Introduction

La prolifération des applications mobiles a entraîné un accroissement du volume de données dans le réseau de mobile 4G. Avec l'adoption de smartphones et les services à large bande, tels que la diffusion de vidéos, les ressources du réseau cellulaire, sont de plus en plus contraintes.

La technologie Wi-Fi est idéalement positionnée pour ajouter de la capacité au réseau cellulaire. Il est nécessaire pour cela d'améliorer l'interfonctionnement entre le réseau de mobiles 4G et le réseau Wi-Fi afin d'offrir à l'utilisateur final un accès haut débit global et homogène.

En plus de la croissance du trafic, les utilisateurs s'attendent à un accès sans contraintes aux applications qu'ils soient à la maison, dans une entreprise ou en déplacement. Pour cette raison, la technologie Wi-Fi, en assurant un complément de couverture, est une solution appropriée pour les utilisateurs itinérants.

La capacité d'exploiter les bandes de fréquence sans licence en plus du spectre attribué aux réseaux cellulaires présente un attrait évident pour les opérateurs de réseau, qui voient la technologie Wi-Fi comme un autre moyen d'accès au réseau de mobiles 4G.

De nombreux mobiles vendus actuellement comprennent à la fois un accès radio-électrique cellulaire et Wi-Fi, et sont capables d'utiliser simultanément les deux radios Il devient donc possible de diriger certains services vers l'accès Wi-Fi et d'autres vers l'accès radioélectrique cellulaire.

Les différents organismes de normalisation, IEEE (Institute of Electrical and Electronics Engineers), WFA (Wi-Fi Alliance) et 3GPP (3rd Generation Partnership Project) ont ouvert la voie à l'intégration de la technologie Wi-Fi au réseau cellulaire, permettant ainsi à un mobile d'accéder à ses services à travers un accès Wi-Fi.

I.1. Le réseau de mobiles 4G

I.1.1. *L'architecture du réseau*

Le réseau de mobiles de 4e génération EPS (*Evolved Packet System*) est constitué d'un cœur de réseau EPC (*Evolved Packet Core*) et d'un réseau d'accès E-UTRAN (*Evolved Universal Terrestrial Radio Access Network*) (figure I.1).

Le réseau d'accès E-UTRAN assure la connexion des mobiles UE (*User Equipment*). Le cœur de réseau EPC interconnecte les réseaux d'accès, fournit l'interface au réseau de données PDN (*Packet Data Network*) et assure l'attachement des mobiles et l'établissement des supports (*bearers*).

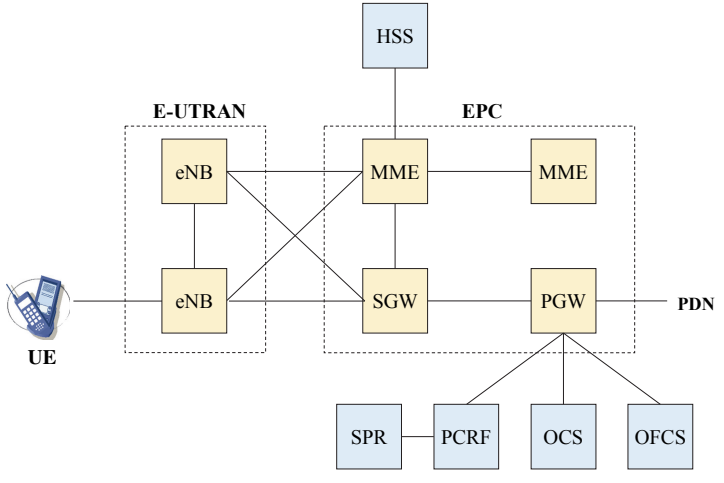

Figure I.1. *L'architecture du réseau de mobiles 4G*

L'entité eNB (*evolved Node B station*) effectue la compression et le chiffrement des données de trafic sur l'interface radioélectrique, et le chiffrement et le contrôle d'intégrité des données de signalisation échangée avec le mobile.

