Université Paris-Sud

Ecole Doctorale Informatique Paris Sud

Laboratoire Recherche en informatique

Discipline : Informatique

SYNTHESE DE THÈSE

Soutenue le 8/12/2014 par

Soran Sabah Hussein

Solutions de Sécurité Légers pour les Réseaux LTE/LTE-A

Directeur de thèse :	Dr. Lila Boukhatem	Université Paris-Sud
Co-directeur de thèse :	Pr. Steven Martin	Université Paris-Sud

Composition du jury :

Reviewers: :	Pr. Hakima Chaouchi	Institut Télécom Sud-Paris
	Dr. Hassnaa Moustafa	Intel Corporation
Examiners :	Pr. Joffroy Beauquier	Université Paris-Sud
	Dr.Thi-Mai-Trang NGUYEN	Université Pierre et Marie Curie, Paris 6
	Dr. Nadjib Ait saadi	Université Paris Est Créteil Val de Marne

Résumé

Récemment, le 3GPP (3rd Generation Partnership Project) a standardisé les systèmes LTE/LTE-A (Long Term Evolution/LTE-Advanced) qui ont été approuvés par l'UIT (Union Internationale des Télécommunications) comme des réseaux de télécommunications mobiles de 4éme génération. La sécurité est l'une des questions essentielles qui doivent être traitées avec soin pour protéger les informations de l'opérateur et des utilisateurs. Aussi, le 3GPP a normalisé plusieurs algorithmes et protocoles afin de sécuriser les communications entre les différentes entités du réseau. Cependant, l'augmentation du niveau de sécurité dans ces systèmes ne devrait pas leur imposer des contraintes lourdes telles qu'une grande complexité de calcul ou encore une forte consommation d'énergie. En effet, l'efficacité énergétique est devenue récemment un besoin critique pour les opérateurs afin de réduire l'empreinte écologique et les coûts opérationnels de ces systèmes. Les services de sécurité dans les réseaux mobiles tels que l'authentification, la confidentialité et l'intégrité des données sont le plus souvent effectués en utilisant des techniques cryptographiques. Toutefois, la plupart des solutions standardisées déjà adoptées par le 3GPP dépendent des algorithmes de chiffrement qui possèdent une grande complexité, induisant une consommation énergétique plus élevée dans les différentes entités communicantes du réseau. La confidentialité des données, qui se réfère principalement au fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé, est réalisée au niveau de la sous-couche PDCP (Packet Data Convergence Protocol) de la pile protocolaire de LTE/LTE-A par l'un des trois algorithmes normalisés (EEA1, EEA2 et EEA3). Or, chacun des trois algorithmes exige une forte complexité de calcul car ils reposent sur la théorie de chiffrement de Shannon qui utilise les fonctions de confusion et de diffusion sur plusieurs itérations. Dans cette thèse, nous proposons un nouvel algorithme de confidentialité en utilisant le concept de substitution et de diffusion dans lequel le niveau de sécurité requis est atteint en un seul tour. Par conséquent, la complexité de calcul est considérablement réduite ce qui entraîne une réduction de la consommation d'énergie par les fonctions de chiffrement et de déchiffrement. De plus, la même approche est utilisée pour réduire la complexité des algorithmes 3GPP d'intégrité des données (EIA1, EIA2 et EIA3) dont le concept de chiffrement repose sur les mêmes fonctions complexes. Enfin, nous étudions dans cette thèse le problème d'authentification dans le contexte du paradigme D2D (Device to Device communications) introduit dans les systèmes 4G. Le concept D2D se réfère à la communication directe entre deux terminaux mobiles sans passer par le cœur du réseau. Il constitue un moyen prometteur pour améliorer les performances et réduire la consommation d'énergie dans les réseaux LTE/LTE-A. Toutefois, l'authentification et la dérivation de clé entre deux terminaux mobiles dans le contexte D2D n'ont pas fait l'objet d'études. Aussi, nous proposons un nouveau protocole léger d'authentification et de dérivation de clé

permettant d'authentifier les terminaux D2D et de dériver les clés nécessaires à la fois pour le cryptage et pour la protection de l'intégrité des données.

1-Introduction

La croissance continue et rapide de la consommation de données mobiles en particulier en raison de la augmentation considérable de l'utilisation de l'appareil Smartphone a motivé les organisations pour la standardisation de développer des technologies 4G, comme (Long Term Evolution /LTE-Advanced (LTE/ LTE-A), de passer à des débits de données plus élevés par rapport aux réseaux 3G. Ce déploiement de systèmes 4G a déclenché la transition de l'existant 3G circuit paquet combiné à le réseau de paquets basé sur IP et de ne plus offrir de mode commuté qui fait des réseaux LTE/LTE-A de posséder une nouvelle et différente architecture de sécurité. Caractéristiques de sécurité comme de nombreuses autres fonctionnalités de réseaux mobiles devraient posséder une interopérabilité mondiale pour atteindre pertinence globale et cela se fait grâce à la standardisation de ces caractéristiques. Par conséquent, le 3GPP qui est la principale organisation dominante pour la standardisation de réseaux mobiles a traité les questions de sécurité dans les systèmes LTE/LTE-A à travers la standardisation des protocoles et des algorithmes à différents niveaux de sécurité de réseau. Au niveau de l'accès au réseau, l'authentification des utilisateurs et l'accord de clé sont effectuées via le protocole EPS-AKA, un protocole d'authentification basé sur la cryptographie symétrique. En outre, afin d'atteindre la confidentialité de données de l'utilisateur, le 3GPP a normalisé pour les réseaux LTE/LTE-A trois algorithmes; EEA1, EEA2 et EEA3. De même, trois autres algorithmes ont été normalisés pour l'intégrité des données EIA1, EIA2 et EIA3. De plus, au cours de la procédure de normalisation, les principaux objectifs des algorithmes et des protocoles choisis étaient atteignaient un maximum de sécurité sans prendre en considération les questions environnementales ou écologiques tels que les économies d'énergie. Par conséquent, il serait souhaitable d'envisager de nouvelles structures pour nouveaux protocoles et algorithmes qui acquissent moins de puissance de calcul pour réduire les consommations d'énergie et par conséquent contribuent à la réduction des émissions de CO2. À la lumière de toutes les considérations précèdent, notre objectif dans cette thèse est de proposer des algorithmes légers de sécurité et plus particulièrement des algorithmes l'intégrité des données et la confidentialité des données en concevant des algorithmes de chiffrement efficaces en termes de complexité et en même temps la possession suffisante de sécurité. Un autre objectif de notre travail est d'examiner la question de la sécurité dans le contexte du paradigme D2D (Device to Device communications) qui ont récemment attiré l'attention des chercheurs pour développer des solutions efficaces pour les communications directes entre deux appareils proches. Notre dernière contribution consiste en la conception d'une authentification légère et un protocole de dérivation de clé entre les deux utilisateurs communiquant par une liaison D2D. Notre solution proposée est basée sur le concept de cryptographie à courbe elliptique qui est considéré comme un outil prometteur pour ces exigences de

sécurité.
Le reste de la thèse est organisé comme suit: dans la section 2, nous allons présenter les services d'architecture et de sécurité de sécurité dans les réseaux LTE/LTE-A. Dans la section 3, nous allons présenter notre première contribution à propos d'algorithme de chiffrement efficace et robuste pour la confidentialité des données. Ensuite, nous allons présenter un algorithme d'intégrité de données nouvelle dans la section 4. Dans la section 5, nous allons présenter un protocole d'authentification et de dérivation de clé pour D2D. Enfin dans la section 6, nous concluons la thèse. données.

