REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE ECHAHID CHEIKH LARBI TEBESSI - TEBESSA

Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie

Département : Mathématiques et Informatique

Mémoire de fin d'étude

Pour l'obtention du diplôme de MASTER

Domaine: MI

Filière: Informatique

Option: Réseaux et Sécurité Informatique

Thème :

Schéma d'intégrité distribuée pour les réseaux sans fils de nouvelle génération

---

Réalisé par:

FARES Kacem

Soutenance le : 08/ 06 / 2022 devant le jury composé de :

Président	*MENASSEL Rafik*	*MCA*	*U-Tébessa*
Rapporteur	*METROUH Abdelmalek*	*MCA*	*U-Tébessa*
Examinateur	*SOUAHI Mohammed Salah*	*MCA*	*U-Tébessa*

Année universitaire : 2022/2023

REMERCIEMENTS

En premier lieu, Nous tenons à remercier notre DIEU, pour nous avoir la force pour accomplir ce travail.

Nous tenons à présenter nos remerciements à notre promoteur, **ABDELMALEK METROUH** qui nous a suivi et dirigé tout au long de la réalisation de ce travail, et qui a été d'une aide très précieuse sur le plan scientifique et moral.

Nous voudrions aussi remercier tous nos enseignants du département de Mathématique et informatique.

Nos derniers remerciements et ce ne sont pas les moindres, vont à tous ceux qui ont contribué de près ou de loin pour l'aboutissement de ce travail.

Et a toute la promotion de I2017/2018, je vous souhaite une bonne continuation dans votre vie personnelle et professionnelle

A la fin nous remercions les nombres jurys d'avoir acceptés d'examiner ce mémoire.

DEDICACE

Je dédie ce modeste travail :

À mon père.

À l'être le plus cher de ma vie, ma mère.

À mes frères et mes sœurs.

À toute ma famille qui a résisté à la souffrance d'être loin d'eux.

À tous mes amis et surtout.

À tous ceux qui ont semés le bonheur dans mon chemin.

À tous les enseignants d' Informatique

Et particulièrement mon encadreur : ABDELMALEK METROUH

FARES KACEM

Résumé :

Ce travail se concentre sur le développement d'un schéma d'intégrité distribuée adapté aux réseaux sans fil de nouvelle génération. Les réseaux sans fil ont connu une évolution rapide ces dernières années, avec l'émergence de la 5G et au-delà, offrant des vitesses de transmission plus rapides, une capacité accrue et une latence réduite. Cependant, cette expansion des réseaux sans fil avancés soulève des défis en matière de sécurité et de confidentialité, notamment en ce qui concerne l'intégrité des données échangées.

Traditionnellement, les schémas d'intégrité étaient mis en œuvre de manière centralisée, ce qui présente des limitations pour les réseaux sans fil de nouvelle génération distribués, évolutifs et hétérogènes. Ce mémoire examine les technologies et les protocoles existants liés à l'intégrité des données dans les réseaux sans fil, mettant en évidence les défis spécifiques et les besoins des réseaux sans fil de nouvelle génération.

En réponse à ces défis, ce mémoire propose un schéma d'intégrité distribuée novateur adapté aux réseaux sans fil de nouvelle génération. Ce schéma vise à surmonter les limitations des approches centralisées en permettant une vérification décentralisée de l'intégrité des données. Il repose sur des mécanismes de confiance et des protocoles de communication sécurisés pour garantir l'intégrité des données dans un environnement sans fil distribué et dynamique.

ملخص :

يركز هذا العمل على تطوير مخطط تكامل موزع مناسب لشبكات الجيل التالي الالسلكية. تطورت الشبكات الالسلكية بسرعة في السنوات

االخيرة، مع ظهور 5 Gوما بعده ، مما يوفر سرعات إرسال أسرع ، وقدرة أكبر ، وخفض زمن الوصول. ومع ذلك، فإن هذا التوسع في

الشبكات الالسلكية المتقدمة يثير تحديات من حيث االمن والسرية، ال سيما فيما يتعلق بسالمة البيانات المتبادلة.

تقليديًا، تم تنفيذ مخططات التكامل مركزًيا، مما يفرض قيوًدا على شبكات الجيل التالي الالسلكية الموزعة والقابلة للتطوير وغير المتجانسة.

تبحث هذه االطروحة في التقنيات والبروتوكوالت الحالية المتعلقة بسالمة البيانات في الشبكات الالسلكية، وتسليط الضوء على التحديات

واالحتياجات المحددة للشبكات الالسلكية من الجيل التالي.

استجابة لهذه التحديات، تقترح هذه االطروحة مخطط تكامل موزع مبتكر مناسب لشبكات الجيل التالي الالسلكية. يهدف هذا المخطط إلى

التغلب على قيود االساليب المركزية من خالل السماح بالتحقق الالمركزي من سالمة البيانات. يعتمد على آليات الثقة وبروتوكوالت االتصال

االمنة لضمان سالمة البيانات في بيئة السلكية موزعة وديناميكية.

Abstract :

This work focuses on the development of a distributed integrity scheme suitable for next-generation wireless networks. Wireless networks have evolved rapidly in recent years, with the emergence of 5G and beyond, offering faster transmission speeds, increased capacity and reduced latency. However, this expansion of advanced wireless networks raises challenges in terms of security and confidentiality, particularly with regard to the integrity of the data exchanged.

Traditionally, integrity schemes were implemented centrally, which presents limitations for distributed, scalable, and heterogeneous next-generation wireless networks. This thesis examines existing technologies and protocols related to data integrity in wireless networks, highlighting the specific challenges and needs of next-generation wireless networks.

In response to these challenges, this thesis proposes an innovative distributed integrity scheme suitable for next-generation wireless networks. This scheme aims to overcome the limitations of centralized approaches by allowing decentralized verification of data integrity. It relies on trust mechanisms and secure communication protocols to ensure data integrity in a distributed and dynamic wireless environment.

Table des matières

Table des matières

Liste des tableaux

Liste des abréviations

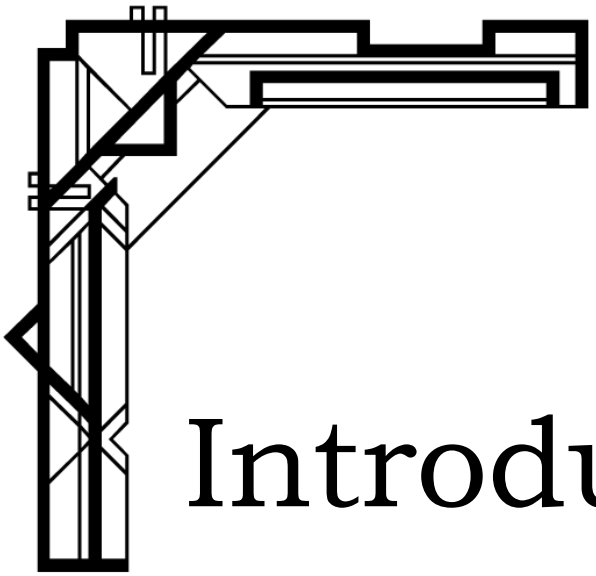
2G	Second Generation of cellular networks.
3G	Third Generation of cellular networks.
4G	Fourth Generation of cellular networks.
5G	Fifth Generation of cellular networks.
APR	Admissible Payload Rate.
BBU	Base Band Unit.
BFT	Byzantine Fault Tolerance.
BS	Base Station.
BSH	Blockchain-based Security and HO.
CDMA	Code Division Multiple Access.
CSWN	Communication System over a Wiretape Network.
D2D	Device to Device.
DN	Destination Node.
eMBB	Enhanced Mobile BroadBand.
ESR	Early Stage Researcher.
ETN	European Training Network.
H2020	Horizon 2020.
HMAC	Homomorphic MAC.
HO	Hand Over.
ITN	Innovative Training Network.
KDC	Key Distribution Center.
KEPTE	Key Predistribution-based Tag Encoding.

Liste des abréviations

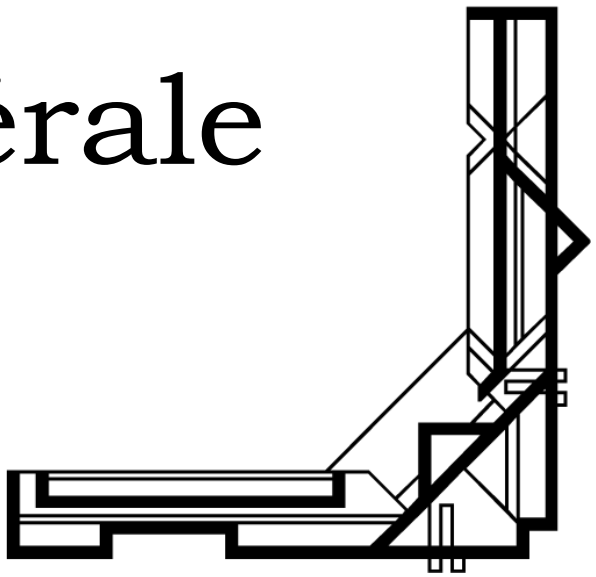
LTE	Long Term Evolution.
MAC	Message Authentication Codes.
M-BAT	Multi-level Binary Authentication Tree.
MH	Multi-Hop.
mMTC	Massive Machine Type Communications.
MP	Multi-Path.
MP-MH	Multi-path Multi-hop.
MSC	Mobile Small Cells.
MSCA	Marie Sklodowska Curie Actions.
NC	Network Coding.
NCC	Network Coded Cooperation.
NC-MSC	NC-enabled Mobile Small Cells.
NCS	Network Coding Signature.
NFV	Network Function Virtualization.
NR	New Radio.
OFDM	Orthogonal Frequency Division Multiple Access.
PoW	Proof of Work.
RLNC	Random Linear Network Coding.
RN	Relay Node.
SDN	Software Defined Network.
SECRET	SEcure Network Coding for Reduced Energy nexT genetation Mobile
SN	Source Node.

Liste des abréviations

TCP	Transmission Control Protocol.
TDMA	Time Division Multiple Access.
UE	User Equipment.
URLLC	Ultra Reliable Low Latency Communication.



Introduction générale



Au cours des dernières décennies, les réseaux sans fil ont connu une évolution significative, devenant une infrastructure essentielle pour la connectivité mondiale. Avec l'émergence des réseaux sans fil de nouvelle génération, tels que la 5G et au-delà, les possibilités de communication sans fil se multiplient, offrant des vitesses de transmission plus rapides, une capacité accrue et une latence réduite. Cependant, cette expansion et cette sophistication croissantes des réseaux sans fil apportent également leur lot de défis en matière de sécurité et de confidentialité.

Un aspect essentiel de la sécurité des réseaux sans fil réside dans l'intégrité des données échangées. L'intégrité garantit que les informations transmises n'ont pas été altérées ou modifiées de manière non autorisée. Traditionnellement, les schémas d'intégrité ont été implémentés de manière centralisée, où un point central vérifie l'intégrité des données échangées. Cependant, cette approche présente des limitations pour les réseaux sans fil de nouvelle génération, caractérisés par leur nature distribuée, leur évolutivité et leur hétérogénéité.

Dans ce contexte, ce mémoire de Master se concentre sur le développement d'un schéma d'intégrité distribuée spécifiquement conçu pour les réseaux sans fil de nouvelle génération. L'objectif est de concevoir un système robuste qui permette la vérification de l'intégrité des données de manière décentralisée, tout en prenant en compte les défis propres à ces environnements sans fil avancés.

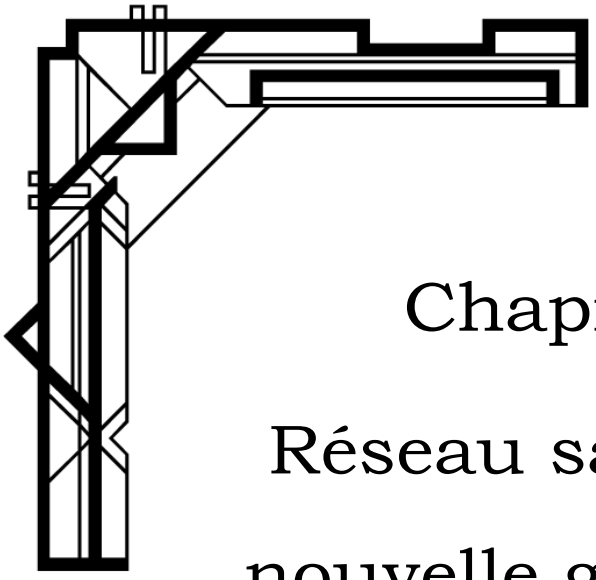
Ce mémoire se propose d'examiner en détail les technologies et les protocoles existants liés à l'intégrité des données dans les réseaux sans fil, en mettant l'accent sur leurs limitations actuelles et les besoins spécifiques des réseaux sans fil de nouvelle génération. Il explorera également les approches de conception distribuée et les mécanismes de confiance nécessaires pour garantir l'intégrité des données dans un environnement distribué et dynamique.

La contribution de ce mémoire consistera en la proposition d'un schéma d'intégrité distribuée adapté aux réseaux sans fil de nouvelle génération. Ce schéma cherchera à surmonter les limitations des approches centralisées tout en répondant aux exigences de sécurité, de confidentialité et de performance inhérentes à ces réseaux avancés.

En conclusion, ce travail vise à apporter une contribution significative à la sécurité des réseaux sans fil de nouvelle génération en proposant un schéma d'intégrité distribuée

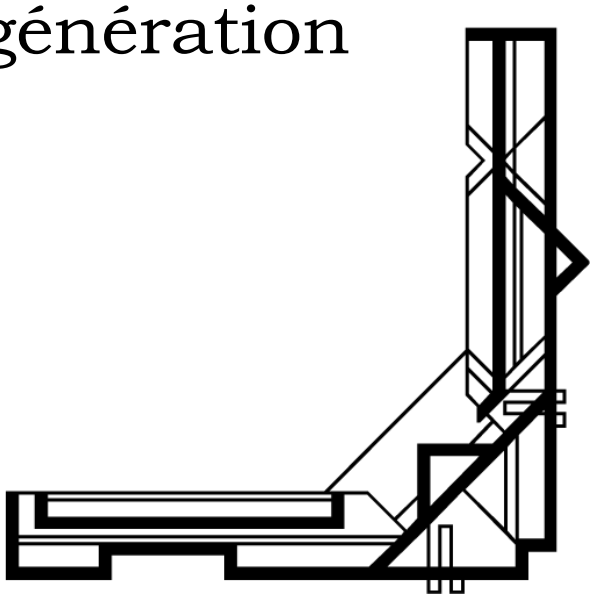
novateur. En permettant une vérification décentralisée de l'intégrité des données, ce schéma contribuera à renforcer la confiance dans les communications sans fil, ouvrant ainsi la voie à l'adoption et à l'expansion de ces réseaux avancés dans divers secteurs tels que les télécommunications, l'Internet des objets (IoT) et les villes intelligentes.

Ce mémoire est scindé en quatre chapitres. Le chapitre 1 est une introduction aux réseaux de future génération (B5G). Le chapitre 2 traite les approches de sécurité les plus avancées pour les environnements compatibles NC. Il traite des fonctionnalités de sécurité inhérentes au NC et des défis de sécurité généraux dans ces réseaux avant de décrire les défis de sécurité spécifiques du NC. De plus, la discussion axée sur les attaques par contamination et l'amélioration de l'intégrité échantillons contre les attaques de contamination. Le chapitre 3 analyse plus en détail les schémas d'intégrité avancés abordés dans le chapitre 2 concernant les futures exigences du réseau sans fil et identifie les lacunes de la recherche. Le chapitre 4 présente notre contribution .



Chapitre I:

Réseau sans fil de nouvelle génération



I.1. Introduction

Bien qu'il n'y ait pas de réponses directes à ces questions, à mesure que la technologie progresse, les deviendra plus clair sur où nous nous dirigeons. Alors que le monde se dirige vers réseaux sans fil de e génération (5G), l'infrastructure réseau traverse différents changements. La croissance sans précédent des appareils mobiles et le trafic de données a entraîné ces changements structurels dans l'environnement sans fil pour répondre aux besoins des utilisateurs. Pour atteindre une haute qualité de service Avec des besoins en puissance moindres, les nouvelles technologies de sont considérés comme faisant partie du système 5G. Le cryptage de réseau (NC)[1] est l'une de ces technologies qui est considérée comme très utile dans l'environnement 5G pour fournir une communication flexible dans un réseau avec perte sans l'énorme aérien. .De l'idée de mélanger les paquets en transit, NC a développé le comme un concept puissant pour optimiser les besoins en bande passante de la communication comme le ainsi que fournir la résilience du réseau [22]. Cependant, pour exploiter pleinement les avantages du cryptage réseau, nous devons relever les défis de sécurité qui y sont associés. La sécurité est une préoccupation majeure à l'ère de la 5G et de l'Internet des objets (IoT) [23], et la mise en œuvre de NC dans des applications du monde réel nécessite que les NC soient complètement protégés contre les cyberattaques. Dans cette thèse, nous nous concentrons sur schémas de cryptage de réseau sécurisés pour les futurs réseaux sans fil. Plus précisément, la mémoire se concentre sur les schémas d'intégrité contre les attaques de contamination, qui sont l'une des attaques les plus dévastatrices dans l'environnement de chiffrement de réseau, qui répondent aux exigences des réseaux. nouvelle génération. Ce chapitre présente les bases de la 5G réseau et plus, NC préliminaire et architecture générale de NC-base réseau de communication. En outre, certains des paramètres clés qui déterminent la pertinence des schémas de sécurité pour les futurs réseaux sans fil sont également abordés dans ce chapitre.

I.2. Réseaux 5G et au-delà

La cinquième génération de communication sans fil opère déjà dans divers domaine partie de la terre. Avec beaucoup de tests en direct et une mise en œuvre partielle, c'est Ce n'est qu'une question de temps avant le lancement des systèmes 5G commerciaux. Cependant, La cinquième génération de télécommunications sans fil diffère à bien des égards de la génération précédente. De la première génération de sans fil Nous n'avons constaté aucun changement majeur dans l'infrastructure de communication 3G Réseau sans fil en plus d'une capacité accrue. Bande aussi Utilisez la même bande basse. Au cours de la première et de la deuxième génération principalement axé sur la communication vocale avec une connexion Internet de base [24], La 3G se concentre davantage sur les communications multimédia telles que les photos et les vidéos Avec les appareils mobiles, cela augmente également les débits de données. La quatrième génération a été introduite pour améliorer encore ces services avec Long Term Evolution (LTE) pour fournir des connexions à haut débit. Cependant, avec la 4G, il y a eu une amélioration technologique majeure. Des bandes de fréquences moyennes ont été introduites dans le spectre et l'accès multiple par répartition orthogonale de la fréquence (OFDM) ont été utilisés pour faciliter le haut débit connectivité [26]. Avec LTE Advanced, nous avons presque épuisé l'optimum la capacité des réseaux 4G et divers services multimédias sont introduits dans le monde des réseaux mobiles. Jusqu'à la 4G, les forces motrices fondamentales derrière les changements n'ont pas changé de manière significative depuis la génération et sont restées simples améliorations apportées aux éléments RAN pour fournir des débits de données plus élevés et nous avons rarement remarqué une différence dans la philosophie de ces avancées. Cependant, la prochaine génération des communications sans fil ont suivi une philosophie d'évolution différente depuis les discussions initiales sur la normalisation. La 5G

introduira non seulement une plus grande capacité de communication de, mais aussi se concentrer sur divers aspects de la technologie sans fil, et introduira des changements significatifs dans l'infrastructure du réseau pour répondre aux besoins futuristes de dans le monde numérique en constante évolution. Évidemment, il comprend également des mesures pour améliorer la connectivité du réseau et les débits de données, mais prend également en compte d'autres aspects techniques tels que la latence, hétérogénéité, résilience, performance, etc. D'autre part, ce sera le premier changement de génération dans l'ère des communications sans fil. Où il y a, aucune nouvelle technologie d'accès ne sera introduite. Alors que la première génération était basé uniquement sur la technologie analogique, 2G utilisé Accès multiple par répartition dans le temps (TDMA) en Europe et aux États-Unis et dans d'autres pays en plus de Accès multiple par répartition dans le temps TDMA (CDMA). Avec la 3G, le CDMA a été défini comme une norme mondiale et la 4G a été introduite OFDM. À l'ère de la 5G, nous espérons continuer avec l'OFDM car c'est toujours le meilleur parmi les technologies d'accès disponibles. Le principal changement avec la 5G, comme nous en avons discuté dans, réside dans les nouveaux cas d'utilisation qu'elle définit et sur lesquels elle se concentre, et pas seulement dans les extensions de capacité. Selon l'Union internationale des télécommunications, il existe trois principaux cas d'utilisation sur lesquels les réseaux 5G se concentreront. Il s'agit du haut débit mobile amélioré (eMBB), Communications ultra-fiables à faible latence (URLLC) et type de machine massive Communications (mMTC) [27, 28]. Dans les développements actuels avec les tests 5G, les exigences d'eMBB et URLLC sont généralement satisfaits, mais Les applications mMTC ne sont toujours pas réalisées de manière satisfaisante dans les tests. L'eMBB peut être considéré comme le plus important progrès que nous avons vu dans la génération précédente développements et se concentre sur les connexions haut

débit mobiles à haute capacité, performantes et plus rapides Connexions. URLLC fait référence aux exigences des missions critiques réseaux avec un délai de bout en bout extrêmement faible pendant la communication. Les systèmes 5G visent à pour obtenir une communication de bout en bout avec un délai d'une milliseconde pour les services en temps réel. Le mMTC relève les défis de l'ère de l'IdO et la grande variété d'appareils pouvant être connectés via Internet. Ce cas d'utilisation 5G tente de fournir une connectivité pour un grand nombre d'appareils numériques, y compris des capteurs à ressources limitées et dispositifs. Dans le cadre de la 5G, le réseau d'accès radio intégrera pleinement le Wifi et d'autres protocoles de communication sans fil pour assurer la connectivité. En tant que tel, doit s'adapter à l'hétérogénéité non seulement dans la variété des dispositifs qui sert, mais aussi dans les diverses technologies qui relèvent du parapluie sans fil. La 5G est considérée comme une étape importante dans l'évolution de la technologie sans fil, car a de multiples dimensions où il prétend faire la différence. Comme déjà mentionné, la philosophie de cette prochaine génération est passée d'une simple expansion de capacité à d'autres aspects tels que la latence et la fiabilité lors de la connexion d'un grand nombre de dispositifs. L'efficacité énergétique est une autre préoccupation majeure dans la conception des réseaux 5G. De plus, en cette ère de cyber-risques accrus, la sécurité des réseaux sans fil est un point d'intérêt majeur pour. Pour répondre à ces préoccupations, la 5G les réseaux utilisent diverses techniques et de nouveaux concepts. Il étend même le spectre de fréquences qui fera partie des communications sans fil en incluant ondes millimétriques dans le scénario. La 5G propose également des logiciels et la virtualisation pour offrir aux opérateurs de réseau la flexibilité de relever les défis et de réorganiser le réseau en fonction de divers cas d'utilisation existants et futurs. Concepts tels que le matériel prêt à l'emploi avec la virtualisation des fonctions réseau

(NFV) et les solutions logicielles permettent également aux opérateurs de maintenir les coûts d'investissement et d'exploitation de à un faible niveau. Des idées telles que le cloud computing et l'informatique de périphérie mobile font partie intégrante des cas d'utilisation et des exemples de la 5G. Elle prend en charge le découpage du réseau, garantissant là Les ressources disponibles de, de la bande passante au matériel, sont utilisées de la manière la plus efficace. En outre, les réseaux 5G bénéficieront également de plusieurs nouveaux concepts tels qu'intelligence artificielle, blockchain, réseaux définis par logiciel (SDN) et NC. Même le l'infrastructure sans fil de a été repensée, modifiant structure cellulaire centrée sur la station de base que nous connaissons aujourd'hui à une approche centrée sur l'utilisateur environnement à petites cellules et structure cellulaire en couches qui prend également en charge les communications entre appareils Appareil sans intervention de la station de base. Plusieurs groupes de recherche étudient ces possibilités et proposent de nouvelles solutions technologiques pour la 5G et au-delà. Le réseau SECure Coding for Reduced Energy nouvelle génération mobile Small cellules (SECRET) [7] est l'un des consortiums du réseau européen de formation (ETN) en collaboration sous l'égide des projets Horizon 2020 étudiant les perspectives des techniques-Codage réseaux pour les petites cellules mobiles de nouvelle génération.