L'entité MME (*Mobility Management Entity*) autorise l'accès des mobiles au réseau EPS et contrôle l'établissement des supports pour la transmission des données de trafic.

L'entité SGW (*Serving Gateway*) constitue le point d'ancrage pour le *handover* intra-système (mobilité à l'intérieur du réseau 4G) et pour le *handover* inter-système en mode PS (*Packet-Switched*), nécessitant le transfert du trafic du mobile vers un réseau de mobiles de 2e ou de 3e génération.

L'entité PGW (*PDN Gateway*) est le routeur de passerelle assurant la connexion du réseau EPS au réseau de données PDN. Elle fournit au mobile sa configuration (adresse IP) et fournit les informations de trafic au système de taxation OCS (*Online Charging System*) pour le pré-payé et OFCS (*Offline Charging System*) pour le post-payé.

L'entité HSS (*Home Subscriber Server*) est une base de données assurant le stockage des données propres à chaque abonné. Les principales données stockées comprennent les identités de l'abonné, les paramètres d'authentification et le profil de service.

L'entité PCRF (*Policy Charging and Rules Function*) fournit à l'entité PGW les règles à appliquer pour le trafic (débit, qualité de service, mode de taxation) lors de l'établissement du support. Ces informations sont stockées dans la base de données SPR (*Subscription Profile Repository*) lors de la création de l'abonnement.

L'authentification mutuelle entre le mobile et l'entité MME est basée sur le mécanisme EPS-AKA (*Authentication and Key Agreement*) :

– l'entité HSS fournit à l'entité MME le vecteur d'authentification (RAND, AUTN, RES, K_{ASME}) à partir de la clé secrète Ki créée lors de l'abonnement du mobile ;

– l'entité MME fournit au mobile l'aléa RAND et le sceau AUTN du réseau ;

– le mobile calcule les sceaux AUTN et RES et la clé K_{ASME} à partir de sa clé Ki stockée dans le module USIM (*Universal Subscriber Identity Module*) de sa carte UICC (*Universal Integrated Circuit Card*) et compare le sceau AUTN reçu avec celui calculé ;

– le mobile transmet son sceau RES à l'entité MME qui le compare à celui reçu de l'entité HSS ;

– la clé K_{ASME} est utilisée pour protéger la signalisation échangée entre le mobile et l'entité MME ainsi que les données du plan de contrôle et de trafic sur l'interface radioélectrique.

I.1.2. *L'établissement du support*

Le réseau EPS transporte le flux de données du mobile (paquets IP) de manière transparente jusqu'à l'entité PGW qui effectue le routage des paquets. Le paquet IP est transporté dans des supports (*bearers*) construits entre les entités du réseau EPS (figure I.2).

Le support radioélectrique DRB (*Data Radio Bearer*) est construit entre le mobile UE et l'entité eNB. La signalisation RRC (*Radio Resource Control*), échangée entre le mobile et l'entité eNB, est chargée de la construction de ce support.