2-Architecture de sécurité pour LTE/LTE-A

L'architecture de sécurité des réseaux mobiles a été soumise à des évolutions ultérieures depuis le premier système mobile. La 4G (LTE / LTEA) architecture représentée sur la figure 1 et également notée Evolved Packet System (EPS) apporte deux nouveaux ingrédients majeurs dans l'environnement 3GPP:

le réseau radio Evolved-Universal Terrestrial Radio Access Network (E-UTRAN) avec une nouvelle interface radio et le cœur de réseau basé sur IP Evolved Packet Core (EPC). De plus, les EPS doivent également être en mesure de fonctionner avec les systèmes existants et de réaliser la compatibilité ascendante. Dans le (3GPP TS 33,401), l'architecture de sécurité est divisé en cinq niveaux de sécurité différents ou (domaines) où les services de sécurité différents sont atteints dans ces niveaux (voir la figure ref11). Le 3GPP TS 33,401 définit ces niveaux que les suivantes:

- Sécurité de domaine de réseau(II)
- Sécurité du domaine de l'utilisateur(III)
- Sécurité du domaine d'application (IV)
- Visibilité et configurabilité de la sécurité(V)
- Sécurité d'accès réseau (I): ce niveau est principalement liée au réseau d'accès radio (E-UTRAN) et décrit comme l'ensemble des services de sécurité qui offrent aux utilisateurs un accès sécurisé à des services et à protéger l'utilisateur contre les attaques. Le sujet de cette thèse est particulièrement lié à la sécurité d'accès au réseau.

Par la suite, nous présentons les services de sécurité les plus importants de l'EPS qui sont principalement effectuées dans le niveau d'accès du réseau:

