Université du Québec
Institut national de la recherche scientifique
Centre Énergie Matériaux Télécommunications

UN MÉCANISME D'AUTHENTIFICATION RAPIDE POUR LE TRANSFERT VERTICAL AUTOMATIQUE ENTRE RÉSEAUX 3GPP-LTE ET WLAN

Par

Abdelhakim Cherif

Mémoire présenté pour l'obtention du grade de
Maître es Sciences, M.Sc.
en télécommunications

Jury d'évaluation

Président du jury et examinateur interne	Monsieur Amar Mitiche INRS Énergie Matériaux Télécommunications
Examinateur externe	Monsieur Fabrice Labeau U. McGill
Directeur de recherche	Monsieur Jean-Charles Grégoire INRS Énergie Matériaux Télécommunications

Avant-propos

Avoir l'appui d'un directeur de recherche dynamique qui se soucie des besoins de ses étudiants autant du point de vue humain, moral que technique est certainement un atout pour tout étudiant aux cycles supérieures. Pour cette raison, J'aimerais tout d'abord remercier mon directeur de recherche, Professeur **Jean-Charles Grégoire** pour m'avoir aidé, conseillé et guidé tout au long des différentes étapes de mon projet de recherche. Je souhaite exprimer toute ma reconnaissance, toute ma gratitude et tout mon respect à mon encadrant à qui je suis redevable pour ses conseils précieux, ses recommandations constructives et son aide continue pour la réalisation et l'amélioration de la qualité de cette mémoire.

J'aimerais remercier également mes collègues du l'INRS. J'ai passé en leur compagnie de nombreuses heures à discuter des travaux de recherche de tous et chacun. Ils ont ainsi suscité en moi l'intérêt pour la recherche, le tout dans une ambiance des plus chaleureuses.

J'ai le devoir et le plaisir de témoigner ma reconnaissance à tous mes enseignants qui m'ont soutenu au long de mon parcours académique. Je tiens particulièrement à exprimer mes remerciements aux membres de jury du qui m'ont fait l'honneur de juger ce travail.

À un niveau plus personnel, le support de ma famille est incontestablement la raison principale qui m'a permis de me surpasser et de mener à bien mes études. Sans son immense soutien je ne saurais trouver le courage de persévérer dans les moments plus difficiles.

Résumé

La demande croissante des services de données mobiles a amené l'émergence d'une nouvelle génération de réseau qui offre des services différents via un cœur tout IP. L'architecture évoluée de réseau par paquets (EPC) a été conçue pour fournir un soutien à la fois à l'accès 2G/3G, à l'accès LTE et de fournir aussi un accès non-3GPP lors de la mobilité. Cette technologie cellulaire de quatrième génération offre l'accès à l'internet et permet également l'interopération ininterrompue entre les réseaux cellulaires et les réseaux locaux sans-fil. Néanmoins, le passage d'un type d'accès à un autre doit être simple et sécurisé. Le service doit également être le même, et il devrait être transféré de façon transparente sans avoir d'interruption en cas de transfert de connexion entre réseaux cellulaires et WLAN.

L'authentification, le contrôle des conditions d'utilisation (PCC), la facturation et la préservation des services établis sont des défis majeurs pour l'opérateur qui doit maintenir la continuité de la session, de manière transparente, lors du passage d'un accès à un autre.

Ce mémoire se penche sur l'une de ces problématiques qui est l'authentification. La majorité des solutions existantes pour un transfert vertical (inter-technologie) ont toujours certaines restrictions qui touchent à la sécurité et au délai inacceptable pour les applications à temps réel, en raison des nombreux messages échangés. Dans ce travail, nous avons proposé un mécanisme d'authentification sécurisé et rapide lors d'un transfert vertical de 3GPP au non-3GPP basé sur la notion de tickets et qui s'exécute sans contacter le serveur d'authentification AAA (Authentification, Autorisation, Comptabilité). Le but de notre proposition est d'avoir une authentification non seulement sécurisée, mais aussi rapide, en diminuant la latence. Les résultats de l'évaluation des performances montrent en effet que notre proposition améliore la latence. En plus le mécanisme a été modélisé et validé en utilisant l'outil AVISPA et les résultats dégagés montrent bel et bien que le schéma proposé est sécurisé contre différents attaques.

Mots-clés : Accès hétérogène, authentification, transfert vertical entres cellulaire et WLAN, LTE, WLAN.

Abstract

The growing demand in mobile broadband traffic brings up a new generation network that offers different services through an IP-core network. As part of mobile networks, fourth generation network (4G) offers access to the Internet and provides a seamless handover with the heterogeneous access network, such as cellular and Wireless Local Area Network (WLAN). In recent years, a tendency is outlined in the telephone market that offers a variety of access networks. In addition to the cellular modem, terminals often support the Wi-Fi. Moreover, the effectiveness of Wi-Fi technologiy have led operators to integrate the Wi-Fi with the 3rd Generation Partnership project (3GPP) Evolved Packet Core (EPC). Roaming from one access to another must be made simple and secure, the service must also be the same, and it should be possible to seamlessly handoff between Wi-Fi and cellular. The mobile device detects movement and selects the best radio access technology and the subscriber is automatically authenticated and connected.

Authentication, policy and charging control (PCC) and preserving the IP address of the mobile device are the main challenges for the operator to maintain session continuity when moving from one access to another.

This thesis focuses on one of these problems which is the authentication. This is very important to achieve seamless handover between cellular and Wi-Fi. The majority of the existing schemas during vertical handover are not suitable for the mobility scenario and the unacceptable delay for real time applications. In this work, we propose a ticket based authentication schema. This schema provides a fast and secure roaming authentication without contacting the AAA server (Authentication, Authorization, and Accounting). Our schema cannot only provide robust security, but also achieve a simple authentication and enhance roaming parameters such as handover latency. Performance evaluation results show that our proposed schema is much better and is secure against different attacks.

Key-words : Heterogeneous access network, authentication, handover between cellular and Wi-Fi, LTE, WLAN.

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations

2G	Second Generation
3DES	Triple Data Encryption Standard
3G	Third Generation
3GPP	3rd Generation Partnership Project
4G	Fourth Generation
AAA	Authentication Authorization Accounting
AES	Advanced Encryption Standard
AS	Access Stratum
AuC	Authentication Center
AVISPA	Automated Validation of Internet Security Protocols and Applications
BCE	Binding Cache Entry
BSC	Base Station Controller
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
CL-AtSe	Contraint Logic-based Attack Searcher
CoA	Care-of Address
DDoS	Distributed Denial of Service
DoS	Denial of Service
DSMIP	Dual-stack Mobile IP
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EAP	Extensible Authentication Protocol
eHSS	enhanced Home Subscriber Server
eNB	enhanced NodeB
EPC	Evolved Packet core
ePDG	Enhanced Packet Data Gateway
EPS	Evolved Packet System

EPS-AKA	Evolved Packet System Authentication and Key Agreement
FMC	Fixe Mobile Convergence
GERAN	GSM EDGE Radio Access Network
GSM	Global System for Mobile Communications
GTP	GPRS (General Packet Radio Service) Tunneling Protocol
HA	Home Agent
HLPSL	High-Level Protocol Specification Language
HLR	Home Location Register
HoA	Home Address
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
IETF	Internet Engineering Task Force
IF	Intermediate Format
IMSI	International Mobile Subscriber Identity
IPsec	IP Security
KDF	Key Derivation Function
LMA	Local Mobility Anchor
LTE	Long Term Evolution
MAC	Message Authentication Code
MAG	Mobile Access Gateway
MD5	Message Digest 5
MIP	Mobile IP
MITM	Man-In-The-Middle
MME	Mobility Management Equipement
NAS	Non Access Stratum
OFMC	On-the-Fly Model-Checker
OTT	Over-The-Top
PDN-GW	Packet Data Network Gateway
PLMN	Public Land Mobile Network
PMIP	Proxy Mobile Internet Protocol
PSK	Pre-Shared Key
RAN	Radio Access Network
RNC	Radio Network Controller

RNS	Radio Network Subsystem
RRC	Radio Resource Control
SATMC	SAT-based Model-Checker
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SN ID	Serving Network ID
SSID	Service-Set Identifier
SWG	Serving Gateway
TA4SP	Tree Automata based Automatic Approximations for the Analysis of Security Protocols
TWAG	Trusted WLAN Access Gateway
TWAP	Trusted WLAN AAA Proxy
UE	User Equipement
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
WAN	WLAN Access Network
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

Chapitre 1

Introduction

1.1 Contexte et motivation

La convergence des réseaux hétérogènes fixes et mobiles (FMC) est un grand changement dans le monde des télécommunications, enclenché depuis de nombreuses années [1]. La FMC a différentes implications, mais la signification la plus importante pour nous est d'offrir une expérience utilisateur transparente, c.-à-d. que le client peut utiliser différents services n'importe où et n'importe quand. Cette évolution technologique est conçue pour réduire les coûts et favoriser l'utilisation des services interactifs en assurant leur continuité.

Ces dernières années, plusieurs raisons ont amené FMC à intégrer des réseaux sans-fil (WLAN) dans l'architecture évoluée de réseau par paquets (EPC) défini par 3GPP: tout d'abord la demande croissante des services de données mobiles, dont Ericsson et Market Data Report indiquent que le nombre d'abonnés haut débit mobile atteindra près de 5 milliards en 2016 [2]. De plus, la plupart des dispositifs informatiques (smartphones, tablettes, netbooks, ordinateurs portables, eReaders, consoles de jeux..) intègrent l'accès au Wi-Fi et aussi aux réseaux cellulaire. Notons que Infonetics Research a publié en mai 2012 un rapport qui montre l'énorme croissance du nombre de déploiements des points d'accès sans-fil dans les espaces publics, qui a augmenté de 20.000 à plus de 150.000 [3] au cours de la dernière décade. La première réponse de la communauté cellulaire était purement défensive. 3GPP a défini une nouvelle architecture pour intégrer l'accès non-3GPP avec 3GPP EPC qui devait répondre à la demande des opérateurs et des fournisseurs de services Over-The-Top (OTT). En outre, IETF a essayé de fournir le soutien à la mobilité en améliorant les protocoles MIP et PMIP pour les adapter au EPC. L'intégration des WLAN avec EPC permet aux clients

de choisir le meilleur service. Néanmoins, le contrôle du transfert vertical (handover) pour avoir un transfert transparent entre les deux types d'accès reste toujours un défi pour l'opérateur qui doit maintenir la continuité de la session.

Le sujet de ce mémoire s'inscrit dans ce contexte. La communauté 3GPP a précisé les exigences pour que les abonnés bénéficient de la continuité de service lorsqu'ils changent d'un accès à un autre. Dans ce cadre, plusieurs approches de la mobilité ont été intégrées à l'architecture EPC pour diminuer l'impact sur la continuité de service. Pourtant, ces approches exigent des procédures de réauthentification complète entre l'équipement usager (UE) et le nouveau réseau d'accès qui induisent un grand délai dû aux nombreux messages échangés pour contacter le serveur d'authentification, autorisation et comptabilité (AAA) lors du roaming. Donc, nous proposons une méthode sécurisée pour diminuer le temps de handover dans le cadre du roaming vertical (intégrant LTE et WLAN).

Ce chapitre d'introduction présente la problématique et les objectifs de recherche. Suivront par la suite la principale contribution et la structure de ce mémoire qui en découlent et la méthodologie adoptée.

1.2 Problématique

Le Wi-Fi est connu pour son architecture simple et son faible coût, il permet aux opérateurs de téléphonie mobile de trouver une solution pour répondre à la demande croissante des services de données mobiles. Pour cela, les opérateurs mobiles ont commencé à déployer des points d'accès (Hotspots) en grand nombre et à intégrer des connexions Wi-Fi dans leurs réseaux de base. Un des principaux défis que les opérateurs considèrent lors de l'intégration Wi-Fi dans le cœur d'un réseau mobile est le maintien de la continuité de la session lors du roaming entre le WLAN et d'autres technologies d'accès telles que WCDMA/HSPA, CDMA2000 1X et LTE. Le 3GPP et l'IETF introduisent deux protocoles, le GTP et le PMIP, pour aider à soutenir la mobilité à faible latence et d'obtenir un débit de données supérieur. De plus, d'autres études ont été proposées pour supporter la continuité de service lors d'un transfert vertical. En effet, pour les services à temps réel, il est important de diminuer le temps de handover dans le cadre du roaming vertical pour diminuer l'impact du transfert sur la continuité de service. Les solutions existantes exigent de refaire toute la procédure d'authentification pour différents scénarios d'accès, ce qui va nous conduire à échanger un grand nombre de messages et à augmenter la complexité du système. En outre, les systèmes de transfert existants

ne sont pas sécuritaires car certaines solutions sont vulnérables à l'usurpation d'identité sont ouvertes à de multiples attaques très néfastes telles que le *man-in-the-middle* et le détournement de sessions.

Dans ce mémoire, nous proposons une méthode d'authentification rapide et sécurisée pour un transfert vertical entre 3GPP et WLAN. Comparé à d'autres systèmes existant, notre mécanisme peut non seulement fournir une forte sécurité, mais aussi obtenir une procédure d'authentification simple et rapide.

1.3 Contribution

Le présent mémoire offre une authentification plus efficace et plus rapide pour diminuer l'impact sur la continuité de service lors d'un roaming vertical entre le réseau cellulaire et le WLAN. Le passage d'un réseau à un autre doit se faire d'une manière simple et sécurisée. Pour cela, nous proposons une méthode d'authentification rapide et sécurisée. La solution proposée se base sur deux phases : une première qui consiste à la préparation d'un futur transfert automatique vertical, où un serveur aux fonctionnalités étendues, l'enhanced Home Subscriber Server (eHSS) prépare des tickets pour chaque point d'accès sans fil (WAP) qui se trouve dans le secteur de couverture cellulaire contrôlé par un enhanced NodeB (eNB). Ensuite, l'eHSS envoie ces tickets encryptés à l'utilisateur qui doit les décrypter et les stocker pour une prochaine utilisation dans l'éventualité où il va se déplacer dans une zone dans laquelle se trouve un autre point accès sans fil d'un réseau WLAN. Dans la deuxième phase, l'utilisateur utilise ces tickets pour faire une authentification mutuelle avec un des points d'accès sans fil, c.-à-d. que chaque entité vérifie l'identité de l'autre. Après l'envoi de trois messages entre les deux entités, la connexion s'établit et l'utilisateur peut recevoir les données sous une clé de session générée par les deux entités.

Cette méthode nous permet d'obtenir un transfert transparent en utilisant les opérations de clés symétriques et d'éliminer la participation d'une tierce partie, ce qui réduit considérablement latence et nombre de messages. L'analyse de la sécurité et de la performance montre que notre système est efficace en termes de sécurité, messages échangés et latence de handover.

1.4 Structure du mémoire

Dans le présent chapitre, nous avons communiqué les éléments de la problématique et le travail accompli ainsi que la contribution de ce mémoire. La structure de ce document est décrite ci-dessous.

Suivant l'introduction, le chapitre 2 présente la mise en contexte sur le sujet abordé dans ce mémoire. Nous mettons l'accent principalement sur l'architecture générale d'accès pour définir les différentes entités d'EPC. De plus, nous détaillons l'architecture d'authentification de base pour LTE d'un part, car notre mécanisme opère après l'établissement d'une authentification cellulaire complète, et d'autre part nous présentons l'architecture d'authentification de base WLAN.

Le chapitre 3 décrit les méthodes d'intégration cellulaire et Wi-Fi existantes. Il présente l'état de l'art en termes d'authentification pour le roaming vertical. Nous commençons ce chapitre par la présentation des défis de l'intégration cellulaire avec Wi-Fi. Ensuite, nous détaillons les méthodes d'intégration existantes. Nous décrivons par la suite les protocoles de mobilité. Finalement, nous décrivons le concept d'authentification lors d'un transfert vertical entre cellulaire et Wi-Fi en précisant ses forces et ses faiblesses.

Le chapitre 4 décrit le nouveau mécanisme d'authentification pour un handover vertical entre 3GPP et WLAN que nous proposons. Nous commençons par présenter la solution. Nous présentons la première phase de préparation au futur transfert automatique en premier lieu. Nous présentons ensuite la deuxième phase, la phase d'authentification.

Le chapitre 5 présente l'étude de la proposition où nous avons validé et modélisé notre proposition en utilisant l'outil AVISPA. Après nous avons comparé notre mécanisme avec d'autres existants et nous avons montré que notre solution reduit significativement le temps de handover.

Le chapitre 6 conclut ce document avec une discussion en regard des aspects méthodologiques et des résultats en lien avec des travaux effectués ainsi que les résultats obtenus. Nous identifions également les travaux futurs afin d'améliorer le mécanisme proposé.

Chapitre 2

L'authentification dans les accès LTE et WLAN

2.1 Introduction

Le 3GPP est un groupe de 3rd generation partnership project (3GPP) et des opérateurs téléphoniques à travers le monde. 3GPP produit les spécifications de réseaux mobiles de deuxième génération (2G), troisième génération (3G) ainsi que LTE qui est associé à l'évolution « toute IP » du cœur de réseau, désigné par EPC. EPC supporte la mobilité entre différents accès hétérogènes comme, par exemple, entre 3GPP et WLAN. Nous allons dans un premier temps faire la présentation de l'architecture générale de LTE/EPC. Ensuite, nous décrirons les mécanismes d'authentification dans l'accès LTE et WLAN.

2.2 Architecture d'accès générale

Avant de rentrer dans les détails de l'architecture EPC, il faut noter que le système cellulaire complet est connu sous le nom d'Evolved Packet System (EPS) [4]. Le EPS est composé de deux sous réseaux :

- *Le Radio Access Network* (RAN).
- *L'Evolved Packet Core* (EPC).

Le RAN contient les éléments d'accès aux réseaux cellulaires dont nous présenterons les noms ci-après:

– *GSM EDGE Radio Access Network* (GERAN) : une technologie d'accès qui sous-tend la 2G; elle est composée des contrôleurs de station de base (BSC) et de sous-systèmes de station de base (BSS) qui contiennent des stations de base radio (BTSs).
– *Universal Terrestrial Radio Access Network* (UTRAN) : une technologie d'accès qui supporte la 3G; son architecture est presque identique à celle de GERAN. Elle se compose des contrôleurs de réseau radio (RNC) et des sous-systèmes de réseau radio (RNS).
– *Evolved Universal Terrestrial Radio Access Network* (E-UTRAN) : une technologie d'accès qui supporte le 4G. Son architecture est simplifiée; elle exige des temps de réponse rapides sur l'interface radio. Pour cela, on trouve que les fonctions du RNC sont implémentées dans les stations de base LTE (eNodeBs). Donc, l'E-UTRAN est composé d'eNodeBs.

Dans l'architecture EPC, l'utilisateur peut communiquer à travers les accès cellulaires cités plus haut tout comme il peut communiquer aussi à travers des réseaux d'accès non-3GPP. En pratique, l'accès non-3GPP comprend les réseaux sans fil comme le WiFi et le WiMAX. Il existe deux types d'accès non-3GPP à EPC comme il est défini dans 3GPP TS 33.402 [5]; les accès de confiance (*Trusted non-3GPP access*) et les accès sans confiance (*Untrusted non-3GPP access*).

– Trusted non-3GPP access : un accès dont l'opérateur est un partenaire, avec lequel une relation d'affaire existe. Il possède une méthode d'authentification sécurisée.
– Untrusted non-3GPP access : un accès qui comprend tous types de connexion WiFi qui ne sont pas sous le contrôle d'un opérateur partenaire (comme les réseaux publics) ou bien qui ne fournissent pas une sécurité suffisante (au niveau d'authentification, cryptage, etc.).

La figure 2.1 présente l'architecture d'accès liée à l'EPC [6]. Dans la perspective de l'accès sécurisé, EPC comprend des nœuds spécifiques aux accès qui sont reliés avec les interfaces de communication pour intégrer les accès 3GPP et le non 3GPP. Ceci comprend le *Mobility Management Equipement* (MME), le *Serving Gateway* (SGW) et le *Packet Data Network Gateway* (PDN-GW) qui constituent le cœur du réseau et le *Home Subscriber Server* (HSS), siège de l'authentification.