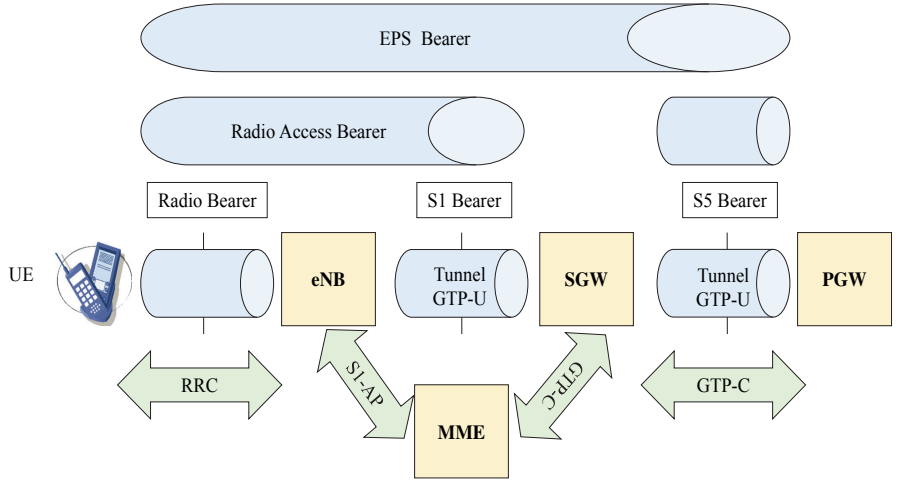

Figure I.2. *L'établissement du support*

Le support S1 est construit entre les entités eNB et SGW. La signalisation S1-AP, échangée entre les entités eNB et MME, et la signalisation GTPv2-C (*GPRS Tunnelling Protocol – Control*), échangée entre les entités MME et SGW, sont chargées de la construction de ce support.

Le support S5 est construit entre les entités SGW et PGW. La signalisation GTPv2-C, échangée entre les entités SGW et PGW, est chargée de la construction de ce support.

La connexion du support radioélectrique et du support S1, effectuée par l'entité eNB, constitue le support E-RAB (*EPS Radio Access Bearer*).

La connexion des supports E-RAB et S5, effectuée par l'entité SGW, constitue le support EPS.

Les supports S1 et S5 sont des tunnels GTP-U (*GPRS Tunnelling Protocol – User*) qui permet au paquet IP du mobile d'être transporté dans le paquet IP du support transmis entre les entités du réseau EPS.

L'entité PGW est la seule entité du réseau EPS qui route le paquet IP du mobile. Le réseau de transport IP qui permet la communication entre les entités du réseau EPS route le paquet IP support S1 ou S5. Les entités eNB et SGW n'effectuent pas de routage. Elles assurent uniquement la connexion entre les supports.

I.2. Le réseau Wi-Fi

I.2.1. *L'architecture du réseau Wi-Fi*

Le réseau Wi-Fi (*Wireless Fidelity*) est constitué de points d'accès AP (*Access Point*) qui effectue un pontage entre l'interface radioélectrique Wi-Fi et l'interface Ethernet vers le réseau LAN (*Local Area Network*) (figure I.3).

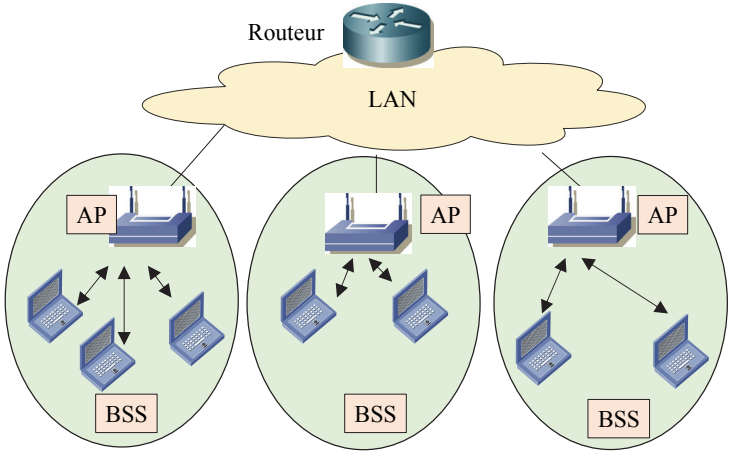

Figure I.3. *L'architecture du réseau Wi-Fi*

La cellule BSS (*Basic Service Set*) est la zone radioélectrique couverte par le point d'accès. L'identifiant BSSID (*BSS Identifier*) de la cellule BSS est l'adresse MAC du point d'accès.

Plusieurs cellules peuvent être déployées afin d'assurer la couverture d'une zone. L'ensemble des cellules constituent un réseau ESS (*Extended Service Set*). Le réseau ESS est identifié par l'identité SSID (*Service Set Identifier*).