SECRET est un consortium MSCA-ITN, composé de 4, partenaires académiques et 4 partenaires industriels dans les cinq États membres de l'UE, formation de 13 Chercheurs en début de carrière (ESR) dans les réseaux et les communications sans fil est hautement interdisciplinaire et pluridisciplinaire. Le projet SECRET vise à combler le fossé entre les technologies de réseau et les besoins futurs prévus en matière de réseau en 2020 et au-delà. , pour offrir une meilleure connectivité réseau, la capacité de prendre en charge plus d'utilisateurs, un coût par bit inférieur, une efficacité énergétique améliorée et,

finalement, une évolutivité. au nouveau nature des services et des appareils (comme la prise en charge des villes intelligentes et de l'IoT). Étude dans SECRET s'appuie sur les tendances technologiques actuelles, largement acceptées comme dans le cadre de la 5G, vise à mettre en œuvre de nouvelles petites cellules basées sur Concept de petites cellules mobiles (MSC). La proposition va alors au-delà de la vision actuelle de la 5G petite cellule grâce à de nouveaux modèles révolutionnaires de type cellule féminine où les utilisateurs finaux agissent en tant que consommateurs de connectivité sans fil, que nous avons appelés Small Cell. À cette fin, SECRET vise à trouver un accès MSC universel basé sur l'exploitation de technologies telles que le cryptage du réseau et la collaboration en synergie avec le cadre de sécurité et communication. L'interface utilisateur intelligente économise de l'énergie. Ces petits points d'accès mobiles formeront un réseau sans fil de MSC afin que les consommateurs à la périphérie de la cellule ou dans les zones à faible couverture puissent accéder au réseau haut débit. Un autre aspect de l'innovation dans SECRET est la fourniture d'une liaison sans fil pour fournir une connectivité à haut débit et à faible puissance aux MSC. Figues. 1.1 décrit la SECRÈTE vision des réseaux de nouvelle génération, qui se décline principalement en quatre axes de recherche, et chaque aspect de la recherche analysé par un groupe de travail spécifique.

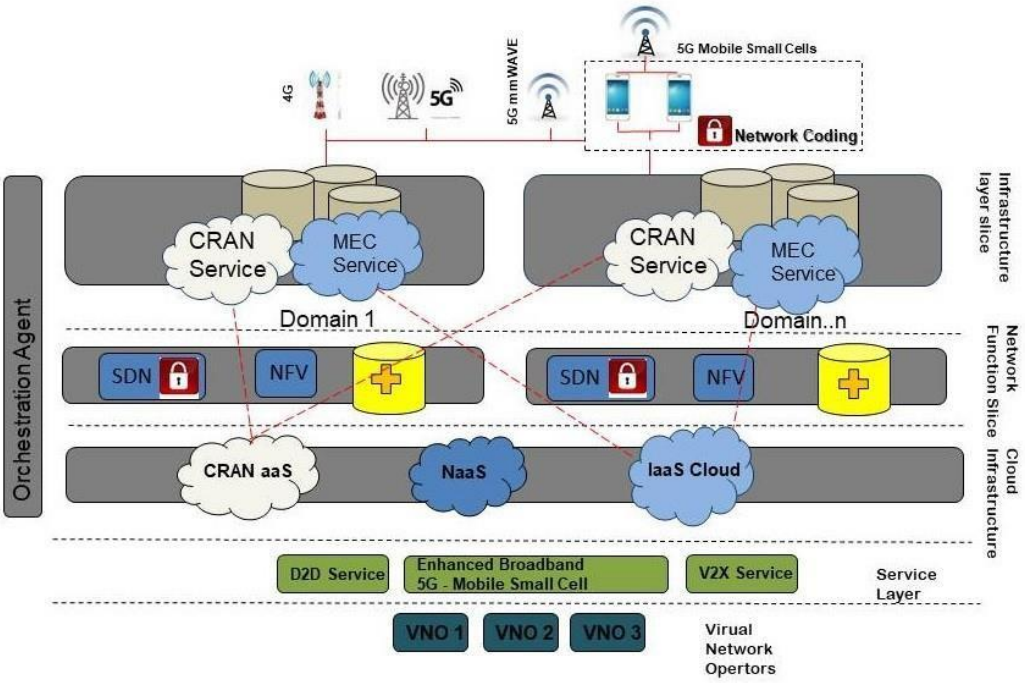


Fig. I.1. Vision SECRÈTE des réseaux de nouvelle génération

Le premier groupe se concentre sur la gestion des ressources radio pour les petites cellules SECRET. Conformément aux attentes du réseau 5G, SECRET s'efforce de répondre à l'hétérogénéité environnement de réseau (HetNet), où plusieurs technologies d'accès radio telles que LTE et WiFi coexisteront pour servir de multiples applications. et les appareils des utilisateurs. Ce groupe de travail se concentre également sur les réseaux Network Coding Cooperative (NCC) afin d'utiliser efficacement les ressources radio disponibles et d'assurer une haute qualité de service pour chaque utilisateur du réseau.

Un autre aspect important de la recherche dans SECRET est la sécurité des futurs réseaux, où la sécurité des petites cellules de nouvelle génération, intégrant la couche de cryptage du réseau, sera étudiée. Malgré Les énormes avantages de NC, en termes de bande passante, de consommation d'énergie et de résistance à la perte de paquets, le NC doit faire face à une foule d'attaques

de sécurité si le NC veut atteindre son plein potentiel. De celui-ci dans les systèmes de communication du monde réel. Ce groupe de travail cible la conception et la mise en œuvre de mécanismes et de schémas de chiffrement de réseau sécurisé efficaces pour atténuer de telles attaques dans le réseau MSC activés par le chiffrement de réseau envisagé.

L'efficacité énergétique et la technologie RF avancée sont des préoccupations majeures dans le monde d'aujourd'hui environnement sans fil. De plus, avec l'introduction des ondes millimétriques dans le spectre disponible, les équipements RF des systèmes 5G présenteront des différences significatives par rapport aux conceptions existantes. Un autre groupe de travail SECRET, Green RF pour les combinés 5G, se concentre sur le développement d'une interface utilisateur RF multimode à économie d'énergie pour la prochaine génération combiné. Le groupe de travail traite de la conception, de la simulation et de la mise en œuvre de solutions à faible coût et économes en énergie. Modules émetteurs-récepteurs RF, compris éco énergétiques l'amplificateur de puissance, le niveau de filtre RF multimode et l'antenne sont configurables.

Le dernier groupe de travail se concentre sur la preuve de concept de la technologie MSC, qui comprend non seulement une étude de faisabilité, mais est également complétée par des recherches spécifiques sur la façon dont la technologie des petites cellules peut être un tremplin pour la division. Partage de réseau sous forme de virtualisation de réseau. Ce groupe de travail fournira également les dorsales pour tester diverses solutions technologiques que d'autres chercheurs proposent dans qui permettent la virtualisation MSC et réseau. Ici, nous allons construire une zone de test de petites cellules prenant en charge différents types de données, en se concentrant sur la vidéo en temps réel qui est le cas d'utilisation le plus exigeant et le plus dominant dans le système 5G et agira comme un véhicule pour promouvoir des projets de

recherche collaboratifs ESR puisque les algorithmes eux-mêmes d'autres groupes de travail peuvent être testés et optimisés ici.

L'architecture de scénario commune du projet financé par l'UE H2020-MSCA SECRET [7] décrit un réseau de communication basé sur NC. La figure 1.2 montre un modèle réseau constitué d'un certain nombre de petites cellules au service de l'utilisateur final. La mini des cellules sont connectées au backbone et à Internet avec l'infrastructure existante des macro cellules disposent également d'un contrôleur SDN centralisé pour la gestion du réseau. Les mini-cellules sont également appelées points d'accès mini-cellules car elles agissent comme des points d'accès pour connecter le réseau aux nœuds dans leur zone de couverture. Les microcellules peuvent également être mobiles et connectées au contrôleur central de la microcellule. De plus, les nœuds du réseau ont également communication edgeband activée, ce qui signifie qu'ils peuvent communiquer directement avec les appareils voisins. Dans un environnement de collaboration, la communication multi-sauts multi- chemins (MP-MH) peut être efficacement réalisée entre nœuds de réseau à l'aide Communication d'appareil à appareil (D2D) [29, 30] et réaliser ainsi une haute résolution intelligente. - connexion rapide.

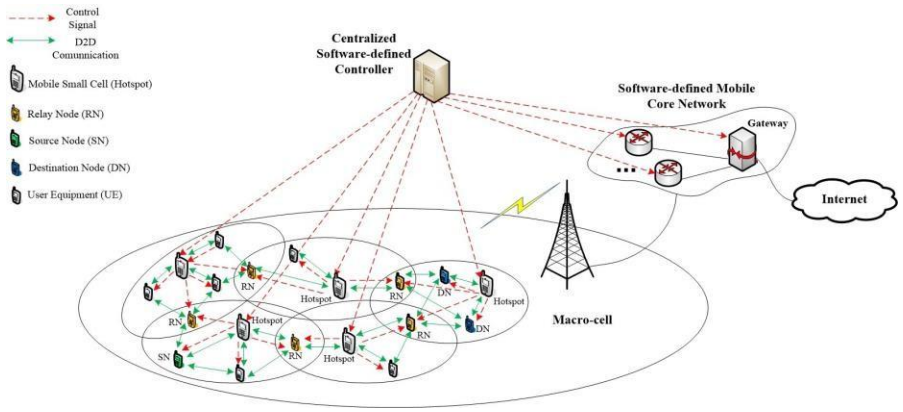


Fig. I.2. Architecture générale des scénarios de SECRET

En plus de ces innovations, NC peut encore améliorer l'utilisation efficace des ressources du réseau. L'utilisation de NC améliorera l'utilisation de la bande passante et, dans un réseau sans fil avec perte l'environnement, il peut également réduire les transmissions, améliorant ainsi l'efficacité énergétique des systèmes. De plus, la résilience et la fiabilité du réseau peuvent être améliorées par NC.

Supposons qu'un nœud mobile veuille partager un fichier multimédia avec deux autres nœuds mobiles. Le nœud mobile est propriétaire du fichier multimédia, le nœud source (SN), envoie ce fichier aux nœuds mobiles demandant le fichier, nœud de destination (DN). Notez que ces nœuds mobiles ne doivent pas nécessairement être dans le même MSC, comme illustré en 1.2. Grâce à la communication D2D, le fichier multimédia est acheminé dans Mode MP-MH, via le petit réseau cellulaire du SN jusqu'au DN. L'architecture de scénario proposée de la prochaine génération le réseau sans fil prend en charge NC, comme illustré à la Fig. 1.2 prend en compte divers secteurs verticaux tels que MSC, NC et D2D communications et présente de nombreux avantages par rapport aux architecture actuellement utilisée.

En activant la communication D2D multi-sauts, le trafic de données dans ce cas n'a plus besoin d'être acheminé via la station de base (BS). Cela signifie que les données ne sont plus nécessaires pour parcourir de longues distances vers et depuis BS, mais ont un impact plus direct itinéraire. Cela réduit considérablement la latence. Depuis que le lien voyage sur des distances plus courtes, il nécessite moins d'énergie pour atteindre sa destination. Cela signifie que cette architecture permet également une transmission de données plus économe en énergie. Cette architecture réduit également la charge de travail BS, ce qui réduit la pression sur le réseau

mobile. Cette architecture commune est considérée comme la base de notre travail, et ses différentes déclinaisons sont utilisées pour décrire les schémas d'intégrité spécifiques que nous proposons dans les chapitres suivants.

I.3. le codage réseau et ses préliminaires

Le codage en réseau est une branche scientifique relativement jeune dans le domaine de la théorie des réseaux, qui a été identifiée dans un travail fondateur par Ahlswede et. al [1] en 2000. Bien que le concept de NC existe beaucoup plus tôt [31], les avantages de la NC ont été bien étudiés depuis lors. L'idée de base de NC est de permettre aux nœuds intermédiaires pour effectuer des opérations linéaires sur les paquets qu'ils reçoivent sur leurs bords entrants et pour envoyer ces paquets chiffrés sur leurs bords sortants, au lieu de simplement retransmettre les paquets sur nombre de paquets à envoyer sur le canal et aide le atteindre les performances maximales promises par le théorème de coupe minimale de débit maximal [32]. La recherche et la discussion initiales sur NC ont été expliquées avec un simple exemple d'un réseau papillon effectuant une addition X-OR sur les paquets, comme illustré à la Figure 1.3. Dans l'exemple donné, chaque bord ou canal a une limite supérieure de bits à la fois, et la combinaison d'informations dans le nœud D atteint l'efficacité optimale pour envoyer des paquets de la source A aux destinations E et F. En outre, évolué à partir de la base en ajoutant deux paquets pour encoder plusieurs paquets et envoyer des épreuves numériques au lieu de paquets entiers. Cela améliore considérablement l'efficacité de la bande passante du réseau. Le codage de réseau linéaire augmente également la résilience et l'adaptabilité aux influences environnementales [33]. Bien que le NC essaie d'obtenir les meilleures performances d'utilisation de la bande passante en envoyant des paquets de combinaisons sur différents canaux, il permet également certains ajustements de masquage et donne la certaine résistance aux attaques d'intermédiaires. Cependant, NC seul n'offre qu'une

faible sécurité [34]. Le codage réseau [1] s'avère être un bon candidat pour permettre aux petites cellules de travailler ensemble pour fournir plus de bande passante dans le réseau. En plus du codage de réseau linéaire aléatoire (RLNC) [35], est également très bien adapté aux environnements sans fil avec une topologie instable. Dans un environnement collaboratif, le peut atteindre la limite supérieure des performances de multidiffusion. Réseaux futurs avec des environnements à petites cellules avec la communication D2D et un environnement de dispositif coopératif s'efforcent de garantir que chaque utilisateur du réseau

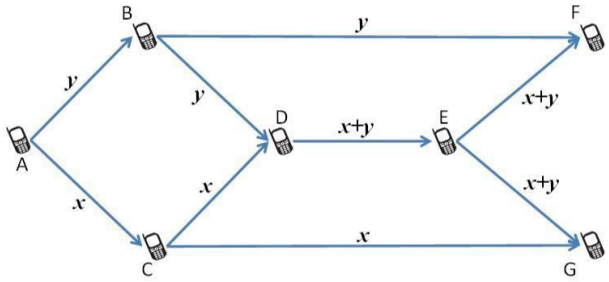


Fig. I.3. Réseau Butterfly présentant les concepts de codage de réseau

Recevront équitablement les services nécessaires [36, 37, 38]. Dans un environnement coopératif comme le montre la figure 1.4, le récepteur reçoit une partie du flux du canal et coopère avec les nœuds voisins pour générer les informations complètes. Cela améliore l'efficacité de la bande passante du système par rapport au réseau actuel basé sur LTE sans coopération, comme le montre la figure 1.5.

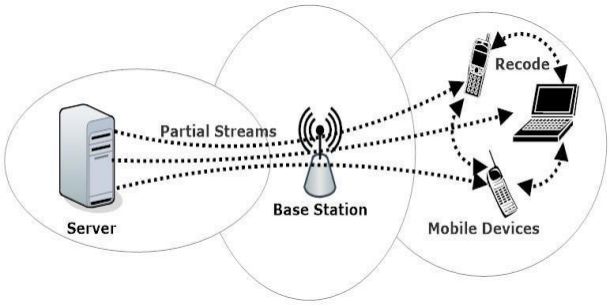


Fig. 1.4. Scénario de coopération codée en réseau

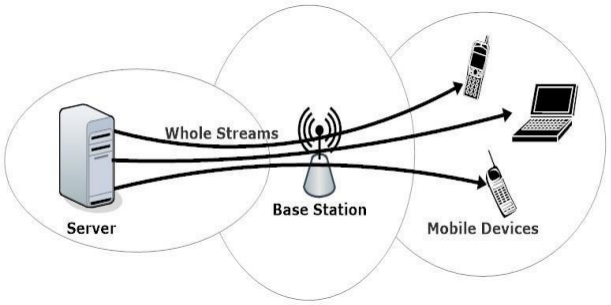


Fig. I.5. Pas de scénario de coopération

Avant de discuter davantage des défis de sécurité des protocoles compatibles NC, cette section introduit quelques concepts préliminaires sur les différents protocoles NC. Partant du concept de base d'addition modulo de deux flux d'information, NC a évolué vers différents protocoles détaillés adaptés à différents conditions du réseau et différents types d'applications. En général, on peut les diviser en deux catégories basées sur la connaissance de l'état du réseau des nœuds, telles que le protocole NC conscient de l'état et le protocole NC sans état [39]. Dans les protocoles NC conscients de l'état, tels que COPE [40], les nœuds participants se font une idée de la topologie du réseau et utilisent ces informations pour améliorer les performances en termes de débit et d'endurance. Les protocoles NC conscients de l'état sont très efficaces car les nœuds ont connaissance du l'état de leurs voisins et la topologie du réseau, mais cette dépendance à l'égard topologie du réseau.

Rend également le système plus vulnérable aux attaques telles que trous de ver, trous noirs et écoutes téléphoniques. COPE est l'un des protocoles NC bien connus basés sur l'approche de codage opportuniste et plusieurs autres tels les protocoles sont discutés dans [41, 42, 43].

Les protocoles NC sont conscients d'un état approprié si les conditions du réseau sont presque stables. Cependant, dans les réseaux sans fil avec de nombreux appareils mobiles, cette situation est difficile à atteindre. De plus, la dépendance les protocoles de communication sur l'état et la topologie du réseau entraînent également des failles de sécurité. Les protocoles NC sans état tels que le cryptage réseau aléatoire [35] sont plus appropriés pour réseaux sans fil. Dans les protocoles NC sans état, le mélange et le cryptage des paquets sont indépendants de la topologie du réseau. Ces protocoles n'attendent aucune condition de réseau particulière et cryptent les paquets car si un nœud reçoit un nombre suffisant des paquets individuels de n'importe quel lien entrant, quel que soit l'état du réseau, les destinataires pourront déchiffrer les paquets. Les protocoles NC sans état sont idéaux pour les topologies dynamiques, telles que les réseaux ad hoc mobiles. Cela rend également les protocoles NC sans état plus adaptés aux futurs réseaux sans fil. Étant donné que ces protocoles sont indépendants des conditions du réseau, ils offrent également une meilleure immunité aux à de nombreux problèmes de sécurité. Cependant, cela nécessite également plus de complexité opérations de chiffrement que les protocoles conscients de l'état. De plus, ces NC les opérations doivent être effectuées dans un champ fini relativement plus grand pour s'assurer que les opérations de chiffrement et de déchiffrement sont effectuées de manière sûre et efficace. Cela introduit un petit coût supplémentaire en termes d'exigences de calcul et de communication pour les systèmes utilisant le protocole NC sans état. RLNC [4] est le protocole NC sans état le plus courant et le plus populaire. RLNC devient l'un des systèmes

les plus efficaces et les plus adaptés aux réseaux sans fil prenant en charge NC. Il permet aux nœuds de chiffrer paquets utilisant des coefficients aléatoires générés localement et transmis paquets. Il réduit également le besoin de chemins prédéfinis, ce qui le rend bien adapté aux environnements sans fil. Dans les réseaux basés sur RLNC, les paquets initiaux de sont ajoutés avec un facteur aléatoire. Ces coefficients aléatoires agissent comme un clé pour déchiffrer les paquets d'origine. Ainsi, le décodage d'un paquet RLNC devient un problème de résolution d'un ensemble d'équations avec un nombre fixe de variables. Il améliore également la correction de suppression car le récepteur peut décrypter les paquets si un nombre spécifique de paquets cryptés est reçu. Ces avantages de RLNC en font le plus approprié candidat pour les futurs réseaux de communication mobile.

Une autre classification du système NC est basée sur le mélange de paquets dans des nœuds intermédiaires. Lorsqu'il y a plus d'un SN dans le réseau, il y a possibilités de flux d'informations multiples passant par un nœud particulier. En fonction de la manière dont les opérations de cryptage réseau sont effectuées sur plusieurs flux, il existe une autre classification des protocoles NC en tant que cryptage réseau inter-thread et cryptage réseau intra-flux. Dans le chiffrement intra-flux, les nœuds intermédiaires effectuent uniquement chiffrement du réseau sur des flux individuels [44, 45, 46]. Cela signifie que seuls les paquets provenant du même source sont pris en compte pour le chiffrement aux nœuds intermédiaires. Cependant, dans les schémas de chiffrement de réseau inter-thread, les paquets provenant de plusieurs flux sont mélangés lors du recodage aux nœuds intermédiaires comme indiqué dans divers schémas tels que [47, 48, 49]. Cela peut cependant améliorer l'efficacité du cryptage, ce qui rend le système très complexe et extrêmement difficile d'identifier les menaces de sécurité. Dans le Protocoles inter-flux NC, les paquets provenant de différentes sources sont cryptés ensemble, ce qui

nécessite un système hautement sécurisé et authentifié environnement. De plus, il rend même l'homomorphe schémas de signature [50] couramment utilisés avec cryptage intranet pour garantir l'intégrité des paquets qui est invalidée par plusieurs sources générant paquets dans un seul paquet crypté.

Les futurs réseaux sans fil impliquent davantage d'appareils mobiles et de topologies dynamiques. De petites cellules autonomes et des appareils hautement mobiles font de la topologie du réseau imprévisible. De plus, le grand nombre d'appareils dotés d'une identité numérique compliquent également l'authentification et garantissent un environnement de confiance privilégié. L'usurpation d'identité et la gestion de l'identité dans les environnements IoT [23] présentent également certains défis pour garantir un environnement sécurisé et authentifié, comme la priorisation du 1087 par les profils chiffrement inter-flux. Par conséquent, dans la prochaine section de ce travail, nous nous concentrerons principalement sur Approches de filetage interne basées sur RLNC, sauf indication contraire. Cela aide également trouver un équilibre entre la sécurité du système et la complexité des opérations de cryptage.

a. Codage de réseau linéaire aléatoire :

En RLNC, un message est considéré comme un ensemble de paquets et des opérations de chiffrement sont effectuées sur chaque paquet. Concrètement, un ensemble de paquets appelé comme une génération sont considérés ensemble et le chiffrement est effectué sur une seule génération. Chaque paquet peut être représenté comme un vecteur de n élément est défini sur un corps fini F n q où q est la taille du champ. Plus la taille du champ augmente, plus la complexité de calculs augmente, mais cela augmente également la probabilité d'un décodage réussi. Un champ fini de 2 8 est généralement considéré comme suffisamment réaliste, et faits sont basés sur

ce compromis. Si l'on considère une génération de m paquets, où chaque paquet de a n symboles, alors chaque paquet de Pi dans cette génération peut être considéré comme {Pi, 1, Pi, 2 Pi,n} et la génération aura un air comme la matrice m×n P :

$$\begin{bmatrix} P_{1,1} & \cdots & P_{1,n} \\ \vdots & \ddots & \vdots \\ P_{i,1} & \cdots & P_{i,n} \\ \vdots & \ddots & \vdots \\ P_{m,1} & \cdots & P_{m,n} \end{bmatrix}$$

Dans l'approche RLNC habituelle (sans souci de sécurité), cette génération originale sera multiplié par une matrice de coefficients générés aléatoirement α est la matrice m×m pour générer la matrice codée P' comme indiqué dans l'eq.1.2 et la génération améliorée sera cette nouvelle matrice jointe à la matrice des coefficients de [α P'].

$$P' = \begin{bmatrix} \alpha_{1,1} & \cdots & \alpha_{1,m} \\ \vdots & \ddots & \vdots \\ \alpha_{i,1} & \cdots & \alpha_{i,m} \\ \vdots & \ddots & \vdots \\ \alpha_{m,1} & \cdots & \alpha_{m,m} \end{bmatrix} \times \begin{bmatrix} P_{1,1} & \cdots & P_{1,n} \\ \vdots & \ddots & \vdots \\ P_{i,1} & \cdots & P_{i,n} \\ \vdots & \ddots & \vdots \\ P_{m,1} & \cdots & P_{m,n} \end{bmatrix}$$

Cette génération de booster sera transmise sur le canal de communication sous la forme d'un mot de code (paquet amélioré). Lorsqu'un nœud intermédiaire reçoit suffisamment mots de code linéairement indépendants pour régénérer la génération, elle peut être recodée en multipliant la génération reçue par ses coefficients générés localement. Considérer que R est la matrice reçue par le nœud intermédiaire. Dans un milieu sans perte, R = [α P']. Si β est la matrice m × m de coefficients générée localement dans le nœud récepteur, alors le recodage se produit comme β × R et cela agira comme la prochaine génération de codé .Au nœud récepteur, le

message final sera décodé si au moins m nombre d'équations indépendantes sont reçues, par élimination gaussienne.

