République Algérienne Démocratique et Populaire

Ministère De l'Enseignement Supérieur et de la recherche scientifique

Université A/MIRA-Bejaia

Faculté de Technologie

Département de Génie Électrique

Mémoire de MASTER

Filière : TÉLÉCOMMUNICATION

Option : Réseaux et Télécommunications

Thème

Réseaux AD-HOC 5G avec Communication D2D

Réalisé par : **IMADALI Safia**

HAMMAM Sabiha

Soutenue le 13/10/2020, devant le jury composé de :

Mr. M. SADI,	Encadreur
Mr. N. BENAMIROUCHE,	Président
Mr. M. AZNI,	Examinateur

Année universitaire : 2019/2020

Remerciement

Nous remercions le dieu tout puissant de nous avoir donné force et courage pour

accomplir cet humble recueil.

Nous tenons à remercier le Professeur SADI de nous avoir accordé le privilège

d'apporter son aide et ses précieuses conseils, sa patience, sa générosité et enfin sa

disponibilité pour l'accomplissement de notre travail.

Nos remerciements vont également aux membres du jury pour l'honneur qu'ils nous font en acceptent d'examiner et de juger notre travail.

Notre reconnaissance à tous ceux qui ont contribue, de prés ou de loin a la réalisation du projet.

Nos sincères remerciements vont particulièrement à nos parents et à nos familles.

Dédicace

A ma très chère mère

Quoi que je fasse ou que je dise, je ne saurai point te remercier comme il se doit. Ton affection me couvre, ta bienveillance me guide et ta présence à mes côtés à toujours été ma source de force pour affronter les différents obstacles

A mon très cher père

Tu as toujours été à mes côtés pour me soutenir et m'encourager. Que ce travail traduit ma gratitude et mon affection.

A mon cher frère BELKACEM qui n'a pas cessé de me conseiller, encourager et soutenir tout au long de mes études. Que dieu le protège et lui offre la chance et le bonheur.

A mon adorable petit frère ALI qui sait toujours comment procurer la joie et le bonheur pour toute la famille.

A toute ma famille, mes amis/es et ma chère binôme HAMMAM SABIHA

Puisse dieu vous donne santé, bonheur, courage et surtout réussite.

Et à tous ceux qui ont contribué de prés ou de loin pour que ce projet soit possible, je vous dis merci.

SAFIA

Dédicace

A ma chère mère,

A mon cher père,

Qui n'ont jamais cessé, de formuler des prières à mon égard, de me soutenir

Et de m'épauler pour que je puisse atteindre mes objectifs.

A ma chère sœur Naima et sa petite fille Noor

A mes frères, Boualem et Zinou,

Pour leurs soutiens moral et leurs conseils précieux tout au long de mes études.

A ma chère binôme et amie Imadali Safia

A toute ma famille, mes amis /es et camarades.

SABIHA

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations

A

Ad hoc	Réseaux sans fil.

B

BS	Base Station.

D

D2D	Device-to-Device.
D2I	Device to Interface.
DARPA	The Defense Advanced Research Projects Agency.
DN	Destination Node.

E

eNB	Evolved NodeB.

G

GECDH	The Group Elliptic Curve Diffie-Hellman.

I

IEEE	Institute of Electrical and Electronics Engineers.
IETF	Internet Engineering Task Force.
IoT	Internet of Things.
IoV	Internet of Vehicles.
ISM	Industrielle, Scientifique et Médicale.

L

LAN	Local Area Network.
LTE	Long Term Evolution.

M

MANET	Mobile Ad hoc NETwork.

P

PAN	Personnal Area Network.

S

SN	Source Node.

T

TGECDH	Tree based Group Elliptic Curve Diffie Hellman.
TRP	Two Round Key Agreement Protocol

U

UE	User Equipment.

V

V2V	Vehicle to Vehicle.

W

Wi-Fi	Wireless Fidelity.
WLAN	Wireless Local Area Network.

Introduction générale

Introduction générale

Les appareils sans fil 5G devraient être la principale cause de l'augmentation rapide du trafic Internet, et plusieurs solutions ont été proposées dans ce sens. L'une de ces solutions consiste à développer des appareils mobiles capables de transmettre le trafic local directement au lieu de transmettre des données à travers une station de base.

