IoT networks : study of secure mobility solutions and integration into the 5G network

Hassan Jradi

THESE DE DOCTORAT DE

L'INSTITUT NATIONAL DES SCIENCES APPLIQUEES RENNES

ECOLE DOCTORALE N° 601
Mathématiques et Sciences et Technologies de l'Information et de la Communication

ET L'UNIVERSITE LIBANAISE
Ecole Doctorale des Sciences et de Technologie

Spécialité : *Télécommunications*

Par

Hassan JRADI

Réseaux IoT : Etude de solutions de mobilité sécurisée et intégration dans le réseau 5G

Thèse présentée et soutenue à Rennes, le 07/12/2022
Unité de recherche : Institut d'Electronique et des Technologies du numéRique (IETR), INSA Rennes
Centre de Recherche Scientifique en Ingénierie (CRSI), Université Libanaise
Thèse N° : 22ISAR 37 / D22 - 37

Rapporteurs avant soutenance :

Antoine GALLAIS	Professeur, INSA Hauts-de-France
Kinda KHAWAM	Maître de conférences, HDR, Université de Versailles Saint-Quentin-En-Yvelines

Composition du Jury :

Président :	Laurent TOUTAIN	Professeur, IMT Atlantique
Examinateurs :	Anis LAOUITI	Professeur, Télécom SudParis, Institut Polytechnique de Paris
	Antoine GALLAIS	Professeur, INSA Hauts-de-France
	Kinda KHAWAM	Maître de conférences, HDR, Université de Versailles Saint-Quentin-En-Yvelines
	Sahar HOTEIT	Maître de conférences, Université Paris Saclay, CentraleSupélec
Dir. de thèse :	Fabienne NOUVEL	Maître de conférences, HDR, INSA Rennes
Co-dir. de thèse :	Abed Ellatif SAMHAT	Professeur, Université Libanaise

Invités

Samer LAHOUD	Maître de conférences, IUT Saint-Malo
Mohamad MROUE	Maître de conférences, Université Libanaise
Jean-Christophe PREVOTET	Professeur, INSA Rennes

THESE de doctorat en Cotutelle

Pour obtenir le grade de Docteur délivré par

L'Université Libanaise

L'Ecole Doctorale des Sciences et Technologie

Spécialité : Ingénierie en Télécommunications et Réseaux

Présentée et soutenue publiquement par

Jradi Hassan

Le 07/12/2022

Réseaux IoT : Etude de solutions de mobilité sécurisée et intégration dans le réseau 5G

Membres du Jury

M. LAOUITI Anis	Professeur, Télécom SudParis, Institut Polytechnique de Paris
M. GALLAIS Antoine	Professeur, INSA Hauts-de-France
Mme. KHAWAM Kinda	Maître de conférences, HDR, Université de Versailles (UVSQ)
M. TOUTAIN Laurent	Professeur, IMT Atlantique
Mme. HOTEIT Sahar	Maître de conférences, Université Paris Saclay, CentraleSupélec
Mme. NOUVEL Fabienne	Maître de conférences, HDR, INSA Rennes
M. SAMHAT Abed Ellatif	Professeur, Université Libanaise

Acknowledgment

To my supervisors, Pr. Abed Ellatif Samhat, Pr. Fabienne Nouvel and Dr. Mohamad Mroue, I would like to thank you, for your patience, guidance, and support. I have benefited greatly from your wealth of knowledge and research experience. I am extremely grateful that you took me on as a researcher and continued to have faith in me over the years.

Most importantly, I am grateful for my family's unconditional, unequivocal, and loving support.

Immense gratitude as always to my wife for her patience and support.

À mes encadrants Pr. Abed Ellatif Samhat, Pr. Fabienne Nouvel et Dr. Mohamad Mroue, je tiens à vous remercier pour votre patience, vos conseils et votre soutien. J'ai grandement bénéficié de votre richesse de connaissances et de votre expérience de recherche. Je suis extrêmement reconnaissant que vous m'ayez accepté comme chercheur et que vous ayez continué à me faire confiance au fil des ans.

Plus important encore, je suis reconnaissant pour le soutien inconditionnel, sans équivoque et affectueux de ma famille.

Immense gratitude comme toujours à ma femme pour sa patience et son soutien.

Abstract

The Internet of Things (IoT) is a new emerging system of interconnected devices that experiences significant growth in a wide variety of applications. The rising communication technologies are the Low Power Wide Area Networks (LPWANs) having long communication range, low power consumption and low deployment cost. These technologies are suitable for applications requiring a small number of transmissions per day like supply chain tracking and healthcare monitoring.

Mobility is a common behavior of several applications using these technologies, where mobility management becomes an important feature that must be ensured to provide continuous service. Besides, protecting the network security against unauthorized access and data exposure must also be guaranteed by using appropriate security mechanisms. However, the diversity of LPWAN technologies from licensed to unlicensed technologies, and the tight constraints like the allowed payload length and the number of transmissions per day, make the integration of these two features a challenge. Thus, in this thesis, we focus on the design of a secure mobility management solution for LPWAN taking into consideration their constraints.

In the literature, several mobility protocols exist where the most commons are that based on the Internet Protocol version 6 (IPv6) like Mobile IPv6 (MIPv6) and Proxy Mobile IPv6 (PMIPv6). These solutions are designed for traditional computer networks where the LPWAN constraints are not considered. However, recent solutions tried to integrate mobility in LPWAN where they achieve good performance efficiency. Nonetheless, these solutions do not take into consideration the security aspect which makes them vulnerable to several security issues.

The contributions of this thesis can be divided into three parts. In the first part, we propose a solution for device mobility inside the coverage of the same operator. This solution is based on PMIPv6 as a network layer mobility management protocol. For that, we propose an adapted protocol stack that should be used by the device to overcome the drawback of using a network layer as the overhead added, and we propose an adapted network architecture to integrate PMIPv6 entities in the LPWAN architecture where we focus on LoRaWAN and NB-IoT technologies. Furthermore, we propose an authentication scheme that ensures secure access for devices to the network along with several security features.

In the second part, we extend the authentication scheme previously proposed to provide a solution for device mobility between the coverages of different operators where we conserve PMIPv6 as a network layer mobility protocol, the adapted proto-

col stack and the network architecture. The performance of this solution is evaluated according to several metrics such as the handoff delay and the signaling overhead theoretically and by simulation using Network Simulator 3 (NS-3). Likewise, we evaluate the security of this solution according to common security issues as well as mobility-related issues investigated in the literature, and using dedicated software for security evaluation called Automated Validation of Internet Security Protocols (AVISPA). Moreover, we compare the mobility and security features provided by our solution with that of related work to prove the efficiency and the security of our solution.

In the third part, we proposed a new solution for the integration of LoRaWAN technology into the 5G system that allows leveraging the simplicity and cost efficiency of LoRaWAN and the power and scalability features of 5G. The integration is made at two levels which are the core network and the radio access network. Moreover, secure access is provided through new authentication methods that are compatible with LoRaWAN and 5G standards. Later on, we evaluate the performance of this solution according to the same previous metrics by simulation using NS-3. Similarly, we evaluate the security according to security issues presented previously and using AVISPA. Furthermore, we compare our solution with related work to prove the efficiency and the security of our solution.

Résumé en Français

Chapitre 1: Introduction

Contexte

L'internet des objets (IoT) correspond au réseau mondial d'appareils interconnectés, appelés objets, remplissant diverses fonctions grâce auxquelles les gens ont la capacité de surveiller, de prendre des décisions, d'échanger des données et de contrôler des appareils placés dans des endroits éloignés. Le large besoin et la variété des applications IoT ont déclenché l'invention de multiples technologies de communication radio adaptées à ces exigences d'application.

Ces technologies de radiocommunication sont classées en trois grandes catégories selon leurs caractéristiques qui sont la portée de communication, la consommation d'énergie et le débit de données. La première catégorie comprend les Low Rate Wireless Personal Area Network (LR-WPAN) telles que Bluetooth et ZigBee, caractérisées par leur courte portée de communication, leur faible consommation d'énergie et leur faible débit de données. La deuxième catégorie comprend les technologies de réseaux cellulaires à large bande normalisées par le 3rd Generation Partnership Project (3GPP) comme les réseaux cellulaires à large bande de quatrième génération (4G) et de cinquième génération (5G) caractérisés par leur longue portée de communication, leur forte consommation d'énergie, et débit de données élevé. La troisième catégorie comprend les Low Power Wide Area Network (LPWAN) qui ont attiré l'attention au cours des dernières années compte tenu de leurs caractéristiques particulières telles que la longue portée de communication et la faible consommation d'énergie, mais des débits plus faibles.

Motivations et défis

Les technologies LPWAN sont divisées en technologies sous licence et sans licence en fonction du spectre de fréquences utilisé. Parmi les technologies LPWAN sans licence, les technologies Long Range Wide Area Network (LoRaWAN) et Sigfox sont les plus populaires. D'autre part, la technologie NarrowBand-IoT (NB-IoT) a été normalisée par le 3GPP dans la version 13 pour devenir la technologie sous licence développée pour le LPWAN.

Afin de fournir une continuité de service, la gestion de la mobilité est une exigence

primordiale pour les applications de santé et de chaîne d'approvisionnement. Par définition, la mobilité est le déplacement d'un appareil provoquant la libération du lien radio établi avec le point d'accès courant, et l'établissement d'un nouveau lien radio avec le point d'accès suivant. Par conséquent, le appareil pourra retrouver l'accès à la session précédemment établie avec le nœud correspondant (CN). Pour parvenir à une gestion de la mobilité performante avec des exigences qualifiées, une solution de gestion de la mobilité appropriée doit être adaptée. De plus, cette solution doit tenir compte du type de mobilité en cours, qui peut être l'un des quatre types suivants:

- Mobilité homogène ou hétérogène: lorsque l'appareil se déplace de la couverture d'un point d'accès à un autre qui utilise respectivement la même technologie de couche de liaison ou une technologie différente.
- Mobilité intra-domaine ou inter-domaine: lorsque l'appareil passe de la couverture d'un point d'accès à un autre appartenant respectivement au même opérateur de domaine ou à un autre domaine.

Une autre exigence importante prise en compte lors de la conception d'une solution de gestion de la mobilité est la sécurité pour protéger le réseau IoT contre les attaques malveillantes. La conception d'une solution sécurisée de gestion de la mobilité est encore plus compliquée dans les réseaux IoT en raison des limitations existantes des appareils IoT. De plus, la mobilité des appareils soulève des problèmes de sécurité supplémentaires qui ne sont pas présents dans les appareils immobiles. Des contraintes plus strictes existent dans les environnements LPWAN, ce qui entraîne une plus grande complexité lors de la conception de telle solution.

Comme dans l'IoT, le LPWAN hérite du défi de l'hétérogénéité en raison de la diversité des technologies développées où plus de six technologies existent, ce qui en fait l'un des challenges à relever pour parvenir à une adoption et une compatibilité à grande échelle. De plus, les messages échangés dans un réseau LPWAN se caractérisent par leur courte longueur de charge utile. A cette contrainte s'ajoute celle du temps radio limité et un nombre limité de messages échangés par jour. Plusieurs travaux ont tenté de traiter le problème de la gestion de la mobilité dans le LPWAN. Cependant, ces travaux souffrent de limitations en termes de fonctionnalités de sécurité assurées ou d'efficacité des performances. Les défis mentionnés ci-dessus et les limites des travaux existants nous ont motivés à étudier la possibilité de concevoir une nouvelle solution de gestion de la mobilité sécurisée pour LPWAN.

Contributions

L'objectif principal de cette thèse est de proposer une nouvelle solution sécurisée de gestion de la mobilité pour LPWAN en tenant compte des contraintes existantes. Les principales contributions de cette thèse sont les suivantes:

- La proposition d'une solution de gestion de la mobilité intra-domaine basée sur les protocoles de la couche réseau et de la couche adaptation, avec un schéma d'authentification légère assurant un accès sécurisé.
- La proposition d'une extension du schéma d'authentification pour devenir capable de fournir un accès sécurisé en cas d'intra-domaine et d'inter-domaine.

- La proposition d'une solution pour intégrer la technologie LoRaWAN dans le système 5G qui permet à LoRaWAN de bénéficier de l'architecture de 5G basée sur les services, d'une gestion efficace de la mobilité, ainsi que d'autres fonctionnalités.

Chapitre 2: Etat de l'art

LoRaWAN

LoRaWAN est une technologie standard ouverte considérée comme la principale technologie LPWAN de nos jours. LoRaWAN a été fondée en janvier 2015 par Cycleo, une société française, puis reprise par Semtech Corporation qui est maintenant membre de LoRa Alliance. LoRaWAN hérite des fonctionnalités LPWAN telles que la longue portée de communication et la faible consommation d'énergie, en plus de plusieurs fonctionnalités spécifiques à LoRaWAN telles que la communication sécurisée de bout en bout entre l'appareil et l'application, le faible coût de déploiement et la capacité élevée du réseau. Les déploiements de réseaux publics et privés sont possibles avec LoRaWAN qui fournit également une intégration simple avec des plates-formes de réseau courantes.

LoRa est une technique de modulation de la couche physique inventée par Semtech Corporation en 2014. LoRa est basée sur la modulation Chirp Spread Spectrum (CSS) fonctionnant dans les bandes libres industriels, scientifiques et médicaux (ISM). LoRaWAN est une couche de Media Access Control (MAC) normalisée par la LoRa Alliance qui s'exécute au-dessus de la couche physique LoRa. LoRaWAN définit le mécanisme d'accès utilisé lors de la communication des appareils LoRaWAN avec les points d'accès radio du réseau.

LoRaWAN a une architecture réseau star-of-star composée de cinq éléments: end device (ED), passerelle (GW), serveur réseau (NS), serveur de jointure (JS), et serveur d'application (AS). LoRaWAN offre des niveaux élevés de sécurité et de confidentialité puisque seuls les ED authentifiés ont la capacité de rejoindre le réseau et de transmettre des messages. LoRaWAN définit deux types d'activation d'appareils appelées Activation By Personalization (ABP) et Over The Air Activation (OTAA). Dans OTAA, l'ED doit compléter une procédure de jointure pour être authentifié auprès du NS et pour dériver les clés de session nécessaires utilisées lors de la communication avec le NS et l'AS. La procédure de jointure nécessite l'utilisation de plusieurs identifiants et clés racine qui sont sauvegardés dans la mémoire ED et le JS. LoRaWAN définit trois procédures de jointure en fonction de l'emplacement de l'ED: dans le réseau domicilié, en itinérance passive et itinérance active.

NB-IoT

NB-IoT est une technologie LPWAN sous licence normalisée par le 3GPP dans la version 13 en 2016. Elle est développée pour fonctionner avec les réseaux cellulaires à large bande, comme le Long-Term Evolution (LTE) définie dans la version 8, et le Global System for Mobile Communications (GSM), dans des bandes de fréquences

sous licence. Dans la version 14, NB-IoT a été amélioré pour fournir une consommation d'énergie plus faible, des débits de données plus élevés et une précision de positionnement accrue. Le NB-IoT étant intégré dans les réseaux LTE ou GSM, il hérite de leurs architectures réseau, et il est complété par un protocole de communication optimisé pour répondre aux exigences massive Machine Type Communications (mMTC). L'architecture réseau de NB-IoT est nommée cellular IoT (CIoT) Evolved Packet System (EPS). CIoT EPS prend en charge deux optimisations de protocole de communication comme suit: l'optimisation du plan d'utilisateur CIoT EPS et l'optimisation du plan de contrôle CIoT EPS. Vu que l'économie d'énergie est une exigence importante pour les technologies LPWAN, NB-IoT prend en charge l'économie d'énergie de deux manières: mode d'économie d'énergie (PSM) et mode réception discontinue étendue (eDRX).

5G

La croissance rapide du nombre d'appareils connectés et la variété des applications utilisant les réseaux 4G ont motivé la communauté 3GPP à ouvrir la voie à l'étude et au développement des réseaux 5G en mars 2017. L'architecture du système 5G (5GS) se compose du Next Generation Radio Access Network (NG-RAN) et du 5G Core (5GC) connectés via l'interface NG. Les principales motivations de la 5G était de fournir des connexions à haut débit de données, une capacité de réseau élevée, une évolutivité élevée du réseau et une gestion transparente de la mobilité. La communauté 3GPP a travaillé à la conception d'une architecture réseau basée sur les principes suivants: architecture basée sur des services (SBA), le découpage du réseau et la séparation du plan de contrôle et du plan utilisateur.

Le 5GC se compose de plusieurs fonction réseau (NF), et chaque NF a son périmètre d'action dédié. Un opérateur a la possibilité de s'abstraire de certaines NF, cependant, les NF suivantes doivent exister et ne peuvent pas être supprimées: fonction de gestion des accès et de la mobilité (AMF), fonction de gestion de session (SMF), fonction de plan utilisateur (UPF), fonction de gestion unifiée des données (UDM), fonction de serveur d'authentification (AUSF). Le NG-RAN est la partie du 5GS qui connecte l'équipement utilisateur (UE) au 5GC via une liaison radio. L'élément principal constituant le NG-RAN est le point d'accès radio appelé gNodeB (gNB). Le NG-RAN se compose de plusieurs gNB interconnectés via l'interface Xn, et chaque gNB est connecté au 5GC via l'interface NG.

La procédure d'accès dans le 5GS garantit plusieurs exigences de sécurité. Il fournit une authentification mutuelle entre l'UE et le 5GS via l'authentification primaire obligatoire, et entre l'UE et le Packet Data Network (PDN) via l'authentification secondaire facultative. Il assure également le chiffrement et la protection de l'intégrité de Non-Access Stratum (NAS) entre l'UE et l'AMF, la signalisation de contrôle des ressources radio (RRC) entre l'UE et le gNB, et le trafic utilisateur.

Proxy Mobile IPv6

Proxy Mobile IPv6 (PMIPv6) est un protocole de gestion de la mobilité basé sur le réseau dans lequel deux nouvelles entités sont ajoutées au réseau. Une modifi-

cation du réseau est donc nécessaire pour prendre en charge PMIPv6. Ces entités sont responsables du suivi du déplacement du nœud mobile (MN) et du lancement des procédures de signalisation. PMIPv6 est également considéré comme un protocole de gestion de la mobilité locale puisqu'il gère la mobilité au sein d'un même domaine. Les nouvelles entités ajoutées au réseau PMIPv6 sont le Local Mobility Anchor (LMA) et la Mobile Access Gateway (MAG). Le LMA agit comme point d'ancrage topologique pour le MN. Il est chargé de maintenir l'accessibilité du MN au CN et fonctionne avec la MAG pour effectuer le transfert et la procédure de mise à jour de liaison. Le MAG réside sur la liaison d'accès où le MN est ancré. Il est responsable du suivi des déplacements du MN depuis et vers la liaison d'accès, et du lancement de la procédure de mise à jour de liaison au nom du MN vers le LMA. Deux procédures fondamentales sont définies dans PMIPv6, la première est l'attachement du MN lorsque celui-ci s'attache pour la première fois au domaine PMIPv6 contrôlé par le LMA via l'un des MAG. Le second est le transfert du MN lorsque le MN se déplace entre différentes MAG connectées au même LMA.

Problèmes de sécurité dans un environnement mobile

Les réseaux IoT héritent des exigences communes de sécurité du réseau, qui sont la confidentialité, l'intégrité et la disponibilité, largement connues sous le nom de triade CIA, ajoutées à l'authenticité. La mobilité des appareils soulève de nouveaux types de problèmes de sécurité liés à la mobilité des appareils elle-même, et liés à la solution de gestion de la mobilité responsable de la gestion de la mobilité. Ces problèmes de sécurité sont les suivants: authentification de l'appareil, attaque par message d'erreur, fausse demande de remise, usurpation d'identité, adresse squattée, usurpation d'adresse, contrôle de l'ancienne adresse, modification du contexte.

Chapitre 3: Solution sécurisée de mobilité intra-domaine pour les LPWAN

Principes de conception

Dans ce chapitre, nous proposons une solution de gestion de la mobilité intra-domaine basée sur PMIPv6 pour les technologies LPWAN. Nous nous concentrons sur les principales technologies LPWAN, à savoir LoRaWAN et NB-IoT. Dans notre solution, nous utilisons PMIPv6 comme protocole de gestion de la mobilité de la couche réseau. Plusieurs fonctionnalités motivent l'utilisation de PMIPv6 par rapport à d'autres protocoles de gestion de la mobilité de la couche réseau: PMIPv6 est un protocole basé sur le réseau contrairement à MIPv6, FMIPv6 et HMIPv6 qui sont considérés comme des protocoles basés sur l'hôte. De plus, un MN implémentant l'IPv6 élémentaire au niveau de la couche réseau n'a besoin d'aucune modification pour prendre en charge PMIPv6. En complément, la procédure de transfert dans PMIPv6 est réactive ce qui est favorable puisqu'une approche proactive conduit à une signalisation supplémentaire dans le réseau.

Les fonctionnalités prises en charge par PMIPv6 en font un choix de protocole de gestion de la mobilité approprié. Cependant, il y a deux aspects de sécurité essentiels

de PMIPv6 à examiner. Le premier est la sécurité des messages de signalisation échangés lors des procédures de rattachement et de transfert entre la MAG et le LMA. La seconde est l'authentification MN avec le domaine PMIPv6. De plus, les contraintes LPWAN donnent lieu à deux défis qui compliquent l'adaptation PMIPv6 en LPWAN comme suit: les entités PMIPv6, c'est-à-dire MAG et LMA, n'existent pas dans l'architecture LPWAN, et la pile de protocoles de certaines technologies LPWAN ne prend pas en charge IPv6 par défaut.

Solution proposée

Pour intégrer les entités PMIPv6 dans l'architecture LoRaWAN, nous proposons l'architecture réseau illustrée à la Figure 1. Dans LoRaWAN, tout message entrant ou sortant doit passer par le NS, ainsi, ce dernier est considéré comme le point d'ancrage des ED. Dans PMIPv6, le LMA est considéré comme le point d'ancrage de la mobilité pour les MN connectés au domaine PMIPv6, où tout message entrant ou sortant doit le traverser. Pour cela, nous proposons de placer le LoRaWAN NS et le PMIPv6 LMA dans la même entité logique. Le défi réside dans l'intégration du MAG dans l'architecture LoRaWAN. Ce défi augmente puisque tout message de liaison montante envoyé de l'ED au NS peut être reçu et transmis par un ou plusieurs GW en même temps, alors que les messages de liaison descendante envoyés du NS à l'ED sont acheminés via un seul GW.

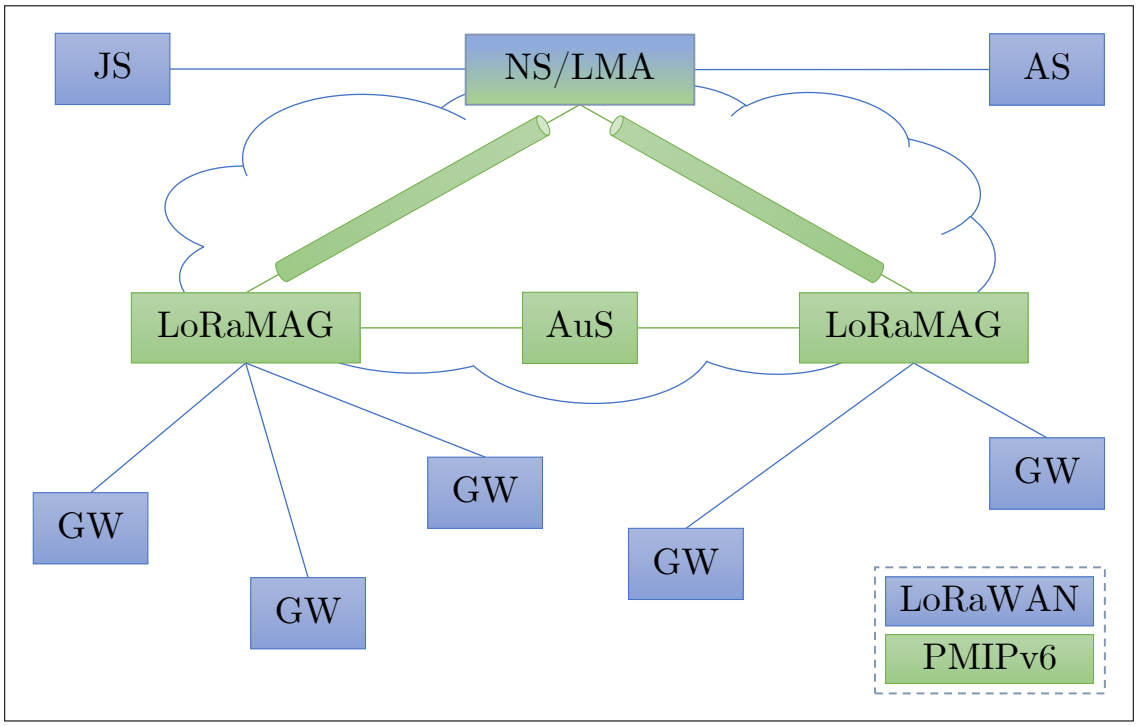


Figure 1: Architecture LoRaWAN évoluée.

Nous proposons d'ajouter une nouvelle entité appelée LoRa Mobile Access Gateway (LoRaMAG) placée topologiquement entre le NS et les GW. Les principales fonctions d'un LoRaMAG sont les suivantes: fonctions liées au LoRaWAN, fonctions liées au PMIPv6, fonctions liées à l'adaptation. En plus de LoRaMAG, une

nouvelle entité appelée serveur d'authentification (AuS) est ajoutée au réseau qui est responsable de l'authentification du MN avec le domaine PMIPv6 pendant les procédures d'attachement et de transfert.

L'interfonctionnement de PMIPv6 avec la technologie NB-IoT dans l'optimisation plan de contrôle CIoT EPS est défini dans les spécifications techniques où l'architecture du réseau, les procédures d'attachement et de transfert sont redéfinies dans LTE.

La communication du plan utilisateur entre le MN et les entités du réseau est donnée par la pile de protocoles illustrée à la Figure 2. Nous proposons d'utiliser IPv6 comme couche réseau pour le routage des données et le partitionnement hiérarchique du réseau. Concernant LoRaWAN, il est considéré comme une technologie de couche liaison. Pour cela, nous proposons d'ajouter la couche réseau entre les couches application et liaison. En ce qui concerne NB-IoT, IPv6 est déjà existant dans la pile de protocoles et configuré par l'optimisation du plan utilisateur lors de la procédure de connexion de l'appareil. Cependant, l'ajout d'une couche réseau pour les technologies LPWAN est difficile en raison des contraintes LPWAN. Pour cela, nous proposons d'utiliser une couche d'adaptation. De cette manière, l'en-tête IPv6 est compressé par la couche d'adaptation de l'expéditeur pour respecter la taille de la charge utile LoRaWAN, puis décompressé par la couche d'adaptation du récepteur dans l'en-tête IPv6 d'origine. Plusieurs algorithmes sont proposés pour compresser l'en-tête IPv6. Cependant, Static Context Header Compression (SCHC) est spécialement conçu pour les LPWAN.

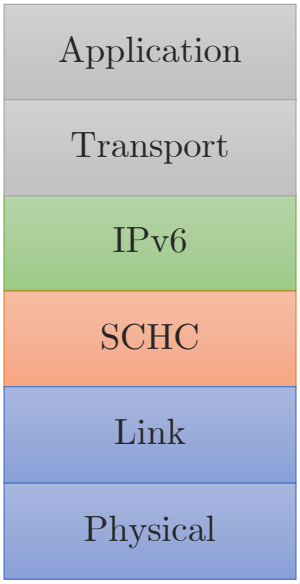


Figure 2: Pile de protocoles de nœud mobile.

Le schéma d'authentification proposé est utilisé pour résoudre le problème d'authentification de MN avec PMIPv6. Ce schéma se compose de deux phases: la phase d'enregistrement exécutée au moment du déploiement du MN et la phase d'authentification exécutée au moment des procédures d'attachement ou de transfert du MN. Ce schéma d'authentification garantit l'authenticité et l'intégrité des

messages de signalisation.

Plusieurs cas de mobilité peuvent se produire. Quel que soit le type, la mobilité est considérée comme se produisant au sein de la même couverture réseau, c'est-à-dire la mobilité intra-domaine. Deux types de mobilité supplémentaires peuvent survenir, appelées mobilité intra-MAG et mobilité inter-MAG. Ces deux types peuvent être combinés avec une mobilité homogène et hétérogène. Ainsi, quatre types de mobilité intra-domaine peuvent exister.

Concernant la procédure de handoff PMIPv6, elle n'est pas exécutée en mobilité intra-MAG homogène, puisque l'identifiant de la couche liaison, l'adresse IPv6 et le contexte SCHC ne changent pas, il n'y a donc pas besoin de mise à jour des informations dans le MN Binding Cache Entry (BCE) stocké dans le LMA. Cependant, la mobilité inter-MAG nécessite l'exécution de la procédure de transfert puisqu'il y a un mouvement entre deux MAG. Une mobilité intra-MAG hétérogène nécessite également l'exécution de la procédure de transfert pour mettre à jour le MN BCE puisque la technologie de couche de liaison et l'identifiant sont modifiés. Concernant l'authentification, elle ne s'exécute pas en mobilité intra-MAG homogène, puisque la mobilité se fait entre plusieurs GW ou eNB connectés à la même MAG.

Dans une mobilité inter-MAG homogène, une authentification est nécessaire car un message de signalisation envoyé par le MN ne peut pas être authentifié par le MAG suivant. Dans une mobilité hétérogène, chaque technologie LPWAN a son propre schéma d'authentification, l'authentification est donc nécessaire dans ce cas. En ce qui concerne l'identifiant de couche liaison, il ne change pas dans une mobilité homogène puisque la technologie utilisée ne change pas, et la mobilité est effectuée à l'intérieur du même réseau attribuant l'identifiant de couche liaison. Cependant, une mobilité hétérogène conduira nécessairement au changement de l'identifiant de la couche de liaison tel qu'il est attribué en fonction de la technologie sous-jacente.

Évaluation des performances et de sécurité

Pour examiner l'efficacité de la solution de mobilité proposée, nous évaluons les performances selon deux métriques principales qui sont le délai de transfert et le surcharge (overhead) de signalisation. Les métriques sont évaluées analytiquement et par simulation. Théoriquement parlant, le délai de transfert est la somme du délai de la procédure de transfert PMIPv6, le délai d'attachement de la couche de liaison, et le délai d'authentification. Cependant, le délai d'authentification est la somme de trois délais principaux qui sont le délai de traitement, les délais des liaisons IP et le délai de liaison radio qui varie en fonction du débit de données utilisé.

Nous avons utilisé Network Simulator 3 (NS-3) pour simuler le schéma d'authentification proposé et évaluer ses performances. La principale métrique prise en compte dans cette simulation est le délai d'authentification qui dépend directement du débit de données utilisé. La plage de débit de données considérée est celle utilisée dans les technologies LPWAN qui sont de l'ordre de 250 bps à 21.9 kbps pour LoRaWAN, et jusqu'à 66 kbps pour NB-IoT. Les résultats sont présentés dans la Figure 3. Nous divisons la gamme de débit de données en trois sous-gammes. La première sous-gamme se situe entre 250 bps et 1.5 kbps, ce qui représente la gamme inférieure des débits de données LoRaWAN et NB-IoT. L'utilisation de cette

plage conduit à un délai d'authentification compris entre 1 et 7 secondes, ce qui peut ne pas être acceptable pour plusieurs applications. Ainsi, nous recommandons l'utilisation de la deuxième sous-gamme qui est comprise entre 1.5 kbps et 20 kbps conduisant à un délai d'authentification inférieur à 1 seconde, délai acceptable pour les applications LPWAN. Nous notons que la limite supérieure du débit de données LoRaWAN est de 21.9 kbps. Quoi qu'il en soit, une troisième sous-gamme peut également être utilisée qui se situe entre 20 kbps et 66 kbps, ce qui conduit à un délai d'authentification inférieur à 140 ms. Cependant, l'augmentation rapide du débit de données ne conduira pas à la diminution prévue de délai d'authentification.

Nous évaluons la sécurité de notre solution en fonction des principales exigences de sécurité et celles liées à la mobilité. L'évaluation porte sur les fonctions de sécurité suivantes: confidentialité, intégrité des messages, authentification mutuelle, actualisation des clés, attaque par relecture, déni de service, usurpation de message de signalisation, squattage d'adresse, usurpation d'identité et contrôle de l'ancienne adresse, modification du contexte. Nous avons utilisé Automated Validation of Internet Security Protocols and Applications (AVISPA) pour évaluer la sécurité de notre schéma d'authentification où l'implémentation est effectuée à l'aide du High Level Protocol Specification Language (HLPSL). Ainsi, après avoir implémenté notre mécanisme à l'aide de HLPSL et exécuté AVISPA, le résultat montre que celui-ci est sécurisé.

Chapitre 4: Solution sécurisée de mobilité inter-domaine pour les LPWAN

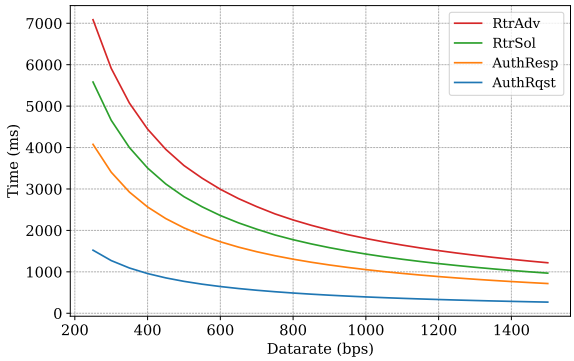
Principes de conception améliorés

Dans le chapitre 3, nous avons proposé une solution de mobilité intra-domaine sécurisée pour les LPWAN. Cependant, la mobilité inter-domaine est un comportement courant et une exigence principale dans plusieurs applications LPWAN. Donc, dans ce chapitre, nous proposons une solution de mobilité inter-domaine sécurisée pour les LPWAN basée sur la solution précédente avec les principes complémentaires suivants: schéma d'authentification étendu, authentification ancrée au domaine visité, l'extension d'authentification optimisée et compatibilité LPWAN.

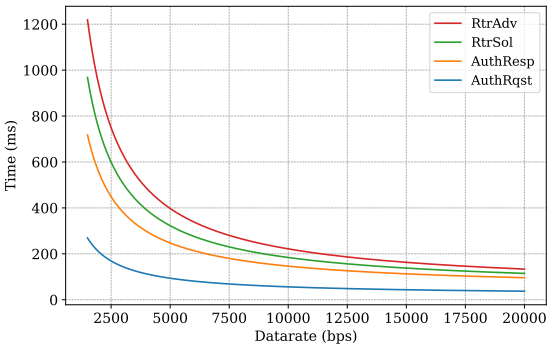
Solution améliorée

L'extension proposée du schéma d'authentification est utilisée pour résoudre le problème d'authentification du MN avec le domaine PMIPv6 en cas de mobilité intra-domaine ou de mobilité inter-domaine. Dans ce chapitre, nous nous concentrons sur le deuxième type où, dans un scénario de mobilité inter-domaine typique, le MN se déplace dans la couverture d'un domaine visité après avoir été dans la couverture de son réseau de domicile déployant la technologie LoRaWAN..

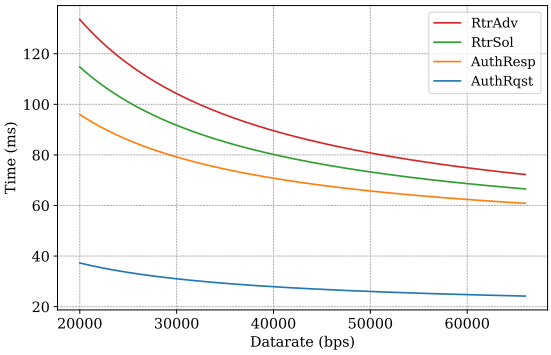
La modification principale est effectuée dans la phase d'authentification pour prendre en charge l'authentification inter-domaine. Cette phase est divisée en deux sous-phases: la sous-phase d'authentification domiciliée et la sous-phase



(a) R_b: 250 bps → 1.5 kbps.



(b) R_b: 1.5 kbps → 20 kbps.



(c) R_b: 20 kbps → 66 kbps.

Figure 3: Résultats de la simulation du délai de l'authentification.

d'authentification visitée. Dans la sous-phase d'authentification domiciliée, le MN envoie sa demande d'authentification qui est transmise à AuS de domicile (hAuS) via l'AuS visité (vAuS). Le hAuS vérifie la validité de la demande d'authentification et dérive deux clés visitées qui sont partagées avec le vAuS qui les utilise dans la sous-phase d'authentification visitée. La sous-phase d'authentification domiciliée est exécutée en cas de mobilité inter-domaine uniquement et une fois par domaine visité. De cette façon, le schéma d'authentification est ancré au domaine visité comme détaillé plus loin. Dans la sous-phase d'authentification visitée, après que hAuS a envoyé les clés visitées à vAuS, ce dernier les utilise pour authentifier le MN tant qu'il se trouve dans le domaine visité sans avoir besoin de transmettre les demandes d'authentification à l'hAuS. Après la sous-phase d'authentification domiciliée, la sous-phase d'authentification visitée peut être répétée plusieurs fois pour authentifier le MN lorsqu'il se déplace entre différents LoRaMAG visités (vLoRaMAG), tout en restant dans le domaine visité.

La gestion de la mobilité intra-domaine est très similaire à la solution précédente où la modification intervient dans la phase d'authentification. Comme défini précédemment, deux cas supplémentaires peuvent se produire, qui sont la mobilité intra-MAG et inter-MAG. Dans la mobilité intra-MAG intra-domaine, le MN envoie un message de signalisation de la même manière que l'authentification normale. Il n'y a aucune procédure supplémentaire qui doit être effectuée dans ce cas. L'authentification de la couche de liaison n'est pas nécessaire car la liaison radio

est toujours active, ce qui est une liaison LoRaWAN. La procédure de transfert PMIPv6 n'est pas nécessaire car le MN ne change pas de vLoRaMAG. Les messages d'attachement, de vérification de profil, de profil trouvé et de vérificateur d'attachement ne sont pas nécessaires puisque la même vLoRaMAG détient le lien de la couche réseau avec le MN. Pour les mêmes raisons, l'adresse IPv6, le contexte SCHC et le tunnel du MN établi entre le vLoRaMAG et le LMA visité (vLMA) ne sont pas modifiés.

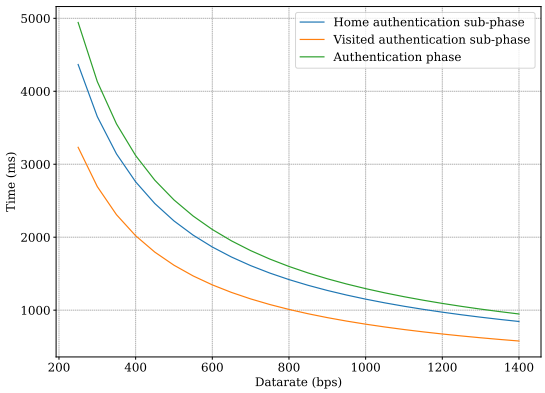
Dans la mobilité intra-domaine inter-MAG, la sous-phase d'authentification visitée doit être exécutée puisque le MN établit un nouveau lien de couche réseau avec le prochain vLoRaMAG nécessitant une authentification de couche réseau. L'événement d'attachement de la couche de liaison ne nécessite pas nécessairement une authentification au niveau de la couche de liaison, où l'événement d'attachement est détecté par le nouveau vLoRaMAG lorsque le MN se trouve dans la couverture d'une GW connectée à cette vLoRaMAG. La procédure de transfert PMIPv6 est nécessaire lorsqu'un nouveau tunnel doit être établi et que le tunnel précédent doit être supprimé. De plus, l'adresse IPv6 et le contexte SCHC peuvent changer.

En mobilité inter-domaine, seule la mobilité inter-MAG est possible, car le MN change nécessairement le vLoRaMAG. Dans ce cas, le schéma d'authentification est entièrement exécuté. Le MN commence par la procédure de jointure au niveau de la couche de liaison où il obtient son nouveau DevAddr. Après cela, le schéma d'authentification est lancé par le MN, où la sous-phase d'authentification domiciliée est exécutée en premier, suivie de la sous-phase d'authentification visitée. Ainsi, le MN obtient les MN-HNP après le schéma d'authentification et configure son interface de couche réseau. Un nouveau tunnel est établi pour ce MN entre le vLoRaMAG et le vLMA, et le tunnel précédent établi entre le vLoRaMAG précédent et le vLMA précédent dans le domaine visité précédent est supprimé après un certain temps selon les spécifications PMIPv6.

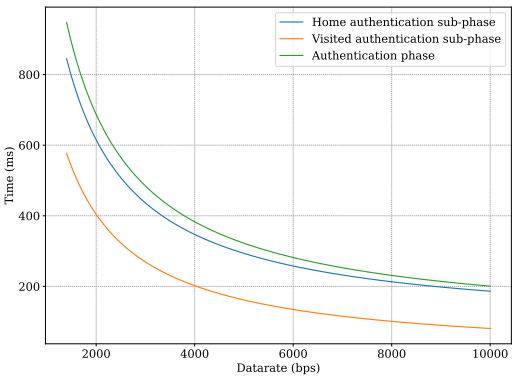
Évaluation des performances et de sécurité

Nous examinons l'efficacité de la solution de mobilité améliorée en évaluant les performances selon deux métriques principales qui sont le délai de transfert et la surcharge de signalisation comme cela a été fait précédemment. De plus, nous montrons comment cette solution peut être déployée dans des environnements LPWAN. Théoriquement parlant, le délai de transfert est la somme du délai de la procédure de transfert PMIPv6, le délai d'attachement de la couche de liaison, et le délai d'authentification. Concernant le délai d'authentification, il dépend du scénario de mobilité qui peut impliquer ou non l'exécution de la sous-phase d'authentification domiciliée. Au cas où il devrait être exécuté, le délai d'authentification est égal à la somme du délai de la sous-phase d'authentification domiciliée et du délai de la sous-phase d'authentification visitée moins un délai de chevauchement entre les deux sous-phases. Dans le cas où la sous-phase d'authentification domiciliée ne devrait pas être exécutée, ce qui se produit lorsque le MN effectue une mobilité intra-domaine, seule la sous-phase d'authentification visitée est exécutée en tant que sous-phase d'authentification de service, et délai d'authentification est égal à délai de la sous-phase d'authentification visitée.

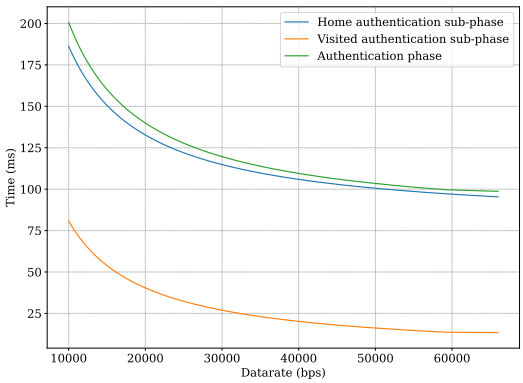
Les principales métriques surveillées dans cette simulation sont le délai de la sous-phase d'authentification domiciliée, visitée et le délai d'authentification. Les délai de la sous-phase d'authentification domiciliée et visitée sont directement liés au débit utilisé, et le délai d'authentification est constitué de leur somme moins un délai de chevauchement qui peut être déduite par simulation. Comme dans la simulation précédente, nous simulons notre solution pour la gamme de débit de données LPWAN, c'est-à-dire entre 250 bps et 21.9 kbps pour LoRaWAN, et jusqu'à 66 kbps pour NB-IoT. Les résultats sont présentés à la Figure 4. Nous divisons la gamme en trois sous-gammes. La première sous-gamme se situe entre 250 bps et 1.4 kbps, ce qui représente la gamme inférieure des débits de données LoRaWAN et NB-IoT. L'utilisation de cette sous-gamme conduit à un délai d'authentification compris entre 1 et 5 secondes, ce qui peut ne pas être acceptable pour plusieurs applications. Ainsi, nous recommandons l'utilisation de la deuxième sous-gamme qui est comprise entre 1.4 kbps et 10 kbps conduisant à un délai d'authentification inférieur à 1 seconde, ce qui est acceptable pour les applications LPWAN. Quoi qu'il en soit, une troisième sous-gamme peut également être utilisée qui est comprise entre 10 kbps et 66 kbps, ce qui conduit à un délai d'authentification inférieur à



(a) R_b: 250 bps → 1.4 kbps.



(b) R_b: 1.4 kbps → 10 kbps.



(c) R_b: 10 kbps → 66 kbps.

Figure 4: Résultats de la simulation du délai de l'authentification.

200 ms, cependant, l'augmentation rapide du débit de données ne conduira pas à la diminution prévue de délai d'authentification. Ainsi, la deuxième sous-gamme est la plus recommandée pour être utilisée dans notre schéma d'authentification étendu. En cas d'authentification intra-domaine, la sous-phase d'authentification domiciliée ne sera pas exécutée, et seule la sous-phase d'authentification visitée est exécutée. Les résultats montrent l'amélioration des performances par rapport à la solution précédente où le délai d'authentification, qui est maintenant égal à délai de la sous-phase d'authentification visitée, peut atteindre un retard compris entre 75 ms et 600 ms dans la deuxième sous-gamme de débit de données. L'évaluation de cette solution améliorée avec d'autres solutions est discutée plus loin.

Cette solution étant conçue pour les technologies LPWAN, nous l'évaluons selon les principales contraintes LPWAN afin de montrer comment cette solution est compatible et peut être déployée dans des environnements LPWAN. En conclusion, cette solution répondait aux exigences LPWAN suivantes: politique d'utilisation, longueur de la charge utile, exigence de stockage.

Nous évaluons la sécurité de notre solution proposée en fonction des principales exigences de sécurité et de sécurité liées à la mobilité présentées précédemment. Plusieurs fonctionnalités de sécurité sont conservées de la solution précédente, à savoir la confidentialité, l'intégrité des messages, la fraîcheur des clés, la prévention du contrôle des anciennes adresses, la résistance aux attaques par relecture et la prévention de l'altération du contexte. Cependant, d'autres fonctions de sécurité sont améliorées comme: l'authentification de l'appareil, attaque par message d'erreur, disponibilité, fausse demande de transfert, authentification mutuelle, usurpation de message de signalisation, squattage et usurpation d'adresse. De plus, nous avons utilisé AVISPA pour évaluer la sécurité de notre schéma d'authentification. Ainsi, après avoir implémenté notre mécanisme à l'aide de HLPSL et exécuté AVISPA, la sortie prouve qu'il est sécurisé.

Solution d'intégration LoRaWAN dans le système 5G

Avantages et principes de conception

Dans ce chapitre, nous proposons une solution pour intégrer la technologie LoRaWAN dans le système 5G (5GS) où l'objectif principal est de tirer partie de la simplicité et du faible coût du LoRaWAN et des fonctionnalités multiples et évolutives de la 5G. Plusieurs avantages peuvent être exploités si cette intégration se fait de manière efficace tels que les avantages : architecture évolutive, fonctionnalité réseau dédiée. Pour cela, les principes de conception suivants doivent être satisfaits lors de la l'intégration: compatibilité entre les normes LoRaWAN et 5G, intégration réseau de niveau N2 dans un réseau plus global, intégration transparente pour les noeuds, bande réseau dédiée.

Solution proposée

Puisque nous intégrons LoRaWAN dans le 5GS, l'architecture réseau adoptée est celle de la 5GS composée de la partie radio (RAN) et de la partie contrôle et données (5GC) comme le montre la Figure 5. Le réseau 5GC est constitué de plusieurs fonctionnalités, auxquelles un ED accédera de façon transparente, au travers du réseau 5GC. Pour cela, l'intégration de l'architecture LoRaWAN dans l'architecture 5GS se fait principalement à deux niveaux. Le premier consiste à intégrer les entités du cœur de réseau LoRaWAN dans le 5GC. La seconde consiste à réaliser une intégration transparente des entités LoRaWAN RAN avec le 5GC.

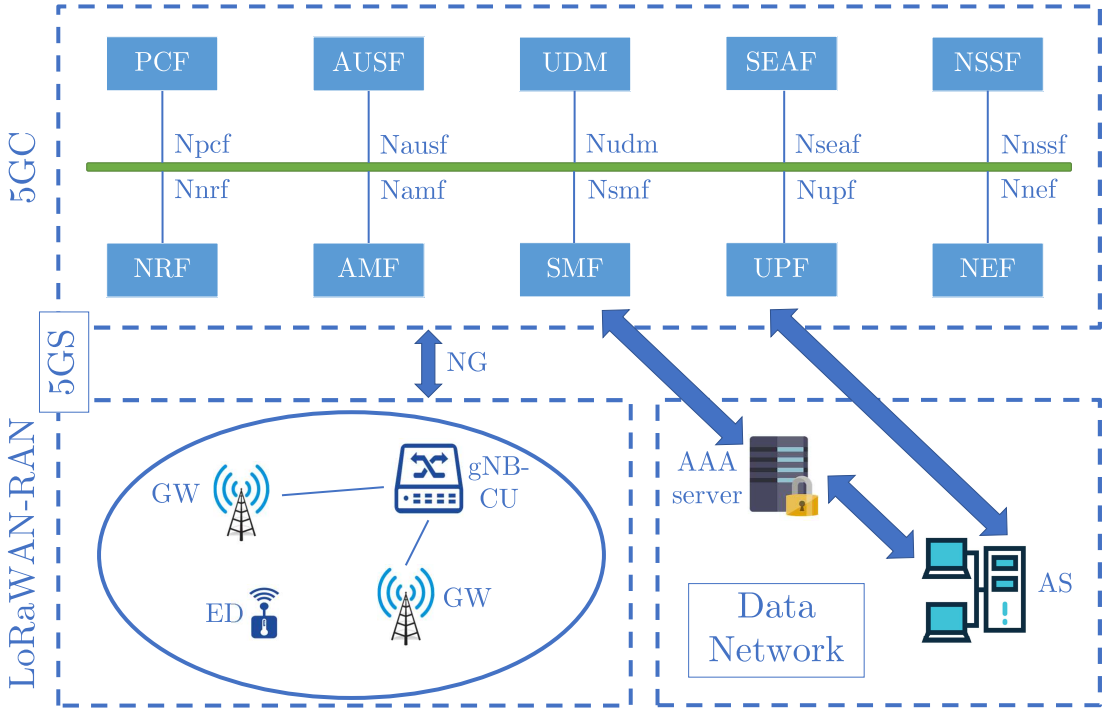


Figure 5: L'architecture de réseau proposée pour l'intégration.