I.4. Paramètres clés et indices de performance

Les futurs réseaux de communication devraient gérer un réseau dense d'appareils mobiles avec des capacités et des exigences dynamiques. L'hétérogénéité des réseaux sera multidimensionnel ; il varie en termes de capacité de calcul, de disponibilité de la mémoire, de technologies d'accès radio, d'exigences d'application, de mobilité et de ressources requises de. De plus, dans l'environnement des petites cellules, le l'architecture du réseau peut varier même pendant la communication. Dans un environnement aussi dynamique, les défis sécuritaires se multiplient également. Chaque schéma de sécurité pour un environnement MSC a pour répondre à certaines exigences supplémentaires en plus des problèmes de sécurité.

a. Scalabilité :

L'environnement sans fil est soumis à des changements fréquents. Appareils participants se déplacent et la dynamique du réseau change très fréquemment de forme. Aussi, périphériques se déplaçant d'une petite cellule à une autre, ou rejoignant et quittant le réseau, rendre le réseau imprévisible. De plus, il exclut toutes les conditions initiales prédéfinies ou dures pour un schéma de sécurité. Tout système de sécurité ou d'intégrité pour un L'environnement MSC doit prendre en compte les défis des nœuds mobiles ainsi que la variation des topologies du réseau. Par exemple, vous ne pouvez pas compter sur une pré-distribution stricte clés pour assurer la sécurité. Il devrait également être en mesure d'accueillir de nouveaux nœuds pour rejoindre le réseau tout en communiquant, et fonctionnera de manière transparente le cas échéant les nœuds quittent le réseau pendant le processus.

Le système devrait fonctionner sans heurts avec seulement quelques participants et être capable de gérer un réseau sans aucun problème.

b. Surcharge :

Les schémas de sécurité créent toujours une surcharge du système. Garder ces frais généraux au minimum est une considération clé lors de la conception de tout schéma d'intégrité. Divers frais généraux doivent être pris en compte au cours du processus, principalement les frais généraux de communication, de calcul et de stockage. La surcharge de stockage est principalement due aux clés supplémentaires que chaque nœud doit stocker pour effectuer la Processus de vérification. Une surcharge de communication ou de bande passante se produit en raison de l'information nécessaire pour traverser le canal de communication. Plus le nombre de bits utilisés pour assurer la sécurité, moins la bande passante du système est efficace. Il convient également de noter que si un autre canal fixe est utilisé pour les informations relatives à la sécurité du, il sera utilisé dans le calcul de congestion et ne pourra pas être pris en compte puisqu'un autre canal fixe est utilisé pour envoyer ces signaux. La surcharge de calcul dû aux schémas d'intégrité est généralement due aux opérations supplémentaires sur les tableaux finis requis par les schémas d'intégrité. En général, dans les schémas basés sur le code d'authentification de message (MAC), les coûts de calcul sont mesurés en termes de les multiplications de champs finis, qui génèrent un surcoût important, et les additions sont considérées surcoût négligeable. Dans les schémas basés sur des signatures homomorphes, les exponentiations finies de champs sont nécessaires pour effectuer les vérifications, et ceux-ci ont une complexité de calcul plus élevée que les multiplications. Au cours des tests de performance, ces frais généraux sont mesurés à l'aide de tels relations

mathématiques ou comme temps de traitement consommé par des opérations supplémentaires. La dépendance de cette surcharge au nombre d'utilisateurs, le cas échéant, conduit également à des problèmes d'évolutivité, qui sont discutés dans certains des schémas discuté dans les sections suivantes.

c. latence :

La communication à faible latence est l'un des principaux objectifs de la 5G et des futurs réseaux. La latence de bout en bout dans la communication ne devrait être que de quelques millisecondes au cours des prochaines générations. Tout retard de calcul ou de communication important dans le cadre du programme d'intégrité peut avoir un effet négatif sur la latence de bout en bout du réseau. De plus, les régimes qui dépendent de l'asymétrie temporelle introduit également un certain retard dans l'achèvement de la communication. En plus de la latence, est également considéré comme un retard dans l'initialisation de tout nœud avec le réseau pendant études, par ex.

B. Pré-distribution des clés. Si le processus d'initialisation peut être effectué sans tenir compte de la topologie du réseau lors de la fabrication de l'appareil, elle est alors omise du calcul du délai d'initialisation. De manière générale, le RLNC peut répondre faibles exigences de latence par rapport au protocole TCP (Transmission Control Protocol) connexions dans un environnement avec pertes. Depuis en NC l'ordre des paquets n'est pas important et un nombre suffisant de des paquets innovants peuvent être utilisés pour décoder les informations, la latence globale de communication peut être considérablement réduite en mettant en œuvre RLNC. De plus, dans un environnement réaliste, un nombre supplémentaire de messages cryptés aléatoirement les paquets peuvent être envoyés de manière proactive en fonction du canal qui perd sans attendre un accusé de réception. Ainsi, l'utilisation de RLNC elle-même améliore la latence du réseau. Par conséquent, dans nos études, la latence supplémentaire due aux schémas

d'intégrité n’est pris en compte que lors de l'analyse. Cependant, ce supplément la latence dépend également de la puissance de traitement et est directement proportionnelle à la frais généraux, il ne peut pas être discuté séparément mais rapporté avec l’aérien. Du point de vue de la conception de tout schéma de sécurité, ces trois exigences et leur interdépendance Sont très importants. Le surcoût peut aussi dépendre de la topologie et varie en fonction du nombre d'utilisateurs sur le réseau. Par conséquent, la taille du réseau affecte également les limites globales. Dans cette thèse, nous nous concentrons sur ces indices de paramètres clés pour évaluer nos propositions de NC sécurisés et discuter de la façon dont chaque schéma est adapté aux futurs réseaux sans fil.

Chapitre II :

Codage de réseau sécurisé et schéma d'intégrité de pointe

II.1. Introduction

Alors que Network Encryption (NC) fournit des communications efficaces en bande passante et hautement résilientes, il crée également de nouvelles vulnérabilités dans les systèmes de sécurité. Les défis de sécurité en NC ont été étudiés pour la première fois dans [53] en 2002. Schéma NC sécurisé pour les systèmes de communication filaires (CSWN). Ils ont analysé la sécurité du chiffrement linéaire sur un réseau d'écoute où l'un des liens était compromis par l'auditeur et ont proposé une condition suffisante pour un chiffrement linéaire sécurisé et déchiffrable. Système de cryptage du réseau. D'accord C'est l'un des premiers travaux à combiner NC avec la sécurité de l'information. Depuis lors, il y a eu beaucoup de recherches sur l'analyse de la sécurité des programmes NC. Comme démontré dans, [53] le chiffrement linéaire lui-même offre une certaine sécurité contre les écoutes clandestines, mais il souffre également d'autres problèmes de sécurité. Certains de ces défis, tels que les attaques contaminantes, sont extrêmement graves dans le scénario NC par rapport aux réseaux commutés conventionnels, car les paquets de transfert sont chiffrés sur nœuds intermédiaires. Dans ce chapitre, nous analysons certains des défis de sécurité communément connus du point de vue de l'environnement cryptographique en réseau en résumant certains des travaux existants sur la sécurité NC [54,55,56] et discutons également de l'attaque par contamination comme un cas particulier de défis de sécurité. Une grande partie de ce chapitre est adaptée de la publication de l'auteur [8].

II.2. Défis de l'écoute clandestine

L'un des plus grands défis de sécurité dans un environnement sans fil est l'écoute clandestine ou l'écoute électronique. Répond à un attaquant qui a compromis un lien et écoute les paquets envoyés sur ce lien. Cette attaque passive sur les informations envoyées sur des liens compromis est courante dans les environnements sans fil. Selon les capacités des liens ou des nœuds attaqués, la gravité des attaques peut aller de la récolte partielle de contenu à l'interception, messages vitaux, clés et autres informations précieuses. Plusieurs publications antérieures ont discuté de la réponse des systèmes NC au cognement [57,34]. Dans l'environnement NC, l'écoute clandestine simple est rendue plus difficile par la transmission de paquets cryptés. Dans le cas des protocoles NC sans état en particulier, l'écoute clandestine d'une connexion ou d'un nœud spécifique peut ne pas aider un attaquant à obtenir des informations utiles. Par exemple, dans RLNC, les paquets sont chiffrés avec des coefficients aléatoires et envoyés sur des canaux aléatoires, donc la capture de paquets monocanal n'aidera pas un attaquant à déchiffrer des informations utiles[53,2]. Ainsi, le NC

fournit intrinsèquement une faible sécurité contre les écoutes clandestines. D'autres améliorations dans la prévention des écoutes clandestines NC sont explorées dans divers articles [2, 58,59].

II.3. Prévention de l'analyse du trafic et schémas de chiffrement

Une autre attaque passive courante sur les réseaux sans fil est la surveillance et l'analyse du trafic où un nœud adverse essaie d'analyser le trafic de données pour trouver les tendances du trafic et des informations sur la topologie participante et du réseau. Autoriser les nœuds intermédiaires à rechiffrer les paquets entrants rend difficile d'empêcher l'analyse du trafic dans un environnement de réseau chiffré. Cependant, un schéma de chiffrement approprié aidera à protéger la confidentialité du nœud. De plus, les apatrides Les schémas NC ne fournissent pas beaucoup d'informations sur la topologie du réseau, ce qui rend l'attaque insignifiante. Plusieurs schémas ont étudié l'impact de l'analyse du trafic dans les environnements NC et ont suggéré des schémas efficaces pour prévenir de telles attaques [60, 61,62].

Bien que le chiffrement du réseau offre une meilleure sécurité que les schémas de routage hérités contre les attaques passives, les effets des attaques actives telles que la modification byzantine peuvent être très dangereux pour les réseaux basés sur NC. Les schémas NC permettent aux nœuds intermédiaires de recoder et de mélanger les paquets à la volée, ce qui rend difficile de déterminer si l'activité d'un nœud est légitime. Dans les réseaux routés traditionnellement, toute modification des paquets en transit peut être considérée comme une activité malveillante, où la modification NC des paquets en transit constitue l'essence du paquet chose. Par conséquent, les attaques actives qui perturbent directement les opérations du réseau ou les paquets en transit deviennent dangereuses dans l'environnement NC [55]. Différents types d'attaques par déni de service (Dos) peuvent cibler des modèles NC et destructeurs. Refuser à un ou à un petit groupe de nœuds de participer au protocole de communication peut ne pas avoir d'impact significatif sur le protocole NC sans état, mais comme le volume de les attaques augmentent, le nombre de les paquets reçus au puits diminueront et peuvent entraîner des paquets d'état insuffisants pour décoder correctement les informations. Les attaques Dos dans les environnements NC sont étudiées en détail par [63] et certains schémas courants de déni de service pour les réseaux sans fil sont discutés dans [64, 65,66]. De plus, le brouillage représente également le Dos dans les réseaux sans fil. Dans l'environnement NC, le brouillage d'un nœud peut être facilement réalisé en lui envoyant un grand nombre de paquets depuis différents nœuds antagonistes. Il sera également difficile pour le nœud intermédiaire de savoir quel package est

authentique et doit être utilisé pour créer son propre package chiffré. Cependant, il n'est pas si important de ne pas transférer de paquets pour empêcher le flux de paquets dans un environnement NC car les paquets sont reçus différents canaux entrants et la plupart du temps aucun canal particulier ne sera particulièrement important. Cependant, l'envoi de ces paquets usurpés pour brouiller un nœud peut également entraîner l'épuisement des ressources et empêcher le nœud de s'engager dans la communication [67, 68,69].

II.4. Attaques entropiques et impact sur l'efficacité des schémas et prévention

Une autre attaque majeure dans l'environnement NC concerne l'entropie des paquets envoyés. En particulier avec les schémas de chiffrement de réseau linéaire, les nœuds récepteurs nécessitent un nombre suffisant de paquets d'amélioration reçus au niveau du puits pour décoder correctement les paquets. À mesure que le nombre de paquets non renouvelés reçus augmente, l'efficacité du schéma diminue et les ressources sont gaspillées. Une attaque d'entropie se produit lorsqu'un nœud attaquant, principalement un nœud interne, envoie à plusieurs reprises des messages valides mais non renouvelables paquets sur ses liaisons sortantes. Cela conduit à l'épuisement des ressources au niveau des nœuds de réception et réduit l'efficacité du schéma. Cela peut être plus grave si ces paquets peuvent être renouvelés vers un voisin direct mais sont inutiles pour un nœud sur le chemin de communication, connu sous le nom d'attaque d'entropie globale. Newell et al. [70] simule des attaques d'entropie et fait la distinction entre l'entropie locale où les paquets ne se renouvellent pas pour le nœud en aval immédiat, et l'entropie globale où les paquets se renouvellent pour le nœud immédiat mais constant pour le nœud aval distant. Plusieurs autres études ont également été menées sur les attaques entropiques sur les NC [71,72].

II.5. Attaques de fabrication et de contamination byzantines

L'artisanat et la modification byzantine sont les attaques les plus courantes et les plus actives dans l'environnement NC. Dans les attaques de fabrication byzantine, l'attaquant génère des paquets avec un contenu invalide et les transmet sur le réseau. Il peut également s'agir de faux en-têtes invalides tels qu'un débordement de table de routage, un empoisonnement de route ou une pollution ACK [73, 74, 75, 76]. Les attaques de modification ou de contamination byzantines sont les plus dangereuses et les plus courantes parmi les différents défis de sécurité cryptographique [54]. En outre, est l'un des défis de sécurité les plus recherchés spécifiques aux environnements NC. Dans les attaques de contamination, les nœuds internes malveillants effectueront des opérations de chiffrement incorrectes et enverront des paquets invalides sur les liaisons en aval. Cela

entraînera le décodage de paquets incorrects au niveau du récepteur et annulera toute performance de débit obtenue par le NC. Cependant, il n'est pas possible d'empêcher des nœuds intermédiaires de chiffrer les paquets qu'ils ont reçus, évitant ainsi des attaques polluantes difficiles. les attaques de contamination seront épidémiques si elles ne sont pas contrôlées au nœud dès que possible. Lorsqu'un paquet contaminé est introduit dans le réseau, il peut se répandre sur tous les chemins qu'il parcourt et réduire les performances de débit d'un facteur deux. De plus, avec les réseaux inter-threads, cela devient plus compliqué car aucun nœud ne peut être totalement fiable et le mélange de différents flux rend très compliqué la détection des paquets contaminés.

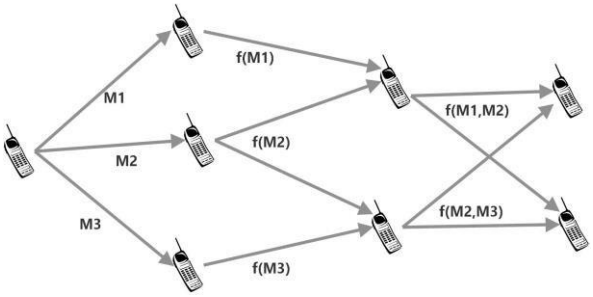


Fig II.1. Scénario bénin

Cependant, nous avons limité nos études uniquement aux protocoles NC in-stream, comme mentionné précédemment. Permettre aux nœuds intermédiaires de mélanger et de crypter les paquets se traduit par un tout nouveau paquet en transit avec des informations sur les paquets d'origine. Cela contredit complètement les bases des schémas d'intégrité les plus couramment utilisés. De plus, l'authenticité et l'authenticité des nœuds intermédiaires sont remises en question. Si un nœud intermédiaire insère un paquet malveillant dans le processus de chiffrement, les nœuds de réception ne seront pas en mesure de déchiffrer les paquets d'origine même s'ils reçoivent un nombre suffisant de paquets renouvelés. Augmentant la puissance destructrice d'un paquet malveillant inséré, il peut voyager à travers le réseau, mélanger et chiffrer avec plus de paquets et détruire complètement les paquets transmis information. C'est l'un des défis majeurs du modèle NC, connu sous le nom d'attaque de pollution. La figure 2.1 montre les conditions de RLNC sans nœuds malveillants dans le réseau et la figure 2.2 montre un réseau RLNC composé d'un nœud malveillant. Les attaques par pollution sont parmi les plus redoutées dans l'environnement cryptographique car elles annulent tous les avantages offerts par NC en exploitant le

concept de base de NC. Les schémas de chiffrement et les solutions de chiffrement couramment utilisés pour l'intégrité des paquets ne fonctionneront pas avec les environnements compatibles NC car les paquets en transit sont fréquemment modifiés. Ainsi, les schémas cryptographiques homomorphes sont apparus comme une solution cryptographique pour la compatibilité NC. Réseaux. Le schéma homomorphe permet un certain degré de calcul sur les paquets cryptés tout en étant capable de les décrypter. Ceci est cohérent avec l'exigence du modèle NC pour le schéma d'intégrité. Cependant, il existe plusieurs autres approches, y compris les schémas de théorie de l'information qui fournissent la sécurité NC. Une analyse détaillée de nombreuses méthodes avancées de protection du CN contre les attaques par contamination est présentée à la sous-section 2.1.

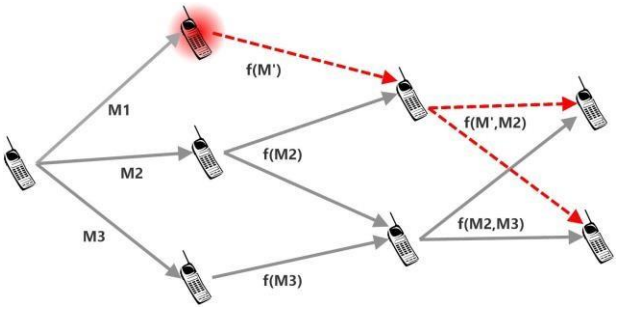


Fig II.2. Scénario malveillant

II.6. Schémas d'intégrité contre les attaques de pollution

L'attaque par contamination NC est une catastrophe par nature car elle se propage à tous les canaux de communication après la première injection d'un colis contaminé. Étant donné que les paquets sont mélangés ou cryptés puis transmis à chaque nœud, un paquet contaminé, s'il n'est pas détecté, entrera également dans le processus et contaminera tous les paquets avec lui. Par conséquent, il est extrêmement important de détecter une attaque de contamination au plus tôt. Il existe différents programmes d'intégrité contre les attaques contaminants dans le NC. Étant donné que la mobilité et l'hétérogénéité sont l'une des exigences fondamentales des futurs réseaux, le NC sans état doit être pris en compte. De plus, le chiffrement de réseau aléatoire linéaire (RLNC) a été identifié et proposé pour les réseaux sans fil [4], nous analyserons donc le plus techniques appropriées pour les réseaux basés sur RLNC. En général, tous ces éléments peuvent être divisés en deux catégories.

a. Approches cryptographiques
b. Approches théoriques de l'information

a. Approches cryptographiques :

Les méthodes de chiffrement traditionnelles ne fonctionnent pas pour les environnements de chiffrement réseau en raison du mélange de paquets en mouvement. Dans les réseaux hérités, une fois qu'un paquet est généré chez l'expéditeur, il ne changera jamais en transit à moins qu'il ne soit modifié par des utilisateurs malveillants. Cela permet aux schémas cryptographiques couramment utilisés comme schémas de signature de vérifier l'intégrité des paquets en transit. Cependant, dans les réseaux prenant en charge NC, les nœuds intermédiaires peuvent crypter les paquets, ce qui les rend approches hors de portée. Les schémas d'intégrité utilisés dans NC doivent être de nature homomorphe. L'exigence de base pour de tels schémas est qu'ils doivent être capables de vérifier l'intégrité des paquets même lorsque des calculs mathématiques linéaires sont effectués sur les paquets. En d'autres termes, les schémas d'intégrité pour les réseaux compatibles NC devraient pouvoir vérifier l'intégrité des paquets individuels à partir d'une combinaison linéaire de ces paquets. Les schémas cryptographiques homomorphes sont classés en schémas de signature homomorphes et codes d'authentification de message homomorphes (MAC). Les signatures homomorphes fonctionnent en signant un sous-espace linéaire des paquets d'origine afin que toute combinaison d'entre eux puisse être identifiée par la signature qui lui est attachée. D'autre part, dans les schémas basés sur MAC homomorphe (HMAC), une étiquette a des propriétés homomorphes (c'est-à-dire, s'il y a deux paires étiquette-vecteur (v1, t1) et (v2, t2), n'importe qui peut créer une étiquette t tel que le vecteur :

$$y = a1v1+a2v2$$

est attaché à chaque paquet. N'importe quel Le schéma de chiffrement nécessite que certaines clés soient distribuées entre les nœuds participants afin d'effectuer des contrôles d'intégrité. Les schémas basés sur les signatures utilisent la cryptographie à clé publique tandis que les schémas basés sur MAC utilisent la cryptographie à clé privée. Dans les deux cas, la plupart du temps, les clés sont pré-distribuées par le Secure Key Distribution Center (KDC) comme le montre la Fig. 2.3. Plusieurs schémas cryptographiques sont discutés ci-dessous. Certains de ces plans utilisent à la fois des

signatures et des MAC pour fournir une meilleure sécurité tandis que certains utilisent des scénarios de distribution de clés spécifiques pour éviter une situation où plusieurs nœuds sont compromis dans le réseau.

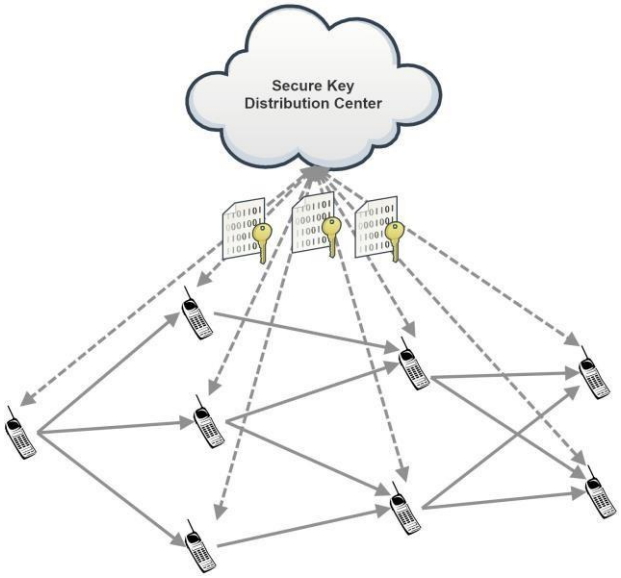


Fig II.3. Scénario généralisé de distribution de clés pour les approches cryptographiques

En 2006, des signatures homomorphes pour le chiffrement de réseau ont été proposées par Charles, Jain et Lauter [50]. Ce travail a proposé un schéma de signature homomorphe basé sur des courbes elliptiques pour assurer la sécurité NC. Le schéma proposé peut signer des espaces linéaires avec des signatures afin que les paquets chiffrés du réseau puissent également être vérifiés. Le schéma de signature prétend avoir les degrés de rigidité du problème du log discret et du co-problème Diffie-Hellman sur les courbes elliptiques. Bien que ce travail réussisse à éviter l'exigence d'un canal sécurisé pour l'échange de valeurs de hachage, la complexité du schéma proposé est très élevée. de O((d + k) log2+ε q) opérations sur les bits par nœud. signature h(e) pour tout ε > 0, où din est le degré du sommet dans(e), d + k est la dimensionnalité de l'espace vectoriel, p est un nombre premier et q est une puissance d'un entier un autre facteur tel que p q est utilisé dans la définition de la courbe elliptique . Cependant, ce schéma a un coût de bande passante fixe de 2 log q bits par signature, qui ne dépend que des nombres premiers choisis. Il convient à l'environnement d'encodage de réseau linéaire mais impose une complexité de calcul élevée de la correspondance de Weil pour les nœuds internes et le processus d'encodage-décodage ainsi que les exigences initiales pour trouver la torsion appropriée des courbes d'ellipse et de points.

