CM. In order to optimize overall INS functionality and reduce power consumption, it might be possible to use CM to process such radio RF specific information especially for Wi-Fi, and only trigger the APIs when certain threshold conditions are met.

In the case of a lightweight-client solution some of the communication will happen within the lower layer entities, therefore the APIs can be simplified. In this case, the APIs are related to specific configuration and thresholds, so that the application layer client can still have control on the overall performance of the device by setting thresholds on different parameters but the actual execution of the policy is done at the OS or lower layers. The INS function provides to the lightweight client notifications and information regarding the selected networks as a result of the information provided.

When considering the design of APIs in the mobile device, in order to develop the client-based INS solution there are some important considerations. In general, some of the relevant network condition information would be platform-dependent by nature. For example, some APIs that provide raw data such as RSSI values to the application layer can be very chatty and therefore power hungry. Thus keeping such information available and consumed only in the CM can improve the overall INS functionality.

In general, the set of APIs defined between the two levels needs to be:

- flexible/customizable to allow operators to customize the mobile device behavior,
- hardware independent to enable the same solution to be adopted in a variety of platforms,
- efficient to limit power consumption (e.g. avoid chatty APIs), and
- able to allow for mobile device and platform differentiation.
-

To address the gap identified in section 2.3.4 regarding the inconsistency of network selection and traffic steering behaviours, it is recommended to standardize a set of APIs to exchange the necessary information needed for INS decision as well as to facilitate the communication between INS client and different OSs/CMs.

CLIENTLESS SOLUTION:

Clientless solutions are ones where the native OS (or specific software modules integrated and embedded within the OS) or the platform provide all the necessary capabilities and functionality without the need for a separate downloaded client and without the need for user intervention to download, install and activate the application. While clientless solutions do exist today (e.g. access selection between 3G and LTE is done natively in the platform today), standards based clientless solutions that allow the operator to communicate policies and control directives to the device connection manager for improved Wi-Fi/cellular interworking do not exist currently. Clientless solutions have the benefit of more ubiquitous deployment (since user cannot de-install or control instantiation of the capability) with less operator management overhead. At the same time, clientless solutions that take operator requirements into consideration have a stronger dependency on OS/CM.

3.2.4 PUTTING THINGS TOGETHER

This section uses examples to illustrate how an INS device performs intelligent network selection and traffic routing based on the combination of operator policy, network condition and UE intelligence.

Example 1: INS decisions based on cellular network condition

This example presents intelligent network selection and traffic steering when the cellular network is congested. When cellular is becoming congested, operators might want to orderly steer of some of user's traffic to WLAN based on policies downloaded as priority in the mobile device. That is, cell edge users will not only suffer more from quality experience perspective, but they also consume more radio resources than the users closer to the center of a cell even though the same throughput is achieved. So, cell edge users will be moved to Wi-Fi first, if available. In addition, operators might want to keep the traffic related to certain applications, e.g., voice, on the cellular radio regardless of load conditions. This example demonstrates how ANDSF can help cell edge users to select a WLAN and how ISRP can be used to steer certain traffic to WLAN vs. cellular.

Mobile device (A) behavior:

1. Mobile device (A) receives ISRP policies from ANDSF server for traffic steering:
    - Streaming Video application identified by app id
        - access network preference: {Operator_A_Premium_wifi(1), public wifi(2), 3GPP network (3)}
            - Conditions:
                - cellular network load is high, and
                - Wi-Fi RSSI is >-85dbm, and
                - BSS threshold, and
                - WAN Metrics threshold, and
                - RSRP<threshold (the actual value will be provided by RAN);
        - Default access network {cellular}

2. Mobile device (A) also receives the following dynamic cellular network conditions, obtained from cellular network via Cell broadcast or SIB messages from RAN:
    - RSRP threshold value, e.g., RSRP threshold = -108dbm (note, this threshold is adaptive to network condition and other conditions such as, device and Wi-Fi AP distribution)
    - Cellular Load-flag, e.g. load flag=high

Note: (load flag) is also received via SIB/CB message whenever there is threshold change (L->H, SST changes, etc.)