Les fonctions NS et JS sont réparties sur des NFs de 5GC, où l'ensemble de ces NF est identifié à l'aide d'un nouveau S-NSSAI qui représente une tranche de réseau distincte pour LoRaWAN. Dans notre solution, nous proposons que l'ED et l'UDM pré-partagent la clef secrete, enregistrée respectivement dans l'ED USIM et dans la base de données de UDM. L'ED doit posséder un USIM puisqu'il est déployé dans un réseau 5G. L'AUSF effectue l'authentification principale et la dérivation de la clé sur la base de l'authentification EAP-LoRaWAN-CN. En cas d'itinérance, l'AUSF réside dans le domaine du réseau à domicile. Le SEAF a le rôle principal dans l'authentification primaire en cas d'itinérance, il réside donc dans le domaine du réseau visité. L'AMF est responsable de l'accès de l'ED et de la gestion de la mobilité dans le réseau de service. Le SMF est responsable de la gestion des sessions et contribue à l'authentification secondaire. Dans notre solution, l'ED se voit attribuer une adresse IP qui est mappée à son DevAddr dans le gNB-CU. Lorsque l'ED envoie des données de liaison montante, le gNB-CU obtient son adresse IP basée sur DevAddr, puis l'envoie à l'UPF via le 5GC.

Dans la 5G, le RAN se compose de plusieurs gNB, qui se déclinent en gNB Distributed Unit (gNB-DU) connectés à gNB Central Unit (gNB-CU) dans le cas d'un Cloud RAN (C-RAN). Dans notre solution, nous adoptons l'architecture C-RAN pour le RAN, où un LoRaWAN GW agit comme un gNB-DU et maintient ses fonctions LoRaWAN. De plus, gNB-CU sera responsable de l'intégration du LoRaWAN dans la 5G via la fonction d'adaptation.

Le réseau de gestion de données (PDN) est composé d'entités indépendantes du 5GS et non contrôlées par l'opérateur du réseau 5G. Un réseau 5G peut communiquer avec plusieurs PDN, cette communication est gérée par le SMF détenant les informations de session. Les principales entités d'un PDN sont le serveur d'Authentication, Authorization and Accounting (serveur AAA) où son rôle est d'effectuer l'authentification secondaire pour obtenir un accès sécurisé de ED à AS. L'AS est responsable du traitement des données transmises par ED.

LoRaWAN et la 5G déploient leur schéma d'authentification pour garantir un accès sécurisé de l'ED au réseau. Dans notre solution, nous proposons deux méthodes d'authentification basées sur le protocole EAP appelées LoRaWAN over EAP for Core Network (EAP-LoRaWAN-CN), et LoRaWAN over EAP for Data Network (EAPLoRaWAN-DN). Puisque nous travaillons avec un LoRaWAN ED, nous avons réduit le nombre d'opérations nécessaires pour qu'il agisse toujours comme dans LoRaWAN. Ainsi, l'ED n'enverra et ne recevra que la demande de connexion et les messages d'acceptation de connexion comme dans la procédure LoRaWAN, tandis que le reste sera fait par le gNB-CU au nom de l'ED.

Dans notre solution, la couche physique ED est inchangée, la modulation LoRa est donc toujours utilisée là où il n'est pas nécessaire de prendre en charge les accès réseaux 5G. De plus, la couche de liaison ED est inchangée, elle communique toujours à l'aide des commandes LoRaWAN MAC avec le 5GC. En outre, la communication du plan de contrôle entre l'ED et le 5GC est gérée via les fonctions AMF et SMF à l'aide de NAS-Mobility Management (NAS-MM) et NAS-Session Management (NAS-SM). Par conséquent, tout message du plan de contrôle de liaison descendante envoyé par l'AMF ou le SMF à ED ne sera pas compris par l'ED puisqu'il ne supporte que les commandes LoRaWAN MAC, et vice versa pour les commandes MAC LoRaWAN de liaison montante. Pour cela, nous introduisons notre nouvelle fonction appelée fonction d'adaptation implémentée dans le gNB-CU. Cette fonction est responsable de la traduction de NAS-MM/NAS-SM en commandes MAC LoRaWAN et vice versa, de la gestion des procédures spécifiques à l'ED telles que la mise à jour de l'enregistrement, et de la gestion des liaisons radio des GW connectés basée sur le protocole LoRaWAN. Ces interfaces vont introduire une latence qu'il faut minimiser pour être transparent vis à vis des ED.

Évaluation des performances et de sécurité

Nous évaluons les performances de notre solution selon le délai de transfert et de la surcharge de signalisation. Le délai de transfert est égal à la somme du délai de demande de connexion, du délai d'authentification primaire, du délai d'authentification secondaire et du délai d'acceptation de connexion. Nous avons utilisé NS-3 pour simuler les différents délais de notre solution. Nous évaluons les performances de

notre solution selon LoRaWAN SF allant de 7 à 12 comme le montre la Figure 6. Pour une valeur SF de 10, 11 ou 12, les retards dominants sont les délais de demande et d'acceptation de connexion car le débit de données est faible, tandis que les délais d'authentification primaire et secondaire ont une contribution mineure dans le délai de transfert. Pour ces valeurs de SF, le délai de transfert varie entre 1182 ms et 3570 ms. Cependant, pour une valeur SF de 7 à 9, les délais de demande et d'acceptation de connexion deviennent faibles et comparables aux délais d'authentification primaire et secondaire, le délai de transfert se situe entre 416 et 730 ms. Nous comparons également notre solution à la procédure classique de LoRaWAN pour le délai de transfert. Comme le montre la figure 6, notre solution et la procédure LoRaWAN entraînent approximativement le même délai.

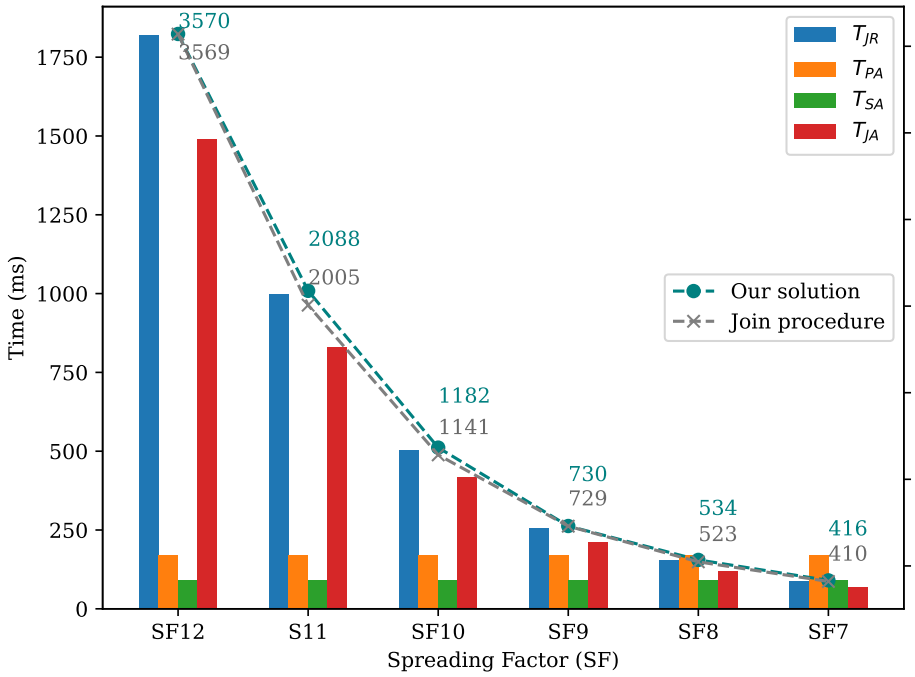


Figure 6: Variation des métriques évaluées en fonction de LoRaWAN SF.

Une métrique importante qui devrait être évaluée est la surcharge de signalisation causée par l'utilisation de messages de signalisation échangés entre l'ED, le gNB-CU et le NF. Nous considérons que la longueur des messages (en octets) représente la surcharge de signalisation. La longueur de chaque message utilisé dans la procédure de connexion LoRaWAN, 5G EAP-AKA', EAP-LoRaWAN-CN et EAP-LoRaWAN-DN est calculée séparément. Plusieurs facteurs, tels que le déplacement de l'ED et l'évanouissement multi-trajets, entraînent une perte de la qualité de la liaison radio entraînant une perte de paquets. Ainsi, la probabilité d'échec (p) d'une liaison radio entraîne une surcharge de signalisation puisque la retransmission est nécessaire pour récupérer les données perdues. La surcharge de signalisation pour chaque tentative de procédure d'accès par ED est représentée dans la Figure 7.

Nous évaluons la sécurité de notre solution proposée en fonction des principales exigences de sécurité et de sécurité liées à la mobilité présentées précédemment. L'évaluation prouve les fonctions de sécurité suivantes: authentification de l'appareil,

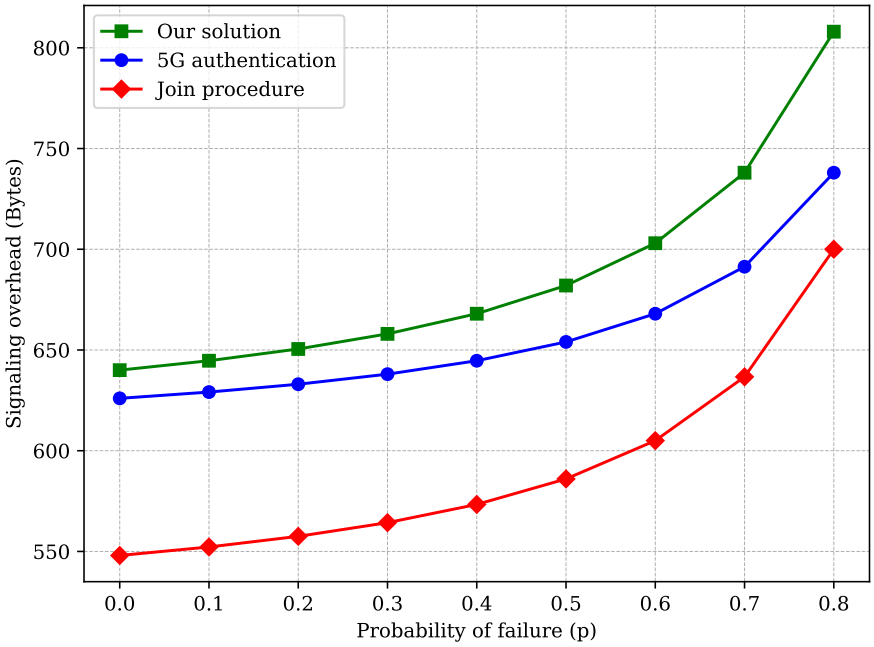


Figure 7: Variation de la surcharge de signalisation des procédures d'accès en fonction de p.

squattage d'adresse, usurpation d'adresse et contrôle de l'ancienne adresse, authentification mutuelle, fraîcheur de la clé, vol ou altération du contexte, et attaque par relecture.

Conclusion

Avec l'avancement et le large déploiement de l'IoT, les technologies LPWAN ont permis de répondre aux exigences des applications nécessitant une faible consommation d'énergie et des fonctionnalités à longue portée. La fonctionnalité de mobilité était une exigence supplémentaire requise par plusieurs applications. Plusieurs types de mobilité existent nécessitant un niveau de sécurité et des mécanismes adaptés.

Nous avons proposé une solution de mobilité intra-domaine basée sur PMIPv6 en tant que protocole de gestion de la mobilité basé sur le réseau. Le problème d'authentification identifié dans PMIPv6 est également considéré, nous avons proposé un schéma d'authentification fournissant un accès sécurisé et résolvant les problèmes de sécurité. Étant donné que la mobilité inter-domaine est un comportement courant et une exigence principale dans plusieurs applications LPWAN, nous avons amélioré la solution proposée par une extension du schéma d'authentification qui permet à l'appareil d'être authentifié en dehors de son domaine d'origine.

Avec l'adoption et le déploiement à grande échelle des réseaux 5G, nous avons identifié les avantages de l'intégration de la technologie LoRaWAN dans le 5GS comme des services faibles coûts et des fonctionnalités de réseau dédiées qui aident en particulier dans le contexte de la gestion de la mobilité. Ainsi, nous avons proposé une solution d'intégration basée sur plusieurs principes de conception qui permettent une intégration efficace telle que la compatibilité avec les normes LoRaWAN et

5G et une intégration transparente pour les appareils ED. De plus, deux nouvelles méthodes d'authentification basées sur EAP sont proposées pour authentifier un appareil LoRaWAN auprès du 5GC de manière à conserver à la fois les spécifications LoRaWAN et 5G. Par ailleurs, une fonction d'adaptation est définie pour la gNB-CU réalisant une intégration transparente et responsable de la traduction des messages de signalisation et de l'exécution des procédures liées au appareil.

Ces solutions sont évaluées en fonction de plusieurs paramètres,puis sont ensuite comparées aux performances d'autres travaux pour prouver les avantages de l'utilisation de nos solutions. En outre, nous évaluons et comparons la sécurité de notre solution à des travaux connexes qui montrent également les fonctionnalités de sécurité assurées dans notre solution.

Publications

Journals

— **H. Jradi**, F. Nouvel, A.E. Samhat, J.-C. Prévotet, M. Mroue. "Secure proxy MIPv6-based mobility solution for LPWAN", *Wireless Networks*, Springer, 2022. DOI: 10.1007/s11276-022-03097-4.

— **H. Jradi**, A.E. Samhat, F. Nouvel, M. Mroue, J.-C. Prévotet. "Overview of the mobility related security challenges in LPWANs", *Computer Networks*, Elsevier, 2021. DOI: 10.1016/j.comnet.2020.107761.

— W. Ayoub, A.E. Samhat, F. Nouvel, M. Mroue, **H. Jradi**, J.-C. Prévotet. "Media independent solution for mobility management in heterogeneous LPWAN technologies", *Computer Networks*, Elsevier, 2020. DOI: 10.1016/j.comnet.2020.107423.

— **H. Jradi**, F. Nouvel, A.E. Samhat, J.-C. Prévotet, M. Mroue. "A seamless integration solution for LoRaWAN into 5G system", submitted to an international journal, 2022.

Conference

— **H. Jradi**, A.E. Samhat, F. Nouvel, M. Mroue, J.-C. Prévotet. "Secure PMIPv6-based mobility solution for LoRaWAN", *in the Twenty-First International Conference on Networks (ICN)*, Barcelona, 2022. ISSN: 2308-4413

Table of Contents

List of Figures

List of Tables

List of Acronyms

3GPP	3rd Generation Partnership Project.
4G	Fourth Generation.
5G	Fifth Generation.
5G-AKA	5G Authentication and Key Agreement.
5G-GUTI	5G Global Unique Temporary Identifier.
5GC	5G Core.
5GS	5G System.
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks.
AAA	Authentication, Authorization and Accounting.
ABP	Activation By Personalization.
AF	Application Function.
AFCntUp	Application Uplink Frame Counter.
AMF	Access and Mobility Management Function.
AMQP	Advanced Message Queuing Protocol.
API	Application Programming Interface.
AppSKey	Application Session Key.
ARPF	Authentication credential Repository and Processing Function.
AS	Application Server.
AS	Access Stratum.
AuS	Authentication Server.
AUSF	Authentication Server Function.
AVISPA	Automated Validation of Internet Security Protocols and Applications.
BCE	Binding Cache Entry.
BW	Bandwidth.
C-RAN	Cloud-RAN.
CDA	Compression Decompression Action.
CIoT	Cellular IoT.
CK	Cipher Key.
CN	Correspondent Node.
CoAP	Constrained Application Protocol.
CP	Control Plane.
CR	Code Rate.
CSPMIPv6	Cluster Sensor PMIPv6.
CSS	Chirp Spread Spectrum.
CUPS	Control and User Plane Separation.
DCHC	Dynamic Context Header Compression.
DCHP	Dynamic Host Configuration Protocol.

DeReg-PBU DeRegistration-PBU.
DevAddr Device Address.
DNN Data Network Name.
DNS Domain Name System.
DoS Denial of Service.
DRB Data Radio Bearer.
DS Distribution Server.
DTLS Datagram Transport Layer Security.

EAP Extensible Authentication Protocol.
EAP-AKA' Improved EAP Method for 3rd Generation Authentication and Key Agreement.
EAP-LoRaWAN-CN LoRaWAN over EAP for Core Network.
EAP-LoRaWAN-DN LoRaWAN over EAP for Data Network.
EAP-TLS EAP Transport Layer Security.
ED End Device.
eDRX Extended Discontinuous Reception.
eMBB Enhanced Mobile Broadband.
eNB Evolved NodeB.
EPS Evolved Packet System.
ETSI European Telecommunications Standards Institute.
EUI Extended Unique Identifier.

FCnt Frame Counter.
FCntUp Uplink Frame Counter.
FCtrl Frame Control.
FHDR Frame Header.
FID Field Identifier.
FMIPv6 Fast MIPv6.
fNS Forwarding Network Server.
FNwkSIntKey Forwarding Network Session Integrity Key.
FOpts Frame Options.
FPMIPv6 Fast PMIPv6.
FPort Frame Port.

gNB gNodeB.
gNB-CU gNB Central Unit.
gNB-DU gNB Distributed Unit.
GSM Global System for Mobile Communications.
GTP-U GPRS Tunneling Protocol for the User plane.
GW Gateway.

hAuS Home AuS.
hLMA Home LMA.
hLoRaMAG Home LoRaMAG.
HLPSL High Level Protocol Specification Language.
HMAG Head MAG.
HMIPv6 Hierarchical MIPv6.
hNS Home Network Server.
HTTP Hypertext Transfer Protocol.

IETF Internet Engineering Task Force.
IK Integrity Key.
IoT Internet of Things.
IPsec IP security.
IPv4 Internet Protocol version 4.
IPv6 Internet Protocol version 6.

ISM Industrial, Scientific and Medical.

JS Join Server.
JSIntKey Join Server Integrity Key.

LMA Local Mobility Anchor.
LoRaMAG LoRa Mobile Access Gateway.
LoRaWAN Long Range Wide Area Network.
LPBA Local PBA.
LPBU Local PBU.
LPWAN Low Power Wide Area Network.
LR-WPAN Low Rate Wireless Personal Area Network.
LTE Long-Term Evolution.

MAC Medium Access Control.
MAG Mobile Access Gateway.
MHDR MAC Header.
MIC Message Integrity Code.
MICS Media Independent Command Service.
MIES Media Independent Event Service.
MIH Media Independent Handoff.
MIIS Media Independent Information Service.
MIPv6 Mobile IPv6.
MME Mobility Management Entity.
mMTC Massive Machine Type Communications.
MN Mobile Node.
MN-HNP MN Home Network Prefix.
MO Matching Operator.
MPL Maximum Payload Length.
MQTT Message Queuing Telemetry Transport.
MSCHC Mobile SCHC.
MType Message Type.

NAS Non-Access Stratum.
NAS-MM NAS-Mobility Management.
NAS-SM NAS-Session Management.
NB-IoT NarrowBand – Internet of Things.
NF Network Function.
NG Next Generation.
NG-AP NG Application Protocol.
NR New Radio.
NS Network Server.
NS-3 Network Simulator 3.
NwkSEncKey Network Session Encryption Key.
NwkSKeys Network Session Keys.

OTAA Over The Air Activation.

P-GW PDN-GW.
PBA Proxy Binding Acknowledgment.
PBQ Proxy Binding Query.
PBU Proxy Binding Update.
PCF Policy Control Function.
PDCP Packet Data Convergence Protocol.
PDN Packet Data Network.
PDU Protocol Data Unit.
PMIPv6 Proxy MIPv6.

PQA Proxy Query Acknowledgment.
PSM Power Saving mode.

QoS Quality of Service.

RAN Radio Access Network.
RAP Radio Access Point.
RAT Radio Access Technology.
RFU Reserved for Future Usage.
ROHC Robust Header Compression.
RRC Radio Resource Control.
RtrAdv Router Advertisement.
RtrSol Router Solicitation.
RU Registration Update.

S-GW Serving-GW.
S-NSSAI Single Network Slice Selection Assistance Information.
SBA Service-Based Architecture.
SCEF Service Capability Exposure Function.
SCHC Static Context Header Compression.
SCMF Security Context Management Function.
SCTP Stream Control Transmission Protocol.
SEAF Security Anchor Function.
SF Spreading Factor.
SHA Secure Hash Algorithm.
SLAAC Stateless Address Auto Configuration.
SMF Session Management Function.
SNID Serving Network Identifier.
sNS Serving Network Server.
SNwkSIntKey Serving Network Session Integrity Key.
SPCF Security Policy Control Function.
SRB Signaling Radio Bearer.
SUCI Subscription Concealed Identifier.
SUPI Subscription Permanent Identifier.

TAU Tracking Area Update.
TCP/IP Transmission Control Protocol/Internet Protocol.
TLS Transport Layer Security.
ToA Time on Air.
TV Target Value.

UDM Unified Data Management Function.
UDP User Datagram Protocol.
UE User Equipment.
UP User Plane.
UPF User Plane Function.
URLLC Ultra Reliable Low Latency Communications.
USIM Universal Subscriber Identity Module.

vAuS Visited AuS.
vLMA Visited LMA.
vLoRaMAG Visited LoRaMAG.
vNS Visited Network Server.

WG Working Group.

XMPP Extensible Messaging and Presence Protocol.

List of Symbols

$\mathbf{K}$	5G key.
$\mathbf{K_{AMF}}$	AMF key.
$\mathbf{K_{AUSF}}$	AUSF key.
$\mathbf{K_{gNB}}$	gNB key.
$\mathbf{K_{NAS_{enc}}}$	NAS encryption key.
$\mathbf{K_{NAS_{int}}}$	NAS integrity key.
$\mathbf{K_{RRC_{enc}}}$	RRC encryption key.
$\mathbf{K_{RRC_{int}}}$	RRC integrity key.
$\mathbf{K_{SEAF}}$	SEAF key.
$\mathbf{K_{UP_{enc}}}$	UP encryption key.
$\mathbf{K_{UP_{int}}}$	UP integrity key.
$\mathbf{L_{HNP}}$	length of MN-HNP.
$\mathbf{L_{H}}$	length of hash.
$\mathbf{L_{ID}}$	length of identity.
$\mathbf{L_{T}}$	length of timestamp.
$\mathbf{MIC_{JA}}$	join accept MIC.
$\mathbf{MIC_{JR}}$	join request MIC.
$\mathbf{p}$	probability of failure.
$\mathbf{R_b}$	data rate.
$\mathbf{R_s}$	symbol rate.
$\mathbf{SO_{Auth}}$	signaling overhead of authentication scheme.
$\mathbf{SO_{Home}}$	signaling overhead of home authentication sub-phase.
$\mathbf{SO_{HO}}$	signaling overhead of handoff procedure.
$\mathbf{SO_{Link}}$	signaling overhead of link layer attachment.
$\mathbf{SO_{PMIPv6}}$	signaling overhead of PMIPv6 handoff procedure.
$\mathbf{SO_{Visited}}$	signaling overhead of visited authentication sub-phase.
$\mathbf{T_{Auth}}$	authentication delay.
$\mathbf{T_{Home}}$	home authentication sub-phase delay.
$\mathbf{T_{HO}}$	handoff delay.
$\mathbf{T_{IP}}$	IP link delay.
$\mathbf{T_{IP}^{Home}}$	IP link delay of home authentication sub-phase.
$\mathbf{T_{IP}^{Visited}}$	IP link delay of visited authentication sub-phase.
$\mathbf{T_{JA}}$	join accept delay.
$\mathbf{T_{JR}}$	join request delay.
$\mathbf{T_{Link}}$	link layer attachment delay.
$\mathbf{T_{Overlap}}$	overlapping delay.

$\mathbf{T_{PA}}$	primary authentication delay.
$\mathbf{T_{PMIPv6}}$	PMIPv6 handoff procedure delay.
$\mathbf{T_{P}}$	processing delay.
$\mathbf{T_{P}^{Home}}$	processing delay of home authentication sub-phase.
$\mathbf{T_{P}^{Visited}}$	processing delay of visited authentication sub-phase.
$\mathbf{T_{R}}$	radio link delay.
$\mathbf{T_{R}^{Home}}$	radio link delay of home authentication sub-phase.
$\mathbf{T_{R}^{Visited}}$	radio link delay of visited authentication sub-phase.
$\mathbf{T_{SA}}$	secondary authentication delay.
$\mathbf{T_{Visited}}$	visited authentication sub-phase delay.

Chapter 1

Introduction

1.1 Context

The Internet of Things (IoT) is the global network of interconnected devices, called things, serving various functions by which people have the ability to monitor, make decisions, exchange data, and control devices placed in distant locations [1]. IoT has seen significant growth in a wide variety of application sectors, including transportation, energy, cities, agriculture, healthcare, and supply chain [2]. Wider deployment of IoT around the world is expected, especially in Western Europe, China, and North America, where the number of IoT devices is anticipated to reach 78 billion in 2025 [3], and the revenue of IoT industry is expected to grow from $892 billion in 2018 to $4 trillion by 2025 [4]. Healthcare represents the major sector of the IoT market with approximately 41% of this market, followed by energy with 33%, and industry with 7%. Other sectors such as cities, agriculture, transportation, and supply chain account for around 15% of the IoT market together [5]. The deployment of an IoT network must follow a rigorous design to attain the intended functionalities that generate the planned economic revenues [6]. The wide need and the variety of IoT applications have triggered the invention of multiple radio communication technologies suitable for these application requirements [7].

These radio communication technologies are classified into three main categories according to their characteristics [8] which are the communication range, the power consumption, and the data rate. The first category consists of Low Rate Wireless Personal Area Network (LR-WPAN) [9] technologies like Bluetooth [10] and ZigBee [11] characterized by their short communication range, low power consumption, and low data rate. The second category consists of broadband cellular network technologies normalized by the 3rd Generation Partnership Project (3GPP) [12] like the Fourth Generation (4G) [13] and Fifth Generation (5G) [14] broadband cellular networks characterized by their long communication range, high power consumption, and high data rate. The third category consists of Low Power Wide Area Network (LPWAN) [15] technologies that attracted attention during the last years considering their special characteristics such as long communication range, and low power consumption required by the major application sector of IoT market, i.e., healthcare, as well as other application sectors [16].

Devices enabled with LPWAN technologies benefit from a communication range of 40 km in rural areas and 10 km in urban areas [17], a battery lifetime of 10 years [18], and a reduced price compared to broadband cellular network devices [19]. LPWAN technologies are primarily designed for applications requiring few messages per day, having short payloads, and sent over a long communication range. LPWAN technologies are divided into licensed and unlicensed technologies according to the used frequency spectrum [20]. Among unlicensed LPWAN technologies, Long Range Wide Area Network (LoRaWAN) [21] and Sigfox [22] are the most popular where more than 170 LoRaWAN operators exist worldwide [23], and Sigfox is deployed in more than 75 countries and regions [24]. On the other side, NarrowBand – Internet of Things (NB-IoT) [25] technology has been normalized by the 3GPP in Release 13 [26] to become the licensed technology developed for LPWAN.

Several years later, intensive efforts collaborated on the completion of the first full set of 5G standards declared in 3GPP Release 15 [27]. However, recent 3GPP releases, including Release 17 [28], and Release 18 [29], are still under development. 5G defines three main application sectors: Enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communications (URLLC), and Massive Machine Type Communications (mMTC). The application sectors served by LPWAN technologies belong to mMTC sector characterized by the huge number of devices sending short messages [30]. In addition, 3GPP approves the deployment of NB-IoT as an LPWAN technology to support mMTC in 5G [31]. Nevertheless, the diversity of applications served in IoT raised various challenges like mobility management and security [32].

1.2 Motivation and challenges

Healthcare IoT allows doctors and hospitals to monitor their patients health status through connected IoT devices like glucometer, blood pressure and heart rate monitoring cuffs [33]. Likewise, supply chain tracking using IoT allows effective tracking and monitoring of the storage conditions of the shipped goods, which improves the quality of services provided to the shipping company and the customer at the same time [34].

In order to provide continuous service, mobility management is a primary requirement for healthcare and supply chain applications that must be ensured [35]. As a definition, mobility is the movement of a device causing the release of the established radio link with the current point of attachment, and the establishment of a new radio link with the next point of attachment [36]. Consequently, the device will be able to regain access to the session previously established with the correspondent node. To achieve competent mobility management with qualified requirements, an appropriate mobility management solution must be adapted, developed, and deployed. Moreover, this solution should consider the type of mobility occurring, which can be one of four types as follow:

- Homogeneous or Heterogeneous mobility [37]: when the device moves from the coverage of a point of attachment to another that employs the same or different link layer technology, respectively. A device can support several link layer technologies that are used to establish the radio link connection.

- Intra-domain or Inter-domain mobility [38]: when the device moves from the coverage of a point of attachment to another that belongs to the same or different domain operator, respectively. A device can move between different domains where each domain has its defined coverage areas.

Another important requirement considered when designing a mobility management solution is security to protect the IoT network from malicious attacks. Designing a secure mobility management solution is further complicated in IoT networks due to the existing limitations of IoT devices such as the processing power, the available storage, and the battery lifetime, which makes the use of traditional security schemes infeasible [39]. Moreover, device mobility raises additional security concerns that are not present in immobile devices such as device authentication, control of device addresses, protection of signaling messages, and secure context exchange [40].

Tighter constrained exists in LPWAN environments leading to more complexity when designing secure mobility management solution. As in IoT, LPWAN inherits the heterogeneity challenge due to the landscape of developed technologies where more than six technologies exist, making it one of the greatest gaps that needs to be addressed to achieve large-scale adoption and compatibility [41]. Furthermore, messages exchanged in LPWAN are characterized by their short payload length, for example, the payload length in LoRaWAN is limited to 222 Bytes. This constraint is more complicated by the limited uplink airtime and the number of messages exchanged per day, for example, LoRaWAN fair use policy recommends an uplink airtime of 30 seconds per day and 10 downlink messages per day [42], likewise, Sigfox allows a total of 144 uplink messages and 4 downlink messages per day [43].

Several works [44–52] have attempted to deal with the problem of mobility management in LPWAN. However, these works suffer from limitations in terms of security features ensured and performance efficiency. The challenges mentioned above and the limitations of existing works motivated us to investigate the possibility of the design of a new secure mobility management solution for LPWAN which will be evaluated based on security and performance.

1.3 Contributions

The main objective of this thesis is to propose a new secure mobility management solution for LPWAN taking into consideration the existing constraints. The main contributions of this thesis are the following:

- The proposal of an intra-domain mobility management solution based on network layer and adaptation layer protocols, with a light authentication scheme ensuring secure access. This solution enables homogeneous and heterogeneous mobility for devices supporting multiple link layer technologies.
- The proposal of an extension of the authentication scheme to become able to provide secure access in case of intra-domain and inter-domain mobility. Thus, the solution is able to provide mobility management in all mobility cases. The efficiency and the security of the solution are evaluated and compared to other works.

- The proposal of a solution to integrate LoRaWAN technology into the 5G system that allows LoRaWAN to benefit the 5G service based-architecture, efficient mobility management, as well as other features, which combines the power of 5G with the simplicity of LoRaWAN.

1.4 Thesis organization

This thesis is composed of four chapters excluding the introduction and the conclusion as presented below.

In Chapter 2, we present the necessary background related to LoRaWAN technology including the network architecture, message format, mobility management, and security framework. Further, we present NB-IoT technology as it is considered the leading licensed LPWAN technology. After that, we explain 5G including the main design principles, the core network and the radio access network, the protocol stack for the communication, and the security framework. Later on, we explain Proxy Mobile IPv6 as a network layer mobility management protocol. Moreover, we present the security requirements and the security issues in mobile environment which are used later during the security evaluation. Regarding related work, we present the works related to the mobility management for IoT networks and LPWANs, and the works related to the integration of LPWAN technologies into 5G.

In Chapter 3, we present our intra-domain mobility solution for LPWANs ensuring homogeneous and heterogeneous mobility. We detail the design principles used in the conception of the mobility solution. After that, we present the proposed solution comprising the network architecture, protocol stack, authentication scheme, mobility management, and a detailed scenario for the operation of solution in case of NB-IoT to LoRaWAN mobility. Thereafter, we evaluate the performance of this solution based on two important metrics, and the security of this solution by security analysis and using a protocol security validation tool.

In Chapter 4, we present our inter-domain mobility solution for LPWANs ensuring also homogeneous and heterogeneous mobility, where this solution is based on the previous one with an extension of the authentication scheme to authenticate the device outside the home network. In addition, we depict how the mobility will be managed, and we detail an inter-domain mobility scenario to clarify the operation of the solution. Thereafter, we evaluate the performance of this solution based on the same previous metrics, and the security of this solution in the same previous way. Later on, we compare the mobility and the security features provided by our solution to that of related work to prove the efficiency of our solution.

In Chapter 5, we present our solution for the integration of LoRaWAN technology into 5G system. We detail the advantages of such integration and the design principles used in our solution. After that, we present the proposed solution comprising the network architecture, two authentication methods based on extensible authentication protocol, and adaptation function achieving the seamless integration. Thereafter, we evaluate the performance of this solution based on three important metrics, the security of this solution in the same previous way, and then we compare our solution to related work based on the performance evaluation metrics and security features to prove its efficiency.

Chapter 2

State of the art

Abstract *— In this chapter, we first present the main concepts used in this thesis. We introduce the leading unlicensed LPWAN technology which is LoRaWAN, its physical layer modulation based on Chirp Spread Spectrum, its link layer operation according to the end device class, the star-of-star network architecture, the security framework ensuring secure end-to-end communication, and the mobility management which allows the end device to communicate with the application from outside its home network. Besides, we introduce NB-IoT as the leading licensed LPWAN technology. Thereafter, we introduce the 5G broadband cellular networks including the design principles, the core and the radio access network, the protocol stack used during the communication, and the security framework. As well, we present Proxy Mobile IPv6 as an important mobility management protocol based on IPv6. In the second place, we present the security issues arising from the device mobility and the mobility management solution employed, as well as several proposed mobility management solutions in IoT and LPWAN environments. Moreover, we present several LPWAN integration solutions into the 5G system which aim to provide enhanced mobility along with further prominent features.*

2.1 LoRaWAN

2.1.1 Overview

LoRaWAN is an open standard technology considered the leading LPWAN technology nowadays [53]. LoRaWAN was founded in January 2015 by Cycleo, a company in France, and later taken by Semtech Corporation [54] which is now a member of LoRa Alliance [21]. LoRaWAN inherits the LPWAN features like the long communication range and the low power consumption, in addition to several LoRaWAN-specific features like the secure end-to-end communication between the device and the application, the low cost of deployment, and the high network capacity. Public and private network deployments are possible with LoRaWAN which also provides simple integration with common network platforms like 'The Things Network' [55]. The latest version of LoRaWAN is v1.1 [56] which is considered in this thesis. In the following sections, we present the main concepts of LoRaWAN.

2.1.2 LoRa layer

LoRa is a physical layer modulation technique invented by Semtech Corporation in 2014. LoRa is based on Chirp Spread Spectrum (CSS) modulation [57] operating in the Industrial, Scientific and Medical (ISM) bands, which takes a modulating signal as input and generates a chirp signal as output. A chirp signal is a continuous sinusoidal signal having a frequency changing continuously over time. This change is linear with respect to the time in case of CSS modulation. A certain time-shifted chirp is generated by the modulator for each input signal, also called a symbol. Thus, having a symbol of N bits needs 2^N different cyclic shifts of the base chirp. N is equal to the Spreading Factor (SF) which varies between 7 to 12. In CSS, the Bandwidth (BW) of the modulated signal is that of the chirp signal. The European ISM band "EU868" ranges from 863 MHz to 870 MHz, and the allowed BWs are 125 kHz and 250 kHz. In USA and Canada, an additional BW of 500 kHz is also allowed where the ISM band "US915" ranges from 902 MHz to 928 MHz.

LoRa reinforces further its robustness against burst interference using diagonal interleaving technique [58], and its robustness against noise using forward error correction [59] where the possible values of Code Rate (CR) are $\frac{4}{5}$, $\frac{4}{6}$, $\frac{4}{7}$, and $\frac{4}{8}$.

The symbol rate (R_s) and the data rate (R_b) formulas are given by 2.1 and 2.2, respectively. These formulas show that the higher the SF, the lower the R_b, thus, the higher the Time on Air (ToA) that a receiver should wait to receive a signal sent by the transmitter. Moreover, a higher SF allows longer coverage range, longer battery lifetime, but shorter payload length [60].

$$R_s = \frac{BW}{2^{SF}} \tag{2.1}$$

$$R_b = SF \times \frac{BW}{2^{SF}} \times CR \tag{2.2}$$

Table 2.1 shows R_b and the Maximum Payload Length (MPL) for different SF and CR values, given that the BW = 125 kHz.

Table 2.1: R_b and MPL for different SF and CR values.

SF	**CR**	**R_b (bps)**	**MPL (bytes)**
SF7	4/5	5470	222
SF8	4/5	3125	222
SF9	4/5	1760	115
SF10	4/5	980	51
SF11	4/6	440	51
SF12	4/6	250	51

2.1.3 LoRaWAN layer

LoRaWAN is a Medium Access Control (MAC) layer standardized by the LoRa Alliance [21] that runs on top of the LoRa physical layer. LoRaWAN defines the medium access mechanism used during the communication of LoRaWAN devices with the Radio Access Points (RAPs). LoRaWAN layer ensures also security, adaptive data rate, and energy control mechanisms.

LoRaWAN specifies three classes of communication between the device and the RAP which are Class A, Class B, and Class C. Anyhow, Class A is necessary to be implemented in all LoRaWAN devices, while Class B and C are optional. The operations of these classes are as follows:

- Class A: an uplink transmission is scheduled by the device each time it has data to send. Two downlink receive windows are scheduled after the transmission. After that, the device cannot be reached for downlink reception. Class A is considered the most effective in terms of power consumption.
- Class B: uplink transmission is similar to Class A. Nevertheless, Class B device opens downlink receive windows which are periodically scheduled, and synchronized based on a beacon frame sent by the RAP. Thus, the device is reachable for downlink reception at regular times. However, a Class B devices consume more power than Class A devices.
- Class C: uplink transmission is similar to Class A. However, a Class C device should still in receive mode after the transmission, i.e., the downlink receive window is open indefinitely after the transmission. This will cause higher power consumption and battery drain.

The protocol stack of the communication between the device and the RAP is shown in Figure 2.1.

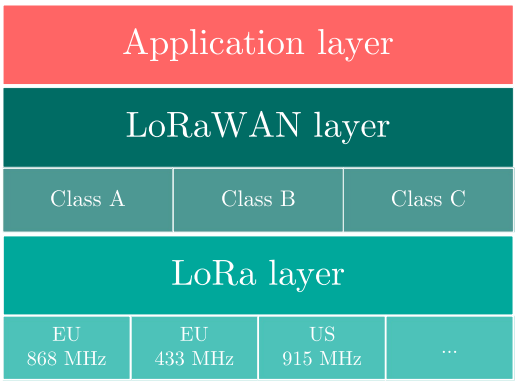


Figure 2.1: LoRaWAN protocol stack.

Further, an important parameter restricting channel access is the duty cycle, which is the time during which the device can occupy the channel as a transmitter. The duty cycle is often regulated by governments, for example, in Europe, the duty cycles are regulated by the European Telecommunications Standards Institute (ETSI) [61]. The ETSI divided the EU868 band into five sub-bands having each its own duty cycle as shown in Table 2.2.

Table 2.2: Duty cycles of EU868 sub-bands.

Label	Band (MHz)	Duty cycle
g	863.0 — 868.0	1%
g1	868.0 — 868.6	1%
g2	868.7 — 869.2	0.1%
g3	869.4 — 869.65	10%
g4	869.7 — 870.0	1%

2.1.4 Network architecture

LoRaWAN has a star-of-star network architecture consisting of five elements as shown in Figure 2.2:

- End Device (ED): the sensor device, like a health monitoring device, sending the captured data to the network as an uplink message.
- Gateway (GW): the RAP to which the ED is connected and acts as a pass-through element that forwards messages in both uplink and downlink directions. The GWs make up the Radio Access Network (RAN) of LoRaWAN.
- Network Server (NS): the core of LoRaWAN network responsible for data routing, control of radio links, data rate adaptation, ED address assignment, and downlink GW selection.
- Join Server (JS): a third-party server holding the ED identifiers and root keys, responsible for the authentication of ED with NS, and for the key derivation.
- Application Server (AS): the server responsible for the processing of data sent by the ED. The data are exposed to the end-user or used to make decisions.

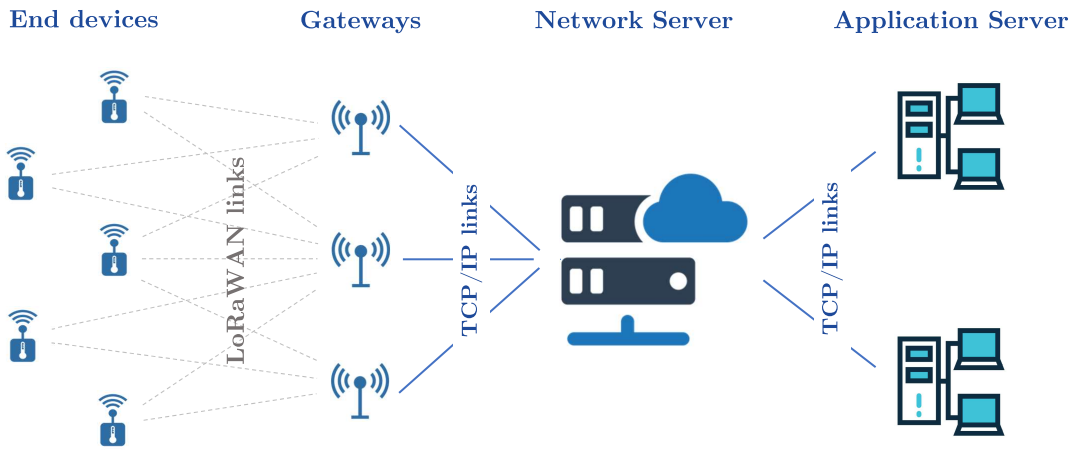


Figure 2.2: LoRaWAN network architecture.

In LoRaWAN, the ED communicates with the GW through a LoRa link, while the communication between the GW and the NS is based on the Transmission

Control Protocol/Internet Protocol (TCP/IP) protocol suite [62]. Regarding uplink transmission, an ED sends an uplink message through the LoRa link. This message can be received by one or more GWs, where each GW forwards the received message to the NS. The NS should eliminate duplicate messages and then send one message copy to the AS. However, in downlink transmission, a downlink message sent from AS to ED is routed through one GW selected by NS according to the radio link conditions.

2.1.5 LoRaWAN message format

The LoRaWAN message format consists of a MAC Header (MHDR), MAC payload, and a Message Integrity Code (MIC) as shown in Figure 2.3.

The MHDR length is eight bits where three bits are dedicated for Message Type (MType) as illustrated in Table 2.3, three bits are Reserved for Future Usage (RFU), and two bits identify the LoRaWAN version named Major. Besides, each message has a 4 Bytes MIC field calculated by the sender and used by the receiver to check the message integrity.

The MAC payload consists of a Frame Header (FHDR), a Frame Port (FPort), and the frame payload. If the FPort byte value is zero, the frame payload contains a MAC command, otherwise, it contains application data. The FHDR consists of 4 Bytes Device Address (DevAddr), 1 Byte for Frame Control (FCtrl) to control the data rate, 2 Bytes Frame Counter (FCnt), and up to 15 Bytes Frame Options (FOpts) transporting MAC commands.

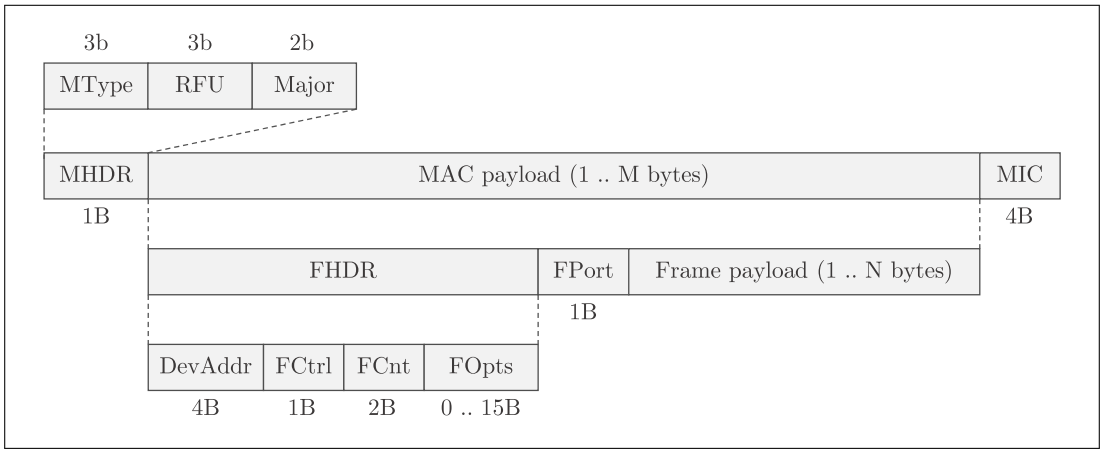


Figure 2.3: LoRaWAN message format.

2.1.6 Mobility management

Several applications using LoRaWAN technology such as healthcare supervision and supply chain tracking require mobility management [63]. Regarding intra-domain mobility, where the ED moves from the coverage of a GW to another that belongs to the same NS, no procedure is required since all the GWs act as pass-through elements and any message sent by an ED will be forwarded to the NS which will process it.

Table 2.3: LoRaWAN MAC message types.

MType	Description
000	Join-request
001	Join-accept
010	Unconfirmed data up
011	Unconfirmed data down
100	Confirmed data up
101	Confirmed data down
110	Rejoin-request
111	Proprietary

Regarding inter-domain mobility, LoRaWAN defines two types which are passive roaming and active roaming [64]. For that, LoRaWAN distinguishes between three types of NS: the Home Network Server (hNS) where the ED is initially registered, the Serving Network Server (sNS) and the Forwarding Network Server (fNS) involved in case of active and passive roaming, respectively.

In active roaming, all the NS functions concerning the ED management are performed by the sNS such as MAC layer control and ED address assignment. In this case, sNS forwards only the LoRaWAN messages to the hNS. In passive roaming, the ED management functions are always performed by the hNS, where the fNS forwards the MAC commands and the LoRaWAN messages between the hNS and the ED. The fNS manages only the GWs constituting its RAN. In non-roaming case, i.e. the ED is within the coverage of a GW belonging to the hNS, the sNS is at the same time the hNS.

2.1.7 Security framework

LoRaWAN provides high levels of security and privacy since only authenticated EDs have the ability to join the network and transmit messages. LoRaWAN defines two types of device activation called Activation By Personalization (ABP) and Over The Air Activation (OTAA). In OTAA, the ED must complete a join procedure to be authenticated with the NS, and to derive the necessary session keys used during the communication with the NS and the AS. The join procedure necessitates the use of several identifiers and root keys which are saved in the ED memory and the JS database as follows:

- DevEUI: the unique identifier of the ED in the Extended Unique Identifier (EUI) address space.
- JoinEUI: the unique identifier of the AS to which the ED will send data, in the EUI address space.
- NwkKey and AppKey: the root keys used to derive the session keys protecting the messages exchanged between ED $\longleftrightarrow$ NS, and between ED $\longleftrightarrow$ AS.

LoRaWAN defines three join procedures according to the ED location: in home network procedure, passive roaming procedure, and active roaming procedure. The join procedure starts with a join request sent by the ED consisting of: JoinEUI, DevEUI and DevNonce. Further, the join procedure ends with a join accept received by the ED consisting of: JoinNonce, NetID, DevAddr, DLSettings, RxDelay, and optional CFList.

The join procedure of an ED in its home network coverage is described below and shown in Figure 2.4.

1. The ED sends a join request which is received by the listening GWs. The GWs identify it as a join request, thus, they forward it to the NS.
2. Using the Domain Name System (DNS) infrastructure specified by the LoRa Alliance [65], the NS lookups at the IP address of the corresponding JS based on JoinEUI sent in the join request, and then, the NS forwards the join request with other parameters to the JS.
3. The JS checks the join request, and if the ED is authenticated, the JS derives the necessary Network Session Keys (NwkSKeys) and the Application Session Key (AppSKey).
4. The JS sends to the NS a join answer consisting of NwkSKeys and the join accept encrypted using NwkKey. In addition, the JS sends the AppSKey to the corresponding AS.
5. The NS sends to the ED the join accept which is checked and used to derive the NwkSKeys and AppSKey.

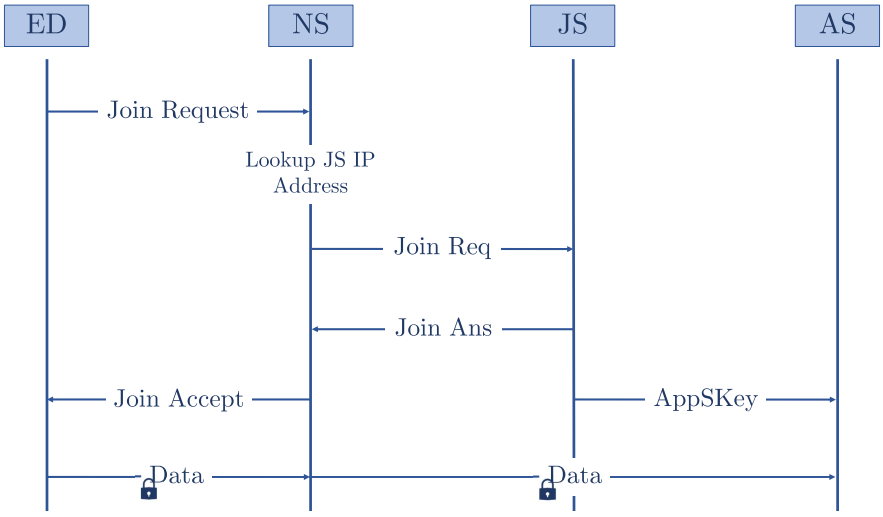


Figure 2.4: LoRaWAN join procedure in home network.

The join procedure of an ED in roaming cases is described below and shown in Figure 2.5.

1. The ED sends a join request which is received by the listening GWs. The GWs identify it as a join request, thus, they forward it to the Visited Network Server (vNS) which may be a sNS or a fNS.

2. Using the DNS infrastructure, the vNS lookups at the IP address of the corresponding JS based on JoinEUI sent in the join request, and then, the vNS sends a hNS request to the JS. Thus, the JS sends the IP address of the hNS to the vNS.
3. The vNS sends a profile request to get the ED information from the hNS. Thus, the hNS replies to the vNS with a profile answer containing the ED information.
4. The vNS sends a passive/handover roaming start request to the hNS containing the join request to ask about the possibility of hosting the ED in the vNS network according to passive/active roaming specifications.
5. The hNS forwards the join request with other parameters to the JS.
6. The JS checks the join request, and if the ED is authenticated, the JS derives the necessary NwkSKeys and the AppSKey.
7. The JS sends to the hNS a join answer consisting of NwkSKeys and the join accept encrypted using NwkKey. In addition, the JS sends the AppSKey to the corresponding AS.
8. The hNS sends a passive/handover roaming start answer containing the join answer to the vNS.
9. The vNS sends to the ED the join accept which is checked and used to derive the NwkSKeys and AppSKey.