Microsoft a été l'un des premiers bénéficiaires de NC. Ils ont lancé une application de capture de fichiers appelée Microsoft Secure Content Downloader, basée sur NC [3]. Il explique un NC sécurisé qui collabore pour la diffusion de contenu à grande échelle avec des clients mobiles dans un réseau hétérogène. De plus, ils ont étendu ce travail pour expliquer les aspects de sécurité du système dans [77]. Ce travail traite des attaques d'entropie et d'obfuscation (attaques de contamination) et propose un mécanisme de sécurité de base basé sur une fonction de hachage homomorphe. Cependant, ils mettent davantage l'accent sur un schéma de sécurité coopératif pour réduire la complexité de calcul causée par le processus de vérification de hachage. Bien que l'idée soit proposée pour la diffusion de contenu, elle peut être bien connectée aux exigences des réseaux mobiles sans fil. Cependant, ce schéma s'attend à ce qu'il existe un canal sécurisé pour communiquer les valeurs de hachage entre les nœuds. Il est abordé dans cet article en mettant à l'échelle ce réseau à partir d'un ensemble fini d'utilisateurs et d'un pourcentage fixe d'utilisateurs malveillants à un nombre théoriquement infini d'utilisateurs. Cependant, les schémas basés sur le hachage nécessitent que la clé privée soit partagée entre chaque paire de nœuds, ce qui crée des défis dans le réseau réel pour s'assurer que le réseau est entièrement connecté. Le coût de calcul et le temps d'exécution dépendent de la multiplication pour le calcul du hachage et de l'exponentiation. Pour le contrôle de hachage, qui dépend à son tour du nombre d'utilisateurs malveillants, de la taille du paquet, du nombre de mots chiffrés. Comme nous en avons discuté, les fonctions de hachage homomorphes sont plus complexes en termes de calcul que les signatures ou les MAC homomorphes.

Un schéma de signature homomorphe efficace contre les attaques par contamination a été proposé par Zhen Yu et al. 2008 [78]. Il s'agit de l'une des premières propositions d'utilisation de la cryptographie à clé asymétrique de type RSA pour générer des schémas de signature homomorphes contre les attaques contaminants. Le schéma introduit un schéma de signature homomorphe linéaire qui permet aux nœuds relais de signer leur sortie en utilisant la signature qu'ils reçoivent en entrée et est utilisé pour le chiffrement sans connaître la clé. Uniquement du bouton d'alimentation. Il permet aux nœuds intermédiaires de vérifier les paquets entrants à l'aide de la clé publique du nœud source et des facteurs de chiffrement attachés aux paquets. De plus, le schéma permet une vérification en bloc des messages, ce qui réduira le calcul requis aux nœuds intermédiaires. La plupart des plans de sécurité contre les attaques par contagion basés sur des signatures

homomorphes suivent le même schéma de génération de signature. La sécurité de ce schéma dépend du problème difficile de l'analyse de l'entier pour trouver une signature valide pour un paquet contaminé, ou trouver une collision de fonction de hachage pour le paquet exact qui correspond au problème du logarithme discret. La découverte des collisions de hachage par force brute dépend du champ fini utilisé pour le diagramme NC. Schéma de sécurité en compromettant le niveau de sécurité du schéma. Ce schéma de signature léger peut être compromis si le nœud malveillant est capable d'écouter certains paquets et signatures. Cependant, ce schéma est beaucoup plus rapide que le précédent en termes de calcul et de vérification de signature. Ce travail présente également une étude comparant le coût opérationnel et le temps de mise en œuvre du schéma de sécurité proposé et de son alternative légère avec ceux de [50,77]. Le coût de calcul de l'original est légèrement supérieur à celui proposé par Gkantidis et Rodriguez [77] mais diminue dans le schéma léger. Cependant, il faut noter que la vérification de la signature nécessite toujours une puissance (2 + m + n) et ce coût n'est pas réduit dans le schéma léger. régime de substitution non plus. Le temps de vérification de la signature sur une machine Linux Pentium IV, 3 GHz est de 1,43 seconde par message lors de l'émulation. Cependant, Aaram Yun et al. Ont identifié des flux dans ce travail et ont proposé une modification mineure de pour le rendre proprement homomorphe. Cependant, le schéma est toujours vulnérable aux attaques par petits messages, ou si un adversaire peut écouter certains messages, le schéma peut être complètement compromis.

Un autre schéma de signature contre les attaques par contamination est expliqué dans par MinJi Kim et al. [85] Cet article se concentre sur la nature destructrice et polluante en augmentation exponentielle des attaques polluantes dans les réseaux peer-to- peer. De plus, ils proposent un schéma de signature qui permet de détecter rapidement les paquets infectés. Les auteurs proposent une signature basée sur un vecteur orthogonal aux vecteurs de paquets d'origine. Ce vecteur orthogonal est signé par la source avec sa clé privée et est distribué. Tout nœud peut vérifier la signature et obtenir ce vecteur orthogonal. Il est alors possible de vérifier toute combinaison linéaire des vecteurs d'origine à l'aide de ce diagramme. Par définition, trouver un autre vecteur qui peut casser ce modèle est aussi difficile que le problème du logarithme discret. Cela aidera également à prévenir les infections multiples sur un seul nœud bénin et garantira ainsi une efficacité maximale de la bande passante pour la transmission. Ce régime a un surcoût total d'environ 6 % si la signature est appliquée à chaque fichier. Le coût réel est de 6(m + l)/ml multiplié par la taille du fichier où m

compresse l'espace vectoriel à dimension sur le champ fini considéré en une génération.

Le schéma de signature basé sur l'identité pour les NC a été proposé par Yixin Jiang et al. Le schéma proposé comprend un schéma dynamique d'authentification et de signature basé sur l'identité qui permet également une vérification en masse des paquets. L'arbre d'authentification binaire à plusieurs niveaux (M-BAT) a été introduit pour atténuer correctement les paquets cassés. Le schéma de signature est basé sur des cartes bilinéaires et une pseudo-identification. Trouver des collisions de hachage pour les signatures est aussi difficile que de calculer le problème du logarithme discret, et les pseudo-identifiants seront changés périodiquement, ce qui empêche également les attaques par falsification de signature. Cet article est également à comparer avec [50,78]. L'approche proposée a un coût similaire à la signature de paquets mais réduit le coût de la vérification puisque le schéma de signature basé sur l'identité élimine l'exigence d'exponentiation modulaire et réduit le nombre d'opérations de concaténation. Demande avec la vérification en bloc, les coûts opérationnels sont encore plus réduits. Ils aussi analysé les coûts de communication et expliqué les coûts de calcul fixes donnés par le diagramme. Il est mentionné que la cryptographie basée sur l'identité ne nécessite aucun certificat (125 octets selon IEEE 1609.2 [86]) associé à la signature, mais ne nécessite que des informations d'identité plus petites (44 octets) avec 22 octets fixes de la même signature ECDSA [50].

L'article de Nuttapong [88] et al. explique une extension du schéma NCS proposé [84] dans et présente le schéma de signature homomorphe pour les NCs dans le modèle standard. Les auteurs utilisent un modèle de double cryptage pour être plus sûr que le modèle oracle aléatoire. Ils ont étendu le schéma NCS en ajoutant un algorithme de vérification de compatibilité pour garantir le caractère aléatoire et en utilisant une fonction pseudo-aléatoire pour généraliser une partie du système afin que la source n'ait pas à attendre que le fichier entier commence à encoder. Au lieu de signer toute la plage du sous- espace vectoriel, les signatures ici sont définies sur les vecteurs transmis à ce moment particulier. Cependant, ce calcul supplémentaire pour rendre le diagramme isomorphe impose également un coût de calcul sur le schéma précédemment proposé.

Un schéma MAC homomorphe basé sur TESLA [92] a été proposé pour l'authentification dans un environnement de streaming P2P. Ce schéma utilise l'idée d'une synchronisation temporelle lâche et d'un partage de clé retardé de la source vers d'autres nœuds, comme suggéré dans le protocole TESLA pour l'authentification multidiffusion [93]. HMAC fait partie intégrante du schéma et est utilisé pour vérifier l'intégrité des paquets.

Cependant, ils l'ont modifié en PMAC en utilisant un générateur pseudo-aléatoire et une fonction pseudo-aléatoire pour réduire la taille de clé et surcharge de calcul. De plus, ils utilisent une balise de contrôle avec une balise MAC pour s'assurer que le traitement NC est effectué correctement en utilisant la livraison de clé retardée du serveur. Cela nécessite que chaque nœud mette en mémoire tampon le paquet reçu pendant un certain temps, mais un débit élevé peut toujours être atteint. en transmettant simultanément plusieurs générations de paquets. Le coût de calcul dû au schéma proposé consiste en un calcul de m + l PRF appels et appels PRG et multiplication (n + 2m + l)(PN + 1) par Fq par nœud par paquet où PN est la taille de l'ensemble des nœuds parents pour les nœuds N et l sont le nombre de balises MAC. Coût de communication dû à la balise MAC et à la balise de test combinées en bits PN •(3l + 1)log2 q.

Key Distribution Basé Tag Encryptions (KEPTE) [94] a été proposé en 2014. Il s'agit d'un schéma d'intégrité associative basé sur la cryptographie contre les attaques de contamination NC. KEPTE utilise différentes clés pour générer des balises à la source et pour vérifier les balises sur les nœuds intermédiaires et récepteurs. Cependant, il diffère du schéma de signature car il ne s'agit pas d'une approche cryptographique à clé publique. KEPTE est un schéma basé sur une clé privée pré distribuée qui crypte les paquets avec des balises. Il fournit plusieurs clés pour la source (pour la génération de balises) et une paire de clés unique pour tous les autres puits. Ces clés contiennent une relation mathématique pour vérifier les jetons générés à l'aide de clés distribuées à la source à l'aide d'une paire de clés unique détenue par d'autres nœuds. Ainsi, il réduit le coût du stockage des clés au niveau des nœuds intermédiaires et offre également une meilleure efficacité de calcul. De plus, en 2016, [95] des recherches sur le protocole KEPTE et des améliorations du schéma de distribution et de gestion des clés ont été proposées. KEPTE discute de la complexité de calcul pour la génération ou la distribution de clés, puis discute des calculs nécessaires pour signer et vérifier les jetons. Pour l'initialisation, la surcharge est de l'ordre de (N 3 + N 2 (m + n)), où N est le nombre d'étiquettes. Pour signer le paquet, le nœud source doit effectuer des calculs dans l'ordre (N(m + n)) où le processus de vérification aux

nœuds récepteurs a une complexité de O(m + n + N). Chaque paquet a N balises qui lui sont attachées, ce qui donne un rapport de coût de N/(m + n). Du point de vue du stockage, la source stockera N clés, chacune de taille égale pour un paquet de données, et les nœuds de destination stockeront deux vecteurs secrets, chacun avec (N + m + n) log2 Pbits.

Un autre travail récent basé sur HMAC est le schéma d'intégrité efficace en bande passante proposé dans [101]. Dans cet article, les auteurs définissent un schéma d'intégrité utilisant un double MAC pour la détection de la pollution, mais améliorent ensuite l'efficacité de la bande passante en utilisant une génération et une distribution de clés soigneusement mises en œuvre. Selon le procédé proposé, les clés utilisées pour générer le MAC sur le paquet chiffré et les clés utilisées pour générer le DMAC sur le MAC ont une relation de liaison telle que les deux clés initiales pour chaque ensemble des clés sont choisies. Sur la même base. Cela réduit les paquets qui doivent être transmis sur le canal de communication, et au nœud de réception, un algorithme de mise à l'échelle est utilisé pour récupérer le paquet entièrement chiffré avec des balises pour le contrôle d'intégrité. Le schéma proposé a le coût de calcul de la multiplication N × (N + m + n) + (N + 1) au nœud source et la multiplication 4 × (N + m + n) + Mk × (N + m). + n) et (N+1) puissances pour les nœuds non source, où N, m, n et Mk sont respectivement le nombre de balises, la taille de génération, la taille de paquet et le nombre de HMAC au niveau du nœud non source. Cependant, cette méthode proposée améliore le taux de charge utile admissible (APR) du réseau et rend ainsi la bande passante efficace. Le coût de communication de la méthode proposée est réduit à N+1 symboles, ce qui rend l'APR meilleur que les méthodes précédentes. Une extension de ce travail avec un schéma de localisation et de débogage pour pointer le nœud ennemi est présentée dans [102].

Référence	Type	Caractéristiques principales	Hypothèse de sécurité/ Dureté	Complexité informatique	Frais généraux de communication
[50]	Signature homomorphe	Appariement basé sur les courbes elliptiques	Problème de logarithme discret (DLP) et Diffie-Problème de Helman (DH)	(m + n)× appariement et (m + n + 1) × multiplications	Surcharge de bande passante fixe qui dépend sur les nombres premiers choisis
[3,77]	Hachages homomorphes	Un mécanisme collaboratif pour réduire la complexité	Sécurité coopérative à l'aide de fonctions de hachage	(m + n) exponentiations	Débit légèrement supérieur à 10Mbps
[78,79]	Signature homomorphe	Active la vérification par lots	Factorisation d'entiers (basée sur RSA)	(2 + m + n) exponentiations	Surcharge de bande passante fixe
[80,81]	Signature homomorphe	NCS1 : modèle oracle aléatoire et NCS2 : plus faible DLP sur sous-espace linéaire	NCS1 : calcul D-H dans les groupes bilinéaires et NCS2 : DLP plus faible	(m + n) exponentiations	borne inférieure sur la taille de la signature comme m log2 q
[9]	MAC homomorphe	Premiers travaux sur les HMAC en temps polynomial	Algorithme de temps polynomial probabiliste (PPT) (avec chaque étiquette fournit un niveau de sécurité de 1/q)	m + n multiplications	Le nombre de balises dépend de la collusion re-coefficient de résistance, c
[84,88]	Signature homomorphe	Signer un vecteur orthogonal pour détecter plusieurs con-taminations dans un seul nœud	Problème de logarithme discret	(m + n) exponentiations	6(m + n)/mn environ 6%
[85]	Signature basée sur l'identité	BAT à plusieurs niveaux pour atténuer les paquets corrompus	problème de calcul Diffie Helman sur elliptique courbes	2 appariements, (m + n) multiplications et 1 exponentiation	66 octets
[87]	HMAC	Intégration de la cryptographie et des technologies de l'information approches théoriques	Algorithme PPT avec transmission spécifiée dans le temps protocole	N × (n + m + (N − 1)/2) pour vérifier N Mots clés	augmente à mesure qu'il voyage nombre d'espoirs
[12]	Hybride	Intégration de signatures homomorphes avec MAC pour prévenir les attaques de pollution par balises	MAC utilisant le principe d'orthogonalité (sécurité niveau de 1/q par balise), DLP pour la signature	(m + N + 1) exponentiations et (m + n + 1)N multiplications	(N + 1)/(m + n) + 32N/|p|(m + n)
[89]	Signature homomorphe	Deux schémas sans utiliser de modèle oracle aléatoire	q-fort DH et RSA	(m + n) exponentiations	f (λ), où λ est le paramètre de sécurité
[92]	HMAC	Synchronisation horaire lâche et partage de clé retardé comme proposé dans TESLA	Algorithme PPT (avec chaque balise assure la sécurité niveau de 1/q)	(n+2m+l)(|PN |+1) multiplication sur Fq	|PN | •(3l + 1)log2 q bits
[94]	HMAC	Algorithme spécifique de distribution de clés pour assurer curité	Algorithme PPT (avec chaque balise assure la sécurité niveau de 1/q)	Multiplications en O(m + n + N) pour ver-ification	N × log2 q bits, où N est le nombre de balises
[96]	HMAC	Un schéma de sécurité basé sur l'espace nul dans lequel les balises sont échangées avec des symboles du paquet	Algorithme PPT (avec chaque balise assure la sécurité niveau de 1/q) et sécurité supplémentaire de 1/m par permutation	(m + n + N) multiplications pour vérification	N × log2 q bits, où N est le nombre de balises
[97,13]	Hybride	Signatures homomorphes et MAC avec schéma de distribution de clé spécifique	MAC utilisant le principe d'orthogonalité (niveau de sécurité de 1/q par tag), problème de logarithme discret à signer	N '+N exponentiations pour la signature, N × (m + n +1) multiplications pour les MAC et N '(N +1) multiplications pour les D-MAC	le nombre de balises N et N' dépend directement de la valeur de résistance aux collisions c
[99,100]	HMAC	Détection d'intrusion et localisation du nœud adverse dans le réseau	Algorithme PPT similaire à [96] pour le schéma d'intégrité et le schéma de localisation basé sur SDN avec secret partagé	O(c), où c est le nombre d'appareils mobiles dans une petite cellule	N × log2 q bits, où N est le nombre de balises
[101]	Hybride	Bandwidth efficient integrity scheme with spe- cific key distribution constraints	MAC utilisant le principe d'orthogonalité (sécurité niveau de 1/q par étiquette), problème de logarithme discret pour la signature	4 × (N + m + n) + Mk × (N + m + n) multiplications et (N + 1) exponentielles-pour les nœuds non sources	N + 1) × log2 q est le coût total de communication, où N est le nombre de balises

Tous les schémas d'intégrité basés sur la cryptographie considérée dans le cadre de la revue de la littérature pour la mémoire sont résumés dans le tableau 2.1 Les caractéristiques principales et les paramètres clés du schéma d'intégrité sont présentés. La recherche montre que la plupart des schémas d'intégrité qui existent dans la littérature ont des problèmes de coût élevé ou d'évolutivité lorsqu'il y a de nombreux adversaires dans le réseau. Une analyse détaillée de ces schémas d'intégrité et de leurs principaux défauts abordés dans cette mémoire est présentée au chapitre 3.

b. Approches théoriques de l'information :

Dans une série de travaux [103,104] S. Jaggi et al. Proposer un code réseau basé sur la théorie de l'information, avec un débit optimal. Les auteurs tentent de résoudre le problème qu'un adversaire byzantin essaie d'injecter des paquets malveillants dans un réseau multicast crypté. Ils proposent des algorithmes en temps polynomial pour empêcher un nœud malveillant d'injecter des paquets corrompus. Dans, différents types de modèles de réseaux et d'adversaires sont étudiés et testés pour déterminer si le schéma proposé peut atteindre un débit optimal. Le rapport optimal pour les réseaux est déterminé en fonction de diverses hypothèses et des capacités de l'adversaire. Contre l'ennemi omniscient le plus puissant, le schéma proposé atteint un taux de C − $2x0$ avec une complexité de chiffrement/déchiffrement de l'ordre de nC3 où C'est la capacité du réseau, n est la longueur de chaque paquet et $x0$ est le nombre d'ennemis injectables paquets. Code de correction fourni par Jaggi. And.al sont quelques-uns des premiers travaux à informer approches théoriques de la lutte contre les attaques de pollution.

Le chiffrement de réseau pratiquement sécurisé (SPOC) [105] est un schéma de sécurité léger basé sur l'idée de facteurs de clé associés aux paquets. Vilela et al. Interprètent ce schéma comme une extension du modèle de secret partagé expliqué dans [104]. Cependant, ils renoncent à l'utilisation d'un canal sécurisé séparé pour partager des secrets en attachant un facteur clé aux paquets d'origine. Certains des coefficients générés au nœud source seront chiffrés avec une clé secrète partagée uniquement entre les nœuds source et destination (cela ne doit être fait qu'une seule fois et aura lieu hors ligne ou avant que la communication n'ait lieu). start) et ils sont appelés les coefficients verrouillés et les autres coefficients les coefficients non chiffrés sont appelés les coefficients sans clé. Les nœuds intermédiaires fonctionnent sur les paquets reçus sans aucune distinction entre les coefficients. Ainsi, lorsqu'un paquet arrive au nœud récepteur, les coefficients non

verrouillés sont utilisés pour décrypter les coefficients verrouillés et puis déchiffrez-le avec la clé pré-partagée. Ensuite, la matrice de décryptage est calculée et les paquets originaux peuvent être décodés. Le schéma garantit que le décryptage des paquets d'origine n'est pas possible sans les valeurs décryptées des coefficients cryptés et garantit ainsi l'intégrité des paquets reçus au niveau du nœud récepteur. Ils ont éliminé le canal de partage de secret séparé nécessaire pour transporter le hachage pour chaque génération au prix d'une clé pré-partagée unique qui peut être prise même hors ligne avec des coûts de calcul supplémentaires pour coder un certain nombre de coefficients de l'ordre des tailles de troisième génération. Cependant, comme la plupart des autres méthodes non cryptographiques, SPOC ne détecte également que les attaques de contamination au niveau du nœud récepteur.

Les schémas DART et EDART [73] sont des schémas d'intégrité basés sur l'asymétrie temporelle qui résistent aux attaques de contamination. Ils utilisent des sommes de contrôle basées sur des décalages temporels pour s'assurer que les paquets reçus sont authentiques. Il permet également la détection de paquets corrompus au niveau des nœuds intermédiaires, ce qui est très rare dans les protocoles non chiffrés contre les attaques contaminants. Dans le protocole DART, les sommes de contrôle sont générées à la source lors de la génération des paquets à l'aide de transformations linéaires aléatoires calculées efficacement combinées à des horodatages. Chaque nœud relais du système ne vérifiera les paquets reçus que s'il reçoit également une somme de contrôle confirmant l'authenticité des paquets reçus. Seuls les paquets vérifiés sont utilisés pour le chiffrement au niveau du nœud relais afin que les paquets contaminés ne soient pas propagés davantage. Cependant, cela représente un délai pour que chaque nœud vérifie un nombre suffisant de paquets avant de les transmettre. EDART est suggéré de réduire ce délai avec une transmission optimiste. Dans le schéma EDART, les nœuds les plus éloignés de l'attaquant transmettront les paquets sans attendre la vérification, tandis que les nœuds proches de l'attaquant vérifieront les paquets avec une somme de contrôle avant de les transmettre. Initialement, chaque nœud démarrera en mode avant, et tout nœud qui détecte une non-concordance dans la somme de contrôle passera en mode vérification. Les nœuds après le nœud de vérification décideront du délai et du temps de transmission en fonction des paramètres de sécurité et de la fréquence de contamination détectée. . Ce schéma est beaucoup plus simple en termes de calcul que n'importe quel schéma de chiffrement, mais ne convient pas aux systèmes qui ne peuvent pas tolérer la latence. Le faible coût de calcul de 5 signatures

par seconde pour le nœud source est dû à la génération de sommes de contrôle, et ces sommes de contrôle représentent également un coût de bande passante de 18 kbps par commutateur.

SpaceMac [106] par Anh Le et Athina Markopoulou considère un sous-espace élargi et une expansion homomac [9] pour empêcher à la fois la pollution des données et les attaques de pollution par les balises. De plus, ils appliquent une sécurité qui coopère avec le contrôleur pour localiser précisément le nœud malveillant, le transformant en un schéma hybride capable non seulement de détecter les attaques contaminantes, mais également de localiser le bouton de l'adversaire. Spacemac considère que le réseau a une coopération parent-enfant pour permettre la sécurité. Tout nœud N sera limité à générer ses paquets d'envoi uniquement à partir des paquets qu'il a reçus de ses nœuds parents. Cela se fait par la coopération des parents et des enfants de N. Puisque les nœuds parents peuvent se connecter à des sous-espaces à partir desquels un nœud peut créer des packages, Spacemac peut être appliqué pour étendre les sous-espaces. Étant donné que chaque nœud vérifiera les balises attachées aux paquets reçus, une attaque de contamination par balise n'aura pas un impact négatif sur Spacemac car les paquets avec des balises corrompues ne voyageront pas plus loin dans le réseau. De plus, avec un contrôleur central et la coopération de tous les boutons, Spacemac identifie l'emplacement d'un attaquant. Cependant, le contrôleur central doit connaître la topologie complète du réseau, ce qui peut ne pas être vrai pour les réseaux sans fil. De plus, la collusion active par des nœuds rivaux adjacents peut réaliser un schéma de sécurité spacemac et créer une vulnérabilité si une région particulière est compromise par un adversaire puissant. l'étiquette attachée au paquet et un coût de calcul de $(3+d+\lambda)(n+2m)+$ w par paquet par nœud de réception, où λ est le nombre total d'étiquettes attachées au paquet, d est le nombre d'étiquettes examiné par ce nœud, et w est le nombre moyen de paquets.