3. Mobile device (A) measures its cellular RF conditions:
    - RSRP = -107dBm

4. Mobile device (A) receives real-time Wi-Fi load conditions and measures its Wi-Fi RF condition:
    - prior to association, during the network selection process the mobile device receives
        - RF condition, e.g., RSSI =-70dBm via Wi-Fi scan
        - Wi-Fi AP condition, e.g., BSS, WAN condition, etc. via HS2.0 [*for simplicity, this is not detailed here]
    - once network selection has been performed, for traffic steering the mobile device performs performance measurement, e.g. RTT, packet loss, etc. [*for simplicity, this is not detailed here]

5. Mobile device (A) then performs the following INS decision logic:
    - Uses the policies from ANDSF
    - Device compares its received Wi-Fi condition from Wi-Fi AP against the threshold set in the ANDSF policy:
        - -70 >-85dBm (UE meets the condition to use Wi-Fi)
    - Device compares its received cellular load condition from RAN (load = high) against the policy condition (device meets the candidate condition to look for Wi-Fi)
    - Follows the policies from ANDSF (with Extended MO RSRP), device compares its measured RSRP level against the received cellular RSRP threshold from RAN:
        - RSRP (-107dBm>-108dBm) (UE RSRP<RSRP threshold condition is not met, Streaming Video application will not use Wi-Fi)
    - INS traffic steering decision:
        - All device A's applications use cellular
    - Device A routes all its traffic per INS decision as well as user preference.

Example 2: Mobile Device Mobility State based INS

In this example, we assume user C is moving at high speed relative to a potential target Wi-Fi AP. ANDSF policy suggests only low speed mobile devices can be considered as candidates with respect to when the mobile device should attempt association with WLAN APs.

1. UE receives policies from ANDSF server:
    - For simplicity and ease of discussion, assume user C receives the same ISMP policy from ANDSF server with additional MO on {max mobility state = low speed}
2. Same as A
3. Same as A
4. Same as A
5. UE detects its motion of UE relative to AP (high speed).

6. UE INS decision for user C:
    - Uses the policies from ANDSF
    - Device compares its received Wi-Fi condition from Wi-Fi AP against the threshold set in the ANDSF policy:
        - -70 >-85dBm (UE meets the condition to use Wi-Fi)

- UE detects its motion relative to AP and compares it against the threshold set by ANDSF policy:
    - high speed > low speed (via configuration), i.e., condition of using Wi-Fi is not met.
- INS decision for network selection with respect to whether to attempt association with a specific Wi-Fi AP:
    - All device C's applications use cellular and the device does not connect to Wi-Fi AP.

Device C routes all its traffic per INS decision as well as user preference.

4 CONCLUSIONS

Wi-Fi has become an increasingly critical tool for wireless carriers to meet the capacity demands of their mobile data users. The amount of traffic carried over Wi-Fi networks has grown dramatically in recent years, and is projected to continue to grow in the years to come. This has been driven by multiple factors. Most mobile devices sold today have multiple network interfaces, and often include both Wi-Fi and cellular radios. There's been increasing user demand for ubiquitous mobile data services – and Wi-Fi is uniquely positioned to serve these users given its harmonized global spectrum allocation and widely adopted technology standard. Lastly, with smartphone adoption continuing to rise and the increasing prevalence of bandwidth-intensive services such as streaming video, the limited licensed spectrum resources of existing cellular networks are as constrained as ever. Wi-Fi, and its associated unlicensed spectrum, presents an attractive option for mobile operators – but improved Wi-Fi/cellular network interworking is needed for carriers to make optimal use of Wi-Fi.

Thus, this paper explores the current state-of-the-art of Wi-Fi/Cellular integration, and makes specific recommendations to enhance a key component of Wi-Fi/Cellular integration: Wi-Fi network selection and traffic steering, which this paper refers to as Intelligent Network Selection (INS).