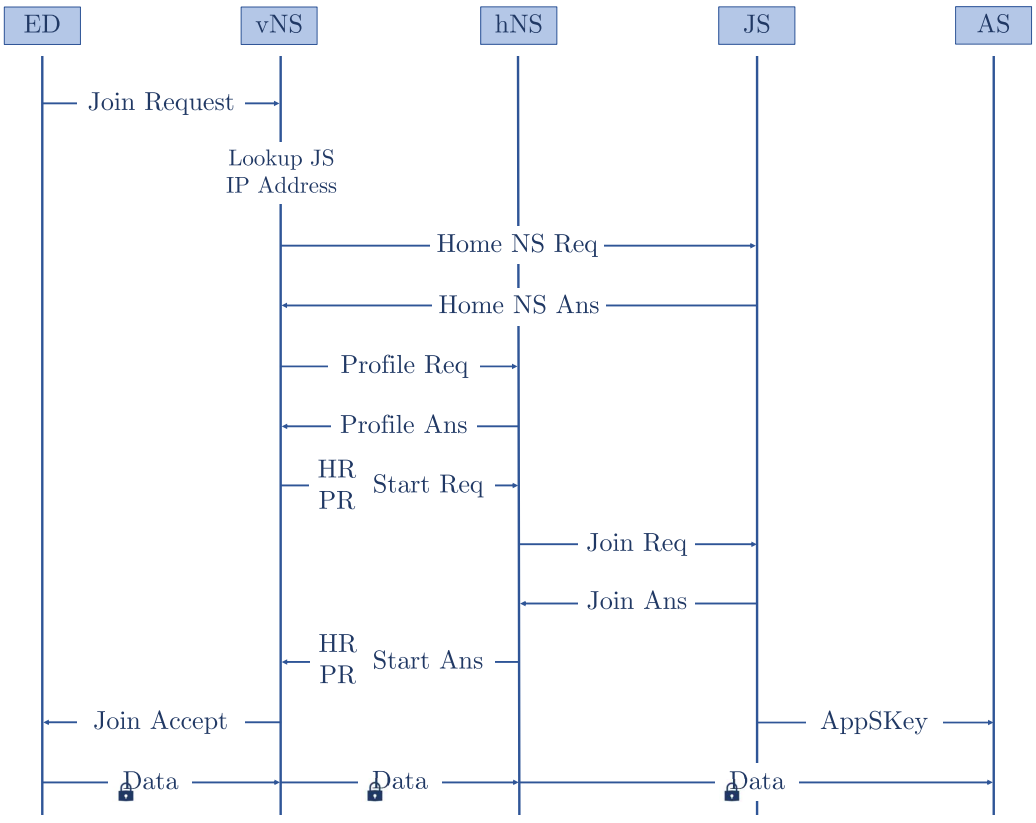


Figure 2.5: LoRaWAN join procedure in roaming cases.

The NwkSKeys derived by the JS are the following:

- Network Session Encryption Key (NwkSEncKey): used to encrypt the content of uplink and downlink MAC commands for home network, passive and active roaming.
- Serving Network Session Integrity Key (SNwkSIntKey): used in case of home network and active roaming to calculate the MIC of uplink and downlink MAC commands.
- Forwarding Network Session Integrity Key (FNwkSIntKey): used in case of passive roaming to calculate the MIC of uplink MAC commands.

The join request MIC (MIC_{JR}) and the join accept MIC (MIC_{JA}) are calculated as follows:

$$MIC_{JR} = aes128\_cmac(\mathbf{NwkKey},\ MHDR \mid JoinEUI \mid DevEUI \mid DevNonce)$$

$$MIC_{JA} = aes128\_cmac(\mathbf{JSIntKey},\ MHDR \mid JoinNonce \mid NetID \mid DevAddr \mid DLSettings \mid RxDelay \mid CFList)$$

The Join Server Integrity Key (JSIntKey) is used in the calculation of MIC_{JA} to protect the integrity of the join accept, and by the ED to authenticate the JS, since only ED and JS can derive it. After the completion of the join procedure, any message sent from the ED to the AS must be encrypted using the AppSKey.

2.2 NB-IoT

NB-IoT is a licensed LPWAN technology standardized by the 3GPP in Release 13 [26] in June 2016. It is developed to work along with broadband cellular networks, like Long-Term Evolution (LTE) defined in Release 8 [66], and Global System for Mobile Communications (GSM) cellular networks, under licensed frequency bands. In Release 14 [67], NB-IoT was further improved to provide lower power consumption, higher data rates, and increased positioning accuracy. Since NB-IoT is integrated into LTE or GSM networks, it inherits their network architectures, and it is assisted by an optimized communication protocol to satisfy the mMTC requirements.

The network architecture of NB-IoT is represented in Figure 2.6, and named Cellular IoT (CIoT) Evolved Packet System (EPS) [68]. CIoT EPS supports two communication protocol optimizations as follows: User Plane (UP) CIoT EPS optimization, and Control Plane (CP) CIoT EPS optimization.

The CP CIoT EPS optimization allows efficient transport of device messages over the Signaling Radio Bearer (SRB) by the Mobility Management Entity (MME) through S1-MME interface, without the trigger of a Data Radio Bearer (DRB) establishment request. The device sends a message to the CIoT RAN point of attachment, called the Evolved NodeB (eNB), which forwards it to the MME. The message may be forwarded by the MME to the AS or CIoT services in two ways. If

the message is an IP packet, it is forwarded by the MME to the Serving-GW (S-GW) through S11 interface, then forwarded by S-GW to PDN-GW (P-GW) through S5 interface, and finally forwarded by the P-GW to CIoT services through SGi interface. However, a non-IP packet is forwarded from MME to Service Capability Exposure Function (SCEF) through T6a interface, then forwarded to CIoT services through T8 interface. The downlink path is the same as the uplink path but in the reverse direction. The CP optimization can support massive connections of more than 52K devices per channel [69].

The UP CIoT EPS optimization allows the Radio Resource Control (RRC) connection to be suspended and resumed, rather than being released and re-established. In LTE, when the device changes from an RRC idle mode to RRC connected mode, a new RRC context must be established with the eNB. However, for devices sending few bytes per packet, establishing an RRC context is considered a significant overhead. Thus, UP optimization allows the RRC context to be saved in the eNB and the device. This context is retrieved and resumed after passing from idle to connected mode. In this case, the messages are transported as the conventional messages traffic using UP DRB to S-GW through S1-U interface, then to P-GW, and finally to CIoT services. This optimization supports IP and non-IP message transport.

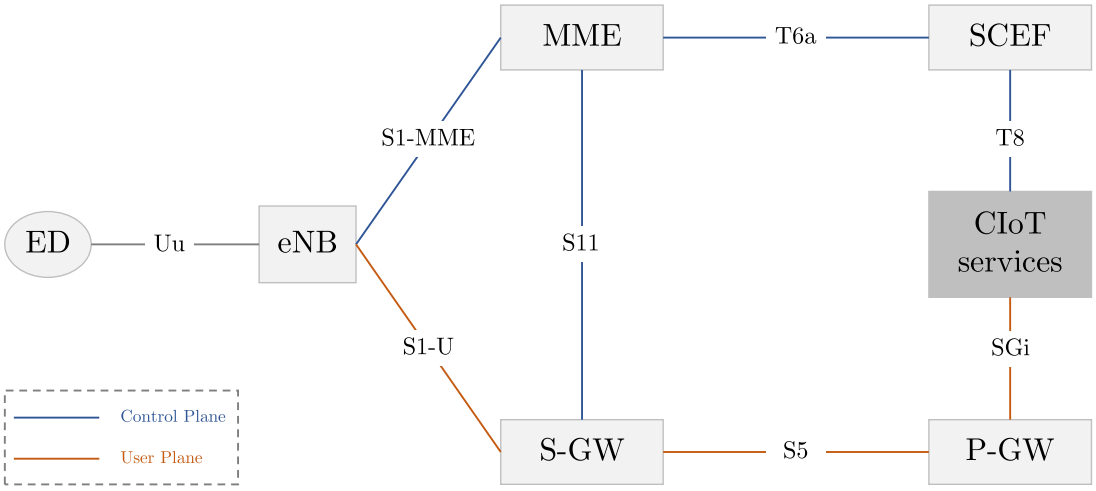
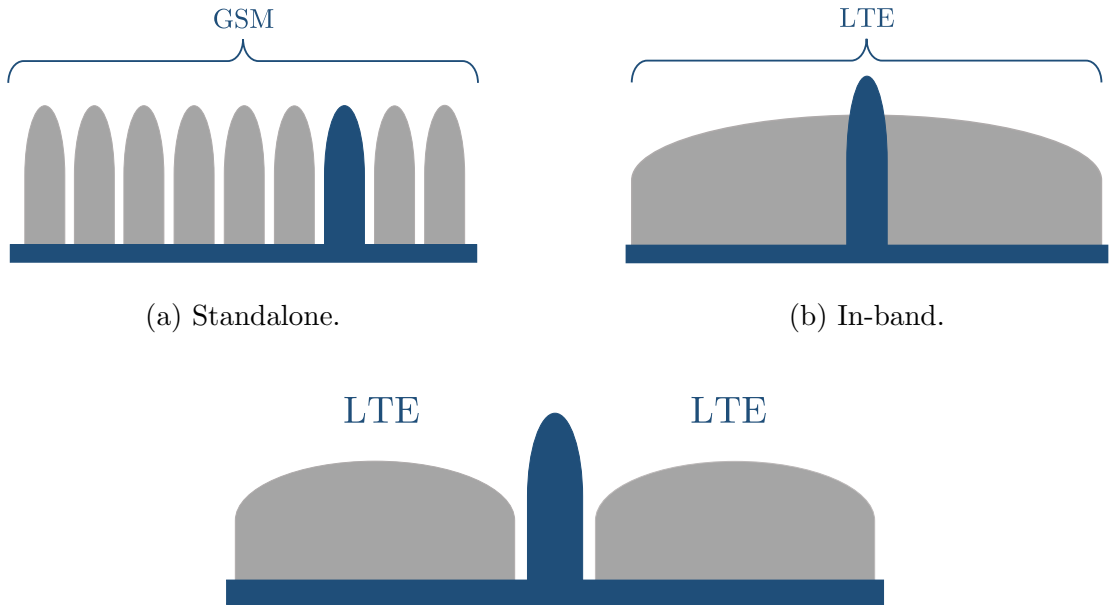


Figure 2.6: NB-IoT network architecture.

The frequency band required for uplink and downlink transmission in NB-IoT is equal to 200 kHz [70]. NB-IoT supports three modes of operation: standalone, in-band, and guard-band [71] as shown in Figures 2.7a, 2.7b, and 2.7c, respectively. In standalone operation, a separated frequency band is dedicated for NB-IoT. For in-band operation, a GSM or LTE frequency band is dedicated for NB-IoT. In guard-band operation, the NB-IoT frequency band is allocated in the LTE frequency guard-band. Regarding the operating data rate range, the peak uplink data rate is 16.9 kbps using single carrier operation, and 66 kbps using multi-carrier operation, while the peak downlink data rate is 26 kbps.

Since power-saving is an important requirement for LPWAN technologies, NB-



(a) Standalone.

(b) In-band.

(c) Guard-band.

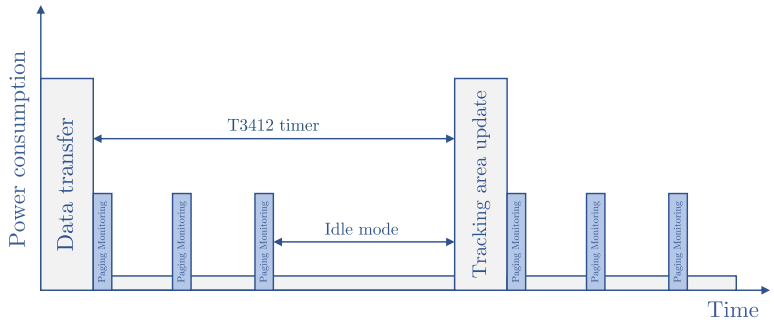
Figure 2.7: NB-IoT modes of operation.

IoT supports power-saving in two ways: Power Saving mode (PSM) and Extended Discontinuous Reception (eDRX) [72] as shown in Figure 2.8a, and Figure 2.8b, respectively. In PSM, the device enters a sleep state after data transmission, and skips the periodic paging channel monitoring after the T3324 timer is elapsed. This mode is used in device-originated traffic or scheduled applications, since the device cannot be reached for a long time. The upper limit for the sleep state is limited by the Tracking Area Update (TAU) timer, named T3412 timer, where the device should monitor paging messages. However, PSM is inappropriate for device-terminated traffic since the device is unreachable for a considerable time, which introduces significant latency and causes problems for time-intolerant applications. For that, eDRX is introduced as a power-saving mode that can be used alone or in conjunction with PSM to attain lower power consumption. eDRX allows the time interval during which the device is not monitoring paging and signaling messages to be extended to 9.22 s, and up to 10485.76 s.

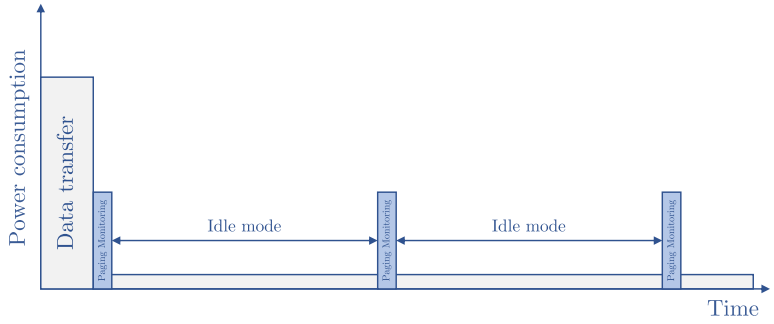
2.3 5G

2.3.1 Overview

The rapid growth in the number of connected devices and the variety of applications severed in 4G networks have motivated the 3GPP community to pave the way for the study and the development of 5G networks in March 2017 [73]. The 5G System (5GS) architecture consists of the Next Generation (NG) RAN and the 5G Core (5GC) connected through the NG interface. The primary consideration in 5G was to provide high data rate connections, high network capacity, high net-



(a) Power Saving Mode (PSM).



(b) Extended Discontinuous Reception (eDRX).

Figure 2.8: NB-IoT power saving modes.

work scalability, and seamless mobility management. In the following sections, we present the main concepts of 5G with particular attention to mobility management and security aspects.

2.3.2 5G design principles

In order to achieve the mentioned network considerations, the 3GPP community worked to design a network architecture based on the following principles:

- Service-Based Architecture (SBA) [74]: to improve the modularity of core networks, the network services in the 5GS are divided into independent Network Functions (NFs) that are exposed by service providers and executed by service consumers through a service-based interface. Thus, instead of defining static interfaces between the network entities, each NF provides a set of services, and any NF can request another NF for a certain service using its Application Programming Interface (API). The communication between the NFs is achieved using one of two mechanisms. The first type is a request-response mechanism where the consumer NF asks the producer NF for a specific service using Hypertext Transfer Protocol (HTTP) [75]. The second type is a subscribe-notify mechanism where the consumer NF subscribes to specific events of the producer NF, and once an event occurs, the producer NF notifies the consumer NF. In this way, any third-party application, called Application Function (AF) is allowed to interact with any 5G NF in a secure way.

- Network slicing [76]: it is the separation of the network physical infrastructure into several virtual networks that are logically isolated, called network slices. A network slice contains a set of NFs that guarantees similar performance requirements and a certain Quality of Service (QoS) for a dedicated service deployment, which improves the deployment flexibility and on-demand scaling of NFs. In a real deployment, several reasons may provoke disruption in a network slice, like unexpected traffic in emergency cases or traffic generated by an attacker. The use of network slicing prevents this disruption from affecting other network slices and guarantees them the required QoS. A network slice is identified using Single Network Slice Selection Assistance Information (S-NSSAI) which is used during the User Equipment (UE) attach process to identify the involved NFs and the required QoS.
- Control and User Plane Separation (CUPS) [77]: due to the increase in the number of smart devices, video streaming users, and industrial automation robotics, user data traffic has doubled over the past few years on an annual basis. At the same time, the demand for high performance and QoS is also growing. CUPS allows independent scaling between UP NFs and CP NFs, thus, the capacity of a UP NF will be directly related to user data traffic. CUPS is enabled by the separation of UP NFs and interfaces from CP NFs and interfaces, and by allowing a CP NF to communicate and control multiple UP NFs through their interfaces. In this way, UP NF may be placed closer to NG-RAN or allocated better connection bandwidth to ensure high performance.
- Access-agnostic core [78]: to minimize the dependencies between the 5GC and the NG-RAN, 5GC is designed on the principle to be independent of the employed Radio Access Technology (RAT) in NG-RAN. Access-agnostic 5GC means that any RAT satisfying the 5G New Radio (NR) specifications [79] can be employed by the UE to reach the network, thus, the NG-RAN is characterized by its heterogeneity due to the existence of several RATs. In order to achieve an access-agnostic 5GC, a common and generalized access framework should be supported by the RAT which can be a 3GPP or non-3GPP technology.

2.3.3 5GC

The 5GC consists of several NFs as shown in Figure 2.9. Each NF has its dedicated scope of operation. An operator has the possibility to abandon some NFs, however, the following NFs must exist and cannot be abandoned:

- Access and Mobility Management Function (AMF): involved in most of 5G procedures like registration and mobility management. It provides CP functions such as Non-Access Stratum (NAS) signaling and Access Stratum (AS) security control. In addition, it manages the tracking areas and controls the paging process which ensures UE reachability in idle mode. Another important role of AMF is to support intra-domain and inter-domain mobility management. The interaction of the AMF with the NG-RAN and the UE is achieved through N2 and N1 interfaces, respectively, using NAS-Mobility Management

(NAS-MM). It also ensures a secure CP connection with the UE through encrypted NAS signaling.

- Session Management Function (SMF): manages the UP connectivity by the creation, modification and release of UE sessions called Protocol Data Unit (PDU) sessions, and IP address allocation for each session. The interaction of the SMF with the UE is achieved through the AMF which forwards the NAS-Session Management (NAS-SM) through N11 interface. A UE can establish several PDU sessions through the SMF, which is useful when a UE needs a voice call and internet connectivity at the same time.
- User Plane Function (UPF): acts as a gateway towards the external IP networks by routing and forwarding UE messages through N6 interface. The UPF is controlled by the SMF through N4 interface. UPF hides the internal UE mobility by providing a stable IP anchor point for connected UEs. UPF sends also traffic usage reports to SMF, and performs a packet inspection process which may be used to apply certain UE-specific policies and analyze the packet contents. Moreover, UPF applies QoS marking for incoming and outgoing packets to achieve suitable queuing and prioritization.
- Unified Data Management Function (UDM): stores UE keys and generates credentials used during the authentication mechanism, such as UE keys, authentication vector, and other UE information. UDM allows a certain level of authorization according to UE subscription, for example, roaming subscribers have different access rules than home subscribers.
- Authentication Server Function (AUSF): executes the authentication mechanism with the UE trying to reach the network. The authentication mechanism is identified by the UE policy stored in the UDM. Additional keys are derived and shared with other NFs to perform the authentication. AUSF is located always in the home network.

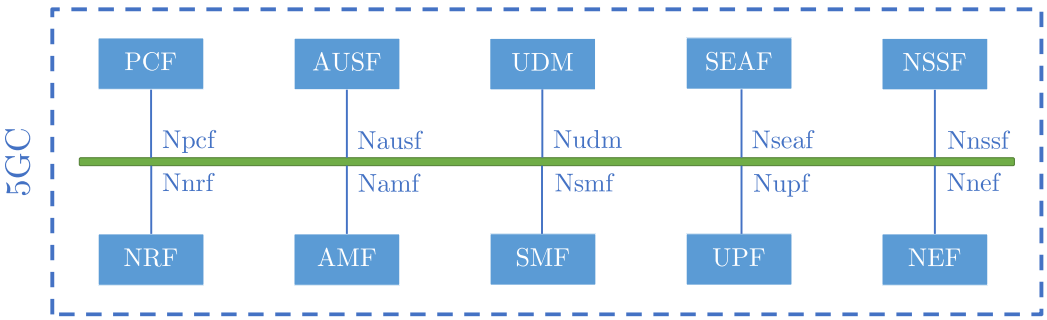


Figure 2.9: 5G core network functions.

2.3.4 NG-RAN

NG-RAN is the part of the 5GS that connects UE to 5GC through a radio link. The main element constituting the NG-RAN is the RAP called gNodeB (gNB). The NG-RAN consists of multiple gNBs interconnected through the Xn interface [80],

and each gNB is connected to the 5GC through the NG interface [81]. The main functions of a gNB are the following [82]:

- Radio resource management including radio admission control, radio bearer control, channel-dependent scheduling, and dynamic bandwidth allocation to maximize the system spectral efficiency.
- Implementation of Packet Data Convergence Protocol (PDCP) [83] incorporating IP header compression using Robust Header Compression (ROHC) [84] algorithm, and IP header encryption and integrity protection.
- Selection of the corresponding AMF during the attach process, and routing of CP messages between UE and AMF.
- Selection and routing of UP messages towards the corresponding UPF identified during the attach process.
- Scheduling and transmission of paging, configuration, and system information messages initiated by the AMF.
- Management of the DRB, measurement and reporting of UE radio link status to AMF, support of network slicing, support and guarantee of the QoS.

Furthermore, a more sophisticated NG-RAN architecture called Cloud-RAN (C-RAN) is possible as shown in Figure 2.10. In C-RAN, the gNB is decoupled into a gNB Central Unit (gNB-CU) and gNB Distributed Unit (gNB-DU) to separate gNB functionalities into higher and lower layer functions, which improves the deployment flexibility and the function usage efficiency. A gNB-CU may be connected to several gNB-DUs, where a gNB-CU and a gNB-DU are connected through F1 interface [85].

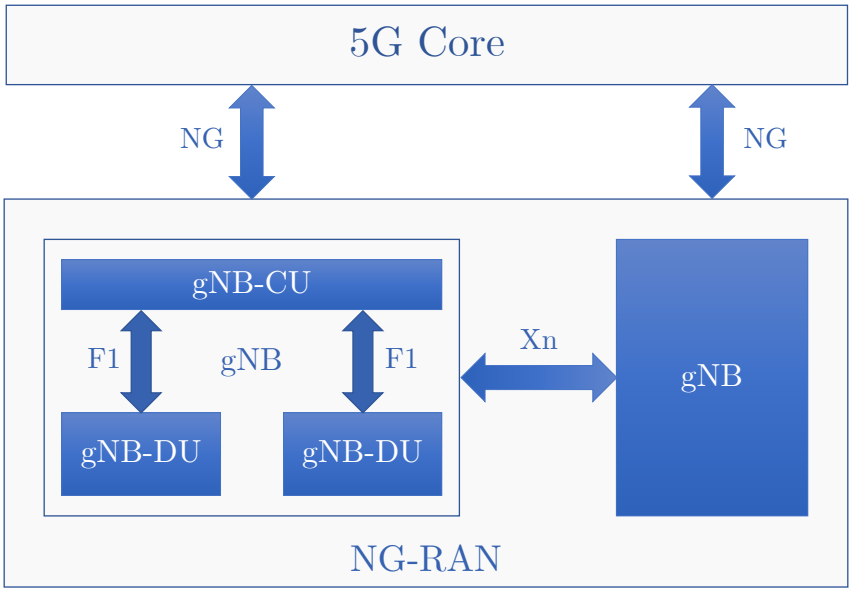


Figure 2.10: Cloud-RAN.

In this context, the gNB-CU is responsible for encoding the system information, providing paging information to gNB-DU, calculating the paging area, and mapping the QoS flows with the corresponding radio bearer. The gNB-DU is responsible

for encoding the remaining system information, transmitting paging information provided by gNB-CU, combining the paging records, and encoding the radio resource management messages.

Since CUPS is a key feature of 5G, NG interface is divided into NG-C and NG-U sub-interfaces, Xn interface is divided into Xn-C and Xn-U sub-interfaces, and F1 interface is divided into F1-C and F1-U sub-interfaces.

In order to achieve a reliable and impeccable connection between the NG-RAN and the 5GC, the NG interface implements the following functions:

- Transport of UP and CP messages between the UE and the 5GC.
- Transmission of paging requests sent from the AMF to the gNBs that belong to the paging area specified in the request.
- Maintaining and management of UE contexts that allow the AMF and the gNBs to create, modify, exchange, and release the UE contexts.
- Intra-domain mobility support which allows the preparation, execution, and termination of the handover procedure.
- PDU session management which allows the creation, modification, and release of the PDU sessions whenever a UE is connected to a gNB.
- Management of the NG interface itself to update any system change, the control of the connection parameters, and ensure NG-RAN to 5GC reachability.

The communication between the gNBs is ensured using the Xn interface implementing the following functions:

- The transfer of signaling information and user traffic.
- The mobility management of UEs which are in connected mode.
- The transfer of UE context during the mobility management from the current gNB serving the UE to the next gNB which will serve the UE.
- The control of UP tunnels between the current gNB and the next gNB during mobility.

2.3.5 Protocol stack

2.3.5.1 Control-plane protocol stack

The CP is used to enable NAS signaling between the UE and the 5GC. There exist several NAS protocols like NAS-MM and NAS-SM. Since AMF is the CP entry point in 5GC, NAS messages are exchanged between AMF and UE through N1 interface. The radio link transporting the CP messages is called the SRB. However, a direct connection between UE and AMF does not exist, and the NG-RAN makes the necessary bridge for this connection. The interface between the UE and the gNB is referred to Uu interface, where the NAS message is sent through this interface using the employed RAT. The interface between the gNB and AMF is referred to N2 interface. This interface uses IP at the network layer, and uses Stream Control Transmission Protocol (SCTP) [86] at the transport layer to guarantee the delivery of signaling messages created by the NG Application Protocol (NG-AP) [81].

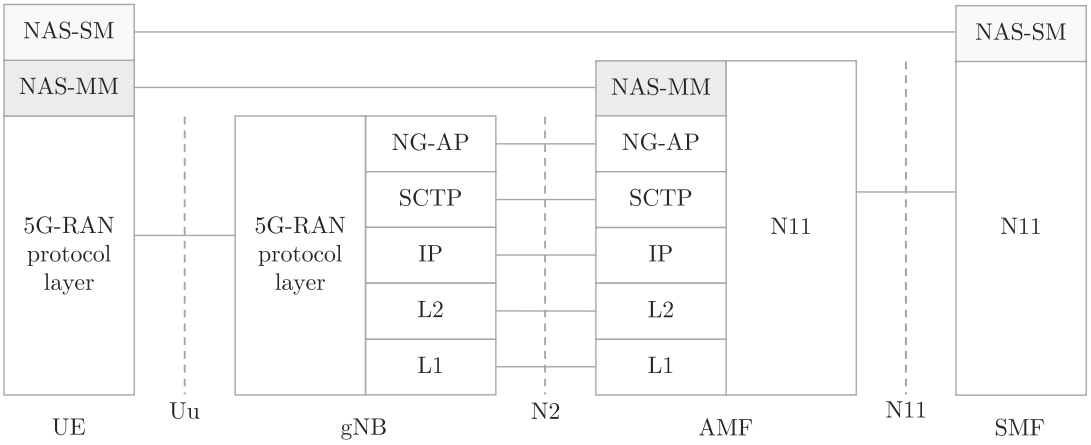


Figure 2.11: Control-plane protocol stack.

The NAS-MM layer in the protocol stack creates NAS-MM messages to execute NAS procedures that terminate at AMF such as location management and registration update. However, the NAS-MM layer encapsulates all the other NAS protocols inside it like NAS-SM. NAS-SM layer creates NAS-SM messages to execute NAS procedures that terminate at SMF such as session establishment and session modification. When a NAS-MM encapsulating a NAS-SM inside reaches the AMF, the latter decapsulates and forwards it to SMF through N11 interface. The CP protocol stack is shown in Figure 2.11.

2.3.5.2 User-plane protocol stack

The UP is used to enable the transport of PDU session data between the UE and the Packet Data Network (PDN). The UP uplink path begins with the UE sending messages via the RAT to the gNB through Uu interface. The radio link transporting the UP messages is called the DRB. A PDU session data is forwarded by the gNB to the corresponding UPF through N3 interface. N3 interface uses IP at the network layer, and uses User Datagram Protocol (UDP) [87] at the transport layer. To encapsulate multiple UE messages over a single link, N3 interface uses

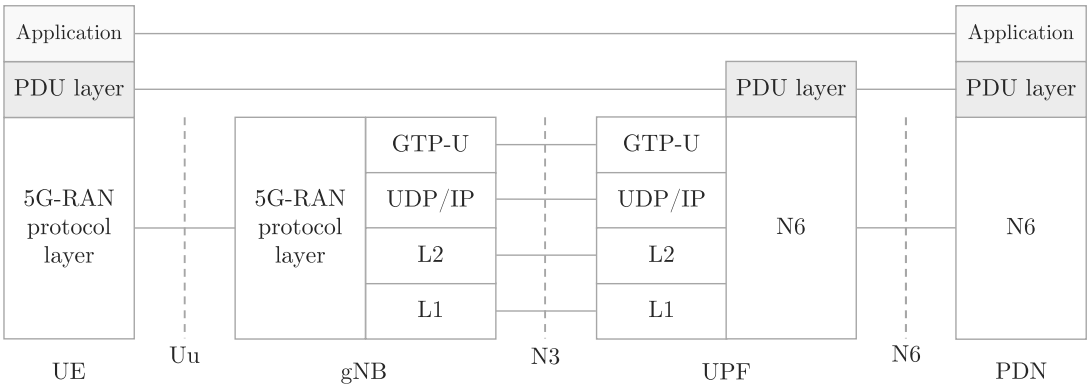


Figure 2.12: User-plane protocol stack.

GPRS Tunneling Protocol for the User plane (GTP-U) [88] multiplexing the traffic from multiple PDU sessions. This layer also supports the QoS flow marking to guarantee the QoS required by each application. In several cases, the UPF may be not the PDU session anchor point, thus the UPF forwards the messages to the PDU session anchor UPF through N9 interface. The UP protocol stack is shown in Figure 2.12.

2.3.6 Security framework

2.3.6.1 Security architecture

The 5GC NFs involved in the 5G security architecture [78] are the following: Security Anchor Function (SEAF), Security Context Management Function (SCMF), AUSF, Authentication credential Repository and Processing Function (ARPF), and Security Policy Control Function (SPCF), as shown in Figure 2.13.

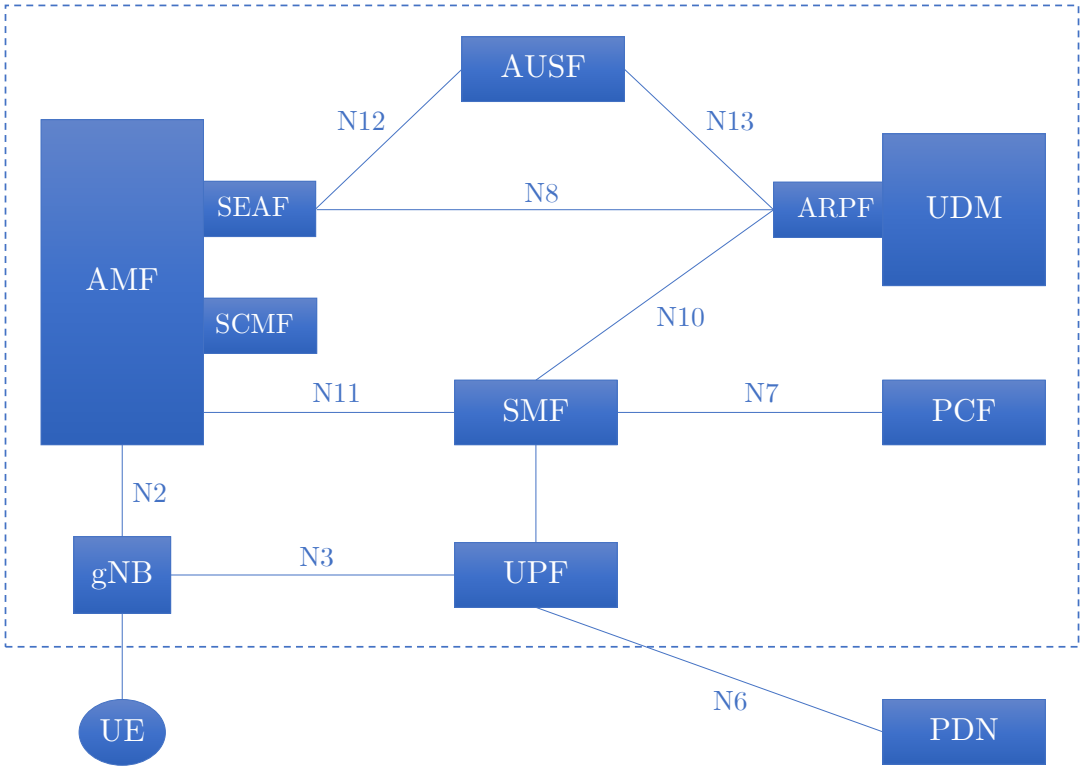


Figure 2.13: 5G security architecture.

The SEAF is considered the security anchor point for UEs outside their home network, i.e., in visited network, and co-located with the AMF. In this case, SEAF drives a unified anchor key, named SEAF key (K_{SEAF}), used by the UE and the visited network to derive the rest of the keys and to protect the coming communications. The SCMF is also co-located with the SEAF in the AMF. The SCMF is responsible for deriving other access network keys from K_{SEAF}. As mentioned before, the AUSF is responsible for the execution of the authentication mechanism, the termination of the requests sent from SEAF through N12 interface, and the

interaction with ARPF co-located with UDM through N13 interface. The ARPF stores the subscribed UEs long-term secret credentials such as the 5G key (K), and derives the authentication vector during the authentication by performing the required cryptography algorithms on the input credentials. The SPCF provides the security policy specified for each UE like the AUSF selection, integrity and confidentiality protection algorithms, and key life cycle. SPCF may be co-located with the Policy Control Function (PCF) in the 5GC.

2.3.6.2 Key hierarchy

The key hierarchy representing the key derivation in 5G from the network side and UE side is shown in Figure 2.14. K stored in ARPF is used to derive the Cipher Key (CK) and the Integrity Key (IK). According to the authentication method, CK and IK are used to derive the AUSF key (K_{AUSF}) directly or indirectly. ARPF sends K_{AUSF} to AUSF during the authentication. If the authentication succeeds, AUSF derives K_{SEAF} used by SEAF as described previously. The AMF key (K_{AMF}) is derived by SEAF from K_{SEAF}. K_{AMF} is used to derive the keys needed to protect the NAS signaling exchanged with the UE which are the NAS encryption key ($K_{NAS_{enc}}$) and the NAS integrity key ($K_{NAS_{int}}$), in addition to the gNB key (K_{gNB}). AMF sends K_{gNB} to the corresponding gNB, which uses it to derive the RRC encryption key ($K_{RRC_{enc}}$) and the RRC integrity key ($K_{RRC_{int}}$) used to protect the RRC signaling, in addition to UP encryption key ($K_{UP_{enc}}$), and UP integrity key ($K_{UP_{int}}$) used to protect the UP traffic.

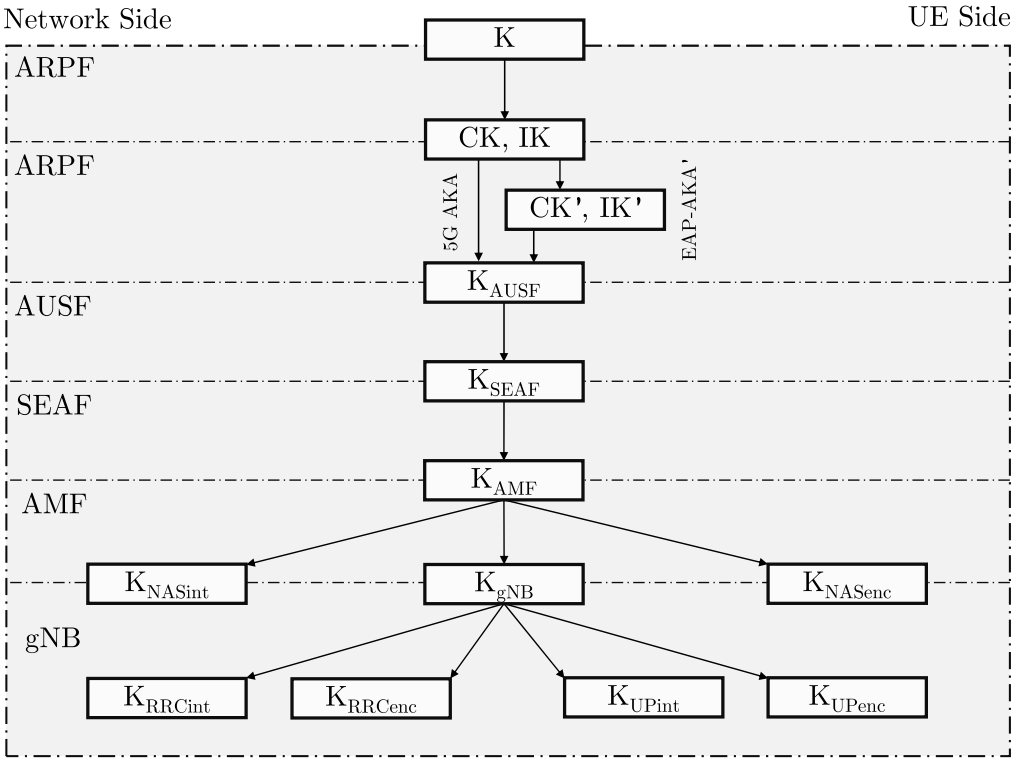


Figure 2.14: 5G key hierarchy.

2.3.6.3 Identifiers

The main identifiers used in the 5GS are the following:

- Subscription Permanent Identifier (SUPI): the unique and permanent subscription identifier assigned by the 5GS for each subscriber. This identifier should not be transmitted in plain text in any case over the radio link.
- Subscription Concealed Identifier (SUCI): since SUPI should not be transmitted in plain text, SUCI is the concealed form of SUPI derived according to a protection scheme and using the home network public key.
- 5G Global Unique Temporary Identifier (5G-GUTI): a temporary identifier assigned by the AMF to the UE after a successful authentication.
- Serving Network Identifier (SNID): the identity of the network to which the UE is attached.
- Data Network Name (DNN): the identifier or the name of the PDN.

2.3.6.4 Access Procedure

The access procedure in the 5GS ensures several security requirements. It provides mutual authentication between the UE and the 5GS through the mandatory primary authentication, and between the UE and the PDN through the optional secondary authentication. It also provides encryption and integrity protection of: the NAS signaling between the UE and AMF, the RRC signaling between UE and gNB, and the UP traffic. Additionally, the UE SUPI is concealed to protect the UE privacy through the use of SUCI. The access procedure ensures separation of visited networks keys through SEAF, thus a UE trying to access through different visited networks will derive different K_{SEAF}.

The primary authentication is achieved using one of three mechanisms: 5G Authentication and Key Agreement (5G-AKA) [78], Improved EAP Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') [89], and EAP Transport Layer Security (EAP-TLS) [90]. EAP-AKA' is similar to 5G-AKA in terms of elements used during the authentication, however, EAP-AKA' uses Extensible Authentication Protocol (EAP) [91] messages including EAP-REQUEST, EAP-RESPONSE, EAP-SUCCESS, and EAP-FAILURE to deliver 5G-AKA elements. The EAP-AKA' authentication method in case of roaming is shown in Figure 2.15 and detailed below:

1. The UE sends an authentication request containing SUCI to AMF/SEAF through N1 interface. The AMF/SEAF checks the validity and the home network of the requested SUCI, then forwards it to the home network AUSF along with the visited SNID using Nausf _ UEAuthentication _ AuthenticateRequest service. The AUSF forwards this request to UDM/ARPF using Nudm _ UEAuthentication _ GetRequest service.
2. UDM/ARPF de-conceals SUCI into SUPI and then gets the corresponding UE policy and other information including the authentication method from SPCF. Thereafter, ARPF generates the authentication vector containing RAND, AU

TN, XRES, CK', IK', and K_{AUSF}, then sends it to AUSF using Nudm _ UEAuthentication _ GetResponse service.

3. AUSF generates the EAP-REQUEST containing the AKA challenge (RAND, AUTN) to SEAF using Nausf _ UEAuthentication _ AuthenticateResponse service. The SEAF forwards this message to UE through N1 interface.
4. The UE computes the response RES to the challenge (AUTN,RAND) and sends an authentication response with EAP-RESPONSE containing RES to SEAF through N1 interface. The SEAF forwards the response to AUSF using Nausf _ UEAuthentication _ AuthenticateRequest service.
5. The AUSF validates RES according to XRES. If the validation passes, AUSF derives K_{SEAF}.
6. The AUSF sends EAP-SUCCESS to SEAF using Nausf _ UEAuthentication _ AuthenticateResponse service containing K_{SEAF}. The SEAF gets its key K_{SEAF} and forwards the EAP-SUCCESS message to UE through N1 interface.
7. The AMF detects the success of the authentication, thus it derives a 5G-GUTI for the UE and then sends it in the authentication response.
8. The UE, AMF and gNB derive the CP and UP keys as described before.

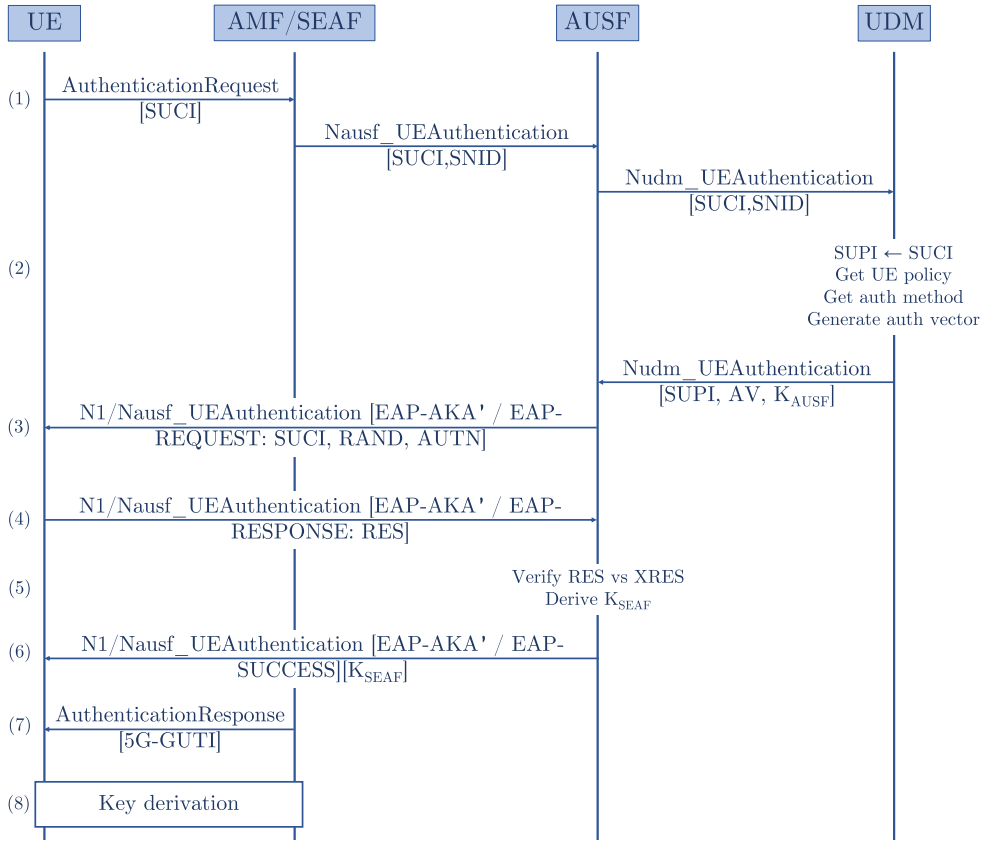


Figure 2.15: 5G EAP-AKA' authentication method.

On the other hand, the secondary authentication defines how the UE and the PDN achieve mutual authentication, where the PDN can be outside the 5GC. The

secondary authentication is performed between the UE, SMF, and an external Authentication, Authorization and Accounting (AAA) server using EAP exchanges where the UE acts as the EAP-peer, the SMF acts as the authenticator, and the AAA server acts as the EAP-server. The authentication starts with a PDU session establishment request sent from the UE to the SMF. After the exchange of the specified EAP messages, and the success of the authentication, the UE is associated with a new PDU session managed by the corresponding SMF, and the messages are routed to PDN through the corresponding UPF.

2.4 Proxy Mobile IPv6

In the protocol stack, a network layer protocol aims to provide packet routing and hierarchical network partitioning [92]. Internet Protocol version 6 (IPv6) [93] and Internet Protocol version 4 (IPv4) [94] are two common network layer protocols. IPv6 is an improved version of IPv4 where several features motivate to use IPv6 in next-generation networks. IPv6 can achieve higher scalability since it has 128 bits for the address space whereas IPv4 has only 32 bits which is almost occupied by the traditional computer networks. Moreover, Stateless Address Auto Configuration (SLAAC) [95] is an important feature in IPv6 that allows network devices to get their addresses without the need for protocols like the Dynamic Host Configuration Protocol (DCHP) [96] used in IPv4.

Mobility is an important requirement needed by several applications as explained before. Several IPv6-based mobility protocols are defined like Mobile IPv6 (MIPv6) [97], Fast MIPv6 (FMIPv6) [98], Proxy MIPv6 (PMIPv6) [99], and Hierarchical MIPv6 (HMIPv6) [100], etc. Nonetheless, PMIPv6 is more suitable for mMTC applications since it provides network-based mobility and low power consumption.

PMIPv6 is a network-based mobility management protocol where two new entities are added to the network, thus network modification is needed to support PMIPv6 as shown in Figure 2.16. These entities are responsible for the tracking of Mobile Node (MN) movement and initiating signaling procedures on its behalf. PMIPv6 is also considered a local mobility management protocol since it manages mobility within the same domain. The new entities added in the PMIPv6 network are the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG).

The LMA acts as the topological anchor point for the MN. It is responsible for maintaining MN accessibility to the Correspondent Node (CN) and operates with MAG to perform the handoff and the binding update procedure. The MAG resides on the access link where the MN is anchored. It is responsible for the tracking of MN movements from and to the access link, and the initiation of the binding update procedure on the MN behalf to LMA.

Two fundamental procedures are defined in PMIPv6, the first is the MN attachment when the MN attaches for the first time to the PMIPv6 domain controlled by the LMA through one of the MAGs. The second is the MN handoff when the MN moves between different MAGs connected to the same LMA.

The MN attachment procedure is shown in Figure 2.17. After the MN attachment at the lower layers, usually a link layer like LoRaWAN, the MAG fetches the MN-ID in the PMIPv6 domain, either from information saved in its database, or

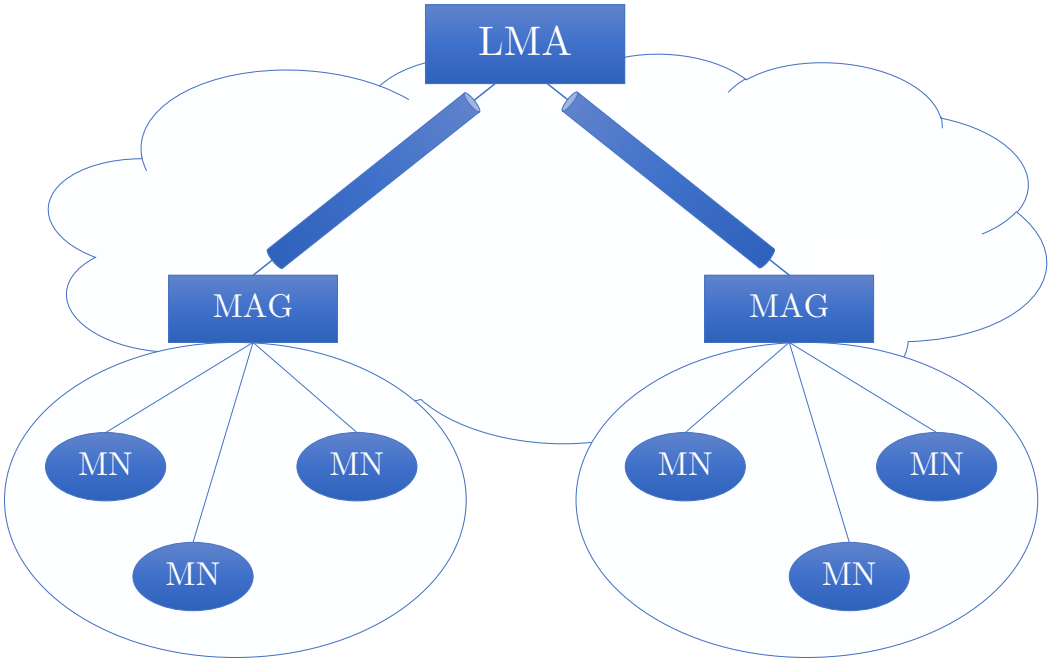


Figure 2.16: PMIPv6 network architecture.

by other ways of authentication. The MN sends a Router Solicitation (RtrSol) message to the MAG to configure its network layer interface, then the MAG sends a Proxy Binding Update (PBU) message to LMA which replies with Proxy Binding Acknowledgment (PBA) message to MAG containing the MN Home Network Prefixs (MN-HNPs). In addition, the LMA creates a bidirectional tunnel with the MAG used for packet routing, and creates a Binding Cache Entry (BCE) for this MN. Finally, the MAG replies with Router Advertisement (RtrAdv) message to the MN containing the MN-HNPs used by the MN to configure its network layer interface.

The MN handoff procedure is shown in Figure 2.18. When the previous MAG detects the MN detachment at the lower layers, it sends a DeRegistration-PBU (DeReg-PBU) message to LMA. The LMA accepts the deregistration after a defined delay, and sends back a PBA message to the previous MAG to discard the established tunnel. When the MN attaches to the next MAG, the latter performs the MN attachment procedure again and finally sends the RtrAdv message to the MN. This message is detected by the MN which finds the same MN-HNPs in the message, therefore it retains the same network layer address, which means that this procedure is completely transparent to the MN network layer interface.

Regarding the packet routing, any outbound packet sent by the MN to the CN is intercepted by the MAG which encapsulates it in another packet having the MAG address as the tunnel source point address, and the LMA address as the tunnel end point address. When the packet reaches the LMA, it decapsulates and sends it to the CN. The reverse procedure applies for inbound packets sent by the CN to the MN.