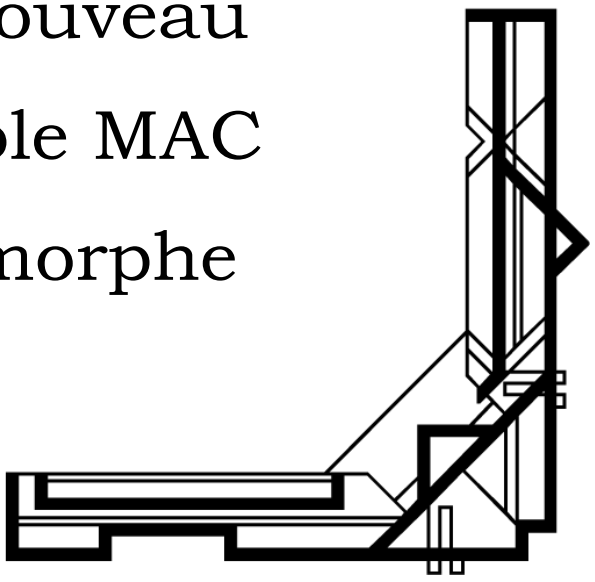
Conclusion

Ce chapitre traite de l'état de l'art lié à la sécurité CNC. Une analyse générale des défis de sécurité dans un environnement CNC est présentée dans ce chapitre, suivie d'une discussion détaillée axée sur les attaques contaminants. Les attaques de contamination sont parmi les attaques les plus redoutées dans les environnements compatibles NC, car l'impact des paquets contaminés se propage à travers le réseau avec la transmission et peut réduire considérablement l'efficacité de la transmission. Pin. Depuis traditionnel les méthodes de cryptage ne peuvent pas être utilisées pour la vérification d'intégrité dans NC, des schémas d'intégrité avec une propriété homomorphe sont nécessaires pour identifier les attaques

contaminants. De tels schémas d'intégrité pour se protéger contre les attaques de contamination sont disponibles dans la littérature, expliqués en détail et résumés des points importants. les futurs réseaux à faible latence devient difficile. D'autre part, les approches basées sur la cryptographie sont beaucoup plus rapides pour identifier les attaques de contamination vers le nœud de validation le plus proche. De plus, les schémas basés sur HMAC peuvent être considérés comme plus adaptés aux réseaux de nouvelle génération en raison de leur faible complexité et de leurs propriétés d'évolutivité. Une analyse détaillée des programmes avancés d'intégrité expliqués dans ce chapitre pour décrire la direction de recherche au-delà de l'état moderne poursuivie dans cette thèse sera présentée dans le chapitre suivant.

Chapitre III :

Au-delà de l'état de l'art: nouveau protocole MAC homomorphe



III.1. Introduction

D'après le chapitre précédent, il est clair que les attaques polluantes dans les environnements qui prennent en charge le cryptage réseau (NC) doivent être traitées avec beaucoup de soin. Il est nécessaire de détecter les attaques le plus tôt possible. La théorie de l'information et les méthodes de codage sont proposées pour résoudre ce problème et nombre d'entre elles ont été discutées ci-dessus. Ce chapitre fournit une analyse de ces programmes en général et discute des avantages et des inconvénients des différentes approches. Il traite également séparément de la différence entre homomorphe schémas basés sur la signature et schémas basés sur HMAC. Cette analyse et cette comparaison ont été réalisées avec un intérêt pour l'utilisation de la NC pour le déploiement de la 5G dans un environnement mobile à petites cellules (MSC). Par conséquent, les points d'analyse clés incluent la latence, l'efficacité énergétique et l'optimisation de la bande passante.

III.2. Comparaison de différents types de schémas d'intégrité

L'approche de la théorie de l'information peut être considérée comme la solution la moins sophistiquée contre les attaques de pollution. Ces approches ne nécessitent pas de calculs complexes mais se concentrent sur des caractéristiques spécifiques du système pour assurer la sécurité. La plupart de ces schémas ne détectent que les paquets contaminés dans le nœud de réception. Cela nécessite également un secret qui n'est partagé qu'entre la source et la destination la plupart du temps. Une autre approche des solutions de la théorie de l'information dépend de l'asymétrie temporelle. Protocoles, la détection des paquets contaminés dépend du temps de retard et des symboles supplémentaires attachés au message. Cette pratique cause un retard dans la communication. De plus, la synchronisation de l'ensemble du système devient un critère inhérent à ces projets. Un autre flux dans lequel les méthodes non chiffrées résistent aux attaques contaminants basées sur la coopération des nœuds voisins. Cependant, ces approches ne sont jamais complètement décodées. Il s'agit principalement d'un approche hybride, où certaines caractéristiques et la coopération du réseau sont utilisées pour appliquer efficacement les techniques cryptographiques. Des méthodes telles que RIPPLE et Spacemac en sont des exemples. Fondamentalement, nous pouvons dire que bien que les méthodes non cryptographiques pour prévenir les attaques polluantes soient efficaces en termes de calcul, elles nécessitent des conditions spécifiques pour être satisfaites et généralement inefficaces pour détecter les paquets contaminés en temps opportun.

En ce qui concerne les approches cryptographiques, elles peuvent être divisées en approche basée sur la signature homomorphe et approche basée sur le code d'authentification de message homomorphe (HMAC). Le premier type dépend de clés asymétriques tandis que le second dépend de clés symétriques. Compte tenu du principe de base de NC, les paquets peuvent ne pas être les mêmes que le paquet envoyé par la source mais plutôt une combinaison linéaire des paquets d'origine, tout calcul sur le paquet pour assurer l'intégrité sera également nécessaire. Nécessite test de combinaison linéaire des données d'origine. Par conséquent, les schémas homomorphes sont nécessaires pour les schémas d'intégrité cryptographique en NC. En outre, cela force plus de calculs et ajoute plus de bits supplémentaires aux paquets pour des raisons de sécurité. Cependant, selon les modèles de distribution de clés, les attaques polluantes peuvent être bloquées plus efficacement par ces modèles au nœud bénin le plus proche. La détection des paquets contaminés au nœud bénin le plus proche est extrêmement importante. Sinon, cela dégradera les performances du système en affectant davantage de paquets et de flux sur son chemin. Concernant la latence, les techniques cryptographiques n'imposent aucun délai dans le cadre de leur mécanisme de sécurité ; mais le calcul prendra du temps. Cependant, ce délai de calcul dépend de la puissance de calcul de l'appareil et est faible par rapport à la latence inhérente à des fins de sécurité dans les approches basées sur la théorie de l'information. Cependant, la distribution des clés peut entraîner un délai initial plus long dans la configuration du système. Compte tenu des exigences de bande passante, les schémas d'intégrité basés sur la cryptographie dépendent toujours de certaines fonctions cryptographiques exécutées sur le message et nécessitent également une communication appropriée des valeurs calculées. là. Ces frais généraux sont inévitables, mais doivent être réduits au minimum

Analysons maintenant la différence entre la signature homomorphe et le schéma basé sur HMAC. Comme mentionné, le schéma de signature homomorphe basé sur une clé publique et le schéma HMAC basé sur une clé secrète sont deux directions différentes du schéma d'intégrité cryptographique dans NC. Les deux approches ont leurs propres avantages et inconvénients. Dans la plupart des cas, les schémas basés sur les signatures nécessitent des calculs plus coûteux à vérifier que les schémas basés sur MAC. D'autre part, avoir une clé secrète partagée entre les nœuds source et récepteur du nécessite plus d'efforts et un protocole de distribution de clé efficace que la gestion de clé publique. De plus, les méthodes basées sur MAC auront un coût de bande passante plus élevé en raison

du plus grand nombre de bits requis pour assurer la sécurité du système. Les approches basées sur MAC sont également vulnérables aux attaques de pollution par les balises NC. Une solution à ce problème consiste à utiliser plusieurs niveaux de balises. Cependant, il peut ne pas convenir car il est sensible et augmente significativement le coût de calcul et la bande passante. Une autre ligne de recherche pour protéger les réseaux cryptés contre les attaques de pollution par les balises conduit à des schémas cryptographiques hybrides. Dans de tels cas, par ex. MacSig, une combinaison de HMAC et de signatures homomorphes est utilisée pour assurer la sécurité. Cette approche trouve un meilleur compromis entre complexité de calcul et complexité de communication sans créer de failles de sécurité. Par conséquent, la recherche de schémas d'intégrité cryptographique efficaces peut conduire à des MSC sécurisés activés par NC (NC-MSC).

III.3. Le codage de réseau sécurisé active les petites cellules mobiles

En partant des schémas d'intégrité les plus avancés, nous examinons les schémas d'intégrité pour le NC-MSC, illustrés dans la figure. 3.1. L'architecture générale du scénario de thèse est étroitement liée à la vision des futurs réseaux présentée dans. Il considère une macro cellule contenant plusieurs MSC prenant en charge un réseau hétérogène d'utilisateurs finaux. Les utilisateurs finaux sont connectés au back-haul via la mini-cellule et peuvent se connecter directement aux appareils voisins en utilisant canaux de liaison latérale qui permettent la communication D2D dans le réseau. Par conséquent, un réseau multivoies multi sauts (MP-MH) entre les nœuds source et destination avec des liaisons de communication D2D peut être envisagé à l'intérieur de la macro cellule. NC s'est avéré être une option évidente à utiliser dans de tels réseaux MP-MH pour améliorer les performances et la fiabilité de la bande passante . De plus, le réseau est surveillé et contrôlé par un contrôleur défini par logiciel, qui connecte également la macro cellule au réseau central. Le SDN Le contrôleur se connecte directement aux sous-cellules et contrôle également la gestion du réseau. L'utilisateur final peut communiquer avec le contrôleur central via les petites cellules chaque fois que nécessaire. Ce contrôleur central joue également un rôle important pour garantir l'authentification des terminaux et la sécurité globale du réseau. Un tel réseau NC-MSC peut être très utile dans des applications du monde réel telles que les villes intelligentes, les sites sportifs compatibles 5G, les parcs industriels à haute densité et de nombreux autres scénarios du monde réel. Dans cette

thèse, nous nous concentrons sur la sécurisation de ces réseaux de petites cellules compatibles NC contre les attaques de contamination.

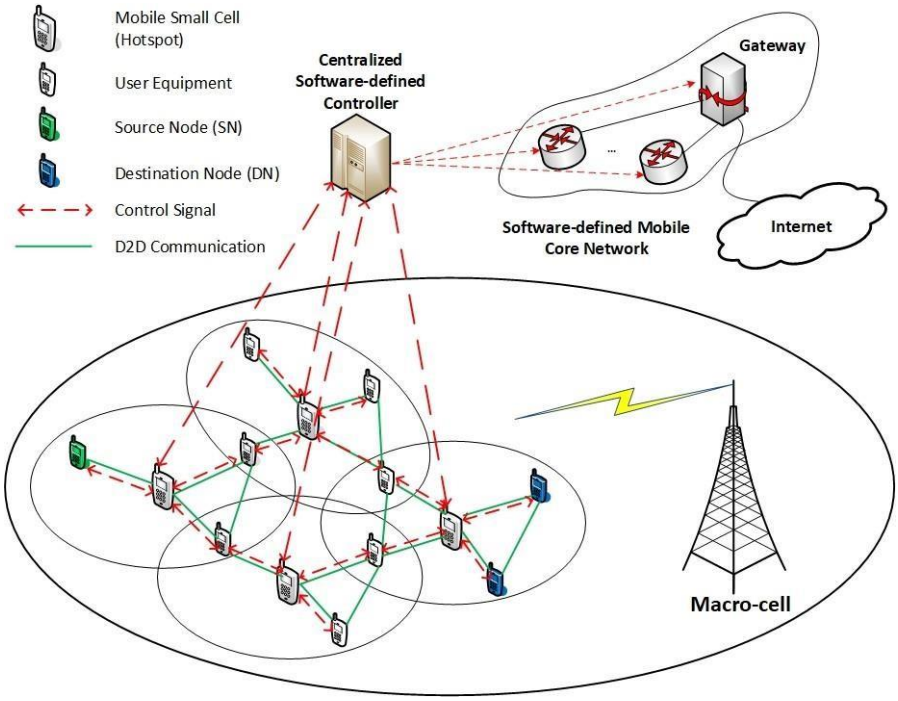


Figure III.1. Scénario de petites cellules mobiles

Étant donné que toute l'idée d'un futur réseau implique un réseau mobile à faible latence et à haute résilience, les méthodes de chiffrement semblent être plus adaptées au système pour résister aux attaques polluantes. infecté. Cependant, l'efficacité énergétique des systèmes d'intégrité doit également être prise en compte. Par conséquent, nous essayons d'étendre et de modifier les méthodes existantes pour être plus efficaces et sécurisées en utilisant les caractéristiques de l'architecture proposée. Cependant, les schémas existants ne peuvent pas être directement adaptés au MSC environnement. La plupart d'entre eux sont étudiés dans une topologie de réseau moins dynamique, et la complexité de ces schémas augmente de façon exponentielle. avec échelle. De plus, la plupart des schémas nécessitent une phase d'installation avant le partage de clés, ce qui est difficile à réaliser dans des conditions de réseau très denses et dynamiques. Dans les approches existantes basées sur HMAC, la sécurité contre une union d'utilisateurs malveillants ou un ensemble compromis de nœuds dans une région dépend toujours de ces modèles de génération de clés. D'autre part, les futurs réseaux fournissent un certain support pour les schémas d'intégrité et aident à réduire la complexité de calcul et les coûts de bande passante des schémas actuels. Le regroupement des BBU et la gestion des petites

cellules basées sur le SDN sont des domaines qui peuvent être utilisés pour développer des schémas d'intégrité plus sûrs et cohérents pour les MSC 5G.

Nous proposons des schémas d'intégrité qui sont cohérents avec l'architecture système proposée des microcellules 5G, illustrée à la figure 3.1. Le premier schéma utilise une unité centrale pour assurer le partage sécurisé des balises tandis que la seconde proposition considère un environnement de réseau plus distribué. Les deux schémas suivent HMAC pour garantir l'intégrité des paquets pendant la transition et utilisent l'architecture réseau pour garantir que MAC est partagé en toute sécurité avec tous les nœuds.

III.4. Modèle adversaire

Considérant maintenant le scénario malveillant, un nœud intermédiaire peut bloquer le paquet pendant la transmission de sorte que le paquet est infecté par P! P. Ce type de pollution s'appelle pollution des données car l'adversaire modifie le paquet lors de la conversion. Les attaques par contamination des données peuvent être détectées à l'aide de schémas d'intégrité basés sur HMAC. Dans de tels schémas d'intégrité, un MAC (étiquette) est généré avec la clé secrète et attaché aux paquets par le nœud source. Cette clé secrète sera partagée avec d'autres nœuds participants afin que l'intégrité des paquets puisse être vérifiée en comparant les balises générées au nœud récepteur avec ceux reçus avec le paquet sur le canal de communication. . Cependant, cela conduit à une autre menace pour la sécurité appelée attaque de pollution par balise. Dans les attaques par pollution par balise, l'attaquant ne modifie pas le paquet pendant la transition mais marque de manière malveillante le paquet d'authentification. Cela se traduira par un échec de la vérification au niveau d'un nœud de réception et par la suppression de paquets authentiques, ce qui réduira les performances du réseau. Dans cette thèse, nous abordons à la fois la pollution des données et les attaques par pollution des balises et proposons un système d'intégrité qui empêchera efficacement la pollution des données et la pollution des balises.

Nous considérons une condition d'adversaire très forte pour évaluer nos systèmes de sécurité. Un nœud adversaire est un nœud intranet et peut également être un adversaire sélectif, agissant uniquement en tant qu'utilisateur malveillant pour un chemin d'information particulier, c'est-à-dire en contaminant des paquets provenant de boutons

d'alimentation spécifiques. Étant donné que l'adversaire est un nœud interne, il aura accès aux clés secrètes partagées entre les nœuds. Il convient de noter que nous n'utilisons pas de schémas de distribution de clés comme la distribution gratuite c-cover, mais permettre à tous les nœuds participants d'accéder à l'ensemble complet des clés requises, ce qui est contraire à la plupart des schémas d'intégrité existants. Cela permet aux nœuds intermédiaires de créer des balises valides pour les paquets pollués. Permettre aux nœuds intermédiaires de créer des balises valides peut entraîner l'échec des schémas d'intégrité et cela est généralement limité par des schémas de distribution de clés spécifiques qui garantiront que toutes les clés ne sont pas distribuées à tous les nœuds. Cependant, cette pratique se complique dans le cas d'adversaires complices. Le schéma d'intégrité dépend fortement du nombre d'utilisateurs malveillants dans le réseau et si plusieurs nœuds malveillants sont combinés, toutes les clés requises peuvent être collectées et gagner contre le schéma d'intégrité. Cela conduit à l'exigence d'un grand nombre de balises dans certains des cas précédents. Dans un environnement dense de nœuds mobiles, ce type de distribution de clés peut ne pas être possible en raison du grand nombre de voisins ainsi que d'une probabilité accrue de nœuds malveillants pour créer des clusters. Ainsi, les défis de la distribution des clés sont également à relever avec l'intégrité des paquets.

III.5. Schéma d'intégrité pour le codage réseau active les petites cellules

L'analyse des schémas d'intégrité les plus avancés nous a permis d'identifier les principales lacunes des schémas actuels pour faire face aux défis du futur environnement sans fil. D'autre part, les schémas d'intégrité basés sur HMAC présentent un potentiel d'amélioration, et la possibilité de modifier l'idée sous-jacente sera étendue pour répondre aux exigences des réseaux 5G compatibles NC et au-delà. Dans cette section, nous présentons les principaux changements et nouveautés que nous introduisons dans le protocole HMAC. Comme mentionné précédemment dans ce chapitre, nous envisageons la disponibilité d'un canal séparé pour le partage des balises, soit via un contrôleur centralisé, soit à l'aide d'un registre distribué. La discussion suivante du protocole HMAC modifié se concentre sur la façon dont les balises attachées à un paquet crypté RLNC et les balises partagées sur le canal alternatif permettront aux nœuds récepteurs de vérifier l'intégrité des paquets. le colis est arrivé. L'algorithme de génération de carte et la preuve mathématique de vérification de carte sont présentés dans la sous-section suivante.

a. Protocole MAC homomorphe modifié :

Dans notre schéma proposé, les avertissements sont générés sur les paquets Pi natifs tels que définis dans la description RLNC, contrairement à la génération d'avertissements sur les paquets chiffrés dans l'article de base.Les jetons sont générés et vérifiés avec le même ensemble de clés, en toute sécurité. répartis entre les utilisateurs du réseau, et un ensemble de clés Ks a L nombre de clés où chaque clé Ki a n + 1 éléments. Chaque clé Ki peut être représentée sous la forme Ki={Ki,1, Ki,2, . . ., Ki,n, Ki,n+1}, est chaque composante Ki,j correspondant à un symbole dans le corps fini . L'étiquette Ti,l sur le paquet Pi en utilisant la clé spécifique Kl sera générée selon l'équation

$$T_{i,l} = \frac{\left(\sum_{j=1}^{n} P_{i,j} \cdot K_{l,j}\right)}{K_{l,n+1}}, \quad l \in (1, L)$$

Maintenant, chaque paquet avec sa balise L ressemblera à [PiT ags(Pi)] = {Pi,1, Pi,2, . . . , Pi,n, Ti,1, Ti,2, .. . ,Ti,L} Le chiffrement sera effectué sur l'ensemble [PiT ags] et la matrice de renforcement sera [α P 'T ags'] où, α est la matrice des coefficients, T ags'= α × T ags et T ags est la matrice m × L des étiquettes attachées aux colis de cette génération comme

$$\begin{bmatrix} T_{1,1} & \dots & T_{1,L} \\ \vdots & \ddots & \vdots \\ T_{i,1} & \dots & T_{i,L} \\ \vdots & \ddots & \vdots \\ T_{m,1} & \dots & T_{m,L} \end{bmatrix}$$

Nous vérifions maintenant la propriété homomorphe selon laquelle ces balises peuvent être vérifiées même après le chiffrement. La propriété homomorphe dans ce diagramme est définie comme suit, même si les paquets et les balises subissent une opération linéaire (codage, dans notre cas multiplication matricielle par une matrice de facteur aléatoire), les paquets doivent toujours être vérifiés par les balises qui leur sont associées. Pour le démontrer, nous devons vérifier si des avertissements sont générés sur

les paquets chiffrés, qui seront égaux aux avertissements après chiffrement. C'est ce qu'il faut dire.

T ag(P *j*) = T ags'= α × T ags pour une génération.

Considérons la situation avec une clé unique K={K1,K2,. . . ,Kn+1} pour plus de simplicité. L'équation représente l'étiquette générée sur le package Pi à la source avant chiffrement. De même, chaque pack de génération aura ses tags.

$$Tag(P_i) = T_i = \frac{\left(\sum_{l=1}^{n} P_{i,l} \cdot K_l\right)}{K_{l+1}}, \quad i \in (1, m)$$

Ainsi, tous les paquets d'origine concaténés avec ces balises seront

$$\begin{bmatrix} P_{1,1} & \dots & P_{1,n} & T_1 \\ \vdots & \ddots & \vdots & \vdots \\ P_{i,1} & \dots & P_{i,n} & T_i \\ \vdots & \ddots & \vdots & \vdots \\ P_{m,1} & \dots & P_{m,n} & T_m \end{bmatrix}$$

L'équation montre l'étiquette générée sur le paquet chiffré Pi' au nœud récepteur.

$$Tag(P_i') = \frac{\left(\sum_{l=1}^{n} P'_{i,l} \cdot K_l\right)}{K_{l+1}}$$

Maintenant, si nous pouvons vérifier que T ag(Pi*j*) est égal à la balise codée T *j*i, cela prouve l'homomorphisme requis par les principes RLNC.

$$
\begin{aligned}
Tag(P_i{}') &= \frac{\left(\sum_{l=1}^{n} P'_{i,l} \cdot K_l\right)}{K_{n+1}} \\
&= \frac{\left(\sum_{l=1}^{n}\sum_{j=1}^{m} \alpha_{i,j} \cdot P_{j,l} \cdot K_l\right)}{K_{n+1}} \\
&= \sum_{j=1}^{m} \alpha_{i,j} \cdot \frac{\left(\sum_{l=1}^{n} P_{j,l} \cdot K_l\right)}{K_{n+1}} \\
&= \sum_{j=1}^{m} \alpha_{i,j} \cdot T_j \\
&= T'_i
\end{aligned}
$$

Cela démontre la propriété isomorphe de la balise sur des opérations linéaires aléatoires.

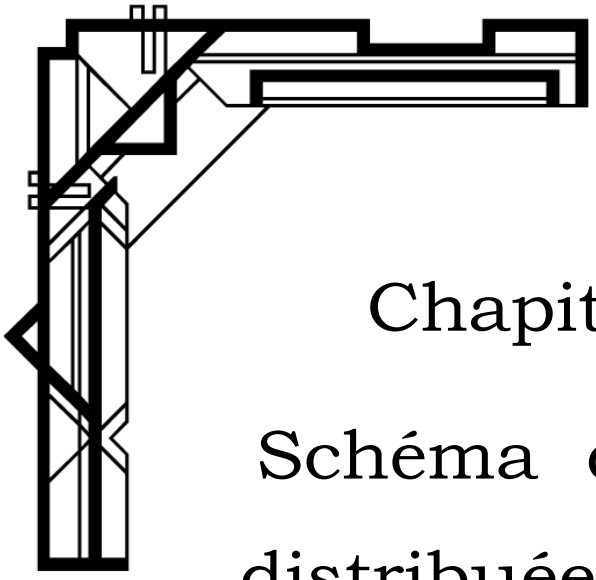
Il existe plusieurs fonctionnalités nouvelles et importantes de ce protocole HMAC modifié.

1- Les balises sont générées sur le paquet d'origine, et non sur le paquet de rappel comme dans les précédents schémas d'intégrité basés sur MAC. Il en résulte une taille de clé plus petite (n + 1) mais toujours une propriété isomorphe sûre et satisfaisante.
2- Pour vérifier une carte avec un mot de passe, il n'est pas nécessaire d'attendre toute une génération. Le nœud récepteur peut générer une balise pour le mot de code reçu et la faire correspondre avec la balise reçue.
3- Lorsque le nœud source génère les balises, il sera traité comme un ajout des paquets d'origine et le chiffrement est également effectué sur les balises. Au nœud de réception, il n'est pas nécessaire de régénérer des étiquettes ou des algorithmes d'association spécifiques comme dans les précédents schémas d'intégrité basés sur MAC. Dans notre cas, les nœuds récepteurs n'ont qu'à ré-encoder les paquets en utilisant leurs coefficients aléatoires générés localement et procéder à la transmission.
4- La distribution des clés pour le schéma d'intégrité est simplifiée. Avec le schéma alternatif de partage de balises, un adversaire ou des adversaires complices peuvent détenir toutes les clés et être toujours incapables de briser le schéma d'intégrité.

Cela élimine le besoin de schémas de distribution de clés spéciaux comme dans les schémas d'intégrité précédents.