La technologie Wi-Fi a défini la couche de liaison de données et la couche physique de l'interface radioélectrique (figure I.4) :

– la couche de liaison de données est constituée de deux sous-couches, la sous-couche LLC (*Logical Link Control*) et la sous-couche MAC (*Medium Access Control*) ;

– la couche physique a défini deux sous-couches, la sous-couche PLCP (*Physical Layer Convergence Protocol*) et la sous-couche PMD (*Physical Medium Dependent*).

Le pontage consiste à modifier la couche de liaison de données et la couche physique utilisées de part et d'autre du point d'accès.

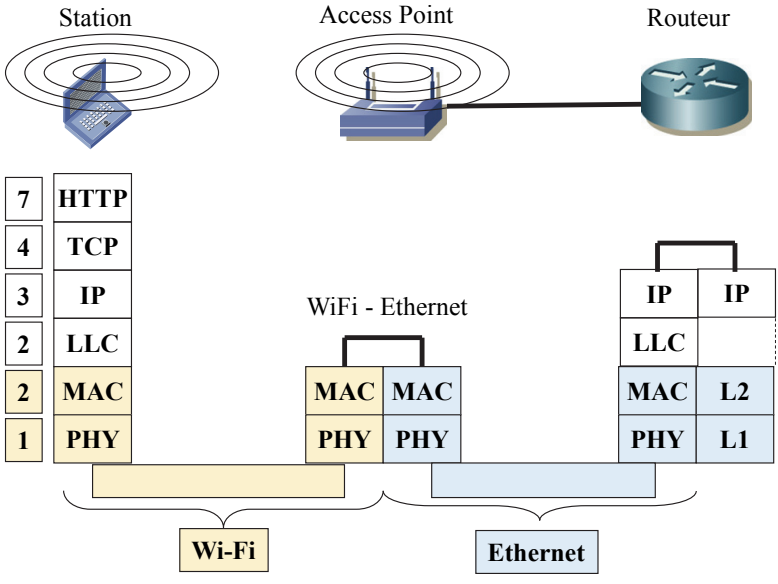

Figure I.4. *L'architecture protocolaire*

La sous-couche LLC n'est pas spécifique à la technologie Wi-Fi. Elle est utilisée également pour d'autres protocoles de la couche de liaison de données, comme par exemple la sous-couche MAC Ethernet. Elle indique la nature des données encapsulées, par exemple un paquet IP.

La sous-couche MAC définit la procédure d'accès du mobile au support physique partagé entre les différents mobiles de la cellule. La procédure CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*) permet de résoudre les problèmes de collision qui se produisent lorsque deux mobiles accèdent simultanément au support physique.

Les trames MAC particulières peuvent être utilisées pour des fonctions de gestion (balayage des canaux radioélectriques, authentification, association) ou de contrôle de transmission (acquittement des trames reçues).

La sous-couche PLCP permet l'adaptation de la sous-couche MAC à la sous-couche PMD, en fournissant les paramètres du traitement du signal pour le récepteur et en indiquant le débit de la trame.

La sous-couche PMD définit les caractéristiques de la transmission radioélectrique.

I.2.2. *L'architecture de sécurité*

Le mécanisme 802.1x définit le contrôle d'accès du mobile au réseau Wi-Fi qui s'effectue entre le mobile et le serveur d'authentification RADIUS (*Remote Authentication Dial-In User Service*).

Le mécanisme 802.1x s'appuie sur les messages d'authentification EAP (*Extensible Authentication Protocol*) – *Method*, pour lesquels plusieurs protocoles sont définis :

– le protocole EAP-CHAP (*Challenge Handshake Authentication Protocol*) permet l'authentification du mobile par le serveur RADIUS, basée sur un mot de passe ;

– le protocole EAP-TLS (*Transport Layer Security*) permet l'authentification mutuelle du mobile et du serveur RADIUS basée sur des certificats ;

– le protocole EAP-TTLS (*Tunneled Transport Layer Security*) permet l'authentification mutuelle du serveur RADIUS, basée sur un certificat, et du mobile, basée sur un mot de passe.