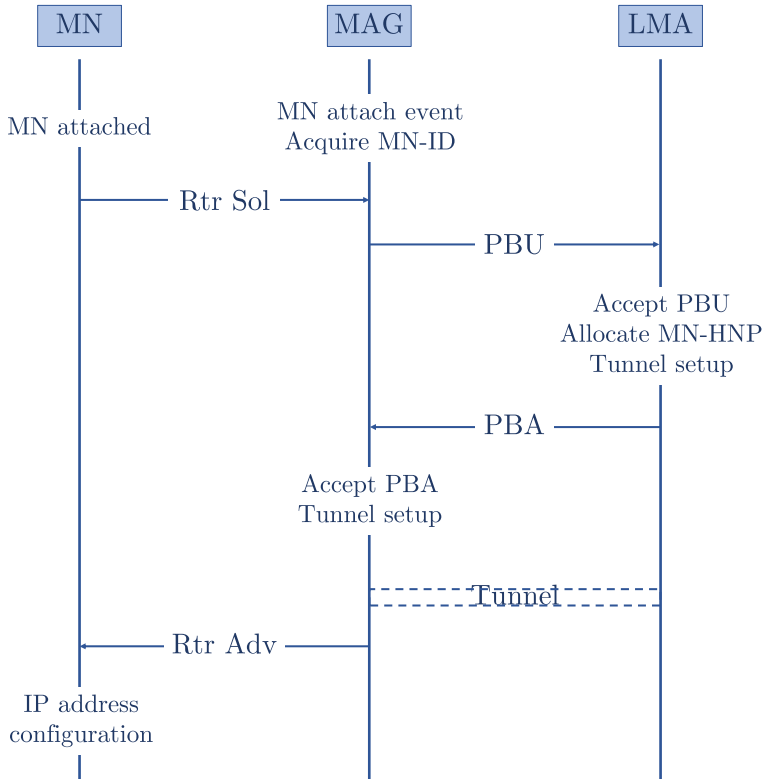


Figure 2.17: Mobile node attachment procedure.

2.5 Security issues in mobile environment

2.5.1 Common security requirements

The IoT networks inherit the common network security requirements, which are **C**onfidentiality, **I**ntegrity, and **A**vailability, widely known as the CIA triad [101], added to the authenticity.

- **Confidentiality:** refers to the prevention of data exposure to unauthorized parties. Since the messages sent by the devices could pass through insecure paths before arriving at the destination, an appropriate mechanism should be employed to prevent an eavesdropper from revealing them.
- **Integrity:** the data should be exchanged and stored in a manner that prevents any unauthorized party from altering them, which may lead to faulty decisions, or manipulating them for other malicious purposes.
- **Availability:** the services provided by the network should be reachable anytime, thus, all the entities forming the network should be protected from attacks that hinder the provision of services like Denial of Service (DoS) and jamming attacks.
- **Authenticity:** refers to the ability of entities constituting the network to identify each other. The identities of the entities participating in a session should be verified when establishing it and until terminated. An attacker succeeding to break the authentication mechanism can hijack the session, spoof

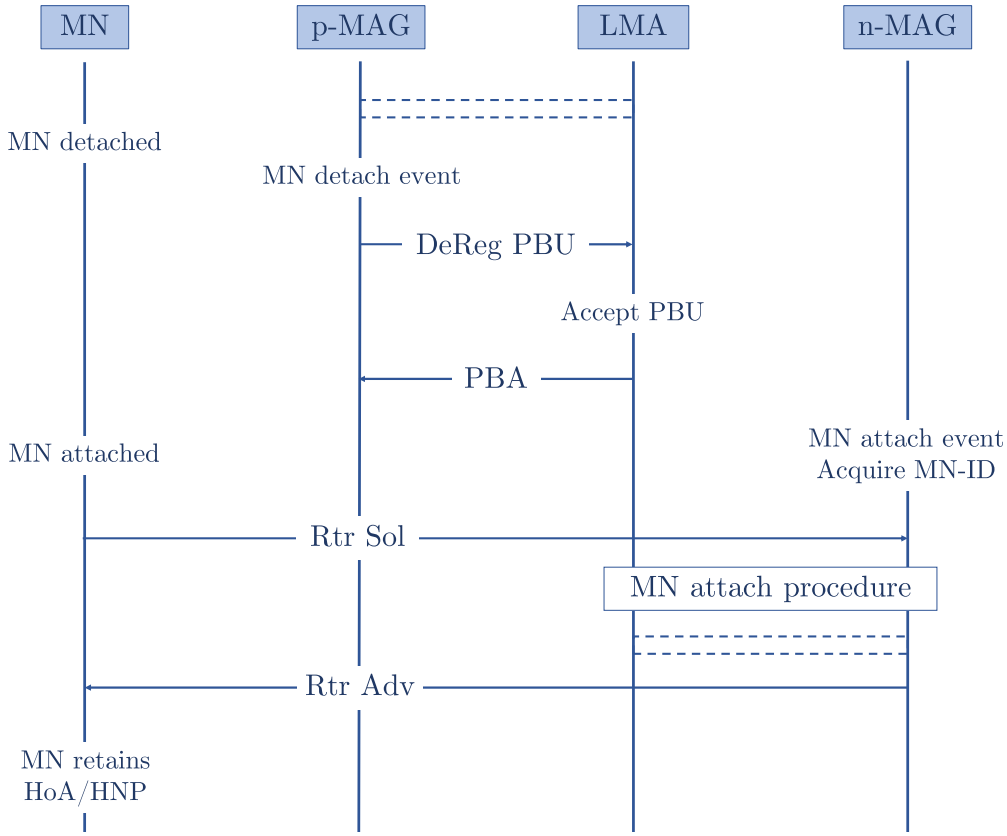


Figure 2.18: Mobile node handoff procedure.

the identities, and violate the privacy of users.

2.5.2 Mobility-related security issues

The mobility of devices rises new types of security issues related to device mobility itself, and related to the mobility management solution responsible for the handling of the mobility. These mobility-related security issues are detailed in the following, and the impacts of each issue in conformity with the security requirements highlighted in the previous section are summarized in Table 2.4.

2.5.2.1 Device authentication

Authentication is the ability of the entities to continuously identify each other. Thus, these entities should be able to identify each other before, during and when terminating a session. Hence, a mobility management solution should ensure the secure management of device identities during device movement between different networks. In a typical scenario, a device establishing a connection with a CN, moves from its home network towards a visited network and desires to resume the established session. For that, an identity verification mechanism should be supported by the solution to verify that any message sent to the visited network is actually sent from the device, and any attempt by an attacker to steal a device identity should be detected and prevented.

2.5.2.2 Error message attack

A mobility management solution is a sequence of actions and operations executed by the involved entities where signaling messages are used to control the progress of the communication. This process may fail or be interrupted before the completion for many reasons, such as battery death, connection loss, etc. To ensure secure communication, the solution must address all the possible failures. To prove how a failure can be a source of threat, consider the following example. A device moving out of its home network coverage towards another network coverage will trigger the mobility management solution. Moreover, suppose that the adopted solution registers the device with the visited network before reaching its coverage area. Since the handoff is triggered, the device is registered now with the visited network, but for some reason, and before the handoff is completely terminated, the handoff is interrupted. If a signaling message, indicating that the handoff is interrupted and any change must be reverted, is not sent to the visited network to revoke the newly registered device, an attacker can hijack the session expected to be established between the visited network and the device.

2.5.2.3 False handover request

The mobility management solution defines certain conditions to trigger the handoff. Suppose that the handoff is triggered when the received signal power drops below a certain threshold. This condition can be ill-used to trigger the handoff and generate a false handover request. For example, an attacker can move towards the boundary of its home network coverage, thus the received signal power decreases until reaching the threshold value which will trigger the handoff to start, then immediately, the attacker will move back towards the coverage of its home network again, which leads to a false handover request. The problem caused seems insignificant if only one attacker is involved. But if a large number of attackers get involved and behave in such a way, a large number of false handover requests should be handled by specific network entities. This may cause performance degradation or even a DoS since the processing power and the network capacity will be massively exceeded.

2.5.2.4 Spoofing signaling message

A signaling message holds a command to control the communication or the session flow between the network entities. Various signaling protocols exist and each has its tailored signaling messages. The role of these messages is the establishment or the termination of a session, updating connection parameters, exposing a device state, etc. A mobility management solution uses signaling messages to control the communication in the network. These messages should be exchanged securely to avoid any alteration or spoofing. By way of illustration, assume that the mobility management solution uses a signaling message that terminates a session between the device with its home network. The message sender should sign it and the receiver should be able to verify the sender identity. If an attacker succeeds to spoof this message, it can terminate an established session that should not be terminated. As another example of message spoofing, assume that the mobility management

solution uses a signaling message that assigns a new identity to a mobile device, if an attacker succeeds to spoof this message, it can assign its identity as the new device identity, and take the control over the device session.

2.5.2.5 Address squatting

Address squatting is preventing a device from getting its genuine address. The address refers here to the link layer identity or the network layer address. This issue occurs when the mobility management solution pre-assigns addresses for the devices based on a known or predictable mechanism. Suppose that a device moving from its home towards a visited network, the latter can identify it based on the assigned address, which cannot be given to another device. If an attacker predicts the address generation mechanism, it can claim the ownership of any valid address that should be given to another device, and any message sent to the device will be routed to the attacker. Thus, a device moving towards a visited network will fail to establish a connection using its address that was stolen by the attacker. For that, it is necessary to adopt a mechanism generating addresses in an unpredictable way, and to support mechanisms protecting counter address squatting.

2.5.2.6 Address spoofing

The same scenario detailed in the previous attack leads to address spoofing attack which can be seen as an active state of address squatting. The difference here is that the attacker does not only steal the address, but sends messages to other devices that appear to come from the genuine device. To prevent such attacks, the mobility management solution should not rely on the basic implementation of protocols at the link and network layers, and a suitable mechanism should be used to manage addresses and identities of devices during mobility.

2.5.2.7 Old address control

Following a device switching to a visited network, it will be assigned a new identity for the link layer and a new address for the network layer, where the obsolete identity and address assigned in the home network will be released. The problem arises if the obsolete identity and address are released in a way that makes it possible for an attacker to resume the session that was established with the home network. Therefore, after completing the handoff, any old session that will not be used in the future should be securely terminated.

2.5.2.8 Context alteration

Several mobility management solutions use a context which is a sort of trace maintaining information about the device and used to resume a session after moving from the home network to another network. The matter is how to maintain the integrity of this context while it is stored, updated, or exchanged. As an example, suppose that the context contains the destination address of every message sent by the context owner. Thus, in case an attacker succeeds to change the destination address in this context, the messages will be forwarded to another destination and

blocked for the intended destination. If the attacker alters a considerable number of contexts, it causes the device to be flooded with a large number of spam messages and may cause a DoS.

Table 2.4: Impact of mobility-related security issues.

	Authenticity	*Confidentiality*	*Integrity*	*Availability*
Device authentication	X			
Error message attack	X	X		
False handover request				X
Spoofing signaling message	X		X	
Address squatting				X
Address spoofing	X	X		
Old address control	X			
Context alteration			X	X

2.6 Mobility management solutions

In this section, we present related work proposing mobility management solutions. Related work is divided into two categories: IoT related work and LPWAN related work. The latter takes into account more constraints existing in LPWANs. Most of the solutions presented are based on MIPv6 and PMIPv6 which are optimized to provide a better performance. However, non-IP solutions are also proposed where the mobility is provided by alternative mechanisms like blockchain-based mobility. These solutions are presented with their limitations in terms of performance and security which motivates us to propose a more efficient solution.

2.6.1 IoT mobility management solutions

- **Jabir *et al.*** [44]

  The authors propose a solution named "A cluster-based proxy mobile IPv6 for IP-WSNs". The Cluster Sensor PMIPv6 (CSPMIPv6) is a solution based on PMIPv6 providing energy-efficient mobility management for IoT devices. The architecture of CSPMIPv6 divides the local domain into several local sub-domains. Each sub-domain groups several MAGs into one cluster. This cluster is controlled and managed by a new entity called Head MAG (HMAG). Therefore, the CSPMIPv6 architecture consists of LMA, MAG, HMAG, and

MN as shown in Figure 2.19. The LMA and the MAG conserve their PMIPv6 functionalities. The main functions of HMAG are to offload the LMA from local mobility management procedures. Further, HMAG acts as a AAA server, thus it provides authentication for MNs which reduces the access signaling overhead. In addition, HMAG provides direct communication in case of intra-cluster mobility which reduces the handoff latency and route optimization.

The signaling messages used in CSPMIPv6 are the PBU, PBA, Local PBU (LPBU), Local PBA (LPBA), Proxy Binding Query (PBQ), and Proxy Query Acknowledgment (PQA). PBU and PBA are used to attach the MN to the LMA or to update its information as in PMIPv6. The LPBU and LPBA are used between the MAG and serving HMAG to attach a MN or to update its information locally in the cluster. The PBQ and PQA are used by the MN to find the HMAG and the MAG serving another MN to communicate with it.

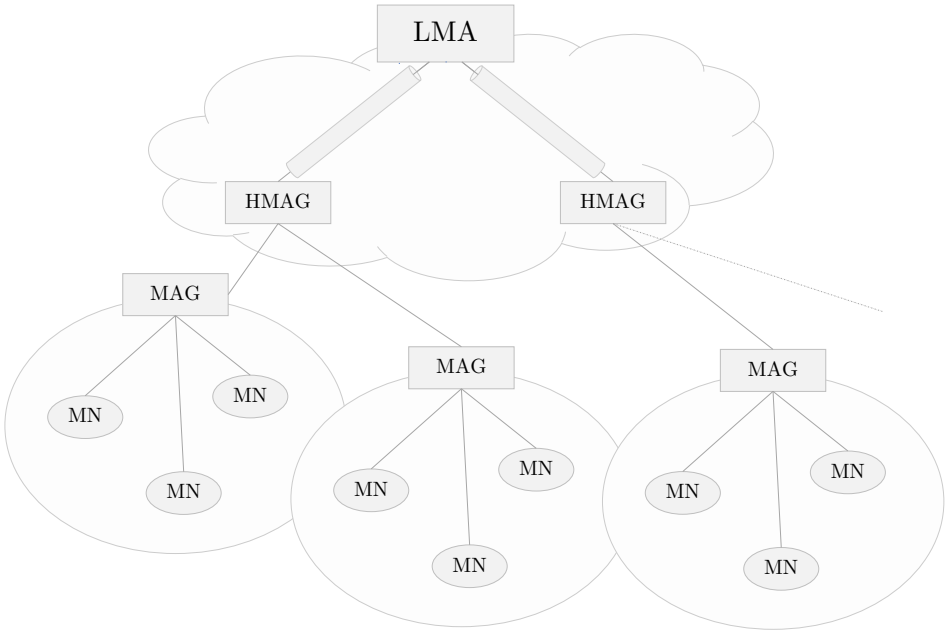


Figure 2.19: Cluster Sensor PMIPv6 network architecture.

Evaluation. Despite the improvements made over the PMIPv6 architecture, CSPMIPv6 suffers from several limitations like single point of failure since the MN relies on a single LMA for inbound and outbound packets. In addition, this solution is not suitable for large-scale deployment since the architecture has a tree-based architecture which increases the number of HMAGs needed as new clusters are formed, which needs also to be configured. Moreover, adding a new entity leads to an increase in the signaling overhead and the end-to-end delay, especially in case of intra-cluster mobility. In terms of security, CSPMIPv6 does not consider the security aspect which makes this solution vulnerable to several threats.

- **Sharma *et al.*** [45]

  The authors propose a solution named "MIH-based secure cross-layer handover protocol for Fast Proxy Mobile IPv6-IoT networks". This solution is based on

Fast PMIPv6 (FPMIPv6) [102] and Media Independent Handoff (MIH) framework [103]. FPMIPv6 allows a PMIPv6 handoff with enhanced performance in terms of latency and packet loss. The MN is able to immediately detect its movement to the new RAP by providing it with the new association while it is still connected to the previous RAP. The MIH is a cross-layer framework that enables heterogeneous handoff and accelerates the operations that should be executed in each layer. Three services constitute the MIH which are the Media Independent Event Service (MIES), the Media Independent Command Service (MICS), and the Media Independent Information Service (MIIS). MIES provides services to the upper layers by reporting the events that occur at the lower layers. The MICS allows the upper layers to control the functions of the lower layers. The MIIS defines the query-response mechanisms that allow an entity using the MIH to obtain information and discover the adjacent networks. In addition to FPMIPv6 and MIH, this solution provides security features by the use of an authentication mechanism ensuring secure access where the security messages are incorporated in the FPMIPv6 and MIH signaling messages.

Evaluation. Despite the good performance and the security features provided in this solution, the uses of MIH and FPMIPv6 in IoT environment leads to high signaling overhead since the number of devices is expected to be large, where MIH and FPMIPv6 involves a lot of signaling messages to complete the handoff procedure. In addition, the use of MIH over an IoT device is not recommended due to the processing and storage needed by MIH services.

- **Moosavi *et al.*** [46]

  The authors propose a solution entitled "End-to-end security scheme for mobility enabled healthcare Internet of Things". This solution provides secure end-user authentication using Datagram Transport Layer Security (DTLS) handshake [104], secure end-to-end communication between the device and the end-user with session resumption in case of device movement, and an efficient mobility management solution based on a virtual layer interconnecting the RAPs called smart gateways. The network architecture consists of three layers which are: cloud layer, fog layer, and device layer as shown in Figure 2.20.

  The device layer is the lower layer consisting of the IoT devices like wearable medical sensors, which transmit the detected data to the middle layer. The fog layer is the middle layer consisting of a network of smart gateways which are interconnected between them. These gateways receive messages from the device layer, perform the necessary protocol conversions, execute the handoff authentication mechanism based on DTLS, ensure session resumption after device movement, and act as repositories to store the device information temporarily. The cloud layer is the upper layer consisting of big data treatment servers, hospital local database, data warehousing, providing data processing and visualization to be used by end-users. In addition, this solution provides end-to-end secure communication through the use of an authentication and authorization mechanism executed by the end-user to access device data.

This mechanism provides also session resumption opportunity in case of device movement where the previous and the next gateways will be involved in the authentication.

Evaluation. This solution ensures high security requirements like mutual authentication, forward secrecy, scalability, reliability, access control, data confidentiality and integrity. In addition, the authors evaluation confirms that this solution achieves good performance in terms of handoff latency. However, this solution requires high signaling in the fog layer between the interconnected gateways to manage mobility, and several messages should be exchanged between the end-user, the gateway, and the IoT device in the authentication mechanism.

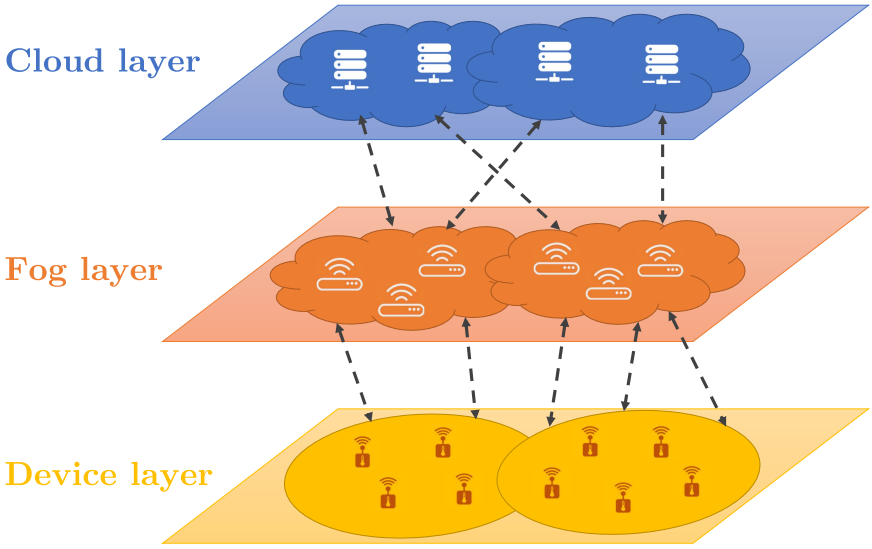


Figure 2.20: End-to-end security scheme network architecture.

2.6.2 LPWAN mobility management solutions

- **Ayoub *et al.*** [47]

  The authors propose a solution entitled "Mobility management with session continuity during handover in LPWAN". The authors propose a framework to manage mobility in case of homogeneous intra-domain mobility, giving a special focus on LoRaWAN technology. The solution is based on a compression algorithm derived from the Static Context Header Compression (SCHC) compression algorithm [105], called Mobile SCHC (MSCHC), and the use of MIPv6 to facilitate the data routing when moving between networks. SCHC is an IPv6 header compression algorithm based on a context stored in the ED and in the network used for compression. SCHC does not take into consideration the ED mobility causing the change of the used context. Thus, the authors propose to have a context that can be changed dynamically when the ED moves. An optimization of SCHC is also proposed to separate the rules in the context according to the application, transport, network, and extension

layer fields, which leads to more flexible use of context and saving memory. Furthermore, to make the IPv6 address assignment easier after entering a new network coverage, the LoRaWAN GW is supposed to send periodically a frame containing a list of addresses from which the ED can configure its network layer interface. In addition, an optimization is proposed on the existing LoRaWAN roaming procedure to avoid triangular routing where any packet sent to the vNS should be routed to the hNS before sending it to its final destination. For that, to reduce the handoff latency and to save network bandwidth, the binding update mechanism existing in MIPv6 is used to make direct routing between the ED and the CN avoiding triangular routing.

Evaluation. This solution provides a mobility solution for LoRaWAN in case of intra-domain mobility, however, inter-domain mobility is required in several cases. In addition, the frame periodically sent causes high link utilization and high signaling overhead. Moreover, the address assignment after this frame broadcasting does not deploy an address duplication check, thus two or more EDs may have the same IP address, which can lead to congestion and open an opportunity for several security threats. In terms of security, this solution is not considered secure since several security issues like device authentication, address squatting, address spoofing, and signaling message spoofing can be conducted by an attacker.

- **Ayoub *et al.*** [48]

  The authors propose a solution entitled "Media independent solution for mobility management in heterogeneous LPWAN technologies". In order to overcome the challenges and the limitations of the previous solution [47], the authors propose a media independent solution providing seamless handoff and session continuity by proactively initiating handoff independently of the used link layer technology. This solution is based on the MIH framework and a new server managing the mobility called the mobility management server. The exchanges expected to take place between the ED, the home network, the visited network, and the mobility management server are initiated either by the ED or the network according to the used configuration. As key features, this solution benefits the features of MIPv6 networks with reduced overhead due to the use of MSCHC recalled Dynamic Context Header Compression (DCHC), and the session continuity provided by the MIH.

  Evaluation. This solution has a better performance compared to the previous one. The frame used in the latter is not used in this solution which reduces the congestion, however, the signaling overhead is not reduced due to the use of the MIH framework requiring the exchange of several signaling messages. In addition, the use of MIH over an IoT device is not recommended as mentioned before. From the security point of view, this solution does not take into consideration the security issues that can threaten the solution.

- **Durand *et al.*** [49]

  The authors propose a solution entitled "Decentralized LPWAN infrastructure using blockchain and digital signatures". The authors endeavor to achieve a

decentralized architecture at the JS level and to optimize the roaming feature of LoRaWAN v1.1. The authors propose an alternative solution that replaces the JS with a blockchain smart contract. This smart contract has two main functions. The first function is 'RegisterJoinEUI' executed by hNS to register EDs under its control. This function binds the ED JoinEUI with the hNS address and appends this record to an array saved in the blockchain smart contract. Thus, if an ED goes out of the coverage of its hNS, the vNS uses the second function called 'GetAddress' taking a JoinEUI as an input parameter and returning the hNS address that has been mapped by the first function. For the rest of the join procedure, the hNS assigns the ED address and sends it to the ED through the vNS encrypted using the NwkSKey, and since the vNS does not have information about the NwkSKey, the authors propose to send it in an out-of-band way.

Evaluation. This solution is based on blockchain, which is a notable type of distributed ledger technologies based on a decentralized system architecture that has several advantages over centralized system architecture. Decentralized systems avoid single point of failure, since the JS, which was a single server, is replaced by a smart contract where the probability of the halt of the whole system at the same time due to a technical or security issue is negligible. Besides, the overall system performance is enhanced as JS services are distributed across the entities holding the blockchain ledger, making this solution more scalable thus supporting a higher number of EDs. However, distributed systems suffer from many drawbacks. Each transaction sent to the blockchain is subject to fees, thus the transactions sent containing the mapping should be paid which makes this solution less interesting to be adopted. Furthermore, many security issues exist in blockchain, because transaction validation takes some time according to the blockchain type, which is 14 seconds in Ethereum [106]. This makes the mapping records susceptible to modification or alteration attacks. Another security issue with a low probability to happen is that blockchain is susceptible to '51% attack' [107], which makes the network under attacker control if it reaches 51% of the total network computational power.

- **Lamberg-Liszkay *et al.* [50]**

  The authors propose a solution entitled "Distribution servers based solution for roaming in LoRaWAN". The authors propose a decentralized architecture to achieve roaming in LoRaWAN v1.0. The authors propose the addition of a new entity called the Distribution Server (DS). This server works as a broker entity in LoRaWAN topology to reinforce roaming as shown in figure 2.21. Four services are implemented in the DS to manage ED roaming as described below.

  - Registration service: this service manages the registration process of a DS with another NS or DS. Thus, an ED affiliated initially to its hNS and roaming in a vNS can only reach its hNS if the two NSs are registered under the same DS or registered under two different DSs having a link between them.
  - Database service: after each registration process, each DS stores in its

database the NetworkID of the newly registered NS mapped to its IP address, or the collaborating DS mapped to its IP address. In this way, the DS builds a database of DSs and NSs registered with their IP addresses. This database is mainly used by the message distribution service.

- Message distribution service: is the service listening to incoming messages that may come from a NS or DS. In any case, the DS must read the destination NetworkID. If the message is sent by a NS, the DS must check if the destination NS is accessible, so it queries the database service. If the NS is accessible directly, it extracts the NS IP and forwards the message. If the NS is accessible by another DS, it extracts the DS IP address and forwards the message, otherwise it must reject it. If the message is sent from another DS, the current DS knows that it has a direct connection with the destination NS, so it checks and extracts its IP address, then forwards the message. Otherwise, the message is rejected.
- Information exchange service: this service is activated if the DS has active collaborator DSs. In this case, each DS must periodically send an update message indicating which NSs are still reachable through it, or which NSs are no longer reachable. This message is sent periodically within a predefined period or conditionally depending on a certain condition that triggers the service.

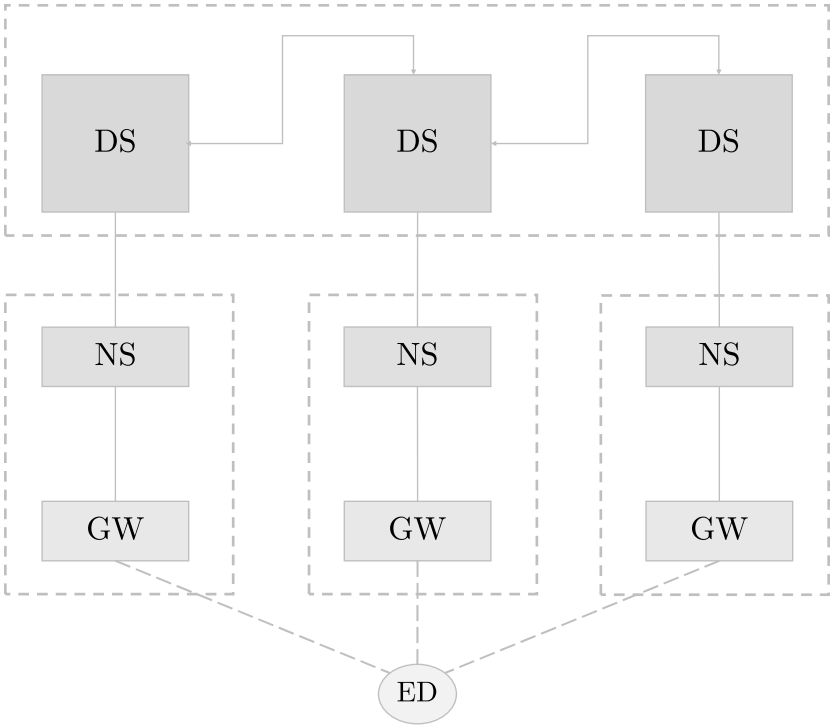


Figure 2.21: Distribution server network architecture.

Evaluation. This solution is based on a distributed system architecture. It has the same advantages as the previous solution [49]. Nevertheless, it bypasses many drawbacks encountered in the previous solution. This solution

is free of charge because it is not based on the blockchain, except in the case where the DS is operated by an operator wishing to provide paid services. In addition, this solution is not vulnerable to '51% attack', but on the other hand, other security issues may threat this solution since the security is not considered in this work. For example, there is not an authentication mechanism to authenticate the DSs between them, nor an encryption mechanism to protect the information update messages. Thus, an attacker can falsify a message update for malicious purposes.

2.7 LPWAN integration solutions into 5G system

Recent work has attempted to integrate LPWAN technologies into the 5GS. This integration allows the operator to take advantage of both the simplicity and cost-efficiency of LPWAN, and the power and scalability features of 5G. From a mobility point of view, LPWAN technologies can benefit the 5G SBA to enhance mobility management if they can be integrated with the 5GS. In this section, we present a work reviewing the main security challenges of LPWAN integration into 5GS, and two integration solutions.

- **Sanchez-Gomez *et al.*** [108]

  This review is entitled 'Integrating LPWAN technologies in the 5G ecosystem: a survey on security challenges and solutions'. This review examines the challenges and the benefits of the integration of LPWANs and 5G. The main contributions of this review are the following:

  - The analysis of the requirements needed for the integration of LPWAN technologies to support the 5G services.
  - A technical description detailing the integration security of NB-IoT into 5GS.
  - A technical discussion detailing the integration security of non-3GPP technologies like LoRaWAN and Sigfox into 5GS.
  - A review of recent works detailing the LPWAN security.
  - A review of the integration initiatives in the European Commission, the research community, and the standardization efforts.

  More importantly, this review details the open challenges for the integration including:

  - LPWAN heterogeneity due to the presence of several LPWAN technologies. The integration should examine the architecture, the protocol stack and the radio link characteristics to achieve efficient integration.
  - Solution interoperability where the integration solution should work consistently with different LPWAN technologies.
  - Mobility support since the device can move between several points of attachments and change its location and the access technology.
  - Scalability since LPWANs deal with mMTC involving a large number of connected devices concurrently.

- **Navarro-Ortiz *et al.*** [51]

  The authors propose a solution entitled 'Integration of LoRaWAN and 4G/5G for the Industrial Internet of Things'. The authors endeavor to integrate LoRaWAN into the 4G/5G system since a network operator may be interested to deploy its LPWAN network over the already deployed 4G/5G infrastructure. The authors propose to leave the ED and the NS unmodified since the lower layers (physical and link) and the upper layers (application and transport) are not modified. Thus, the LoRaWAN security is maintained, where data integrity is ensured between the ED and the NS, and data confidentiality is ensured between the ED and the AS. Moreover, LoRaWAN GW behaves as a combination of eNB and ED. Since the GW acts as an eNB, it is responsible for the NAS connectivity setup between the eNB and the MME, and to execute the attach and bearer establishment procedures. As an ED, the GW holds a Universal Subscriber Identity Module (USIM) storing the necessary network keys used to perform the attach procedure. After a successful attachment, the messages sent from the ED to GW are routed through the 4G/5G core network towards the NS, which in turn routes them to the correspondent AS.

  Evaluation. This solution provides a way to authenticate the ED with the NS and the AS through the 4G/5G infrastructure. This solution provides an energy-efficient authentication since the GW is responsible for the execution of the ED attach procedure, and an end-to-end secure communication between the ED and the AS since the LoRaWAN security is maintained. However, this solution has several limitations. This solution does not support mobility in case an ED moves to another network, or even to another GW of the same network, since the USIM of that ED is installed statically in one GW, and if the ED moves to a new GW coverage, the new GW cannot authenticate the ED. This makes also a limitation in terms of scalability since an operator should install for each ED a USIM in the corresponding GW leading to additional cost and difficulties if the GW is deployed in urban locations. Finally, this solution does not benefit the 4G/5G core features, since the network is used to authenticate the ED only, where the NS still operates outside the core network.

- **Torroglosa-Garcia *et al.*** [52]

  The authors propose a solution entitled 'Enabling roaming across heterogeneous IoT wireless networks: LoRaWAN meets 5G'. The authors propose an integration solution that relies on the 5GS to perform authentication with LoRaWAN. To do that, a new interface is defined between the JS and the UDM responsible to perform the authentication of LoRaWAN and 5G devices with the network, respectively. Two suppositions are handled in this solution. The first supposes that the ED has already an active connection with the 5GS, where the already derived keys can be used to protect uplink messages. The second supposes that the ED does not have an active connection with the 5GS, which means that there is not any session key that can be used to protect uplink messages. Anyway, the ED should have a valid USIM containing K in addition to LoRaWAN root keys. The ED tries to authenticate via LoRaWAN with the usual join procedure. If the procedure fails, the ED sends another

join request containing 5G authentication parameters, which are processed by the 5GC as a 5G authentication request. Upon authentication success, the 5GC notifies the NS and sends the LoRaWAN session keys also generated by the ED. Thus the ED is authenticated in LoRaWAN through the 5GC and establishes a secure connection.

Evaluation. This solution provides an integration of LoRaWAN authentication scheme using the existing 5G UDM. This solution overcomes several limitations of the previous solution [51]. This solution provides mobility features since the ED authentication relies on the JS and the UDM that communicate through the new interface, where the ED can be authenticated if it has an active connection with the 5GS or if it is in the coverage of a LoRaWAN GW. This solves also the problem of scalability since the ED credentials and root keys are saved in the UDM and the JS without the need to store them in a RAP. However, this solution does not benefit the 5GC features since the 5GC is used to authenticate the ED only, and there is not an interface that makes it possible to communicate with the 5GC NFs.

2.8 Conclusion

In this chapter, we presented the main concept of LoRaWAN and NB-IoT as leading LPWAN technologies, and the 5G broadband cellular network features and architecture. In addition, we presented PMIPv6 mobility management protocol. The problem investigated in this thesis is to provide a secure mobility management solution for LPWAN technologies, thus, we detailed the security issues related to device mobility, and several important works trying to solve this problem. However, these solutions suffer limitations either in terms of security where the proposed solution does not take into consideration the security aspect making it vulnerable to several attacks, or in terms of mobility where the solution cannot handle all the mobility types or have some performance limitations like the high signaling overhead. Thus, in the following chapters, we propose efficient mobility solutions that take into consideration the security aspect.

Chapter 3

Secure Intra-domain Mobility Solution for LPWANs

Abstract *— In this chapter, we present our proposed mobility management solution for intra-domain mobility in case of homogeneous and heterogeneous mobility in LPWANs. We detail first the design principles considered to build our solution including the motivation behind using PMIPv6 and the need for an adapted protocol stack. Next, we present our mobility management solution consisting of four main parts which are the network architecture integrating PMIPv6 entities into the architecture of LPWAN technologies, the adapted protocol stack ensuring the communication of the mobile node with the corresponding node through the network, the authentication scheme deployed by PMIPv6 entities to authenticate a mobile node attaching or moving in the PMIPv6 domain, and the handling of each type of intra-domain mobility as well as the impact of each type on several mobility parameters. Later on, we evaluate the performance of the proposed solution according to two main metrics which are the handoff delay and the signaling overhead. These metrics are evaluated theoretically and by simulation to validate the obtained results. Finally, and as we are proposing a secure mobility solution, we evaluate its security according to the common security requirements and mobility-related security issues explained before, and using an automated security protocol validation software.*

3.1 Design principles

In this chapter, we propose an intra-domain mobility management solution based on PMIPv6 for LPWAN technologies. We focus on the leading LPWAN technologies nowadays which are LoRaWAN and NB-IoT [8]. In our solution, we use PMIPv6 as a network layer mobility management protocol. Several features motivate the use of PMIPv6 over other network layer mobility management protocols like MIPv6, FMIPv6, and HMIPv6 as detailed below:

- PMIPv6 is a network-based protocol unlike MIPv6, FMIPv6, and HMIPv6 which are considered host-based protocols. A network-based protocol means that the MN is not responsible to perform any mobility procedure, where the associated MAG should monitor the MN movement and initiate the mobility

procedures on the MN behalf. This will save the MN battery and reduce the processing time since the MAG does not have processing and battery lifetime constraints. Contrarily, if MIPv6, FMIPv6, or HMIPv6 are used, the MN should be involved in the mobility procedures which leads to additional processing and battery drain.

- A MN implementing the elementary IPv6 at the network layer does not need any modification to support PMIPv6 since the MN is not required to recognize other than RtrSol and RtrAdv messages as described in the attachment and handoff procedures in Section 2.4. However, the use of MIPv6, FMIPv6, or HMIPv6 requires MN modification to recognize and process additional protocol-related messages like binding update message in MIPv6 and HMIPv6, and proxy RtrSol message in FMIPv6. Hence, the cost of deployment a MN supporting PMIPv6 is considered lower than the cost of deployment a MN supporting other mobility protocols, where in the former a simple MN supporting IPv6 is able to operate normally.
- The handoff delay in FMIPv6 is considered low, while it is considered moderate in case of PMIPv6 and HMIPv6, and considered long in case of MIPv6. Since the application sector served by the LPWAN technologies does not have strict handoff delay constraints, i.e. time-tolerant applications, a moderate handoff delay is acceptable. However, achieving a lower handoff delay is more favorable if the mobility protocol does not overhead the MN by additional processing or message exchanges. Thus, the use of PMIPv6 is more favorable than FMIPv6 even though the latter provides lower handoff delay.
- In addition to the previous point, the handoff procedure in PMIPv6 is a reactive handoff, which means that the handoff procedure starts after the movement of the MN to the new RAP. However, the handoff procedure in FMIPv6 is a proactive handoff, which means that the MN starts the handoff procedure before establishing the link with the new RAP. The proactive approach leads to additional signaling in the network which is not suitable for mMTC.
- An additional feature provided by PMIPv6 is multi-homing where a MN supporting multiple RATs can establish multiple connections with the network. Although, this feature cannot be exploited in mMTC environment due to the large number of devices where establishing multiple connections will cause significant signaling and a drain of the device battery. However, this feature may be used in some cases to achieve reliable handoff if required by certain applications.

The features supported by PMIPv6 make it a suitable mobility management protocol choice, however, there are two essential security aspects of PMIPv6 to review. The first is the security of signaling messages exchanged during the attachment and handoff procedures between the MAG and the LMA. According to PMIPv6 specification, the security of signaling messages exchanged is ensured using IP security (IPsec) [109] between the MAG and the LMA. In this way, signaling message confidentiality, integrity and authenticity are ensured. The second is the MN authentication with the PMIPv6 domain. When the MN attaches to the RAP, the MAG and the LMA should be able to authenticate the MN in order to check its right

to access the network services. The specifications for how MAG and LMA achieve this truth are not given in PMIPv6 which assumes to have pre-established mutual trusts. Therefore, in our solution, we propose a suitable authentication scheme to authenticate the MN with the PMIPv6 domain during the attachment and handoff procedures.

Furthermore, the LPWAN constraints give rise to two challenges that complicate the PMIPv6 adaptation in LPWAN as follows:

- The PMIPv6 entities, i.e. MAG and LMA, do not exist in the LPWAN architecture. Thus, an adapted architecture must be used to support the functionalities of these entities either by adding new entities, or by integrating PMIPv6 entities with LPWAN entities.
- The protocol stack of some LPWAN technologies does not support IPv6 by default, while the use of PMIPv6 necessitates the support of IPv6. In addition, adopting IPv6 directly over an LPWAN protocol stack may rise compatibility issues since an LPWAN technology can employ another network layer protocol, or it may not be realizable due to LPWAN constraints since IPv6 adds a considerable overhead for each message payload.

In the following, we present our solution that takes into consideration the challenges of adapting PMIPv6 in LPWAN. We use the terms (ED and MN) and (UE and MN) interchangeably in the following, where MN is more related to mobility or PMIPv6 context, ED is more related to LoRaWAN context, and UE is more related to the context of broadband cellular networks.

3.2 Proposed solution

In this section, we present our mobility management solution consisting of four main parts. First, we describe the proposed network architecture of LoRaWAN and NB-IoT technologies for PMIPv6 integration in Section 3.2.1. Second, we proposed a modified protocol stack of MN communications with the network to support IPv6 for UP and CP messages in Section 3.2.2. Third, we present the authentication scheme used to provide secure access for a MN attaching or moving in the PMIPv6 domain in Section 3.2.3. Fourth, we described the proposed mobility management for each type of intra-domain mobility and its impact on several mobility parameters in Section 3.2.4. Finally, we describe in detail the operation of the proposed solution during a mobility scenario in Section 3.2.5.

3.2.1 Network architecture

As indicated previously, an adapted network architecture is required to integrate PMIPv6 entities into the LPWAN architecture. In the following, we show the proposed integration of PMIPv6 entities into LoRaWAN and NB-IoT architectures.

3.2.1.1 Evolved LoRaWAN architecture

To integrate the PMIPv6 entities into LoRaWAN architecture, we propose the network architecture shown in Figure 3.1. In LoRaWAN, any incoming or outcoming

message should pass through the NS, thus, the latter is considered the anchor point of LoRaWAN EDs. In PMIPv6, the LMA is considered the mobility anchor point for the MNs connected to the PMIPv6 domain, where any incoming or outcoming message should pass through it. For that, we propose to place the LoRaWAN NS and the PMIPv6 LMA at the same logical entity.

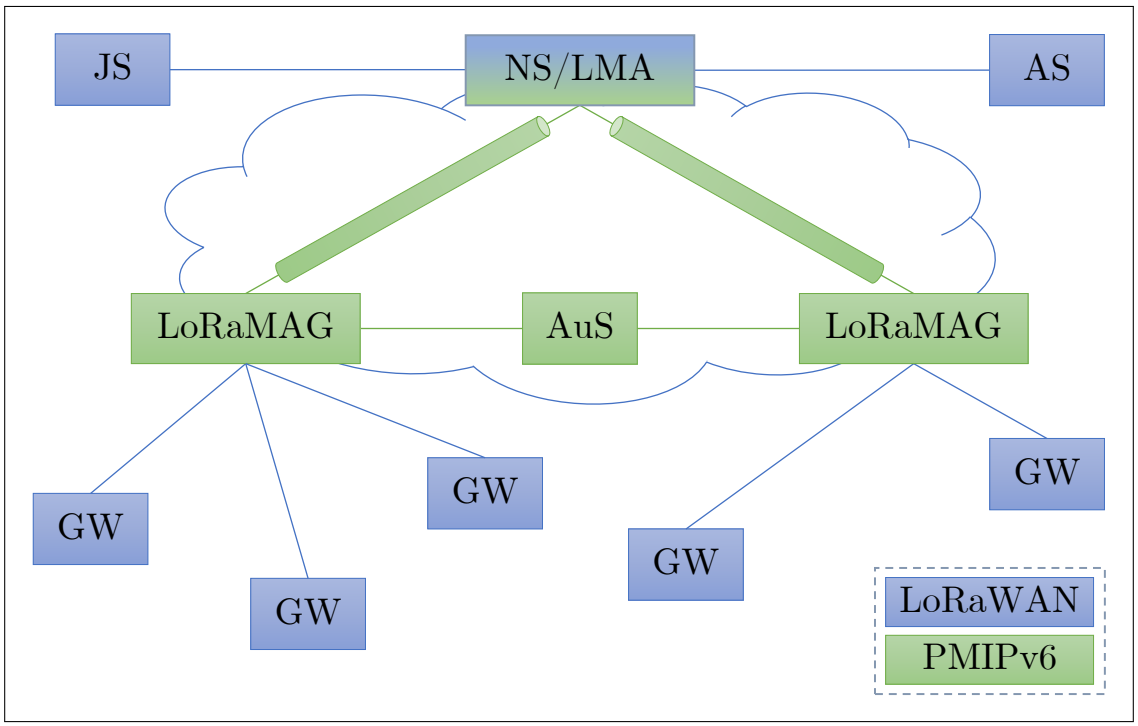


Figure 3.1: Evolved LoRaWAN architecture.

The challenge lies in integrating the MAG into the LoRaWAN architecture. This challenge rises since any uplink message sent from the ED to the NS may be received and forwarded by one or more GW at the same time, whereas, downlink messages sent from the NS to the ED are routed through a single GW, having the best link conditions. If the MAG and the GW are placed at the same logical entity, the ED must authenticate each time it attaches through a GW/MAG. This proposal has two drawbacks:

- A hard increase in the signaling cost: since in the default LoRaWAN architecture, the ED moves between different GWs without the need to be authenticated, although it must be authenticated after a connection loss or a move to new network coverage.
- A deterioration in network performance: a mobile ED is expected to send a very small number of messages through one GW, thus if the authentication is required whenever the ED is under a GW coverage, the number of signaling messages exchanged will be in the order of the number of data messages, which is not efficient especially for LPWAN.

To overcome these limitations, we propose a new entity called LoRa Mobile Access Gateway (LoRaMAG) to be placed topologically between the NS and the GWs, where multiple GWs are connected to one LoRaMAG, and all LoRaMAGs

in the domain are connected to the unique NS/LMA. The main functions of a LoRaMAG are the following:

- LoRaWAN-related functions: the LoRaMAG maintains the connection between the ED and the NS/LMA through the GW covering the ED. In case of uplink transmission, an ED message forwarded by several GWs connected to one LoRaMAG is forward by the latter once to the NS. Anyway, the NS still performs its duplication check in case two GWs connected to different LoRaMAGs forward the same uplink message. However, the duplication check process is offloaded from one NS into multiple LoRaMAGs, which enhances the network performance. In case of downlink transmission, the NS acts as in default LoRaWAN architecture, where the downlink message is routed to the best GW through its serving LoRaMAG. Another function offloaded from the NS to LoRaMAG is radio link management, where the LoRaMAG should manage the radio links of the connected GWs.
- PMIPv6-related functions: the LoRaMAG is responsible for the tracking of the MN movement to and from the RAP, and for performing the mobility procedures on the MN behalf as shown in Section 2.4. In addition, the LoRaMAG maintains a tunnel with the LMA/NS for each MN used to send/receive outgoing/incoming messages after performing the necessary encapsulation/decapsulation process. It is responsible also to discard the established tunnel after the MN move to another LoRaMAG. Moreover, the LoRaMAG should listen to incoming RtrSol messages sent from the MN, and send RtrAdv messages containing MN-HNPs after a successful authentication.
- Adaptation-related functions: LoRaMAG contributes to the ED authentication to ensure its right to send and receive data, and contributes to IPv6 adaptation over LoRaWAN technology by the compression and decompression of IPv6 headers using SCHC algorithm as detailed later.

In addition to LoRaMAG, a new entity called the Authentication Server (AuS) is added to the network which is responsible for the authentication of the MN with the PMIPv6 domain during the attachment and handoff procedures. The authentication is achieved by the execution of the authentication scheme described in Section 3.2.3. Comparing AuS to JS, the latter provides authentication of the ED at the link layer with the NS through the join procedure. However, after adding the LoRaMAG to the network, the authentication between the MN and the LoRaMAG is necessary. The join procedure cannot be used to authenticate the MN with the LoRaMAG since it provides authentication with the NS only. Further, the connection between the LoRaMAG and the MN is a network layer connection. For that, a separate authentication scheme is deployed to authenticate the MN and the LoRaMAG at the network layer.

3.2.1.2 NB-IoT architecture

The inter-working of PMIPv6 with NB-IoT technology in CP CIoT EPS optimization is defined in technical specifications TS 29.275 [110] where the network architecture, the attachment and handoff procedures are re-defined in LTE. According to the specifications, the P-GW acts as the anchor point of the connected devices

in LTE networks, thus, the P-GW and the LMA are placed at the same logical entity as shown in Figure 3.2. Moreover, the S-GW acts as a MAG according to the technical specifications. In this way, the S-GW performs the MAG functions like MN movement tracking and management of tunnels.

In the LTE attach procedure [111], the UE is authenticated at the link layer first. This authentication is used directly by the authenticating entities to create a network layer session. Thus, the UE is authenticated at the link and network layers, and has an active session with the EPS. Therefore, there is no need to add any new entity or to deploy any authentication scheme to authenticate the UE with the PMIPv6 in case of NB-IoT.

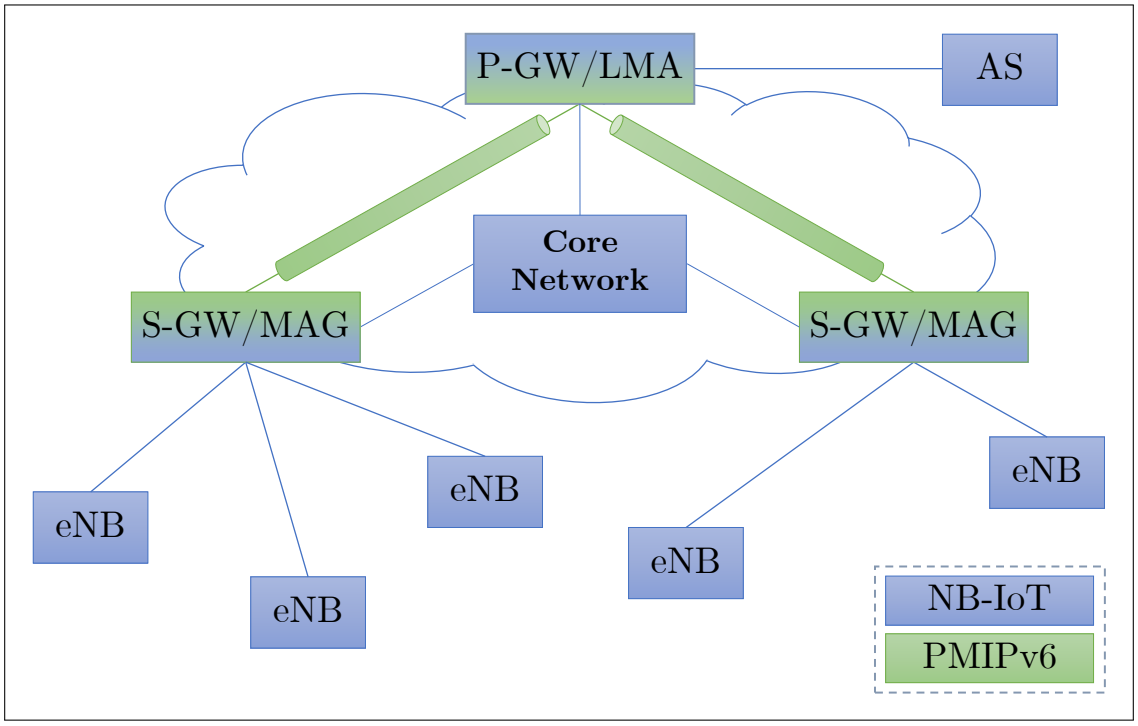


Figure 3.2: NB-IoT network architecture with PMIPv6.