Le domaine lié au périphérique à périphérique (D2D) devient le moyen le plus pratique pour fournir un déploiement rapide et une connexion sans fil autogérée afin de répondre aux besoin des fonctionnalités et caractéristiques offrent une possibilité plus large de recherches approfondies dans la construction de la future communauté de réseaux sans fil 5G. La communication D2D permet de fournir plus de fonctionnalités pour améliorer l'expérience utilisateur et de faciliter l'interactivité. La technologie D2D permet à chaque appareil d'établir des liaisons de communication directes à la place de la transmission de données via une station de base. La couverture de D2D peut être étendue en laissant plusieurs équipements former un réseau D2D ad hoc. Ensuite, n'importe quelle paire de 5G appartenant à un réseau, peuvent communiquer entre eux soit par un lien direct, ou bien par la méthode multi hop tant que leurs appareils sans fil formant un réseau ad hoc D2D.

Les réseaux mobiles Ad-Hoc sont des réseaux radio sans infrastructure, aptes à se créer et à s'organiser dynamiquement. Une des principales caractéristiques de ces réseaux est que les nœuds sont mobiles, et qu'ils peuvent rejoindre ou quitter le réseau de façon dynamique. Les nœuds ne s'appuient pas sur un point d'accès ou une station de base pour communiquer entre eux. Un réseau Ad-Hoc est caractérisé par un événement tel qu'un changement constant de la topologie du réseau, ce qui conduit souvent à une défaillance fréquente de la liaison, à une qualité de transmission dégradée et à un débit réseau réduit. Pour surmonter ces problèmes, il est impératif de concevoir, développer et implémenter une nouvelle génération de protocoles de routage qui prennent en charge un routage robuste et efficace dans les réseaux Ad-Hoc. Par ailleurs, des mesures de sécurité sont mises en place, tel que les mécanismes de la sécurité traditionnels, dont la signature digitale et la cryptographie qui ont resté toujours des outils essentiels pour garantir les besoins de sécurité dans les réseaux ad hoc, ces mécanismes nécessitent un service de gestion de clés afin de garantir l'authenticité des parties et l'intégrité des données transmises, et d'établir une confiance entre les nœuds du réseau.

Dans ce projet de fin d'étude, nous proposons d'étudier les réseaux Ad-Hoc avec communication D2D dans la technologie de cinquième génération. Le mémoire est structuré en 3 chapitres plus cette introduction et une conclusion générale.

Le premier chapitre sera consacré à la présentation de la nouvelle technologie 5G et à la communication D2D. Dans le second chapitre, nous intéressons aux réseaux Ad-Hoc (MANETs) à savoir leurs caractéristiques et leurs domaines d'application, ainsi que les différents types de protocoles de routage existants pour ces réseaux. Nous décrivons l'aspect sécuritaire des MANETs, les vulnérabilités aux attaques et les solutions existantes. Dans le troisième chapitre nous présentons notre modèle de subdivision en cellules et les résultats de simulations sous python du coût énergétique de communication lors de la génération de clés selon une subdivision hexagonale afin d'avoir une longue durée de vie du réseau.

Nous achevons ce manuscrit par une conclusion générale et les perspectives qui résument nos objectifs estimés tout en évoquant les problèmes que nous avons rencontrés et les améliorations envisageables.

Chapitre 1

CHAPITRE 1 : Notions sur la 5G et la communication D2D

1.1. Introduction

Pour satisfaire les besoins des utilisateurs, de nouvelles technologies émergent pour créer la prochaine génération du réseau 5G. Dans ce chapitre, nous allons donner une vue globale d'un réseau de cinquième génération et de la communication D2D. Nous présenterons d'abord la 5G où nous donnerons ses avantages, ses inconvénients et ses opportunités, puis nous étudierons le principe général de la communication D2D, ainsi que son application dans la 5G et ses atouts.

1.2. Cinquième génération de téléphonie mobile 5G

Avec l'adoption généralisée de l'Internet des objets dans les applications d'entreprise, telles que la fabrication, l'agriculture, la santé,…etc. Parallèlement à la dépendance croissante à l'égard des Smartphones et des ordinateurs toujours connectés, les contraintes de la technologie 4G LTE incitent les opérateurs de réseaux mobiles à se lancer sur un déploiement accéléré des communications 5G pour suivre le rythme des besoins actuels et futurs du réseau.