La protection des données sur l'interface radioélectrique introduit une extension de l'en-tête MAC :

– l'extension TKIP (*Temporal Key Integrity Protocol*) pour le mécanisme WPA (*Wi-Fi Protected Access*) basé sur les algorithmes RC4 (*Rivest Cipher*) pour le chiffrement et MICHAEL pour le contrôle d'intégrité ;

– l'extension CCMP (*Counter-mode/CBC-MAC-Protocol*) pour le mécanisme WPA2 basée sur l'algorithme AES (*Advanced Encryption Standard*) pour le chiffrement et le contrôle d'intégrité.

I.2.3. *Les couches physiques*

L'interface 802.11a définit la couche physique OFDM (*Orthogonal Frequency Division Multiplexing*) fonctionnant dans la bande de fréquence U-NII (*Unlicensed-National Information Infrastructure*) à 5 GHz.

L'interface 802.11g définit la couche physique ERP (*Extended Rate Physical*) fonctionnant dans la bande de fréquence ISM (*Industrial, Scientific, and Medical*) à 2,4 GHz.

Les interfaces 802.11a/g ont un débit dont la valeur 6, 9, 12, 18, 24, 36, 48 et 54 Mbit/s dépend du schéma de modulation et de codage :

– les sous-porteuses du système OFDM sont modulées en BPSK (*Binary Phase Shift Keying*), QPSK (*Quadrature Phase Shift Keying*), 16-QAM (*Quadrature Amplitude Modulation*) ou 64-QAM ;

– le code de correction d'erreur BCC (*Binary Convolutional Coding*) est utilisé un taux de codage de 1/2, 2/3 ou 3/4.

L'interface 802.11n définit la couche physique HT (*High Throughput*) fonctionnant dans les bandes de fréquence U-NII à 5 GHz et ISM à 2,4 GHz.

L'interface 802.11n utilise le système OFDM pour lequel la modulation des sous-porteuses est celle définie pour les interfaces 802.11a/g et introduit une nouvelle valeur (égale à 5/6) pour le taux de codage et un nouveau code de correction d'erreur LDPC (*Low-Density Parity Check*).

L'interface 802.11n a un débit maximal de 600 Mbit/s obtenu à partir de deux nouvelles fonctionnalités :

– l'agrégation de deux canaux radioélectriques permettant d'obtenir une bande passante de 40 MHz ;

– le multiplexage spatial SU (*Single User*) MIMO (*Multiple Input Multiple Output*) de deux à quatre flux pour un utilisateur.

L'interface 802.11ac définit la couche physique VHT (*Very High Throughput*) fonctionnant uniquement dans la bande de fréquence U-NII à 5 GHz.

L'interface 802.11ac introduit de nouvelles fonctionnalités pour atteindre un débit maximal de 6,9 Gbit/s :

– l'agrégation de 8 canaux radioélectriques permettant d'obtenir une bande passante de 160 MHz ;

– le multiplexage spatial SU-MIMO de deux à huit flux pour un utilisateur ;

– le multiplexage spatial MU (*Multi User*) MIMO supportant 4 utilisateurs, avec un maximum de quatre flux pour chaque utilisateur, le nombre total de flux étant limité à huit ;

– la modulation 256-QAM.

I.3. L'intégration de Wi-Fi au réseau de mobiles 4G

L'intégration de l'accès Wi-Fi au réseau de mobiles 4G a un impact sur l'architecture du cœur de réseau EPC qui présente plusieurs variantes en fonction des caractéristiques suivantes :

– l'accès Wi-Fi est contrôlé ou non contrôlé par l'opérateur ;

– la mobilité est gérée par le réseau ou par le mobile.