3.2.2 Protocol stack

The UP communication between the MN and the network entities described in the previous section is given by the protocol stack shown in Figure 3.3 and detailed in the following.

3.2.2.1 Application and transport layers

These layers are used to exchange captured data with the CN or AS. They depend on the MN deployment purpose. Thus, they are application-specific and independent of the rest of the layers needed to make the mobility solution. At the application layer, two main protocols are used: Constrained Application Protocol (CoAP) [112] and Message Queuing Telemetry Transport (MQTT) [113]. CoAP is used as a web communication protocol adopted in networks having resource constraints like

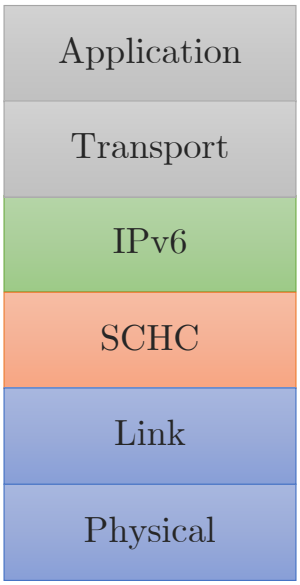


Figure 3.3: Mobile node protocol stack.

in LPWANs. CoAP is based on request/response model and designed to be easily integrated into the Web. CoAP uses UDP at the transport layer and a simple mechanism for re-transmission in case of packet loss. However, MQTT is based on publish/subscribe model and TCP at the transport layer. MQTT is designed to work in narrow bandwidth environments allowing at the same time many to many communication, and can support Transport Layer Security (TLS) [114] to ensure data protection. Other application layer protocols exist such as the Extensible Messaging and Presence Protocol (XMPP) [115], and Advanced Message Queuing Protocol (AMQP) [116].

As mentioned, UDP is used at the transport layer for CoAP. Although a reliable protocol is required at this layer, the TCP is less used for many reasons. In many LPWAN technologies, devices are scheduled to enter sleep mode regularly or after transmission, and a long-term connection cannot be maintained. Moreover, TCP adds a considerable overhead compared to the length of data sent by the device, while UDP adds less overhead. For that, UDP is more preferred than TCP for applications that require a transport layer. However, some applications directly implement a custom transport layer without using either UDP or TCP, which reduces the overhead added by a transport layer.

3.2.2.2 Network layer

We propose to use IPv6 as a network layer for data routing and hierarchical network partitioning. This layer already exists in some LPWAN technologies like NB-IoT, and needs to be adapted in other LPWAN technologies like LoRaWAN. The use of PMIPv6 does not necessitate any change for devices implementing IPv6 since the modification is done at the network architecture level.

Regarding LoRaWAN, it is considered a link layer technology since its protocol stack consists of a link layer that receives application data from the application layer

directly without a network layer. For that, we propose to add the network layer between the application and link layers. Thus, a LoRaWAN ED is able to operate as an IPv6 device benefiting from the IPv6 functionalities. The main functions that should be implemented by an IPv6 device are the configuration of its network layer interface by an IPv6 address, and the use of this interface to send and receive messages. This is achieved by sending the RtrSol message followed later by the reception of the RtrAdv message. Since PMIPv6 is the mobility protocol used, these messages are used in conjunction with the attachment and handoff procedures defined, and the RtrAdv message will contain the MN-HNPs needed to configure the MN network interface. Thus, upon an ED attachment at the link layer, achieved by the join procedure in LoRaWAN, the PMIPv6 attachment procedure is launched by the corresponding LoRaMAG that completes this procedure with the assistance of the LMA. Thus, a tunnel is established for this ED to forward the incoming and outcoming messages. For an outgoing packet sent by the ED, the IPv6 source address is set to the ED IPv6 address configured after the attachment procedure, and the IPv6 destination address is set to the AS IPv6 address. This packet sent to the LoRaMAG is encapsulated according to PMIPv6 specifications before sending it to LMA, which decapsulates it before sending it to the AS.

Regarding NB-IoT, IPv6 is formerly existing in the protocol stack and configured by UP CIoT EPS optimization during the device attachment procedure. Therefore, there are no modifications to be made on NB-IoT technology to support IPv6.

However, adding a network layer for LPWAN technologies is challenging because of LPWAN constraints. For that, we propose to use an adaptation layer under the network layer as detailed below.

3.2.2.3 Adaptation layer

As discussed before, LPWAN technologies have payload length constraint, where the use of IPv6 at the network layer causes an overhead of 40 Bytes. This overhead is added by the network layer for each application data as an IPv6 header before sending it over the link layer. Therefore, we propose to add an adaptation layer located between the network and the link layers for LoRaWAN to perform the compression/decompression of IPv6 headers. In this way, the IPv6 header is compressed by the adaptation layer of the sender to match the LoRaWAN payload length, and then decompressed by the adaptation layer of the receiver into the original IPv6 header. In case of LoRaWAN uplink transmission, the sender is the ED and the receiver is the LoRaMAG.

Several algorithms are proposed to compress the IPv6 header like SCHC [105], ROHC [117], and IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) [118]. However, SCHC is specially designed for LPWANs characterized by the star-of-star network topology and asymmetrical communication type. In [119], the authors review the existing compression algorithms, where SCHC is proved to be the most suitable in LPWAN communications. SCHC is invented by the LPWAN Working Group (WG) of the Internet Engineering Task Force (IETF) in October 2015. During connection establishment, the communicating entities agree on a SCHC context, thus SCHC is a stateful compression algorithm. This context contains several rules identified by a RuleID. Each rule contains a list of entries. An

entry contains a Field Identifier (FID), a Target Value (TV), a Matching Operator (MO), and a Compression Decompression Action (CDA), and other information as shown in Figure 3.4. For an IPv6 packet generated by the network layer during an uplink transmission, an IPv6 header field like the address destination or the header checksum, identified by a FID is compared with the TV according to the MO. If the comparison test succeeds, the CDA action is executed. The MO can be 'Equal', 'Ignore', etc. For example, if MO is 'Equal', the field value in the IPv6 header field should be equal to the TV to execute the CDA. If MO is 'Ignore', the CDA is directly executed regardless of the field value. The CDA can be 'not-sent', 'value-sent', 'mapping-sent', etc. For example, if CDA is 'not-sent', nothing will be sent instead of this field. If CDA is 'mapping-sent', an identifier is sent instead of the field value that can be used by the receiver to retrieve the field value from a list of field values saved in the context. Since the context consists of several rules, the rule attaining the best compression ratio is used. In this way, the RuleID and the compression residues are sent instead of sending the entire header. At the receiver side, the reverse process is executed to reconstitute the IPv6 header.

For NB-IoT technology, the protocol stack already contains an adaptation layer named the PDCP, which contains the compression/decompression algorithm along with the ciphering/deciphering mechanism. ROHC is the compression algorithm specified by the 3GPP to be used in the adaptation layer, however, SCHC can be adapted instead of ROHC without any impact on the network architecture or network entities. For that, SCHC is considered as the compression algorithm for NB-IoT.

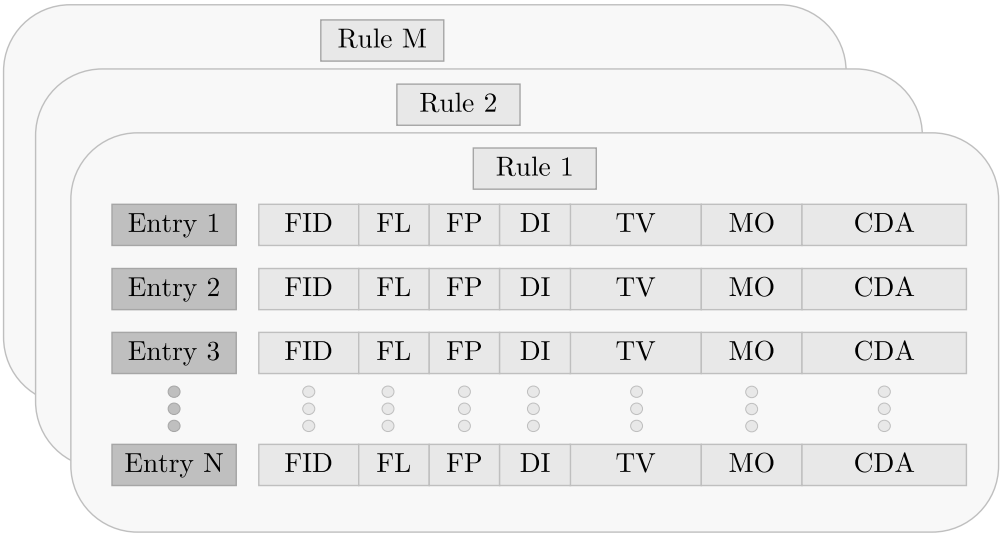


Figure 3.4: SCHC context.

3.2.2.4 Link and physical layers

These layers are dependent on the LPWAN technology used. In case of LoRaWAN, LoRa and LoRaWAN are the physical and link layers used, respectively. In case of NB-IoT, the physical and links are detailed in [120]. Anyway, the link

layer receives the data packet with a compressed IPv6 header from the adaptation layer, schedules it for transmission according to the link protocol used, and then sends it through the physical layer which performs the necessary modulation and the data rate selection.

3.2.2.5 Protocol stack in evolved LoRaWAN architecture

- **User-plane protocol stack**

  The UP protocol stack for an ED communicating with the AS using the evolved LoRaWAN architecture is shown in Figure 3.5. An ED data is encapsulated into an IPv6 packet. The header of this packet is encapsulated through the SCHC algorithm as described before. Thereafter, this packet is scheduled to be sent by LoRaWAN link layer according to the ED class. At the time of transmission, LoRa physical layer applies the necessary modulation to send the uplink message over the LoRaWAN link established with the GW which forwards it to the connected LoRaMAG over a transport network. The LoRaMAG gets the message payload consisting of a compressed IPv6 header and the IP packet. The LoRaMAG decompresses the received packet into the original IPv6 packet with the original header using the SCHC algorithm and the saved context. After that, the LoRaMAG encapsulates the original packet into another IPv6 packet according to PMIPv6 specifications, and then sends it to the LMA/NS through the established tunnel. Upon message reception, the LMA/NS decapsulates the packet and forwards it to the AS as an IPv6 packet.

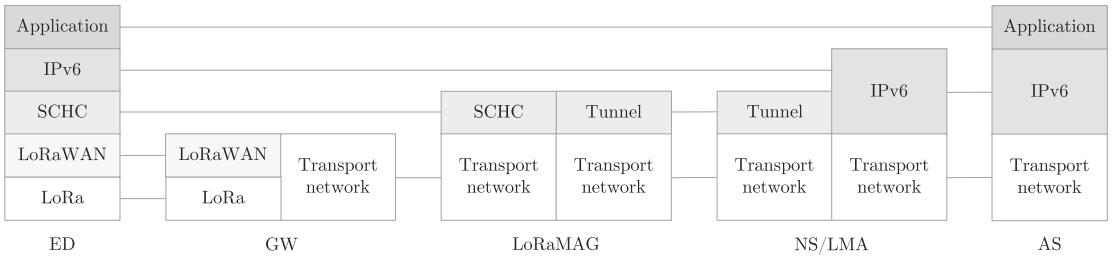


Figure 3.5: Evolved LoRaWAN user-plane protocol stack.

- **Control-plane protocol stack**

  The CP protocol stack for an ED communicating with the NS using the evolved LoRaWAN architecture is shown in Figure 3.6. In LoRaWAN, the CP is the group of messages exchanged between the ED and the NS containing LoRaWAN MAC commands. A downlink LoRaWAN MAC command is sent by the NS/LMA to the serving LoRaMAG without encapsulation since it is not an IP packet and its security is ensured by LoRaWAN security. The LoRaMAG forwards it to the GW over a transport network, which forwards it to the ED through the LoRaWAN link.

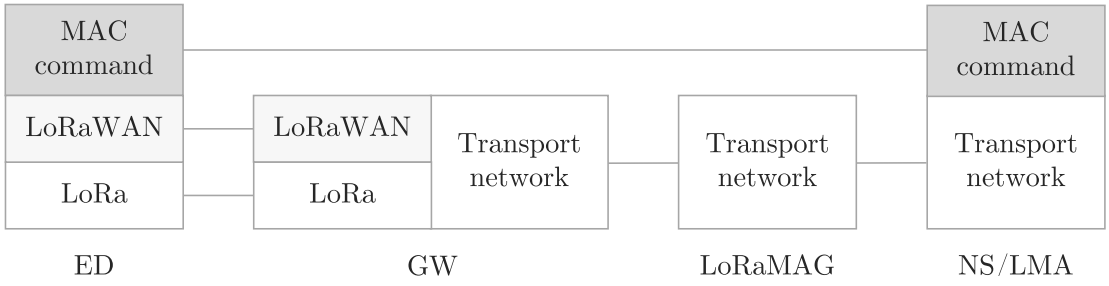


Figure 3.6: Evolved LoRaWAN control-plane protocol stack.

3.2.3 Authentication scheme

The proposed authentication scheme is used to solve the authentication problem of MN with PMIPv6 domain described in Section 3.1 in case of intra-domain mobility. This scheme belongs to hash-based authentication schemes, since it is based on hashes to achieve the authentication, without the need for encryption/decryption, public/private keys, certificates and signatures.

In the first place, the AuS holds two secret keys X and Y, and a database containing an entry for each MN registered. For a MN_i, this entry contains:

- ID_i : the MN_i identifier in the PMIPv6 domain.
- X_i : the first half key of MN_i.
- Y_i : the second half key of MN_i.

This scheme consists of two phases: the registration phase executed at the time of MN deployment, and the authentication phase executed at the time of MN attachment or handoff to authenticate with the PMIPv6 domain.

3.2.3.1 Registration phase

During this phase, a MN_i associated with K LPWAN technologies generates its ID_i as shown in 3.1. For example, if a MN_i uses only LoRaWAN and NB-IoT technologies, its ID_i is shown in 3.2.

$$ID_i = H(\|_{j=1}^{K} ID_{Tech_j}) \tag{3.1}$$

$$ID_i = H(DevEUI \parallel SUPI) \tag{3.2}$$

Moreover, AuS generates the half keys X_i and Y_i according to 3.3 and and preshares them securely with MN_i.

$$X_i = H(H(X) \oplus ID_i) \qquad Y_i = H(H(Y) \oplus ID_i) \tag{3.3}$$

3.2.3.2 Authentication phase

This phase is the core of the authentication scheme by which the MN authenticates itself with the PMIPv6 domain, i.e., with the PMIPv6 entities which are the LoRaMAG and LMA/NS. The authentication with the LMA/NS is achieved through

the LoRaWAN join procedure, thus, the authentication with the LoRaMAG is still missing. Since the GWs only forward the signaling messages, we do not show them for the sake of simplicity. The authentication phase is shown in Figure 3.7 and detailed below:

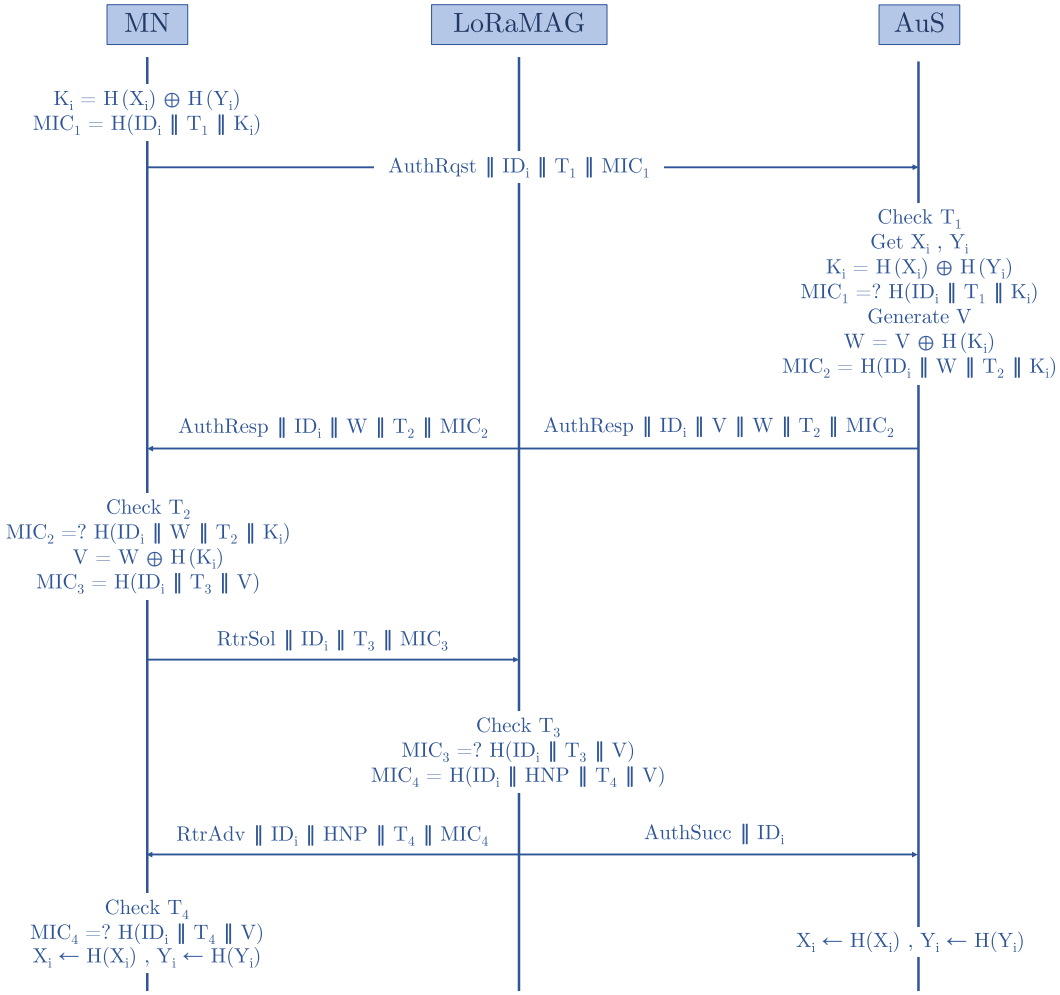


Figure 3.7: Authentication phase.

1. MN_i gets the timestamp T_1, calculates the hash key $K_i = H(X_i) \oplus H(Y_i)$ and the message integrity code $MIC_1 = H(ID_i \| T_1 \| K_i)$, and then sends an authentication request to AuS containing $ID_i \| T_1 \| MIC_1$ through LoRaMAG. The latter receives the authentication request and forwards it to AuS.
2. AuS checks the timestamp T_1 if it is within the acceptable time range. Based on ID_i, AuS gets X_i and Y_i from the database, and calculates the hash key K_i and MIC_1. If the received MIC_1 is equal to the calculated one, MN_i message is authenticated by the AuS. Thus, the AuS generates a random number V, and calculates $W = V \oplus H(K_i)$. The AuS gets the timestamp T_2, calculates $MIC_2 = H(ID_i \| T_2 \| W \| K_i)$, and then sends the authentication response for LoRaMAG containing $ID_i \| V \| W \| T_2 \| MIC_2$. LoRaMAG gets the random number V and forwards the rest of the authentication response to MN_i.

3. MN_i checks the timestamp T_2 if it is within the acceptable time range, and calculates MIC_2. If the received MIC_2 is equal to the calculated one, the AuS message is authenticated by the MN_i which gets the random number V by calculating $V = W \oplus H(K_i)$. Moreover, MN_i gets the timestamp T_3, calculates $MIC_3 = H(ID_i \parallel T_3 \parallel V)$, and then sends a RtrSol message containing $ID_i \parallel T_3 \parallel MIC_3$.

4. LoRaMAG checks the timestamp T_3 if it is within the acceptable time range and calculates MIC_3. If the received MIC_3 is equal to the calculated one, the MN_i message is authenticated by the LoRaMAG. Thus, the latter should reply to the RtrSol message by a RtrAdv message containing the MN-HNPs. Therefore, the LoRaMAG gets the timestamp T_4 and calculates $MIC_4 = H(ID_i \parallel T_4 \parallel HNP \parallel V)$, and then sends a RtrAdv message containing $ID_i \parallel T_4 \parallel HNP \parallel MIC_4$. In addition, LoRaMAG sends an authentication success message containing ID_i to the AuS indicating the success of the authentication.

5. MN_i checks the timestamp T_4 if it is within the acceptable time range and calculates MIC_4. If the received MIC_4 is equal to the calculated one, the LoRaMAG message is authenticated by the MN_i which gets the MN-HNPs from the message to configure its network layer interface.

6. After a successful authentication, the AuS updates the database entry $\{ID_i, X_i \longleftarrow H(X_i), Y_i \longleftarrow H(Y_i)\}$. At the same time, the MN_i updates the two memory registers containing the half keys by saving $X_i \longleftarrow H(X_i)$ and $Y_i \longleftarrow H(Y_i)$.

This authentication scheme guarantees the authenticity and the integrity of RtrSol and RtrAdv messages. The data confidentiality between the MN and the LoRaMAG is not provided since it is not recommended, while it is recommended for the MN communication with the NS and AS which is ensured through LoRaWAN security. For that, we do not overload the authentication scheme with additional data encryption mechanisms. In addition, this authentication scheme provides continuous authentication as long as the MN moves inside the PMIPv6 domain where two cases are investigated.

In the first case, the MN moves between GWs connected to the same LoRaMAG, called intra-MAG mobility. In this case, the MN should resend a RtrSol message in the same way explained in the authentication scheme. The LoRaMAG can verify its authenticity by performing the same check on the MIC, and sends a RtrAdv message containing the MN-HNPs which is also authenticated by the MN. In this case, the random number V is the source of authentication and is considered the anchor hash key.

In the second case, the MN moves between GWs connected to different LoRaMAGs, called inter-MAG mobility. In this case, the MN should begin the authentication scheme again. However, the new hash key K_i^{new} used in the following steps will be different from the previous one K_i^{old} used during the past authentication with the previous LoRaMAG. In addition, the previous LoRaMAG cannot derive K_i^{new} since it is derived by the hash of two half keys. Thus, in case an attacker takes control over a LoRaMAG, it cannot break the subsequent authentications.

The lengths of the parameters used during the authentication are shown in Table

3.1 and as follows. The length of identity (L_{ID}) is proposed to be equal to 4 Bytes, where the PMIPv6 domain is not supposed to carry more than 2^{32} devices. The length of timestamp (L_T) should be between 4 to 8 Bytes according to [121], we choose an L_T equal to 8 Bytes to guarantee higher security, which is equal to the timestamp length used in PMIPv6. The length of hash (L_H) is equal to the hash algorithm output length. In our solution, we propose to use one of the Secure Hash Algorithms (SHAs) [122] to generate the hashes. Several SHA algorithm exists like SHA-1, SHA-224, SHA-256, and SHA-384. SHA-1 and SHA-224 are not considered secure, thus we propose to select from SHA-256 or SHA-384. Taking into account the processing power and battery lifetime constraints, we propose to use SHA-256 hash algorithm, thus L_H is equal to 32 Bytes. The length of MN-HNP (L_{HNP}) is equal to 16 Bytes according to PMIPv6 specifications.

Table 3.1: Length of authentication parameters.

Parameter	**Length (Bytes)**
ID	4
Timestamp	8
Hash	32
MN-HNP	16

3.2.4 Mobility management

Several types of mobility may happen as summarized in Table 3.2. In any type, the mobility is considered to happen within the same network coverage, i.e., intra-domain mobility. As discussed before, two additional types of mobility may happen called intra-MAG mobility, and inter-MAG mobility. These two types can be combined with homogeneous and heterogeneous mobility, thus, four intra-domain mobility types may exist. In this section, we describe the behavior of our solution in each mobility type based on the following parameters: PMIPv6 handoff procedure, authentication scheme, link layer identifier, IPv6 address and SCHC context.

Regarding the PMIPv6 handoff procedure, it is not executed in homogeneous intra-MAG handoff, since the link layer identifier, the IPv6 address and the SCHC context do not change, thus there is no need for any information update in the MN BCE stored in the LMA. However, inter-MAG handoff necessitates the execution of the handoff procedure since there is a movement between two MAGs. A heterogeneous intra-MAG handoff necessitates also the execution of the handoff procedure to update the MN BCE since the link layer technology and identifier are changed.

Regarding the authentication, it is not executed in homogeneous intra-MAG handoff, since the handoff is between several GWs or eNBs connected to the same MAG. For example, when a MN moves to a new GW in LoRaWAN, and sends a RtrSol message to the LoRaMAG, the latter can authenticate the MN directly based on the hash key V as discussed before. In homogeneous inter-MAG handoff, authentication is needed since a RtrSol message sent by the MN cannot be authenticated

by the next MAG. In heterogeneous handoff, each LPWAN technology has its own authentication scheme, thus authentication is needed in this case.

Regarding the link layer identifier, it does not change in homogeneous handoff since the used technology does not change, and the handoff is confined inside the same network assigning the link layer identifier. However, heterogeneous handoff will lead necessarily to the change in the link layer identifier as it is assigned according to the underlying technology.

Regarding the SCHC context saved in the MN and the LoRaMAG, there are several static fields that do not change. The version field indicating the IP version used during the communication is static and always indicates 'IPv6 version'. The differential service and flow label fields indicating the packet priority and path required are also static since the application served by the MN is unique. The next header field is static since no additional headers are used in PMIPv6 as detailed before, and the hop limit field is set once during the interface configuration. The destination address field is also constant since it represents the CN or AS address. The unique field that may change is the source address. This may happen when the MN receives a RtrAdv message containing MN-HNPs different than the previously used. However, this case is not frequent in PMIPv6 but should be taken into consideration.

Thus, each mobility scenario requires specific handling by the mobility solution as detailed before to reach an optimal performance and reduced overhead.

Table 3.2: Mobility management in different mobility scenarios.

Mobility type	MAG	PBU	Auth	L2 ID	IPv6 address	SCHC context
Homogeneous	Intra	No	No	Invariable	Invariable	
	Inter	Yes	Yes		May vary	
Heterogeneous	Intra	Yes	No	Variable	Invariable	
	Inter	Yes	Yes		May vary	

3.2.5 Intra-domain mobility scenario

In Figure 3.8, we show a detailed mobility scenario for a MN performing heterogeneous inter-MAG mobility, where the MN moves from an NB-IoT eNB coverage to a LoRaWAN GW coverage connected to different MAGs. These two MAGs are connected to the same LMA. The PMIPv6 domain consists of:

- NB-IoT sub-network containing mainly: eNBs, S-GW acting as a MAG, P-GW acting as a LMA, and MME.
- LoRaWAN sub-network containing: GWs, LoRaMAG, NS acting as a LMA, and AuS.
- External entities: JS and AS.

At the beginning of this scenario, the MN enters the coverage of the NB-IoT network, thus it sends an attach request and completes the attach procedure described in [111]. After this procedure, the MN is attached to the NB-IoT network representing a PMIPv6 domain, and obtains its link layer identifier, its IPv6 address, and the SCHC context used to compress the IPv6 headers.

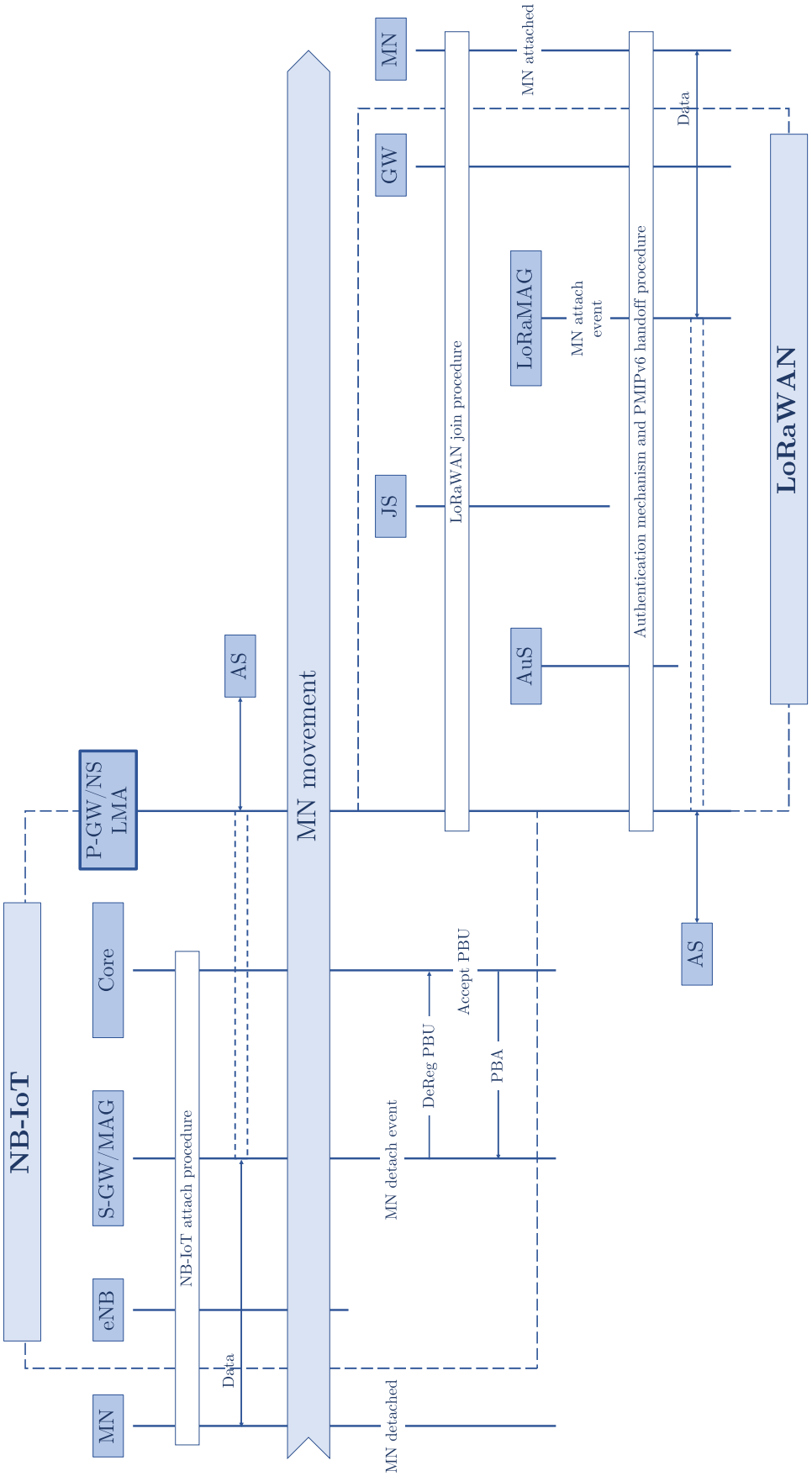


Figure 3.8: Intra-domain mobility scenario.

This context is saved in the MN and the eNB. In addition, a tunnel is established between the MAG/S-GW and the LMA/P-GW to tunnel the MN packets.

When the MN needs to send application data to the AS, it should encapsulate them in an IPv6 packet. The packet header is compressed by the SCHC algorithm located in the MN adaptation layer. After that, this packet is sent over the DRB to the eNB having the SCHC context, thus, it decompresses the packet header and rebuilds the original header. Thereafter, the eNB forwards the original packet to the MAG/S-GW through S1 interface which tunnels them to the LMA/P-GW. The latter removes the tunnel header, and then forwards the original packet to the AS.

After that in this scenario, the MN moves away from the coverage of the NB-IoT network, thus the MAG/S-GW will detect the detachment and send DeReg-PBU message to LMA/P-GW. The LMA/P-GW accepts the DeReg-PBU and sends a PBA to the MAG/S-GW to discard the established tunnel. At the same time, the MN tries to find a network to attach, and as it is supporting LoRaWAN technology, it sends a join request to the listening GWs which forward it to LMA/NS through LoRaMAG. The MN completes the LoRaWAN join procedure with the assistance of the JS. Right away, the MN obtains its LoRaWAN identifier which is a link layer identifier. The LoRaMAG detects the MN attachment, which also tries to rejoin the PMIPv6 domain by sending a RtrSol message which needs to be authenticated by the LoRaMAG. The authentication scheme described in Section 3.2.3 is executed between MN, LoRaMAG and AuS. After a successful authentication, the LoRaMAG sends PBU to update the BCE fields in LMA/NS, and to create a new tunnel. The updated fields are the link layer identifier, the tunnel interface identifier, the access technology type, and the timestamp value. In this way, the LMA/NS will reply with a PBA to LoRaMAG. The latter sends a RtrAdv to the MN which can retain or reconfigure its IPv6 address. The SCHC context may vary in this case if the MN changes its IPv6 address. After finishing this procedure, the MN can send application data to LoRaMAG encapsulated and compressed in packets. The LoRaMAG decompresses the packet header and then tunnels them to LMA/NS. The LMA/NS removes the tunnel headers, and finally forwards the original IPv6 packets to the AS.

This scenario is considered a heterogeneous inter-MAG mobility. Thus, the PMIPv6 handoff procedure is needed to disconnect the MN from the NB-IoT network and reconnect it through the LoRaWAN network. The link layer authentication is needed to authenticate the MN with LoRaWAN network, and the network layer authentication is required to authenticate the MN with the LoRaMAG. In addition, the SCHC context and the IPv6 address of the MN are not changed, however, they are generated and saved in the new LoRaMAG to activate the communication.

3.3 Performance evaluation

To examine the efficiency of the proposed mobility solution, we evaluate the performance according to two main metrics which are the handoff delay and the signaling overhead. This is achieved theoretically and by simulation as described in the following.

3.3.1 Handoff delay

The handoff delay (T_{HO}) represents the time needed for the MN to establish the new radio access link and resume data sending. The handoff starts when the MN is no longer able to send or receive messages through the current RAP and needs to detach from it. The handoff ends when the MN is able again to send or receive messages through the new RAP after a successful attachment. In our solution, the handoff starts with the detachment of the MN at the link layer followed by DeReg-PBU and PBA messages between the current MAG and the LMA to discard the current MN tunnel. After that, the MN should attach at the link layer using the new LPWAN technology attachment procedure. Thereafter, the proposed authentication scheme is executed to authenticate the MN at the network layer with the PMIPv6 domain again. After that, the next MAG and the LMA exchange the PBU and PBA to establish the new MN tunnel. The handoff is terminated at this point and the MN is able to send application data through the new LPWAN technology to the AS. In the following, we evaluate T_{HO} by theoretical and simulation results, and we validate them after that.

3.3.1.1 Theoretical results

Theoretically speaking, T_{HO} is the sum of the PMIPv6 handoff procedure delay (T_{PMIPv6}), the link layer attachment delay (T_{Link}), and the authentication delay (T_{Auth}) as shown in 3.4.

$$T_{HO} = T_{PMIPv6} + T_{Link} + T_{Auth} \tag{3.4}$$

T_{PMIPv6} and T_{Link} are related to PMIPv6 and the LPWAN technology. However, T_{Auth} is related to the proposed authentication scheme presented in Section 3.2.3. As described before, several steps are executed to complete the authentication scheme. T_{Auth} is the sum of three main delays as shown in 3.5. The first delay contributing to T_{Auth} is the processing delay (T_P) which is the time needed to perform some operations like hashing, concatenation, writing in the database, fetching a record from the database, etc. T_P is highly dependent on the processor used to perform these operations. The second delay contributing to T_{Auth} is the IP link delay (T_{IP}) which is the time needed to exchange the messages between the GW, LoRaMAG and AuS over the IP links, therefore, this delay is dependent on the IP link throughput. The third and most contributing delay to T_{Auth} is the radio link delay (T_R) given in 3.6. It is the time needed to exchange the messages between the MN and RAP over the radio link. As discussed before, in case of LoRaWAN, this delay is dependent on R_b, which is dependent on the BW and SF used.

$$T_{Auth} = T_P + T_{IP} + T_R \tag{3.5}$$

$$T_R = \frac{4L_{ID} + 4L_T + 5L_H + L_{HNP}}{R_b} = \frac{1792}{R_b} \tag{3.6}$$

In the following, we focus on T_R which contributes mainly in T_{Auth}. T_{IP} is dependent on the throughput of the IP links between the GWs, LoRaMAG and AuS,

and since this throughput is in the range of several Mbps or Gbps, T_{IP} is considered negligible with respect to T_R. In addition, T_P is dependent on the processing power of the used processor and contributes insignificantly to T_{Auth}. Therefore, we focus on T_R as it represents approximately T_{Auth} as shown in 3.7.

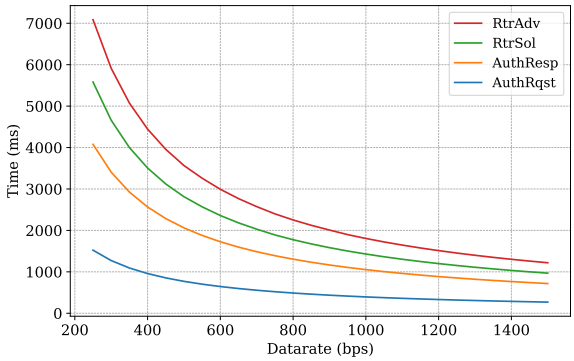
$$T_{Auth} \approx T_R \qquad T_{IP} \to 0,\ T_P \to 0 \tag{3.7}$$

3.3.1.2 Simulation results

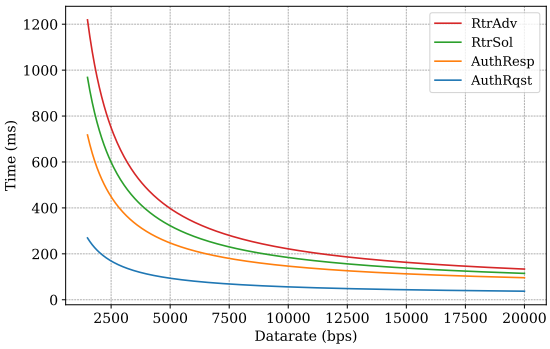
We used Network Simulator 3 (NS-3) [123] to simulate the proposed authentication scheme and evaluate its performance based on the monitored metrics. NS-3 is a discrete event network simulator targeted for educational and research use. It is an open-source software maintained by a worldwide community. The simulation scenario consists of a MN/ED, GWs, LoRaMAG, NS/LMA, and AuS. The MN has an active LoRaWAN link with a GW connected to the NS/LMA through a LoRaMAG. This link is characterized by its data rate which changes according to the BW and SF used. The MN is trying to authenticate itself to the PMIPv6 domain using the previously described authentication scheme. Thus, the authentication scheme messages are exchanged between the MN, LoRaMAG, and AuS. In addition, IP links are set up between the GWs, LoRaMAG, and AuS. We consider that the links between the LoRaMAG and the connected GWs forward uplink and downlink messages in both directions. The implementation source codes can be found in [124].

The main metric monitored in this simulation is the T_{Auth} which is directly dependent on the data rate used. The considered data rate range is that used in LPWAN technologies which is in the range of 250 bps and 21.9 kbps for LoRaWAN, and up to 66 kbps for NB-IoT. To be more adequate, we checked the burden of each step executed during the authentication scheme which are the AuthRqst, AuthResp, RtrSol, and RtrAdv. For that, we logged the time needed to execute each step by running the simulation at each data rate from 250 bps to 66 kbps. Then we traced the duration of each step over the data rate range. The results are shown in Figure 3.9 where T_{Auth} is represented by the RtrAdv plot since it is the last step executed in the authentication scheme. We divide the data rate range into three sub-ranges. The first sub-range is between 250 bps and 1.5 kbps which represents the lower range of LoRaWAN and NB-IoT data rates. The use of this range leads to a T_{Auth} between 1 and 7 seconds as shown in Figure 3.9a, which may not be acceptable for several applications. Thus, we recommend the use of the second sub-range which is between 1.5 kbps and 20 kbps leading to a T_{Auth} of less than 1 second as shown in Figure 3.9b, which is acceptable for LPWAN applications. We note that the upper LoRaWAN data rate bound is 21.9 kbps. Anyway, a third sub-range may be also used which is between 20 kbps and 66 kbps which leads to a T_{Auth} of less than 140 ms as shown in Figure 3.9c, however, the fast increase of data rate will not lead to the intended decrease of T_{Auth}, and this sub-range is available only for NB-IoT technology using multi-tone operation. Thus, the second sub-range is the most recommended to be used in our authentication scheme.

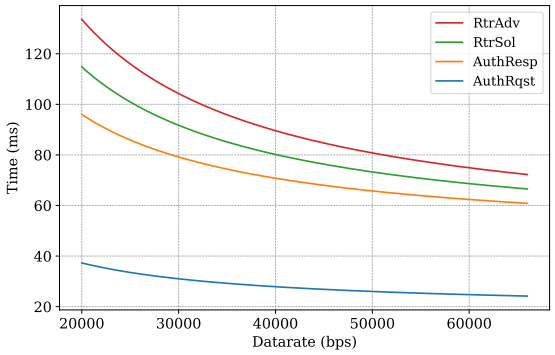
Regarding the time needed by each step, we can see the AuthRqst, RtrSol messages need approximately the same time since they are constituted by the same number of bytes which is 44 Bytes. The RtrAdv message needs a little more time



(a) R_b: 250 bps → 1.5 kbps.



(b) R_b: 1.5 kbps → 20 kbps.



(c) R_b: 20 kbps → 66 kbps.

Figure 3.9: Simulation results of the time of authentication.

since MN-HNPs are sent in addition, where this message is constituted of 60 Bytes. The AuthResp message is the longest message in the authentication scheme needing more time where it is constituted of 76 Bytes.

3.3.1.3 Validation of the results

To validate the theoretical and simulation results, we compared T_R given theoretically by 3.6, and T_R given by the simulation. Although T_{Auth} is approximately equal to T_R, the latter can be gotten accurately in the simulation by the summation of the time of messages exchanged over the LoRaWAN link. We plot the simulation results along with the theoretical results in Figure 3.10 for the second data rate sub-range, i.e., between 1.5 kbps and 20 kbps. The figure shows the validity of the obtained results with a very small margin of error.

3.3.2 Signaling overhead

The signaling overhead of handoff procedure (SO_{HO}) represents the number of bytes required by the signaling messages used during the handoff procedure. As described before, the handoff consists of three main procedures: the PMIPv6 handoff procedure, the link layer attach procedure of the next LPWAN technology, and the authentication scheme procedure. Each procedure contributes in the SO_{HO}, thus,

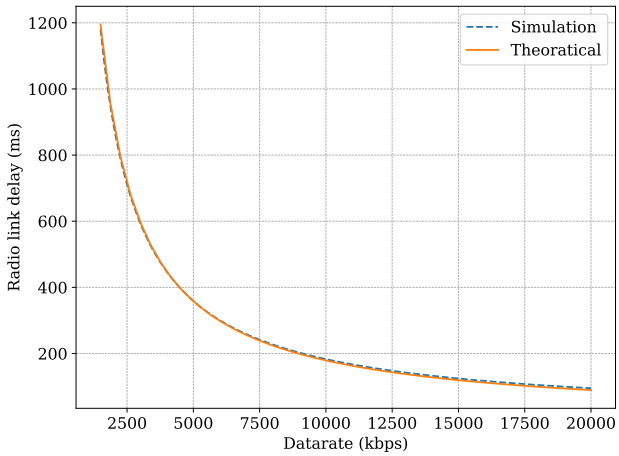


Figure 3.10: Validation of the results.

SO_{HO} is the sum of the signaling overhead of PMIPv6 handoff procedure (SO_{PMIPv6}), the signaling overhead of link layer attachment (SO_{Link}), and the signaling overhead of authentication scheme (SO_{Auth}) as shown in 3.8.

$$SO_{HO} = SO_{PMIPv6} + SO_{Link} + SO_{Auth} \tag{3.8}$$

SO_{Auth} is the signaling overhead due to messages exchanged during the authentication scheme described in Section 3.2.3. The SO_{Auth} per MN authentication is given by 3.9. We should differentiate here between uplink and downlink messages since uplink messages are routed through several GWs that are connected to the serving LoRaMAG. We consider that N GWs are connected to one LoRaMAG in average, although N may be variable from one LoRaMAG to another. However, downlink messages are routed by the LoRaMAG through one GW as detailed before. In Table 3.3, we show the SO_{Auth} for several values of N.

$$SO_{Auth} = (L_{ID} + L_T + L_H)(2N + 7) + L_H + 2L_{HNP} = 88 * N + 372\ [Bytes] \tag{3.9}$$

Table 3.3: Signaling overhead of the authentication scheme.

N	**SO_{Auth}**
2	548
3	636
4	724
5	812

3.4 Security evaluation

Since we propose a secure solution for mobility management in LPWANs, we evaluate the security of this solution through security analysis and using a protocol security validation tool as shown below.

3.4.1 Security analysis

We evaluate the security of our proposed solution according to the common security requirements and mobility-related security issues presented in Section 2.5.2 as shown below:

- Confidentiality: we distinguish between two types of confidentiality which are data confidentiality and signaling message confidentiality. For data confidentiality, we rely on the application or transport layers for data encryption. For example, in LoRaWAN, the AppSKey is used to secure the session data between the ED and AS. In NB-IoT, the PDCP consists of a sub-layer for data ciphering/deciphering where key agreement is achieved during the attachment procedure. Thus, data confidentiality is ensured. For signaling message confidentiality, although there is no encryption mechanism used in the authentication scheme, confidential data such as hash keys and half keys are never revealed to any entity other than the MN and AuS, and the secret variable V is still secret in all the exchanged signaling messages.
- Message integrity: the integrity of each message used during the authentication scheme is ensured by the MIC field. MIC_1 and MIC_2 use hash key K_i only known by the MN and AuS. MIC_3 and MIC_4 use V as a hash key, which is known by the LoRaMAG who receives it from AuS, and known by the MN performing the XORing of W and $H(K_i)$, and since K_i is only known by the MN and AuS, an attacker is not able to reveal the value of V. Thus, all signaling messages are integrity protected in a secure manner.
- Mutual authentication: the entities participating in the authentication scheme authenticate each other on the MIC generated using a certain hash key. There are three security associations needing mutual authentication which are between MN and AuS, AuS and LoRaMAG, MN and LoRaMAG. The first is ensured by K_i only known to MN and AuS. The second is considered an assumption as specified in PMIPv6 specification. The third is ensured using V exchanged securely, thus when the MN checks MIC_3 and verifies that the same V sent by AuS is used by LoRaMAG, the MN authenticates LoRaMAG. The same is performed with MIC_4 to authenticate the MN by LoRaMAG.
- Key freshness: at the end of each authentication, the MN and AuS update the registers and the database records containing X_i and Y_i by $H(X_i)$ and $H(Y_i)$, respectively. For that, in the next authentication, the new hash key used K_i^{new} is quite different from the previous K_i^{old}. This protects the key generation if a LoRaMAG becomes malicious, which will be able to extract $H(K_i^{old})$ from the received V and the listened W. LoRaMAG is not able to get K_i^{old} as hash functions are irreversible. In any case, if K_i^{old} is revealed, K_i^{new} cannot be deduced, since it is derived from half keys X_i^{new} and Y_i^{new}, and $K_i^{new} = H(X_i^{new}) \oplus H(Y_i^{new}) = H(H(X_i^{old})) \oplus H(H(Y_i^{old}))$, is not equal to $H(K_i^{old})$, i.e., $H(H(X_i^{old}) \oplus H(Y_i^{old}))$. Thus an attacker should reveal X_i^{old} and Y_i^{old} separately, which is computationally infeasible.
- Replay attack: each sender of a signaling message adds a timestamp field. Thus, each receiver should check the timestamp to ensure the freshness of this

message in order to prevent replay attacks.

- Denial of service: to prevent a MN from randomly sending authentication requests, the AuS must keep a track of the MN authentication requests. The AuS can deploy an algorithm that takes as input several parameters such as MN speed, network coverage and other parameters to calculate the expected number of authentication requests. If the number of authentication requests is greater than the excepted one, the AuS should consider this MN to be malicious, and should stop responding to its authentication requests. The exact specifications of the aforementioned algorithm are beyond the scope of this solution.
- Spoofing signaling message: each signaling message is integrity protected by the sender using the MIC field, which is used by the receiver to authenticate the sender. Thus, an attacker cannot spoof any signaling message on behalf of another entity in the network.
- Address squatting, spoofing, and old address control: since the MN authenticates itself when moving in the PMIPv6 domain, the LMA is aware of its address using the BCE saved in the LMA. This prevents an attacker to squat and spoof a MN address. In addition, a MN retains its old address in case of intra-domain mobility, thus its address is prevented from squatting.
- Context alteration: in this solution, the SCHC compression/decompression context is saved and managed by the SCHC algorithm. Thus, it is considered tamper-resistant and saved safely in the corresponding entities.

3.4.2 AVISPA evaluation

We use Automated Validation of Internet Security Protocols and Applications (AVISPA) [125] software to evaluate the security of our authentication scheme. AVISPA is a software performing automated validation of internet security protocols. AVISPA contains four sub-components to evaluate the security of the implemented protocol. The implementation is made using High Level Protocol Specification Language (HLPSL).

In Figure 3.11, we show the last part of the implementation of the authentication scheme using HLPSL which contains the environment and the goals intended by the implemented protocol. In the environment, we declare three agents that will play the role of MN, MAG, and AuS. In addition, we declare the keys used during the authentication which are the half keys X and Y, and a key named SK to protect the exchanges between AuS and MAG since this link is considered secure. Moreover, we declare a hash function and the channels used to send and receive messages between the agents. Besides, we declare the protocol identifiers used later in the goals. As a part of the implementation, the intruder knowledge should be given in the environment which is the set of agents and keys accessible by the intruder. In the end, we declare the session that aggregates these parameters in one communication scenario. This session declares the set of agents involved where the operation of each agent is defined in the rest of the implementation.

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

role enviroment()

        def=

                const
                        mn,mag,aus : agent,
                        h : hash_func,
                        x,y,sk : symmetric_key,
                        snd,rcv : channel(dy),

                        sec_x, sec_y, sec_hk : protocol_id,
                        auth_aus_mn, auth_mn_aus, auth_mag_mn, auth_mn_mag : protocol_id

                intruder_knowledge = {mn,mag,aus,h,i}

                composition
                        session(mn,mag,aus,x,y,sk,h,snd,rcv)

end role

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

goal
        secrecy_of sec_x
        secrecy_of sec_y
        secrecy_of sec_hk

        authentication_on auth_aus_mn
        authentication_on auth_mn_aus
        authentication_on auth_mag_mn
        authentication_on auth_mn_mag

end goal

enviroment()

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

Figure 3.11: HLPSL implementation of intra-domain authentication.