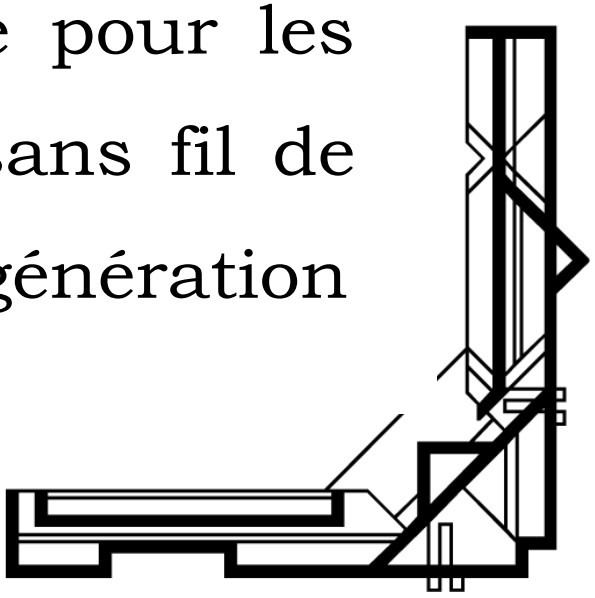
5- Le cas de la vérification d'étiquette après recodage n'est pas spécifiquement traité ici, car ce qui se passe lors du recodage est une multiplication par une matrice de coefficients aléatoires, qui est considérée lors du processus de recodage. encoder. Par conséquent, la preuve est valide pour la propriété homomorphe à tout nœud récepteur, même après recodage.

Ce protocole HMAC modifié constitue le concept de base de nos schémas d'intégrité pour les futurs réseaux sans fil compatibles NC. Bien que le concept de base de la génération et de la vérification de MAC reste le même que les précédents schémas d'intégrité basés sur MAC, notre méthode proposée présente quelques nouveautés par rapport à eux. Premièrement, le MAC est généré sur les paquets d'origine par rapport aux paquets améliorés dans les schémas d'intégrité précédemment connus, mais conserve la propriété homomorphe pour les opérations RLNC. Deuxièmement, les attaques de contamination par balise sont empêchées en utilisant un schéma de partage de balises comme alternative à l'utilisation de signatures, ce qui le rend moins coûteux en termes de calcul que De plus, en supposant que nous disposions d'un mécanisme de partage de balises alternatif sécurisé, la distribution des clés peut être beaucoup plus simple que le schéma précédent, et la sécurité ne dépendra que du nombre de balises, même lorsqu'il y a de nombreux concurrents sur le réseau. Discussion plus détaillée sur les avantages de modifié Le protocole HMAC est présenté dans les chapitres appropriés. Il existe deux variantes majeures des schémas d'intégrité dont nous discutons dans cette thèse, l'approche centralisée et l'approche distribuée, en fonction de la manière dont les balises sont communiquées aux nœuds participants à partir du nœud source. Ainsi, les discussions ultérieures sont divisées en deux parties en fonction de l'approche choisie pour le partage de balises.



Chapitre IV :

Schéma d'intégrité distribuée pour les réseaux sans fil de nouvelle génération



Un schéma d'intégrité distribuée pour les réseaux sans fil de nouvelle génération pourrait être mis en place en utilisant des techniques de cryptographie et de vérification de l'intégrité des données.

Ce schéma d'intégrité distribuée permet de garantir la sécurité et l'intégrité des données échangées entre les nœuds du réseau sans fil, même en cas d'attaques malveillantes. Il est important de noter que ce n'est qu'un exemple de schéma d'intégrité distribuée et qu'il existe de nombreuses autres méthodes pour sécuriser les réseaux sans fil de nouvelle génération.

IV.1. Scénario de référence

Nous considérons le scénario d'un canal de communication multi-sauts sur un petit support tel que représenté sur la Fig. 6.1, similaire à l'architecture générique définie sur la Fig. 3.1.Un nœud qui initie la communication est appelé le nœud source et les nœuds de destination sont appelés un nœud récepteur. Tous les nœuds du milieu peuvent être normaux utilisateurs ou petites têtes de tuiles. Chaque nœud participant à une sous- parcelle est connecté directement à la tête de sous-parcelle correspondante via un canal de contrôle, et les nœuds font partie de nombreuses sous-parcelles appelées nœuds relais. Les nœuds relais seront connectés à un certain nombre de petites cellules. Tous les nœuds sont capables d'effectuer RLNC opérations sur les paquets et sont connectés via des canaux D2D. L'approche RLNC éprouvée pour fournir des performances améliorées dans les communications D2D multi-sauts [5]. les nœuds peuvent multidiffuser des paquets aux nœuds voisins ou les envoyer à des nœuds voisins via ce canal D2D. Le réseau utilise uniquement le cryptage intranet, ce qui signifie que seuls les paquets de même génération sont cryptés ensemble.

Dans ce cas, cependant, nous considérons la superposition de petites cellules pour former un grand livre distribué de style blockchain. Ce registre distribué remplacera le contrôleur central dans intégrité du schéma. Cela signifie que le partage de jetons sécurisé est mis en œuvre à l'aide de registre distribué. Les jetons générés sur les nœuds source et le nœud source enverra les jetons au sommet de sa sous-cellule immédiate, où les jetons de la registre sont stockés. Les nœuds récepteurs peuvent interroger la sous-cellule correspondante pour obtenir des informations d'identification à l'aide des informations de certificat requises. Le registre distribué de type blockchain à petites cellules basé sur

bigchainDB est créé sur le réseau. BigchainDB est une base de données distribuée de type blockchain qui utilise l'algorithme Byzantine Fault Tolerance (BFT) pour vérifier le bloc et établir un consensus entre les nœuds participants [21].L'algorithme BFT est un protocole Proof of Stake (PoS) pour parvenir à un consensus avec un coût de calcul beaucoup plus faible que les protocoles de consensus Proof of Work (PoW) basés sur l'exploitation minière. Tous les nœuds du réseau peuvent accéder au grand livre directement au sommet de sa petite cellule la plus proche, cependant, les utilisateurs finaux sont appelés nœuds légers et ne stockent pas l'intégralité du grand livre sur leur matériel. Ces nœuds ne stockent que la version allégée du grand livre et ne peuvent y ajouter que des transactions ou lire un transaction à partir de celui-ci, mais ne peut pas vérifier un nouveau bloc. Seuls les chefs des petites cellules du réseau peut valider un nouveau bloc selon l'algorithme de consensus PoS et soi-disant nœuds complets. Un nouveau bloc est ajouté à la chaîne lorsqu'un des full nodes termine avec succès la vérification de toutes les transactions collectées entre le bloc précédent et la vérification du nouveau bloc. Toutes ces transactions sont stockées dans un seul bloqué dans la chaîne. Les nœuds légers peuvent interroger le nœud complet le plus proche (en-têtes de petites cellules) à l'aide de métadonnées de transaction et lire le contenu requis à partir du bloc sélectionné à tout moment.

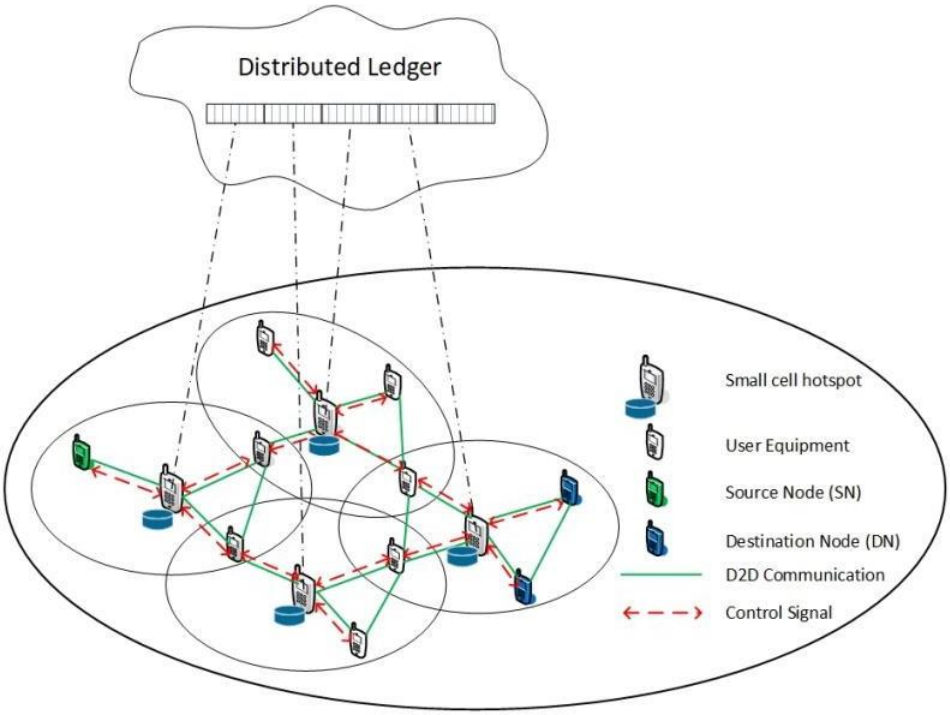


Figure IV.1. Architecture de scénario

IV.2. Amélioration de la sécurité à l'aide de petites cellules distribuées similaires à la blockchain

Le protocole MAC défini ci-dessus peut assurer l'intégrité des paquets dans un environnement RLNC, mais il est vulnérable aux attaques de pollution de balises. Pour relever ce défi, les schémas d'intégrité proposés sont améliorés en utilisant une superposition de dispersion similaire à la blockchain des petites cellules. Dans ce scénario NC sécurisé proposé, les balises sont également stockées dans un registre distribué sécurisé des petites cellules par les nœuds source. Ce registre distribué peut être mis en œuvre en utilisant BigchainDB [118], une base de données similaire à la blockchain. Cela offre un moyen secondaire et sécurisé de partager les balises avec les nœuds participants. Cela aide les nœuds récepteurs à vérifier si les balises ont été modifiées pendant la transition. Lorsque le nœud source génère des balises sur les paquets à construire et est prêt à transmettre, il télécharge également les balises générées pour ce build ainsi que le numéro de build et l'ID source en tant que transaction dans le registre. Le registre génère périodiquement des blocs en examinant toutes les transactions reçues pendant la période de collecte, l'intervalle entre deuxcréations de blocs et en atteignant un consensus parmi les petites cellules distribuées à travers le bloc grâce à l'algorithme BFT. Chaque transaction reçue pendant la période de collecte sera combinée et stockée en tant que bloc unique dans le registre. Une fois que les transactions sont vérifiées et que le bloc est enregistré, il sera accessible à tous les nœuds du réseau.Lorsqu'un nœud qui rejoint reçoit un paquet via le canal de communication, il récupère les balises stockées dans le registre distribué correspondant à ce paquet en utilisant le numéro de génération et l'ID source. Étant donné que la balise reçue via le canal de communication a pu passer par un processus de cryptage, elle ne sera pas identique à la balise récupérée dans le registre distribué, mais le nœud peut facilement effectuer des opérations cryptographiques à l'aide des vecteurs de codage reçus via le canal de communication et rendre les balises comparables. Les balises extraites du registre seront multipliées par le facteur de cryptage reçu avec le paquet, et si ces balises cryptées correspondent aux balises reçues avec les paquets, alors nous pouvons garantir qu'aucune modification des balises n'a été effectuée pendant la transition et conclure qu'il n'y a pas d'attaque de pollution de balises. De plus, en recréant les balises sur le paquet reçu à l'aide de clés partagées, l'intégrité des paquets peut être vérifiée pour s'assurer qu'il n'y a pas non plus d'attaques de contamination de données. Ce processus de

vérification en deux étapes assure la sécurité contre les attaques de contamination dans le réseau. La procédure de vérification de l'intégrité proposée au nœud récepteur est décrite dans l'algorithme suivant.

Algorithme : Algorithme de vérification

Data: Received packet $\mathbf{C}_i'$, $\mathbf{L}$ tags corresponding to $\mathbf{C}_i'$ retrieved from the bigchainDB database, Key set $\mathbf{K}_s$
Result: **1** if verification is successful and **0** if verification is failed. In case of a failed verification, the type of the attack is also reported.

Step 1:
Retrieve the coefficient matrix from the received packet
Step 2:
Multiply the tags retrieved from the database with the corresponding coefficients
Step 3:
Compare the tags with those appear in the received codeword.
if *they dont match* **then**
    Report Warning and Proceed
else
    Proceed
Step 4:
Create tags for the received packet using MAC algorithm on the packet payload
Step 5:
if *MAC algorithm output matches with the tags retrieved from database* **then**
    $1 \longleftarrow$ Return
else
    $0 \longleftarrow$ Return

IV.3. Modèle de distribution des clés

Pour vérifier les jetons et assurer la sécurité du schéma proposé, tous les nœuds participants doivent avoir au moins un ensemble de clés utilisées par le nœud source pour générer les jetons. Une bonne distribution des clés fait partie intégrante du succès d'un système d'intégrité. Cependant, le partage de la clé entière avec chaque nœud participant permettra au nœud adverse d'obtenir la clé et de contourner le contrôle d'intégrité. Le nœud

adverse peut polluer le paquet ainsi que créer un nouvel ensemble de balises à l'aide des clés qu'il détient afin que les paquets contaminés passent le contrôle de pollution des données. Pour éviter cela, de nombreux schémas d'intégrité antérieurs ont proposé un modèle de distribution de clés dans lequel seul un sous-ensemble de clés utilisées par le nœud source sera distribué aux nœuds participants. Cependant, ce modèle de distribution de clés présente limitations dans les situations de collusion contradictoire, où plusieurs nœuds malveillants se combinent pour vaincre les schémas d'intégrité. De plus, dans un réseau dense de nœuds cellulaires envisagé dans les cas d'utilisation de la 5G et au-delà, de tels schémas de distribution de clés partielles seraient difficiles et complexes. Dans notre schéma d'intégrité proposé, nous fournissons un chemin de partage de balise secondaire pour garantir que même si le nœud adverse a accès à toutes les clés, il ne peut pas frauder le schéma d'intégrité. En fait, nous proposons un modèle de distribution de clés où tous les nœuds participants ont accès à l'ensemble complet des clés. Dans ce cas, même si un nœud adverse injecte dans un paquet contaminé des balises correspondant au paquet contaminé, le nœud valideur suivant identifiera ces balises contaminées en les comparants à des balises issues de petites cellules. Étant donné que les entrées du registre distribué sont immuables et sécurisées, les nœuds récepteurs peuvent toujours traiter les jetons récupérés à partir d'eux comme les jetons d'origine et toute incohérence dans les jetons récupérés. La récupération du registre et des jetons reçus via la communication indiquerait une attaque par contamination. . Cependant, dans ce cas, le nœud honnête qui détecte l'attaque polluante interprétera l'attaque comme une attaque polluante par balise plutôt qu'une attaque par pollution de données, puisque les balises correspondront au paquet reçu.

Le partage de la clé complète avec tous les nœuds participants est un processus simple par rapport au modèle de partage de clé partiel calculé. Cependant, dans l'environnement dense des petites cellules mobiles, cela présente des problèmes de praticité et d'évolutivité pour partager en toute sécurité les clés avec tous les nœuds. Si tous les nœuds participants pouvaient également être des nœuds sources, il y aurait un grand nombre de clés, et le stockage de toutes ces clés à chaque nœud nécessite que les nœuds aient une grande capacité de stockage. En outre, l'ensemble du réseau peut s'étendre sur une vaste zone géographique et faire partie de différentes petites cellules, de sorte que le partage de l'ensemble des clés avec tous les nœuds est également inutile. Par conséquent, nous proposons une distribution initiale des clés au niveau des sous-cellules, et que les clés

soient également partagées via la superposition des petites cellules selon les besoins [16].La pré-distribution des clés est effectuée par les sous-parcelles, et chaque nœud de la sous-parcelle se voit attribuer un ensemble de clés. Cet ensemble de clés peut être utilisé par n'importe quel nœud de la sous-parcelle pour créer des balises. Étant donné que tous les nœuds de la sous-parcelle ont accès au jeu de clés, ces nœuds peuvent vérifier les jetons si nécessaire. Cependant, dans le cas d'une communication entre les sous-parcelles , les nœuds d'une autre sous-parcelle n'auront pas accès aux clés utilisées par le bouton d'alimentation. Dans de tels cas, les clés d'une petite cellule doivent être partagées avec d'autres tuiles, et un registre distribué peut être utilisé pour partager les clés entre les tuiles.Chaque fois qu'un nœud source lance une transaction qui a un nœud de destination dans une autre sous-parcelle, l'en-tête de la sous-parcelle génère une transaction qui inclut le jeu de clés correspondant à cette sous-cellule ainsi que des détails sur la sous-parcelle, le bouton d'alimentation et le haut de la petite cellule. Une fois que le jeu de clés est vérifié et stocké dans le registre, n'importe quel nœud de n'importe quelle sous-parcelle peut récupérer le jeu de clés et effectuer la vérification nécessaire. Cependant, dans le cas de nœuds qui n'ont pas besoin de clé, ils peuvent ne pas les télécharger. De plus, lorsque les clés correspondant à une petite cellule sont stockées dans un registre distribué détenu par la microcellule, tout nœud de cette tuile particulière peut initier une communication intercellulaire et les nœuds récepteurs peuvent dériver les clés nécessaires de la cellule existante entrée. Ainsi, toutes les clés seront éventuellement disponibles dans le magasin distribué et n'importe quel nœud pourra y récupérer les clés nécessaires si nécessaire. Parfois, il est nécessaire de mettre à jour périodiquement la clé [119] dans le réseau pour résoudre diverses difficultés. Dans de tels cas, nous pouvons suivre le même processus de mise à jour de la clé au niveau de la tuile, puis télécharger la clé si nécessaire. Les dernières entrées du registre sont toujours utilisées pour mettre à jour la clé.

IV.4. Schéma d'intégrité léger

Une version allégée du schéma d'intégrité est discutée ici pour réduire les coûts de calcul et de communication du système. Ici, nous réduisons le coût de calcul en réduisant le nombre de balises vérifiées à chaque nœud, et le coût de bande passante est réduit en limitant le partage de balises uniquement à travers la superposition de sous-plots. Dans la carte d'origine, plusieurs jetons ont été créés pour un paquet spécifique pour une sécurité accrue. Chaque balise fournit un niveau de sécurité de 1/q où q est la taille du champ fini

utilisé dans le descripteur RLNC. Dans la version complète du schéma d'intégrité, toutes ces balises sont vérifiées à chaque nœud intermédiaire pour assurer un niveau de sécurité élevé. Si L balises sont attachées aux paquets, cela fournit un niveau de sécurité de 1/qL de probabilité de violation du schéma d'intégrité par un nœud malveillant. Cependant, pour les applications pratiques, ce niveau de sécurité élevé peut ne pas être nécessaire. Dans le schéma compact, nous limitons le nombre de balises vérifiées à un niveau inférieur, en fonction du niveau de sécurité requis. Cela réduit le nombre de vérifications effectuées au nœud récepteur et réduit ainsi les exigences de calcul à ce niveau.

Une autre amélioration de la version Lite concerne la surcharge de bande passante. Dans la version complète du schéma, les paquets transmis sont étendus avec des balises. De plus, les balises sont également fournies sur une petite superposition de cellules. Cependant, retirer les balises des paquets à envoyer sur le canal de communication ne réduit pas la sécurité du schéma. Cela garantit que le schéma d'intégrité non seulement réduit la surcharge de communication, mais évite également la probabilité d'une attaque de contamination de balises. Dans ce scénario, les paquets transmis sur le canal n'ont pas d'overhead autre que le taux de code des paquets d'origine. À la réception du paquet, le nœud récepteur récupère les balises appropriées du grand livre distribué. Ces balises sont chiffrées en utilisant les coefficients reçus, comme décrit dans le chapitre 3, section a - Protocole MAC homomorphe modifié. À la fin de ce processus, ces balises brouillées sont identiques aux balises brouillées lors de la transmission sur le canal. Maintenant qu'il n'y a plus de balises à comparer, le nœud récepteur peut directement effectuer une vérification de l'attaque de contamination de données, comme discuté ci-dessus. De cette manière, nous éliminons la possibilité d'une attaque de contamination de balises sur le réseau et minimisons la charge de bande passante.

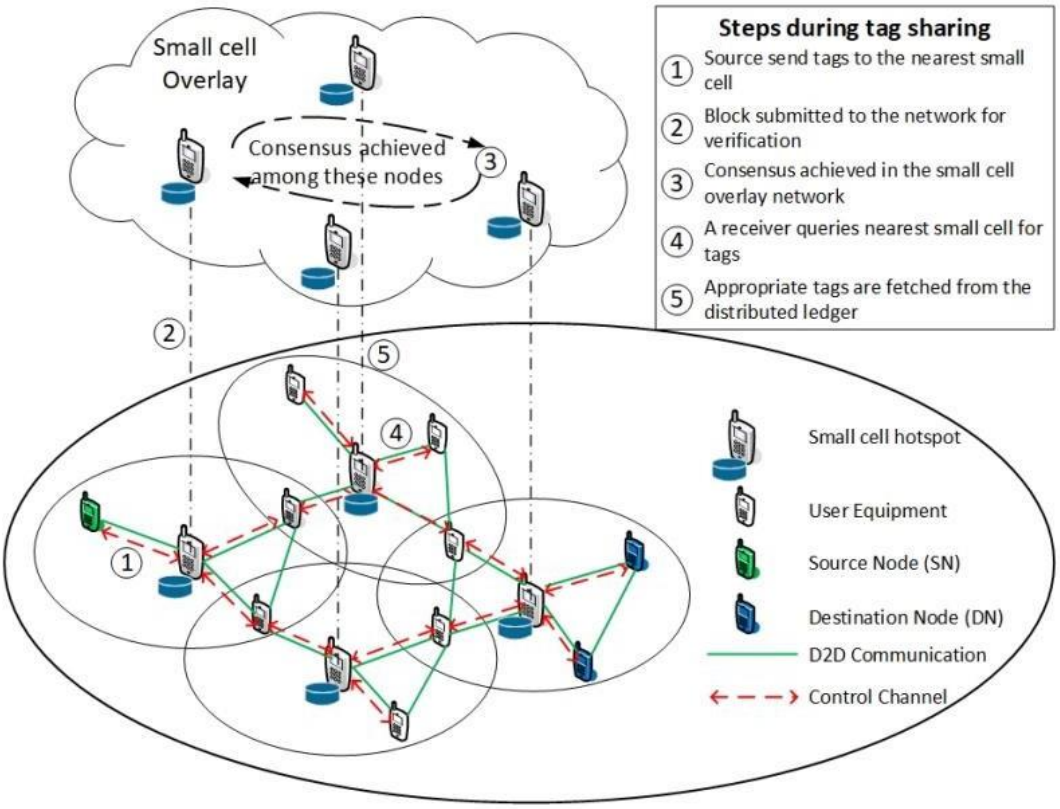


Figure IV.2. Description étape par étape du schéma de partage de balises proposé

VI.5. Protocole de gestion de clés distribuées pour les schémas d'intégrité

Les schémas d'intégrité que nous avons proposés pour les réseaux mobiles de nouvelle génération compatibles avec NC nécessitent encore un ensemble de clés privées partagées avec les nœuds participants. Ces clés sont utilisées pour générer des codes MAC au niveau des nœuds sources et pour la vérification au niveau des nœuds récepteurs. La plupart des schémas d'intégrité traditionnels ont des modèles de distribution de clés spécifiques, tels que le système sans c-couverture. Ces schémas de distribution de clés jouent un rôle important dans la protection du schéma d'intégrité contre les adversaires complices. Essentiellement, les schémas de distribution de clés traditionnels sont utilisés pour distribuer un ensemble de clés de telle manière qu'aucun nœud n'ait l'ensemble complet de clés utilisé par le nœud source pour générer les signaux. Cependant, effectuer une telle distribution de clés avec des contraintes en fonction du nombre de participants dans le réseau peut être fastidieux dans un réseau dense de nœuds mobiles. De plus, dans le cas des réseaux mobiles, le voisinage des nœuds peut être instable, ce qui rend encore plus

difficile la mise en pratique.Ainsi, pour passer aux réseaux futurs, l'idée de distribuer des clés à des environnements sécurisés compatibles avec NC nécessite des avancées majeures. Le protocole de gestion de clés distribuées est une solution proposée pour résoudre ce problème. Ce protocole permet de distribuer les clés de manière dynamique et distribuée, en utilisant des techniques de partage de secrets, de sorte que chaque nœud ne possède qu'une fraction des clés nécessaires pour vérifier l'intégrité des paquets. De plus, ce protocole permet également de renouveler régulièrement les clés pour éviter les attaques de cryptanalyse. En utilisant ce protocole de gestion de clés distribuées, les schémas d'intégrité peuvent être utilisés efficacement dans les réseaux mobiles de nouvelle génération, en garantissant la sécurité des données transmises entre les nœuds, même dans un environnement instable et dense.