I.3.1. *L'authentification mutuelle*

L'authentification mutuelle s'effectue entre le mobile et le serveur AAA (*Authentication, Authorization and Accounting*). Elle utilise le mécanisme AKA adapté au protocole EAP-*Method* :

– l'entité HSS fournit au serveur AAA le vecteur d'authentification (RAND, AUTN, RES) ;

– le serveur RADIUS fournit au mobile l'aléa RAND et le sceau AUTN du réseau ;

– le mobile calcule les sceaux AUTN et RES à partir de sa clé Ki stockée dans le module USIM de sa carte UICC et compare le sceau AUTN reçu avec celui calculé ;

– le mobile transmet son sceau RES au serveur AAA qui le compare à celui reçu de l'entité HSS.

Le protocole EAP-AKA' est une évolution de la méthode EAP-AKA qui concerne le mécanisme de dérivation des clés.

I.3.2. *L'architecture basée sur l'interface S2a*

L'architecture basée sur l'interface S2a correspond à un accès Wi-Fi contrôlé et à une mobilité basée sur le réseau.

Le flux du mobile transite par l'interface radioélectrique Wi-Fi et le tunnel S2a, construit entre le point d'accès et l'entité PGW, pour accéder au réseau de données PDN (figure I.5).

L'interface S2a supporte plusieurs mécanismes pour l'établissement du tunnel :

– le mécanisme PMIPv6 (*Proxy Mobile IP version 6*) s'appuie sur la signalisation fournie par l'extension *Mobility* de l'en-tête IPv6 échangée entre l'accès Wi-Fi et l'entité PGW et sur le tunnel GRE (*Generic Routine Encapsulation*) pour le flux du mobile ;

– le mécanisme MIPv4 FA (*Mobile IP version 4 Foreign Agent*) s'appuie sur la signalisation MIPv4 et sur le tunnel IP dans IP pour le flux du mobile ;

– le mécanisme GTPv2 (*GPRS Tunnelling Protocol version 2*) s'appuie sur la signalisation GTPv2-C échangée entre l'accès Wi-Fi contrôlé et l'entité PGW et sur le tunnel GTP-U pour le flux du mobile.

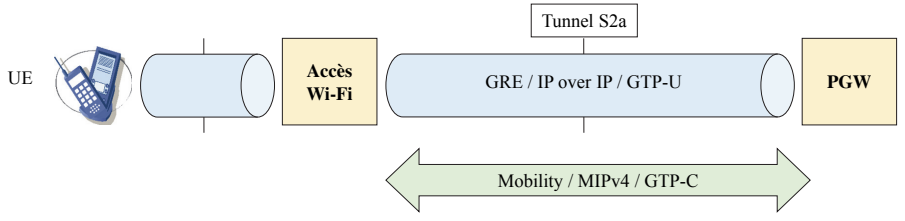

Figure I.5. *L'établissement de la session – architecture basée sur l'interface S2a*

I.3.3. *L'architecture basée sur l'interface S2b*

L'architecture basée sur l'interface S2b correspond à un accès Wi-Fi non contrôlé et à une mobilité basée sur le réseau.

Le flux du mobile transite par le tunnel SWu, construit entre le mobile et l'entité ePDG, et le tunnel S2b, construit entre les entités ePDG (*evolved Packet Data Gateway*) et PGW, pour accéder au réseau de données PDN (figure I.6).

L'interface S2b supporte les mécanismes PMIPv6 ou GTPv2 pour l'établissement du tunnel.

L'interface SWu supporte le mécanisme IPSec (*IP Security*) comprenant la signalisation IKEv2 (*Internet Key Exchange version 2*) et le tunnel ESP (*Encapsulating Security Payload*) pour le flux du mobile.

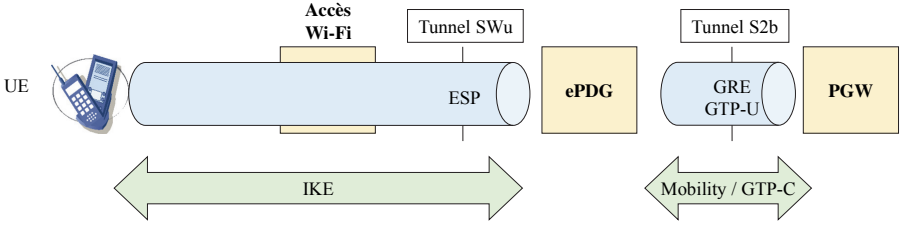

Figure I.6. *L'établissement de la session – architecture basée sur l'interface S2b*

I.3.4. *L'architecture basée sur l'interface S2c*

L'architecture fonctionnelle basée sur l'interface S2c correspond à un accès Wi-Fi contrôlé ou non contrôlé et à une mobilité basée sur le mobile.