Regarding the goals intended by the authentication scheme, two types can be defined: a secrecy goal and an authentication goal. The secrecy goal is achieved when a secret parameter is not revealed to an intruder, and the authentication goal is achieved based on a secret parameter only known to the communicating agents. Thus, we specify that half keys X and Y, and the hash key K_i should be secret. In addition, we specify that the MN and AuS should achieve a mutual authentication based on K_i, and the MN and MAG should achieve a mutual authentication based on V, as defined in the rest of the implementation.

After running AVISPA for an implemented scheme, the output proves if the mechanism is secure or not by visualization of a screen containing a safe or unsafe message. In case of an insecure protocol, AVISPA gives the method by which the attacker is able to break the authentication scheme. Thus after implementing our mechanism using HLPSL and running AVISPA, the output proves that it is safe as shown in Figure 3.12. The implementation source codes can be found in [126].

3.5 Conclusion

In this chapter, we presented our mobility solution based on PMIPv6 for homogeneous and heterogeneous intra-domain mobility for LPWAN technologies. Addi-

tionally, we evaluated the performance of our solution according to the handoff delay and the signaling overhead. Moreover, we evaluated the security of our solution as we propose a secure mobility solution, where the security is ensured through the proposed authentication scheme. Although this solution has a decent performance and security features, we still need an inter-domain mobility management solution. Thus, in the next chapter, we propose an improved authentication scheme that enables inter-domain mobility, and we compare our solution with related work in terms of performance and security which proves the supremacy of our solution over related work.

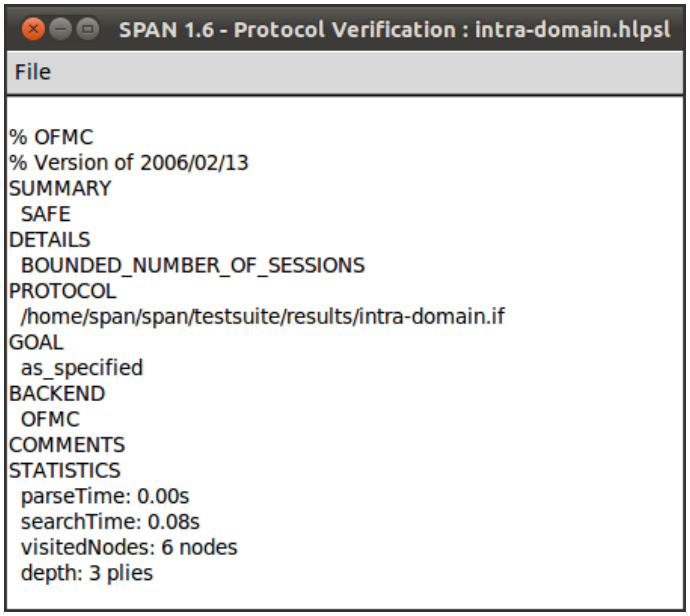


Figure 3.12: Security evaluation using AVISPA.

Chapter 4

Secure Inter-domain Mobility Solution for LPWANs

Abstract *— In this chapter, we present our improved mobility management solution for inter-domain mobility in LPWAN environments. We detail first the improved design principles, then we present the extension of the authentication scheme used by PMIPv6 entities to authenticate a mobile node registered or not with the PMIPv6 domain. Next, we detail how mobility is managed in each type of inter-domain mobility as well as the impact of each type on several mobility parameters. We show also a detailed inter-domain mobility scenario along with the functions of each network entity and the messages flow. Later on, we evaluate the performance of the improved solution after adding the extension of the authentication scheme according to handoff delay and signaling overhead. Moreover, we detail how this solution is compatible and satisfy the LPWAN constraints. The security is also evaluated according to the common security requirements and mobility-related security issues presented before, as well as using AVISPA software. To understand the obtained results, we compare the mobility and the security features provided by this solution to that provided by related work presented before. This will prove also the efficiency and the security ensured by the deployment of our solution.*

4.1 Improved design principles

In Chapter 3, we proposed a secure intra-domain mobility solution for LPWANs. However, inter-domain mobility is a common behavior and a main requirement for several LPWAN applications. Thus, in this chapter, we propose a secure inter-domain mobility solution for LPWANs based on the previous solution with the following improved design principles where we focus on LoRaWAN technology:

- Same as previous network architecture and protocol stack: since the main objective in this solution is to support inter-domain mobility, which cannot be supported in the previous solution due to the limitation of the authentication scheme, we propose to use the same network architecture and protocol stack. Thus, LoRaMAG is used in LoRaWAN architecture to support MAG functions as well as other LoRaWAN functions as described in Section 3.2.1, and AuS is

used to perform the extended authentication scheme described later in Section 4.2.1 in order to achieve inter-domain authentication. At the same time, the protocol stack proposed in the previous solution is not modified where IPv6 is used at the network layer for data routing, hierarchical network partitioning, and support of PMIPv6 as an intra-domain mobility protocol. Besides, SCHC is used at the adaptation layer for the reasons presented previously. Thus, this improved solution is based on the previous one regarding the network architecture and protocol stack.

- Extended authentication scheme: the previous authentication scheme supports intra-domain authentication only, which means that a MN cannot be authenticated outside its home domain. This is because the keys used during the authentication are saved in the Home AuS (hAuS) where the MN is initially registered, thus, when the MN moves to a visited domain, the Visited AuS (vAuS) cannot authenticate the MN since it does not possess the needed keys, and there is not a protocol to communicate with hAuS in order to get them. Since the authentication with vAuS cannot be achieved, the authentication with the Visited LoRaMAG (vLoRaMAG) cannot be achieved also. For that, in Section 4.2.1, we propose an extension of the previous authentication scheme to be able to support inter-domain authentication in case of MN movement towards a visited domain.
- Authentication anchored to the visited domain: as a simple extension for the previous authentication scheme, the visited domain can forward the authentication messages to the home domain until authentication is achieved. However, this simple extension has a significant drawback which is the need to forward the authentication messages to the home domain each time the MN moves inside the visited network and needs to authenticate with another vLoRaMAG. This will lead to considerable signaling overhead exhausting the resources reserved for the communication between the home and visited domains. Moreover, this leads to an additional handoff delay since the signaling messages should be sent to home network instead of being processed locally in the visited domain. For that, we propose an extension of the authentication scheme that is anchored to the visited domain to overcome the mentioned drawback and its consequences. Thus, the authentication is relied from the home network to the visited network as described in Section 4.2.1.
- Optimized authentication extension: in the previous authentication scheme, a secret parameter V is used as a hash key in the MIC calculation of RtrSol and RtrAdv messages. This secret necessitates the calculation of the hash key K_i first and then XORing it with a parameter W. In this authentication extension, we proposed a lighter version of the previous authentication that uses directly K_i to calculate the MICs to protect the integrity of messages, and at the same time ensures the same security level as evaluated in Section 4.4.
- LPWAN compatibility: since this mobility solution is designed to work in LPWAN environments, LPWAN constraints should be carefully taken into consideration. In this improved version, we reduced the number of signaling messages needed, which allows a more adapted data rate range to be used

which is more suitable for LPWAN. We evaluate the compatibility of the improved solution with LPWAN constraints in Section 4.3.3.

4.2 Improved solution

In this section, we present the improved solution supporting inter-domain mobility management. We first describe the extended authentication scheme in Section 4.2.1, after that we describe how mobility is managed after the modification of the authentication scheme in Section 4.2.2. We present another improvement based on the previous design principles that allows to an ED to send data in RtrSol message in Section 4.2.3, and finally we describe a homogeneous inter-domain mobility scenario.

4.2.1 Extended authentication scheme

The proposed extension of the authentication scheme is used to solve the authentication problem of MN with PMIPv6 domain described in Section 3.1 in case of intra-domain mobility or inter-domain mobility. In this chapter, we focus on the second type where in a typical inter-domain mobility scenario, the MN moves in the coverage of a visited domain.

As in the previous authentication scheme, the AuS holds the same secret keys X and Y, and the database contains an entry for each MN registered. The authentication extension consists also of the same registration phase described in Section 3.2.3.1. However, the main modification is performed in the authentication phase to support inter-domain authentication as described below.

In the authentication phase, the MN tries to authenticate itself in the visited PMIPv6 domain with vLoRaMAG through vAuS and hAuS, using the exchanges shown in Figure 4.1. Each AuS is now identified by an AuS identifier ID_{AuS}. Since the GWs only forward the signaling messages, we do not show them for the sake of simplicity. Moreover, this phase is divided into two sub-phases: home authentication sub-phase, and visited authentication sub-phase.

In home authentication sub-phase, represented by the red part in the figure, the MN sends its authentication request which is forwarded to hAuS through vAuS. The hAuS checks the authentication request validity and derives two visited keys that are shared with vAuS who uses them in the visited authentication sub-phase. The home authentication sub-phase is executed in case of inter-domain mobility only and once per visited domain. In this way, the authentication scheme is anchored to the visited domain as detailed later.

In visited authentication sub-phase, represented by the green part in the figure, after hAuS sends the visited keys to vAuS, the latter uses them to authenticate the MN as long as it is in the visited domain without the need to forward the authentication requests to hAuS. After the home authentication sub-phase, the visited authentication sub-phase can be repeated several times to authenticate the MN when it moves between different vLoRaMAGs in the visited domain. The extended authentication phase is shown in Figure 4.1 and detailed below:

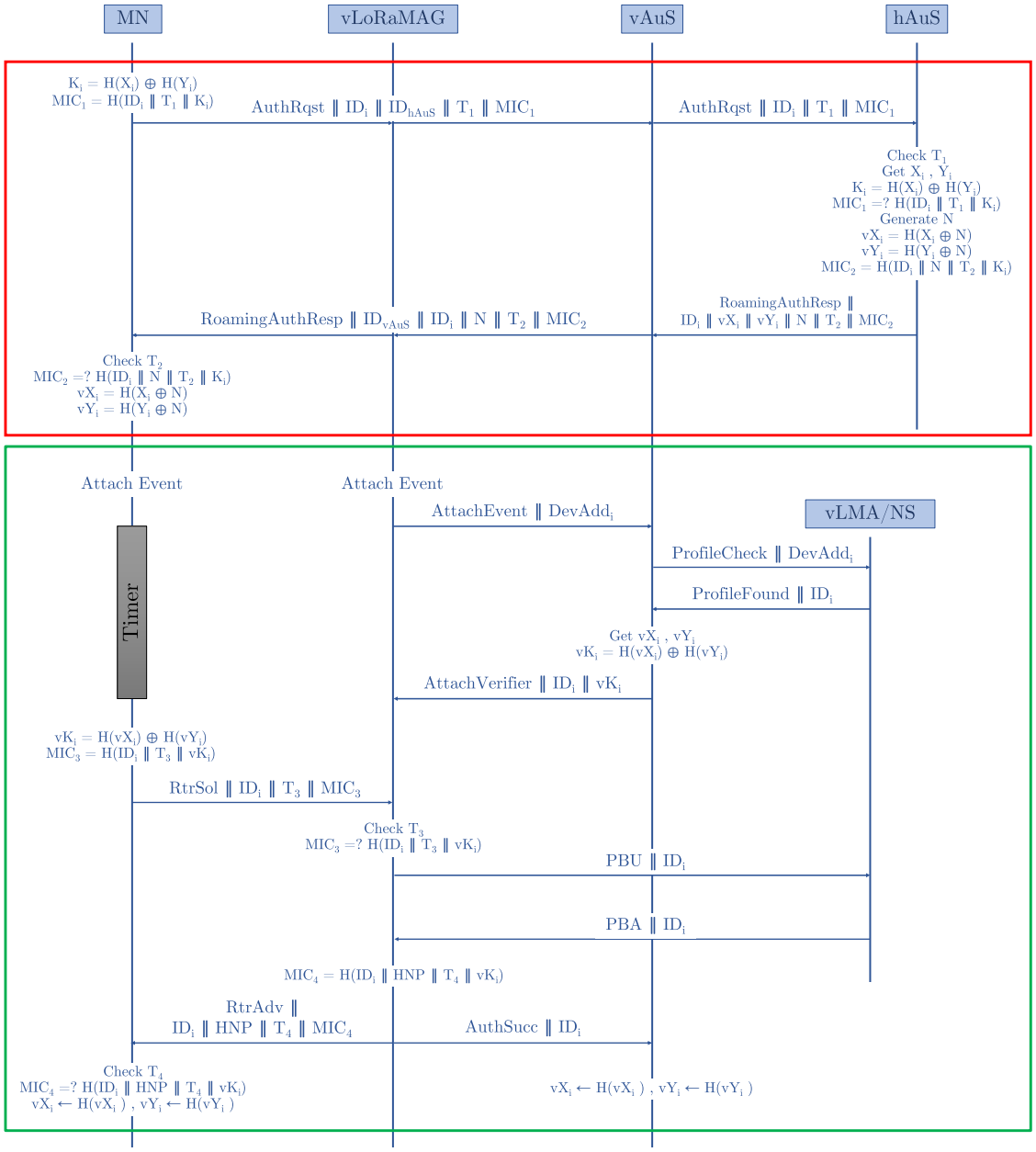


Figure 4.1: Extended authentication phase.

1. MN_i gets the timestamp T_1, calculates the hash key $K_i = H(X_i) \oplus H(Y_i)$ and the message integrity code $MIC_1 = H(ID_i \| T_1 \| ID_{hAuS} \| K_i)$, and then sends an authentication request containing $ID_i \| T_1 \| ID_{hAuS} \| MIC_1$ through vLoRaMAG. The latter receives the authentication request and forwards it to vAuS.

2. vAuS checks the requested AuS by inspecting the third field of the authentication request. Since the requested AuS is hAuS, the vAuS forwards this request to hAuS in case of the existence of a roaming agreement between the home and visited domains.

3. hAuS checks the timestamp T_1 if it is within the acceptable time range. Based

on ID_i, hAuS gets X_i and Y_i from the database, and calculates the hash key K_i and MIC_1. If the received MIC_1 is equal to the calculated one, MN_i message is authenticated by the hAuS. Thus, the hAuS generates a random number N, and calculates two visited half keys $vX_i = H(X_i \oplus N)$ and $vY_i = H(Y_i \oplus N)$. The hAuS gets the timestamp T_2, calculates $MIC_2 = H(ID_i \parallel T_2 \parallel N \parallel K_i)$, and then sends the roaming authentication response to vAuS containing $ID_i \parallel vX_i \parallel vY_i \parallel N \parallel T_2 \parallel MIC_2$.

4. vAuS receives the response and gets the visited half keys vX_i and vY_i, and saves them along with ID_i in its database. Thereafter, vAuS forwards the rest of the response to MN_i with its identity ID_{vAuS}. A mapping between ID_i and $DevAddr_i$ is saved in the vLMA/NS.

5. MN_i checks the timestamp T_2 if it is within the acceptable time range, and calculates MIC_2. If the received MIC_2 is equal to the calculated one, the hAuS message is authenticated by the MN_i. In addition, MN_i gets the random number N, and then computes $vX_i = H(X_i \oplus N)$ and $vY_i = H(Y_i \oplus N)$ which are used in the visited authentication sub-phase. At this step, home authentication sub-phase is finished and should not be executed again as long as MN_i is inside this visited domain.

6. After the reception of the roaming authentication response by the vLoRaMAG in case of first authentication request during home authentication sub-phase, or in case of detection of an attach event by vLoRaMAG in second or more MN_i attachment, the vLoRaMAG sends an attach event message containing $DevAddr_i$ to vAuS. At the same time, the MN_i launches a timer configured to a certain duration. This step represents the first step of visited authentication sub-phase. vAuS receives the attach event message from vLoRaMAG, and then sends a profile check message containing $DevAddr_i$ to vAuS/NS. The latter replies with a profile found message containing the corresponding ID_i by querying its database.

7. vAuS queries its database based on ID_i to get vX_i and vY_i, then it computes the visited hash key $vK_i = H(vX_i) \oplus H(vY_i)$, and sends an attach verifier message consisting of $ID_i \parallel vK_i$ to vLoRaMAG.

8. The timer duration launched before should be equivalent to the previous exchanges duration. After the timer elapses, the MN_i gets the timestamp T_3, computes $vK_i = H(vX_i) \oplus H(vY_i)$ and $MIC_3 = H(ID_i \parallel T_3 \parallel vK_i)$, and then sends a RtrSol message containing $ID_i \parallel T_3 \parallel MIC_3$ to vLoRaMAG.

9. vLoRaMAG checks the timestamp T_3 if it is within the acceptable time range and calculates MIC_3. If the received MIC_3 is equal to the calculated one, the MN_i message is authenticated by the vLoRaMAG. If so, vLoRaMAG sends a PBU message along with ID_i to vLMA/NS. Therefore, vLMA/NS performs the needed operations according to PMIPv6 handoff procedure and updates the BCE of MN_i. After that, vLMA/NS replies with PBA message along with ID_i to vLoRaMAG.

10. vLoRaMAG accepts the PBA message to MN_i, gets the timestamp T_4, calculates $MIC_4 = H(ID_i \parallel T_4 \parallel HNP \parallel vK_i)$, and then sends a RtrAdv message

containing $ID_i \parallel T_4 \parallel HNP \parallel MIC_4$. In addition, vLoRaMAG sends an authentication success message containing ID_i to the vAuS indicating the success of the authentication.

11. MN_i checks the timestamp T_4 if it is within the acceptable time range and calculates MIC_4. If the received MIC_4 is equal to the calculated one, the vLoRaMAG message is authenticated by the MN_i which gets the MN-HNPs from the message to configure its network layer interface.
12. After a successful authentication, the vAuS updates the database entry $\{ID_i, vX_i \longleftarrow H(vX_i), vY_i \longleftarrow H(vY_i)\}$. At the same time, the MN_i updates the two memory registers containing the half keys by saving $vX_i \longleftarrow H(vX_i)$ and $vY_i \longleftarrow H(vY_i)$.

We optimize the previous authentication scheme by leaving the use of the secret parameter V, whereas in this authentication extension, we use directly the visited hash key vK_i to calculate MIC_3 and MIC_4. This reduces the processing and complexity needed by the authentication scheme. At the same time, we conserve the same security level provided in the previous authentication scheme, where key freshness is still ensured since the use of V is substituted by the attach event and attach verifier messages. In the attach verifier message, vK_i is sent by vAuS to vLoRaMAG which uses it in the RtrSol and RtrAdv integrity protection and check.

We note that the same parameter lengths are conserved in this authentication extension. The unique new parameter used here is ID_{AuS} where we propose a length of 4 Bytes.

4.2.2 Mobility management

In this section, we discuss mobility management after the modification of the authentication scheme which supports now intra-domain and inter-domain authentication. A summary on the mobility types and their impact on several mobility parameters is shown in Table 4.1 and detailed below. We focus on homogeneous mobility where the MN deploys LoRaWAN technology at the link layer.

The intra-domain mobility management is very similar to the previous solution where the minor modification occurs in the authentication phase by substituting the use of secret parameter V by the attach event and attach verifier messages. As defined also, two additional cases may happen which are intra-MAG and inter-MAG mobility.

In intra-MAG intra-domain mobility, the MN sends a RtrSol message in the same way explained in the authentication extension, which is integrity protected using the same vK_i since the MN authenticates with the same vLoRaMAG. In this case, vK_i is the source of authentication and is considered the hash key. There is any additional procedure that should be performed in this case. The link layer authentication is not needed since the radio link is still active which is a LoRaWAN link. The PMIPv6 handoff procedure is not needed since the MN does not change the vLoRaMAG. The attach event, profile check, profile found and attach verifier messages are not needed since the same vLoRaMAG holds the network layer link with the MN. For the same reasons, the IPv6 address, the SCHC context, and the tunnel of the MN established between the vLoRaMAG and vLMA/NS are not changed.

In inter-MAG intra-domain mobility, the visited authentication sub-phase should be executed since the MN establishes a new network layer link with the next vLoRaMAG requiring network layer authentication. In this case, the attach event, profile check, profile found and attach verifier messages are needed, where the next vLoRaMAG receives the new visited hash key vK_i^{new} calculated by the vAuS after the link layer attach event. The link layer attach event does not necessarily require authentication at the link layer, where the attach event is detected by the new vLoRaMAG when the MN is in the coverage of a served GW. Thus, PMIPv6 handoff procedure is needed where a new tunnel must be established and the previous tunnel must be discarded. In addition, the IPv6 address and the SCHC context may change as detailed in Section 3.2.4.

In inter-domain mobility, only inter-MAG mobility is possible, where the MN changes the vLoRaMAG necessarily. In this case, the authentication scheme is executed entirely. The MN starts with the attachment at the link layer where it gets its new DevAddr. After that, the authentication scheme is launched by the MN, where the home authentication sub-phase is executed first, followed by the visited authentication sub-phase. Thus, the MN gets the MN-HNPs after the authentication scheme, and configures its network layer interface. A new tunnel is established for this MN between the vLoRaMAG and vLMA, and the previous tunnel established between the previous vLoRaMAG and previous vLMA in the previous visited domain is discarded after a certain time according to PMIPv6 specifications.

Table 4.1: Mobility management in different mobility scenarios.

Mobility type	**MAG**	**PBU**	**Auth**	**L2 ID**	**IPv6 address**	**SCHC context**
Intra-domain	Intra	No	No	Invariable	Invariable	
	Inter	Yes	Yes		May vary	
Inter-domain	Intra	Not possible				
	Inter	Yes	Yes	Variable		

4.2.3 Data in RtrSol message

Since LPWAN technologies have a limitation in the number of messages that can be sent per day, we propose to benefit the maximum payload length allowed in LoRaWAN to send application data in the RtrSol message. The length of this message is equal to the sum of L_{ID}, L_T and L_H, which is equal to 44 Bytes. The maximum payload length for a LoRaWAN message is 222 Bytes when using SF7 or SF8 with a BW of 125 kHz in European region. Thus, an extra 178 Bytes are allowed to be sent along with the RtrSol message, that may carry application data. We consider here four parameters which are: tunneling, IPv6 address, SCHC compression, and buffering.

In case the MN has an active network layer session with the vLoRaMAG, which happens in case of intra-MAG mobility, the IPv6 address, the SCHC context and the tunnel are already configured. Thus, the MN may encapsulate application data in an IPv6 packet, where its header is compressed by the SCHC algorithm, and then sent with the RtrSol message. The maximum application data length is equal to 178 Bytes minus the compressed header length.

In case the MN does not have an active network layer session with the vLoRaMAG, which happens in case of inter-MAG mobility, the IPv6 address, the SCHC context, and the tunnel are not already configured. Thus, the MN cannot send an IPv6 packet since it does not have an active network layer session where the IPv6 address is not configured yet. In addition, the MN cannot compress the packet header since it does not have a SCHC context. In this case, we propose to encapsulate the application data in an IPv6 packet where the IPv6 source address is equal to the old IPv6 address of the MN, which is mostly retained by the MN after the PMIPv6 handoff procedure. In any case, this address is mapped to the DevAddr when the packet is received by the vLoRaMAG. Moreover, the packet header is not compressed and its length is the IPv6 header length, i.e., 40 Bytes, thus, the remaining length for application data is equal to 138 Bytes. If the application data has a length less than or equal to 138 Bytes, it can be sent with the RtrSol message, otherwise, it should be sent separately.

4.2.4 Inter-domain mobility scenario

In Figure 4.2, we show a detailed mobility scenario for a MN performing homogeneous inter-domain mobility, where the MN moves from a home LoRaWAN GW coverage to a visited LoRaWAN GW coverage, i.e., moving from home domain coverage to visited domain coverage. Thus, two PMIPv6 domains exist as follows:

- Home domain: GWs, Home LoRaMAG (hLoRaMAG), hNS acting as Home LMA (hLMA), and hAuS.
- Visited domain: GWs, vLoRaMAG, vNS acting as Visited LMA (vLMA), and vAuS.
- External entities: JS and AS.

At the beginning of this scenario, the MN enters the coverage of home domain, thus it sends a join request and completes the join procedure described in Section 2.1.7 with the assistance of hNS/hLMA and JS. The MN is attached at the link layer, however, the MN still needs to authenticate at the network layer with the home domain. This is achieved by the execution of the visited authentication sub-phase of the authentication scheme re-called here the serving authentication sub-phase since the visited domain is the same as the home domain. Anyway, the home authentication sub-phase is not needed since the MN keys are saved in the hAuS and the serving authentication sub-phase is enough to authenticate the MN at the network layer. During the authentication, the MN obtains its IPv6 address and the SCHC context used to compress the IPv6 headers. This context is saved in the MN and the hLoRaMAG. In addition, a tunnel is established between the hLoRaMAG and the hLMA/hNS to tunnel the MN packets.

When the MN needs to send application data to the AS, it should encapsulate them in an IPv6 packet. The packet header is compressed by the SCHC algorithm located in the MN adaptation layer. After that, this packet is sent through the GW over the LoRaWAN link to the hLoRaMAG having the SCHC context, thus, it decompresses the packet header and rebuilds the original header. Thereafter, the LoRaMAG tunnels the original packet to the hLMA/hNS. The latter removes the tunnel header, and then forwards the original packet to the AS.

After that in this scenario, the MN moves away from the coverage of the home network, thus the hLoRaMAG will detect the detachment and send a DeReg-PBU message to hLMA/hNS as per PMIPv6 specifications. The hLMA/hNS accepts the DeReg-PBU and sends a PBA to the LoRaMAG to discard the established tunnel. At the same time, the MN tries to find a new network to attach through it, thus it sends a join request to the listening GWs which forward it to vLMA/vNS through vLoRaMAG. The MN completes the LoRaWAN join procedure with the assistance of the JS to authenticate with the visited network at the link layer. Right away, the MN obtains its LoRaWAN identifier which is a link layer identifier. The vLoRaMAG detects the MN attachment, which also tries to join the visited PMIPv6 domain by sending a RtrSol message which needs to be authenticated by the vLoRaMAG. Thus, the authentication scheme described in Section 4.2.1 is executed between MN, vLoRaMAG, vAuS, and hAuS. The home authentication sub-phase is executed first between the MN, vAuS, and hAuS to agree on the visited keys. Thereafter, the visited authentication sub-phase is executed between the MN, vLoRaMAG, and vAuS to authenticate the MN with the vLoRaMAG. The MN can send data in the RtrSol message where the IPv6 header must not be compressed since the SCHC context is not established yet, and the IPv6 source address is equal to the old address as detailed in Section 4.2.3. The vLoRaMAG sends PBU to create a BCE for the MN in vLMA/vNS, and to create a new tunnel. The vLMA/vNS replies with a PBA to vLoRaMAG. The latter sends a RtrAdv to the MN which configures its IPv6 address with the received MN-HNPs. After finishing this procedure, the MN can send application data to vLoRaMAG encapsulated and compressed in packets. The vLoRaMAG decompresses the packet header and then tunnels them to vLMA/vNS. The vLMA/vNS removes the tunnel headers, and finally forwards the original IP packets to the AS.

4.3 Performance evaluation

We examine the efficiency of the improved mobility solution by evaluating the performance according to two main metrics which are the handoff delay and the signaling overhead as done previously. In addition, we show how this solution is suitable to be deployed in LPWAN environments.

4.3.1 Handoff delay

As defined before, the T_{HO} is the time needed for the MN to establish the new radio link with the new RAP and resume data sending to the AS. In this solution, the handoff starts with the detachment of MN at the link layer from the home domain followed by DeReg-PBU and PBA messages between the hLoRaMAG and hLMA. After that, the MN attaches at the link layer using LoRaWAN technology with the visited domain through the join procedure. This is followed by the execution of the extended authentication scheme consisting of home authentication sub-phase and visited authentication sub-phase to authenticate the MN at the network layer with the visited domain with the assistance of vAuS and hAuS. The PMIPv6 handoff procedure is executed also as a part of the visited authentication sub-phase.

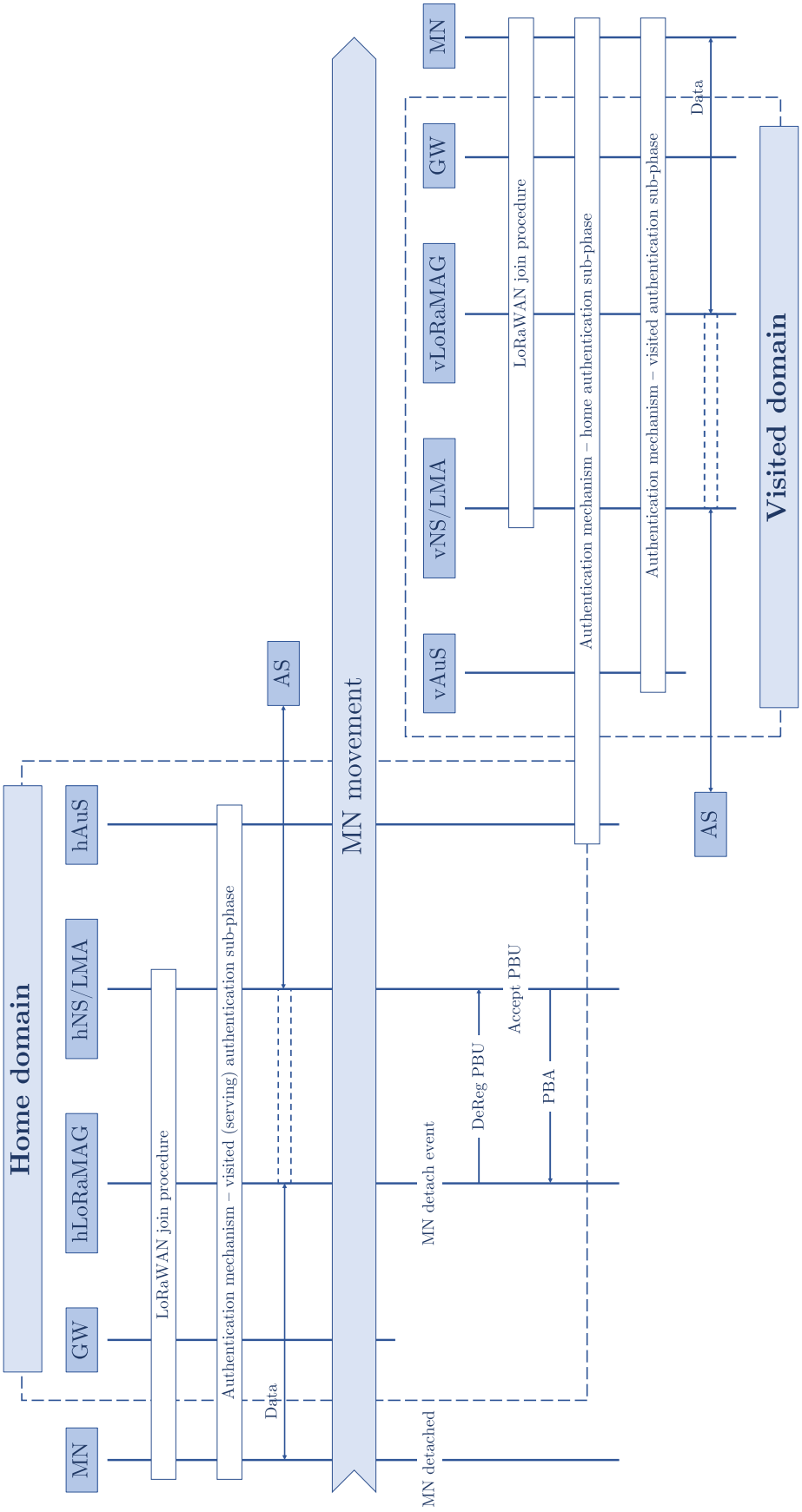


Figure 4.2: Inter-domain mobility scenario.

4.3.1.1 Theoretical results

T_{HO} is the sum of T_{PMIPv6}, T_{Link}, and T_{Auth} as detailed before and shown in 3.4. Regarding T_{Auth}, it depends on the mobility scenario which may imply or not the execution of the home authentication sub-phase. In case it should be executed, T_{Auth} is equal to the sum of home authentication sub-phase delay (T_{Home}) and visited authentication sub-phase delay ($T_{Visited}$) minus an overlapping delay ($T_{Overlap}$) as shown in 4.1.

In case the home authentication sub-phase should not be executed, which happens when the MN performs intra-domain mobility, only the visited authentication sub-phase is executed as a serving authentication sub-phase, and T_{Auth} is equal to $T_{Visited}$ only as shown in 4.1.

$$\begin{cases} T_{Auth} = T_{Home} + T_{Visited} - T_{Overlap} & : \text{with home authentication} \\ T_{Auth} = T_{Visited} & : \text{without home authentication} \end{cases} \tag{4.1}$$

Regarding T_{Home}, it consists of the $T_P{}^{Home}$, $T_{IP}{}^{Home}$, and $T_R{}^{Home}$ as shown in 4.2. The same applies for $T_{Visited}$ consisting of the $T_P{}^{Visited}$, $T_{IP}{}^{Visited}$, and $T_R{}^{Visited}$ as shown in 4.3.

$$T_{Home} = T_P^{Home} + T_{IP}^{Home} + T_R^{Home} \tag{4.2}$$

$$T_{Visited} = T_P^{Visited} + T_{IP}^{Visited} + T_R^{Visited} \tag{4.3}$$

As detailed before, $T_{IP}{}^{Home}$ and $T_{IP}{}^{Visited}$ are dependent on the IP link throughputs which are in the range of several Mbps or Gbps, thus, these two delays are considered negligible with respect to $T_R{}^{Home}$ and $T_R{}^{Visited}$. In addition, $T_P{}^{Home}$ and $T_P{}^{Visited}$ are dependent on the processing power of the used processor and contribute insignificantly to T_{Home} and $T_{Visited}$. Therefore, T_{Home} and $T_{Visited}$ are approximately equal to $T_R{}^{Visited}$ and $T_R{}^{Visited}$ as shown in 4.4 and 4.5.

$$T_{Home} \approx T_R^{Home} \qquad T_{IP}^{Home} \to 0,\ T_P^{Home} \to 0 \tag{4.4}$$

$$T_{Visited} \approx T_R^{Visited} \qquad T_{IP}^{Visited} \to 0,\ T_P^{Visited} \to 0 \tag{4.5}$$

$T_R{}^{Home}$ and $T_R{}^{Visited}$, shown in 4.6 and 4.7, are dependent on the link established between the MN and RAP. In case of LoRaWAN, this link is characterized by its R_b, which is dependent on the BW and SF used. We conserve the same length of parameters used during the authentication as shown in 3.1.

$$T_R^{Home} = \frac{4L_{ID} + 2L_T + 3L_H}{R_b} = \frac{1024}{R_b} \tag{4.6}$$

$$T_R^{Visited} = \frac{2L_{ID} + 2L_T + 2L_H + L_{HNP}}{R_b} = \frac{832}{R_b} \tag{4.7}$$

4.3.1.2 Simulation results

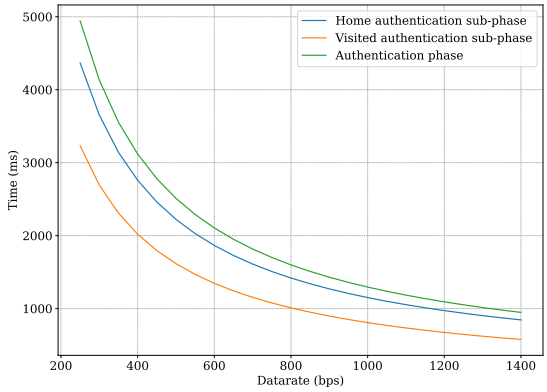
We used NS-3 to simulate and evaluate the performance of the improved solution. The simulation scenario consists of a MN/ED, GWs, vLoRaMAG, vLMA, vAuS and hAuS. In the first place, the MN has an active LoRaWAN link with a GW connected to hLMA/hNS through hLoRaMAG. The MN moves from the home domain coverage towards a visited domain coverage. Thus, the MN tries to establish a link through the visited domain having LoRaWAN as a link layer technology, thus, the LoRaWAN join procedure is executed. Thereafter, the MN starts the extended authentication scheme to authenticate at the network layer with the vLoRaMAG with the assistance of vAuS and hAuS. Therefore, the signaling messages used in the extended authentication scheme are exchanged between the MN, GWs, vLoRaMAG, vLMA/vNS, vAuS, and hAuS. The links between the network entities are IP-based, and the GWs connected to LoRaMAG forward uplink and downlink messages in both directions. The implementation source codes can be found in [127].

The main metrics monitored in this simulation are the T_{Home}, $T_{Visited}$, and T_{Auth}. T_{Home} and $T_{Visited}$ are directly related to the data rate used, and T_{Auth} consists of their sum minus $T_{Overlap}$ which can be deduced by simulation. As in the previous simulation, we simulate our solution for the LPWAN data rate range, i.e., between 250 bps and 21.9 kbps for LoRaWAN, and up to 66 kbps for NB-IoT. The results are shown in Figure 4.3. We divide the range into three sub-ranges. The first sub-range is between 250 bps and 1.4 kbps which represents the lower range of LoRaWAN and NB-IoT data rates. The use of this sub-range leads to a T_{Auth} between 1 and 5 seconds as shown in Figure 4.3a, which may not be acceptable for several applications. Thus, we recommend the use of the second sub-range which is between 1.4 kbps and 10 kbps leading to a T_{Auth} of less than 1 second as shown in Figure 4.3b, which is acceptable for LPWAN applications. Anyway, a third sub-range may be also used which is between 10 kbps and 66 kbps which leads to a T_{Auth} of less than 200 ms as shown in Figure 4.3c, however, the fast increase of data rate will not lead to the intended decrease of T_{Auth}. Thus, the second sub-range is the most recommended to be used in our extended authentication scheme.

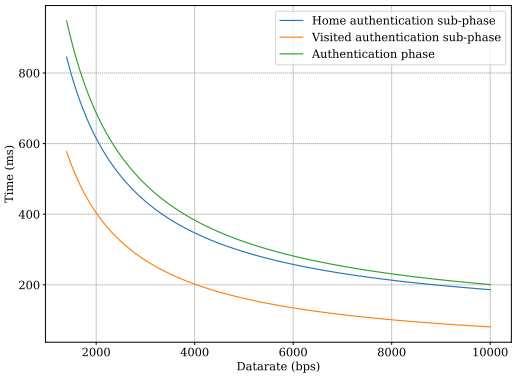
In case of intra-domain authentication, the home authentication sub-phase will not be executed, and only the visited authentication sub-phase is executed. The results show the performance improvement over the previous solution where the T_{Auth}, which is equal now to $T_{Visited}$, can attain a delay between 75 ms and 600 ms in the second data rate sub-range. The evaluation of this improved solution with other solutions is discussed later.

4.3.1.3 Validation of the results

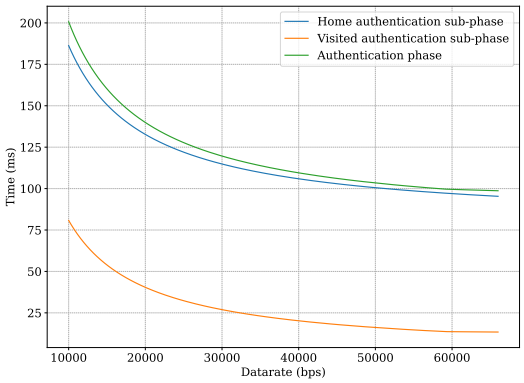
To validate the theoretical and simulation results, we compared T_{Home} and $T_{Visited}$ given theoretically by 4.4 and 4.5 with the simulation results. We plot them in Figure 4.4 for the second data rate sub-range, i.e., between 1.4 kbps and 10 kbps. The figure shows the validity of the obtained results with a very small margin of error.



(a) R_b: 250 bps → 1.4 kbps.



(b) R_b: 1.4 kbps → 10 kbps.



(c) R_b: 10 kbps → 66 kbps.

Figure 4.3: Simulation results of the time of authentication.

4.3.2 Signaling overhead

SO_{HO} is the number of bytes exchanged between the network entities during the handoff procedure in form of signaling messages. SO_{HO} is the sum of SO_{PMIPv6}, SO_{Link}, and SO_{Auth} as shown in 3.8.

SO_{Auth} is the signaling overhead due to the extended authentication scheme where we distinguish between two cases according to the type of mobility. In case of inter-domain mobility, the home authentication sub-phase is executed, thus SO_{Auth} is the sum of signaling overhead of home authentication sub-phase (SO_{Home}) and signaling overhead of visited authentication sub-phase ($SO_{Visited}$) as shown in 4.8. However, in case of intra-domain mobility, only the visited authentication sub-phase is executed as a serving authentication sub-phase, and SO_{Auth} is equal to $SO_{Visited}$ as shown in 4.8.

$$\begin{cases} SO_{Auth} = SO_{Home} + SO_{Visited} & : \text{with home authentication} \\ SO_{Auth} = SO_{Visited} & : \text{without home authentication} \end{cases} \tag{4.8}$$

As detailed before, we distinguish between uplink and downlink messages where

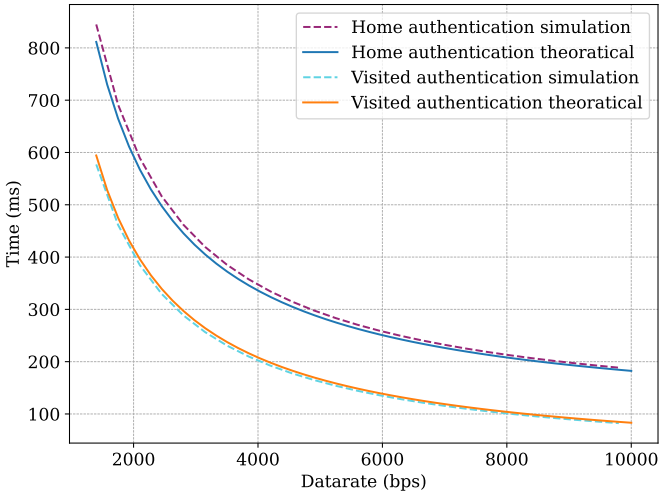


Figure 4.4: Validation of the results.

uplink messages are routed through N GWs to the serving LoRaMAG, and downlink messages are routed by the LoRaMAG through one GW. SO_{Home} and SO_{Visited} are shown in 4.9 and 4.10, and SO_{Auth} is calculated for several values of N with home authentication sub-phase in Table 4.2. We note that the main overhead is due to SO_{Home} which is executed sporadically in the extended authentication scheme. Otherwise, SO_{Visited} exists only and is considered in the acceptable overhead range. In addition, the application data sent in the RtrSol message is not considered part of the signaling overhead since it is not used for signaling and it is the data intended to be exchanged with the AS.

$$SO_{Home} = (2N+12)L_{ID} + (N+7)L_T + (N+13)L_H = 48 * N + 520\ [Bytes] \quad (4.9)$$

$$SO_{Visited} = (N+6)L_{ID} + (N+1)(L_T + L_H) + L_{HNP} = 44 * N + 80\ [Bytes] \quad (4.10)$$

Table 4.2: Signaling overhead of the extended authentication scheme.

N	**SO_{Home}**	**SO_{Visited}**	**SO_{Auth}**
2	616	168	784
3	664	212	876
4	712	256	968
5	760	300	1060

4.3.3 LPWAN compatibility

Since this solution is designed for LPWAN technologies, we evaluate it according to the main LPWAN constraints in order to show how this solution is compatible and may be deployed in LPWAN environments. We consider LoRaWAN as a direct LPWAN technology:

✓ **Use policy:** it limits the number of messages and the airtime for uplink and downlink transmission. The fair use policy of LoRaWAN limits the uplink airtime to 30 seconds per 24 hours, and the downlink transmissions to 10 messages per 24 hours. In our mobility solution, the MN sends a roaming authentication request message in case of inter-domain mobility, and a RtrSol message in case of intra-domain mobility. The first message represents approximately half of the home authentication sub-phase which lasts for less than one second in the second data rate sub-range, thus, this first message will last half of a second approximately. The RtrSol message represents approximately half of the visited authentication sub-phase which lasts for less than 600 ms in the second data rate sub-range, thus, the RtrSol message will last for less than 300 ms. In some cases, the RtrSol message can carry application data as detailed before, thus, the time needed for this message is not considered lost. Regarding downlink transmission, our mobility solution requires a necessary downlink message in home authentication sub-phase, and a necessary downlink message in visited authentication sub-phase. In conclusion, the home authentication sub-phase, executed infrequently, requires less than half second uplink transmission and one downlink message, and the visited authentication sub-phase requires less than 300 ms uplink transmission that may carry uplink data and one downlink message, which is considered appropriate for fair use policy.

✓ **Payload length:** since we are dealing with LPWAN technologies having short payload length, the payload length of signaling messages exchanged during the mobility solution and the messages containing application data after the link establishment with the network should not exceed the allowed payload length. In the extended authentication scheme specified for LoRaWAN technology, the longest message is the roaming authentication response message in the home authentication sub-phase. This message has a total length of 80 Bytes. As shown in Section 2.1.2, three payload lengths are allowed according to the SF and BW used which are 51, 115, and 222 Bytes. Thus, our extended authentication scheme can be deployed if the allowed payload length is 115 or 222 Bytes which requires a SF less than or equal to 9 for a BW of 125 kHz. Regarding the messages containing application data, they are encapsulated in an IPv6 packet with a compressed header using SCHC algorithm before being transmitted in LoRaWAN message to fit the allowed payload length as detailed before.

✓ **Storage requirement**: the device equipped with LPWAN technologies are characterized by their small storage. The storage needed by a device employing our improved mobility solution is divided into long-term storage and run-time storage. The long-term storage includes ID_i, and half keys X_i and Y_i, which is equal to 68 Bytes. The run-time storage includes the K_i, vK_i, vX_i, vY_i, and ID_{vAuS} which is equal to 136 Bytes. The overall storage needed by the improved mobility solution is 204 Bytes which is considered acceptable for an LPWAN device, for example, an LA66 LoRaWAN shield [128] has a storage of 64 Kilobytes, thus the storage requirement is effortlessly met.

4.4 Security evaluation

We prove the security of the improved solution through a security analysis according to several security issues and using AVISPA software since we are proposing a secure mobility solution for LPWAN technologies.

4.4.1 Security analysis

We evaluate the security of our improved solution according to the common security requirements and mobility-related security issues presented in Section 2.5.2. Several security features are retained from the previous solution which are the confidentiality, message integrity, key freshness, old address control prevention, replay attack resistance, and context alteration prevention. However, other security features are improved as described below:

- Device authentication: the extended authentication scheme aims to provide secure access when the MN moves between different domains, thus it can be identified and authenticated in case of intra-domain and inter-domain mobility.
- Error message attack: the mobility solution follows a determined signaling message flow where the procedures executed during the mobility scenario resists this type of attack. For example, LoRaWAN join procedure protects each signaling message by a MIC field, and the extended authentication scheme differentiates between the home authentication and visited authentication subphases and where each one should be executed, thus, this solution resists this attack.
- Availability and false handover request: the handoff procedure of PMIPv6 determines a certain timer to de-register the MN from the home or visited domain after sending the DeReg-PBU message. After that, the MN should attach with the visited domain that communicates with the home domain during the authentication scheme. Thus, a MN trying to send a false handover request can be detected by the corresponding LMA or AuS which ensures also network availability.
- Mutual authentication and spoofing signaling message: the exchanged signaling messages between the MN and the network entities are integrity protected using the MIC field. MIC_1 and MIC_2 use hash key K_i which is only known by the MN and hAuS, as well, MIC_3 and MIC_4 use hash key vK_i which is only known to the MN, vAuS and vLoRaMAG which are the concerned entities to use it. Thus, an attacker cannot modify the content of these messages without being detected and the corresponding entities authenticate each other based on the hash key used.
- Address squatting and spoofing: during the MN authentication with the visited domain, vLoRaMAG sends the corresponding HNPs to the MN which configures its network interface accordingly. The network interface configuration is performed according to the PMIPv6 specifications which are based on IPv6. The MN can use SLAAC to configure the network interface which tests the generated address based on the received HNP to check for address

duplication. For that, an attacker cannot use the same MN address, thus, address squatting and spoofing are not possible.

4.4.2 AVISPA evaluation

In the same way, we used AVISPA to validate the security of the extended authentication scheme which is implemented using HLPSL. In Figure 4.5, we show the last part of the implementation containing the environment and the goals intended. In the environment, we declare five agents that will play the role of MN, vLoRaMAG, vAuS, vLMA and hAuS. In addition, we declare the keys used during the authentication which are the half keys X and Y, a key named SK1 to protect the exchanges between vAuS and vLoRaMAG, and a key named SK2 to protect the exchanges between hAuS and vAuS since these links are considered secure. Moreover, we declare a hash function and the channels used to send and receive messages between the agents. Besides, we declare the protocol identifiers used later in the goals. As a part of the implementation, the intruder knowledge should be given in the environment which is the set of agents and keys accessible by the intruder. In the end, we declare the session that aggregates these parameters in one communication scenario. This session declares the set of agents involved where the operation of each agent is defined in the rest of the implementation.

Regarding the goals intended by the extended authentication scheme, the secrecy goals are the secrecy of the half keys X and Y, the secrecy of the visited half keys vX and vY, the secrecy of hash key K_i, and the secrecy of visited hash key vK_i. The authentication goals are the mutual authentication between the MN and hAuS based on K_i, and the mutual authentication between the MN and vLoRaMAG based on vK_i, as defined in the rest of the implementation.

After running AVISPA for the implemented extended authentication scheme, the output proves that it is safe as shown in Figure 4.6. The implementation source codes can be found in [126].

4.5 Comparison with related work

To prove the improvements made by our solution over related work presented in Section 2.6, we compare the main mobility and security features provided by each solution.

4.5.1 Comparison of mobility features

Several properties seem to be important when comparing the mobility solutions where each property makes a solution more suitable to be deployed in a certain operating environment. For that, we compare the mobility solutions according to the following properties as summarized in Table 4.3:

- Technology: the subset of technologies that can be served by the mobility solution.
- Protocols: the set of protocols used to build the solution.

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role enviroment()

        def=

                const
                        mn,vmag,vaus,haus,vlma : agent,
                        h : hash_func,
                        sk1,sk2,x,y : symmetric_key,
                        snd,rcv : channel(dy),

                        sec_sk1, sec_sk2, sec_x, sec_y, sec_hk, sec_vx, sec_vhk, sec_vy : protocol_id,
                        auth_haus_mn, auth_mn_haus, auth_vmag_mn, auth_mn_vmag : protocol_id

                intruder_knowledge = {mn,vmag,vaus,haus,vlma,h,i}

                composition
                        session(mn,vmag,vaus,haus,vlma,sk1,sk2,x,y,h,snd,rcv)

end role

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

goal
        secrecy_of sec_x
        secrecy_of sec_y
        secrecy_of sec_hk
        secrecy_of sec_vx
        secrecy_of sec_vy
        secrecy_of sec_vhk

        authentication_on auth_haus_mn
        authentication_on auth_mn_haus
        authentication_on auth_vmag_mn
        authentication_on auth_mn_vmag

end goal

enviroment()

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

Figure 4.5: HLPSL implementation of inter-domain authentication.