Les systèmes de communication cellulaire sont passés de l'analogique 1G, représenté par les services vocaux, au haut débit sans fil 4G, représenté par les données mobiles, l'informatique et le multimédia. Avec la prévalence des terminaux intelligents et la croissance explosive du trafic réseau, il existe un besoin plus clair et plus urgent d'évolution vers la technologie mobile 5G.

Dans l'évolution vers la 5G, les indicateurs de performance traditionnels, tels que la capacité du réseau et l'efficacité spectrale, doivent être continuellement améliorés, et une plus grande variété de modes de communication et d'applications doit être fournie pour améliorer l'expérience utilisateur. La technologie Ad-Hoc D2D a attiré une large attention dans l'industrie pour son potentiel à améliorer les performances du système, améliorer l'expérience utilisateur et étendre les applications cellulaires.

1.2.1. Qu'est-ce que la 5G exactement ?

Il s'agit de la prochaine génération de connectivité d'Internet mobile de cinquième génération qui promet des vitesses de téléchargement et d'envoi de données beaucoup plus rapides, une couverture plus large et des connexions plus stables. Il s'agit de mieux utiliser le spectre radioélectrique et de permettre à un plus grand nombre d'appareils d'accéder à l'internet mobile en même temps [1]. La 5G devrait jouer un rôle important dans le développement d'applications pour les villes intelligentes. Elle est très prometteuse, donnant potentiellement aux individus la possibilité de communiquer avec qui ils veulent quand ils le souhaitent dans le contexte d'un «système centré sur l'humain» [2].

1.2.2. Les exigences et les avantages de la 5G

La figure 1.1 illustre les exigences spécifiques de la technologie 5G et ses principaux avantages [3] qu'on va détailler juste ci-dessous :

Figure 1 1 : Les exigences du réseau 5G

- **Nombre énorme d'appareils connectés:** le réseau d'accès radio 5G doit pouvoir fournir la connectivité à un nombre considérable d'appareils pour la réalisation complète de l'IoT. Environ 300 000 appareils connectés par AP (point d'Accès) devraient être réalisables.
- **Débit de données de 1 à 10 Gb/s dans les réseaux réels:** la 5G devra fournir plus de 10 fois le débit de données actuellement fourni par les réseaux LTE.

- **Latence de bout en bout d'au plus 1 ms:** cela sera nécessaire pour prendre en charge les applications émergentes sensibles à la latence telle que les jeux en temps réel bidirectionnel, les hologrammes 3D, les applications basées sur le Cloud, la réalité augmentée, l'Internet tactile et les communications avec des machines.
- **Disponibilité et fiabilité perçues de près de 99,999%:** Cela signifie que le réseau 5G devrait être pratiquement disponible pour toute utilisation.
- **Couverture du réseau de presque 100%:** le réseau 5G devrait pouvoir fournir une connectivité réseau aux utilisateurs à tout moment, indépendamment de leur emplacement.
- **Réduction de la consommation d'énergie de près de 90%:** l'efficacité énergétique avec les technologies vertes sera cruciale pour le réseau 5G en raison de la très grande capacité et de la connectivité massive.
- **Durée de vie prolongée de la batterie pouvant aller jusqu'à dix ans**: cela sera essentiel pour le déploiement massif de dispositifs, capteurs et actionneurs de type machine à faible puissance.
- **Bande passante supérieure par unité de surface:** cela est nécessaire pour fournir un grand nombre de périphériques avec des largeurs de bande élevées aussi longtemps que possible dans certaines zones.

1.2.3. Inconvénients de cette future technologie

Bien que la technologie 5G soit étudiée et conceptualisée pour résoudre tous les problèmes de signaux radio et les difficultés du monde mobile, mais pour des raisons de sécurité et de manque de progrès technologiques dans la plupart des régions géographiques, elle présente les lacunes suivantes [4] :

- La technologie est toujours en cours et la recherche sur sa viabilité est en cours.
- La vitesse revendiquée par cette technologie semble difficile à atteindre (à l'avenir, cela pourrait être le cas) à cause du soutien technologique incompétent dans la plupart des régions du monde.
- La plupart des anciens appareils ne seraient pas compétents pour la 5G, il est donc nécessaire de les remplacer tous par un nouvel appareil coûteux.
- Le développement d'infrastructures nécessite des coûts élevés.