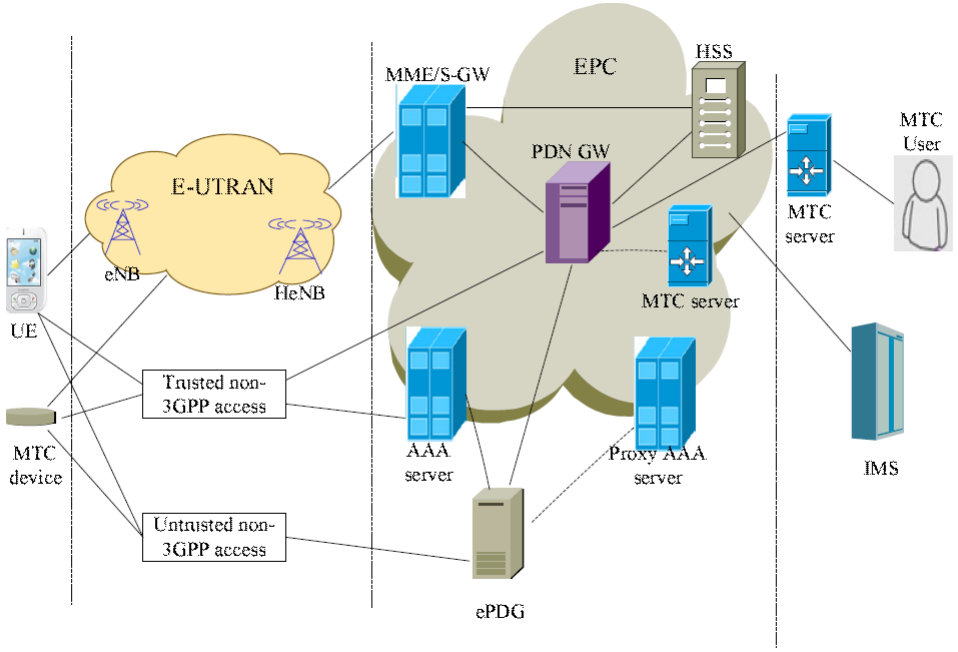

FIGURE 1: Architecture de LTE/LTE-A

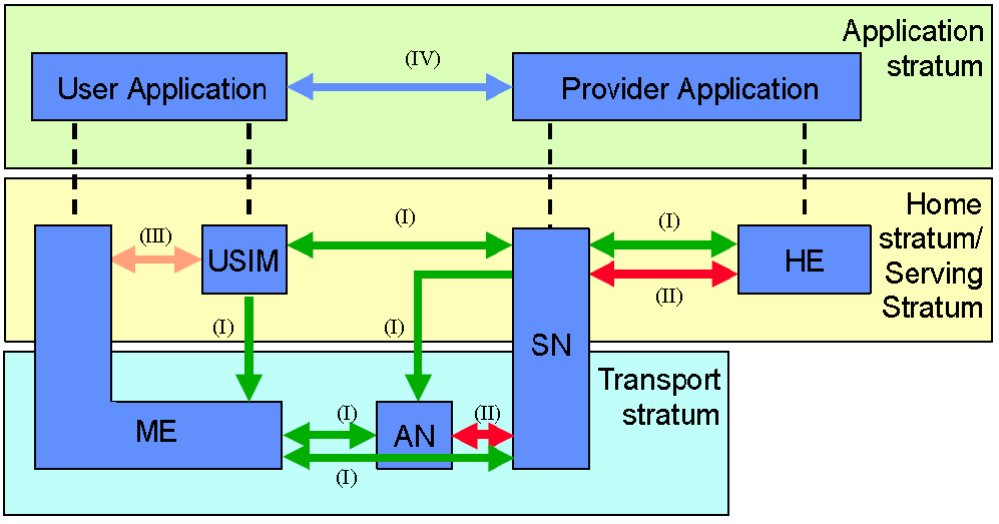

FIGURE 2: Niveaux de sécurité de réseaux LTE/LTE-A

a-Authentification et dérivation de clé: L'authentification mutuelle entre les User Equipements (UEs) et le réseau et dérivation de clé pour établir des sessions clés pour le chiffrement et la protection de l'intégrité sont des caractéristiques de sécurité essentielles pour tout réseau mobile. Le 3GPP adopté pour LTE/LTE-A un nouveau protocole d'authentification et accord de clé appelés EPS-AKA.
b-La confidentialité des données de l'utilisateur et de contrôle: La confidentialité est obtenue par chiffrement de la communication numérique dans le but de protéger les contenu des paquets d'être vu par les tiers puissent en particulier sur l'interface radio. Par conséquent, le 3GPP standardisé trois algorithmes notamment EEA1 basé sur (SNOW 3G), EEA2 basé sur (AES) et EEA3 basé sur (ZUC) à être utilisé dans les réseaux LTE/LTE-A.
c-Intégrité des données de contrôle: Le but de cette fonction est de s'assurer de l'authenticité de chaque message de control séparément, cet-a-dire faire en sorte que le message n'a pas été modifié pendant la transmission et a été reçu par la destination comme il a été effectivement envoyé par la source. le 3GPP standardisé trois algorithmes, notamment ; EIA1 basé sur (SNOW 3G), EIA2 basé sur (AES) et EIA3 basé sur (ZUC) à être utilisé dans les réseaux LTE / LTE-A.

3-Algorithmes de chiffrement efficace et robuste pour la confidentialité des données de la technologie LTE/LTE-A (ERCA)

Dans cette section, nous proposons une nouvelle technique de chiffrement de flux basé sur la structure Substitution Diffusion Network (SDN) qui son principal avantage est d'une main sa complexité réduite à un tour au lieu de plusieurs tours utilisées dans les algorithmes standardisé, et d'autre part, il possède une force de sécurité forte que les solutions standardisées. L'algorithme proposé consiste en une addition, une substitution et une couche de diffusion.

Généralement, l'algorithme de chiffrement considère un flux de paquets en texte brut P existe à la source (UE ou eNB) et doit être transmis en toute sécurité. Ce flux est divisé en plusieurs paquets P^w, ($w = 1,\ ldots,$ h) et chaque paquet est divisé en plusieurs blocs M_j^w ($j = 1,\ 2,\ \ldots,\ q$) d'une longueur de 128 bits. Le processus de cryptage et décryptage dans EEA est représenté dans la figure 3
Le schéma de base de l'algorithme de chiffrement proposé est présenté dans la figure 4.

Pour chaque bloc d'entrée, le processus d'addition est appliqué en premier, puis le processus de substitution. Après cela, nous remodeler la sortie du processus de substitution

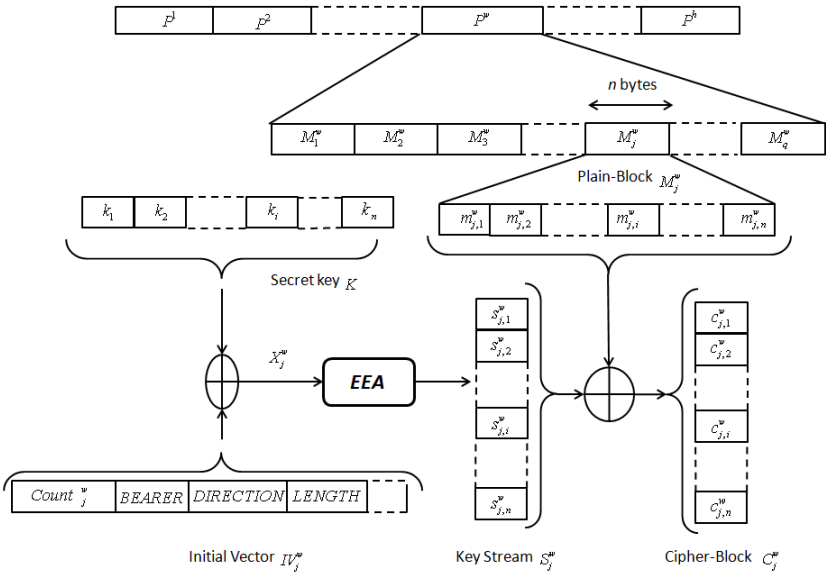

FIGURE 3: Ciphering a block of data.

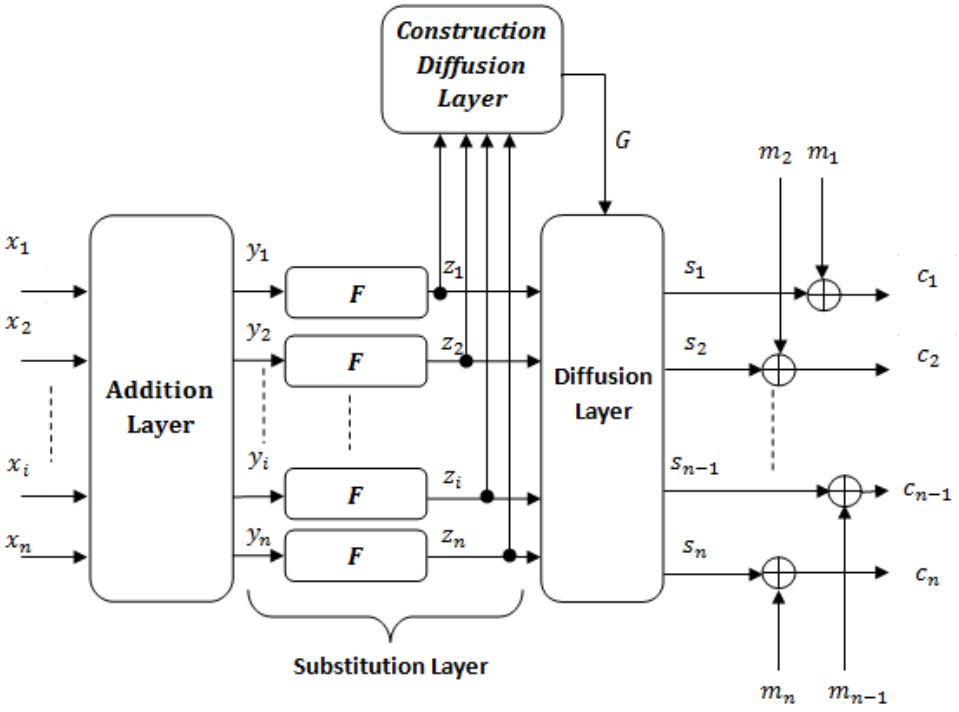

FIGURE 4: ERCA stream cipher

(ligne) pour former une sous-matrice, qui est utilisé pour construire la matrice de diffusion. Enfin, le processus de diffusion est appliqué en utilisant la matrice de diffusion obtenu à la sortie de la couche de substitution.