The Current State-of-the-Art

One of the important aspects of Wi-Fi/cellular interworking is the seamless service continuity when users move between Wi-Fi and Cellular networks. Several options are possible today: service layer session continuity, client-based mobility mechanisms and network-based mobility mechanisms. In particular, this paper discusses a network-based mobility mechanism (SaMOG) that has been standardized in 3GPP to support tight integration of Trusted Wi-Fi networks with 3GPP cellular networks – such a tightly integrated model has been recognized by recent GSMA/WBA work as the direction the industry is headed. By leveraging recently defined TWAG & TWAP functions, carriers can enable subscribers to move between LTE and Trusted Wi-Fi networks while preserving their IP address and allowing access to Operator Services (e.g., IMS) over Wi-Fi. And, further building on that SaMOG model, this paper explores how to enable real-time services and end-to-end QoS over an integrated Trusted Wi-Fi network.

In addition to recent 3GPP standards work to enable mobility between Wi-Fi and Cellular, there has been considerable work in the IEEE and WFA to enhance Wi-Fi network security and discovery/selection. Much of this work has been done under the umbrella of HotSpot 2.0. To provide security that is on par with cellular networks, there's been a drive to enable seamless authentication via EAP-AKA/AKA' (which leverages USIM credentials present on a mobile device) and airlink encryption via WPA2-Enterprise. To enhance network discovery and selection, IEEE 802.11u provides mechanisms to distribute additional information about an AP to devices without the need for a device to associate to that AP. For instance, AP's can broadcast info such as real-time load using its beacon, or enable queries using ANQP to allow unassociated devices to learn about the APs backhaul capabilities, roaming affiliations and more.

Of particular importance in making optimal use of Wi-Fi networks is INS. Today, Access Network Discovery and Selection Function (ANDSF) is a key enabler of INS. The 3GPP-defined ANDSF provides a framework for carriers to distribute operator-defined policies to devices in order to guide network selection and traffic routing decisions between Wi-Fi and cellular networks (although user preference will always take precedence over operator-defined policy). Using ANDSF for Wi-Fi network selection and managing traffic across networks can contribute to a better network performance and lead to improved user experience

The Challenges Identified and Recommended Solutions

While ANDSF provides a robust, standardized framework, this paper identified a number of challenges associated with current ANDSF-based solutions. These gaps need to be addressed in order to fulfill market needs. For instance, HS2.0 provides information about Wi-Fi networks (e.g., AP Load, backhaul metrics, Venue Info) but HS2.0 info is not integrated into ANDSF. A set of information is currently not considered in ANDSF policies and therefore cannot be used in conjunction with ANDSF policies defined by the operator. Examples include cellular network conditions (e.g., real-time load), information such as subscriber profiles, and intelligence available locally in the device, e.g. how fast device is moving in relevance to Wi-Fi AP(s). Lastly, existing devices have proprietary mechanisms for network selection and traffic steering making it difficult to manage user experience for dual mode (Wi-Fi + cellular) devices across different UE/OS/OEM implementations.

Chapter 3 of this paper provides detailed recommendations on how to address some of the existing gaps in standards by proposing enhancements to ANDSF-based solutions. A well-designed, enhanced ANDSF solution will make use of several types of additional information. This includes leveraging subscriber and subscription information along with rich analytics, using additional network-based information available to devices, and enabling real-time network conditions to be factored into INS decisions.

As discussed in sections 3.1.4 and 3.2.2.4, one of the most critical pieces of a good INS solution will be to inform decisions based on the real-time network conditions. For instance, when the cellular network is heavily loaded, it may be beneficial to steer more users towards a Wi-Fi network. Similarly, when devices have particularly poor cellular radio conditions, and a Wi-Fi network is available with a better signal, the user may have a better experience on the Wi-Fi network. The ability to steer traffic dynamically to a given network based on these conditions would provide a significant enhancement to existing INS solutions. To enable this functionality, this paper recommends:

- Enhancements to the LTE SIB broadcast messages to convey additional information to devices. Specifically, it is recommended that:
    - the SIB include both 3G & LTE network load,
    - a variable signal strength threshold that indicates the radio conditions at which another access be preferred,
    - and a calculated randomization value (to mitigate ping-ponging effects during multiple device steering).
- Enhancements to ANDSF policies for Wi-Fi network selection and traffic steering also need in order to include cellular network condition, which enables device to perform intelligent network selection and traffic steering of user traffic based on these policy rules and the real time network conditions provided by cellular access network.