- Model type: either the solution is network-based or host-based. A network-based solution reduces the number of operations that should be performed by the device, while a host-based solution requires more operations by the device.
- Mobility type: either the solution is an intra-domain or inter-domain mobility.
- Handoff category: which means how the solution acts to manage mobility. A reactive solution means that the link release and re-establishment are executed at the time of device mobility, while a proactive solution prepares the new link before device mobility leading to a faster but heavier solution.
- Additional entities: these are the entities that should be added to the network to implement the solution.
- Data rate range: used during the simulation or the testbed to evaluate the solution.
- Handoff delay and signaling overhead.

In [45, 46], the mobility solutions are designed to serve IoT networks in general, which means that the LPWAN constraints are not taken into consideration when designing the solution, which are considered tighter than IoT constraints. Moreover, the considered network architecture does not necessarily have a star-of-star topology as in [46] which is based on three layers. In [49, 50], the mobility solutions are designed especially to work with LoRaWAN technology, thus, the LoRaWAN

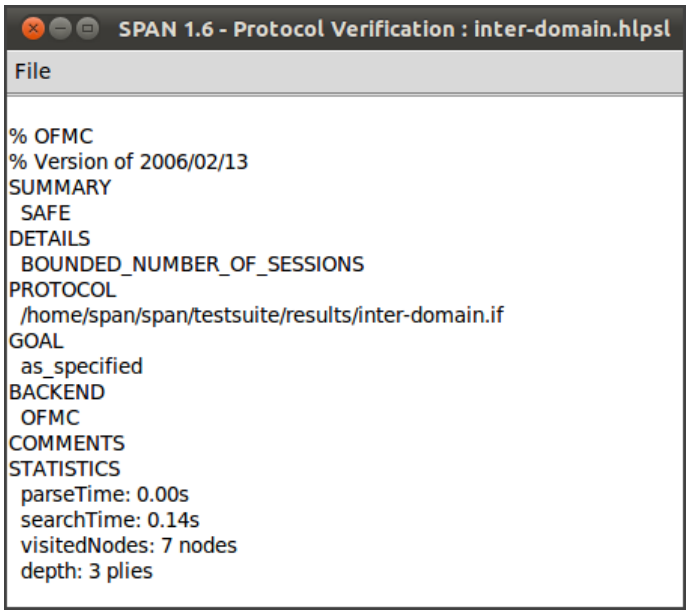


Figure 4.6: Security evaluation using AVISPA.

constraints are taken into consideration, however, these solutions do not support heterogeneous mobility since only LoRaWAN technology is considered and can be served, and a mobility using another link layer technology may fail. In [47, 48] and our improved solution, the mobility solutions consider that a device may support several LPWAN technologies like LoRaWAN and NB-IoT, thus, the mobility solutions are designed to meet the LPWAN constraints and support heterogeneous mobility.

In [45], the mobility solution employs FPMIPv6 which provides fast mobility management, i.e., reduced handoff delay, and employs MIH framework, thus this solution supports heterogeneous mobility. In [46], the mobility solution uses DTLS protocol customized with a communication protocol to achieve a secure solution, and the network is divided virtually to three layers to manage the mobility efficiently using the specified communication protocol. In [47, 48], the mobility solutions employ MIPv6 and a variant of SCHC algorithm, in addition, [48] uses the MIH framework to achieve seamless and heterogeneous mobility. However, using MIPv6 and MIH at the same time for an LPWAN device is not recommended due to LPWAN limitations to support such protocols. Regarding [49, 50], the mobility solutions are based on distributed systems where [49] uses blockchain smart contracts and [50] uses distributed servers to achieve mobility. Our improved solution is based on PMIPv6 as a network layer mobility management protocol assisted with SCHC algorithm to solve the IPv6 overhead drawback.

Regarding the model type, [45, 46, 48–50] and our improved solution are network-based mobility solutions which means that a reduced number of operations is performed by the device. For example, our solution, using PMIPv6, eliminates the need of performing MIPv6 binding update procedure by the device and makes this procedure a responsibility of another entity, and [45] uses FMIPv6 as a mobility protocol which is considered a network-based protocol. However, [47] is the only work

considered a host-based mobility solution from the related work since it uses MIPv6, thus, the device contribute directly to the mobility procedure, and [48] can operate as a host-based or network-based solution according to the entity that initiates the mobility procedure since the authors propose to use MIH framework.

The type of mobility that can be managed is an important feature investigated by any network operator before deploying a mobility solution. [45, 46, 48, 50] and our improved solution provide inter-domain mobility management, thus, a device moving outside its home domain will still be able to establish a connection through the visited domain to communicate with the CN. However, [47, 49] ensure only intra-domain mobility where a device moving outside its home domain is not guaranteed to have a connection with the AS through the visited domain. In this case, the device may use the technology-specific mobility management procedure to establish a connection, however, if this procedure fails or the technology does not have a mobility management procedure, the device cannot establish a connection from outside its home domain.

In [45, 47, 49, 50] and our improved solution, the mobility solutions belong to reactive handoff category since the mobility procedure starts after the device movement. In [45], the authors use the reactive version of FMIPv6 as a part of mobility solution, and [47] uses MIPv6 assisted with MSCHC, thus, no pro-activity is implemented in these solutions. In addition, [49, 50] are based on distributed systems that necessitate the communications with the blockchain smart contracts or the DS after the device mobility to perform the mobility solution. In our improved solution also, we do not add any proactive procedure that allows the network to proactively manage the device mobility. On the other hand, [46] uses the second layer called the fog layer to achieve a proactive handoff solution, where the device notifies the network about its movement and establish a new connection before its mobility. Likewise, [48] uses MIH framework with a mobility management server to achieve proactive handoff. A proactive handoff contributes mainly in reducing the handoff delay, however, it necessitates additional overhead for signaling messages that should be exchanged before the mobility that may not happen. In addition, a handoff delay of less than a second in LPWAN is acceptable since LPWAN applications are time-tolerant and do not belong to real-time applications category, thus, we prefer to reduce the signaling overhead using a reactive handoff.

Regarding the handoff delay, [45] attains a latency between 150 ms and 470 ms using a data rate range between 4 Mbps and 8 Mbps since the solution considers common IoT networks which may have such data rate range. Likewise, a handoff delay of 2.8 ms is attained using a data rate of 20 Mbps in [46]. These delays are considered very low, however, the data rate range used cannot be achieved using LPWAN technologies. For LPWAN mobility solutions in [47–50] and our improved solution, the considered data rate range is that of LPWAN technologies, which is between 250 bps and 21.9 kbps for LoRaWAN, and can reach 66 kbps for NB-IoT. In [47], the use of MSCHC and MIPv6 with route optimization for packets after the handoff leads to a high handoff delay of 7.41 s because of the high number of signaling messages used. This is optimized in [48] to reach a handoff delay of about 2.6 seconds using the proactive handoff assisted using the mobility management server, however, this latency is still considered high. In [49, 50], the considered

technology is LoRaWAN, and the proposed solutions do not involve an additional handoff delay to that of LoRaWAN, however, the latency in [49] is caused by the time needed to verify the smart contract transaction, and in [50], the latency is the time needed to build the database table using the database service. In our improved solution, we achieve an authentication delay of less than 1 second using a data rate range between 1.4 kbps and 10 kbps. This delay is accumulated with PMIPv6 handoff procedure delay and link layer attachment delay which are in order of 500 ms [129], thus, the handoff delay will be less than 1.5 second. Thus, we attain competitive results compared to [45, 46] which use a higher data rate range, and far better results compared to [47, 48] which use the same data rate range.

In terms of signaling overhead, [45] has an overhead of 10000 Bytes for each device handoff due to the use of MIH framework which necessitates a lot of signaling. In [46], the signaling overhead is about 1190 Bytes which is less than the overhead in [45]. In our improved solution, the signaling overhead of the authentication scheme is in the range of 784 — 1060 Bytes in case of home authentication sub-phase execution, and in the range of 168 — 300 Bytes if it is not executed. Although only the signaling overhead of the authentication scheme is calculated in our solution, it shows that our solution provides good performance compared to related work. This also proves the avoidance of employing a heavy framework like MIH framework in our solution and replacing it with a network-based mobility protocol.

As a result, our improved solution is the best compared to related work to be deployed in LPWAN environments due to the type of mobility that can be managed, the light model type, the handoff category, and the performance efficiency using the LPWAN data rate range.

4.5.2 Comparison of security features

Since security is a crucial requirement of any mobility solution that may be deployed by a network operator, we compare the security features provided by each mobility solution in the related work with our improved solution as shown in Table 4.4. The security features evaluated are already presented in Section 2.5.2.

In [47, 48, 50], the security aspect is not considered during the design of mobility solutions, thus, they do not provide any security feature.

In [45], the security was the main concern to be achieved by the mobility solution. The handoff procedure consists mainly of an authentication scheme to provide device authentication with the PMIPv6 domain. Moreover, the signaling message exchanged are protected using a MIC field that guarantees their integrity, ensures mutual authentication between the device and the network entities, prevents the device address from being spoofed, and avoids error message attack. In addition, this solution is based on FPMIPv6 protocol which handles device addresses and prevents them from squatting or being used after release. False handover request is handled also by PMIPv6 in the same way described before. Moreover, a sequence number is used for the key generation which is modified or incremented after each handoff, thus, key freshness is guaranteed and an old key cannot be reused to break the authentication. Hence, this solution guarantees a high level of security and provides all the required security features.

Table 4.3: Comparison of mobility features.

#	[45]	[46]	[47]	[48]	[49]	[50]	**Our solution**
Technology	IoT	IoT	LPWAN	LPWAN	LoRaWAN	LoRaWAN	LPWAN
Protocols	FPMIPv6, MIH	DTLS, three-layers	MIPv6, MSCHC	MIPv6, DCHC, MIH	Smart contracts	Distribution servers	PMIPv6, SCHC
Model type	Network-based	Network-based	Host-based	Host/Network - based	Network-based	Network-based	Network-based
Mobility type	Inter-domain	Inter-domain	Intra-domain	Inter-domain	Intra-domain	Inter-domain	Inter-domain
Handoff category	Reactive	Proactive	Reactive	Proactive	Reactive	Reactive	Reactive
Additional entities	PMIPv6 entities	Smart Gateways	No	Mobility server	No	Distribution servers	PMIPv6 entities
Data rate range	4 — 8 Mbps	20 Mbps	250 bps — 10 kbps	250 bps — 10 kbps	LoRaWAN data rates	LoRaWAN data rates	1400 bps — 10 kbps
Handoff latency	150 — 470 ms	2.8 ms	7.41 s	2.6 s	as LoRaWAN	as LoRaWAN	$\leq$ 1.5 s
Signaling overhead	10,000 Bytes	1190 Bytes	*No study is done*				784 — 1060 or 168 — 300 Bytes

In [46] also, the security of the mobility solution is ensured using an authentication scheme executed during the device attachment. This authentication scheme ensures end-to-end security between the device and the end user. This is followed by a key generation process to protect the exchanged data. Thus, confidentiality, integrity, device authentication and mutual authentication security features are provided by this solution. In addition, spoofing signaling messages and error message attack are not possible due to the protection of signaling messages using digital signatures. Address squatting, spoofing, old address control, and false handover requests are prevented by the use of DTLS protocol and session tickets which conserve device information that should be used during the authentication like the device address. Moreover, key freshness feature is provided where session keys are derived after the authentication success. Hence, this solution is secure and provides directly an end-to-end secure communication.

In [49], several security features are missing although the solution is based on blockchain smart contracts. The security features provided are the integrity, device authentication, error message attack and spoofing signaling prevention since a smart contract is saved on the distributed ledger which cannot be falsified, and the device is authenticated after getting its home network information from the smart contract. However, confidentiality is not guaranteed since the device information are saved in plain text in the smart contract which can be accessed by anyone. In addition, address squatting, spoofing, old address control, and mutual authentication cannot be ensured since an attacker can add altered information for the same device on the smart contract where no protection scheme is used to prevent such a scenario.

Consequently, [45, 46] and our improved solution ensures the security features required to deploy a mobility solution, and [49] ensures partially these features. However, our solution is more suitable for LPWAN technologies because of the mobility features provided and the optimal performance achieved with low data rate range which cannot be achieved using [45, 46] as mobility solutions.

Table 4.4: Comparison of security features.

	[45]	[46]	[47, 48]	[49]	[50]	Our
Confidentiality	✓	✓	Not considered		Not considered	✓
Integrity	✓	✓				✓
Device authentication	✓	✓		✓		✓
Error message attack	✓	✓		✓		✓
False handover request	✓	✓				✓
Spoofing signaling message	✓	✓		✓		✓
Address squatting and spoofing	✓	✓				✓
Old address control	✓	✓				✓
Mutual authentication	✓	✓				✓
Key freshness	✓	✓				✓

4.6 Conclusion

In this chapter, we presented our improved mobility solution assisted with an extended authentication scheme to support inter-domain mobility which was missing in the previous solution. Moreover, we evaluated the performance of this solution according to handoff delay and signaling overhead, and we prove how it satisfies LP-WAN constraints. Besides, we evaluate the solution security according to common and mobility-related security issues, and using AVISPA software. Furthermore, we compare our improved solution with related work to show how our solution provides better performance with additional mobility and security features.

Chapter 5

LoRaWAN Integration Solution Into 5G System

Abstract *— In this chapter, we present our new solution for the integration of LoRaWAN technology into the 5G system making it possible to benefit LoRaWAN and 5G features. We detail first the advantages of such integration and the design principles considered during the conception of our integration solution ensuring the presented advantages. Next, we present the network architecture where we detail the integration of LoRaWAN entities in the 5G core and radio access network, as well as the entities constituting the packet data network. This is followed by the presentation of the new authentication methods based on EAP and called EAP-LoRaWAN-CN and EAP-LoRaWAN-DN to achieve the primary and secondary authentication in the context of LoRaWAN join procedure. Moreover, we detail the adaptation function implemented in the gNB-CU achieving seamless integration, and the mobility management in several mobility scenarios. Later on, we evaluate the security as well as the performance of the proposed solution according to the handoff delay, signaling overhead and storage requirement. We conclude this chapter with a comparison of the performance and the security of our solution with those of related work to prove the efficiency of deploying our solution.*

5.1 Advantages and design principles

In this chapter, we propose an integration solution for LoRaWAN into 5G where the main objective is to leverage the simplicity and cost efficiency of LoRaWAN and the power and scalability features of 5G. Several advantages may be exploited if this integration is done in an efficient way such as the following advantages:

- Quasi-free services: if the RAN is formed by the LoRaWAN RAN, quasi-free services may be provided. This is possible for devices existing within the coverage of a LoRaWAN RAN and implementing LoRaWAN technology, similar to WiFi calling in LTE. Since LoRaWAN uses an unlicensed bandwidth for the communication between the EDs and GWs, the cost of using LoRaWAN is reduced to the cost of deployment of ED and GWs, where the high cost of owning a licensed bandwidth is eliminated. Thus, in case an ED is using an

LPWAN application requiring a small number of transmissions, it can benefit from such integration to send application data through the LoRaWAN RAN rather than sending them over a standard 5G RAN and occupying the licensed bandwidth.

- Highly scalable architecture: although LoRaWAN is characterized by its scalability and high network capacity, the use of a SBA core network is considered even more scalable. A SBA core network consisting of NFs interconnected through interfaces and manageable in a flexible way can achieve higher scalability. Thus, going from a simple LoRaWAN architecture to a SBA while conserving the main LPWAN functions and characteristics will increase LoRaWAN ability to serve mMTC applications.
- Dedicated network functionality: the integration of LoRaWAN into the 5GS makes it possible for LoRaWAN to benefit the existing NFs which were not implemented initially. For example, special algorithms that improve the mobility management like ED tracking and status monitoring may be implemented in the AMF, and others like roaming agreement and data buffering may be implemented in their corresponding NFs. Thus, an integrated LoRaWAN will benefit these implemented functions and exploit them to improve the performance and the QoS provided to the served EDs.

As said before, these advantages are achieved if the integration is done in an efficient way. For that, the following design principles are satisfied during the conception of our solution:

- Compatibility with LoRaWAN and 5G standards: in our solution, this compatibility is achieved at three levels. The first is at the network architecture level where the 5GC is adopted as the reference architecture and the LoRaWAN core network functionalities are divided over the corresponding NFs. The second is at the access procedure level where the LoRaWAN join procedure will be used as the network access procedure with the needed wrappings to be compatible with 5G primary and secondary authentication. The third is at the signaling and control level which are adapted to remain compatible with both standards by the use of an adaptation function.
- Network in network integration: this is related to the integration of NS and JS representing the main LoRaWAN core entities in the 5GC. Several concepts may be used to achieve this integration as the use of a connector entity that connects the LoRaWAN entities with the 5GC, or the use of the 5GC as a bridge network to connect the ED and LoRaWAN core entities. These concepts are simple to implement and can achieve integration, however, the integration will not be efficient as intended. For that, we use a more complex concept for integration that achieves superior performance where the concept used is to divide the functionalities performed by the NS and JS over the 5GC NFs.
- Seamless integration for devices: since the EDs in LoRaWAN have several constraints in terms of processing power and battery lifetime, we adopt a solution that avoids any additional procedures to be executed by the ED. Thus, the procedures involving the ED are the LoRaWAN procedures like the join procedure and data rate adaptation procedure. This is achieved thanks

to the adaptation function responsible to provide translation of the signaling commands.

- Dedicated network slice: to complete the network in network integration design principle, we propose to assign a new network slice that allows to identify the required procedures in each NFs achieving the specified integration process.

5.2 Proposed solution

In this section, we present our proposed solution to integrate LoRaWAN into 5GS. We first describe the network architecture consisting of the RAN and the 5GC. After that, we show the derivation scheme of the unique ED identifier in 5Gs from the unique identifier of the ED in LoRaWAN technology. Then we present our new authentication methods based on EAP to achieve primary and secondary authentication. After that, we detail the gNB-CU adaptation function used to provide seamless integration for LoRaWAN RAN into 5GC. Finally, we show how mobility is managed in several mobility scenarios.

5.2.1 Network architecture

Since we are integrating LoRaWAN into 5GS, the adopted network architecture is that of 5GS consisting of the RAN and the 5GC as shown in Figure 5.1. For that, the integration of LoRaWAN architecture into 5GS architecture is mainly done at two levels. The first is integrating LoRaWAN core network entities in the 5GC. The second is to make seamless integration of LoRaWAN RAN entities with the 5GC. Furthermore, although the PDN is not considered a part of the 5GS, we present the principal entities involved during a communication scenario.

5.2.1.1 Network server and join server integration into 5GC

The NS and JS functions are distributed over 5GC NFs, where the set of these NFs is identified using a new S-NSSAI named S-NSSAI$_{\text{LoRaWAN}}$ which represents a separate network slice for LoRaWAN. In the following, we depict the operation of each 5GC NF in the LoRaWAN network slice.

- UDM: in LoRaWAN, the ED and JS pre-share NwkKey and AppKey which are used to derive NwkSKeys and AppSKey. In our solution, we propose that the ED and UDM pre-share the long-term secret K which is saved in the ED USIM and UDM database respectively. The ED should possess a USIM since it is deployed in a 5G network. K will be used to derive K_{AUSF} which will be equivalent to NwkKey. We note that in LoRaWAN, NwkKey is static (constant over time) whereas it is dynamic (changes over time) in our solution, which improves the security level. Hence, the UDM should hold a profile for each registered ED including: (i) SUPI equivalent to DevEUI to fulfill 5G specifications (described later) (ii) long-term secret key K (iii) ED policy (iv) authentication type set to EAP-LoRaWAN-CN (described later) (v) S-NSSAI set to S-NSSAI$_{\text{LoRaWAN}}$.

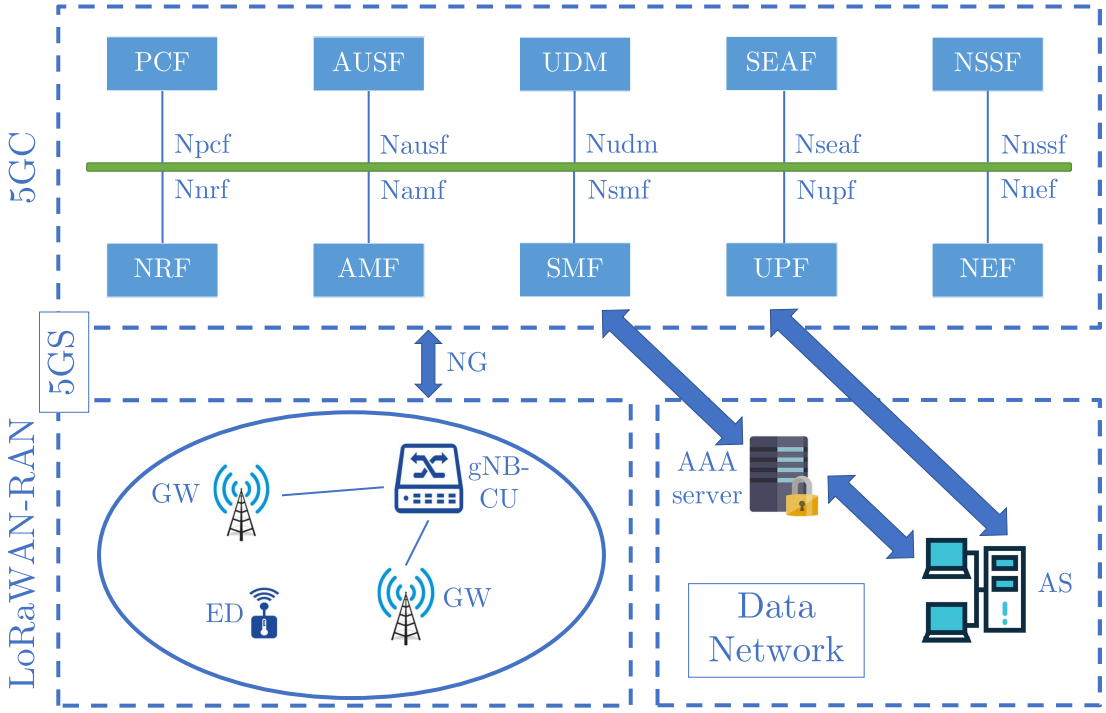


Figure 5.1: Proposed network architecture for integration.

- AUSF: gets K_{AUSF} and ED profile from UDM, then performs the primary authentication and key derivation based on EAP-LoRaWAN-CN authentication. In case of roaming, AUSF resides in the home network domain.
- SEAF: has the main role in the primary authentication in case of roaming, thus it resides in the visited network domain. SEAF gets K_{SEAF} derived by AUSF based on 5G specifications which acts as the domain anchor key and is used to derive K_{AMF}.
- AMF: responsible for ED access and mobility management in the serving network. In our solution, we integrate LoRaWAN into 5G network, where ED realizes only LoRaWAN MAC commands, while a communication between an AMF/SMF and an ED is achieved through NAS-MM/NAS-SM in 5G. Therefore, NAS-MM/NAS-SM messages sent from AMF/SMF to ED should be translated into LoRaWAN MAC commands. The translation mechanism will be performed by the gNB-CU adaptation function (described later).
- SMF: responsible for session management and contributes to the secondary authentication. In LoRaWAN, the ED establishes a session with the AS and protects the application data using AppSKey. The LoRaWAN session context consists of the AppSKey, Uplink Frame Counter (FCntUp) and Application Uplink Frame Counter (AFCntUp) saved in the NS. In our solution, upon a session establishment with the 5G network, the SMF should store the LoRaWAN session context excluding the AppSKey. This key will be delivered by the AAA server to the AS after the secondary authentication using EAP-LoRaWAN-DN. Moreover, the SMF will assign an IP address and control a virtual PDU session established with the gNB-CU. The latter will handle the

virtual PDU session instead of ED to maintain 5G compatibility through the adaptation function.

- UPF: in LoRaWAN, the routing is performed by the NS based on the ED DevAddr assigned after the session establishment. In our solution, the ED is assigned an IP address that is mapped to its DevAddr in the gNB-CU. When the ED sends uplink data, the gNB-CU gets its IP address based on DevAddr and then sends it to UPF through the 5GC. Finally, UPF routes the data to the ultimate destination according to ED policy.

5.2.1.2 Gateways integration into RAN

In 5G, the RAN consists of several gNBs, which are formed by gNB-DUs connected to gNB-CU in case of C-RAN. In our solution, we adopt C-RAN architecture for the RAN, where a LoRaWAN GW acts as gNB-DU and maintains its LoRaWAN functions. In addition, gNB-CU will be responsible for LoRaWAN integration into 5G through the adaptation function described in Section 5.2.4.

5.2.1.3 Packet data network

The PDN consists of the entities that are independent of the 5GS and is not controlled by the 5G network operator as shown in Figure 5.1. A 5G network may communicate with several PDNs where this communication is managed by the SMF holding the session information. The main entities in a PDN are the following:

- AAA server: its role is to perform the secondary authentication to achieve secure access from ED to AS. AAA server has a database containing DevEUI with the correspondent AppKey. AAA server uses EAP-LoRaWAN-DN during secondary authentication and then derives AppSKey according to LoRaWAN key derivation scheme. After successful secondary authentication, AppSKey is delivered to AS.
- AS: responsible for the processing of data sent by ED. These data are protected using AppSKey delivered by AAA server to AS after the secondary authentication.

5.2.2 SUCI derivation

A USIM stores the SUPI that should not be exchanged in plain text on the air interface to conserve user anonymity. Thus, 5G standards propose to send SUCI instead of SUPI. SUCI contains SUPI encrypted in addition to several fields. In our solution, we consider that SUPI is equivalent to DevEUI, and used to derive SUCI as shown in Figure 5.2 where:

- Home Network Identifier: set to the identifier of the LoRaWAN network where the ED is initially registered.
- Protection Scheme, Home Network Public Key ID, Scheme Output: since the DevEUI is sent in plain text in LoRaWAN, we can discard the protection and the public key where DevEUI is used as the scheme output. Note that the proposed fields could be adapted according to any future modification.

SUCI Type	Home Network Identifier	Routing Indicator	Protection Scheme ID	Home Network Public Key ID	Scheme Output
LoRaWAN	LoRaWAN NetID	∀	0x00	0x00	DevEUI

Figure 5.2: Derivation of SUCI from DevEUI.

For example, if LoRaWAN modifies the protocol or 5G forces the protection scheme, these fields will be modified accordingly.

5.2.3 EAP-LoRaWAN authentication

Both LoRaWAN and 5G deploy their authentication scheme to guarantee secure access from ED to the network. Nevertheless, integrating LoRaWAN into 5G requires either using one of the 5G authentication methods (5G-AKA, EAP-AKA', EAP-TLS), or inventing a new authentication method considering 5G specifications and LoRaWAN join procedure at the same time.

In our solution, we choose the second approach and we propose two authentication methods based on EAP [91] called LoRaWAN over EAP for Core Network (EAP-LoRaWAN-CN), and LoRaWAN over EAP for Data Network (EAP-LoRaWAN-DN). Since we are working with a LoRaWAN ED, we reduced the number of operations needed by it to still acts as in LoRaWAN. Thus, the ED will only send and receive the join request and join accept messages as in LoRaWAN join procedure, while the rest will be done by the gNB-CU on behalf of ED.

EAP has gained popularity in the last years since it provides a generic authentication framework based on the three-party authentication model [130] using a specific EAP authentication method. This model consists of three main elements:

- Peer: is the device trying to access or authenticate with the authenticator.
- Authenticator: an entity acting as a pass-through element that forwards the messages between the peer and the EAP-server.
- EAP-server: is the entity performing the EAP authentication method with the peer.

Flexibility is an important feature provided by EAP since whenever an authentication method is updated or a new one is added, only the EAP-server needs to be updated. The authenticator should not be modified and still acts as a pass-through element waiting for the authentication success or failure message. This saves a lot of administration effort and trouble in updating a large number of authenticators. EAP does not provide authentication by itself, but provides the mean of negotiation between the peer and the EAP-server. The EAP packet format is shown and detailed in Figure 5.3. The EAP code field identifies the type of EAP message as follows:

- EAP request: messages transporting data from EAP-server to peer.
- EAP response: messages transporting data from peer to EAP-server.
- EAP success: message transporting authentication success.

- EAP failure: message transporting authentication failure.

The EAP identifier is used to match requests to responses, and the EAP message length indicates the length of the entire EAP packet. An EAP packet can consist of one or more EAP data. An EAP data includes data content and data type indicating the type based on a predefined set of data types.

EAP-LoRaWAN-CN is used to achieve the primary authentication between ED and 5GC. The entities involved in this phase are ED, gNB-CU, AMF, SEAF, AUSF, and UDM. EAP-LoRaWAN-CN is inspired by LoRaWAN join procedure, therefore the same parameters are exchanged and the LoRaWAN key derivation process is used to obtain the NwkSKeys. At the same time, we strive to take 5G standards into account.

At the other end, EAP-LoRaWAN-DN is used to achieve the secondary authentication between the ED and PDN. The entities involved in this phase are ED, gNB-CU, SMF, AAA server and AS. Upon the end of this phase, the ED and AS get the AppSKey needed for application data protection.

To start up with the access procedure, the ED sends a LoRaWAN join request containing JoinEUI, DevEUI, DevNonce, MIC_{JR} and MIC_{AAA}. MIC_{JR} is the MIC defined in LoRaWAN join request and used in EAP-LoRaWAN-CN. However, the new MIC_{AAA} is used in EAP-LoRaWAN-DN authentication and calculated as follows:

$$MIC_{AAA} = aes128\_cmac(\mathbf{AppKey},\ MHDR \mid JoinEUI \mid DevEUI \mid DevNonce)$$

This request is received by gNB-DU (LoRaWAN GW) and forwarded to gNB-CU as shown in Figure 5.4.

The primary and secondary authentication using EAP-LoRaWAN-CN and EAP-LoRaWAN-DN are shown in Figure 5.5 and 5.6 respectively.

Primary Authentication.

1. The gNB-CU saves ED join request and derives SUCI as detailed in Section 5.2.2, then sends an authentication request to AMF through N2 interface containing SUCI.
2. The AMF forwards this request to AUSF using Nausf _ UEAuthentication _ AuthenticateRequest service containing also the SNID.
3. The AUSF forwards this request to UDM using Nudm _ UEAuthentication _ GetRequest service.

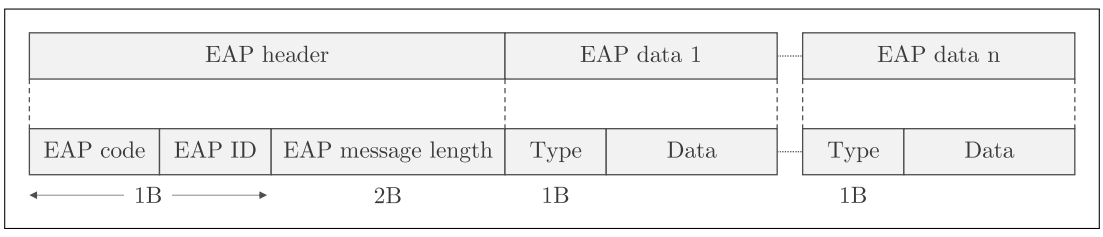


Figure 5.3: EAP packet format.

Figure 5.4: Join request message at the beginning of the access procedure.

4. The UDM gets SUPI from SUCI according to the protection scheme. Then UDM fetches the ED policy and other information saved in its database. Furthermore, UDM derives K_{AUSF} from K according to 5G key derivation scheme.
5. UDM replies to AUSF using Nudm _ UEAuthentication _ GetResponse service with SUPI, SUCI, the authentication type that should be used which is EAP-LoRaWAN-CN, and K_{AUSF} (=NwkKey). In the following, AUSF takes the role of EAP-server, AMF/SEAF takes the role of authenticator and gNB-CU takes the role of peer.
6. The AUSF sends an EAP-REQUEST containing SUCI to gNB-CU using Nausf _ UEAuthentication _ AuthenticateResponse indicating the start of EAP-LoRaWAN-CN authentication.
7. The gNB-CU replies with EAP-RESPONSE consisting of join request parameters sent by ED at the beginning excluding MIC_{AAA}, in addition to a JoinNonce using Nausf _ UEAuthentication _ AuthenticateRequest.
8. The AUSF verifies MIC_{JR} using NwkKey. If MIC_{JR} is valid, the AUSF derives NwkSKeys and K_{AMF}, then the AUSF generates the join accept parameters according to LoRaWAN specifications with the corresponding MIC_{JA}.
9. The AUSF sends the EAP-SUCCESS message to gNB-CU through AMF which is notified of the authentication success using Nausf _ UEAuthentication _ AuthenticateResponse.
10. The AMF gets K_{AMF} then derives K_{NAS} and 5G-GUTI.
11. The NwkSKeys and K_{NAS} are shared with gNB-CU to be able to perform the translation of NAS to LoRaWAN commands.

Secondary Authentication.

1. The gNB-CU sends a PDU session establishment request to AMF containing 5G-GUTI and DevEUI protected using K_{NAS} and encapsulated into NAS-SM.
2. The AMF detects the type of NAS-SM, thus AMF decrypts it and forwards it to SMF using Nsmf _ PDUSession _ CreateRequest.
3. The SMF receives the session establishment request, thus it sends an authentication start flag containing DevEUI to AAA server residing in the PDN. The SMF stores a mapping between 5G-GUTI and DevEUI.
4. The AAA server starts the EAP-LoRaWAN-DN authentication by sending an EAP-REQUEST message to SMF containing the DevEUI. This request is forwarded by the SMF to the corresponding gNB-CU. In the following, AAA

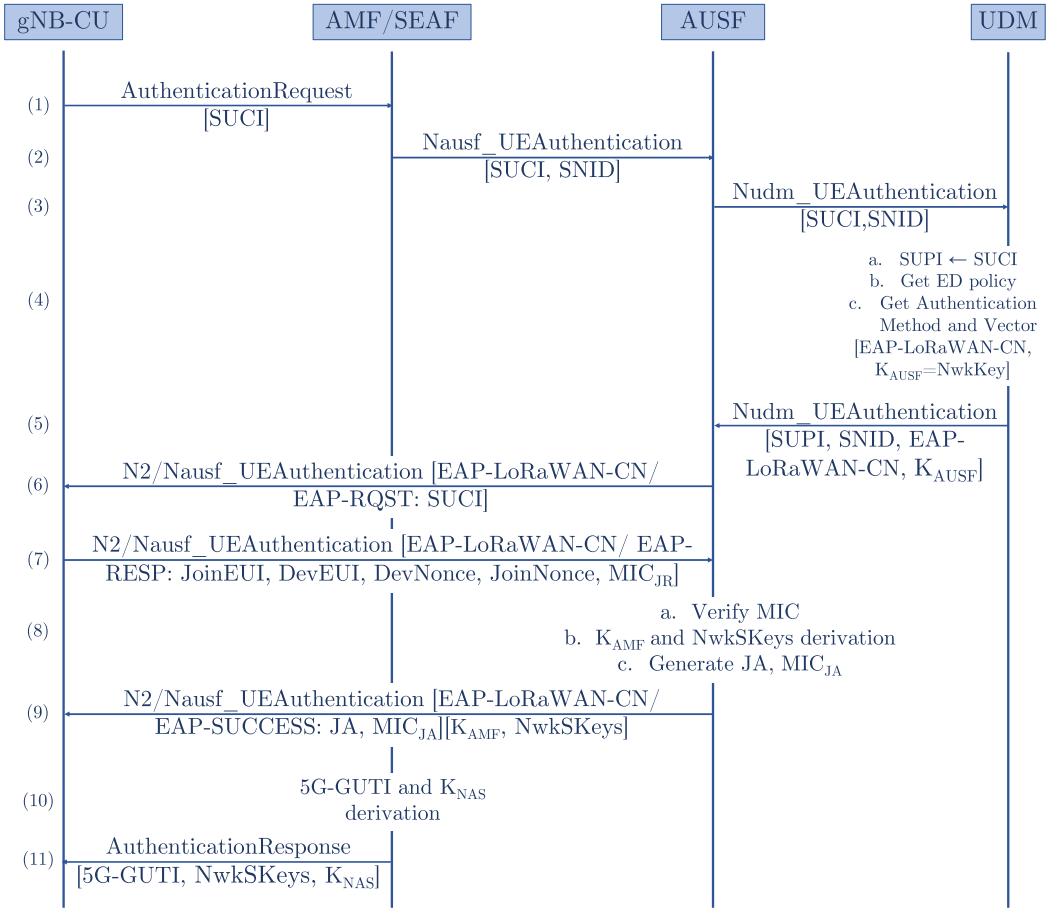


Figure 5.5: Primary authentication using EAP-LoRaWAN-CN.

server takes the role of EAP-server, SMF takes the role of authenticator and gNB-CU takes the role of peer.

5. The gNB-CU sends an EAP-RESPONSE message containing the join request parameters sent by ED at the beginning excluding MIC_{JR} and the saved JoinNonce used to derive the AppSKey.

6. The AAA server verifies MIC_{AAA} using the pre-shared AppKey. If MIC_{AAA} is valid, the AAA server sends an EAP-SUCCESS message which indicates to SMF that the authentication has succeeded.

7. The SMF allocates the necessary session parameters including the IP address and sends an Namf _ Communication _ N1N2MessageTransfer to AMF to setup the uplink/downlink data path.

8. The AMF sends a PDU session establishment accept to gNB-CU with the 5G-GUTI and the other session parameters.

At the end of secondary authentication, the AAA server derives the AppSKey and sends it to AS. Moreover, the gNB-CU replies to the ED with LoRaWAN join accept containing JoinNonce, NetID, DevAddr, DLSettings, RxDelay, optional CFList, and MIC_{JA} as shown in Figure 5.7. The ED derives the NwkSKey and AppSKey, and configures its radio link interface based on the received parameters.

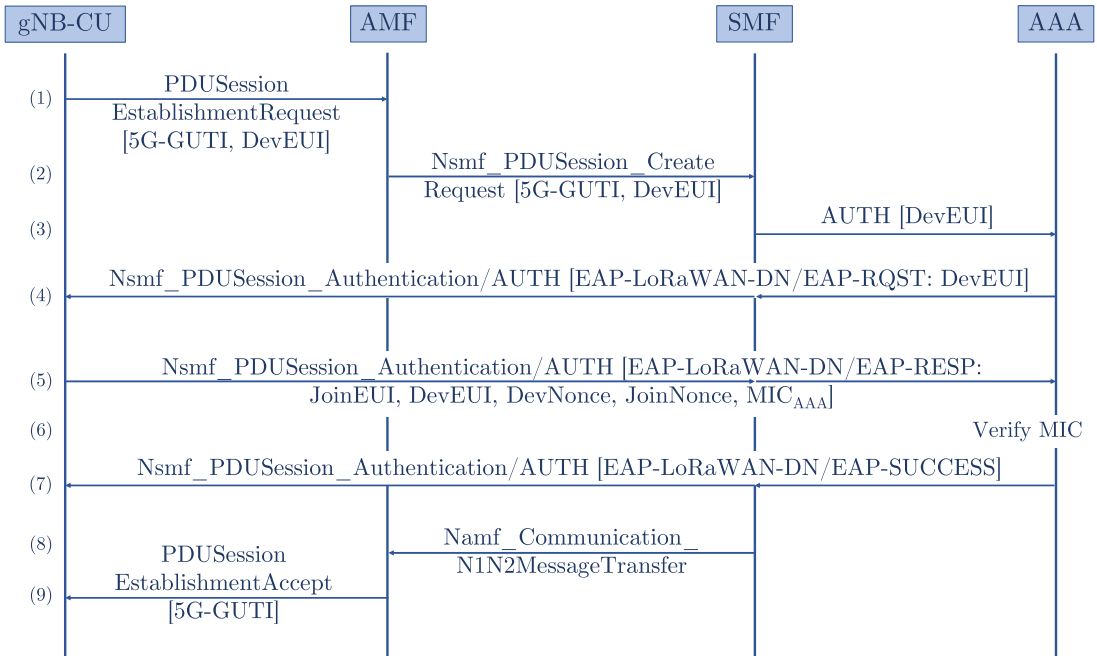


Figure 5.6: Secondary authentication using EAP-LoRaWAN-DN.

Figure 5.7: Join accept message at the end of the access procedure.

In this way, the ED is authenticated with the 5GC and AS, and able to send and receive data securely.

5.2.4 gNB-CU adaptation function

In our solution, the ED physical layer is unchanged, thus LoRa modulation is still used where there is no need to support 5G RATs. Also, the ED link layer is intact, where it should still communicate using LoRaWAN MAC commands with the 5GC substituting the NS. Besides, the control-plane communication between the ED and 5GC is managed through AMF and SMF using NAS-MM and NAS-SM. Therefore, any downlink control-plane message sent from AMF or SMF to ED will not be understood by the ED since it realizes only LoRaWAN MAC commands, and vice versa for uplink LoRaWAN MAC commands. For that, we introduce our new function called the adaptation function implemented in gNB-CU. This function is responsible for:

1. **Translation of NAS-MM/NAS-SM into LoRaWAN MAC commands and vice versa:** the main NAS-MM procedure messages that should be translated are the service request, primary authentication, security mode control,

configuration update, and identification. The first three procedures are part of authentication achieved as explained previously using EAP-LoRaWAN-CN. The translation of the rest procedure messages is as follows:

- Configuration update procedure: this procedure is translated according to the NAS message content into one of the following LoRaWAN commands: LinkCheckReq/Ans, NewChannelReq/Ans, ReKeyInd/Conf, ForceRejoinReq, RejoinParamSetupReq/Ans. The gNB-CU identifies the intended ED using the 5G-GUTI in the NAS message.
- Identification procedure: this procedure is translated into DevStatusReq/Ans LoRaWAN commands, where the AMF asks about the ED identity or status. The ED identity is the DevAddr translated into SUCI or 5G-GUTI in the gNB-CU. The status consists of ED related information such as battery level.

The main NAS-SM procedure messages that should be translated are the session establishment and secondary authentication. These procedures are part of authentication achieved as explained in the previous subsection using EAP-LoRaWAN-DN.

2. **Handling of ED specific procedures:** three NAS procedures are handled by gNB-CU on the ED behalf for two reasons:
   (a) ED is not aware of the 5G parameters.
   (b) ED has battery and power consumption constraints.

   The three procedures are detailed below:

   - Registration Update (RU) procedure: for periodic RU, the gNB-CU launches a timer for each served ED, when the timer elapses, gNB-CU sends a RU message to the AMF on ED behalf. For mobility RU, when the next gNB-CU receives uplink data sent from an ED, it tries to find the last serving gNB-CU (previous gNB-CU). When the next gNB-CU belongs to a tracking area different from the previous gNB-CU tracking area, it sends a mobility RU request to AMF on ED behalf, indicating the change of ED location and its RAP. The ED context is sent from the previous to the next gNB-CU through the Xn or N2 interface.
   - Session modification procedure: since the gNB-CU creates a virtual session for each ED, it is responsible to manage the session where the whole procedure is transparent to the ED. Moreover, the virtual session parameters are quasi-static since the gNB-CU has not the same ED dynamic behavior, thus this procedure is executed rarely. This procedure involves the tuning of parameters such as the maximum data rate and the quality of service.
   - Session release procedure: this procedure comes after the RU procedure. When the ED moves from a previous to the next gNB-CU connected to AMF, it sends a mobility RU to the previous gNB-CU. Thus, the latter should send a session release message to the SMF. Moreover, a new LoRaWAN session context is established through the next gNB-CU and SMF.

3. **Management of the radio links of the connected GWs based on the LoRaWAN protocol:** the gNB-CU is responsible for radio link management which is a pure LoRaWAN process previously performed by the NS. The LoRaWAN MAC commands involved in this context are LinkADRReq/Ans, DutyCycleReq/Ans, RxParamSetupReq/Ans, NewChannelReq/Ans, RxTimingSetupReq/Ans, TxTimingSetupReq/Ans, DIChannelReq/Ans, ADRPara mSetupReq/Ans, DeviceTimeReq/Ans. However, the gNB-DU, which is the GW, still acts as a relay for uplink and downlink messages as in LoRaWAN.

5.2.5 Mobility management

We focus on mobility management for three types of mobility that may occur in 5GS. The main parameters that can be changed in a mobile environment are the following:

- Radio link parameters including data rate, spreading factor, transmission and reception time window, etc.
- Session keys including K_{NAS} and NwkSKeys.
- Virtual PDU session including LoRaWAN session context, mapping between DevAddr and IP address, and other PDU session parameters.

The first type of mobility is the ED movement between two gNB-DU connected to the same gNB-CU, called intra-gNB-CU mobility. In this scenario, the radio link parameters change according to the new gNB-DU. However, the session keys are not modified since K_{NAS} changes whenever gNB-CU changes and NwkSKeys change whenever the ED changes the visited network domain. Moreover, the virtual PDU session is not affected since it is managed by the same gNB-CU. The ED is not required to perform any mobility-related procedure.

The second type of mobility is the ED movement between two gNB-DUs connected to different gNB-CUs, called inter-gNB-CU mobility. In this scenario, the radio link parameters change according to the new gNB-DU. In addition, the virtual PDU session parameters should be sent from the previous to the next gNB-CU and then updated. The session keys are not changed for the same previous reasons. The ED is not required to perform any mobility-related procedure.

The third type of mobility is the ED movement between two gNB-CU connected to different AMFs, called N2-based mobility. A force rejoin request is sent to ED, thus ED starts the join procedure followed by the primary and secondary authentication. In this way, the ED gets the new radio link parameters, the new session keys, and the next gNB-CU holds and manages the new virtual PDU session parameters.

5.3 Performance evaluation

In this section, we evaluate the performance of our solution according to the handoff delay, signaling overhead, and storage requirement.

5.3.1 Handoff delay

T_{HO} represents the time needed for the ED to establish a new link with the new RAN and resume sending application data through this link to the AS. In our solution, the handoff starts when the ED is no longer able to send or receive messages through the current RAP and fetches a new RAP to resume the connection, thus the ED sends a join request message followed by the execution of the primary and secondary authentication using EAP-LoRaWAN-CN and EAP-LoRaWAN-DN. The handoff ends with the reception of the join accept message where the ED gets the necessary parameters to resume the connection and sends application data. Thus, T_{HO} is equal to the sum of the join request delay (T_{JR}), primary authentication delay (T_{PA}), secondary authentication delay (T_{SA}), and join accept delay (T_{JA}) as shown in 5.1.

$$T_{HO} = T_{JR} + T_{PA} + T_{SA} + T_{JA} \tag{5.1}$$

T_{JR} and T_{JA} are the times needed for the join request and join accept messages to be transmitted over the LoRaWAN link. They are dependent directly on the SF and BW used, which determine the data rate used. We remind that the higher the SF, the lower the data rate, thus, the higher the ToA that a receiver should wait to receive a signal sent by the transmitter. Besides, T_{PA} and T_{SA} are dependent mainly on the processing time needed to perform the operations by the NFs involved in the primary and secondary authentication, and on the characteristics of the links connecting the different NFs.

We used NS-3 to simulate the different delays in our solution, thus we create our new module called 'lorawan-5g-integration' implementing the solution. The LoRaWAN module [131] is already created and can be used to test the radio link, however, a 5GC module is not built yet. For that, our module implements the main 5GC NFs including AMF, AUSF, SMF, UDM and UPF, as well as the main PDN entities which are AAA sever and AS. In addition, we implement the gNB-CU to operate as explained in our solution. The implementation source codes can be found in [132].

The simulation scenario is made by an ED trying to enter a LoRaWAN network coverage. Thus it starts the access procedure by sending a join request to the network, then the primary and secondary authentications are achieved as explained before. Therefore, the link between the ED and the RAN is a LoRaWAN radio link, and the RAN is connected to 5GC through NG interface. The metrics evaluated in the simulation are T_{JR}, T_{PA}, T_{SA}, and T_{JA}, which consist T_{HO}. In our simulation, the BW used is equal to 125 kHz (supported in Europe and USA). We evaluate the performance of our solution according to LoRaWAN SF ranging from 7 to 12 as shown in Figure 5.8. For a SF value of 10, 11 or 12, the dominant delays are T_{JR} and T_{JA} since the data rate is low, while T_{PA} and T_{SA} have minor contribution in T_{HO}. For these values of SF, the T_{HO} varies between 1182 ms and 3570 ms. However, for a SF value of 7, 8 or 9, T_{JR} and T_{JA} become low and comparable to T_{PA} and T_{SA}, where T_{HO} decreases to the range between 416 and 730 ms.

In Figure 5.8, we compare also our solution to LoRaWAN join procedure on T_{HO}. As shown in the figure, our solution and the join procedure lead approximately to

the same delay since we use the same number of messages on the radio link with a minor modification which is MIC_{AAA} that increases T_{HO} slightly.

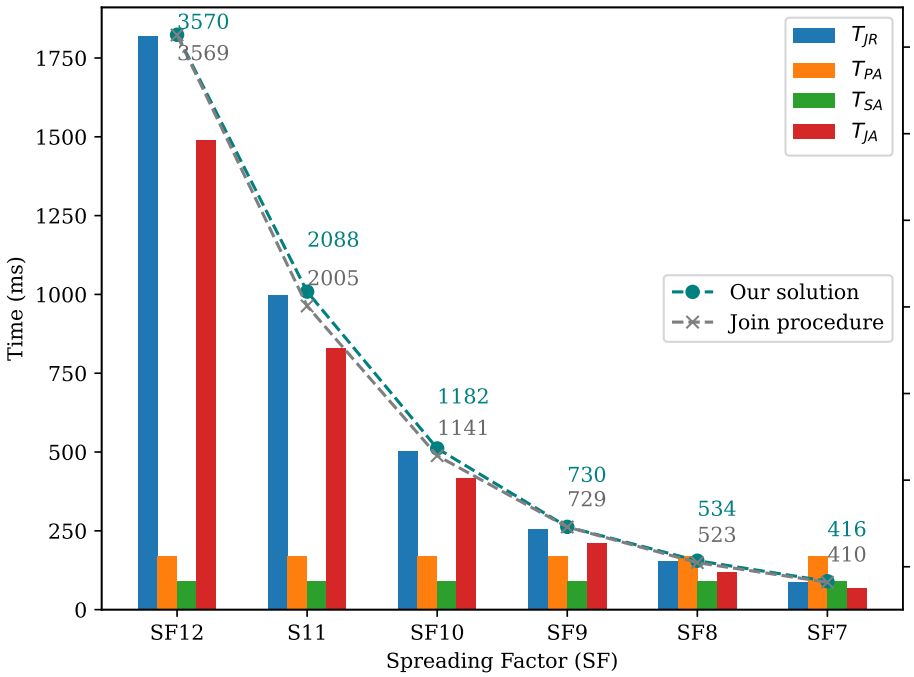


Figure 5.8: Variation of evaluated metrics in function of LoRaWAN SF.