Pour démontrer les performances de la couche de substitution proposée, ses propriétés sont comparées avec la couche de substitution de l'AES et ZUC (S_0 et S_1) dans le tableau 1. Les résultats ont montré que la couche de substitution proposé possède performances

TABLE 1: Comparison Analysis of Substitution Layer

Test	Proposed	AES	S_0	S_1
LP_F	$2^{-5.3}$	2^{-6}	2^{-5}	2^{-6}
DP_F	2^{-4}	2^{-6}	2^{-4}	2^{-6}
SAC	0.5	0.4998	0.494	0.509
BIC	0.502	0.4998	0.4951	0.505

cryptographiques suffisantes et les résultats obtenus de Linear Probability Approximation Boolean Function (LP_F),Differential Probability Approximation Function (DP_F), Strict Avalanche Criterion (SAC) et Output Bit Independence Criterion (BIC) sont très proches les solutions standardisées.

Après confirmation de forte caractéristique de sécurité de l'algorithme proposé, nous avons comparé le temps de chiffrement moyen (en ms), contre Tb en comparaison avec AES. Le schéma proposé est sûr au moins $4,5$ fois plus rapide que l'algorithme AES comme indiqué dans la figure 5.

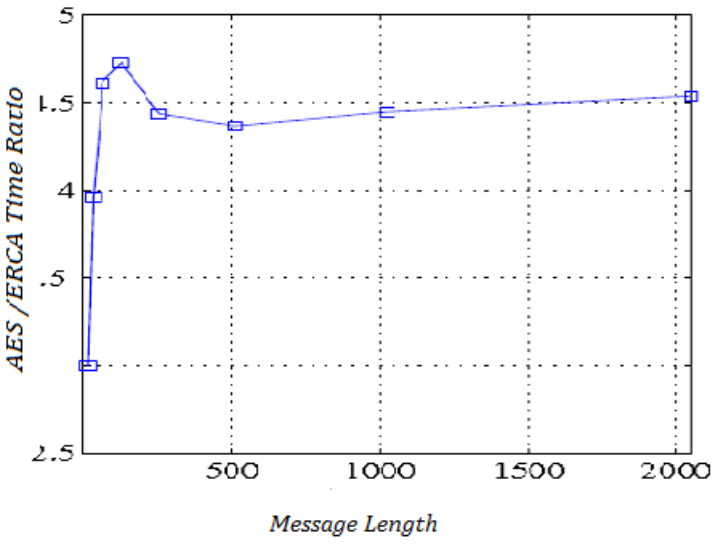

FIGURE 5: Variations of the average time ratio for messages encryption (AES/ERCA) in function to its length

4-Algorithme efficace et robuste pour LTE / LTE-A intégrité des données

Dans cette section, nous proposons un nouvel algorithme de DI efficace et robuste. Son principal avantage est l'utilisation d'une technique de substitution-diffusion dynamique dans le noyau de l'algorithme de chiffrement qui ne nécessite qu'un seul tour de traitement au lieu de plusieurs séries de traitement comme l'exigent les solutions de référence normalisées. Le processus de génération MAC qui utilise le concept de Merkle et Damgard est représenté dans la figure 10. Il se compose d'une fonction de compression (une fonction de hachage sur la base d'un algorithme de chiffrement par bloc), qui est appliqué dans un processus itératif.
La valeur de hachage est calculée selon l'équation suivante:

$$H_i = ERADI(H_{i-1}, M_i) \qquad i = 1,\ 2, \ldots, nb$$

La dernière sortie H_{nb} est tronqué en obtenant le 32 MSB (Most Significant Bits), qui est exploité directement comme MAC-I.

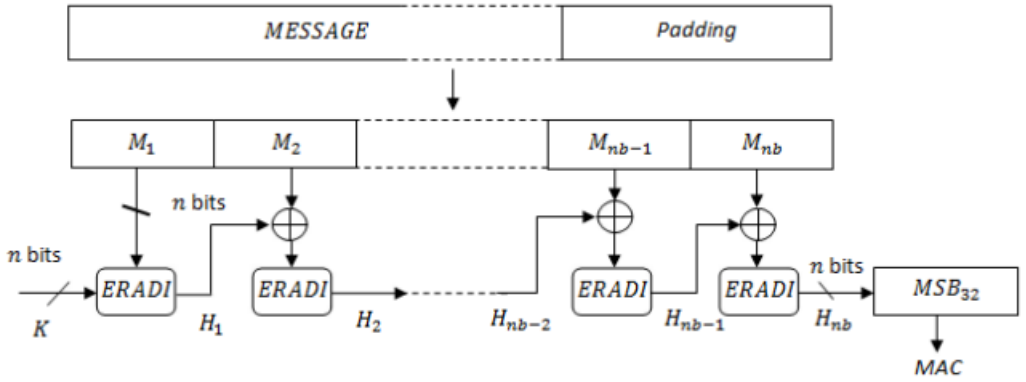

FIGURE 6: The iterated design of the proposed keyed hash function for ERADI

Il est important de noter que la structure générale de ce chiffrement est presque similaire à la structure des algorithmes ERCA. La principale différence est que dans cet algorithme, une couche de chaînage est ajoutée à la structure originale qui est représenté sur la figure 11

Plusieurs tests sont effectués pour analyser et prouver la faisabilité et la force de notre algorithme proposé. Plusieurs tests de simulation ont été effectués et les résultats de collision, les tests de l'espace et de sensibilité clés ont été analysés. Également une comparaison est effectuée entre notre algorithme et le standard de EIA2 récente en termes de vitesse d'exécution.