2.2.1 Home Subscriber Server (HSS)

Le HSS est une base de données qui contient les profils de tous les abonnés du réseau. Il prend part à l'authentification et à l'autorisation des services fournis aux utilisateurs. Le HSS remplace les entités *Home*

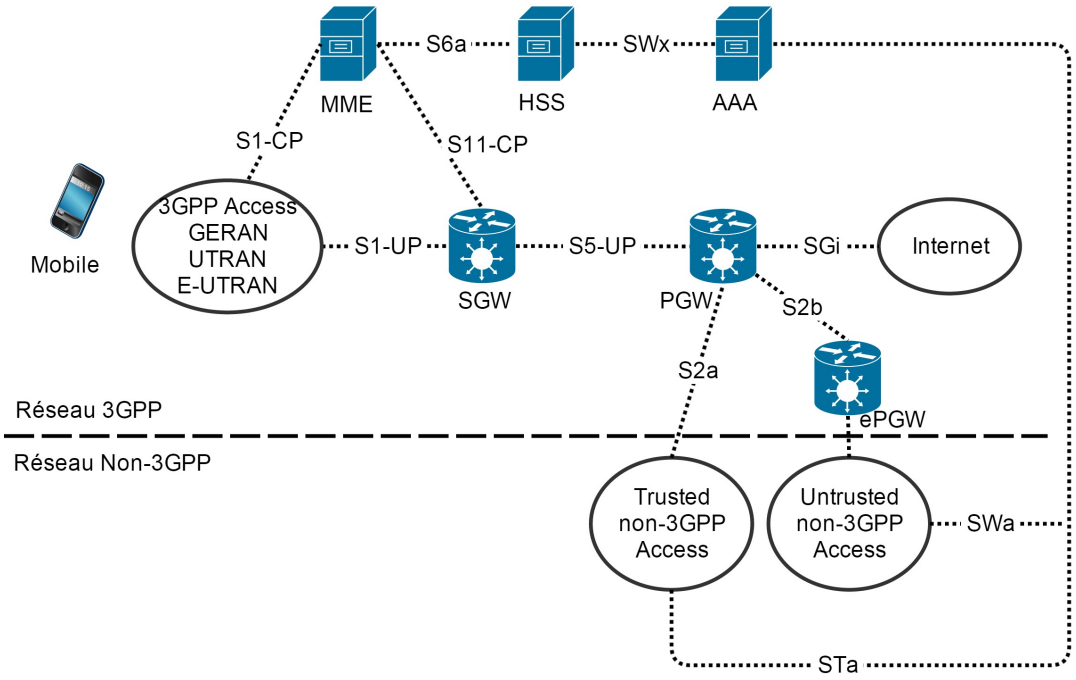

FIGURE 2.1 – Architecture d'accès liée à l'Evolved Packet Core.

Location Register (HLR) et *Authentication Center* (AuC) des architectures UMTS et GSM. Dans LTE, le HSS utilise le protocole Diameter pour échanger les informations à travers l'interface S6a. HSS stocke plusieurs données sur l'utilisateur comme son identité universelle ou son *International Mobile Subscriber Identity*, les informations d'authentification des abonnés, les services que l'utilisateur est autorisé à utiliser, etc.

2.2.2 Mobility Management Entity (MME)

MME est l'entité principale de contrôle pour l'accès LTE. Elle est responsable de l'authentification et de l'autorisation (par l'interaction avec le HSS), et de la gestion de mobilité. MME coordonne l'accès entre les eNodeBs et les équipements du cœur réseau d'une part et entre l'abonné et le réseau cœur d'autre part. Une autre fonction importante du MME est de sélectionner les relais S-GW et le P-GW pour établir un chemin sécurisé pour les communications de l'abonné.

2.2.3 Serving Gateway (S-GW)

Le S-GW est situé entre l'eNodeB et P-GW. Il sert de relais de transmission des paquets entre ces deux entités. Le S-GW est connecté à l'eNodeB à travers l'interface S1 et au P-GW à travers l'interface S5. De plus, le S-GW stocke temporairement les données destinées aux terminaux en mode veille pendant que le MME les invite à se reconnecter au réseau.

2.2.4 Packet Data Network (PDN) Gateway (P-GW)

Le P-GW permet d'avoir une connexion entre l'EPC et un réseau IP externe (comme Internet). Il est connecté au S-GW à travers l'interface S5 et au réseau IP externe à travers l'interface SGi. Une autre fonction du P-GW est d'assigner les adresses IP pour les utilisateurs. Un utilisateur peut être connecté à un ou plusieurs P-GW.

2.3 Architecture d'authentification côté LTE

L'authentification dans un réseau mobile consiste à déterminer si un usager est autorisé à accéder à ce réseau. Plusieurs méthodes d'authentification existent pour différents réseaux. Dans cette section, nous allons présenter la méthode d'authentification pour LTE. LTE utilise la procédure d'authentification *Evolved Packet System Authentication and Key Agreement* (EPS-AKA) [7]. EPS-AKA offre la confidentialité, la protection de l'intégrité et l'authentification mutuelle entre l'utilisateur et le réseau. Lorsqu'un utilisateur demande l'accès à un réseau LTE, une authentification mutuelle s'établit entre les deux côtés (utilisateur et réseau) en utilisant l'EPS-AKA. Un ou plusieurs vecteurs d'authentification EPS, de forme AV= RAND, AUTN, XRES, K_{ASME}, sont générés par le HSS et transmis au MME. Par la suite, le MME choisit un de ces vecteurs pour établir une authentification mutuelle avec l'utilisateur et partage avec lui une clé d'authentification K_{ASME}.

2.3.1 Procédure d'authentification

Dans cette partie, nous présentons la procédure d'authentification au réseau LTE qui est basée sur ESP-AKA. La figure 2.2 montre les étapes de cette procédure [8]. La procédure commence lorsqu'un utilisateur

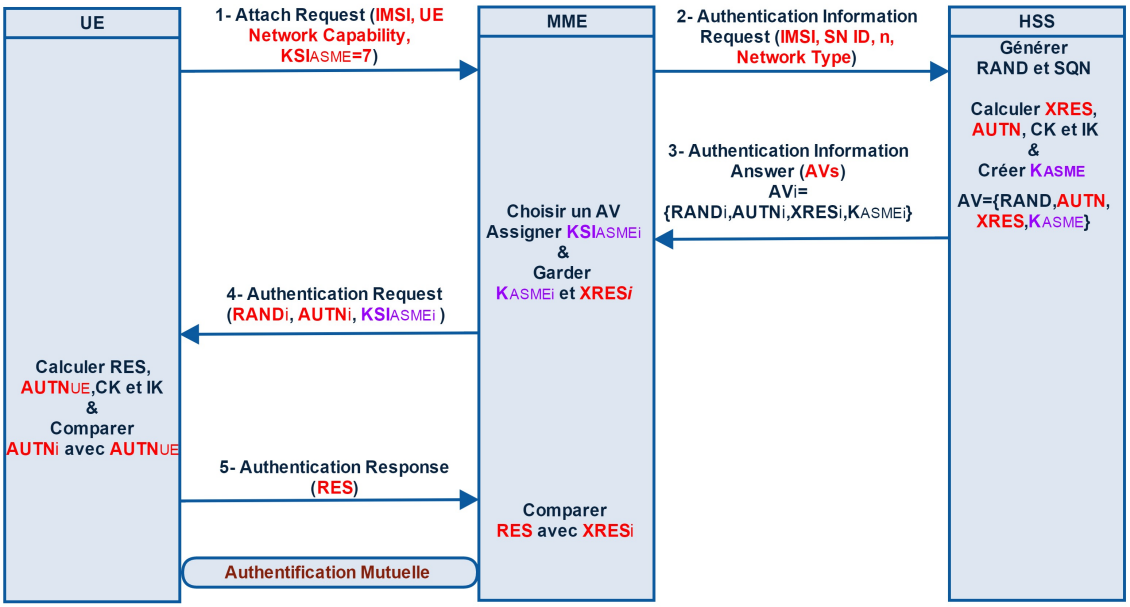

FIGURE 2.2 – Procédure d'authentification LTE

demande l'accès à un réseau LTE. Dans la carte USIM et le HSS on trouve une clé permanente (K) et un *International Mobile Subscriber Identity* (IMSI) que nous allons utiliser pour la procédure d'authentification.

Demande d'authentification de l'utilisateur

Comme une première étape, l'utilisateur va demander l'authentification au réseau. Il envoie le message « *Attach Request (IMSI, UE Network Capability,* KSI_{ASME}*)* » au MME. L'IMSI est une identité unique pour chaque utilisateur, le UE Network Capability est un algorithme de sécurité utilisé par l'utilisateur et le champ KSI_{ASME}=7 indique que l'utilisateur n'a pas de clé d'authentification.

Échange de l'information entre le MME et le HSS

À la réception de la demande d'authentification « *Attach Request (IMSI, UE Network Capability,* KSI_{ASME}*=7)*» de la part de l'utilisateur, le MME envoie le message « *Authentication Information Request (IMSI, SN ID, n, Network Type)* » au HSS. SN ID est l'abréviation de *Serving Network ID* qui consiste en l'identité du réseau *Public Land Mobile Network* (PLMN). Le paramètre n est le nombre de vecteurs d'authentification demandés par le MME et le *Network Type* représente le type d'accès que l'utilisateur a utilisé (E-UTRAN).

À la réception du message « *Authentication Information Request* », le HSS génère une valeur aléatoire RAND et SQN. Ensuite, il calcule XRES, AUTN, CK et IK en utilisant l'algorithme EPS-AKA avec la clé k, et les valeurs RAND et le SQN calculées auparavant. Puis il utilise SQN, IK, CK et SN ID pour créer la clé KSI_{ASME} avec la fonction de dérivation de clé (KDF). Dès que la clé K_{ASME} est calculée, le HSS crée les vecteurs d'authentification AVi= $RAND_i$, $AUTN_i$, $XRES_i$, K_{ASMEi}, avec i=0, 1, 2,.., n.

Authentification mutuelle entre le MME et l'utilisateur

Après la création des vecteurs AVs, le HSS envoie le message «*Authentication Information Answer (AVs)*» au MME. Ce dernier choisit un de ces vecteurs et assigne un KSI_{ASME}comme identifiant de K_{ASME}.

Le quatrième message dans la séquence est le « *Authentication Request (*KSI_{ASMEi}*,* $RAND_i$*,* $AUTN_i$*)* » transmis par le MME à l'utilisateur après avoir conservé K_{ASMEi} et le XRESi.

En recevant le message « *Authentication Request (*KSI_{ASMEi}*,* $RAND_i$*,* $AUTN_i$*)* », le mobile utilise l'algorithme utilisé dans HSS pour générer $AUTN_{UE}$, RES, IK et CK avec la clé K, RANDi et SQN de HSS. Ainsi, il compare l'$AUTN_{UE}$ avec AUTN pour authentifier le réseau.

Ensuite, le mobile envoie le message « *Authentication Response* » au MME. Dans ce cas, MME compare la composante RES reçue dans ce message avec le XRESi existant dans le vecteur d'authentification et que le MME garde toujours. Si RES est égale au $XRES_i$, le client est bien authentifié.

2.3.2 La sécurité dans LTE

Dans la partie précédente 2.3.1, nous avons présenté la procédure d'authentification de LTE qui se base sur une authentification mutuelle en utilisant le mécanisme EPS-AKA. Après l'authentification, la connexion est établie et l'équipement usager et le MME partagent la clé K_{ASME}. Dans cette clé principale dérivent d'autres clés qui ont des missions plus particulières. Dans cette section, nous allons discuter les procédures de configuration de sécurité NAS et AS qui sont basées sur la clé K_{ASME} [9].

– Sécurité NAS : NAS est l'abréviation de « *Non Access Stratum* ». Le but principal de la sécurité NAS est de transmettre les messages de signalisation entre le MME et l'équipement usager en toute sécurité, donc chiffrés, au niveau du plan de commande. Les clés de sécurité NAS sont générées à partir de la

clé K_{ASME}. Après avoir établi la sécurité NAS, le MME et le UE partagent une clé de chiffrement (K_{NASenc}) et une clé d'intégrité (K_{NASint}) utilisées pour le chiffrement et la protection de l'intégrité de la signalisation entre l'UE et le MME.

– Sécurité AS : AS est l'abréviation de « *Access Stratum* ». Les clés de sécurité AS sont utilisées pour transmettre en toute sécurité des paquets IP et des messages *Radio Resource Control* (RRC) entre le point d'accès (ENodeB) et le UE. Elles sont générées à partir de la clé K_{eNB}. Après avoir établi la sécurité AS, l'eNodeB et l'équipement usager partagent une clé d'intégrité RRC (K_{RRCint}), une clé de cryptage RRC (K_{RRCenc}) et la clé de cryptage du plan d'usager (K_{UPenc}). Ces clés servent au chiffrement et à la protection de l'intégrité.

Nous remarquons que les clés de sécurité utilisées pour l'architecture LTE ont leur propre hiérarchie et sont séparées. La clé K_{ASME} est obtenue à partir de la clé CK et IK. Les clés de NAS (K_{NASenc}, K_{NASint}) sont générées à partir de la clé K_{ASME} et les clés d'AS (K_{RRCint}, K_{RRCenc}, K_{UPenc}) sont générées à partir de la clé K_{eNB}.

2.4 Architecture d'authentification côté WLAN

Les réseaux de type WLAN, bénéficient de différentes méthodes d'authentification sécurisées afin que le réseau ne puisse être utilisé que par les individus et les dispositifs qui sont autorisés. De nos jours, il existe trois méthodes d'authentification dominantes [10]:

– Authentification ouverte: c'est une méthode d'authentification la plus simple. Le fait que l'équipement usager connait le *Service-Set Identifier* (SSID) du réseau, l'autorisera à accéder au réseau.
– Authentification partagée : ce type d'authentification est utilisé dans des réseaux individuels ou bien dans les petites entreprises. Cette méthode est basée sur une clé convenue *Pre-Shared Key* (PSK) partagée entre le réseau et l'équipement usager. Si les clés correspondent, alors le dispositif est admis sur le réseau.
– Extensible Authentication Protocol (EAP) : c'est la méthode d'authentification la plus connue. Elle est fréquemment adoptée, surtout dans les entreprises. EAP repose sur un serveur d'authentification et permet d'utiliser divers algorithmes de chiffrement.

Outre la méthode utilisée pour l'authentification, le choix de la méthode de chiffrement est également critique. À ce jour, trois méthodes sont possibles:

– *Wired Equivalent Privacy* (WEP): C'est un algorithme de sécurité qui utilise l'algorithme RC4 pour le cryptage. Cette méthode n'est plus utilisée puisqu'elle a des faiblesses au niveau du partage des clés de sécurité.
– *Wi-Fi Protected Access* (WPA) : Cette méthode répond à la faiblesse que nous trouvons dans le WEP. WPA utilise le protocole Temporal Key Integrity (TKIP) qui utilise des clés dynamiques.
– *Wi-Fi Protected Access* (WPA2) : WPA2 utilise le Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) à la place de TKIP. Cette méthode est basée sur l'algorithme Advanced Encryption Standard (AES).

2.4.1 Authentification EAP

Après avoir discuté les différentes méthodes d'authentification et de cryptage, nous allons parler dans cette partie un des protocoles les plus connus pour l'authentification qui est l'EAP. EAP fournit un niveau de sécurité très élevé pour le WLAN. Cette méthode utilise un serveur RADIUS pour établir une authentification mutuelle et génère la clé d'authentification WEP. La figure 2.3 expose la procédure d'authentification d'EAP, qui comprend le point d'accès sans-fil (WAP) et un serveur d'authentification RADIUS [11].

9 étapes sont nécessaires pour établir une authentification à un réseau sans fil. L'équipement usager et le serveur RADIUS utilisent 801.1x et EAP pour effectuer une authentification mutuelle via le point d'accès (WAP). L'équipement usager envoie comme premier message une demande d'authentification au WAP. Ensuite, le serveur RADIUS répond à cette demande en envoyant un défi à l'UE. L'utilisateur entre un mot de passe qui va être chiffré et envoyé comme réponse au défi envoyé par le serveur. En recevant cette réponse, le serveur utilise des informations stockées dans sa base de données et calcule sa propre réponse pour la comparer à la réponse envoyée par le client. Si les deux réponses correspondent, le serveur RADIUS authentifie l'équipement usager. Et de la même façon, l'équipement usager doit authentifier le serveur RADIUS. Une fois que l'authentification mutuelle est effectuée, le serveur et l'équipement usager partagent une clé d'authentification WEP qui est unique à l'utilisateur. Il existe plusieurs options pour le mécanisme d'authentification EAP, mais elles utilisent une authentification mutuelle et le WAP se comporte toujours de la même façon, son rôle principal étant de relayer les messages d'authentification entre le client et le serveur.

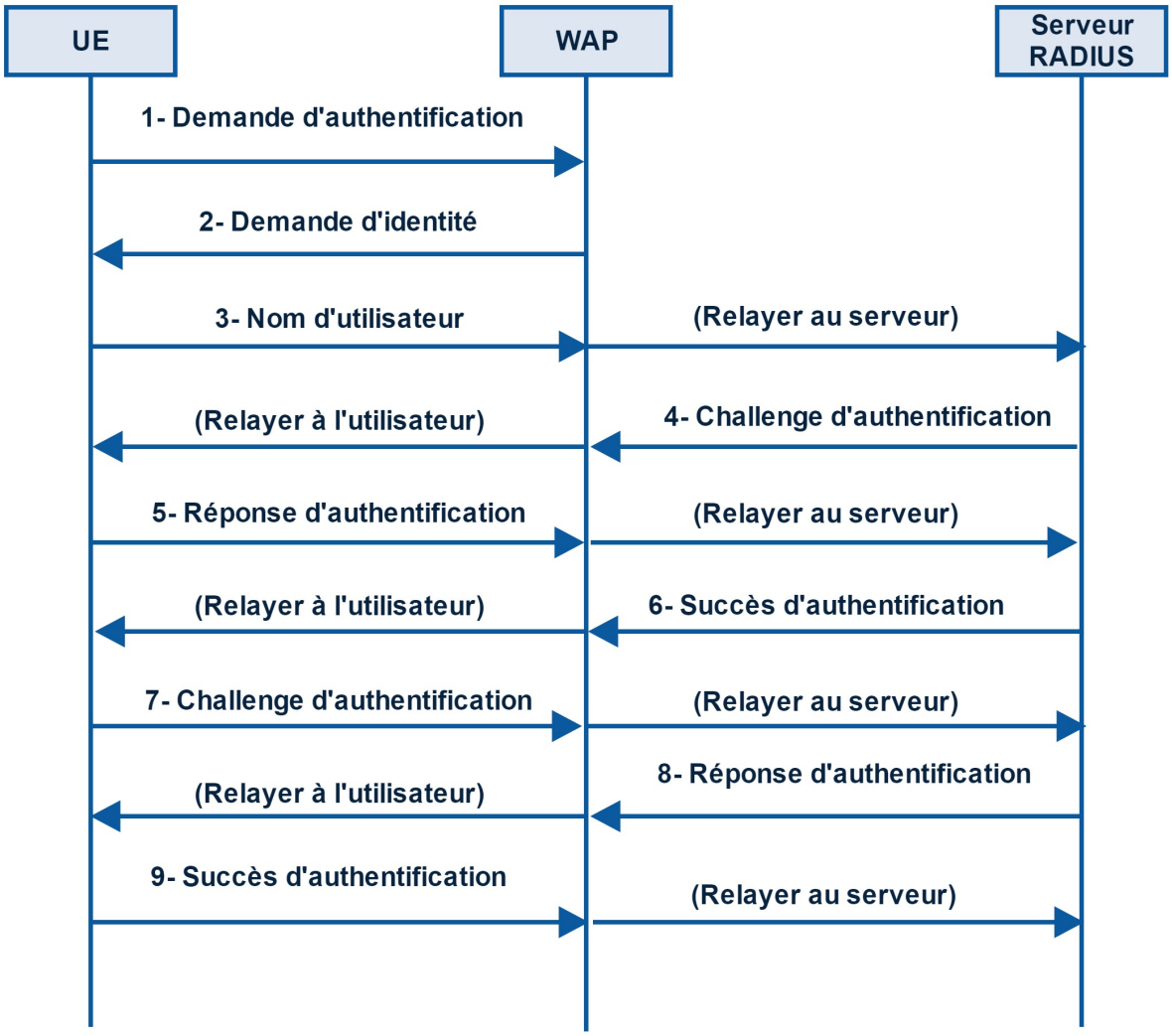

FIGURE 2.3 – Procédure d'authentification EAP

2.5 Conclusion

Dans ce chapitre, nous avons étudié l'architecture d'EPC et les méthodes d'authentification existantes tant du côté de LTE que du côté du WLAN pour introduire le contexte général de notre travail. Ceci nous permet maintenant de nous pencher sur la gestion de la mobilité entre réseaux LTE et WLAN, et sur le problème de la continuité de session des utilisateurs lorsqu'ils changent de réseau d'accès.

Chapitre 3

Intégration des réseaux cellulaires et Wi-Fi

3.1 Introduction

Récemment, 3GPP a défini une solution pour permettre l'accès au cœur du réseau 3GPP via les accès de type WLAN [12]. Cette solution facilite l'interopérabilité entre le réseau cellulaire et les réseaux Wi-Fi. De plus, la plupart des nouveaux dispositifs informatiques (smartphones, tablettes, netbooks, ordinateurs portables, eReaders, consoles de jeux..) intègrent l'accès au Wi-Fi. Un grand nombre de ces appareils sont capables d'utiliser deux radios à la fois, cellulaire et Wi-Fi. On note également, qu'il est possible d'exploiter une connexion Wi-Fi lorsque l'utilisateur est dans une zone couverte par un réseau de ce type, et un accès 3GPP sinon. Pour que ceci soit utile, il faut pouvoir fournir la continuité de service lors de la mobilité des utilisateurs. Tous les abonnés doivent être capables de se déplacer dans la zone de couverture offerte par leur opérateur sans interruption de service s'ils changent de la technologie d'accès.