- Problème de sécurité et de confidentialité à résoudre.

1.2.4. Opportunités offertes par la 5G

Le déploiement du réseau 5G arrive à grands pas! Cette nouvelle technologie amènera de grandes transformations dans plusieurs secteurs et domaines [5].

La figure 1.2 est un bon exemple de la future société connectée dans laquelle dépendra la plupart de nos activités sur le réseau 5G.

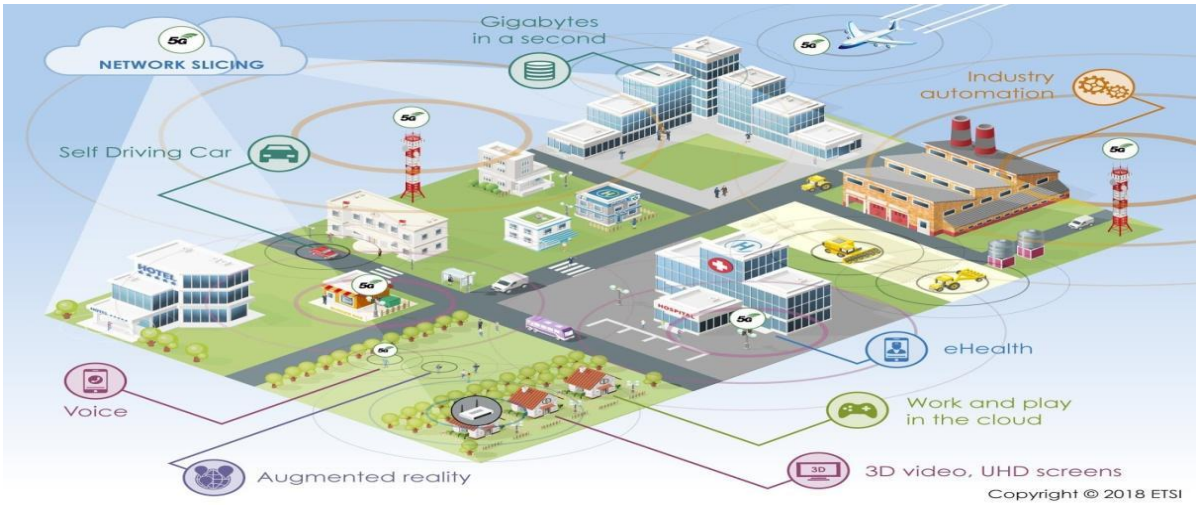

Figure 1 2 : Secteurs et domaines de l'utilisation de la 5G

- **Internet des objets (IoT) :** pour l'internet des objets, c'est un grand pas vers l'avant. La 5G va servir à connecter les objets à Internet, soit des dizaines de milliards d'appareils, machines et engins en tous genres. Les appareils seront contrôlables à distance de façon fiable, sécurisée et économe en énergie.
- **Jeux en ligne:** Grâce à la bande passante plus rapide, les réseaux 5G créeront de nouvelles possibilités dans le secteur des jeux vidéo, et offriront une meilleure expérience à l'utilisateur.
- **Le Cloud:** la 5G fournira à l'utilisateur une expérience améliorée lors de l'utilisation des services de stockage dans le Cloud et des plates-formes de streaming.
- **Voitures autonomes:** le réseau 5G devrait permettre aux véhicules de communiquer entre eux et donc de réagir de manière quasi instantanée en cas d'accident ou d'une perturbation quelconque du trafic routier.

- **Télémédecine:** la 5G pourrait développer des applications futures dans le domaine de la santé. Elle pourrait permettre, par exemple, une chirurgie à distance où le chirurgien et le patient se trouveraient à deux endroits différents.