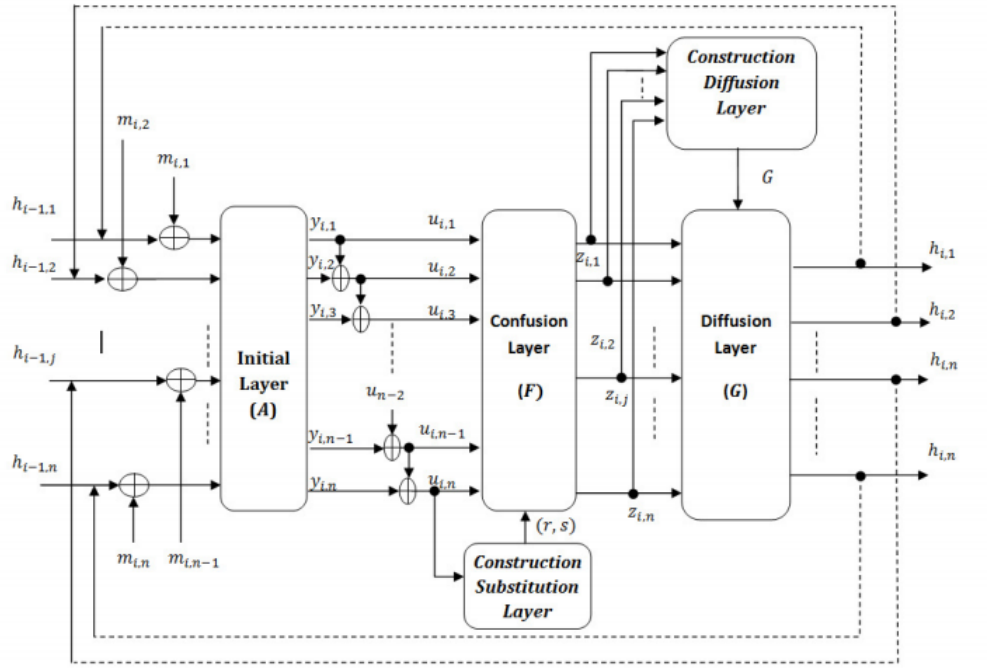

FIGURE 7: Proposed compression function (ERADI)

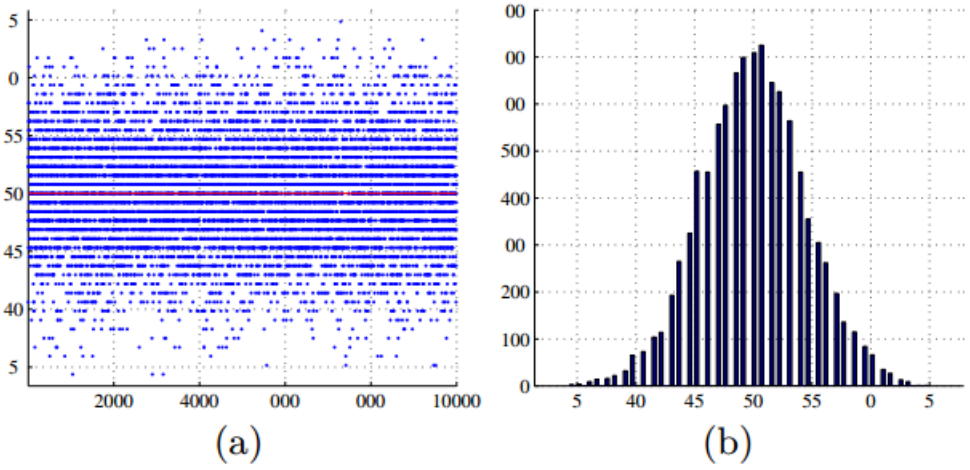

FIGURE 8: Percent of number of the changed bits versus 1000 original tests (changed random bit of the message) (a) and its corresponding distribution (b)

Dans la figure 12, la sensibilité du message original par rapport 1000 messages aléatoires sont présentés, alors que seulement un Least Significant Bit (LSB) est modifiée du message M. Nous pouvons observer que la majorité des échantillons est plus proche des valeurs optimales du niveau de bits (50%). En plus des fonctions de sécurité, la vitesse d'exécution est un critère important pour quantifier la complexité de calcul de notre algorithme proposé et de le comparer à la solution standardisée. La comparaison est réalisée avec l'algorithme EIA2 (AES), car il est considéré comme le plus sûr par rapport

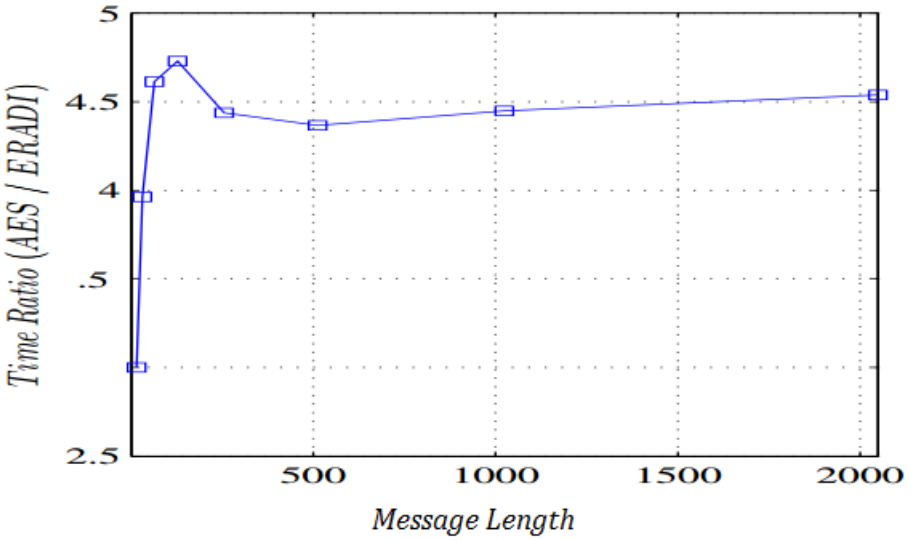

FIGURE 9: Variations of the average time ratio versus message length

aux deux autres algorithmes EIA1and EIA3. Le rapport des temps de calcul de moyenne (ERADI/EIA2) au message haché M avec des longueurs différentes est représenté sur la figure 13.

4-Algorithme efficace et robuste pour LTE / LTE-A intégrité des données

Dans cette section, nous proposons un nouvel algorithme d'intégrité efficace et robuste. La principal avantage de cet algorithme est l'utilisation d'une technique de substitution-diffusion dynamique dans le noyau de l'algorithme de chiffrement qui ne nécessite qu'un seul tour de traitement au lieu de plusieurs tours de traitement comme appliqué dans les solutions de référence standardisé. Le processus de génération de Message Authentication Code (MAC) qui utilise le concept de Merkle et Damgard est représenté dans la figure 10. Il se compose d'une fonction de compression (une fonction de hachage sur la base d'un algorithme de chiffrement par bloc), qui est appliqué dans un processus itératif.
La valeur de hachage est calculée selon l'équation suivante:

$$H_i = ERADI(H_{i-1}, M_i) \qquad i = 1,\ 2, \ldots, nb$$

La dernière sortie H_{nb} est tronqué en obtenant le 32 Most Significant Bit (MSB) qui est exploité directement comme MAC-I.