5.3.2 Signaling overhead

An important metric that should be evaluated is the signaling overhead caused by the use of signaling messages exchanged between ED, gNB-CU and NFs. We consider that the length of these messages (in Bytes) represents the signaling overhead. The length of each message used in LoRaWAN join procedure, 5G EAP-AKA', EAP-LoRaWAN-CN, and EAP-LoRaWAN-DN is calculated separately and shown in Table 5.1.

We distinguish between two types of signaling messages. The first type represents the signaling messages sent over a radio link which can be a LoRaWAN radio link in case of LoRaWAN RAN. The second type represents the signaling messages sent over a direct link, like the signaling messages between NS and JS in LoRaWAN or between 5G NFs. For each access procedure, the signaling overhead is as follows:

- The signaling overhead of LoRaWAN join procedure is equal to 548 Bytes where 38 Bytes are due to radio link messages (join request and join accept), thus 510 Bytes are exchanged over a direct link.
- The signaling overhead of 5G EAP-AKA' is equal to 362 Bytes where 28 Bytes are due to radio link messages (M1' and M10'). We note that signaling overhead of 5G EA-AKA' should be accumulated with a secondary authentication signaling overhead in order to compare with other signaling overheads.
- In our solution, the signaling overhead of EAP-LoRaWAN-CN is equal to 362 Bytes and the signaling overhead of EAP-LoRaWAN-DN is equal to 236

Table 5.1: Length of signaling messages of access procedures

Method	Message	Description	Length
LoRaWAN join procedure	JR	Join Request (ED-NS)	22
	HNSR	Home NS Request	8
	HNSA	Home NS Answer	3
	PR	Profile Request	8
	PA	Profile Answer	50
	HR	Handover Request	156
	JRq	Join Request (NS-JS)	62
	JAn	Join Answer (JS-NS)	64
	HA	Handover Answer	139
	JA	Join Accept (NS-ED)	16
	KD	AppSKey Delivery	20
	Total		**548**
5G EAP-AKA'	M1'	Authentication Request	17
	M2'	Nausf _ UEAuthentication _ Authenticate Request	18
	M3'	Nudm _ UEAuthentication _ Get Request	22
	M4'	Nudm _ UEAuthentication _ Get Response	88
	M5'	Nausf _ UEAuthentication _ Authenticate Response	44
	M6'	EAP-REQUEST	43
	M7'	EAP-RESPONSE	39
	M8'	Nausf _ UEAuthentication _ Authenticate Request	36
	M9'	EAP-SUCCESS	44
	M10'	Authentication Response	11
	Total		**362**
EAP-LoRaWAN-CN	M1	Authentication Request	17
	M2	Nausf _ UEAuthentication _ Authenticate Request	18
	M3	Nudm _ UEAuthentication _ Get Request	22
	M4	Nudm _ UEAuthentication _ Get Response	44
	M5	Nausf _ UEAuthentication _ Authenticate Response	36
	M6	EAP-REQUEST	39
	M7	EAP-RESPONSE	47
	M8	Nausf _ UEAuthentication _ Authenticate Request	36
	M9	EAP-SUCCESS	60
	M10	Authentication Response	43
	Total		**362**
EAP-LoRaWAN-DN	M11	PDU Session Establishment Request	23
	M12	Nsmf _ PDUSession _ Create Request	23
	M13	AUTH (SMF-AAA)	8
	M14	EAP-REQUEST	12
	M15	Nsmf _ PDUSession _ Authentication Command	23
	M16	Nsmf _ PDUSession _ Authentication Command	55
	M17	EAP-RESPONSE	44
	M18	EAP-SUCCESS	4
	M19	Nsmf _ PDUSession _ Authentication Complete	15
	M20	Namf _ Communication _ N1N2Message Transfer	10
	M21	PDU Session Establishment Accept	19
	Total		**236**

Bytes, with a total of 598 Bytes, where any of these bytes is due to radio link. However, join request and join accept messages are sent before and after EAP-LoRaWAN-CN and EAP-LoRaWAN-DN messages. The length of join

request and join accept messages are 42 Bytes which is equal to 38 Bytes (as in LoRaWAN join procedure) plus 4 Bytes for MIC_{AAA}.

Several factors, like ED movement at high velocity and multi-path fading, lead to hardness on the radio link resulting in packet loss. Thus, the probability of failure (p) of a radio link leads to additional signaling overhead since re-transmission is needed to recover lost data. The signaling overhead for each access procedure attempt per ED is shown in Table 5.2 and represented in Figure 5.9.

Table 5.2: Signaling overhead of access procedures.

Access procedure	**Signaling overhead**
LoRaWAN join procedure	$510 + \frac{38}{1-p}$
5G primary and secondary authentication	$598 + \frac{28}{1-p}$
Our solution	$598 + \frac{42}{1-p}$

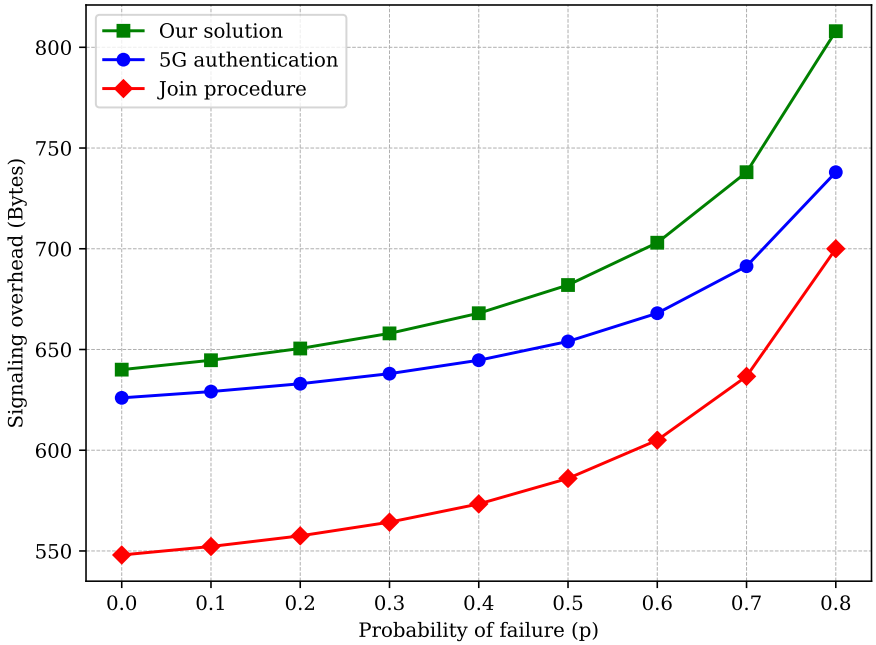


Figure 5.9: Variation of signaling overhead of access procedures in function of p.

The results show that LoRaWAN join procedure has the lowest signaling overhead since LoRaWAN uses a network architecture simpler than that of 5G, resulting in less signaling. Our solution requires more signaling than EAP-AKA' (combined with a secondary authentication method) since LoRaWAN parameters are sent during EAP-LoRaWAN-CN and EAP-LoRaWAN-DN to be compatible with both 5G and LoRaWAN standards. However, the signaling overhead in our solution is about 640 Bytes for p = 0, and 658 Bytes for p = 0.3, which is considered acceptable as compared with other solutions in Section 5.5.

5.3.3 Storage requirement

The adaptation function requires certain storage space in the gNB-CU. This is due to the session context of each ED managed by the gNB-CU. The session context consists of the following elements:

- The LoRaWAN session context.
- A mapping record between the 5G-GUTI, LoRaWAN DevAddr and IP address.
- The PDU session context of the session managed by the gNB-CU on the behalf of ED.
- The session keys including K_{NAS} and NwkSKeys.

In Table 5.3, we detail the size of each parameter constituting the session context elements. The total size of storage needed for one ED management is equal to 122 Bytes. This value is compared with other solutions in Section 5.5.

Table 5.3: Storage requirement per ED session context in gNB-CU.

Element	Parameter	Size (Bytes)
LoRaWAN session context	FCntUp	4
	AFCntUp	4
	Total	**8**
Mapping record	5G-GUTI	10
	DevAddr	8
	IPv6 address	16
	Total	**34**
PDU session context	Identifier	1
	S-NSSAI	4
	DNN	8
	Session Type	1
	Mode	1
	UP Security	1
	Total	**16**
Device session keys	K_{NAS}	32
	SNwkSIntKey	16
	NwkSEncKey	16
	Total	**64**
Total	**122 Bytes**	

5.4 Security evaluation

The security of the proposed authentication methods is evaluated according to security issues detailed in Section 2.5.2 and using AVISPA software. We evalu-

ate the security in order to prove that the integration solution including the new authentication methods achieves a secure integration solution.

5.4.1 Security analysis

- Device authentication: an ED should be authenticated with 5GC in roaming and non-roaming scenarios. This is guaranteed in 5G using one of the primary authentication methods (5G-AKA, EAP-AKA' and EAP-TLS). In roaming scenario, the SEAF is responsible for the authentication of ED with the home network through AUSF. In our solution, the ED is authenticated with the 5GC using a new primary authentication method called EAP-LoRaWAN-CN involving SEAF and AUSF as required in 5G standards. Moreover, in case of the movement inside the same network coverage, i.e., intra-gNB-CU, inter-gNB-CU and N2-based mobility, the authentication and key agreement are managed as detailed in the previous section.
- Address squatting, spoofing and old address control: the address that should be protected from squatting and spoofing is the ED DevAddr. DevAddr is assigned by gNB-CU after the secondary authentication and sent in an encrypted and integrity-protected message. Moreover, data sent from ED to AS are encrypted using AppSKey, thus, an attacker trying to spoof the DevAddr could not send data to AS. In addition, LoRaWAN commands sent from ED to gNB-CU are protected using NwkSKeys preventing the spoofing of DevAddr.
- Mutual authentication: it implies that 5GC authenticates the ED, and ED authenticates 5GC. This is achieved using EAP-LoRaWAN-CN as detailed before, the 5GC authenticates the ED using the MIC_{JR} in the join request message, and the ED authenticates 5GC using the MIC in the join accept message. In addition, mutual authentication is achieved between the ED and the PDN using MIC_{AAA} checked by the AAA server during the secondary authentication. Moreover, ED knows that an attacker cannot decrypt the data since they are encrypted using AppSKey which guarantees secure data delivery.
- Key freshness: it ensures that the session keys are updated occasionally or on-demand to provide forward secrecy and to avoid the use of keys stolen by an attacker. Session keys are updated usually in case of mobility when the ED changes its radio access point. As detailed in our solution, the intra-gNB-CU and inter-gNB-CU do not require an update of NwkSKeys or K_{NAS}. However, in N2-based mobility, NwkSKeys and K_{NAS} are updated by sending a force rejoin request to the ED in order to re-authenticate with the 5GC.
- Context steal or alteration: The main context that should be protected is the PDU session context containing the LoRaWAN session context and other session parameters. This context is saved in the gNB-CU and in the SMF. As described before, this context is exchanged between the gNB-CU in case of mobility. However, it is not exchanged or disclosed to any entity which is not authorized to access.

- Replay attack: performed by the re-transmission of the initial attach request messages usually. However, the proposed authentication method resists this attack using the DevNonce field sent in the join request message. In addition, the join accept message is protected from replay attack using JoinNonce field.

5.4.2 AVISPA evaluation

We used also AVISPA to validate the security of the proposed authentication methods which are EAP-LoRaWAN-CN and EAP-LoRaWAN-DN, more especially, we focus on the authentication part of these methods. In Figure 5.10, we show the last part of the implementation containing the environment and the goals intended. In the environment, we declare five agents that will play the role of ED, gNB, AMF, SMF, AUSF, UDM, and AAA. In addition, we declare the keys used which are K and AppKey, as well as ED parameters like JoinEUI and DevEUI which are passed to the corresponding agents in the session declaration. Moreover, we declare a hash function, and the channels used to send and receive messages between the agents. Besides, we declare the protocol identifiers used later in the goals and the intruder knowledge. In the end, we declare the session that aggregates these parameters in one communication scenario, while the rest of the code defines the exact operation of each agent according to authentication methods.

In the goal part, we focus mainly on the mutual authentication of ED with 5GC represented by the AUSF, and with the PDN represented by the AAA server. The authentication with the 5GC is based on K and the derived NwkKey, while the authentication with the PDN is based on AppKey, as defined in the rest of the implementation.

After running AVISPA for the implemented authentication methods, the output proves that it is safe as shown in Figure 5.11. The implementation source codes can be found in [126].

5.5 Comparison with related work

In this section, we compare our solution with related works proposed by Navarro-Ortiz *et al.* [51] and Torroglosa-Garcia *et al.* [52] according to the metrics evaluated in the previous section which are the handoff delay, signaling overhead, and storage requirement. Moreover, we present the security features provided by each solution. The related works did not evaluate completely their proposals according to our metrics, thus we studied them deeply to evaluate them according to our metrics.

5.5.1 Performance comparison

5.5.1.1 Handoff delay

In [51], the handoff delay is evaluated through an experimental testbed using 'The Things Network' [55] where the results show that handoff delay is approximately 792 ms assuming a bandwidth of 500 kHz and SF equals 7. In [52], a regular LoRaWAN join procedure is needed for the authentication preceded by a failed LoRaWAN join

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

role enviroment()

        def=

                const
                        ed,gnb,amf,smf,ausf,udm,aaa : agent,
                        joineui,deveui : nat,
                        h : hash_func,
                        k,appkey,sk : symmetric_key,
                        snd,rcv : channel(dy),

                        auth_cn_ed, auth_ed_cn, auth_dn_ed : protocol_id

                intruder_knowledge = {ed,gnb,amf,smf,ausf,udm,aaa,joineui,deveui,h,i}

                composition
                        session(ed,gnb,amf,smf,ausf,udm,aaa,joineui,deveui,k,appkey,sk,h,snd,rcv)

end role

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

goal

        authentication_on auth_cn_ed
        authentication_on auth_ed_cn
        authentication_on auth_dn_ed

end goal

enviroment()

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

Figure 5.10: HLPSL implementation of the new authentication methods.

request attempt, thus the handoff delay is greater than LoRaWAN join procedure handoff delay. For a bandwidth of 250 kHz and SF equals 7, the handoff delay is approximately 733 ms. The authentication delays of the three solutions are shown in Table 5.4.

5.5.1.2 Signaling overhead

In [51], the authentication method used is EAP-AKA' where the gNB performs a part of the authentication on behalf of ED, thus the signaling overhead is equal to EAP-AKA' with a secondary authentication to authenticate ED with the AS. In [52], two approaches are proposed, but we consider the default case where an ED does not have an active 5G radio link. In this case, a join request re-transmission is needed. Moreover, two new services are defined in the UDM and accessed by JS to complete the authentication. The signaling overheads of the three solutions are shown in Table 5.4.

5.5.1.3 Storage requirement

In [51], the LoRaWAN GW holds a USIM containing the long-term secret K and acts as a gNB, thus GW should hold a session context consisting of a mapping record, a PDU session context and the derived session keys. In [52], the ED stores an additional JoinEUI, SUPI and long-term secret K to perform the alternate authentication using the 5G network. The storage requirements of the three solutions are shown in Table 5.4.

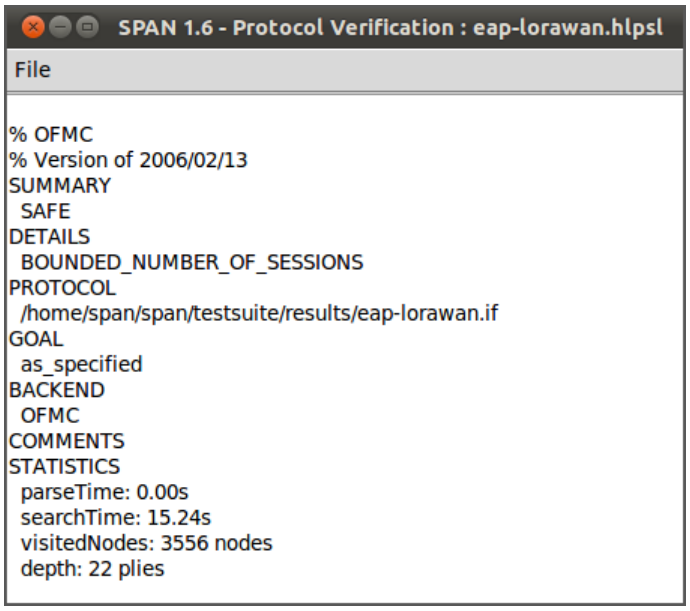


Figure 5.11: Security evaluation using AVISPA.

Table 5.4: Performance comparison of our solution and related work.

Solution	[56]	[51]	[52]	**Our solution**
Model type	Default	Network-Based	Host-Based	Network-Based
Adapted approach		LoRaWAN GW as 5G gNB	5G keys in ED	C-RAN & EAP
Mobility support	Yes	No	Yes	Yes
Handoff delay	410 ms	792 ms	733 ms	416 ms
Signaling overhead	548 → 700	610 → 722	738 → 1170	640 → 808
Storage requirement	N/A	114 Bytes	48 Bytes	122 Bytes

5.5.2 Security comparison

We evaluate the security of [51, 52] according to the security issues investigated in our previous work [40]. The comparison of these solutions is summarized in 5.5.

- Device authentication: the authors in [51] proposed an access procedure replacing the LoRaWAN join procedure providing device authentication. However, the authentication cannot be achieved outside the location of the ED where it is considered an immobile ED, and can establish a connection with only one eNB. In [52], the authors propose an alternative way to provide LoRaWAN authentication using 5G network which support also authentication in case of roaming.
- Address squatting, spoofing and old address control: these security issues are not applicable in [51] since the ED is considered immobile. In [52], address squatting and spoofing are prevented since the ED DevAddr is assigned by the NS after each authentication success, and old address control is prevented since any packet sent from an ED is encrypted using the corresponding AppSKey

mapped to DevEUI.

- Mutual authentication: this security feature is not achieved in [51] since the ED cannot authenticate the 4G/5G network. The authors propose that the eNB holds USIM containing 4G/5G credentials are not saved in the ED, thus it is not possible to authenticate the 4G/5G network. However, the authentication between the ED and the NS is achieved. In [52], mutual authentication between the ED and the NS is achieved although an alternative to LoRaWAN join procedure is used.
- Key freshness: after a successful authentication in [51], the ED and the NS derive the session keys according to LoRaWAN key derivation scheme. However, as the ED is immobile, the session keys are changed rarely and key freshness is not ensured. In [52], the session keys are also derived according to LoRaWAN key derivation scheme and are updated regularly according to the ED movement.
- Context steal or alteration: in [51], the context is not transferred from an eNB to another one since the ED is immobile, thus this security issue is not considered. In [52], the context is saved according to 5G and LoRaWAN standards thus it is considered secure.
- Replay attack: this security issues is prevented in the two solutions using LoRaWAN nonce fields employed in the join procedure, which are DevNonce and JoinNonce.

As a result, our solution provides competitive results in terms of performance, where we achieve a good signaling overhead, an acceptable storage requirement and the best handoff delay. At the same time, our solution ensures secure access along with additional security features.

Table 5.5: Security comparison of our solution and related work.

	[51]	[52]	Our
Device authentication	✓	✓	✓
Address squatting and spoofing		✓	✓
Old address control		✓	✓
Mutual authentication		✓	✓
Key freshness		✓	✓
Context alteration		✓	✓
Replay attack	✓	✓	✓

5.6 Conclusion

In this chapter, we proposed a new solution for the integration of LoRaWAN into 5GS. We proposed a network architecture where the RAN is the LoRaWAN RAN,

and the core network is based on 5GC. In addition, we proposed two authentication methods called EAP-LoRaWAN-CN and EAP-LoRaWAN-DN to achieve primary and secondary authentication. Moreover, the gNB-CU is supposed to perform an adaptation function to achieve seamless integration. The evaluation of our solution shows that it provides good performance, security features, and competitive results with related works.

Chapter 6

Conclusion and perspectives

6.1 Conclusion

With the advancement and wide deployment of IoT, LPWAN technologies are invented to fulfill the requirements of applications requiring low power consumption and long coverage range features. Mobility feature was an additional requirement needed by several applications like supply chain tracking and healthcare supervision. The movement of a device may be in the coverage of the same network operator called intra-domain mobility, or towards the coverage of another network operator called inter-domain mobility. Moreover, if the device uses the same technology during the mobility, the latter is called homogeneous mobility, otherwise, it is called heterogeneous mobility. Thus, several types of mobility exist requiring a mobility management solution. In addition, the security of this solution should be a main concern during the conception phase since several security issues may threaten the network operation. These security issues threaten the main requirements of secure communication which are confidentiality, integrity, availability, and authenticity. Moreover, the mobility context complicates the situation with additional security issues that are related and specific to the mobility behavior like the device authentication in the visited domain and the device address control.

Therefore, we started our thesis by investigating the mobility solutions designed for computer networks that do not have IoT networks or LPWAN constraints, where a vast of solution exists which are based on IPv6 like FMIPv6, HMIPv6, and PMIPv6. Then we focus on mobility solutions designed for IoT networks and LPWANs that take into consideration the existing constraints and the network topology. At the same time, we investigated the security issues that arise from device mobility with the possible countermeasures to solve such issues.

After establishing the necessary background including the mobility part and the security part, we proposed an intra-domain mobility solution based on PMIPv6 as a network-based mobility management protocol. The use of PMIPv6 has resulted in two challenges since it is deployed in an LPWAN environment, where the first is the compatibility of LPWAN technology with PMIPv6, and the second is the overhead caused by using a network layer for LPWAN technologies that do not use a network layer like LoRaWAN. Our solution tackled these two challenges by the addition of

a new entity called LoRaMAG, and the modification of the device protocol stack to reduce the overhead caused and to met the payload length constraint. Regarding the security side, the problem of authentication identified in PMIPv6 is also considered where we proposed an authentication scheme providing secure access and solving the security issues investigated formerly. To analyze the efficiency of the proposed solution, we evaluated the performance according to two main metrics which are the handoff delay and the signaling overhead. In addition, we evaluated the security of this solution through security analysis according to security issues investigated before and using AVISPA software.

Since inter-domain mobility is a common behavior and a main requirement in several LPWAN applications, we improved the proposed solution by an extension of the authentication scheme that allows the device to be authenticated outside its home domain. This authentication extension provides also a visited domain anchored authentication where the home domain is involved in the authentication during the first time of authentication, while the following authentications are performed by the visited domain. Moreover, we detailed how mobility is managed in different scenarios and how this solution is compatible with LPWAN technologies, especially LoRaWAN. The evaluation of this improved solution performance is also made according to handoff delay and signaling overhead, and the security evaluation is made also through security analysis and using AVISPA software. To understand the obtained results, we compared the mobility and the security features provided by this improved solution to that provided by related work presented before. The results show the improvement and the supremacy of our solution compared to related work when used in an LPWAN environment.

With the wide adoption and deployment of 5G networks, we spotted the advantages of integrating LoRaWAN technology into the 5G system like quasi-free services, and dedicated network functionality assisting in the context of mobility management. Thus, we proposed an integration solution based on several design principles that allow efficient integration such as compatibility with LoRaWAN and 5G standards and seamless integration for devices. The integration solution adopts the network architecture of 5G where the network server and join server functionalities are divided into the 5G NFs. In addition, two new authentication methods based on EAP are proposed to authenticate a LoRaWAN device with the 5GC in a way conserving both LoRaWAN and 5G specifications. Moreover, an adaption function is defined for the gNB-CU achieving seamless integration and responsible for the translation of signaling messages, and performing device-related procedures. This solution performance is evaluated according to the handoff delay, signaling overhead, and storage requirement, which are later compared with related work performance to prove the advantages of using our solution. Besides, we evaluate and compare the security of our solution to related work which shows also the security features ensured in our solution.

6.2 Perspectives

This thesis covers a considerable part of the proposition of a secure mobility solution for LPWANs. However, the contributions of our thesis can be strength-

ened either by the proposal of supplementary concepts or by the evaluation of our solutions through testbeds and real deployments. Therefore, several ideas can be applied as follows:

- Study of LoRaMAG deployment: the addition of LoRaMAG entity in intra-domain and inter-domain mobility solutions to support PMIPv6 network layer necessitates a study of the deployment of these LoRaMAGs. For example, the number of LoRaMAG needed and the number of LoRaWAN GWs served by a single LoRaMAG should be well studied to improve the efficiency of the solution especially in terms of signaling overhead. In addition, the link management between the LoRaMAG and the NS, and between the LoRaMAG and the GWs should meet the capacity requirements regarding the number of devices served by the LoRaMAG where a load study can provide a lower deployment cost.
- Adaptation function optimization: the use of adaptation function to achieve seamless integration for LoRaWAN into 5G can be further optimized in several ways like the distribution of sub-functions over the gNB-DU based on the device profile which reduces the load and signaling overhead caused. Moreover, a cache layer may be added to save recent device status making it possible for several device-related functions to be discarded or performed less often.
- Testbeds and real deployments: in the evaluation of our solutions, we used NS-3 to implement the proposed solution and to simulate the performance. However, a better and more adequate evaluation can be achieved using testbeds or real deployments that involve several devices in case of mobility and performing the necessary mobility procedures or sending application data. The difference here is that more realistic parameters will be taken into consideration like a server capacity which limits the number of served devices, and the probability of a link failure which necessitates additional time to complete the handoff and additional re-transmissions causing more overhead.

Bibliography

[1] G. Aloi *et al.*, "Enabling iot interoperability through opportunistic smartphone-based mobile gateways," *Journal of Network and Computer Applications*, vol. 81, pp. 74–84, 2017.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] M. S. Bali, K. Gupta, D. Koundal, A. Zaguia, S. Mahajan, and A. K. Pandit, "Smart architectural framework for symmetrical data offloading in iot," *Symmetry*, vol. 13, no. 10, p. 1889, 2021.

[4] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[5] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for iot big data and streaming analytics: A survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2923–2960, 2018.

[6] H.-C. Lee and K.-H. Ke, "Monitoring of large-area iot sensors using a lora wireless mesh network system: Design and evaluation," *IEEE Transactions on Instrumentation and Measurement*, vol. 67, no. 9, pp. 2177–2187, 2018.

[7] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "Iot middleware: A survey on issues and enabling technologies," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 1–20, 2016.

[8] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of lpwan technologies for large-scale iot deployment," *ICT Express*, vol. 5, no. 1, pp. 1–7, 2019.

[9] K. Zen, D. Habibi, A. Rassau, and I. Ahmad, "Performance evaluation of ieee 802.15. 4 for mobile sensor networks," in *2008 5th IFIP International Conference on Wireless and Optical Communications Networks (WOCN'08)*, IEEE, 2008, pp. 1–5.

[10] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd, and T. Hayajneh, "Security vulnerabilities in bluetooth technology as used in iot," *Journal of Sensor and Actuator Networks*, vol. 7, no. 3, p. 28, 2018.

[11] C. M. Ramya, M. Shanmugaraj, and R. Prabakaran, "Study on zigbee technology," in *2011 3rd International Conference on Electronics Computer Technology*, IEEE, vol. 6, 2011, pp. 297–301.

[12] F. Ghavimi and H.-H. Chen, "M2m communications in 3gpp lte/lte-a networks: Architectures, service requirements, challenges, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 525–549, 2014.

[13] E. Dahlman, S. Parkvall, and J. Skold, *4G: LTE/LTE-advanced for mobile broadband*. Academic press, 2013.

[14] S. Ahmadi, *5G NR: Architecture, technology, implementation, and operation of 3GPP new radio standards*. Academic Press, 2019.

[15] B. S. Chaudhari, M. Zennaro, and S. Borkar, "Lpwan technologies: Emerging application characteristics, requirements, and design considerations," *Future Internet*, vol. 12, no. 3, p. 46, 2020.

[16] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "Overview of cellular lpwan technologies for iot deployment: Sigfox, lorawan, and nb-iot," in *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, IEEE, 2018, pp. 197–202.

[17] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range communications in unlicensed bands: The rising stars in the iot and smart city scenarios," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 60–67, 2016.

[18] D. Patel and M. Won, "Experimental study on low power wide area networks (lpwan) for mobile internet of things," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, IEEE, 2017, pp. 1–5.

[19] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 855–873, 2017.

[20] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on lpwa technology: Lora and nb-iot," *ICT Express*, vol. 3, no. 1, pp. 14–21, 2017.

[21] *Lora alliance*, Jun. 2022. [Online]. Available: `http://lora-alliance.org`.

[22] *Sigfox*, Jun. 2022. [Online]. Available: `http://sigfox.com`.

[23] H. H. R. Sherazi, L. A. Grieco, M. A. Imran, and G. Boggia, "Energy-efficient lorawan for industry 4.0 applications," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 891–902, 2020.

[24] F. Pitu and N. C. Gaitan, "Surveillance of sigfox technology integrated with environmental monitoring," in *2020 International Conference on Development and Application Systems (DAS)*, IEEE, 2020, pp. 69–72.

[25] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "Nb-iot system for m2m communication," in *2016 IEEE Wireless Communications and Networking Conference*, IEEE, 2016, pp. 1–5.

[26] *3gpp release13*, Oct. 2015. [Online]. Available: `http://3gpp.org/release-13`.

[27] *3gpp release15*, Apr. 2019. [Online]. Available: http://3gpp.org/release-15.

[28] *3gpp release17*, Jun. 2022. [Online]. Available: http://3gpp.org/release-17.

[29] *3gpp release18*, Jun. 2022. [Online]. Available: http://3gpp.org/release18.

[30] S. Böcker, C. Arendt, P. Jörke, and C. Wietfeld, "Lpwan in the context of 5g: Capability of lorawan to contribute to mmtc," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, IEEE, 2019, pp. 737–742.

[31] H. Fattah, *5G LTE Narrowband Internet of Things (NB-IoT)*. CRC Press, 2018.

[32] I. Lee and K. Lee, "The internet of things (iot): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[33] B. Muthu *et al.*, "Iot based wearable sensor for diseases prediction and symptom analysis in healthcare sector," *Peer-to-Peer Networking and Applications*, vol. 13, no. 6, pp. 2123–2134, 2020.

[34] E. Manavalan and K. Jayakrishna, "A review of internet of things (iot) embedded sustainable supply chain for industry 4.0 requirements," *Computers & Industrial Engineering*, vol. 127, pp. 925–953, 2019.

[35] S. M. Ghaleb, S. Subramaniam, Z. A. Zukarnain, and A. Muhammed, "Mobility management for iot: A survey," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 1, pp. 1–25, 2016.

[36] A. Dutta and H. Schulzrinne, *Mobility Protocols and Handover Optimization: Design, Evaluation and Application*. John Wiley & Sons, 2014.

[37] A. Ahmed, L. M. Boulahia, and D. Gaiti, "Enabling vertical handover decisions in heterogeneous wireless networks: A state-of-the-art and a classification," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 776–811, 2013.

[38] J. M. L. Caldeira, J. J. P. Rodrigues, and P. Lorenz, "Intra-mobility support solutions for healthcare wireless sensor networks–handover issues," *IEEE Sensors Journal*, vol. 13, no. 11, pp. 4339–4348, 2013.

[39] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[40] H. Jradi, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prévotet, "Overview of the mobility related security challenges in lpwans," *Computer Networks*, vol. 186, p. 107 761, 2021.

[41] Y. Chen, Y. A. Sambo, O. Onireti, and M. A. Imran, "A survey on lpwan-5g integration: Main challenges and potential solutions," *IEEE Access*, vol. 10, pp. 32 132–32 149, 2022.

[42] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of lorawan," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 34–40, 2017.

[43] C. Gomez, J. C. Veras, R. Vidal, L. Casals, and J. Paradells, "A sigfox energy consumption model," *Sensors*, vol. 19, no. 3, p. 681, 2019.

[44] A. J. Jabir, S. K. Subramaniam, Z. Z. Ahmad, and N. A. W. A. Hamid, "A cluster-based proxy mobile ipv6 for ip-wsns," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1, pp. 1–17, 2012.

[45] V. Sharma *et al.*, "Mih-spfp: Mih-based secure cross-layer handover protocol for fast proxy mobile ipv6-iot networks," *Journal of Network and Computer Applications*, vol. 125, pp. 67–81, 2019.

[46] S. R. Moosavi *et al.*, "End-to-end security scheme for mobility enabled healthcare internet of things," *Future Generation Computer Systems*, vol. 64, pp. 108–124, 2016.

[47] W. Ayoub, F. Nouvel, A. E. Samhat, M. Mroue, and J.-C. Prevotet, "Mobility management with session continuity during handover in lpwan," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6686–6703, 2020.

[48] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, H. Jradi, and J.-C. Prévotet, "Media independent solution for mobility management in heterogeneous lpwan technologies," *Computer Networks*, vol. 182, p. 107 423, 2020.

[49] A. Durand, P. Gremaud, and J. Pasquier, "Decentralized lpwan infrastructure using blockchain and digital signatures," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 12, e5352, 2020.

[50] J. Lamberg-Liszkay and T. Lisauskas, *An alternative roaming model in lorawan*, Linnaeus University, Jul. 2018. [Online]. Available: `http://diva-portal.org/smash/get/diva2:1277620/FULLTEXT01.pdf`.

[51] J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler, "Integration of lorawan and 4g/5g for the industrial internet of things," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 60–67, 2018.

[52] E. M. Torroglosa-Garcia, J. M. A. Calero, J. B. Bernabe, and A. Skarmeta, "Enabling roaming across heterogeneous iot wireless networks: Lorawan meets 5g," *IEEE Access*, vol. 8, pp. 103 164–103 180, 2020.

[53] R. Fujdiak, K. Mikhaylov, J. Pospisil, A. Povalac, and J. Misurec, "Insights into the issue of deploying a private lorawan," *Sensors*, vol. 22, no. 5, p. 2042, 2022.

[54] *Company semtech corporation*, Jun. 2022. [Online]. Available: `http://semtech.com`.

[55] *The things network*, Jun. 2022. [Online]. Available: `http://thethingsnetwork.org`.

[56] N. Sornin and Y. Alper, *Lorawan specification v1.1*, Oct. 2017. [Online]. Available: `http://lora-alliance.org/resource_hub/lorawan-specification-v1-1`.

[57] B. Reynders and S. Pollin, "Chirp spread spectrum as a modulation technique for long range communication," in *2016 Symposium on Communications and Vehicular Technologies (SCVT)*, IEEE, 2016, pp. 1–5.

[58] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: Turbo-codes," *IEEE Transactions on Communications*, vol. 44, no. 10, pp. 1261–1271, 1996.

[59] F. Chang, K. Onohara, and T. Mizuochi, "Forward error correction for 100 g transport networks," *IEEE Communications Magazine*, vol. 48, no. 3, S48–S55, 2010.

[60] J. Haxhibeqiri, E. De Poorter, I. Moerman, and J. Hoebeke, "A survey of lorawan for iot: From technology to application," *Sensors*, vol. 18, no. 11, p. 3995, 2018.

[61] "Short range devices (srd) operating in the frequency range 25 mhz to 1 000 mhz," ETSI, Tech. Rep. EN 300 220-1 V3.1.1, Feb. 2017. [Online]. Available: `http://etsi.org/deliver/etsi_en/300200_300299/30022001/03.01.01_60/en_30022001v030101p.pdf`.

[62] T. Socolofsky and C. Kale, *A tcp/ip tutorial*, RFC 1180, Jan. 1991.

[63] M. Luvisotto, F. Tramarin, L. Vangelista, and S. Vitturi, "On the use of lorawan for indoor industrial iot applications," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[64] L. Vangelista and M. Centenaro, "Worldwide connectivity for the internet of things through lorawan," *Future Internet*, vol. 11, no. 3, p. 57, 2019.

[65] N. Sornin and Y. Alper, *Lorawan backend interfaces 1.0 specification*, Oct. 2017. [Online]. Available: `http://lora-alliance.org/resource_hub/lorawan-back-end-interfaces-v1-0`.

[66] *3gpp release8*, Dec. 2008. [Online]. Available: `http://3gpp.org/specifications/releases/72-release-8`.

[67] *3gpp release14*, Jun. 2017. [Online]. Available: `http://3gpp.org/release-14`.

[68] "Evolved universal terrestrial radio access (e-utra) and evolved universal terrestrial radio access network (e-utran)," ETSI, Tech. Rep. TS 36.300 version 14.10.0, Jul. 2019. [Online]. Available: `http://etsi.org/deliver/etsi_ts/136300_136399/136300/14.10.00_60/ts_136300v141000p.pdf`.

[69] S. Popli, R. K. Jha, and S. Jain, "A survey on energy efficient narrowband internet of things (nbiot): Architecture, application and challenges," *IEEE Access*, vol. 7, pp. 16 739–16 776, 2018.

[70] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prévotet, "Internet of mobile things: Overview of lorawan, dash7, and nb-iot in lpwans standards and supported mobility," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1561–1581, 2018.

[71] A. Adhikary, X. Lin, and Y.-P. E. Wang, "Performance evaluation of nb-iot coverage," in *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, IEEE, 2016, pp. 1–5.

[72] A. K. Sultania, P. Zand, C. Blondia, and J. Famaey, "Energy modeling and evaluation of nb-iot with psm and edrx," in *2018 IEEE Globecom Workshops (GC Wkshps)*, IEEE, 2018, pp. 1–7.

[73] M. Shafi *et al.*, "5g: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 6, pp. 1201–1221, 2017.

[74] "System architecture for the 5g system (5gs)," ETSI, Tech. Rep. TS 23.501 v16.6.0, Oct. 2020. [Online]. Available: http://etsi.org/deliver/etsi_ts/123500_123599/123501/16.06.00_60/ts_123501v160600p.pdf.

[75] R. Fielding *et al.*, *Hypertext transfer protocol – http/1.1*, RFC 2616, Jun. 1999.

[76] "Management and orchestration; concepts, use cases and requirements," ETSI, Tech. Rep. TS 28.530 v15.2.0, Oct. 2019. [Online]. Available: http://etsi.org/deliver/etsi_ts/128500_128599/128530/15.02.00_60/ts_128530v150200p.pdf.

[77] "Architecture enhancements for control and user plane separation of epc nodes," ETSI, Tech. Rep. TS 23.214 v14.2.0, May 2017. [Online]. Available: http://etsi.org/deliver/etsi_ts/123200_123299/123214/14.02.00_60/ts_123214v140200p.pdf.

[78] "Security architecture and procedures for 5g system," ETSI, Tech. Rep. TS 33.501 v16.3.0, Aug. 2020. [Online]. Available: http://etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf.

[79] "5g release description; release 15," ETSI, Tech. Rep. TS 21.915 v15.0.0, Oct. 2019. [Online]. Available: http://etsi.org/deliver/etsi_tr/121900_121999/121915/15.00.00_60/tr_121915v150000p.pdf.

[80] "Xn application protocol (xnap)," ETSI, Tech. Rep. TS 38.423 v15.4.0, Jul. 2019. [Online]. Available: http://etsi.org/deliver/etsi_ts/138400_138499/138423/15.04.00_60/ts_138423v150400p.pdf.

[81] "Ng application protocol (ngap)," ETSI, Tech. Rep. TS 38.413 v15.0.0, Jul. 2018. [Online]. Available: http://etsi.org/deliver/etsi_ts/138400_138499/138413/15.00.00_60/ts_138413v150000p.pdf.

[82] "Security assurance specification (scas) for the next generation node b (gnodeb) network product class," ETSI, Tech. Rep. TS 33.511 v16.7.0, Aug. 2021. [Online]. Available: http://etsi.org/deliver/etsi_ts/133500_133599/133511/16.07.00_60/ts_133511v160700p.pdf.

[83] "Packet data convergence protocol (pdcp) specification," ETSI, Tech. Rep. TS 38.323 v15.2.0, Sep. 2018. [Online]. Available: http://etsi.org/deliver/etsi_ts/138300_138399/138323/15.02.00_60/ts_138323v150200p.pdf.

[84] L. Jonsson, K. Sandlund, G. Pelletier, and P. Kremer, *Robust header compression (rohc): Corrections and clarifications to rfc 3095*, RFC 4815, Feb. 2007.

[85] "F1 application protocol (f1ap)," ETSI, Tech. Rep. TS 38.473 v15.3.0, Oct. 2018. [Online]. Available: http://etsi.org/deliver/etsi_TS/138400_138499/138473/15.03.00_60/ts_138473v150300p.pdf.

[86] R. Stewart, *Stream control transmission protocol*, RFC 4960, Sep. 2007.

[87] J. Postel, *User datagram protocol*, RFC 768, Aug. 1980.

[88] "General packet radio system (gprs) tunnelling protocol user plane (gtpv1-u)," ETSI, Tech. Rep. TS 29.281 v15.7.0, Jan. 2020. [Online]. Available: http://etsi.org/deliver/etsi_ts/129200_129299/129281/15.07.00_60/ts_129281v150700p.pdf.

[89] J. Arkko and H. Haverinen, *Extensible authentication protocol method for 3rd generation authentication and key agreement (eap-aka)*, RFC 4187, Jan. 2006.

[90] D. Simon, B. Aboba, and R. Hurst, *The eap-tls authentication protocol*, RFC 5216, Mar. 2008.

[91] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, *Extensible authentication protocol (eap)*, RFC 3748, Jun. 2004.

[92] A. Triantafyllou, P. Sarigiannidis, and T. D. Lagkas, "Network protocols, schemes, and mechanisms for internet of things (iot): Features, open challenges, and trends," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[93] S. Deering and R. Hinden, *Internet protocol, version 6 (ipv6) specification*, RFC 2460, Dec. 1998.

[94] U. o. S. C. Information Sciences Institute, *Internet protocol*, RFC 791, Sep. 1981.

[95] F. Gont, *A method for generating semantically opaque interface identifiers with ipv6 stateless address autoconfiguration (slaac)*, RFC 7217, Apr. 2014.

[96] R. Droms, *Stateless dynamic host configuration protocol (dhcp) service for ipv6*, RFC 3736, Apr. 2004.

[97] D. Johnson, C. Perkins, and J. Arkko, *Mobility support in ipv6*, RFC 6275, Jul. 2011.

[98] R. Koodli, *Mobile ipv6 fast handovers*, RFC 5568, Jul. 2009.

[99] K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, *et al.*, *Proxy mobile ipv6*, RFC 5213, Aug. 2008.

[100] H. Soliman, C. Castelluccia, K. Elmalki, and L. Bellier, *Hierarchical mobile ipv6 (hmipv6) mobility management*, RFC 5380, Oct. 2008.

[101] A. Shabtai, Y. Elovici, and L. Rokach, "Introduction to information security," in *A Survey of Data Leakage Detection and Prevention Solutions*, Springer, 2012, pp. 1–4.

[102] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, *Fast handovers for proxy mobile ipv6*, RFC 5949, Sep. 2010.

[103] A. Dutta, V. Fajardo, Y. Ohba, K. Taniuchi, and H. Schulzrinne, *A framework of media-independent pre-authentication (mpa) for inter-domain handover optimization*, RFC 6252, Jun. 2011.

[104] E. Rescorla and N. Modadugu, *Datagram transport layer security version 1.2*, RFC 6347, Jan. 2012.

[105] A. Minaburo, L. Toutain, C. Gomez, D. Barthel, and J.-C. Zúñiga, *Static context header compression (schc) for the constrained application protocol (coap)*, RFC 8724, Jun. 2021.

[106] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for iot," *Computers & Security*, vol. 78, pp. 126–142, 2018.

[107] F. A. Aponte-Novoa, A. L. S. Orozco, R. Villanueva-Polanco, and P. Wightman, "The 51% attack on blockchains: A mining behavior study," *IEEE Access*, vol. 9, pp. 140 549–140 564, 2021.

[108] J. Sanchez-Gomez *et al.*, "Integrating lpwan technologies in the 5g ecosystem: A survey on security challenges and solutions," *IEEE Access*, 2020.

[109] S. Frankel and S. Krishnan, *Ip security (ipsec) and internet key exchange (ike) document roadmap*, RFC 6071, Feb. 2011.

[110] "Proxy mobile ipv6 (pmipv6) based mobility and tunnelling protocols," ETSI, Tech. Rep. TS 29.275 v13.5.0, Aug. 2016. [Online]. Available: `http://etsi.org/deliver/etsi_ts/129200_129299/129275/13.05.00_60/ts_129275v130500p.pdf`.

[111] "3gpp system architecture evolution (sae); security architecture," ETSI, Tech. Rep. TS 33.401 v15.7.0, May 2019. [Online]. Available: `http://etsi.org/deliver/etsi_ts/133400_133499/133401/15.07.00_60/ts_133401v150700p.pdf`.

[112] Z. Shelby, K. Hartke, and C. Bormann, *The constrained application protocol (coap)*, RFC 7252, Jun. 2014.

[113] *Mqtt specifications*, Jun. 2022. [Online]. Available: `http://mqtt.org/mqtt-specification`.

[114] T. Dierks and E. Rescorla, *The transport layer security (tls) protocol version 1.2*, RFC 5246, Aug. 2008.

[115] P. Saint-Andre, *Extensible messaging and presence protocol (xmpp): Core*, RFC 6120, Mar. 2011.

[116] S. Vinoski, "Advanced message queuing protocol," *IEEE Internet Computing*, vol. 10, no. 6, pp. 87–89, 2006.

[117] K. Sandlund, G. Pelletier, and L.-E. Jonsson, *The robust header compression (rohc) framework*, RFC 5795, Mar. 2010.

[118] P. Thubert, C. Bormann, L. Toutain, and R. Cragie, *Ipv6 over low-power wireless personal area network (6lowpan) routing header*, RFC 8138, Apr. 2017.

[119] W. Ayoub, M. Mroue, F. Nouvel, A. E. Samhat, and J.-C. Prévotet, "Towards ip over lpwans technologies: Lorawan, dash7, nb-iot," in *2018 Sixth International Conference on Digital Information, Networking, and Wireless Communications (DINWC)*, IEEE, 2018, pp. 43–47.

[120] M. Kanj, V. Savaux, and M. Le Guen, "A tutorial on nb-iot physical layer design," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2408–2446, 2020.

[121] T. Mizrahi, J. Fabini, and A. Morton, *Guidelines for defining packet timestamps*, RFC 8877, Sep. 2020.

[122] S. Debnath, A. Chattopadhyay, and S. Dutta, "Brief review on journey of secured hash algorithms," in *2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix)*, IEEE, 2017, pp. 1–5.

[123] *Network simulator 3*, Jun. 2022. [Online]. Available: `http://nsnam.org`.

[124] *Secure-intra-domain-mobility ns-3 module*, Jun. 2021. [Online]. Available: `http://github.com/HassanJradi/intra-domain-solution`.

[125] A. Armando *et al.*, "The avispa tool for the automated validation of internet security protocols and applications," in *International Conference on Computer Aided Verification*, Springer, 2005, pp. 281–285.

[126] *Avispa hlpsl implementation*, Oct. 2021. [Online]. Available: `http://github.com/HassanJradi/avispa`.

[127] *Secure-inter-domain-mobility ns-3 module*, Oct. 2021. [Online]. Available: `http://github.com/HassanJradi/inter-domain-solution`.

[128] *La66 lorawan shield*, May 2021. [Online]. Available: `http://dragino.com/products/lora.html`.

[129] S. Ryu, G.-Y. Kim, B. Kim, and Y. Mun, "A scheme to reduce packet loss during pmipv6 handover considering authentication," in *2008 International Conference on Computational Sciences and Its Applications*, IEEE, 2008, pp. 47–51.

[130] M. Nakhjiri and M. Nakhjiri, *AAA and network security for mobile access: radius, diameter, EAP, PKI and IP mobility*. John Wiley & Sons, 2005.

[131] *Lorawan ns-3 module*, Jan. 2022. [Online]. Available: `http://github.com/signetlabdei/lorawan`.

[132] *Lorawan-5g-integration ns-3 module*, May 2022. [Online]. Available: `http://github.com/HassanJradi/lorawan-5g-integration`.

Titre : Réseaux IoT : Etude de solutions de mobilité sécurisée et intégration dans le réseau 5G.

Mots clés : IoT, LPWAN, 5G, Mobilité, Sécurité

Résumé : L'Internet des objets (IoT) est un nouveau système émergent d'appareils interconnectés qui connaît une croissance significative. Les technologies de communication en plein essor sont les Low Power Wide Area Networks (LPWANs) ayant une longue portée de communication, une faible consommation d'énergie et un faible coût de déploiement. La mobilité est un comportement commun à plusieurs applications, et la sécurité est une exigence cruciale dans tout système de communication. Cependant, la diversité des technologies LPWAN et leurs contraintes fortes font de l'intégration de ces fonctionnalités un défi. Donc, dans cette thèse, nous nous concentrons sur la conception d'une solution sécurisée de gestion de la mobilité pour les LPWAN. Dans une première partie, nous proposons une solution pour la mobilité des appareils à l'intérieur de la couverture du même opérateur basée sur le protocole réseau Proxy Mobile IPv6, une architecture réseau adaptée, et un schéma d'authentification qui assure un accès sécurisé. Dans la deuxième partie, nous étendons le schéma d'authentification précédemment proposé pour fournir une solution de mobilité des appareils entre les couvertures des différents opérateurs où nous évaluons également les performances et la sécurité de la solution. De plus, nous comparons notre solution avec des travaux connexes pour prouver son efficacité et sa sécurité. Dans la troisième partie, nous proposons une nouvelle solution pour l'intégration de la technologie LoRaWAN dans le système 5G qui permet de tirer partie de la simplicité et de la rentabilité de LoRaWAN et des fonctionnalités de puissance et d'évolutivité de la 5G. De plus, un accès sécurisé est fourni grâce à de nouvelles méthodes d'authentification compatibles avec les normes LoRaWAN et 5G.

Title: IoT networks: Study of secure mobility solutions and integration into the 5G network

Keywords: IoT, LPWAN, 5G, Mobility, Security

Abstract: The Internet of Things (IoT) is a new emerging system of interconnected devices that experiences significant growth. The rising communication technologies are the Low Power Wide Area Networks (LPWANs) having long communication range, low power consumption, and low deployment cost. Mobility is a common behavior of several applications, and security is a crucial requirement in any communication system. However, the diversity of LPWAN technologies and their tight constraints make the integration of these features a challenge. Thus, in this thesis, we focus on the design of a secure mobility management solution for LPWAN. In the first part, we propose a solution for device mobility inside the coverage of the same operator based on Proxy Mobile IPv6 network protocol, an adapted network architecture, and an authentication scheme that ensures secure access. In the second part, we extend the authentication scheme proposed previously to provide a solution for device mobility between the coverages of different operators where we also evaluate the performance and the security of the solution. Moreover, we compare our solution with related work to prove its efficiency and security. In the third part, we propose a new solution for the integration of LoRaWAN technology into the 5G system that allows leveraging the simplicity and cost efficiency of LoRaWAN and the power and scalability features of 5G. Further, secure access is provided through new authentication methods that are compatible with LoRaWAN and 5G standards.