3.2 Roaming vertical entre 3GPP et WLAN

Le roaming est un transfert intercellulaire qui permet à une station mobile de changer d'une cellule à une autre en bénéficiant du même service avec un minimum d'interruption pour l'utilisateur. En réalité, il existe plusieurs types de transfert:

– Transfert horizontal: c'est un transfert qui s'effectue entre deux nœuds d'accès qui ont la même technologie (par exemple entre des points d'accès sans fil).
– Transfert vertical: c'est un transfert qui s'effectue entre deux nœuds d'accès de technologies différentes (par exemple entre LTE et Wi-Fi).

3.3 Défis de l'intégration cellulaire-Wi-Fi

Avoir un transfert vertical (cellulaire/Wi-Fi) d'une manière transparente et efficace est l'un des principaux problèmes pour les protocoles de gestion de la mobilité. Les protocoles dans les réseaux IP, ne supportent généralement pas les communications mobiles à cause de leurs mécanismes de routage et d'adressage. Il est souhaitable pour les utilisateurs d'une part et les fournisseurs de service d'autre part d'avoir un transfert transparent lors de déplacement d'un réseau cellulaire à Wi-Fi. Dans cette perspective, lors du transfert vertical au niveau de la frontière cellulaire/Wi-Fi on peut rencontrer les problèmes suivants [13]:

– Sélection du réseau: la sélection d'un point d'accès WLAN convenable représente un défi lors d'un transfert.
– Ping-Pong: cet effet de transfert rapide d'un réseau à l'autre se produit lorsque l'utilisateur se trouve sous la couverture cellulaire et un WLAN présente un signal fort équivalent à celui de LTE. Sa connectivité peut alors osciller entre les deux réseaux.
– Préservation de l'adresse IP: l'incohérence de l'adresse IP lors d'un transfert fournit l'interruption de service. Donc, l'obtention d'une nouvelle adresse IP valide dans le réseau étranger est nécessaire.

Résoudre le problème de la continuité de service lors d'un transfert offre à l'utilisateur la souplesse de choisir le réseau le plus favorable et permet à l'opérateur de profiter de l'existence d'infrastructures à faible coût tout en conservant la qualité de service. Pour cela, il est nécessaire de maintenir la continuité de service pour toutes les applications et surtout pour les applications en temps réel comme le streaming, les jeux en ligne ou bien la voix sur IP; sinon le service est perturbé. Par suite, la rapidité lors de la réalisation d'une opération de mobilité permettra d'avoir une meilleure qualité pour les applications qui sont très sensibles aux délais.

3.4 Méthodes de mobilité entre les réseaux 3GPP et WLAN

L'architecture EPC (présentée dans 2.2) a été proposée pour intégrer les accès cellulaires (comme le 2G, 3G et LTE) et aussi pour faciliter la mobilité pour l'accès non-3GPP (Wi-Fi, WiMAX) [14]. Lorsque l'accès non-3GPP est considéré suffisamment sécurisé en partenariat avec l'opérateur cellulaire, il peut être traité comme un accès de confiance (Trusted). Sinon il sera considéré non sécurisé (Untrusted) et, dans ce cas là, l'équipement usager doit établir un tunnel IPsec (Internet IP Security) directement avec le Enhanced Packet Data Gateway (ePDG) pour sécuriser ses échanges de trafic. En pratique, il existe deux méthodes pour la gestion de la mobilité IP qui sont proposées par le 3GPP :

- Mobilité basée sur le réseau: ce mécanisme utilise deux interfaces différents, le S2a pour les accès Trusted de EPC et le S2b pour les accès Untrusted de EPC. Les interfaces S2a et S2b utilisent les protocoles de mobilité comme le GPRS tunneling Protocol (GTP) et le Proxy Mobile IP (PMIP).
- Mobilité basée sur client/hôte: ce mécanisme utilise l'interface S2c qui repose sur le protocole bi-pile (dual-stack) Mobile IP (DSMIP) entre l'équipement usager et le PDN-GW.

3.4.1 Accès Non-3GPP via l'interface S2a

L'interface S2a permet l'accès à l'architecture EPC à travers un réseau WLAN de confiance en utilisant le protocole GTP. Cette nouvelle architecture offre la mobilité à travers l'interface S2a et est connue sous le nom S2a Based Mobiliy On GTP (SaMOG) [15]. Comme présentée dans la figure 2.1 l'interface S2a est reliée au PDN-GW. Un tunnel GTP s'établit entre la passerelle d'accès WLAN et le PDN-GW. Cette méthode fournit la préservation de l'adresse IP lors du transfert vertical entre accès 3GPP et non-3GPP.

3.4.2 Accès Non-3GPP via l'interface S2b

L'interface S2b fournit l'accès à l'architecture EPC à partir d'un réseau non sécurisé (Untrusted). Dans ce cas l'équipement usager doit mettre en place un réseau virtuel privé (VPN) pour maintenir la relation de confiance. Un tunnel IPSec est établi entre l'utilisateur et l'ePDG pour accéder à l'EPC. Ensuite, un tunnel GTP ou bien PMIP est établi entre le ePDG et le PDN-GW.

3.4.3 Accès Non-3GPP via l'interface S2c

Dans ce cas, l'équipement usager établit une connexion DSMIP avec l'EPC. Cette méthode nécessite le support d'IPSec entre l'équipement usager et le PDN-GW pour protéger la signalisation entre ces deux derniers.

3.5 Les protocoles de mobilité

Cette section est réservée à la présentation de quelques protocoles de mobilité utiles dans la compréhension des solutions existantes. La première partie se penche sur la définition du protocole GPRS Tunneling Protocol (GTP) et le protocole Mobile IP (MIP). Dans la seconde moitié nous définissons les protocoles Proxy Mobile IP (PMIP) et Dual-Stack Mobile IP (DSMIP).

3.5.1 GPRS Tunneling Protocol

Le GTP a été développé pour un réseau de coeur GPRS. C'est un protocole basé sur IP qui permet aux utilisateurs de se déplacer d'un réseau d'accès à un autre tout en préservant la continuité de session IP [16]. Les paquets des utilisateurs sont encapsulés dans les tunnels GTP, au niveau des interfaces eNodeB/SGW et SGW/PDN Gateway. Ces tunnels IP sont propres à chaque utilisateur et transmis à travers un transport UDP. La figure 3.1 représente deux types de tunnel GTP: le GTP-U qui se trouve dans le plan de transmission pour transporter les paquets de données de l'usager, et le GTP-C utilisé dans le plan de signalisation pour spécifier les fonctions de contrôle et de gestion des tunnels.

Dans la mise en œuvre de réseau, le GTP-U est utilisé dans les interfaces S5 et S11 alors que le GTP-C est utilisé sur les interfaces S1 et S5.

3.5.2 Mobile IP Protocol

Le MIP supporte le routage ininterrompu de paquets IP pour les appareils mobiles. Il a été défini à l'origine pour supporter les appareils et réseaux IPv4, et a ensuite été étendu pour supporter la technologie IPv6 [17]. Il permet d'assurer la continuité de la session à l'aide d'un Home Agent (HA), entité située dans le réseau de l'opérateur qui ancre l'adresse IP attribuée à l'appareil mobile (Home Address (HoA)). Le HA

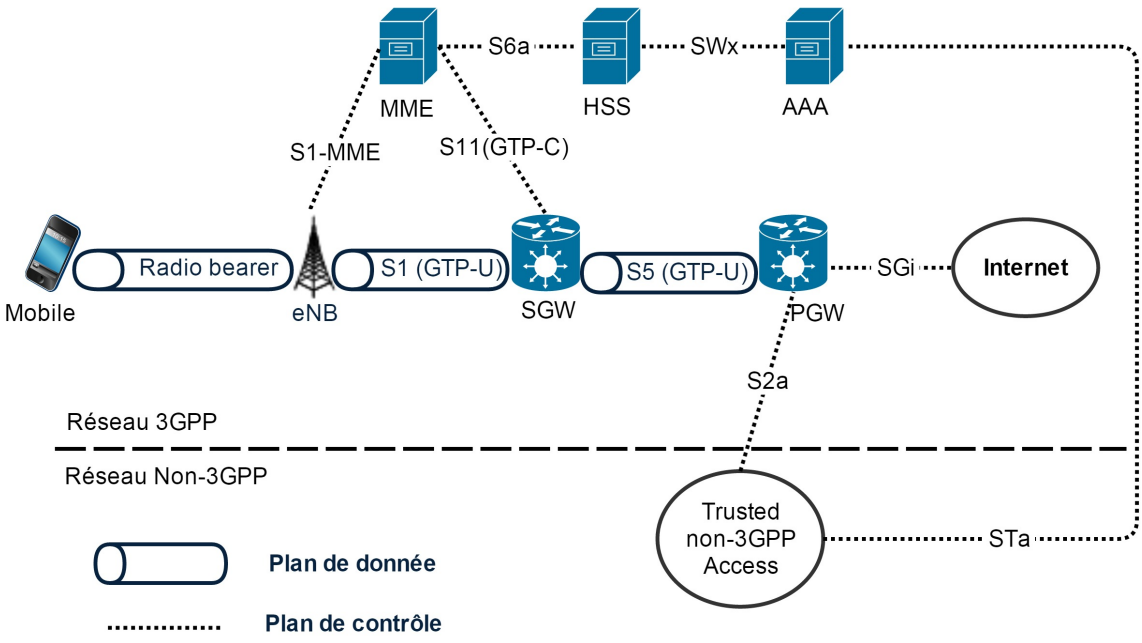

FIGURE 3.1 – Interface GTP en EPC.

maintient l'adresse HoA lors du déplacement de l'utilisateur. Le HA utilise une adresse IP temporaire ou bien une Care-of Address (CoA) pour localiser l'emplacement de l'utilisateur. Ainsi un tunnel IP bidirectionnel s'établit entre le client et le HA pour rediriger le trafic.

Proxy Mobile IP

PMIP et son extension IPv6, PMIPv6, sont des exemples de protocoles de mobilité IP qui facilitent le handover en conservant la même adresse IP de l'équipement usager lors du passage d'un réseau à un autre [18]. Il est considéré comme une extension de la mobilité sur la couche IP. L'architecture de réseau pour le protocole PMIP consiste en deux entités pour supporter la mobilité : le Mobile Access Gateway (MAG) et le Local Mobility Anchor (LMA).

Quand un équipement usager pénètre dans le domaine d'exploitation du PMIP il s'attache au MAG qui joue le rôle d'un lien d'accès. MAG assure la signalisation de la mobilité à l'utilisateur. Comme montré à la figure 3.2, le MAG envoie un message de mise à jour « Proxy Binding Update » contenant l'identité de l'équipement usager au LMA. À la réception de ce message, le LMA attribue un préfixe à l'UE, génère un lien Binding Cache Entry (BCE) et établit un tunnel bidirectionnel vers le MAG. Ensuite, le LMA envoie

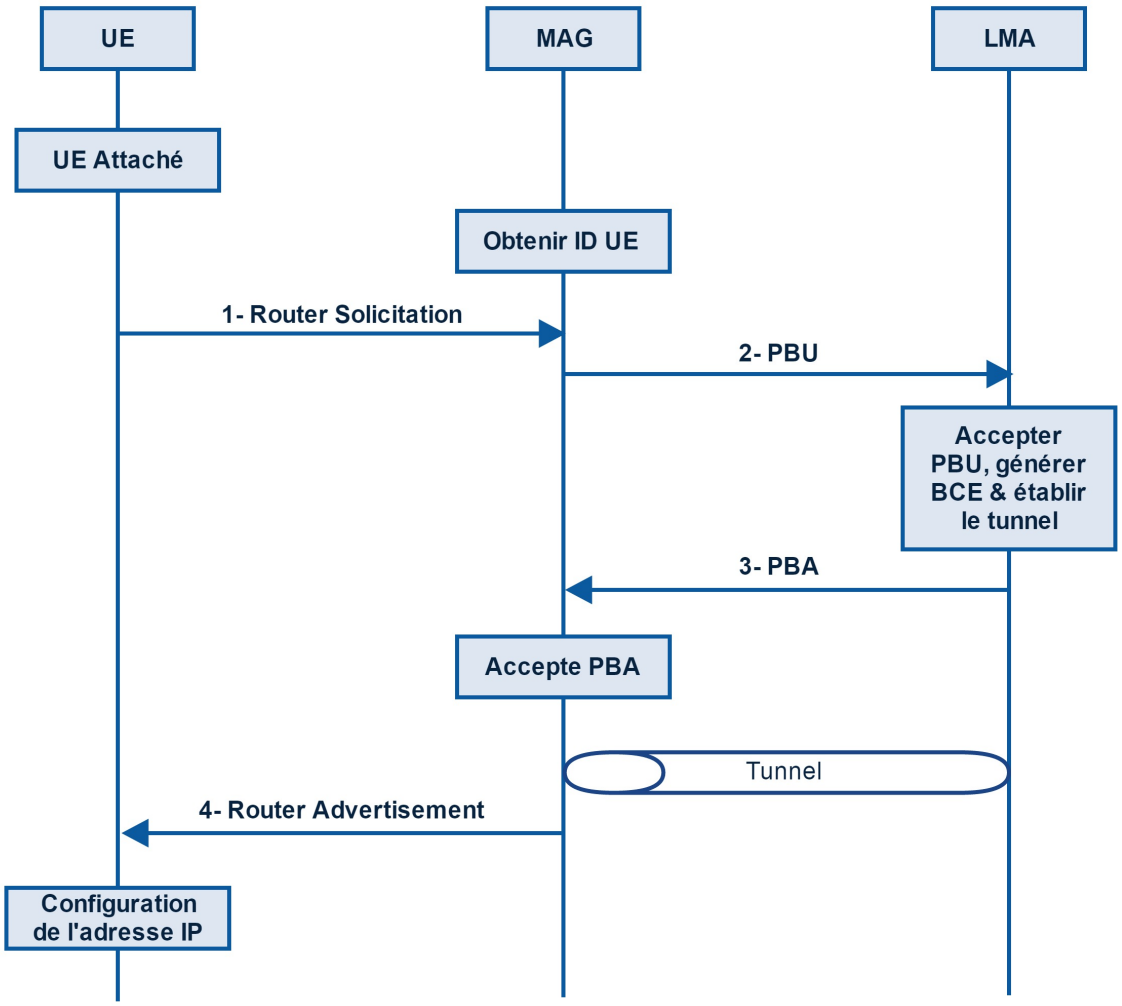

FIGURE 3.2 – Procédure de signalisation PMIP.

un message « Proxy Binding Acquittement » au MAG. Pour que l'équipement usager puisse s'attribuer une adresse, le MAG envoie un message « Router Advertisement » au UE contenant le préfixe attribué.

À chaque fois qu'équipement usager se déplace, un MAG détecte sa présence, assure la mise à jour de sa localisation et lui assigne le même préfixe. Cette méthode offre une mobilité transparente à l'équipement usager. L'adresse IP sera configurée au moment de l'accès au domaine de localisation.

Dual-Stack Mobile IP

DSMIP supporte plusieurs accès, dont 3GPP et non-3GPP sans les modifier et peut être utilisé dans les accès Trusted et Untrusted. DSMIPv6 est une nouvelle extension de MIPv6 où les fonctionnalités de mobilité

de base sont étendues pour supporter les deux technologies IPv4 et IPv6 [19]. Sa fonction principale est d'assurer la mobilité et de faciliter le transfert entre différents accès. Il est simple et plus efficace en terme de sécurité, comme IPsec est utilisé entre l'utilisateur et le Home Agent pour les applications IPv4 et aussi IPv6. En fait, l'utilisateur doit obtenir une Care-of Address (CoA) de la part du réseau d'accès (le CoA peut être IPv4 ou IPv6). L'utilisateur a toujours une Home Address (HoA) obtenue de la part de HA via IKEv2. Par la suite, l'équipement usager envoie un Binding Update (BU) avec le CoA au HA pour localiser l'emplacement de l'utilisateur et les données seront transférées au HA par un tunnel IP bidirectionnel.

3.6 Authentification Cellulaire/WLAN

Dans cette section nous décrivons la procédure d'authentification lors d'un transfert vertical entre accès 3GPP et non-3GPP. Plusieurs standards existent, comme le protocole Extensible Authentication Protocol-Authentication and Key agreement (EAP-AKA) ou le protocole EAP-SIM qui se base sur la carte SIM dans son mécanisme d'authentification. EAP-AKA est standardisé par le 3GPP ; il est basé sur la clé symétrique Universal Subscriber Identity Mobile (USIM) et réalise une authentification mutuelle entre l'équipement usager et le HSS. Ces méthodes d'authentification requièrent le soutien du mécanisme IEEE 802.1x. L'architecture d'intégration cellulaire WLAN représente l'interconnexion entre les différents serveurs d'authentification. La figure 3.3 montre l'architecture d'authentification lors d'un transfert vertical entre 3GPP LTE et WLAN.

Cette figure 3.3 montre un accès de confiance pour WLAN (Trusted WLAN access network). Dans le TWAN nous trouvons quelques fonctions [1]:

- WLAN Access Network (WAN) : représente les points d'accès sans fil où l'équipement usager peut se connecter via l'interface SWw en utilisant le standard 802.11.
- Trusted WLAN AAA Proxy (TWAP) : Cette entité communique avec le AAA et le WAN via l'interface STa.
- Trusted WLAN Access Gateway (TWAG) : Utilise l'interface S2a pour que l'utilisateur puisse avoir un accès à EPC.

TWAP est connecté au proxy 3GPP AAA via l'interface STa. Le proxy 3GPP AAA transfert la signalisation de l'authentification entre le TWAP et le serveur AAA via l'interface SWd. Le serveur AAA vérifie

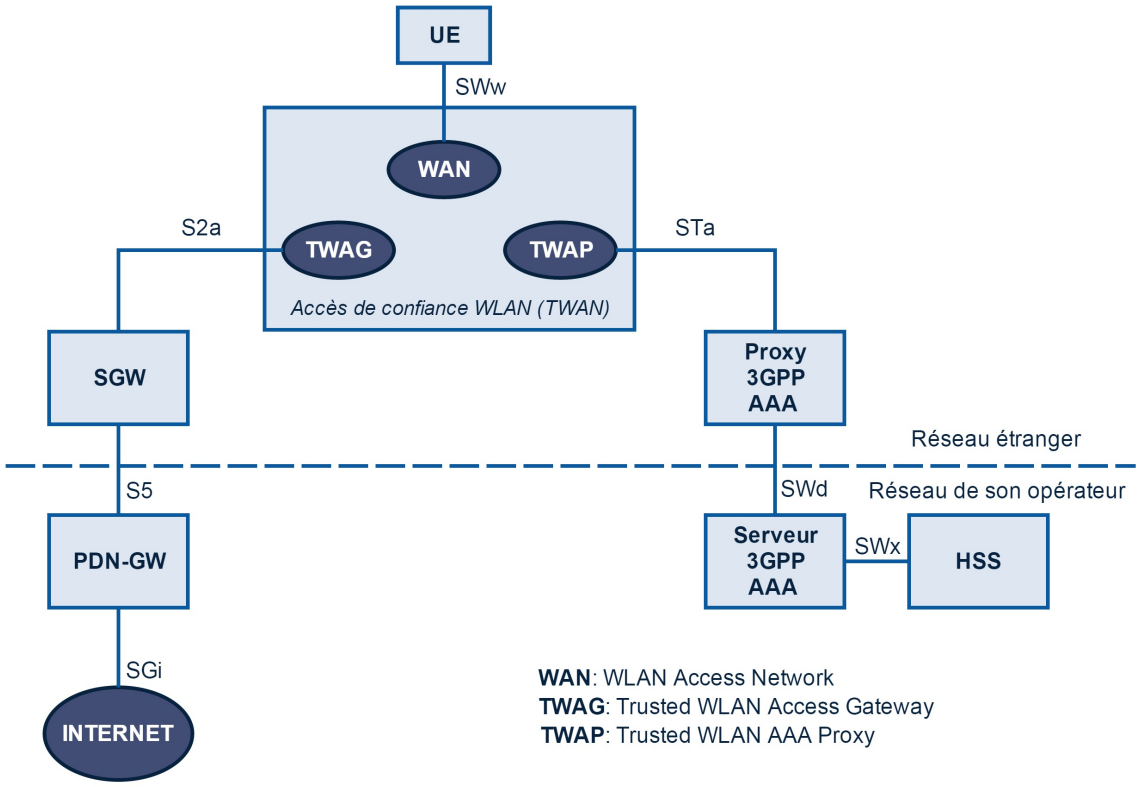

FIGURE 3.3 – Architecture d'authentification de 3GPP-WLAN.

si l'utilisateur est autorisé à utiliser le WLAN en contactant le HSS via l'interface SWx. La procédure d'authentification au complet est présentée ci-dessous dans la figure 3.4.