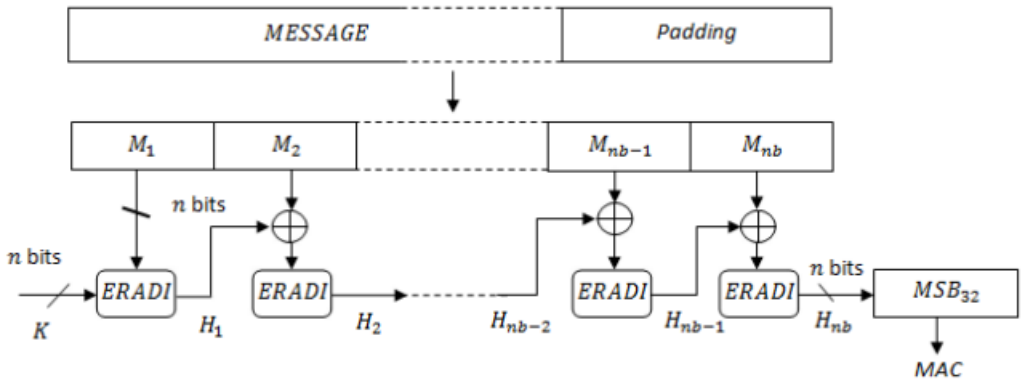

FIGURE 10: The iterated design of the proposed keyed Hash function for ERADI

Il est important de noter que la structure générale de ce chiffrement est presque similaire à la structure des algorithmes ERCA. La principale différence est que dans cet algorithme, une couche de chaînage est ajoutée à la structure originale qui est représenté sur la figure 11

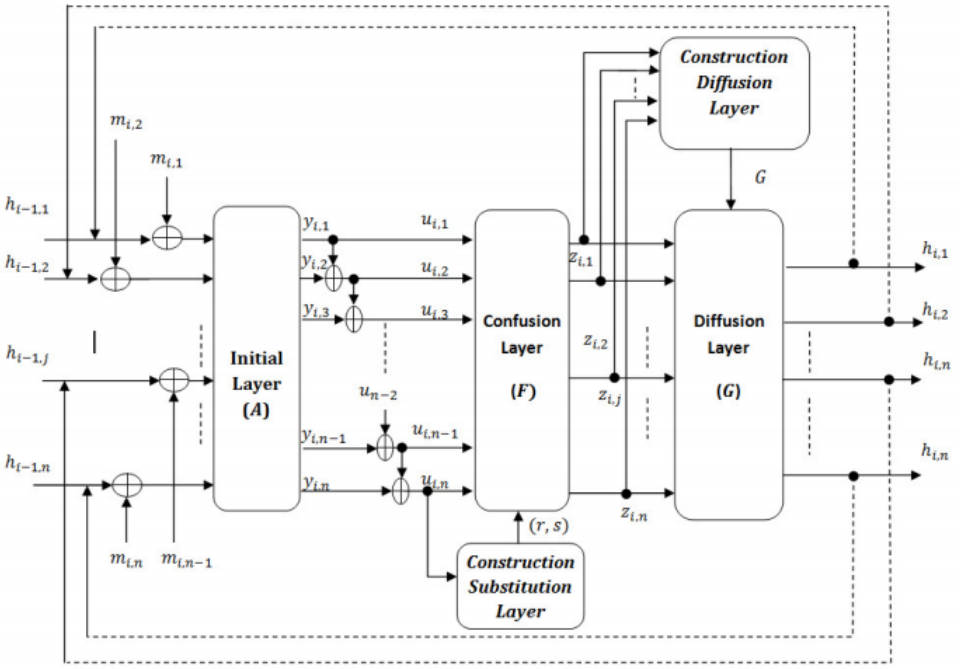

FIGURE 11: Proposed compression function (ERADI)

Plusieurs tests sont effectués pour analyser et prouver la faisabilité et la force de l'algorithme proposé. Plusieurs tests de simulation ont été effectués et les résultats de collision, les tests de sensibilité des messages ont été analysés. Également une comparaison est effectuée entre notre algorithme et l'algorithme du standard (EIA2), en termes de vitesse d'exécution.

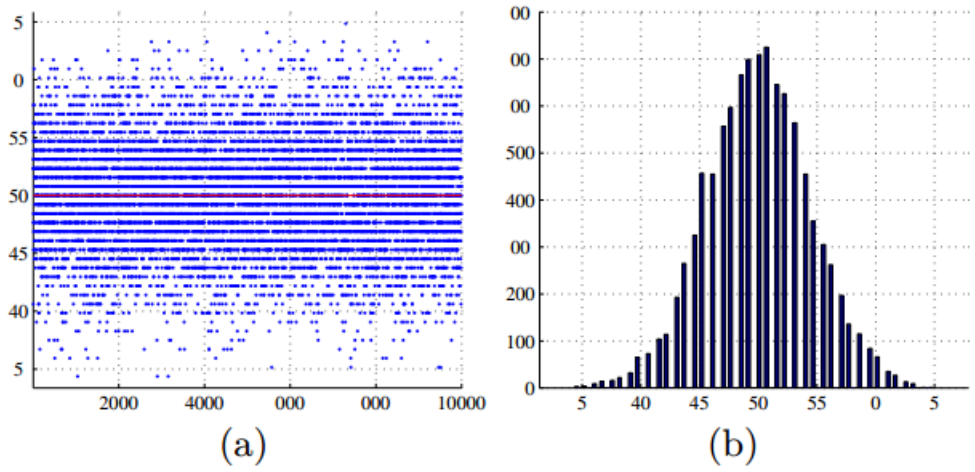

FIGURE 12: Percent of number of the changed bits versus 1000 original tests (changed random bit of the message) (a) and its corresponding distribution (b)

Dans la figure 12, la sensibilité du message original par rapport 1000 messages aléatoires sont présentés, alors que seulement un Least Significant Bit (LSB) est modifiée du message M. Nous pouvons observer que la majorité des échantillons est plus proche des valeurs optimales du niveau de bits (50%). En plus des fonctions de sécurité, la vitesse d'exécution est un critère important pour quantifier la complexité de calcul de notre algorithme proposé et de le comparer à la solution standardisée. La comparaison est réalisée avec l'algorithme EIA2 (AES), car il est considéré comme le plus sûr par rapport aux deux autres algorithmes EIA1and EIA3. Le rapport des temps de calcul de moyenne (ERADI/EIA2) au message haché M avec des longueurs différentes est représenté sur la figure 13. L'algorithme proposé est aussi au moins $4,5$ fois plus rapide que l'algorithme EIA2, comme indiqué.

5-Authentification léger et protocole d'accord de clé pour communication de périphérique à périphérique (D2D)

Le scénario de D2D comme illustré sur la figure 14 montre que le trafic entre deux UE ($UE2$ et $UE3$) ne passe pas à travers le réseau de cœur.