Contrairement aux schémas d'intégrité traditionnels, nos propositions dans la mémoire considèrent ce problème de génération de clés comme faisant partie de l'analyse de la scalabilité et garantissent que la confidentialité du schéma d'intégrité ne dépend pas du nombre de clés compromises. Même s'il existe des ennemis complices qui peuvent accumuler tous les ensembles de clés utilisés par le bouton d'alimentation, ils ne peuvent pas tromper un nœud authentique en raison de notre mécanisme de partage de balises alternatif, qu'il soit centralisé ou distribué. Étant donné que le partage de balises sur le canal alternatif permet au nœud récepteur d'avoir la possibilité de vérifier l'intégrité des paquets et des balises qu'il reçoit en les comparant aux balises originales extraites du mécanisme de partage, la distribution de clés pour le schéma d'intégrité proposé est beaucoup plus simple que le schéma d'intégrité traditionnel. Cependant, il a encore certaines contraintes et nécessite la satisfaction des mécanismes de distribution des clés. L'analyse de sécurité du schéma d'intégrité a montré que dans la plupart des cas, une seule balise ne sera pas en mesure d'atteindre un niveau de sécurité satisfaisant, et la probabilité de casser le schéma d'intégrité dépend uniquement du nombre de balises utilisées. Plus il y a de balises, plus le schéma d'intégrité est sûr. Par conséquent, avoir plusieurs balises, et donc plusieurs clés, est une exigence nécessaire du réseau. Cependant, dans un réseau dense avec un grand nombre de dispositifs dans de nombreuses petites cellules, couvrant une grande zone géographique, la distribution du même ensemble de clés à tous les participants via une distribution centralisée est en fait une tâche difficile. Pour contourner cela, comme décrit dans la section III. Modèle de distribution des clés, les clés peuvent être

initialement partagées dans une petite cellule de base, et chaque fois que des clés doivent être partagées avec des sous-plots différents, le profil du schéma de partage de clés distribué peut être activé. Cela rend la gestion de la distribution de clés un processus en deux étapes. Initialement, un centre de distribution de clés attribue un ensemble de clés pour chaque sous-cellule ou groupe de sous-cellules voisines avec le même domaine de sécurité. La communication multi-sauts compatible avec NC est couramment utilisée dans des zones plus petites telles que les villes intelligentes ou les stades pour la diffusion de contenu, et dans la plupart des cas, elle peut être un domaine sécurisé avec un mot de passe unique. Dans le domaine sécurisé, tous les nœuds participants utiliseront le même ensemble de clés pour générer et vérifier la balise. Cependant, dans un réseau cellulaire, il est possible qu'un utilisateur mobile passe d'un domaine sécurisé à un autre, ou qu'un nouveau nœud apparaisse sur le réseau. Lorsqu'un nouveau nœud entre dans un domaine sécurisé, afin de devenir partie prenante d'un réseau de communication MP-MH compatible avec NC, il doit également posséder l'ensemble spécifique de clés utilisé dans cette zone.

L'objectif est de résoudre le problème de partage de clés et de fournir une solution de registre distribué similaire à la blockchain qui répond aux exigences de faible latence et de débit minimal. Ce schéma est en outre soutenu par le schéma HO basé sur le signal de référence montant (UL RS), qui résout le problème d'une en-tête de signalisation HO élevée dans les mises en œuvre de petites cellules comprenant un grand nombre d'échanges de clés. Nous analysons également le coût de la gestion des clés dans HO pour assurer une NC sûre dans un environnement de petites cellules. Nous combinons le schéma HO basé sur UL RS (UL-HO) et la méthode de partage de clés basée sur la blockchain, et fournissons un contrôleur de sécurité basé sur la blockchain et HO (contrôleur BSH) pour assurer un processus HO fluide et sûr pour les téléphones cellulaires compatibles avec NC dans les petites cellules. La gestion des clés basée sur la blockchain réduit le nombre d'échanges de signaux dans le HO par rapport aux méthodes traditionnelles, et les plans HO basés sur UL RS réduisent la latence entraînée par la vérification de la blockchain. Cette approche proposée est étudiée et comparée à d'autres schémas traditionnels en termes d'en-têtes de signalisation et de différents paramètres de sécurité.

a. Modèle de système:

Dans ce chapitre, un environnement de petites cellules est discuté dans lequel les dispositifs mobiles participants (c'est-à-dire, UE) utilisent le NC pour la communication D2D. Plus précisément, les mobiles utilisent RLNC pour la communication D2D et ces mobiles sont connectés au réseau central via des points d'accès ou des stations de base (BS) cellulaires de petite taille. De plus, nous croyons que les BS connectés auront une fonctionnalité intégrée appelée Contrôleur de sécurité et de HO basé sur la blockchain (BSH). Ces BS peuvent potentiellement être n'importe quel dispositif (par exemple, BS pico/micro/macro, dispositifs mobiles, etc.). Nous appelons cette cellule une cellule compatible BSH ou une cellule BSH. Ces contrôleurs BSH forment une superposition blockchain qui sert de registre distribué sécurisé pour le schéma d'intégrité et le protocole de gestion de clés décrits dans ce chapitre. Tous les dispositifs mobiles, également appelés nœuds dans le contexte de NC et de blockchain, sont connectés à au moins un contrôleur BSH sur le canal de contrôle sécurisé, comme indiqué dans la figure 4.2. Dans ce chapitre, nous nous concentronsspécifiquement sur l'échange de clés qui a lieu pendant le processus HO lorsqu'un nœud faisant partie du réseau de communication NC dans une cellule BSH se déplace vers une autre cellule BSH pour devenir partie prenante de la communication NC activée dans la cellule BSH cible.

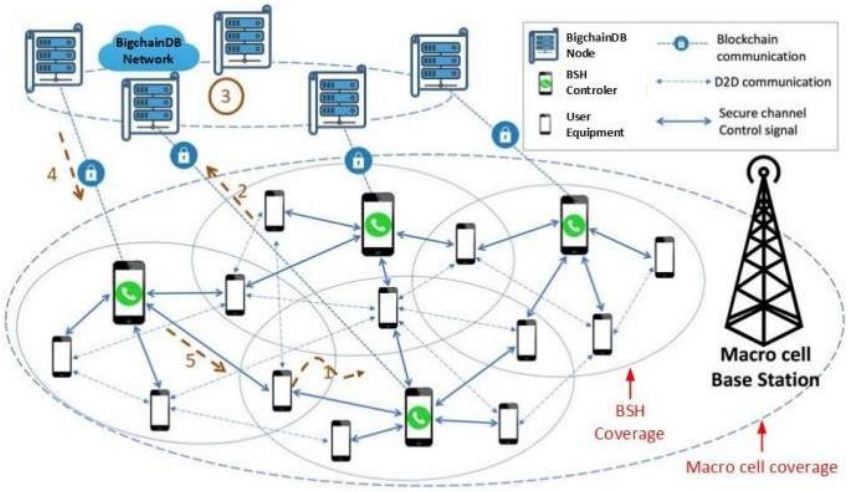


Figure IV.2. Échange des clés via la superposition blockchain des contrôleurs BSH. Les flèches numérotées représentent les différentes étapes de la procédure HO.

b. Schéma de gestion des clés basé sur la blockchain proposé:

Dans le schéma d'intégrité basé sur MAC, le nœud source génère des jetons de sécurité sur les paquets d'origine. Ces jetons sont attachés aux paquets avant la transmission et sont partagés dans le réseau via une superposition de blockchain implémentée à l'aide de bigchainDB [21]. Un nœud de réception peut vérifier l'authenticité des balises reçues sur le canal de communication en les comparant avec les jetons correspondants stockés dans bigchainDB, puis vérifier l'intégrité des paquets en régénérant les balises à l'aide de la clé secrète partagée sur les paquets reçus. Le schéma d'intégrité dans [11] prend en compte une condition d'adversaire très forte où l'adversaire peut avoir accès à toutes les clés utilisées par le nœud source mais ne peut toujours pas contourner la vérification d'intégrité. Cela simplifie le processus de distribution de clés car tous les nœuds participants peuvent avoir accès à toutes les clés utilisées pour générer la balise.

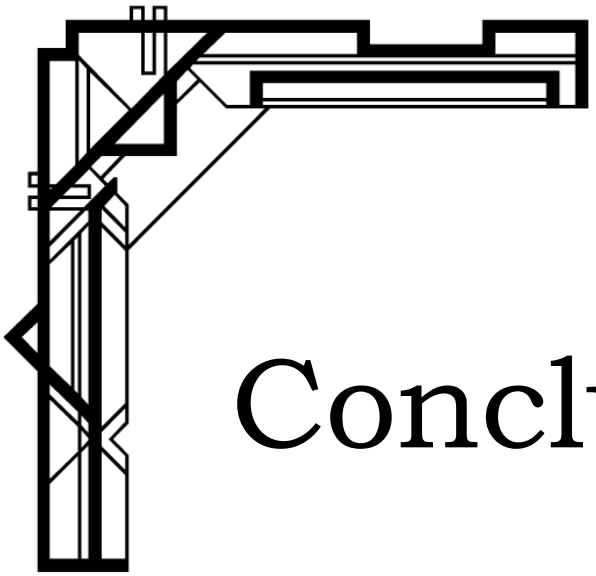
Cependant, dans un environnement de petites cellules denses, il peut ne pas être pratique de distribuer directement des clés à chaque nœud participant par une seule entité de distribution de clés. De plus, différents sous-parcelles peuvent appartenir à différents contrôleurs BSH et donc à différents domaines de sécurité en fonction de leur emplacement, du fournisseur de services et de la plateforme d'application. Ainsi, les clés pour le schéma d'intégrité peuvent être partagées au sein d'une cellule BSH. Chaque nœud (par exemple un UE) dans une cellule BSH particulière doit avoir accès à l'ensemble de clés utilisé dans cette cellule afin de pouvoir vérifier l'intégrité des paquets générés et transmis dans cette cellule BSH. Cependant, tout nouveau nœud entrant dans la nouvelle cellule BSH doit obtenir cet ensemble de clés dans le cadre de son authentification pour devenir partie prenante dans la communication NC dans la cellule BSH. Cela s'applique également à un nœud qui se déplace d'une cellule BSH à une autre. Cela est rendu possible par le revêtement distribué du contrôleur BSH qui est similaire en concept à [16]. Dans ce chapitre, nous concentrons sur l'impact de ce schéma de partage de clés sur la procédure de HO. Chaque contrôleur BSH fait partie de la superposition de blockchain telle que décrite dans [14]. De plus, ces contrôleurs BSH conservent les clés secrètes utilisées dans la cellule BSH respective pour assurer l'intégrité des paquets. Chaque fois qu'un nœud passe d'une cellule BSH à une autre, dans le cadre du processus de HO, ces clés doivent également être partagées avec le nœud

entrant. Cependant, dans notre schéma de partage de clés basé sur la blockchain, nous proposons une méthode de partage de clés légèrement différente de la méthode de partage de clés traditionnelle, c'est-à-dire que le contrôleur de la cellule cible, appelé contrôleur BSH cible, partage directement la clé avec le contrôleur BSH source et la partage avec l'utilisateur demandant le HO. Contrairement à notre approche, au lieu de partager directement les clés avec le contrôleur BSH source, les clés sont partagées via une blockchain. Ainsi, chaque fois qu'un nœud demande un HO, le contrôleur BSH cible télécharge l'ensemble de clés utilisées dans cette cellule sur la blockchain en tant que bloc candidat. La blockchain validera les blocs candidats pendant la période de collecte entre deux vérifications de blocs, et une fois le bloc candidat validé, le contrôleur BSH source aura également une copie du bloc vérifié grâce au consensus obtenu dans la blockchain, et pourra partager les clés requises avec le nœud subissant le HO. Ce partage de clés est effectué avec des processus d'authentification dans le HO car tous les nœuds du réseau n'ont pas besoin de détenir des clés pour toutes les sous-parcelles. Seuls les nœuds mobiles qui se déplacent vers une petite cellule peuvent les récupérer auprès du contrôleur BSH, et cela se fait dans le cadre du signal HO. La description étape par étape du processus de HO est présentée dans la figure 4.2. Il convient de noter que tous les nœuds demandant un HO entre la validation de deux blocs consécutifs recevront la clé après la mise à jour du nouveau bloc dans la blockchain.

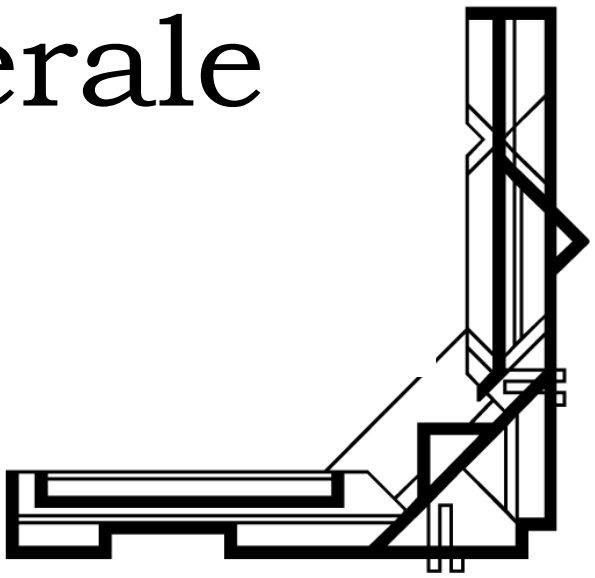
Une fois que le contrôleur BSH a stocké son ensemble de clés dans la blockchain, tout autre nœud entrant (via le HO) aura un accès facile à cet ensemble de clés particulier. Étant donné que la blockchain est une liste de dossiers en constante évolution, un bloc vérifié ne sera jamais modifié et sera toujours disponible pour les nœuds participants. De plus, c'est un registre distribué et décentralisé, de sorte qu'une fois qu'un bloc est vérifié et ajouté à la chaîne, il sera mis à disposition non seulement du contrôleur BSH qui a initié la demande, mais aussi de tous les contrôleurs BSH qui font partie de la blockchain. Par conséquent, tout autre nœud qui nécessite le HO peut recevoir la clé directement du contrôleur BSH source. De plus, tous les blocs candidats dans une période de collecte spécifique seront mis à jour sur la blockchain en une seule vérification de bloc. Cela réduit considérablement le coût de signalisation dans un réseau dense de nœuds mobiles.

Conclusion

Un nouveau schéma d'intégrité efficace soutenu par la superposition distribuée de sous-parcelles est présenté et analysé dans ce chapitre. S'appuyer sur un contrôleur central pour sécuriser le réseau peut entraîner un certain nombre de problèmes, tels que des vulnérabilités et des problèmes de mise à l'échelle. De plus, pour les réseaux mobiles dans les dynamiques de prochaine génération, le schéma d'intégrité distribué serait plus approprié. Enfin, l'utilisation d'une base de données distribuée de style blockchain pour une sécurité renforcée et une distribution de clés à travers un réseau dense de petites cellules s'est avérée efficace contre les attaques de contamination qui ne pouvaient pas être détectées sans coûts significatifs. Dans cette proposition, nous utilisons le protocole HMAC modifié proposé dans le chapitre 3 pour assurer l'intégrité du réseau MP-MH activé par NC, et utilisons le registre distribué pour le partage d'étiquettes, une substitution nécessaire pour le schéma d'intégrité. De plus, une légère variante de l'approche proposée, plus adaptée aux environnements de type IoT à ressources limitées, et un modèle de distribution de clés efficace sont introduits dans le chapitre.



Conclusion générale



Ce mémoire de Master a exploré le concept d'un schéma d'intégrité distribuée spécifiquement conçu pour les réseaux sans fil de nouvelle génération. L'objectif était de répondre aux défis de sécurité et de confidentialité posés par ces réseaux avancés, caractérisés par leur nature distribuée, leur évolutivité et leur hétérogénéité.

Au cours de cette étude, nous avons examiné les approches traditionnelles d'intégrité des données, qui sont principalement centralisées, et mis en évidence leurs limitations dans le contexte des réseaux sans fil de nouvelle génération. Nous avons également étudié les technologies et les protocoles existants liés à l'intégrité des données dans les réseaux sans fil, en mettant l'accent sur les défis spécifiques et les besoins particuliers de ces réseaux avancés.

En nous appuyant sur ces connaissances, nous avons proposé un schéma d'intégrité distribuée novateur adapté aux réseaux sans fil de nouvelle génération. Ce schéma vise à surmonter les limitations des approches centralisées en permettant une vérification décentralisée de l'intégrité des données. Il repose sur des mécanismes de confiance et des protocoles de communication sécurisés pour garantir que les données échangées restent intègres, même dans un environnement sans fil distribué et dynamique.

L'implémentation de ce schéma d'intégrité distribuée ouvre la voie à de nombreux avantages pour les réseaux sans fil de nouvelle génération. Il renforce la sécurité des communications en détectant rapidement toute altération ou modification non autorisée des données, ce qui est crucial dans des domaines sensibles tels que les systèmes de santé connectés, les véhicules autonomes et les infrastructures intelligentes.

Cependant, il convient de noter que notre schéma n'est pas exempt de défis. Des questions telles que l'overhead de communication, la gestion des clés de sécurité et l'évolutivité du système nécessiteront une attention continue dans les travaux futurs. De plus, des études supplémentaires seront nécessaires pour évaluer la performance et la robustesse de notre schéma dans des environnements réels et à grande échelle.

En conclusion, ce mémoire de Master a proposé un schéma d'intégrité distribuée prometteur pour les réseaux sans fil de nouvelle génération. Ce schéma représente une avancée significative dans le renforcement de la sécurité des communications sans fil, en offrant une vérification décentralisée de l'intégrité des données. Nous espérons que cette contribution stimulera davantage de recherches et d'innovations dans le domaine de la

sécurité des réseaux sans fil, favorisant ainsi le développement et l'adoption des réseaux sans fil de nouvelle génération dans divers secteurs de l'économie numérique.

Bibliographie

[1] Rudolf Ahlswede, Ning Cai, S-YR Li, and Raymond W Yeung. Network information flow. IEEE Transactions on information theory, 46(4):1204–1216, 2000 (cited on pages vii, xv, 1,).

[2] Ning Cai and Raymond W Yeung. Secure network coding on a wiretap network. IEEE Transactions on Information Theory, 57(1):424–435, 2010 (cited on pages vii, xv, 20, 117).

[3] Christos Gkantsidis and Pablo Rodriguez Rodriguez. Network coding for large scale content distribution. In Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Volume 4, pages 2235–2245. IEEE, 2005 (cited on pages vii, xv, 25, 35).

[4] Tracey Ho, Muriel Médard, Ralf Koetter, et al. A random linear network coding approach to multicast. IEEE Transactions on Information Theory, 52(10):4413–4430, 2006 (cited on pages vii, ix, xv, xvii, 10, 23).

[5]N. J. Hernandez Marcano, J. Heide, D. E. Lucani, and F. H. P. Fitzek. On transmission policies in multihop device-to-device communications with network coded cooperation. In European Wireless 2016; 22th European Wireless Conference, pages 1–5, 2016 (cited on pages vii, xv, 41, 76).

[6] Alejandro Cohen, Homa Esfahanizadeh, Bruno Sousa, et al. Bringing network coding into sdn: architectural study for meshed heterogeneous communications. IEEE Communications Magazine, 59(4):37–43, 2021 (cited on pages vii, xv, 51, 117).

[7] Jonathan Rodriguez, Ayman Radwan, Cláudia Barbosa, et al. Secret - secure network coding for reduced energy next generation mobile small cells: a european training network in wireless communications and networking for 5g. In 2017 Internet Technologies and Applications (ITA), pages 329–333. IEEE, 2017 (cited on pages vii, viii, xv, xvi, 4, 6, 39, 41, 111).

[8]V. Adat Vasudevan, C. Tselios, and I. Politis. On security against pollution attacks in network coding enabled 5g networks. IEEE Access, 8:38416–38437, 2020 (cited on pages viii, xvi, 19, 63).

[9] Shweta Agrawal and Dan Boneh. Homomorphic macs: mac-based integrity for network coding. In International Conference on Applied Cryptography and Network Security, pages 292–305. Springer, 2009 (cited on pages viii, xvi, 27, 35, 37, 44, 45).

[10] Vipindev Adat, Ilias Politis, Christos Tselios, and Stavros Kotsopoulos. Secure network

coding for sdn-based mobile small cells. In International Conference on Broadband Communications, Networks and Systems, pages 347–356. Springer, 2018 (cited on pages viii, ix, xvii, 51, 54, 60, 63, 66, 68).

[11] Vipindev Adat, Ilias Politis, Christos Tselios, Panagiotis Galiotos, and Stavros Kotsopoulos. On blockchain enhanced secure network coding for 5g deployments. In 2018 IEEE Global Communications Conference (GLOBECOM), pages 1–7. IEEE, 2018 (cited on pages viii, xvii, 58, 63, 88–90, 97, 104).

[12] Peng Zhang, Yixin Jiang, Chuang Lin, et al. Padding for orthogonality: efficient subspace authentication for network coding. In 2011 Proceedings IEEE INFOCOM, pages 1026–1034. IEEE, 2011 (cited on pages viii, xvii, 30, 35, 41, 44, 61, 63, 104, 105).

[13] Alireza Esfahani, Georgios Mantas, Jonathan Rodriguez, and José Carlos Neves. An efficient homomorphic mac-based scheme against data and tag pollution attacks in network coding-enabled wireless networks. International Journal of Information Security, 16(6):627–639, 2017 (cited on pages viii, xvii, 32, 35, 48, 61, 63, 104, 105).

[14]V. Adat, I. Politis, C. Tselios, and S. Kotsopoulos. Blockchain enhanced secret small cells for the 5g environment. In 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pages 1– 6, September 2019 (cited on pages ix, xvii, 88, 96, 97).

[15]V. Adat Vasudevan, I. Politis, and F. Gil-Castiñeira. A distributed integrity scheme for network coding enabled future networks. In preparation, 2021 (cited on pages ix, xvii).

[16] Vipindev Adat, Tafseer Akhtar, Ilias Politis, Christos Tselios, and Stavros Kotsopoulos. Towards secure network coding enabled mobile small cells. In 2019 IEEE Global Communications Conference (GLOBECOM), pages 1–6. IEEE, 2019 (cited on pages ix, xvii, 80, 94, 97).

[17] Vipindev Adat Vasudevan, Muhammad Tayyab, George P Koudouridis, Xavier Gelabert, and Ilias Politis. An integrated approach for energy efficient handover and key management protocol for secure nc-enabled small cells. Computer Networks, Under review (cited on pages ix, xvii).

[18] Vipindev Adat, Reza Parsamehr, Ilias Politis, Christos Tselios, and Stavros Kotsopoulos. Malicious user identification scheme for network coding enabled small cell environment. In ICC 2020-2020 IEEE International Conference on Communications (ICC), pages 1–6. IEEE, 2020 (cited on pages ix, xvii, 65).

[19] Vipindev Adat Vasudevan, Tafseer Akhtar, Christos Tselios, Ilias Politis, and Stavros Kotsopoulos. Study of secure network coding enabled mobile small cells. In ICC 2021- IEEE International Conference on Communications, pages 1–5. IEEE, 2021 (cited on pages ix, xvii).

[20] Morten V Pedersen, Janus Heide, and Frank HP Fitzek. Kodo: an open and research oriented network coding library. In International Conference on Research in Networking, pages 145–152. Springer, 2011 (cited on pages ix, xviii, 82).

[21] Germany BigchainDB GmbH Berlin. Bigchaindb 2.0 : the blockchain database. BigchainDB white paper:1–14, 2018 (cited on pages ix, xviii, 76, 85, 97, 103).

[22] Frank Gabriel, Giang T Nguyen, Robert-Steve Schmoll, et al. Practical deployment of network coding for real-time applications in 5g networks. In 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), pages 1–2. IEEE, 2018 (cited on page 1).

[23] Vipindev Adat and BB Gupta. Security in internet of things: issues, challenges, axonomy, and architecture. Telecommunication Systems, 67(3):423–441, 2018 (cited on pages 1, 11).