Le flux du mobile transite par le tunnel S2c construit entre le mobile et l'entité PGW pour accéder au réseau de données PDN (figure I.7).

Dans le cas d'un accès Wi-Fi non contrôlé, le tunnel S2c transite par le tunnel SWu construit entre le mobile et l'entité ePDG (figure I.7).

L'interface S2c supporte le mécanisme DSMIPv6 (*Dual Stack Mobile IP version 6*) pour l'établissement du tunnel S2c construit entre le mobile et l'entité PGW.

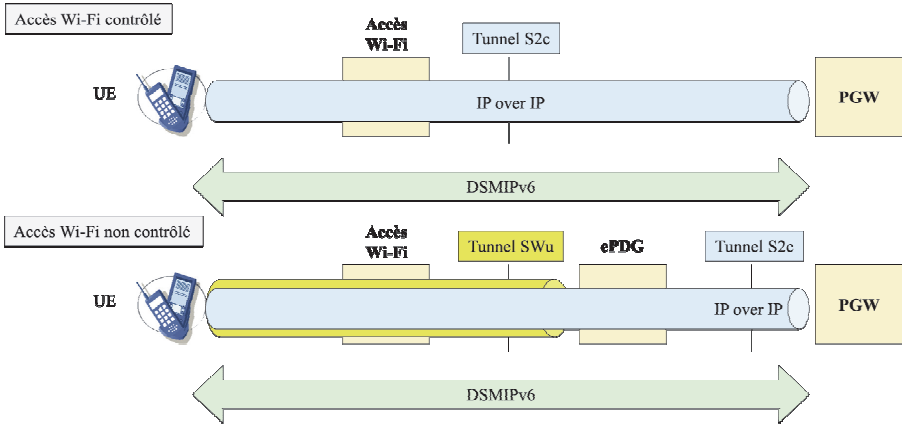

Figure I.7. *L'établissement de la session – architecture basée sur l'interface S2c*

Dans le cas d'un accès Wi-Fi contrôlé, cette interface supporte la signalisation DSMIPv6 et le tunnel IP dans IP pour le flux du mobile.

Dans le cas d'un accès Wi-Fi non contrôlé, le tunnel ESP, établi entre le mobile et l'entité ePDG, protège l'interface S2c.

I.3.5. *La découverte et la sélection du réseau*

Les réseaux de mobiles deviennent de plus en plus hétérogènes. Il est possible pour un mobile d'être couverts simultanément par différents réseaux : les réseaux cellulaires traditionnels, les petites cellules intégrant les accès LTE et Wi-Fi, et les

points d'accès Wi-Fi autonomes. Compte tenu de cette variété, le choix du meilleur réseau pour un mobile est essentiel.

La fonction ANDSF (*Network Discovery and Selection Function*) permet la détection et la sélection du réseau entre un accès LTE et un accès Wi-Fi. Les règles définies par l'opérateur du réseau de mobiles 4G sont fournies par le serveur ANDSF qui est un élément optionnel du cœur de réseau EPC.

Hotspot 2.0 (HS2.0) est un groupe de travail de l'organisme WFA. La cible du travail HS2.0 est de faciliter l'utilisation du point d'accès Wi-Fi dans le un réseau de mobiles 4G. Le programme de certification HS2.0 s'appelle Passpoint.

Les principales fonctionnalités de la version 1 sont basées sur la norme 802.11u et incluent des ajouts à la balise du point d'accès et au serveur ANQP (*Access Network Query Protocol*) qui fournit les règles définies par l'opérateur du service Wi-Fi.