L'authentification et le protocole d'accord de clé actuelle (EPS-AKA) est utilisé pour authentifier les UEs avec le réseau de cœur et aussi pour générer les clés symétriques nécessaires diverses pour assurer la confidentialité et la protection de l'intégrité. La procédure d'authentification et de dérivation de clé du protocole AKA est assurée par quatre entités dans les réseaux LTE/LTE-A; l'UE, l'eNB, l'entité de gestion de mobilité

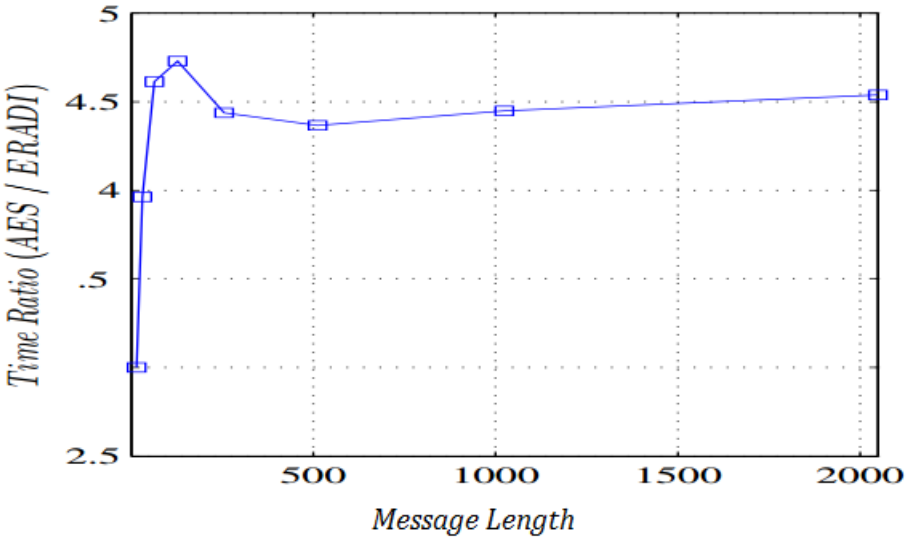

FIGURE 13: Variations of the average time ratio versus message length

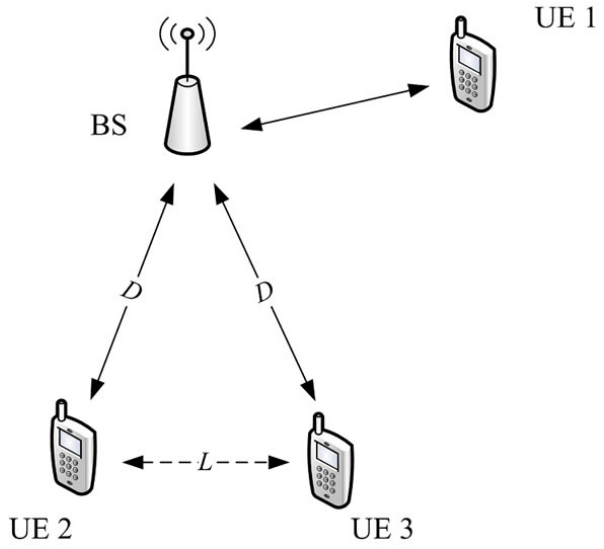

FIGURE 14: Scenario of LTE-A D2D communication

(MME) et le Home Subscriber Server (HSS). Toutefois, la participation de toutes ces entités peut avoir un effet négatif sur la latence et la bande passante de la consommation si AKA doit être utilisé pour les communications D2D. Il est donc souhaitable de disposer d'un protocole indépendant pour assurer l'authentification des deux UE ainsi que dériver les clés nécessaires à la fois pour assurer la confidentialité et la protection de l'intégrité.

Dans cette section, nous proposons un protocole d'authentification et dérivation de clé pour les communications D2D dans le LTE-A. La solution présentée est construit pour utiliser la cryptographie asymétrique pour authentifier deux UE souhaitant lancer la

communication D2D uns avec les autres et plus tard dériver des clés symétriques pour le chiffrement des données et la protection de l'intégrité, mais sans aucune implication du réseau de cœur .Par conséquent, l'idée principale de notre dispositif à l'authentification de l'appareil et la solution d'accord de clé, sur la base de courbe elliptique Diffie-Hellman (ECDH) schéma, ce est que chaque UE a une paire de clés publiques et privées. La clé publique n'est connue que par l'eNB, tandis que la clé privée reste secrète. De même, le eNB est également pourvu d'une paire de clés; un est privé et gardé secret et l'autre public et communiqués à l'intention des deux UE d'initier la communication de D2D. Notre schéma est divisé en cinq phases: A) d'initialisation, (B) génération de clé temporaire, (C) l'identification, (D) la production d'identité permanente et enfin (E) génération de clé de chiffrement et l'intégrité.
La procédure d'initialisation qui est lié au dispositif de découverte de périphériques est en dehors du champ d'application de cette thèse.
La génération de clé temporaire, comme cela a été montré dans nom de la figure 15 , est réalisé séparément dans chacune des deux partis de communication. Les UE de chaque partie de communication sont responsables de générer leurs propres clés publiques et privées sur la base de courbe elliptiques.

Le système d'identification est montré dans le figure 16. Afin d'identifier chacun des

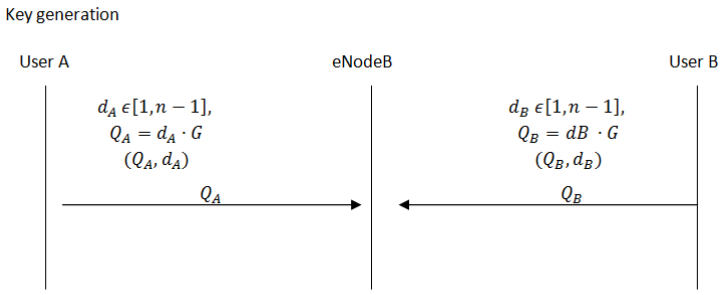

FIGURE 15: Temporary key generation

deux dispositifs par l'eNB, (Trois way handshake) protocole (engagement, défi, réponse) est adopté sans divulguer d'informations sur l'identité réelle de l'EU.
Après l'authentification, la production d'identité partagée est exécuté comme dans Figure 17 .

Pour offrir plus de robustesse contre les attaques, nous proposons un nouveau système de génération de clé dynamique pour KI et KE en utilisant le secret ID comme indiqué dans le Figure 18.