[24] Theodore S Rappaport, Annamalai Annamalai, R Michael Buehrer, and William H Tranter. Wireless communications: past events and a future perspective. IEEE ommunications Magazine, 40(5):148–161, 2002 (cited on page 2).

[25] Bjorn A Bjerke. Lte-advanced and the evolution of lte deployments. IEEE Wireless Communications, 18(5):4–5, 2011 (cited on page 2).

[26] Frank HP Fitzek and Patrick Seeling. Why we should not talk about 6g. arXiv preprint

arXiv:2003.02079, 2020 (cited on page 2).

[27] Petar Popovski, Kasper Fløe Trillingsgaard, Osvaldo Simeone, and Giuseppe Durisi. 5g

wireless network slicing for embb, urllc, and mmtc: a communication-theoretic view. Ieee Access, 6:55765–55779, 2018 (cited on page 3).

[28] ITU-R M.2150-0. Detailed specifications of the terrestrial radio interfaces of international mobile telecommunications-2020 (imt-2020). URL: https://www.itu.int/rec/R-REC-M.2150-0-202102-I. (accessed: 15.07.2021) (cited on page 3).

[29] Akhil Gupta and Rakesh Kumar Jha. A survey of 5g network: architecture and emerging technologies. IEEE access, 3:1206–1232, 2015 (cited on page 6).

[30] Shih-Fan Chou, Te-Chuan Chiu, Ya-Ju Yu, and Ai-Chun Pang. Mobile small cell deployment for next generation cellular networks. In 2014 IEEE Global Communications Conference, pages 4852–4857. IEEE, 2014 (cited on page 6).

[31]M Celebiler and G Stette. On increasing the down-link capacity of a regenerative satellite repeater in point-to-point communications. Proceedings of the IEEE, 66(1):98– 100, 1978 (cited on page 8).

[32]S-YR Li, Raymond W Yeung, and Ning Cai. Linear network coding. IEEE transactions on information theory, 49(2):371–381, 2003 (cited on page 8).

[33] Christina Fragouli, Jean-Yves Le Boudec, and Jörg Widmer. Network coding: an instant primer. ACM SIGCOMM Computer Communication Review, 36(1):63–68, 2006 (cited on page 8).

[34] Kapil Bhattad, Krishna R Narayanan, et al. Weakly secure network coding. NetCod, Apr, 104, 2005 (cited on pages 8, 20).

[35] Tracey Ho, Muriel Medard, Jun Shi, Michelle Effros, and David R Karger. On andomized network coding. In Proceedings of the Annual Allerton Conference on Communication Control and Computing, volume 41 of number 1, pages 11–20. Citeseer, 2003 (cited on pages 8, 10).

[36]P. Georgakopoulos, T. Akhtar, I. Politis, et al. Coordination multipoint enabled small

cells for coalition-game-based radio resource management. IEEE Network, 33(4):63–69, July 2019 (cited on page 9).

[37]T. Akhtar, I. Politis, P. Georgakopoulos, and S. Kotsopoulos. Efficient radio resource management scheme in cooperative network using coalition game. In 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pages 1–6, September 2019 (cited on page 9).

[38]P. Georgakopoulos, T. Akhtar, and S. Kotsopoulos. On game theory-based coordination schemes for mobile small cells. In 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pages 1–5, September 2019 (cited on page 9).

[39]Lusa Lima, João P Vilela, Paulo F Oliveira, and João Barros. Network coding security: attacks and countermeasures. arXiv preprint arXiv:0809.1366, 2008 (cited on page 9). [40]Sachin Katti Dina Katabi Wenjun Hu and Hariharan Rahul Muriel Médard. The importance of being opportunistic: practical network coding for wireless environments. Newsletter ACM SIGCOMM Computer Communication Review, 36(4), 2006 (cited on page 9).

[41] Martin Hundebøll, Jeppe Ledet-Pedersen, Janus Heide, et al. Catwoman: implementation and performance evaluation of ieee 802.11 based multi-hop networks using network coding. In 2012 IEEE Vehicular Technology Conference (VTC Fall), pages 1–5. IEEE, 2012 (cited on page 9).

[42] Sudipta Sengupta, Shravan Rayanchu, and Suman Banerjee. An analysis of wireless network coding for unicast sessions: the case for coding-aware routing. In IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications, pages 1028–1036. IEEE, 2007 (cited on page 9).

[43] Alberto Lopez Toledo and Xiaodong Wang. Efficient multipath in sensor networks using diffusion and network coding. In 2006 40th Annual Conference on Information Sciences and Systems, pages 87–92. IEEE, 2006 (cited on page 9).

[44] Xinyu Zhang and Baochun Li. Optimized multipath network coding in lossy wireless networks. IEEE journal on selected areas in communications, 27(5):622–634, 2009 (cited on page 10).

[45]S Chachulski. Trading structure for randomness in wireless opportunistic routing. Proc. ACM SIGCOMM, Aug. 2007:169–180, 2007 (cited on page 10).

[46] Xinyu Zhang and Baochun Li. Dice: a game theoretic framework for wireless multipath network coding. In Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing, pages 293–302. ACM, 2008 (cited on page 10).

[47] Sachin Katti, Hariharan Rahul, Wenjun Hu, et al. Xors in the air: practical wireless network coding. In ACM SIGCOMM computer communication review, volume 36 of number 4, pages 243–254. ACM, 2006 (cited on page 11).

[48] Jilin Le, John CS Lui, and Dah-Ming Chiu. Dcar: distributed coding-aware routing in wireless networks. IEEE Transactions on Mobile Computing, 9(4):596–608, 2009 (cited on page 11).

[49] Saumitra Das, Yunnan Wu, Ranveer Chandra, and Y Charlie Hu. Context-based routing: techniques, applications and experience. In Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation, pages 379–392. USENIX Association, 2008 (cited on page 11).

[50] Denis Charles, Kamal Jain, and Kristin Lauter. Signatures for network coding. In 2006 40th Annual Conference on Information Sciences and Systems, pages 857–863. IEEE, 2006 (cited on pages 11, 24–26, 28, 29, 35).

[51] Philip A Chou, Yunnan Wu, and Kamal Jain. Practical network coding. In Proceedings of the annual Allerton conference on communication control and computing, volume 41 of number 1, pages 40–49. The University; 1998, 2003 (cited on pages 11, 58).

[52] Marcus De Ree, Georgios Mantas, Ayman Radwan, et al. Key management for beyond 5g mobile small cells: a survey. IEEE Access, 7:59200–59236, 2019 (cited on page 13).

[53] Ning Cai and Raymond W Yeung. Secure network coding. In Proceedings IEEE International Symposium on Information Theory, page 323. IEEE, 2002 (cited on pages 19, 20).

[54] Jing Dong, Reza Curtmola, Ruben Sethi, and Cristina Nita-Rotaru. Toward secure network coding in wireless networks: threats and challenges. In 2008 4th workshop on secure network protocols, pages 33–38. IEEE, 2008 (cited on pages 19, 21).

[55] Vahid Nazari Talooki, Riccardo Bassoli, Daniel E Lucani, et al. Security concerns and countermeasures in network coding based communication systems: a survey. Computer Networks, 83:422–445, 2015 (cited on pages 19, 20).

[56] Reza Parsamehr, Georgios Mantas, Ayman Radwan, Jonathan Rodriguez, and JoséFernán Martnez. Security threats in network coding-enabled mobile small cells. In International Conference on Broadband Communications, Networks and Systems, pages 337–346. Springer, 2018 (cited on page 19).

[57] Sidharth Jaggi, Michael Langberg, Tracey Ho, and Michelle Effros. Correction of adversarial errors in networks. In Proceedings. International Symposium on Information Theory, 2005. ISIT 2005. Pages 1455–1459. IEEE, 2005 (cited on page 20).

[58] Salim El Rouayheb, Emina Soljanin, and Alex Sprintson. Secure network coding for wiretap networks of type ii. IEEE Transactions on Information Theory, 58(3):1361– 1371, 2012 (cited on page 20).

[59] Kunihiko Harada and Hirosuke Yamamoto. Strongly secure linear network coding. IEICE transactions on fundamentals of electronics, communications and computer sciences, 91(10):2720–2728, 2008 (cited on page 20).

[60] Yanfei Fan, Yixin Jiang, Haojin Zhu, and Xuemin Shen. An efficient privacy- preserving scheme against traffic analysis attacks in network coding. In IEEE INFOCOM 2009, pages 2213–2221. IEEE, 2009 (cited on page 20).

[61] Yanfei Fan, Yixin Jiang, Haojin Zhu, Jiming Chen, and Xuemin Sherman Shen. Network coding based privacy preservation against traffic analysis in multi-hop wireless networks. IEEE Transactions on Wireless Communications, 10(3):834–843, 2010 (cited on page 20).

[62] Hugo Sousa-Pinto, Daniel E Lucani, and Joao Barros. Hide and code: session anonymity in wireless line networks with coded packets. In 2012 Information Theory and Applications Workshop, pages 262–268. IEEE, 2012 (cited on page 20).

[63] Lusa Lima, João Barros, and Ralf Koetter. Byzantine attacks against network coding in peer to peer distributed storage. In 2009 IEEE International Symposium on Information Theory, pages 1164–1168. IEEE, 2009 (cited on page 20).

[64] Konstantinos Pelechrinis, Marios Iliofotou, and Srikanth V Krishnamurthy. Denial of service attacks in wireless networks: the case of jammers. IEEE Communications surveys & tutorials, 13(2):245–257, 2010 (cited on page 20).

[65] Rutvij H Jhaveri. Mr-aodv: a solution to mitigate blackhole and grayhole attacks in aodv based manets. In 2013 Third International Conference on Advanced Computing and Communication Technologies (ACCT), pages 254–260. IEEE, 2013 (cited on page 20).

[66] BB Gupta, Ramesh Chandra Joshi, and Manoj Misra. Defending against distributed denial of service attacks: issues and challenges. Information Security Journal: A Global Perspective, 18(5):224–247, 2009 (cited on page 20).

[67] Hongyi Yao, Danilo Silva, Sidharth Jaggi, and Michael Langberg. Network codes resilient to jamming and eavesdropping. IEEE/ACM Transactions on networking, 22(6):1978–1987, 2014 (cited on page 21).

[68] Elias Kehdi and Baochun Li. Null keys: limiting malicious attacks via null space properties of network coding. In IEEE INFOCOM 2009, pages 1224–1232. IEEE, 2009 (cited on page 21).

[69] Alfred Asterjadhi and Michele Zorzi. Jenna: a jamming evasive network-coding neighbor-discovery algorithm for cognitive radio networks [dynamic spectrum management]. IEEE Wireless Communications, 17(4):24–32, 2010 (cited on page 21).

[70] Andrew John Newell, Reza Curtmola, and Cristina Nita-Rotaru. Entropy attacks and countermeasures in wireless network coding. In Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, pages 185–196. ACM, 2012 (cited on page 21).

[71] Yixin Jiang, Yanfei Fan, Xuemin Sherman Shen, and Chuang Lin. A self-adaptive probabilistic packet filtering scheme against entropy attacks in network coding. Computer Networks, 53(18):3089–3101, 2009 (cited on page 21).

[72] Ryo Iguchi and Yoshifumi Manabe. An efficient edge-based authentication for network coding against entropy attacks. In 2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW), pages 133–139. IEEE, 2014 (cited on page 21).

[73] Jing Dong, Reza Curtmola, and Cristina Nita-Rotaru. Secure network coding for wireless mesh networks: threats, challenges, and directions. Computer Communications, 32(17):1790–1801, 2009 (cited on pages 21, 37).

[74] Vahid Nazari Talooki and Jonathan Rodriguez. Jitter based comparisons for routing protocols in mobile ad hoc networks. In 2009 International Conference on Ultra Modern Telecommunications & Workshops, pages 1–6. IEEE, 2009 (cited on page 21).

[75] Dr G Padmavathi, Mrs Shanmugapriya, et al. A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576, 2009 (cited on page 21).

[76] Yuanyuan Zhang, Wassim Znaidi, Cédric Lauradoux, and Marine Minier. Flooding attacks against network coding and countermeasures. In 2011 5th International Conference on Network and System Security, pages 305–309. IEEE, 2011 (cited on page 21).

[77] Christos Gkantsidis, Pablo Rodriguez, et al. Cooperative security for network coding file distribution. In INFOCOM, volume 3 of number 2006, page 5, 2006 (cited on pages 25, 26, 35).

[78] Zhen Yu, Yawen Wei, Bhuvaneswari Ramkumar, and Yong Guan. An efficient signaturebased scheme for securing network coding against pollution attacks. In IEEE INFOCOM 2008-The 27th Conference on Computer Communications, pages 1409–1417. IEEE, 2008 (cited on pages 25, 28, 35).

[79] Aaram Yun, Jung Hee Cheon, and Yongdae Kim. On homomorphic signatures for network coding. IEEE Transactions on Computers, 59(9):1295–1296, 2010 (cited on pages 26, 35).

[80] Dan Boneh, David Freeman, Jonathan Katz, and Brent Waters. Signing a linear subspace: signature schemes for network coding. In International Workshop on Public Key Cryptography, pages 68–87. Springer, 2009 (cited on pages 26, 35).

[81] Maxwell N Krohn, Michael J Freedman, and David Mazieres. On-the-fly verification of

rateless erasure codes for efficient content distribution. In IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004, pages 226–240. IEEE, 2004 (cited on pages 26, 35).

[82]J Lawrence Carter and Mark N Wegman. Universal classes of hash functions. Journal of computer and system sciences, 18(2):143–154, 1979 (cited on page 27).

[83] Ran Canetti, Juan Garay, Gene Itkis, et al. Multicast security: a taxonomy and some efficient constructions. In IEEE INFOCOM'99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now (Cat. No. 99CH36320), volume 2, pages 708–716. IEEE, 1999 (cited on pages 27, 93, 103).

[84] MinJi Kim, Lusa Lima, Fang Zhao, et al. On counteracting byzantine attacks in network coded peer-to-peer networks. IEEE Journal on Selected Areas in Communications, 28(5):692–702, 2010 (cited on pages 28–30, 35).

[85] Yixin Jiang, Haojin Zhu, Minghui Shi, Xuemin Sherman Shen, and Chuang Lin. An efficient dynamic-identity based signature scheme for secure network coding. Computer Networks, 54(1):28–40, 2010 (cited on pages 28, 35).

[86] Intelligent Transportation Systems Committee et al. Ieee trial-use standard for wireless access in vehicular environments-security services for applications and management messages. IEEE Vehicular Technology Society Standard, 1609:2006, 2006 (cited on page 29).

[87] Yaping Li, Hongyi Yao, Minghua Chen, Sidharth Jaggi, and Alon Rosen. Ripple authentication for network coding. In 2010 Proceedings IEEE INFOCOM, pages 1–9. IEEE, 2010 (cited on pages 29, 35, 40).

[88] Nuttapong Attrapadung and Benot Libert. Homomorphic network coding signatures in the standard model. In International Workshop on Public Key Cryptography, pages 17–34. Springer, 2011 (cited on pages 29, 30, 35).

[89] Dario Catalano, Dario Fiore, and Bogdan Warinschi. Efficient network coding signatures in the standard model. In International Workshop on Public Key Cryptography, pages 680–696. Springer, 2012 (cited on pages 30, 35).

[90] Dan Boneh and Xavier Boyen. Short signatures without random oracles and the sdh assumption in bilinear groups. Journal of Cryptology, 21(2):149–177, 2008 (cited on page 30).

[91] Dario Catalano, Dario Fiore, and Bogdan Warinschi. Adaptive pseudo-free groups and applications. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 207–223. Springer, 2011 (cited on pages 30, 31).

[92] Chi Cheng, Tao Jiang, and Qian Zhang. Tesla-based homomorphic mac for authentication in p2p system for live streaming with network coding. IEEE Journal on Selected Areas in Communications, 31(9):291–298, 2013 (cited on pages 31, 35).

[93] Adrian Perrig, Ran Canetti, Dawn Song, and J Doug Tygar. Efficient and secure source authentication for multicast. In Network and Distributed System Security Symposium, NDSS, volume 1 of number 2001, pages 35–46, 2001 (cited on page 31).

[94] Xiaohu Wu, Yinlong Xu, Chau Yuen, and Liping Xiang. A tag encoding scheme against pollution attack to linear network coding. IEEE Transactions on Parallel and Distributed Systems, 25(1):33–42, 2014 (cited on pages 31, 35).

[95] Chi Cheng, Jemin Lee, Tao Jiang, and Tsuyoshi Takagi. Security analysis and improvements on two homomorphic authentication schemes for network coding. IEEE Transactions on Information Forensics and Security, 11(5):993–1002, 2016 (cited on page 31).

[96] Alireza Esfahani, Georgios Mantas, and Jonathan Rodriguez. An efficient null spacebased homomorphic mac scheme against tag pollution attacks in rlnc. IEEE Communications Letters, 20(5):918–921, 2016 (cited on pages 32, 33, 35).

[97] Alireza Esfahani, Du Yang, Georgios Mantas, Alberto Nascimento, and Jonathan Rodriguez. Dual-homomorphic message authentication code scheme for network coding-enabled wireless sensor networks. International Journal of Distributed Sensor Networks, 11(7):510251, 2015 (cited on pages 32, 35, 44, 48).

[98] Reza Parsamehr, Alireza Esfahani, Georgios Mantas, et al. A novel intrusion detection and prevention scheme for network coding-enabled mobile small cells. IEEE Transactions on Computational Social Systems, 6(6):1467–1477, 2019 (cited on pages 33, 63).

[99] Reza Parsamehr, Alireza Esfahani, Georgios Mantas, Jonathan Rodriguez, and JoseFernán Martnez-Ortega. A location-aware idps scheme for network coding-enabled mobile small cells. In 2019 IEEE 2nd 5G World Forum (5GWF), pages 91–96. IEEE (cited on pages 33, 35, 63–65, 68, 71).

[100] Reza Parsamehr, Georgios Mantas, Jonathan Rodriguez, and José-Fernán MartínezOrtega. Idlp: an efficient intrusion detection and location-aware prevention mechanism for network coding-enabled mobile small cells. IEEE Access, 8:43863–43875, 2020 (cited on pages 33, 35).

[101] Tandoh Lawrence, Ikram Ali, Tandoh Christopher, and Fagen Li. A bandwidth efficient hmac-based authentication scheme for network coding. Journal of Information Security and Applications, 55:102658, 2020 (cited on pages 34, 35, 59).

[102] Tandoh Lawrence, Fagen Li, Ikram Ali, et al. An hmac-based authentication scheme for network coding with support for error correction and rogue node identification. Journal of Systems Architecture, 116:102051, 2021 (cited on pages 34, 65).

[103] Sidharth Jaggi, Peter Sanders, Philip A Chou, et al. Polynomial time algorithms for multicast network code construction. IEEE Transactions on Information Theory, 51(6):1973–1982, 2005 (cited on page 36).

[104] Sidharth Jaggi, Michael Langberg, Sachin Katti, et al. Resilient network coding in the presence of byzantine adversaries. In IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications, pages 616–624. IEEE, 2007 (cited on page 36).

[105] Joao P Vilela, Lusa Lima, and Joao Barros. Lightweight security for network coding. In 2008 IEEE International Conference on Communications, pages 1750–1754. IEEE, 2008 (cited on page 36).

[106] Anh Le and Athina Markopoulou. Cooperative defense against pollution attacks in network coding using spacemac. IEEE Journal on Selected Areas in Communications, 30(2):442–449, 2012 (cited on pages 37, 40, 63–65).

[107] Alejandro Cohen, Guillaume Thiran, Vered Bar Bracha, and Muriel Médard. Adaptive causal network coding with feedback for multipath multi-hop communications. IEEE Transactions on Communications, 69(2):766–785, 2020 (cited on page 41).

[108] Hassan Ali-Ahmad, Claudio Cicconetti, Antonio De la Oliva, et al. An sdn-based network architecture for extremely dense wireless networks. In 2013 IEEE SDN for Future Networks and Services (SDN4FNS), pages 1–7. IEEE, 2013 (cited on page 42).

[109] Toktam Mahmoodi and Srini Seetharaman. On using a sdn-based control plane in 5g mobile networks. In Wireless World Research Forum, 32nd Meeting. Citeseer, 2014 (cited on page 42).

[110] Sandra Scott-Hayward, Gemma O'Callaghan, and Sakir Sezer. Sdn security: a survey. In 2013 IEEE SDN For Future Networks and Services (SDN4FNS), pages 1–7. IEEE, 2013 (cited on page 58).

[111] Mahdi Jafari Siavoshani, Christina Fragouli, and Suhas Diggavi. On locating byzantine attackers. In 2008 Fourth Workshop on Network Coding, Theory and Applications, pages 1–6. IEEE, 2008 (cited on pages 63–65, 72).

[112] Qiyan Wang, Long Vu, Klara Nahrstedt, and Himanshu Khurana. Identifying malicious nodes in network-coding-based peer-to-peer streaming networks. Technical report, 2009 (cited on pages 63–65, 67, 68, 72).

[113] MinJi Kim, Muriel Médard, and Joao Barros. Algebraic watchdog: mitigating misbehavior in wireless network coding. IEEE Journal on Selected Areas in Communications, 29(10):1916–1925, 2011 (cited on page 63).

[114] Angelos Antonopoulos and Christos Verikoukis. Misbehavior detection in the internet of things: a network-coding-aware statistical approach. In 2016 IEEE 14th International Conference on Industrial Informatics (INDIN), pages 1024–1027. IEEE, 2016 (cited on page 63).

[115] Ferran Adelantado and Christos Verikoukis. Detection of malicious users in cognitive radio ad hoc networks: a non-parametric statistical approach. Ad Hoc Networks, 11(8):2367–2380, 2013 (cited on page 63).

[116]C. Tselios, I. Politis, and S. Kotsopoulos. Enhancing SDN security for IoT-related deployments through blockchain. In 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pages 303–308, November 2017 (cited on page 66).

[117] Xiaodong Liang and Xiaofeng Qiu. A software defined security architecture for sdnbased 5g network. In 2016 IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC), pages 17–21. IEEE, 2016 (cited on page 66).

[118] Trent McConaghy, Rodolphe Marques, Andreas Müller, et al. Bigchaindb: a scalable blockchain database. white paper, BigChainDB, 2016 (cited on pages 77, 82, 85).

[119] Marcus de Ree, Georgios Mantas, Jonathan Rodriguez, and Ifiok E Otung. Distributed trusted authority-based key management for beyond 5g network coding- enabled mobile small cells. In 2019 IEEE 2nd 5G World Forum (5GWF), pages 80–85. IEEE (cited on page 81).

[120] Vitalik Buterin. Slasher: a punitive proof-of-stake algorithm. Ethereum Blog URL: https://blog. ethereum. org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm, 2014 (cited on page 85).

[121] Peter Fairley. Ethereum will cut back its absurd energy use. IEEE spectrum, 56(1):2932, 2018 (cited on page 85).

[122] Elli Androulaki, Artem Barger, Vita Bortnikov, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, page 30. ACM, 2018 (cited on page 85).

[123] Leif Walsh, Vyacheslav Akhmechet, and Mike Glukhovsky. Rethinkdb-rethinking database storage. Hexagram 49, Inc., 2009 (cited on page 85).

[124] Muhammad Tayyab, George P Koudouridis, Xavier Gelabert, and Riku Jäntti. Uplink reference signals for energy-efficient handover. IEEE Access, 8:163060–163079, 2020 (cited on pages 94, 101).

[125] Sarah Underwood. Blockchain beyond bitcoin, 2016 (cited on page 95).

[126] Muhammad Tayyab, Xavier Gelabert, and Riku Jäntti. A simulation study on handover in lte ultra-small cell deployment: a 5g challenge. IEEE 5G World Forum Conference, Dresden, Germany, 2019 (cited on page 101).

[127] Jeppe Krigslund, Jonas Hansen, Martin Hundeboll, Daniel E Lucani, and Frank HP Fitzek. Core: cope with more in wireless meshed networks. In 2013 IEEE 77th vehicular technology conference (VTC Spring), pages 1–6. IEEE, 2013 (cited on page 116).

[128] Alejandro Cohen, Rafael GL DOliveira, Salman Salamatian, and Muriel Médard. Network coding-based post-quantum cryptography. IEEE Journal on Selected Areas in Information Theory, 2(1):49–64, 2021 (cited on page 117).

[129] Craig Gentry. Fully homomorphic encryption using ideal lattices. In Proceedings of the forty-first annual ACM symposium on Theory of computing, pages 169–178, 2009 (cited on page 117).