La méthode EAP-SIM/AKA supporte le 802.1x qui permet de crypter le contenu des communications dans l'accès [20]. Cette méthode est utilisée pour effectuer une authentification d'un équipement usager au moment de transfert du réseau cellulaire au WLAN à l'aide de l'identité de l'abonné et des informations d'authentification basées sur la carte SIM. EAP est constitué d'un nombre d'étapes qui réalisent l'authentification sans aucune action de l'utilisateur. La procédure d'authentification démarre lorsqu'un utilisateur s'approche à un point d'accès sans fil (WAP). Lors de l'initialisation, seule la procédure EAP over WLAN (EAPOW) 802.1x est autorisée entre l'équipement usager et le WAP. L'équipement usager envoie un message « EAPOW-start » au WAP pour déclencher le début de l'authentification. Ensuite, l'équipement usager et le WAP échangent deux messages « EAP-Request/Response » pour valider l'identité de l'équipement usager. Par la suite, les informations de l'identification de l'utilisateur sont livrées par le WAP dans une demande d'authentification EAP à travers un dialogue RADIUS. Ces informations incluent le International Mobile Subscriber Identity (IMSI) qui est stocké dans la carte SIM. En effet, le serveur AAA contacte le HSS/HLR

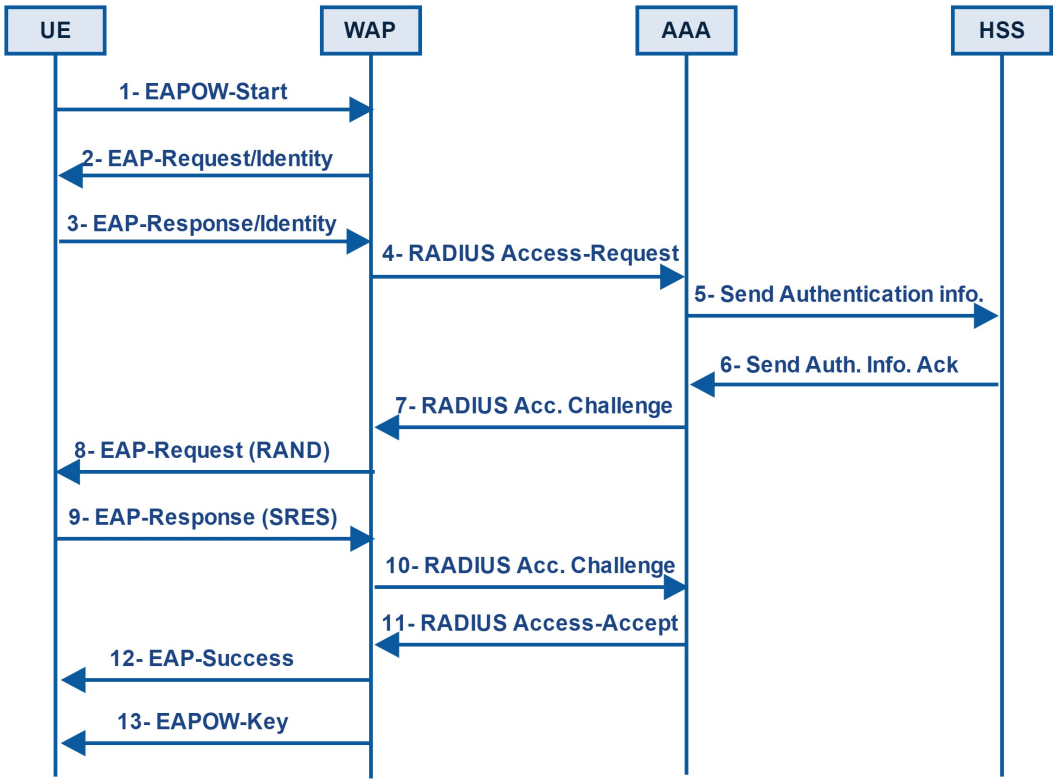

FIGURE 3.4 – Procédure d'authentification au moment de transfert cellulaire WLAN.

en utilisant le protocole Diameter et récupère les vecteurs d'authentification (LTE, UMTS ou bien GSM) qui sont utilisés pour authentifier le client. Ces vecteurs incluent des valeurs aléatoires RAND et les réponses attendues XRES (eXpected RESponse). Le RAND est envoyé à l'équipement usager dans les étapes 7 et 8, où il va utiliser l'algorithme d'authentification utilisé dans la carte SIM pour générer SRES. Après avoir généré le SRES, il sera transféré au serveur AAA qui va le comparer avec le XRES obtenu de HSS. Si les deux valeurs correspondent, alors l'authentification est réussie et un message « RADIUS access-accept » est envoyé au WAP. Dans l'étape 12, le WAP envoie un message « EAP-success » à l'équipement usager et un autre message « EAPOW-Key » pour configurer la clé de session (WEP).

3.7 Faiblesse d'authentification pour un roaming vertical

Plusieurs propositions ont été faites pour avoir une authentification sécurisée lors du transfert vertical de 3GPP au WLAN. Dans la partie précédente, nous avons décrit la procédure d'authentification EAP-AKA standardisée de 3GPP. EAP-AKA est bien connu comme un protocole d'authentification pour les

réseaux d'accès de confiance (Trusted), il permet d'établir une authentification mutuelle entre l'utilisateur et le HSS et de partager les clés de sécurité entre l'utilisateur et le serveur de WLAN. EAP-AKA possède jusqu'à aujourd'hui un délai de réauthentification très important considéré trop élevé pour les applications à temps réel dû au nombre de messages échangés entre les différentes entités (UE, HSS, AAA) contenant les informations d'authentification. Pour s'authentifier, l'utilisateur doit contacter le serveur AAA qui lui-même contacte le HSS qui réside dans le réseau de l'opérateur. En plus, une réauthentification complète doit être établie. La plupart des méthodes existantes (comme EAP-SIM/AKA) exigent la communication entre le UE et le serveur AAA qui accuse un grand délai et une vulnérabilité dans la phase de l'authentification. En plus de cela, et puisque la localisation du serveur AAA est loin des points d'accès sans fil (WAP), ce type de mécanisme peut affecter la performance du système par exemple par la perte de connexion entre le serveur AAA et le WAP.

3.8 Analyse critique

Nous présentons ici les travaux qui visent généralement à trouver une méthode rapide et sécurisée dans le cadre d'un roaming vertical entre LTE et WLAN. Parmi ces travaux, on peut citer l'article [21]. Dans cet article, l'auteur a proposé un schéma d'authentification uniforme qui peut être utilisé dans différents types de scénarios de mobilité entre l'E-UTRAN et les accès non-3GPP. Dans les faits, cette solution présente en réalité deux phases: la phase de préparation au transfert vertical et la phase d'authentification. Le but de la phase de préparation est d'intégrer un centre de génération de clés (KGC) dans l'architecture pour que les équipements usagers et les points d'accès obtiennent des clés privées. Cette procédure nécessite l'établissement d'un tunnel IPsec. Dans la deuxième phase, lorsque l'UE est connecté à un AP, une authentification mutuelle entre l'UE et le nouveau AP s'établit avant le roaming. Cette méthode ne peut pas réduire les délais de réauthentification à cause de l'échange de beaucoup de messages entre l'UE, l'AP et le KGC.

Dans l'article [22], les auteurs proposent un mécanisme d'authentification entre 3GPP-LTE et WLAN. Le protocole proposé peut atteindre deux objectifs : une authentification mutuelle entre l'UE et le WLAN, et obtenir une clé de session entre l'UE et l'AP. Ce travail demande des communications avec le serveur AAA. Ce dernier doit générer et stoker une clé locale (LK) qui va être utilisée dans la procédure de réauthentification. Tout comme la méthode du premier article, cette méthode a besoin de plusieurs échanges de messages entre l'UE et le serveur AAA et oblige l'UE à stoker et transmettre plusieurs informations.

Dans le travail [23] on traite aussi le problème d'authentification lors d'un roaming vertical. Cette méthode est proposée pour permettre au UE de réutiliser des informations d'authentification émis par le serveur AAA. Ces informations vont être transmises à base des tickets. Selon les auteurs de cet article, le système a besoin de plusieurs changements dans l'architecture. En plus, ce travail ne permet pas de réduire les délais de réauthentification car cette méthode a besoin toujours de communiquer avec le serveur AAA.

Les auteurs de [24] proposent une nouvelle méthode qui permet d'avoir une réauthentification rapide lors d'un roaming. Le protocole utilise les clés symétriques et exclut l'engagement du serveur AAA pour réduire la latence. Une authentification mutuelle s'implique ici entre l'UE et les points d'accès. De ce fait, le schéma demande une capacité de stockage très élevée en obligeant l'UE de stocker plusieurs informations.

Un autre mécanisme, proposé dans [25], exclut aussi l'engagement d'une tierce partie. Ce travail a pour but de distribuer des tickets d'authentification pour l'EU pendant l'authentification initiale. Lors d'un roaming, l'utilisateur peut utiliser le ticket pour avoir une authentification mutuelle avec le point d'accès sans contacter une tierce partie. Cependant, il existe des problèmes de sécurité. En fait, dans la partie analyse de sécurité, les auteurs ont validé la sécurité de l'authentification mutuelle entre l'UE et le point d'accès, et ils ont abandonné le secret de la clé partagée.

En résumé, les travaux présentés ci-dessus résolvent la même problématique en essayant de trouver un schéma d'authentification rapide et sécurisé dans le cadre d'un roaming vertical entre LTE et WLAN. Les trois première propositions [21], [22] et [23], ont besoin de la participation d'une tierce partie ce qui va nous conduire à échanger un grand nombre de messages et à augmenter la complexité du système. Néanmoins, les travaux proposés dans [24] et [25] présentent autres types de problèmes comme l'inefficacité ou bien les vulnérabilités en matière de sécurité pour satisfaire les objectifs primordiaux qu'un protocole sécuritaire ait besoin comme l'intégralité, la confidentialité et la disponibilité des données.

Le but de notre travail est de résoudre la même problématique en essayant de réduire la latence et le nombre de messages échangés en utilisant les opérations des clés symétriques et en éliminant de participation d'une tierce partie. En plus, notre schéma offre les propriétés de sécurité nécessaires pour avoir une protection contre différents types d'attaques contre lesquelles un protocole d'authentification doit se prémunir.

3.9 Conclusion

Dans ce chapitre, nous avons discuté la méthode d'authentification existante pour un transfert vertical. Ce schéma permet de fournir un transfert transparent entre le cellulaire et le Wi-Fi. Comme le 3GPP a suggéré le support de la mobilité entre le cellulaire et le non-3GPP qui exige des méthodes de réauthentification complète et distinctes pour différents scénarios de mobilité qui nécessitent l'échange de nombreux messages et augmentent la complexité du système. Nous devons penser à une méthode qui permet d'avoir une authentification rapide et sécurisée. Cette méthode doit faciliter l'intégration cellulaire WLAN en supportant la mobilité.

Chapitre 4

Mécanisme proposé

4.1 Introduction

Plusieurs solutions ont été proposées pour améliorer la mobilité, l'objectif final étant de diminuer le temps de handover lors d'un roaming vertical entre réseau cellulaire et WLAN pour minimiser l'impact sur la continuité de service. Néanmoins ces propositions n'offrent pas, à ce point, les performances souhaitables: chaque mécanisme a ses propres avantages et inconvénients.

Dans ce chapitre, nous proposons une nouvelle méthode d'authentification sécurisée et rapide lors d'un roaming vertical entre cellulaire et WLAN.

4.2 Présentation générale

Nous avons vu que le 3GPP a suggéré le soutien de la mobilité entre l'E-UTRAN et le réseau d'accès Non-3GPP [14]. Ceci nécessite d'implémenter la procédure d'authentification complète entre l'utilisateur et le réseau d'accès sans fil. Ceci va conduire à augmenter la complexité du système d'une part, et d'avoir un retard de transfert automatique dû aux nombreux messages échangés entre les différentes entités pour contacter le serveur AAA d'autre part.

L'authentification dans le domaine de l'intégration cellulaire/WLAN est l'un des défis majeurs auquel l'opérateur doit faire face pour maintenir la continuité de la session lors du passage d'un accès à un autre.

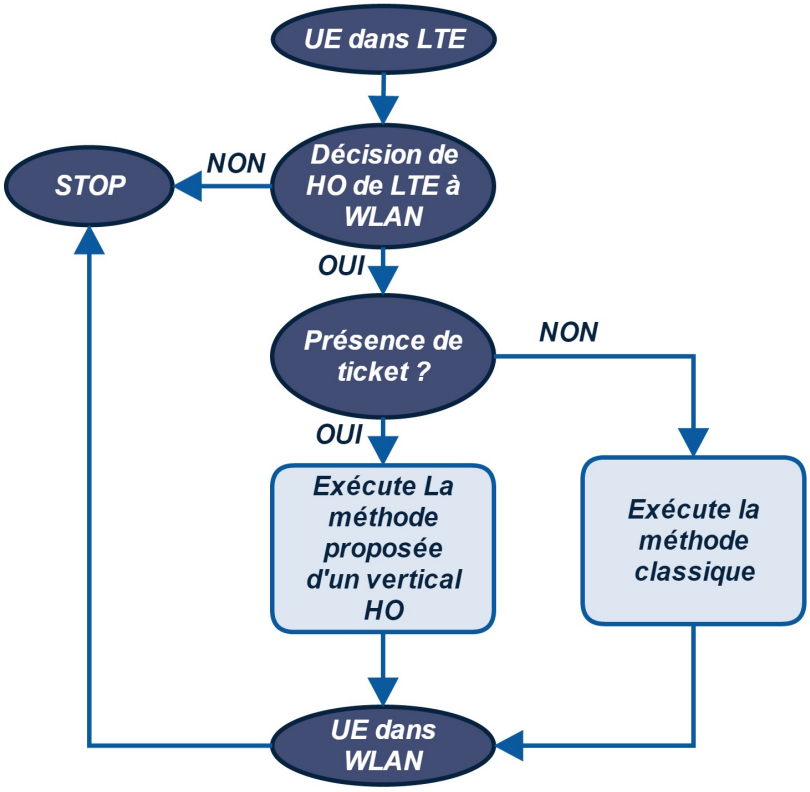

FIGURE 4.1 – Procédure d'authentification lors d'un transfert de LTE à WLAN

Notre mécanisme est inspiré de [24], [25], [26] et [27] qui utilisent des méthodes d'authentification basées sur les tickets. Ainsi, nous proposons une méthode d'authentification plus rapide et plus efficace que les méthodes existantes qui permet d'accélérer l'authentification en réduisant les délais de réauthentification lors de la mobilité de l'utilisateur du réseau LTE vers le WLAN sans avoir d'interruption de service. Cela se fait en donnant l'autorisation à l'UE d'accéder au réseau WLAN en présentant certaines informations. Pour réaliser cet objectif, l'eHSS distribue d'abord des tickets au UE; ensuite ce dernier et le point d'accès sans fil s'authentifient mutuellement. La figure 4.1 présente la procédure d'authentification lors d'un roaming vertical d'un accès LTE à un accès WLAN. Une fois que l'UE reçoit les informations nécessaires pour prendre la décision de transfert il exécute le mécanisme d'authentification proposé.

En fait, le protocole proposé permet de réaliser deux objectifs:

- Une authentification mutuelle entre l'UE et le réseau d'accès WLAN après un transfert vertical automatique avec un faible coût de latence (Overhead en terme de délai).
- La dérivation d'une clé de session entre l'UE et le point d'accès sans fil pour assurer la sécurisation de la communication.

Par l'utilisation d'une clé symétrique et l'élimination de la participation d'une tierce partie dans notre proposition, nous réduisons le nombre de message échangés entre les différentes entités du système. La plupart des opérations cryptographiques seront effectuées entre l'eHSS et les points d'accès. De plus, les calculs sont effectués d'une manière simple avec l'utilisation de quatre fonctions principales [28] :

- Cryptage ou fonction de chiffrement.
- Décryptage ou fonction de déchiffrement.
- Hachage : aussi appelé fonction de hachage à sens unique ou « one-way hash function ». C'est une fonction de cryptographie qui permet de calculer une empreinte servant à authentifier rapidement la donnée source.
- Code d'authentification de message (MAC) : un code qui permet de vérifier l'identité de la source pour empêcher la réception d'un message provenant d'une source fraudeuse [29]. Le MAC permet aussi de protéger des données pour éviter les risques de modification.

4.3 Description de la méthode proposée

La solution proposée se base sur deux phases : une première qui consiste en la préparation d'un futur transfert automatique vertical, où l'eHSS prépare des tickets pour chaque réseau pour lequel un point d'accès sans fil (WAPi) se trouve dans le secteur de couverture d'eNB. Ensuite, l'eHSS envoie ces tickets chiffrés à l'utilisateur qui doit les décrypter et les stocker pour une prochaine utilisation dans la possibilité d'un déplacement dans une zone dans laquelle se trouve un autre point accès sans fil appartenant au même réseau WLAN. Chaque ticket contient l'identité de l'UE, le nom du réseau sans fil (SSID), une clé d'authentification, un nombre aléatoire choisi par l'eHSS et le temps d'expiration du ticket. Dans la deuxième phase, l'utilisateur exploite ces tickets pour réaliser une authentification mutuelle avec un des points d'accès sans fil, c.-à-d. que les enitités participantes vérifient leur identité réciproque. Cette étape est basée sur la génération d'un code d'authentification de message entre les deux entités.

Après l'envoi des trois messages entre les deux entités, la connexion s'établit et l'utilisateur peut recevoir les données protégées par une clé de session générée par les deux entités.

Le tableau 4.1 représente les différentes notations utilisées dans la solution.

Tableau 4.1 – Tableau de définition des notations

Notation	Définition
MK	Clé maîtresse
SSID	Nom de réseau sans fil (service set identifier)
Q	Clé d'authentification
ID_x	Identité de x
H()	Fonction de hachage sécurisée
$H_k()$	Fonction de hachage sécurisée basée sur la clé secret k
T_i	Ticket de Handover
G	Générateur
T_{exp}	Temps d'expiration
$ENC_k()$	Fonction de chiffrage en utilisant la clé symétrique k
$DEC_k()$	Fonction de déchiffrage en utilisant la clé symétrique k
$MAC_k()$	Code d'identification de message en utilisant la clé symétrique k
|	Concaténation

4.3.1 Préparation au futur transfert automatique vertical

La première phase est une phase de préparation au transfert automatique vertical. Dans cette étape, l'utilisateur a déjà accompli la procédure d'authentification complète d'accès au réseau LTE avant son transfert à l'accès Wi-Fi, ce qui signifie qu'on a une relation de confiance entre les différentes entités de notre architecture. La figure 4.2 et les étapes suivantes décrivent en détails cette phase:

Étape préliminaire:

Dans notre travail, on considère qu'il existe une relation de confiance à l'intérieur de l'architecture c.-à-d. entre l'UE, le WLAN via les points d'accès et son serveur AAA et l'eHSS. Les différentes entités forment une zone sécurisée. L'UE et l'eHSS possèdent une clé maîtresse MK_{UE} partagée entre eux et dont la génération n'est pas importante ici. Les WLANs via le serveur AAA génèrent aussi d'une autre côté les clés maîtresses MK_{SSIDi} pour chaque réseau.

Étape 2:

eNB –> eHSS : (ID_{UE}, $SSID_i$)

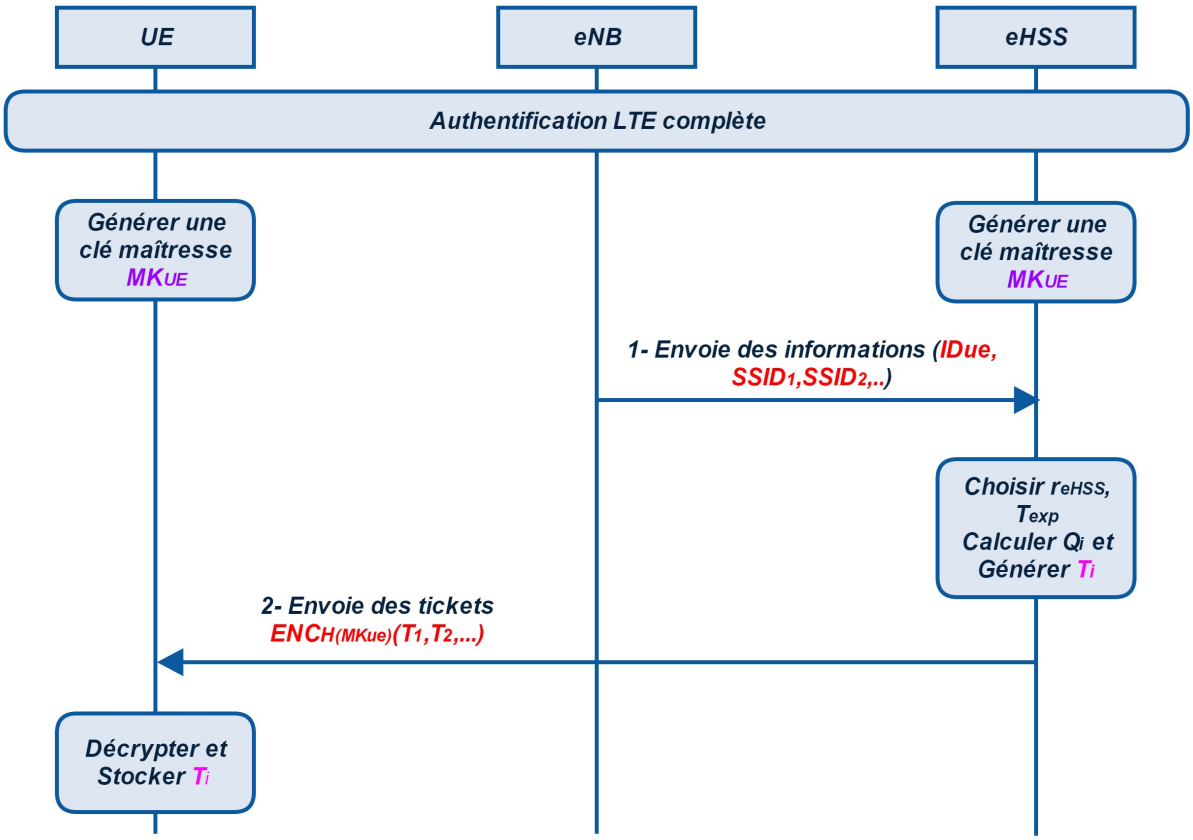

FIGURE 4.2 – Préparation au futur Handover

Dans cette étape, l'eHSS distribue les tickets relatifs à chaque WLAN pour l'UE. Pour simplifier notre proposition, on suppose que l'eNB connait les informations (identités, localisations) des WLAN qui sont dans sa zone de couverture et leur SSID [30] .