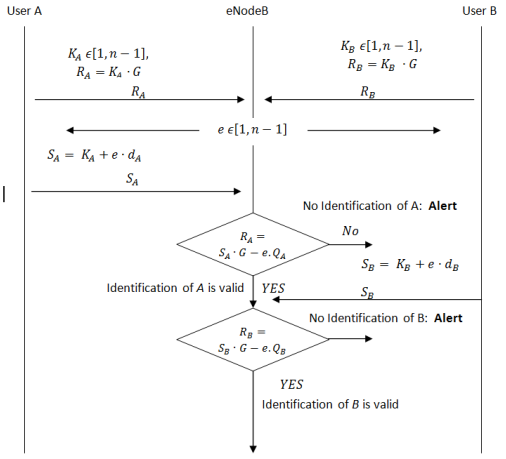

FIGURE 16: Identification

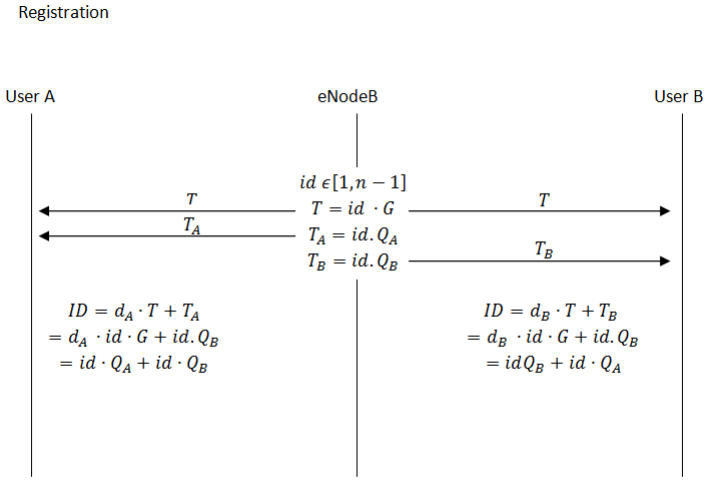

FIGURE 17: Shared identity Generation

Conclusions

Dans cette thèse, nous avons abordé deux principaux défis liés aux services de sécurité des réseaux (LTE/LTE-A): nous avons proposé des algorithmes de chiffrement et d'intégrité légers afin de parvenir à la confidentialité des données et l'intégrité des données et un nouveau protocole de l'authentification et la clé d'accord pour communications (de périphérique à périphérique) D2D.

Pour une meilleure compréhension des fonctionnalités requises des services de sécurité ainsi que des paradigmes employés pour réaliser ces services, nous avons présenté une description détaillée d'architecture de sécurité des réseaux (LTE/LTE-A). Notre analyse approfondie de cette architecture comme il a été proposé et rédigé par le 3GPP, qui nous

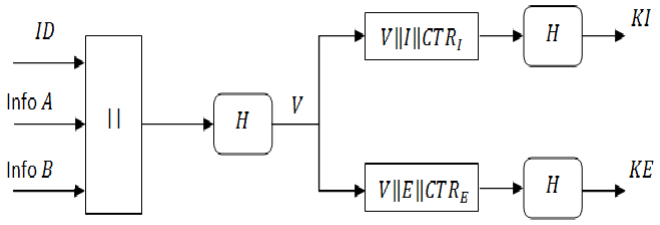

FIGURE 18: Cipher and Integrity Key generation

avait permis de découvrir où, quand et comment les services de sécurité demandée sont réalisés.

Jusqu'à présent, le 3GPP standardisé trois algorithmes de chiffrement à employer dans les réseaux LTE /LTE-A, notamment ; EEA1, EEA22 et EEA3 qui leur conception basés sur SNOW 3G, AES et ZUC, respectivement. Cependant, l'état de l'art lié à ces solutions standardisées a clairement révélé inconvénients considérables en termes de complexité de calcul ainsi que défauts de sécurité. Pour faire face à des limitations, nous avons proposé un nouvel algorithme de chiffrement robuste et léger, nommé ERCA qui a montré moins de complexité de calcul et par conséquent une meilleure consommation d'énergie. ERCA a été soumis à des tests statistiques et analytiques les plus nécessaires pour vérifier sa résistance à la sécurité et les résultats de simulation ont démontré clairement qu'il possède la plupart des propriétés cryptographiques demandé à être considéré comme un robuste algorithme de chiffrement sécurisé. En termes de complexité, nous avons comparé à ERCA à EIA2. Les résultats de la simulation en termes de temps d'exécution ont démontré que notre proposition est d'au moins 4,5 fois plus rapide qu'AES (EIA2)

La protection de l'intégrité est un autre service de sécurité importante en particulier dans les réseaux LTE/LTE-A pour assurer l'exactitude et la cohérence des données de contrôle. ERADI algorithme était notre deuxième contribution dans cette thèse. Contrairement à la solution standardisée où le même algorithme de chiffrement est utilisé dans le chiffrement et l'intégrité protection seulement en raison de la réutilisabilité, dans cette thèse, nous avons utilisé une version différente modifiée de l'algorithme de chiffrement dans le noyau de l'ERADI proposé par l'ajout d'une couche de chaînage à l'algorithme original utilisé dans la confidentialité des données. Ajoutant une couche de chaînage nous avait permis d'avoir une meilleure dépendance de bits avec une surcharge négligeable à la complexité de l'algorithme de chiffrement. La performance d'ERADI a été évaluée en utilisant des tests statistiques et analytiques bien connus en termes de robustesse et de sécurité. Les résultats obtenus ont montré son efficacité dans la génération de MAC crédible à être utilisé dans la protection de l'intégrité. Afin de quantifier le gain

de complexité, une comparaison a été réalisée avec l'algorithme d'EIA2 qui est basé sur AES. Les résultats ont montré une meilleure performance de l'algorithme d'ERADI qui était au moins environ 4,5 fois plus rapide qu'EIA2.
Enfin, la dernière contribution de notre thèse a été propose un protocole d'authentification et de dérivation de clé pour les communications D2D sous le milieu de LTE-A car les communications D2D contribueraient aussi aux économies d'énergie dans ces réseaux. Contrairement au protocole original EPS-AKA qui est basé sur la cryptographie symétrique, notre schéma proposé utilise la cryptographie à clé publique pour l'authentification et en même temps dérive clés symétriques utilisant des fonctions de hachage unidirectionnel. En effet, nous avons utilisé le concept de ECC en raison de son utilisation de clé de petite taille par rapport aux autres systèmes de cryptographie à clé publique tels que RSA, ce qui en retour permet d'obtenir une réduction complexité de calcul et de communication. Le schéma d'authentification a été analysé en termes de sa force de sécurité contre plusieurs attaques différentes pour évaluer sa pertinence pour ces scénarios.