Another recommendation has to do with the information that is available to the ANDSF server. As discussed in section 3.1.2, currently 3GPP standards neither enable nor preclude the ANDSF server to interconnect with other network elements. These other network elements could provide additional information that may be useful in crafting policy (for instance, subscription information that can be used to tailor policies towards specific users). There is value in standardizing these interfaces, particularly in terms of enabling interoperability between products from different vendors. To that end, this white paper recommends:

- that 3GPP standardize additional interfaces to ANDSF (e.g., the Ud interface between the UDR and ANDSF to enable subscriber-specific information in ANDSF policy).

In addition, as described in section 3.1.3, there is a variety of useful information that may be available from the network, but which cannot currently be utilized in crafting ANDSF policy. For example, HotSpot 2.0 provides a variety of information about the Wi-Fi network either by broadcast or via ANQP query. One such piece of information, Venue Type information, provides helpful hints to the device about the type of venue the AP is currently in, what the venue name is, and more. This could all be useful information in crafting ANDSF policy for network selection and traffic steering, though it is not expected that such information will be used to restrict access to specific APs. For instance, an operator may want to steer users towards a certain network when the user is in a retail shop, but a different network when the user is in a large stadium. To accomplish facilitate this, this white paper recommends:

- that 3GPP enhance ANDSF standards to enable policy based on a Wi-Fi AP's Venue Information, Venue Type, and Access Network Type.

Additionally, as discussed in section 3.2, to address the limitation of Wi-Fi access network selection and maximize the flexibility of Wi-Fi selection, this paper recommends:

- The ANDSF policy and MO enhancement should also include UE intelligence, such as device mobility state, etc.

- ANDSF enhancement of Wi-Fi network selection to allow for selection of Wi-Fi networks that belong to the registered PLMN as well as Wi-Fi access network that not belong to the registered PLMN.

Finally, to achieve consistent behavior across device implementations in support of network selection and traffic steering, this paper recommends:

- the definition of a common set of APIs to exchange necessary information between the INS and OS/CM in order to enable INS decisions as well as to facilitate the communication between an INS client and different OSs/CMs.

- the optimization of functional distribution between INS client and OSs/CMs in order to enable reduced power consumption resulting in improved battery life.

The Key Takeaways

In summary, this paper recommends the industry take the following actions:

The Standards Bodies

- 3GPP should work to enhance the existing ANSDF solution by standardizing additional interfaces, incorporating HS2.0 information such as Venue Type, and enable real-time loading to be provided via SIB messages and used in INS policy.

- The appropriate standards body/forum should define a common set of APIs to exchange information between the INS and OS/CM.

The Device-side Suppliers

- Vendors should work to implement existing standardized INS mechanisms, and proposed enhancements, in such a way that INS behavior is consistent across device platforms.

The Network Infrastructure Suppliers

- Vendors should work to implement proposed enhancements in support of ANDSF-based INS (e.g., new SIB mechanisms, ANSDF interfaces, etc.).

The current phase of this work was focused on identifying ANDSF related requirements and recommendations on both the infrastructure and device aspects of the ecosystem. Other industry approaches, including active support from the RAN for Wi-Fi/Cellular mobility, could be addressed at a future time as well.

5 ACKNOWLEDGEMENTS

The mission of 4G Americas is to promote, facilitate and advocate for the deployment and adoption of the 3GPP family of technologies throughout the Americas. 4G Americas' Board of Governor members include Alcatel-Lucent, América Móvil, AT&T, Blackberry, Cable & Wireless, Cisco, CommScope, Entel, Ericsson, Gemalto, HP, Mavenir Systems, Nokia Solutions and Networks, Openwave Mobility, Powerwave, Qualcomm, Rogers, T-Mobile USA and Telefónica.

4G Americas would like to recognize the joint project leadership and important contributions of Farooq Bari of AT&T and Gautam Talagery of Ericsson, as well as representatives from the other member companies on 4G Americas' Board of Governors who participated in the development of this white paper.