L'eNB envoie les $SSID_i$ des WAPs voisins et l'identité de chaque utilisateur en itinérance verticale (ID_{UE}, $SSID_1$, $SSID_2$, ..) à l'eHSS. Ce dernier reçoit la liste des WAPs qui sont dans le secteur de couverture d'eNB où l'UE est connecté au réseau cellulaire.

Étape 3:

L'eHSS reçoit (ID_{UE}, $SSID_1$,$SSID_2$, ...) puis choisit un nombre aléatoire r_{eHSS} appartenant à $\mathbb{Z}$* et un temps d'expiration du ticket T_{exp}. Ensuite il utilise les clés maitresses MK_{SSIDi} de la WAP en question pour calculer les clés d'authentification (Q_i) en utilisant l'équation 4.1.

$$Q_i = H_{MKssid}(ID_{UE}|SSID_i|T_{exp}|r_{eHSS})\,. \tag{4.1}$$

$$T_i = (Q_i, ID_{UE}, SSID_i, T_{exp}, r_{eHSS})\,. \tag{4.2}$$

Q_i est une clé d'authentification qu'on utilisera dans un futur transfert vers le WLAN. On obtient cette clé en appliquant la fonction de hachage $H_{MK}()$ sur (ID_{UE}, $SSID_i$, T_{exp}, r_{eHSS}) en utilisant la clé secrète MK_{SSIDi}.

Une fois que les clés d'authentification sont disponibles, l'eHSS génère les tickets T_i pour chaque point d'accès sans fil en utilisant l'équation 4.2.

Étape 4:

eHSS –> UE : (T_i)

L'eHSS envoie les tickets cryptés en utilisant l'équation 4.5 et la clé MK_{UE} à l'UE. L'UE est donc la seule entité qui est capable de connaitre les tickets (T_1, T_2,...).

$$E = ENC_{H(MK)}(T_i)\,. \tag{4.3}$$

Étape 5:

L'UE reçoit les tickets et les décrypte avec l'équation 4.4 puis les stocke pour une utilisation future.

$$T_1|T_2|... = DEC_{H(MK)}(E)\,. \tag{4.4}$$

L'UE stocke les T_i pour les réutiliser lors d'un déplacement vers un WAP. Si les tickets expirent avant leur utilisation, l'utilisateur peut faire les mêmes étapes expliquées en haut pour avoir d'autres tickets. Comme on le remarque dans les étapes de la phase de préparation d'un futur transfert automatique vertical, l'eNB envoie les $SSID_i$ des WAPs voisins et l'identité de chaque utilisateur donc l'eHSS a déjà (ID_{UE}, $SSID_1$,$SSID_2$, ...). Dans ce cas, si un ticket expire, les opérations en cours ne peuvent pas être interrompues. Donc, si une connexion a été mise en place où le ticket est en cours d'utilisation, la validité n'a plus d'importance. Les tickets ne sont utilisés que pour avoir une nouvelle authentification. Néanmoins, si un ticket expire avant d'être utilisé, l'utilisateur obtient le nouveau ticket en suivant les mêmes étapes.

Communication entre les entités AAA et eHSS

La communication entre le serveur AAA et le eHSS se fait via l'interface Wx en utilisant le protocole Diameter [30], conformément à l'architecture existante. Diameter est un protocole qui peut être modifié ou étendu grâce à sa flexibilité par l'ajout de nouvelles applications, des commandes et des AVPs (Attribute Value Pair) qui désignent une structure de données ouverte qui permet de transporter les données relatives aux extensions. Les AVPs peuvent transporter des données de différents types (entiers, chaines de caractères...) et sont embarqués, individuellement ou en agglomérat, dans les messages. Diameter fournit les mécanismes nécessaires pour effectuer un transport fiable, délivrer les messages et réaliser des négociations. Dans notre cas, le rôle principal de l'interface Wx est d'échanger les données nécessaires entre les entités AAA et eHSS pour la communication des tickets. Dans notre étude, nous adoptons les hypothèses suivantes:

- La relation de confiance entre le serveur AAA et l'entité eHSS est une relation qui peut être établie pour une longue durée c.-à-d. une relation d'affaires à long terme, dont la gestion ne rentre pas en considération ici.
- L'autorisation d'accès aux usagers dans le réseau est un processus ponctuel, établi avant la possibilité de roaming, et dont l'effet dure au-delà du roaming et dans ce sens nous considérons qu'il a été réalisé par les moyens traditionnels. Ce processus est obligatoire pour identifier les utilisateurs en vérifiant leur identité.

L'échange des tickets, par contre, est un processus récurant à court terme, car les tickets doivent être renouvelés une fois expirés. Le temps d'expiration du ticket est un paramètre à spécifier. Cette entité doit choisir le temps de début et de fin de chaque ticket. La durée de vie des tickets dépend non seulement de la robustesse des mécanismes, mais a un impact sur la capacité du eHSS selon le nombre d'utilisateurs, car

Tableau 4.2 – Nouvel AVP

Message	Interface	Nouveau AVP	Type d'AVP	Description
PPA	Wx	Ticket	Grouped	Contiens les donnés des tickets

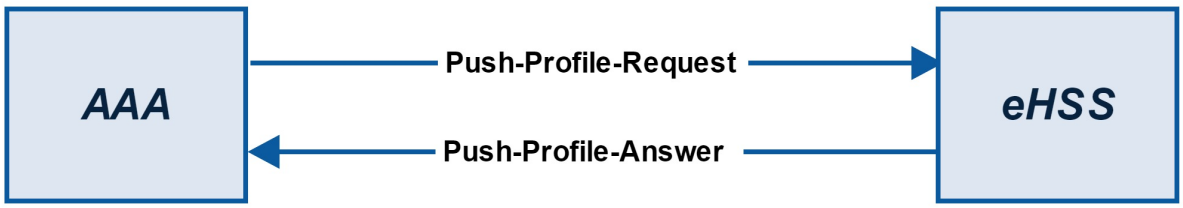

FIGURE 4.3 – Procédure de communication avec Diameter

le renouvellement des tickets implique un échange d'information additionnel entre les différentes entités, ce qui peut créer une charge de calcul significative en plus d'un volume d'échange important.

Notre objectif est de communiquer les tickets entre les entités eHSS et AAA. Etant donné que les tickets ont un temps d'expiration, l'eHSS doit les envoyer au serveur AAA chaque fois qu'il génère de nouveaux tickets. Le protocole Diameter offre les commandes « Push-Profile-Request » et « Push-Profile-Answer » qui peuvent être exploitées dans cette procédure d'intercommunication en y ajoutant de nouveaux AVPs (Voir la figure 4.3). Le « Push-Profile-Request (PPR) » est envoyé par le serveur AAA à l'entité eHSS pour télécharger les tickets, alors que le « Push-Profile-Answer (PPA) » est envoyé par l'entité eHSS au serveur AAA pour répondre à la commande « Push-Profile-Request ». Les mises à jour des tickets vont être transportées dans les AVPs et nous aurons plusieurs AVP dans le « Push-Profile-Answer (PPA) » et chaque AVP concerne un utilisateur. Le tableau 4.2 représente les nouveaux AVP ajoutés dans les messages de type « Push-Profile-Answer (PPA) ».

Nous supposons que la demande des tickets de serveur AAA à l'entité eHSS se fait spontanément, et périodiquement. Chaque période du temps, le serveur AAA doit envoyer une requête à l'entité eHSS pour lui demander des nouveaux tickets. Ces derniers pourront soit appartenir à de nouveaux utilisateurs qui viennent d'entrer dans le réseau, soit être le renouvèlement de tickets expirés pour des usagers toujours actifs. Essayons de déterminer le volume de trafic que ceci encourt entre le AAA et le eHSS. Rappelons d'abord que la durée de vie de chaque ticket est choisie pour assurer la sécurité de notre mécanisme contre différents types d'attaques. D'autre part, augmenter la durée de l'intervalle entre chaque requête pour de nouveaux tickets augmente la probabilité qu'un usager ne puisse se connecter immédiatement au réseau, en attendant que son ticket soit communiqué.

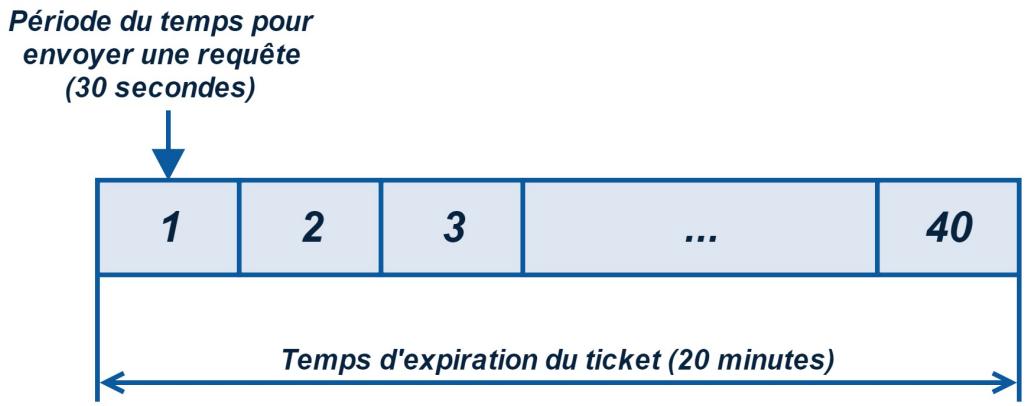

FIGURE 4.4 – Période du temps pour envoyer une requête

Appelons d la durée de vie moyenne de chaque ticket, p la période de rafraichissement des tickets, n le nombre de tickets et t la taille d'un ticket. Le débit d'information sera en conséquence :

$$D = \frac{n * t * p}{d}. \tag{4.5}$$

Choisissons d = 20 minutes, et fixons à 30 secondes la période du temps pour envoyer chaque requête, comme illustré sur la Figure 4.4. Ceci, pour 1000 tickets de 100o chacun (en intégrant l'overhead du protocole), résulte en un débit moyen de 4Mo par seconde, qui reste une charge raisonnable. Cette opération peut donc être coûteuse en termes de communication grâce à la demande périodique des données sur les tickets mais ceci est le prix à payer pour avoir des informations fraîches qui permettent d'atteindre une authentification automatique, en réduisant le risque pour l'usager d'avoir un temps d'attente.

Par ailleurs, la durée de vie du ticket est critiquable. Si on se réfère à certaines utilisations dans les services de Microsoft, par exemple, un ticket aura une durée de vie minimale de 10m et une longévité par défaut de 600m, ou 10h. Notre choix de 20m est donc agressif et on pourrait fixer une durée de vie journalière ou bi-journalière, ce qui diminuerait le volume de données d'un ordre de grandeur.

Le tableau 4.3 représente la liste des messages. Un message peut être une requête ou une réponse. Il consiste en un entête suivi par les AVPs. Les commandes entre des accolades représentent les AVPs de base qui peuvent être utilisés pour le routage où nous trouvons le « Hostname » et « le nom de domaine », alors

Tableau 4.3 – Liste des messages

	Messages
PPR	< Push-Profile-Request > ::= < Diameter Header: 305, REQ, 16777265 > < Session-Id > { Vendor-Specific-Application-Id } { Auth-Session-State } { Origin-Host } { Origin-Realm } { Destination-Host } { Destination-Realm } { User-Name } ***[Ticket-REQ]** *[AVP] *[Proxy-Info] *[Route-Record]
PPQ	< Push-Profile-Answer > ::=< Diameter Header: 305, 16777265 > < Session-Id > { Vendor-Specific-Application-Id } [Result-Code] [Experimental-Result] { Auth-Session-State } { Origin-Host } { Origin-Realm } ***[Ticket-ANS]** *[AVP] *[Proxy-Info] *[Route-Record]

que les commandes entre des crochets représentent les AVPs au niveau de la session qui ont des nouvelles fonctions. L'étoile est pour dire que nous pouvons avoir un ou plusieurs AVP.

Comme le nous remarquons dans le tableau 4.3, nous avons encapsulé les AVPs « Ticket-REQ » et « Ticket-ANS » dans les messages utilisés dans notre solution. Nous ajoutons pour chaque utilisateur un « Ticket-REQ » dans le message « Push-Profile-Request (PPR) » et « Ticket-ANS » dans le message « Push-Profile-Answer (PPA) » ce qui nous permet d'avoir plusieurs tickets, un pour chaque utilisateur. Le « Ticket-REQ » est un AVP envoyé par le serveur AAA à l'entité eHSS pour demander les données sur les tickets. Il est présenté par le type de données « OctetString » qui transporte le nom du réseau sans fil ($SSID_i$). Chaque fois que le serveur AAA se rend compte qu'un ticket a expiré, il émet une requête « Push-Profile-Request » à l'eHSS qui doit envoyer le nouveau ticket avec un nouveau temps d'expiration du point d'accès en question. Le « Ticket-REQ » est capable d'envoyer la demande d'un ou plusieurs tickets

lorsqu'il se rend compte que plusieurs tickets expirent en même temps. Le « Ticket-ANS » est un AVP capable de transporter les tickets qui peuvent être représentés par le type « Grouped ». « Grouped » est un type de données qui permet d'encapsuler plusieurs AVPs fils dans un AVP père qui est en l'occurrence le Ticket-ANS. Chaque AVP fils représente un champ du ticket. Chaque ticket est composé de cinq champs: la clé d'authentification (Q_i), l'identité de l'équipement usager (ID_{UE}), le nom du réseau sans fil ($SSID_i$), le temps d'expiration de ticket (T_{exp}) et la valeur aléatoire (r_{eHSS}). Chaque champ peut être représenté par le type de donnés «OctetString ». Ces champs de données sont rassemblés en séquence d'AVP.

A la fin de cette séquence, on est prêt pour un futur roaming. La préparation des tickets se fait lorsque l'UE est déjà authentifié au réseau LTE où la relation de confiance est établie entre les différents entités du réseau. Cette première phase nous permet d'accélérer la procédure d'authentification de handover à la deuxième phase, que nous allons décrire maintenant.

4.3.2 Mécanisme d'authentification

Cette phase présente la phase d'authentification pour un transfert automatique vertical. L'UE se déplace et peut se trouver dans une situation telle qu'un transfert à un WLAN est possible. Une authentification mutuelle doit s'établir, c-à-d. que l'UE doit authentifier le réseau et le réseau doit authentifier l'UE. La figure 4.5 représente une poignée de main (3-way handshake) entre l'UE et le WAP correspondant. Le processus d'authentification de transfert est décrit comme suit :

Étape 1:

UE –> WAP_i : (ID_{UE}, $SSID_i$, R_{UE}, r_{eHSS}, T_{exp})

L'UE choisit un nombre aléatoire R_{UE} appartenant à $\mathbb{Z}^*$ et calcule R_{UE}= $G\ r_{UE}$ (G est un générateur). Après la génération de R_{UE}, l'UE trouve le ticket correspondant au point d'accès sans fil ayant la puissance de signal la plus élevée puis il lui envoie les ID_{UE}, $SSID_i$, R_{UE}, r_{eHSS} et le T_{exp}.

Étape 2:

À la réception de ces données, le WAP_i vérifie tout d'abord le $SSID_i$ et le temps d'expiration du ticket. Une fois que cette procédure est validée, le WAP calcule la clé d'authentification Q_i avec la clé maîtresse

MK_{SSIDi} en utilisant l'équation 4.1. À ce niveau, Q_i est considérée comme une clé d'authentification entre l'UE et le WLAN.

Après cette étape, le WAP choisit un nombre aléatoire r_{WAP} appartenant à $\mathbb{Z}^*$ et calcule R_{WAP}= G r_{WAP}.

Étape 3:

Le WAP calcule maintenant le message K_{WAP} en utilisant l'équation 4.6; après il utilise l'équation 4.7 pour calculer le MAC_1 de ce message en utilisant la clé secréte Q_i.

$$K_{WAP} = SSID_i|R_{WAP}|R_{UE}\,. \tag{4.6}$$

$$MAC1_{Qi}(K_{WAP}) = H_{Qi}(K_{WAP})\,. \tag{4.7}$$

Étape 4:

WAP –> UE : ($MAC1_{Qi}(K_{WAP})$, K_{WAP})

WAP envoie $MAC1_{Qi}(K_{WAP})$ et le message K_{WAP} au UE. Dans ce cas , l'UE vérifie le R_{UE} envoyé dans le message et utilise le message K_{WAP} pour calculer le MAC_1' en utilisant la clé d'authentification Q_i stockée dans le ticket. Une fois que le MAC_1' et le MAC_1 concordent, l'UE génère la clé de session SK_i selon la formule 4.8.

$$SK_i = R_{UE}\, r_{WAPi}\,. \tag{4.8}$$

Étape 5:

L'UE calcule le message K_{UE} en utilisant l'équation 4.9; après il utilise l'équation 4.10 pour calculer le MAC_2 de ce message en utilisant la clé secréte Q_i.

$$K_{UE} = ID_{UE}|R_{UE}|R_{WAP}\,. \tag{4.9}$$

$$MAC2_{Qi}(K_{UE}) = H_{Qi}(K_{UE})\,. \tag{4.10}$$

Étape 6:

UE –> WAP : ($MAC2_{Qi}(K_{UE})$, K_{UE})

À la réception de $MAC2_{Qi}(K_{UE})$ et du message K_{UE}, le WAP vérifie le R_{WAP} dans le message K_{UE} et utilise ce message pour calculer MAC_2' avec la clé Q_i calculée auparavant. Dès que MAC_2' est disponible, il est comparé avec MAC_2. Une fois que c'est validé, le WAP génére la clé de session SK_i comme indiqué dans la formule 4.11.

$$SK_i = R_{WAPi}\, r_{UE}\,. \tag{4.11}$$

Après la poignée de main, les différentes entités ont validé leur identité mutuelle. La connexion s'établit et l'utilisateur peut recevoir les données sous une clé de session générée par les deux entités.

Cette méthode peut être utilisée dans tout type de mobilité entre E-UTRAN et un accès non-3GPP qui doit être de confiance (trusted). En plus, notre proposition peut être appliquée entre plusieurs points d'accès sans fil connectés à différents EPCs.