La version 2 permet au mobile d'identifier l'opérateur nominal et les partenaires qui devraient être utilisés lorsque l'opérateur nominal n'est pas accessible directement.

I.4. L'agrégation des accès LTE et Wi-Fi

L'intégration du réseau Wi-Fi dans le réseau de mobiles 4G apporte des modifications sur le cœur de réseau EPC, le point d'ancrage étant réalisé par l'entité PGW. L'agrégation des canaux LTE et Wi-Fi constitue une autre approche qui n'impacte pas la structure du cœur de réseau EPC (figure I.8).

L'accès LTE fonctionne dans une bande de fréquence licenciée. Les évolutions LTE Advanced et LTE Advanced Pro ont défini respectivement une agrégation de 5 et de 32 canaux LTE. L'entité eNB constitue le point d'ancrage de l'agrégation des canaux.

L'agrégation LAA (*Licensed Assisted Access*) est une extension de l'agrégation LTE. La transmission LTE s'effectue sur des bandes de fréquence LTE et Wi-Fi, entre le mobile et l'entité eNB, sans point d'accès intermédiaire. L'entité eNB constitue le point d'ancrage de l'agrégation des canaux.

L'agrégation LWA (*LTE-Wi-Fi Aggregation*) utilise les bandes de fréquence LTE et Wi-Fi. La transmission sur le canal radioélectrique Wi-Fi s'effectue entre le mobile et le point d'accès, conformément aux normes 802.11. L'entité eNB constitue le point d'ancrage de l'agrégation des canaux.

L'agrégation MPTCP (*Multi-Path Transmission Control Protocol*) présente l'avantage de de transmettre des données en utilisant plusieurs chemins sans provoquer de modifications dans les infrastructures existantes (le réseau de mobiles 4G, le réseau Wi-Fi). L'agrégation est réalisée par un serveur MPTCP.

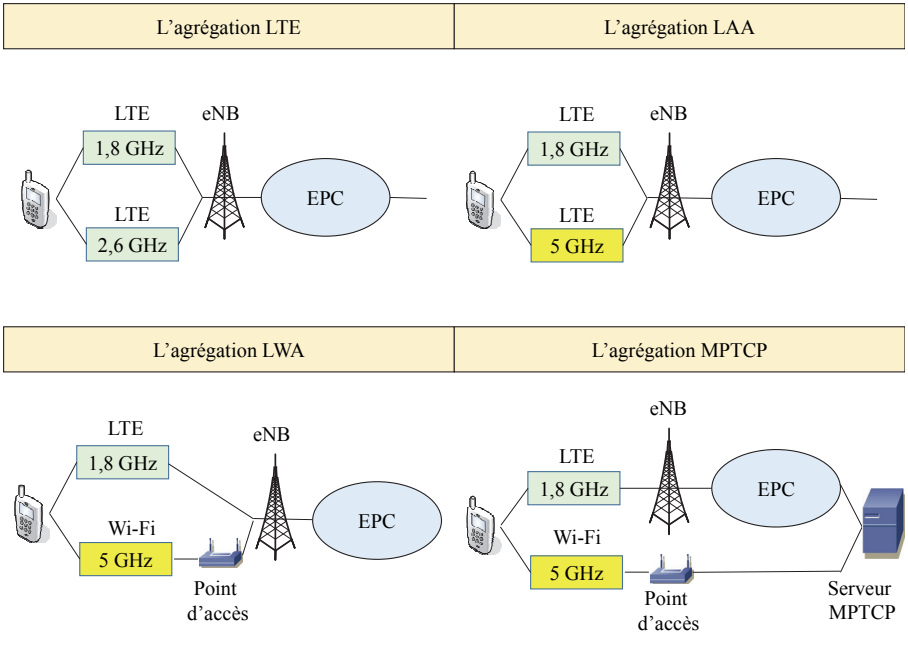

Figure I.8. *L'agrégation des accès LTE et Wi-Fi*