4.4 Conclusion

Dans ce chapitre, nous avons présenté comme une contribution majeure une méthode d'authentification pour un transfert automatique vertical entre le 3GPP et le WLAN. Cette proposition est basée sur la distribution des tickets qui facilite l'intégration cellulaire/Wi-Fi. Les tickets sont générés en utilisant la clé maîtresse

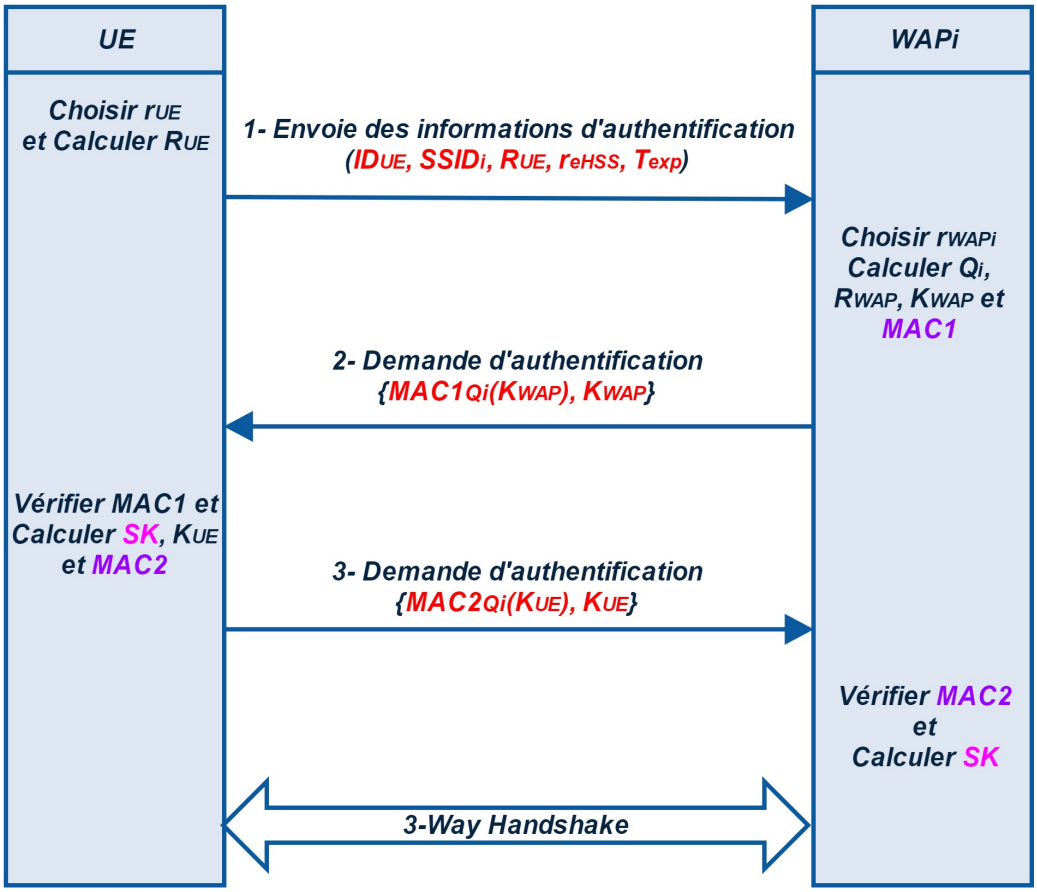

FIGURE 4.5 – Mécanisme d'authentification

entre l'eHSS et l'UE. Avec ce ticket, l'UE peut se connecter à un WAP sans communiquer avec une tierce partie. Réduire les délais d'authentification lors d'un roaming vertical nous permet de diminuer l'impact sur la continuité de service et de satisfaire les applications à temps réel comme la voix sur IP.

Dans la section suivante nous allons montrer que notre mécanisme peut jouer un rôle pour diminuer les délais de réauthentification lors de la mobilité de l'utilisateur du réseau cellulaire vers Wi-Fi. L'analyse de sécurité joue aussi un rôle très important pour montrer que notre proposition offre une sécurité contre plusieurs attaques.

Chapitre 5

Analyse de sécurité et évaluation des performances

5.1 Introduction

Le ticket est simplement un moyen de distribuer l'information de sécurité qui, dans notre contexte, protège la confidentialité des utilisateurs et contribue à la réduction de latence de la réauthentification lors d'une transition verticale entre un réseau cellulaire et un réseau WLAN. En effet, pour implémenter un mécanisme d'authentification, il faut que ce dernier offre les propriétés de sécurité nécessaire pour avoir une protection contre différents types d'attaques et offre également des bonnes performances au niveau des délais d'authentification pour réduire la latence.

Dans ce chapitre nous présentons l'analyse de sécurité de notre proposition. Nous commençons par décrire les différents types d'attaques existants et nous présentons ensuite les résultats des analyses de sécurité de notre proposition. Puis, nous dévoilons les métriques d'évaluation et les méthodes utilisées pour les mesures. Finalement, nous discutons les résultats obtenus.

5.2 La sécurité des réseaux

5.2.1 Principales attaques dans les réseaux mobiles

L'attaque la plus simple contre laquelle il faut se prémunir est l'écoute, la possibilité d'intercepter des conversations. L'usurpation d'identité est l'une des attaques les plus dangereuses dans les réseaux informatiques : l'attaquant emprunte l'identité de sa victime avec tous les privilèges qui lui sont associés. Ceci n'est pas limité à une simple retransmission des messages interceptés de sa victime, mais inclut également forger des messages en utilisant l'identité de sa victime [31]. Cette attaque peut être liée à l'attaque *Man-In-The-Middle* (MITM) où la communication entre la source et la destination est relayée par un intermédiaire malicieux qui peut accéder à et potentiellement modifier le contenu de la communication à son gré. Pour assurer sa réussite, l'attaquant joue le rôle de la source aux yeux du destinataire et le rôle de destinataire aux yeux de la source. Typiquement, l'attaque se limite à usurper uniquement l'identité de l'un des deux rôles pour ainsi lire les messages et les retransmettre au bon destinataire. L'attaquant a la possibilité de modifier subrepticement les messages envoyés par la victime dont l'identité a été usurpée. L'attaque MITM est une vulnérabilité commune des protocoles ne pouvant assurer qu'une authentification faible.

Les dénis de service (DoS) constituent une catégorie d'attaques différentes, très fréquentes dans lesquelles l'attaquant épuise suffisamment les ressources de la victime pour que cette dernière n'ait plus la possibilité de répondre aux requêtes légitimes [32]. De telles attaques sont dues à l'inondation ou une mauvaise implémentation du protocole ou du service. L'inondation est une attaque généralement répartie (DDoS) par laquelle plusieurs nœuds envoient continuellement de nombreuses requêtes vers la victime ciblée sans attendre de réponse. Ces requêtes visent une opération demandant un temps de calcul important et un grand nombre de ressources. Elle est extrêmement difficile, voire impossible à bloquer vu sa nature légitime qui n'exploite aucune faille. Le second type d'attaques DoS vise une faiblesse dans l'implémentation des protocoles ou services s'exécutant sur la victime et qui n'exige pas la participation de plusieurs nœuds. En effet, elles s'acharnent sur une vulnérabilité logicielle qui conduit à l'instabilité du service et réduit ainsi son aptitude à répondre.

5.2.2 Objectifs de base d'une solution sécuritaire

Les trois objectifs primordiaux qu'un protocole sécuritaire doit satisfaire sont l'intégrité, la confidentialité et la disponibilité des données.

L'intégrité des données signifie qu'aucune altération non autorisée n'est possible et est donc étroitement liée à l'authentification. Une authentification faible survient quand aucune relation n'existe au préalable entre les entités impliquées et elles doivent donc s'échanger de l'information pour pouvoir s'authentifier par la suite. Ce premier échange n'étant pas authentifié, un attaquant peut facilement s'y insérer en prétendant être une entité légitime. Au contraire, une authentification forte signifie que les parties se connaissent déjà à travers un échange authentifié. L'intégrité d'un message prévient également la possibilité qu'il soit rejoué ultérieurement par un attaquant qui l'intercepte et le retransmet dans un autre environnement.

La confidentialité d'un message est l'assurance que son contenu ne sera lu que par le ou les destinataires légitimes. Par conséquent, si une tierce partie intercepte le message, elle serait incapable de le comprendre, de l'analyser ou encore d'y répondre. Cet objectif est essentiel lors de l'échange d'information sensible qui compromettrait le bon fonctionnement du protocole.

Finalement, la disponibilité des données se définit comme la capacité de fournir des ressources ou des services soit à un moment bien déterminé, soit d'une façon continue pendant un laps de temps donné. Les attaques de déni de service causées soit par une inondation ou l'exploitation d'une faille ont pour but de déjouer cet objectif.

5.2.3 Primitives cryptographiques de sécurité

Les systèmes de sécurité informatique utilisent souvent les primitives cryptographiques qui sont des algorithmes de base publics, normalisés. Les deux principales catégories de primitives sont les fonctions de hachage (dont SHA et MD5) [33] et de chiffrement (p.ex. AES, 3DES et blowfish) [34]. Une fonction de hachage transforme irréversiblement une entrée en une séquence (hash) de taille fixe, plus petite, qui est fréquemment utilisée comme empreinte cryptographique pour vérifier si l'entrée n'a pas été modifiée. Cependant, comme chaque nœud peut régénérer un nouveau hash, cette empreinte doit être chiffrée pour éliminer les risques de modifications non autorisées.

Les algorithmes de chiffrement sont soit symétriques soit asymétriques. En fait, ceci dépend du fait que les clés de chiffrement ont été au préalable partagées ou non. Bien qu'il soit nettement plus efficace, le chiffrement symétrique, qui repose sur une clé unique utilisée pour chiffrer et déchiffrer un message, demande une relation déjà existante entre les entités pour ne pas devoir divulguer les clés. De l'autre coté, le chiffrement asymétrique fait appel à deux clés par entité : l'une est publique et divulguée, l'autre est privée et n'est connue que de l'entité. Ainsi, on ne peut déchiffrer un message chiffré avec la clé publique que par la clé privée correspondante, garantissant ainsi la confidentialité. D'autre part, une fois une empreinte cryptographique chiffrée avec la clé privée, elle serait validée par la clé publique accessible à tous les nœuds, assurant l'authentification. On peut combiner les avantages des deux types de clés dans un chiffrement hybride qui permet à deux entités inconnues de partager une clé symétrique en la chiffrant par une clé asymétrique. Ce troisième type de chiffrement est le mécanisme le plus utilisé dans les solutions de sécurité.

5.3 Analyse et validation de la sécurité

5.3.1 Analyse de la sécurité

En général, la réauthentification cause un retard inacceptable dans la transition d'un réseau à un autre, surtout pour les applications à temps réel. Assurer une transition verticale transparente et sécurisée, est parmi les sujets les plus importants dans le domaine d'intégration cellulaire/WLAN. Notre design est soigneusement conçu pour répondre aux besoins de sécurité tels que les attaques par réinsertion, les attaques dues à la mauvaise utilisation des services cryptographiques, *Man-In-The-Middle* (MITM), l'écoute clandestine.

Protection contre les attaques par réinsertion

L'attaque par réinsertion est l'une des attaques les plus connues qui représente un risque majeur pour les protocoles d'authentification. Cette attaque consiste à répéter une transmission d'une manière malicieusement ou frauduleusement par une tierce partie. Notre proposition assure la protection contre ce type d'attaque par l'utilisation de valeurs à usage unique, générées aléatoirement. Les messages d'authentification sont tous générés par R_{UE} et R_{WAP}. L'utilisateur génère R_{UE} et l'envoie au WAP. Ensuite, le WAP accepte le message d'authentification si et seulement s'il contient la même valeur que R_{UE}. De la même façon, le WAP génère R_{WAP} et l'envoie au UE. Ensuite, le message d'authentification sera accepté par l'UE si et

seulement s'il contient la même valeur que R_{WAP}. De plus, toutes les valeurs aléatoires sont rafraîchies et elles ont une limite de validité dans le temps ce qui protège contre ce type d'attaque.

Protection contre la dérivation de la clé

L'utilisation de clés de session statiques peut représenter une faiblesse pour un protocole donné. Dans notre proposition, la clé de session SK_i est générée dynamiquement entre l'UE et le WAP. Les seules entités qui sont capables de connaître cette clé sont l'UE et le WAP. Si l'utilisateur se déplace vers un autre point d'accès, une nouvelle clé de session doit être générée indépendamment.

Protection contre l'écoute clandestine

L'écoute clandestine consiste à intercepter les messages et les clés par des récepteurs furtifs. Notre proposition est déjà protégée contre ce type d'attaque puisque les différents messages échangés sont chiffrés, y compris ceux qui permettent le transfert des clés.

Protection contre l'attaque MITM

Pour empêcher ce type d'attaque, on utilise une authentification mutuelle entre l'utilisateur et le point d'accès sans fil. L'utilisation du code d'authentification de message entre les deux entités ($MAC_{Qi}(K_{UE})$ et $MAC_{Qi}(K_{WAP})$) assure l'intégrité des données et l'authentification de l'expéditeur (détenteur de la clé secrète).

5.3.2 Validation de la sécurité

AVISPA : Outil de validation

AVISPA (Automated Validation of Internet Security Protocols and Applications) [35] est un outil de validation des protocoles et des applications de sécurité internet. Il offre un langage modulaire et expressif pour spécifier des protocoles et des propriétés de sécurité. Ce langage est le HLPSL (High-Level Protocol Specification Language). AVISPA intègre quatre outils arrière-plans qui représentent des techniques d'analyse et de

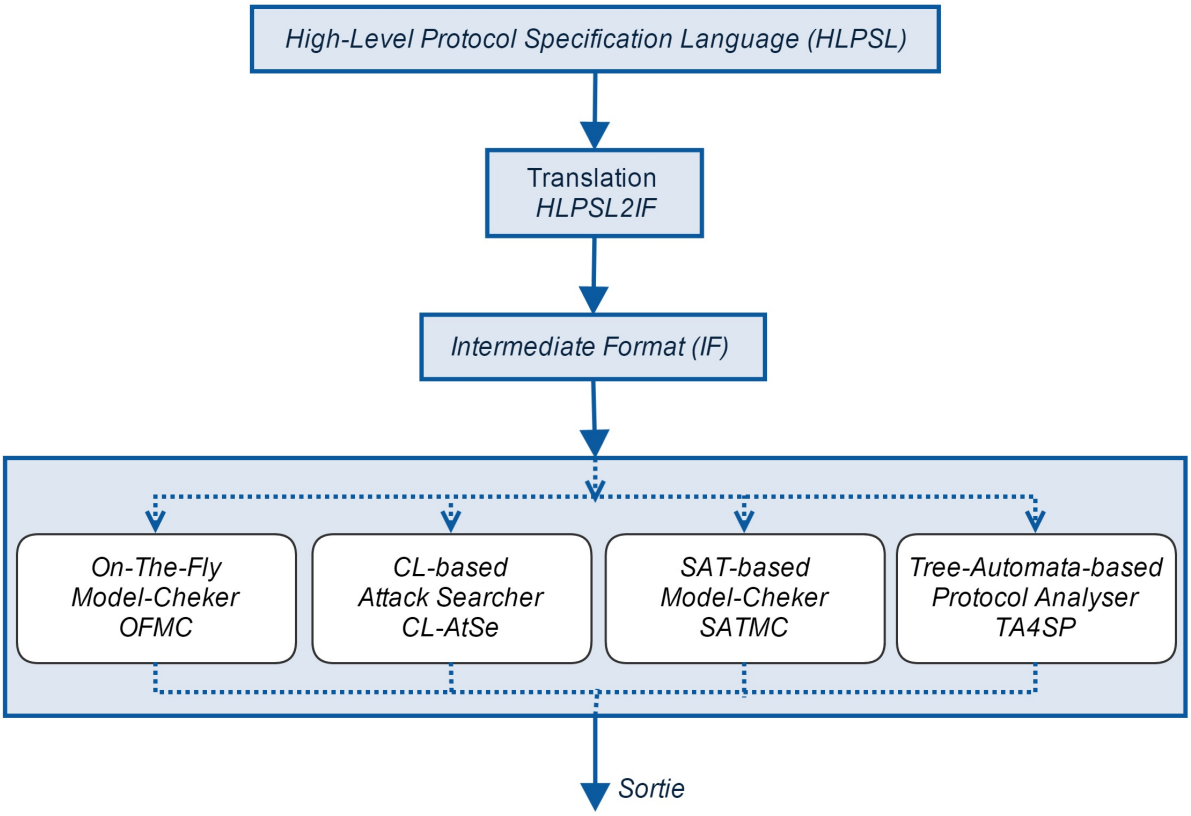

FIGURE 5.1 – Architecture d'AVISPA

vérification de sécurité automatique. L'architecture d'AVISPA est représentée dans la figure 5.1 [36]. L'utilisateur interagit avec l'outil en spécifiant le problème de sécurité avec le langage HLPSL. Le HLPSL est un langage modulaire basé sur les rôles. Il prend en compte la spécification des modèles du flux de contrôle, les structures de données, les différents opérateurs cryptographiques...

AVISPA traduit (avec l'outil HLPSL2IF) un problème de sécurité spécifié par l'utilisateur en langage HLPSL, en un format intermédiaire (IF) qui a des spécifications équivalentes. IF est le langage d'entrée de l'un des outils d'arrière-plan d'AVISPA. Soit, à ce jour, «*On-the-Fly Model-Checker*» (OFMC), «*Contraint Logic-based Attack Searcher*» (CL-AtSe), «*SAT-based Model-Checker*» (SATMC) et le «*Tree Automata based Automatic Approximations for the Analysis of Security Protocols*» (TA4SP). Les outils analysent les protocoles en modélisant un intrus actif qui contrôle le réseau mais qui ne peut pas briser la cryptographie. La figure 5.2 représente l'interface graphique d'AVISPA.

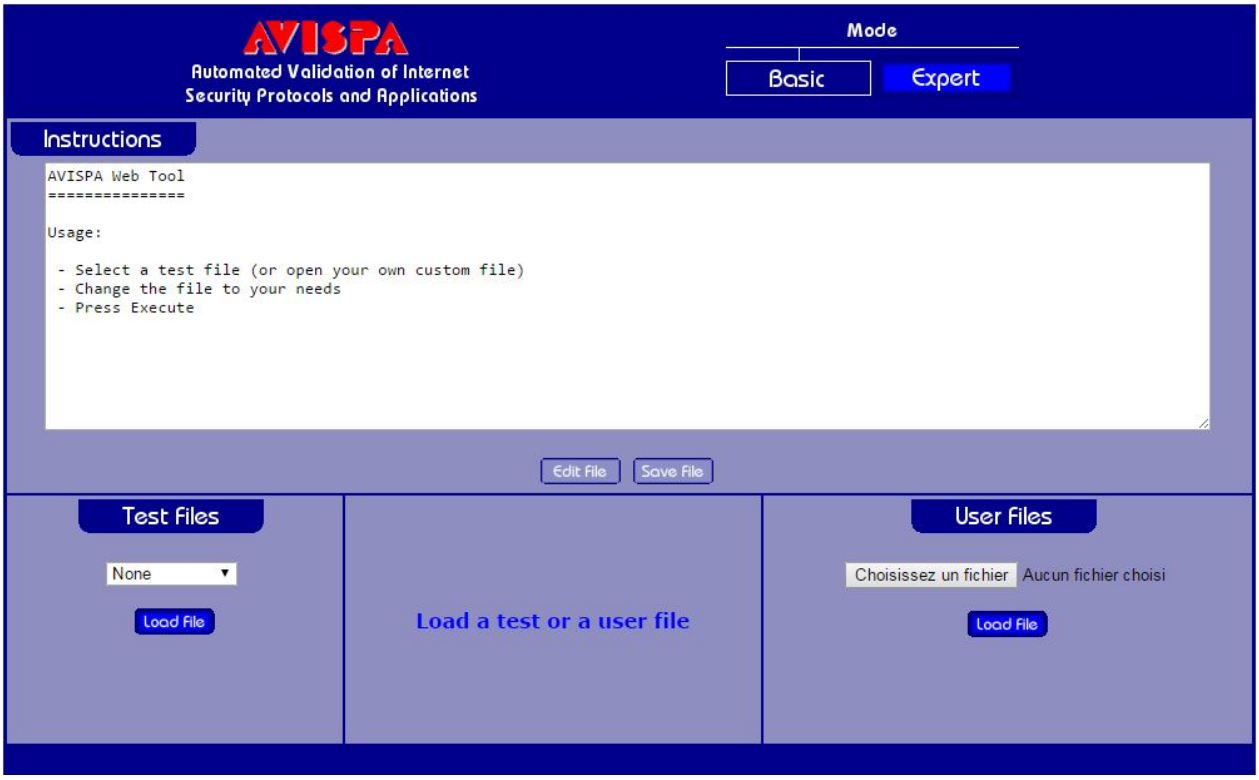

FIGURE 5.2 – Capture d'écran de l'outil AVISPA

Vérification avec AVISPA

Dans l'outil AVISPA on code un modèle avec des rôles. Notre design implémente quatre rôles: UE, WAP, session et environnement. UE et le WAP sont les rôles de base qui représentent les entités de notre proposition. Le rôle « session » est composé de l'entité UE et de l'entité WAP ensemble, qui partagent leurs informations en une seule session. Le rôle « environment » détermine les informations de l'intrus et les paramètres de la session entre les différentes entités. Pour trouver les attaques, on a créé la section «goal », présentée dans la figure 5.3, pour définir les objectifs de sécurité.

La figure 5.3 montre les propriétés de sécurité définies par les objectifs d'authentification et les clés secrètes partagées dans notre solution. Les objectifs de sécurité disponibles dans ce mécanisme sont :

– Vérifier la solidité du processus d'authentification entre les différentes entités.
– Vérifier le secret des clés symétriques partagé entre L'UE et le WAP.

```
goal

%Le secret de Q_I

secrecy_of sec_qi1, sec_qi2


%Mobile authentifie WAP par at_rand

authentication_on at_rand

%WAP authentifie Mobile par at_rand2

authentication_on at_rand2


end goal
```

FIGURE 5.3 – Section Goal

Notre proposition intègre un échange de messages entre l'utilisateur UE et le point d'accès sans fil WAP. Avant que le mécanisme ne démarre, on suppose que l'UE aura déjà obtenu les tickets, T_i :(Q_i, ID_{UE}, $SSID_i$, T_{exp}, r_{eHSS}) à partir d'eHSS par un lien de communication sécurisé.

Le rôle de l'utilisateur (UE) est présenté dans la figure 5.4 avec le langage HLPSL. Ce rôle présente les différents scénarios que l'UE exécute dans notre mécanisme après avoir eu les tickets.

Le rôle « WAP » décrit les tâches du point d'accès sans fil. La figure 5.5 montre un extrait de ce rôle (en HLPSL) qui décrit les différents scénarios que le WAP exécute.

Un autre rôle qui est défini dans notre code, est le rôle « session » représenté par la figure 5.6. Ce rôle est composé de l'union des entités UE et WAP et partage leurs informations en une seule session.

La figure 5.7 présente le rôle « environment », où nous avons développé les scénarios testés où l'intrus prend la place d'UE et de WAP. Ce rôle détermine les informations de l'intrus et les paramètres de la session qui sont communiqués entre les différentes entités.

Résultat d'AVISPA

Le but de ce test est de trouver les vulnérabilités de sécurité dans le design proposé. L'AVISPA vérifie s'il existe une attaque lors de l'exécution du protocole. En réalité, si un protocole est non sécurisé, AVISPA donnera la trace détaillée de l'attaque et il nous montre comment des dommages peuvent être faits.

```
    transition
 1. State   = 0
    /\ RCV(request_id)
   =|>
   State' := 2
    /\ ID_UE' := new()
    /\ SSID'  := new()
    /\ R_HSS' := new()
    /\ R_UE'  := new()
    /\ T_EXP' := new()
    /\ SND(respond_id.ID_UE'.SSID'.R_HSS'.T_EXP'.R_UE')
 2. State   = 2
    /\ RCV(K_WAP'.MAC1')
    /\ K_WAP'  = F2(SSID'.R_UE'.R_WAP')
    /\ Q_I'    = F3(MK.ID_UE'.SSID'.R_HSS'.T_EXP')
    /\ MAC1'  = HMAC(PRF_SHA1(Q_I').K_WAP')
   =|>
   State' := 4
    /\ K_UE'  := F1(ID_UE'.R_UE'.R_WAP')
    /\ MAC2'  := HMAC(PRF_SHA1(Q_I').K_UE')
    /\ SND(K_UE'.MAC2')
    /\ request(UE,WAP,at_rand,R_WAP')
    /\ witness(UE,WAP,at_rand2,R_WAP')
    /\ secret(Q_I',sec_qi1,{UE,WAP})
 3. State   = 4 /\ RCV(success) =|>
   State' := 6
end role
```

FIGURE 5.4 – Spécification du rôle de l'utilisateur avec HLPSL

Nous avons utilisé les différents outils d'arrière-plan d'AVISPA pour vérifier la sécurité. Chaque étape est testée contre l'ensemble des objectifs de sécurité fournis. Les résultats nous confirment qu'il n'y a aucune brèche de sécurité, ni pour l'authentification, ni de confidentialité. Le rapport obtenu dans la figure 5.8 et l'annexe A justifie que notre mécanisme est sécurisé. Il est bien protégé contre les différentes attaques

```
    transition
 1. State   = 1
    /\ RCV(start)
   =|>
   State' := 3
    /\ SND(request_id)
 2. State   = 3
    /\ RCV(respond_id.ID_UE'.SSID'.R_HSS'.T_EXP'.R_UE')
   =|>
   State' := 5
    /\ R_WAP' := new()
    /\ K_WAP'   := F2(SSID'.R_UE'.R_WAP')
    /\ Q_I'     := F3(MK.ID_UE'.SSID'.R_HSS'.T_EXP')
    /\ MAC1'    := HMAC(Q_I.K_WAP')
    /\ SND(K_WAP'.MAC1')
    /\ witness(UE,WAP,at_rand,R_WAP')
    /\ secret(Q_I',sec_qi2,{UE,WAP})
      3. State   = 5
    /\ RCV(K_UE'.MAC2')
    /\ K_UE'  = F1(ID_UE'.R_UE'.R_WAP')
    /\ MAC2' = HMAC(Q_I.K_UE')
   =|>
   State' := 7
    /\ SND(success)
    /\ request(UE,WAP,at_rand2,R_WAP)
end role
```

FIGURE 5.5 – Spécification du rôle du point d'accès sans fil avec HLPSL

```
role session(
   UE,WAP            : agent,
   F1,F2,F3        : hash_func,
   PRF_SHA1        : hash_func,
   HMAC            : hash_func,
   MK              : symmetric_key)
def=
local
   SNDUE, RCVUE, SNDWAP, RCVWAP : channel (dy)
const
   at_rand,at_rand2      : protocol_id
 composition
    mobile(UE,WAP,F1,F2,F3,PRF_SHA1,HMAC,MK,SNDUE,RCVUE)
 /\ wap(UE,wap,F1,F2,F3,PRF_SHA1,HMAC,MK,SNDWAP,RCVWAP)
end role
```

FIGURE 5.6 – Spécification du rôle session avec HLPSL

```
role environment() def=
 const
   ue,wap              : agent,
   kps,kis             : symmetric_key, % !!one per user   !!
   f1,f2,f3            : hash_func,
   prf_sha1            : hash_func,
   hmac                : hash_func
 intruder_knowledge = {ue,wap,i,f1,f2,f3,prf_sha1,hmac}
 composition
    session(ue,wap,f1,f2,f3,prf_sha1,hmac,kps)
%  /\ session(ue,wap,f1,f2,f3,prf_sha1,hmac,kps)
% /\ session(i,wap,f1,f2,f3,prf_sha1,hmac,kis)
end role
```

FIGURE 5.7 – Spécification du rôle environnement avec HLPSL

```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/avispa/web-interface-computation/./tempdir/workfile4rTPlW.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 0.04s
 visitedNodes: 4 nodes
 depth: 3 plies
```

FIGURE 5.8 – Vérification avec OFMC

comme celles par réinsertion, celles dues à la mauvaise utilisation des services cryptographiques, l'attaque MITM, l'écoute clandestine… L'authentification s'effectue entre les deux entités en toute sécurité. Aucune attaque n'est trouvée sur la clé de session par l'intrus.

5.4 Étude de la performance

Dans cette section, nous allons comparer la performance de notre mécanisme à celle d'autres mécanismes existants. Notre proposition se compose de deux messages échangés dans la phase de préparation du transfert et de trois messages pour la génération de la clé de session c.-à-d. au moment du transfert. On analyse notre proposition par une étude détaillée sur la performance qui consiste à vérifier deux points principaux; le coût d'infrastructure et le coût d'utilisation.

5.4.1 Outils de mesures et d'évaluation

Comme nous l'avons indiqué dans le chapitre précédent, le but principal de tous les protocoles d'authentification est de diminuer le délai de cette dernière. En conséquence, dans le cadre du roaming vertical, un bon mécanisme de réauthentification est un mécanisme qui permet de diminuer le temps de handover pour diminuer l'impact sur la continuité de service. Nous allons évaluer l'authentification lors du handover par l'analyse du coût de point de vue infrastructure d'une part et de point de vue utilisateurs d'autre part. Ensuite, notre solution sera comparée à trois schémas : un premier schéma proposé dans [21] présente un mécanisme d'authentification pour un handover entre E-UTRAN et les réseaux d'accès non-3GPP, un deuxième schéma [22] présente une authentification sécurisée entre 3GPP LTE et les systèmes WLANs, et le dernier schéma est le EAP-AKA [37]. La solution proposée dans [21] exige l'utilisation d'équations elliptiques pour avoir une authentification rapide et sécurisée lors d'un transfert automatique vertical. Ce schéma est présenté en deux phases: la phase de préparation d'un handover et la phase d'authentification ce qui facilite la comparaison avec notre schéma. La solution dans [22] présente deux schémas : un schéma lors d'un premier transfert vertical et un autre qui s'exécute localement dans le réseau WLAN lors d'un transfert horizontal (d'un WAP à un autre WAP) sans contacter le serveur d'authentification.

La performance des schémas d'authentification peut être analysée par des méthodes différentes. Par exemple, le nombre de messages échangés pour l'authentification est mesuré afin de calculer le coût de l'authentification, alors que le délai de traitement pour le processeur est utilisé comme une mesure de performance. Néanmoins, dans le contexte d'authentification lors d'un transfert, la latence de l'authentification est cumulée durant l'échange des messages entre les différentes entités du réseau. De plus, les dispositifs et les entités du réseau d'aujourd'hui sont supposés avoir la capacité suffisante pour mesurer les opérations cryptographiques. Par conséquent, nous devons considérer les opérations cryptographiques dans chaque nœud et aussi les délais d'authentification.

5.4.2 Coût d'infrastructure

Délai d'authentification

Dans cette partie, on va étudier la performance de notre système qui se base sur la mesure du délai de réauthentification lors d'un roaming. La latence est la différence de temps entre le début et la fin d'un transfert vertical de cellulaire au WLAN. Notre proposition présente deux parties : une pour la préparation

Tableau 5.1 – Délai de traitement

	Délai de traitement (ms)
Schéma [21]	4,6
Notre proposition	4,07

du transfert où la génération des clés symétriques se fait entre les différentes entités (UE, eHSS, AAA et WAP) afin de préparer les tickets, et une pour la phase d'authentification. Cette étude représente juste la deuxième phase, la première phase n'est pas considérée car le délai de réauthentification démarre à la phase d'authentification. En effet, le délai de réauthentification est composé de trois éléments; le délai de traitement, le délai de transmission et le délai de propagation.

$$T_{auth} = T_{trans} + T_{trait} + T_{prop}\,. \tag{5.1}$$

Le délai de transmission est le temps de transmission des messages entre les entités. Ce délai est considéré négligeable par rapport au délai de traitement et au délai de propagation [38]. Pour cela, T_{trans} n'a pas été inclus dans le calcul du délai d'authentification totale donc on aura:

$$T_{auth} = T_{trait} + T_{prop}\,. \tag{5.2}$$

Le délai de traitement, T_{trait}, est le temps subi par chaque nœud lors du traitement d'un message pour exécuter les opérations telles que le chiffrement, le déchiffrement, la génération de clé et le calcul de MAC. Le délai de traitement dépend principalement de la capacité des dispositifs, y compris la capacité du processeur et de la mémoire.

Selon le temps de l'exécution des opérations cryptographiques étudié en [39], la comparaison de notre solution avec [21] au terme du délai de traitement est indiquée dans le tableau 5.1. Le délai de traitement dépend principalement de la capacité des dispositifs, y compris la capacité du processeur et de la mémoire. Dans notre étude, nous avons utilisé un codage en C++ sur un processeur Intel Core i3-2120@3.3 GHz et avec une mémoire de 2GB RAM pour estimer le délai de traitement.

Comme nous ignorons le délai de transmission et nous présentons le délai de traitement en haut, nous pouvons dire que le délai d'authentification total dépend principalement du délai de propagation. Dans notre

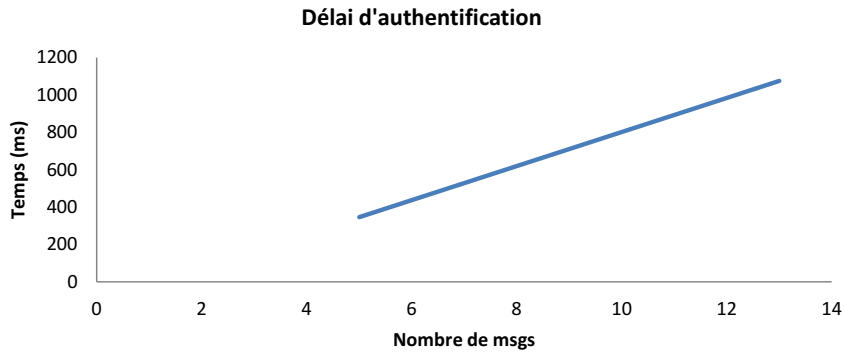

FIGURE 5.9 – Délai d'authentification

proposition, nous définissons le délai de propagation comme suit:

$$T_{prop} = T_{prop}(eNB - eHSS) + T_{prop}(eHSS - UE) + 3 * T_{prop}(UE - WAP)\,. \tag{5.3}$$

Notons :

- T_{prop} (eNB-eHSS) : Le délai de propagation entre l'eNB et l'eHSS.
- T_{prop} (eHSS-UE) : Le délai de propagation entre l'eHSS et l'UE.
- T_{prop} (UE-WAP) : Le délai de propagation entre l'UE et le WAP.

Comme nous n'avons pas réalisé de banc d'essai pour mesurer les temps de retard réels, nous avons utilisé les valeurs trouvées dans [38] et [40] pour faire les calculs. La figure 5.9 présente le délai de réauthentification de notre solution lors d'un transfert par rapport au nombre des messages échangés entre les entités alors que la figure 5.10 montre que notre mécanisme est une nette amélioration par rapport au protocole EAP-AKA en terme du délai de réauthentification [40].

L'idée principale de notre proposition est l'utilisation de tickets, qui vont être l'élément clé pour un futur transfert automatique. Avec ces tickets, l'utilisateur peut se réauthentifier sans interaction avec une tierce partie. Cette méthode va accélérer la procédure d'authentification tout en gardant l'aspect de sécurité dans notre système. Ceci permet de réduire de manière significative les délais d'authentification selon les résultats obtenus. Notre méthode améliore considérablement les délais d'authentification mais, néanmoins, d'autres améliorations sont encore requises pour pouvoir supporter des applications temps réel comme la voix sur IP.

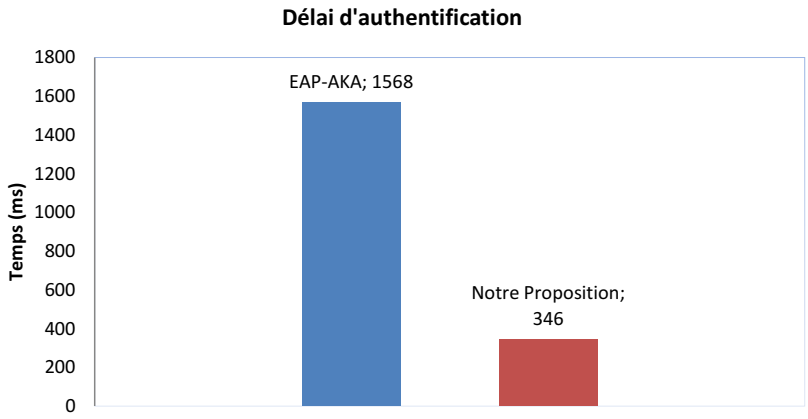

FIGURE 5.10 – Comparaison du délai d'authentification entre EAP-AKA et notre mécanisme

La formule 5.4 présente le nombre de messages échangés par notre proposition pour avoir la réauthentification.

$$N = 4 + \lceil \frac{T_{actuelle} - T_{départ}}{T_{exp}} \rceil . \tag{5.4}$$

Notons :

$\lceil \rceil$: est la fonction ceiling (valeur entière strictement supérieure).

Latence de la transmission

Nous avons comparé la latence de transmission de notre schéma avec les schémas dans [21], [22] et [37]. Notre design est une poignée de main unique ce qui nous conduit à avoir une authentification simple et rapide sans interagir avec une tierce partie. La comparaison de notre schéma avec d'autres existants va nous donner une mesure de sa performance d'authentification.

On considère que le coût de transmission d'un message d'authentification entre le point d'accès et le serveur AAA ou le MME est égal à l'unité α et le coût entre l'UE et le point d'accès est égal à l'unité β. Le tableau 5.2 montre la latence de transmission en comparant notre schéma par rapport à d'autres schémas de référence. On remarque bien que notre mécanisme permet de transmettre des messages d'authentifica-

Tableau 5.2 – Comparaison de la latence de transmission

Schémas	T_{UE-WAP}	$T_{WAP-AAA/MME}$
Schéma [21]	4 β	0
Schéma [22]	5 β	4 α
Schéma [37]	5 β	4 α
Notre proposition	3 β	0

tion entre l'UE et le point d'accès sans avoir communiqué avec une tierce partie (serveur AAA ou MME). Par contre, dans les autres schémas plus de messages et échanges d'information sont nécessaires. Notre proposition n'exige qu'un échange de trois messages entre l'utilisateur et le point d'accès, ce qui mène à un mécanisme meilleur que les schémas d'authentification existants et par suite notre design est plus avantageux en pratique.

Notons que :

- T_{UE-WAP}: le coût de transmission d'un message d'authentification entre l'utilisateur et le point d'accès.
- $T_{WAP-AAA/MME}$: le coût de transmission d'un message d'authentification entre le point d'accès et le serveur AAA ou le MME.

5.4.3 Coût utilisateurs

Taille des messages

Nous choisissons d'utiliser l'algorithme « message-digest » [41] MD5 pour les fonctions de hachage et le « advanced encryption standard » [42] AES pour le chiffrement et le déchiffrement. De plus, nous prenons en considération notre hypothèse qu'il existe une communication entre eHSS et AAA/WAP pour avoir les clés symétriques. Donc, nous donnons l'analyse numérique suivante :

Dans chaque ticket, le MAC doit avoir une espace de 20 octets comme sortie, 4 octets pour les IDs et 22 octets pour la longueur d'entrée d'une fonction de hachage. La figure 5.11 montre la taille des messages par rapport au nombre d'utilisateurs de notre solution. Nous remarquons que si le nombre d'utilisateurs ou bien le nombre d'expirations augmente, la taille des messages augmente aussi.

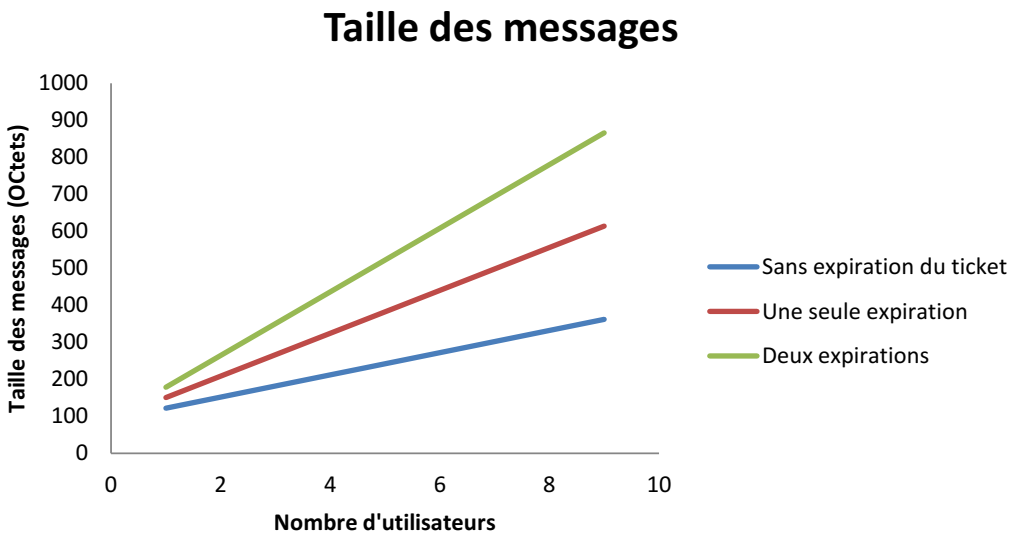

FIGURE 5.11 – Taille des messages

Coût des communications entre les entités AAA et eHSS

Un message Diameter consiste en un entête de taille fixe (20 octets) suivi par un nombre variable d'AVPs. La valeur d'un AVP Diameter a une longueur maximum de 16 millions d'octets. Ceci est très utile lorsque l'AVP transporte des données qui peuvent atteindre plusieurs kilooctets. Le format de l'AVP contient cinq champs principaux [43]: le champ « AVP-Code » (4 octets) représente l'identifiant de l'AVP, viennent ensuite les « Fanions » (8 bits), le champ « Length » qui représente la longueur de l'AVP incluant l'entête et les données (mesurées en octets), ensuite « Vendor-ID » (4 octets) pour identifier le constructeur de l'AVP et enfin les données qui ont des longueurs variables selon l'application. Dans notre proposition, nous avons un entête qui mesure 9 octets (champs AVP Code, Flags et Length) suivi par les données. Dans les AVPs concernant la commande « Push-Profile-Answer (PPA) », la longueur est de 9+85 octets, soit 94 octets. Ces 94 octets représentent la taille des 5 AVPs pour les (Q_i, ID_{UE}, $SSID_i$, T_{exp}, r_{eHSS}). Par contre, l'AVP concernant la commande « Push-Profile-Request (PPR) » a une longueur de 33 octets avec un en-tête de 9 octets, ce qui donne une longueur totale de 41 octets.

La figure 5.12 présente la taille des messages échangés entre les deux entités AAA et eHSSS. Nous avons varié le nombre d'usagers jusqu'au 1000 pour estimer la capacité des messages. Nous remarquons que si le nombre d'utilisateurs ou bien le nombre d'expirations augmente (facteur temps), la taille des messages

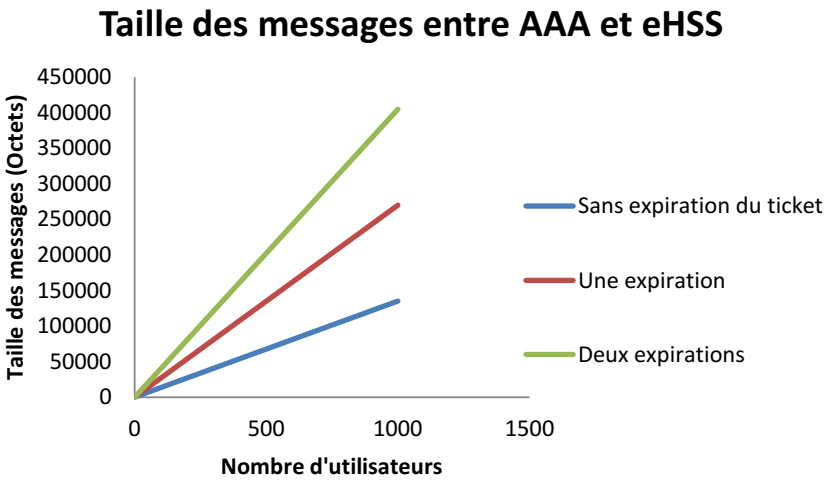

FIGURE 5.12 – Taille des messages entre AAA et eHSS

augmente aussi. En réalité, le débit des messages échangés entre l'eHSS et le serveur AAA dépend nécessairement de taux d'expiration des tickets. Donc la variation du nombre d'utilisateurs et la durée de vie des tickets ont des effets sur la charge de calcul dans notre système. De même, avec l'augmentation du nombre d'usagers nous augmentons le taux de gaspillage potentiel et ça s'explique par l'augmentation du temps d'attente adopté par les informations échangées dans chaque nœud de notre système. Par cette analyse, nous pouvons dire que notre proposition peut avoir des améliorations au niveau de gaspillage, car lors de réauthentification pour un roaming de LTE au WLAN nous allons éviter de contacter le serveur AAA. Néanmoins, comme on l'a vu au chapitre précédent, ceci se fait moyennant un transfert d'information important entre AAA et eHSS.

Estimation de coût de calcul pour générer un ticket

L'objectif de cette partie est d'estimer le coût de calcul pour générer les tickets. Chaque ticket dans notre système a une taille de 38 octets; 20 octets sont réservés pour la clé d'authentification, 4 octets pour le SSID, 4 octets pour l'identité de l'équipement usager, 5 octets pour le temps d'expiration et en fin 5 octets pour la valeur aléatoire reHSS. Le temps de calcul des opérations cryptographiques a été évalué sur un processeur Intel Core i3-2120@3.3 GHz et avec une mémoire de 2GB RAM pour estimer le délai de traitement, où

l'auteur dans [25] a fait l'expérience plusieurs fois et il a estimé que le temps de cryptage moyen est de 16 ms, le temps de décryptage moyen de 0.0288 ms et le temps de hachage moyen est de 0,0535 ms, ce qui donne un temps de génération moyenne de 16,823 ms pour un ticket, ce qui résulte à 59 tickets par seconde, pour un seul processeur. En travaillant avec une grille de calcul, on peut aisément passer à l'échelle. Si nous prenons un exemple réel, on peut supposer que nous avons 50 000 utilisateurs en itinérance potentielle pour dix réseaux partenaires. En fixant 20 minutes comme durée de vie moyenne de chaque ticket pour assurer la sécurité de notre mécanisme contre différents types d'attaques, nous devons dans ce cas générer 417 tickets chaque seconde et, nous communiquons 38 octets pour chaque ticket, ce qui donne 16Mops. Les mesures montrent bien que notre modèle est un peu plus coûteux en termes de calcul, communications et de l'énergie consommée au niveau des dispositifs par rapport à l'approche traditionnelle, où on fait l'authentification seulement à la demande. Néanmoins, ce coût est modéré et facilement absorbable dans une infrastructure « classique ».

Latence de transfert

La latence d'un transfert intercellulaire est définie comme la période de temps qui commence à partir du moment où l'UE sélectionne le WAP et se termine au moment où les communications entre l'UE et le WAP correspondant est reprise.

Dans cette section, nous allons comparer la latence de notre proposition par rapport au protocole EAP-AKA et le schéma [21]. La latence totale est la somme des latences propre au réseau WLAN et au réseau 3GPP LTE. La figure 5.13 présente la moyenne de la latence lorsque le nombre d'utilisateurs augmente. Les résultats obtenus montrent bien que notre mécanisme a de meilleures performances que le protocole EAP-AKA et la solution proposée dans [21].

L'équation 5.5 représente la formule de la latence d'un transfert intercellulaire [23] :

$$L_{HO} = L_{L2} + D_{Auth} + D_{SA}\,. \tag{5.5}$$

Notons que :

- L_{HO} : est le temps de latence pour la couche liaison [44] .
- D_{Auth} : est le temps d'avoir le 3 way-Handshake qui représente $3T_{UE-WAP}$.

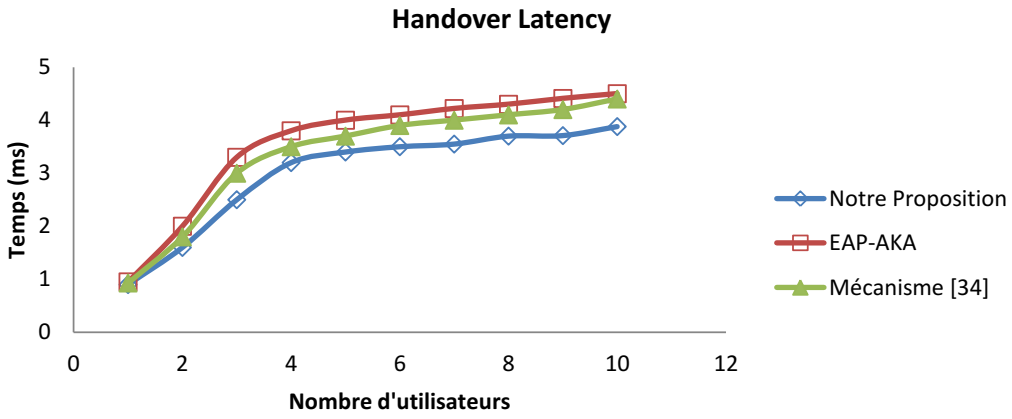

FIGURE 5.13 – Comparaison de la latence du Handover

– D_{SA} : est le temps moyenne de transmission entre l'UE et le WAP.

L'amélioration présenté dans la figure 5.13 s'explique par le fait que nous éliminons la participation d'une tierce partie, ce qui réduit considérablement la latence et le nombre de messages. Le graphique montre qu'il y a une rédaction significative au terme de coût d'authentification qui nous conduit d'avoir un transfert automatique transparent.

5.5 Conclusion

Dans ce chapitre, nous avons détaillé la démarche suivie afin d'analyser la sécurité et la performance de notre mécanisme d'authentification pour un transfert vertical automatique entre réseaux 3GPP-LTE et WLAN. Les résultats de notre analyse montrent bien que notre solution est sécurisée et elle a réussi la majorité des tests. De cette façon, nous pouvons donc conclure que le protocole proposé peut résister à différents types d'attaques. Nous avons également présenté différentes solutions pour comparer l'évaluation de la performance d'authentification de notre proposition avec les schémas existants. Notre mécanisme a montré de très bonnes performances.

Chapitre 6

Conclusion et perspectives

6.1 Conclusion

Le Wi-Fi est devenu un outil essentiel pour les opérateurs sans fil pour répondre aux exigences de données mobiles de leurs utilisateurs. Le volume du trafic transporté dans les réseaux Wi-Fi a considérablement augmenté au cours des dernières années, et devrait continuer à croître dans les années à venir. De plus, la plupart des appareils mobiles (smartphones, tablettes, netbooks, ordinateurs portables, eReaders, consoles de jeux..) intègrent l'accès au Wi-Fi et aussi la disponibilité des réseaux sans fil. Tout ça a conduit à un besoin imminent d'intégrer le WLAN avec le 3GPP EPC.

Ce mémoire touche à l'intégration des réseaux WLANs avec des réseaux cellulaires. Cette diversité a mené vers des contributions touchant un plus large éventail de problématiques mais toujours sous le thème générale d'améliorer l'intégration cellulaire Wi-Fi. Plus précisément, la principale contribution dans ce mémoire est que nous avons proposé un mécanisme d'authentification qui mène à la facilité d'intégration. Cette méthode peut être utilisée dans tout type de mobilité entre E-UTRAN et un accès non-3GPP qui doit être un accès de confiance. Notre mécanisme d'authentification est basé sur la notion des tickets et qui s'exécute sans contacter le serveur d'authentification AAA. Le but de notre proposition est d'avoir une authentification non seulement sécurisée, mais aussi rapide, en diminuant la latence. Cela se fait en donnant l'autorisation à l'UE d'accéder au réseau WLAN en présentant certaines informations. Pour réaliser cet objectif, l'eHSS distribue d'abord des tickets au UE dans une première phase; ensuite et dans une deuxième phase, ce dernier et le point d'accès sans fil s'authentifient mutuellement. Cette méthode nous permet d'obtenir un transfert

transparent en utilisant les opérations de clés symétriques et d'éliminer la participation d'une tierce partie, ce qui réduit considérablement la latence et le nombre de messages.

Pour évaluer notre mécanisme, nous avons utilisé AVISPA qui est un outil de validation automatisée des protocoles et des applications de sécurité internet. Cet outil offre un langage modulaire et expressif pour spécifier des protocoles et des propriétés de sécurité.

Notre analyse montre bien que la solution proposée offre une sécurité contre plusieurs attaques et garantir de bonnes performance et qualité de service. Il a le potentiel de réduire le nombre de messages échangés entre les différentes entités. En outre, il a le potentiel de réduire les délais de réauthentification lors d'un transfert vertical. Ce point est très important car les protocoles de sécurité sont actuellement une source majeure de latence dans les réseaux mobiles.

6.2 Perspectives

L'identification des limitations de notre travail est une étape incontournable. Dans le chapitre 4, où nous avons décrit notre proposition, un point très important n'a pas été discuté, c'est comment l'UE choisit le bon point d'accès sans fils du réseau WLAN. Ce point (présenté à la première étape de la figure 4.5) est très important pour bien choisir le point d'accès sans fil qui permet aux utilisateurs d'avoir le bon service après qu'il atteint une certaine valeur bien déterminée du signal. Ce sujet a été discuté dans le projet de 3GPP « WLAN Network Selection for 3GPP Terminals » [45]. Ceci est lié à la spécification technique de HotSpot 2.0 qui est en cours de développement par le Wi-Fi Alliance [46]. Un autre point doit être discuté dans ce mémoire : est comment préserver l'adresse IP lors d'un transfert vertical. Ce cas est typiquement utilisé pour les appels à voix sur IP (VoIP) lors d'un roaming d'un réseau LTE à un réseau WLAN. Également, d'autres applications comme les applications d'Internet sécurisées ne sont pas désignées pour gérer le changement de l'adresse IP. Donc, le manque de la préservation d'une adresse IP lors d'un transfert peut être considéré comme un sujet à discuter dans le futur. Enfin, la réduction du volume de communication entre AAA et eHSS doit également faire l'objet d'une étude plus approfondie.

Références

[1] Roeland, D. et Rommer, S., "Advanced WLAN integration with the 3GPP evolved packet core," *Communications Magazine, IEEE*, vol. 52, no. 12, pp. 22–27, 2014.

[2] Anders Lundström et Göran Hall, "Wi-Fi integration," Ericsson, Whitepaper, Février 2011. [Online]. Available: http://www.ericsson.com/res/docs/2012/ER-WiFi-Integration.pdf

[3] InterDigital, "Cellular-Wi-Fi Integration," InterDigital, Whitepaper, Juin 2012. [Online]. Available: http://wpuploads.interdigital.com.s3.amazonaws.com/uploads/2012/08/Cellular_WiFi_Integration-White-Paper.pdf

[4] Magnus Olsson, Shabnam Sultana, Stefan Rommer, Lars Frid et Catherine Mulligan , *SAE and Evolved packet core: Driving the mobile broadband revolution*. Elsevier, 2009.

[5] 3GPP, "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses," 3rd Generation Partnership Project (3GPP), TS 33.402, Déc 2014. [Online]. Available: http://www.3gpp.org/DynaReport/33402.htm

[6] Alcatel-Lucent, "Introduction to Evolved Packet Core," Alcatel-Lucent, Whitepaper, Juillet 2009. [Online]. Available: http://lte.alcatel-lucent.com/locale/en_us/downloads/wp_evolved_packet_core.pdf

[7] 3GPP, "3GPP System Architecture Evolution (SAE); Security architecture," 3rd Generation Partnership Project (3GPP), TS 33.401, Mars 2015. [Online]. Available: http://www.3gpp.org/DynaReport/33401.htm

[8] nmcgroups, "LTE Security," nmcgroups, Whitepaper, 2012. [Online]. Available: http://www.nmcgroups.com/en/expertise/lte/security.asp

[9] 3GPP, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)," 3rd Generation Partnership Project (3GPP), TS 24.301, Septembre 2014. [Online]. Available: http://www.3gpp.org/dynareport/24301.htm

[10] CISCO, "Cisco IOS Software Configuration Guide for Cisco Aironet Access Points," CISCO, Whitepaper, 2006. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-3_8_JA/configuration/guide/1238jasc.pdf

[11] Jyh-Cheng Chen et Yu-Ping Wang, "Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience," *Communications Magazine, IEEE*, vol. 52, no. 12, pp. 26–32, 2005.

[12] 3GPP, " Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks," 3rd Generation Partnership Project (3GPP), TS 24.302, Mars 2012. [Online]. Available: http://www.3gpp.org/dynareport/24301.htm

[13] 4G Americas, "Integration of Cellular and Wi-Fi Networks," 4G Americas, Whitepaper, Septembre 2013. [Online]. Available: http://www.ietf.org/mail-archive/web/mif/current/pdfczA7kI0W3X.pdf

[14] 3GPP, " Architectural Enhancements for non-3gpp accesses," 3rd Generation Partnership Project (3GPP), TS 23.402, Mars 2015. [Online]. Available: http://www.3gpp.org/DynaReport/23402.htm

[15] 3GPP, "Study on S2a Mobility based on GPRS Tunnelling Protocol (GTP) and Wireless Local Area Network (WLAN) access to the Enhanced Packet Core (EPC) network (SaMOG)," 3rd Generation Partnership Project (3GPP), TS 23.852, Septembre 2013. [Online]. Available: http://www.3gpp.org/DynaReport/23852.htm

[16] Adnan Basir, "GPRS Tunneling Protocol (GTP) in LTE," 4G LTE World, Bog, Mars 2013. [Online]. Available: http://4g-lte-world.blogspot.ca/2013/03/gprs-tunneling-protocol-gtp-in-lte.html

[17] C. Perkins, "IP Mobility Support," RFC 2002, Octobre 1996.

[18] V. Devarapalli, Wichorus, K. Chowdhury, "Proxy Mobile IPv6," RFC 5213, Août 2008.

[19] G. Tsirtsis, H. Soliman, "Dual-Stack Mobile IPv4," RFC 5454, Mars 2008.

[20] Vijay Garg, *Wireless Communications and Networking*. Elsevier, 2007.

[21] Jin Cao, Maode Ma et Hui Li, "An Uniform Handover Authentication between E-UTRAN and Non-3GPP Access Networks," *Wireless Communications, IEEE Transactions on*, vol. 11, no. 10, pp. 3644–3650, 2012.

[22] Imen Elbouabidia, Faouzi Zaraia, Mohammad S. Obaidatb, et Lotfi Kamounai, "An efficient design and validation technique for secure handover between 3GPP LTE and WLANs systems," *Journal of Systems and Software*, vol. 91, pp. 163–171, 2014.

[23] Jong-Hyouk Lee et Jean-Marie Bonnin, "HOTA: Handover optimized ticket-based authentication in network-based mobility management," *Information Sciences*, vol. 230, pp. 64–77, 2013.

[24] Anmin Fu and Yuqing Zhang and Zhenchao Zhu and Xuefeng Liu, "A fast Handover Authentication mechanisme based on ticket for IEEE 802.16m," *Communications Letters, IEEE*, vol. 14, no. 12, pp. 1134–1136, 2010.

[25] Li Xu, Yuan He, Xiaofeng Chen et Xinyi Huang , "Ticket-based handoff authentication for wireless mesh networks," *Computer Networks*, vol. 73, no. 0, pp. 185–194, 2014.

[26] Qi Jiang, Jianfeng Ma, Guangsong Li et Li Yang , "An Efficient Ticket Based Authentication Protocol with Unlinkability for Wireless Access Networks," *Wireless Personal Communications*, vol. 77, no. 2, pp. 1489–1506, 2014.

[27] Rafa Marin-Lopez,Fernando Pereñiguez-Garcia,Yoshihiro Ohba,Fernando Bernal-Hidalgo et Antonio F. Gomez , "A Kerberized Architecture for Fast Re-authentication in Heterogeneous Wireless Networks," *Mobile Networks and Applications*, vol. 15, no. 3, pp. 392–412, 2010.

[28] Alfred J. Menezes, Paul C. van Oorschot et Scott A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.

[29] John Richard Black, "Message authentication codes," Ph.D. dissertation, California State University at Hayward, 1988.

[30] Etemad, K. and Elliott, B., "Devices and methods for radio communication network guided traffic offload," Janvier 2014. [Online]. Available: https://www.google.com/patents/US20140003239

[31] Yvo Desmedt, *Man-in-the-Middle Attack*. Springer US, 2011.

[32] Stéphane Boeuf et Grégory Danelon, "Denial of Service," Université Claude Bernard Lyon 1, Sujet Bibliographique Scientifique , 2002. [Online]. Available: http://cpham.perso.univ-pau.fr/M2SIR/BIBLIO/DOC01-02/DoS.pdf

[33] T. Hansen, "US Secure Hash Algorithms (SHA and HMAC-SHA)," RFC 4634, Jully 2006.

[34] Pierre-Alain Fouque, “Algorithmes de chiffrement symétrique par bloc (DES et AES),” Ecole normale supérieure, Sujet Bibliographique Scientifique , 2010. [Online]. Available: http://www.di.ens.fr/~fouque/mpri/des-aes.pdf

[35] “The AVISPA Project.” [Online]. Available: http://www.avispa-project.org/

[36] Luca Viganò, “Automated Security Protocol Analysis With the AVISPA Tool,” *Electronic Notes in Theoretical Computer Science*, vol. 155, no. 6, p. 61– 86, 2006.

[37] J. Arkko et H. Haverinen, “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA),” RFC 4187, Janvier 2006.

[38] Prasithsangaree, P. et Krishnamurthy, P., “A new authentication mechanism for loosely coupled 3G-WLAN integrated networks,” in *Vehicular Technology Conference, 2004. VTC 2004-Spring. 2004 IEEE 59th*, vol. 5, 2004.

[39] Imen Elbouabidia, Faouzi Zaraia, Mohammad S. Obaidatb, et Lotfi Kamounai, “A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges,” *Information Sciences*, vol. 180, no. 15, pp. 2895–2903, 2010.

[40] H. Kwon, K.-Y. Cheon, K.-H. Roh et A. Park, “USIM based Authentication Test-bed for UMTS-WLAN Handover,” in *IEEE Infocom*, vol. 5, 2006.

[41] R. Rivest, *The MD5 message-digest algorithm*. RFC Editor, 1992.

[42] J. Daemen et V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer, 2002.

[43] “Protocole de Base DIAMETER Architecture, Entités et Commandes,” EFORT, Sujet Bibliographique Scientifique , 2014. [Online]. Available: http://www.efort.com/r_tutoriels/DIAMETER_BASE_EFORT.pdf

[44] Pack, S., Jaeyoung Choi, Taekyoung Kwon et Yanghee Choi, “A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges,” *Communications Surveys Tutorials, IEEE*, vol. 9, no. 1, pp. 2–12, 2007.

[45] 3GPP, “Study on Wireless Local Area Network (WLAN) network selection for 3GPP terminals,” 3rd Generation Partnership Project (3GPP), TS 23.865, Décembre 2013. [Online]. Available: http://www.3gpp.org/DynaReport/23865.htm

[46] “Wi-Fi Alliance.” [Online]. Available: http://http://www.wi-fi.org/

Annexe A

Résultat d'AVISPA

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/avispa/web-interface-computation/./tempdir/workfile4rTPlW.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 4 states
  Reachable  : 1 states
  Translation: 0.02 seconds
  Computation: 0.00 seconds
```

FIGURE A.1 – Vérification avec CL-AtSe

```
SUMMARY
  SAFE
DETAILS
  STRONGLY_TYPED_MODEL
  BOUNDED_NUMBER_OF_SESSIONS
  BOUNDED_SEARCH_DEPTH
  BOUNDED_MESSAGE_DEPTH
PROTOCOL
  workfile4rTPlW.if
GOAL
  %% see the HLPSL specification..
BACKEND
  SATMC
COMMENTS
STATISTICS
  attackFound            false    boolean
  upperBoundReached      true     boolean
  graphLeveledOff        0        steps
  satSolver              zchaff   solver
  maxStepsNumber         11       steps
  stepsNumber            1        steps
  atomsNumber            0        atoms
  clausesNumber          0        clauses
  encodingTime           0.01     seconds
  solvingTime            0        seconds
  if2sateCompilationTime 1.53     seconds
ATTACK TRACE
  %% no attacks have been found..
```

FIGURE A.2 – Vérification avec SATMC