Cependant, la partie accès dans tous les réseaux cellulaires souffre d'une multitude de problèmes qui peuvent avoir une incidence sur les services offerts aux utilisateurs finaux. En effet, les points morts constituent un inconvénient majeur dans de tels réseaux. Dans ce type de zones, le signal reçu est très faible en raison des obstacles entravant la propagation des ondes radio. Pour faire face à ce genre de problèmes, les opérateurs de télécommunications doivent déployer plus d'infrastructures et assurer suffisamment de ressources réseau afin de garantir une bonne qualité de service au client final. En effet, les microcellules et les pico-cellules peuvent être déployées dans des zones souffrant de manque de couverture. Cependant, le coût lié à cette opération est élevé car il comprend le coût de planification, les coûts en énergie, de maintenance et des licences de fréquences,…etc. La communication Ad-Hoc D2D est identifiée pour constituer une alternative intéressante pour surmonter les principaux inconvénients de la partie accès des réseaux cellulaires avec moindre coût [6].

1.3. La communication D2D dans les réseaux 5G

Le nombre d'appareils devrait augmenter radicalement dans le futur, avec une estimation de plus de 50 milliards d'appareils connectés dans les années à venir. Les abonnés exigent des débits de données améliorés, avec une latence réduite et une grande capacité du système. La communication D2D devrait répondre aux objectifs des prochaines générations, elle fait référence à la transmission directe entre appareils, sans relayer d'informations via la station de base (BS). Une telle transmission directe améliore l'efficacité spectrale et réduit la latence.

1.3.1. Evolution de la D2D à travers les générations

La communication sans fil a évolué depuis la première génération (1G) à la quatrième génération (4G), et pour répondre aux exigences des abonnés, le réseau de cinquième génération (5G) sera bientôt disponible.

La communication cellulaire a commencé avec l'introduction de la première génération (1 G). En 1G, uniquement la technologie analogique a été utilisée. Le numérique a vu le jour dans

la deuxième génération (2G). Jusqu'à ce moment, aucune communication directe entre les utilisateurs n'a été introduite. Cela était dû à un faible nombre d'abonnés et leurs demandes se limitent uniquement aux réseaux voix et données (WPAN) et au réseau local sans fil (WLAN) dans les réseaux de troisième génération (3G). Ces technologies autorisaient le partage de contenu dans une bande, à faible coût et faible consommation d'énergie. Cependant, les niveaux d'interférence étaient incontrôlables. Aucune garantie de qualité de service (QoS) n'a pu être fournie. De plus, cela impliquait une consommation excessive d'énergie. En raison de la croissance massive du trafic et de l'évolution des demandes de l'utilisateur, la communication directe dans le groupe a commencé a gagné une popularité pour les réseaux 4G (Long Term Evolution Advanced, LTE-A) [7].

Le besoin d'une prochaine génération de réseau se fait sentir suite à l'augmentation du trafic de données. C'est là qu'intervient la communication D2D qui améliore la couverture, l'efficacité des coûts, la fiabilité, la densité de capacité et l'efficacité du spectre.

1.3.2. Principe général de la communication D2D

La figure 1.3 illustre le principe général de la communication D2D

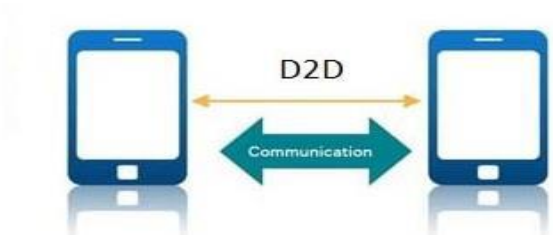

Figure 1 3: Communication D2D

Lors d'une communication cellulaire standard, toutes les parties doivent passer par les infrastructures du réseau pour échanger de l'information. Ce procédé s'appelle une communication D2I (Device to Infrastructure). En revanche, une communication D2D est une communication qui a lieu entre deux terminaux de façon directe où échangent des informations directement sans passer par un intermédiaire (comme cela pourrait se faire en Bluetooth, par exemple) [8].

1.3.3. Fonctionnement du D2D

La communication entre périphériques peut être réalisée selon plusieurs modes de fonctionnement, en fonction des scénarios. Selon la situation, le mode de fonctionnement le plus approprié sera choisi pour établir une transmission efficace [9]. La figure 1.4 suivante montre ces différents cas possibles pour la communication D2D :

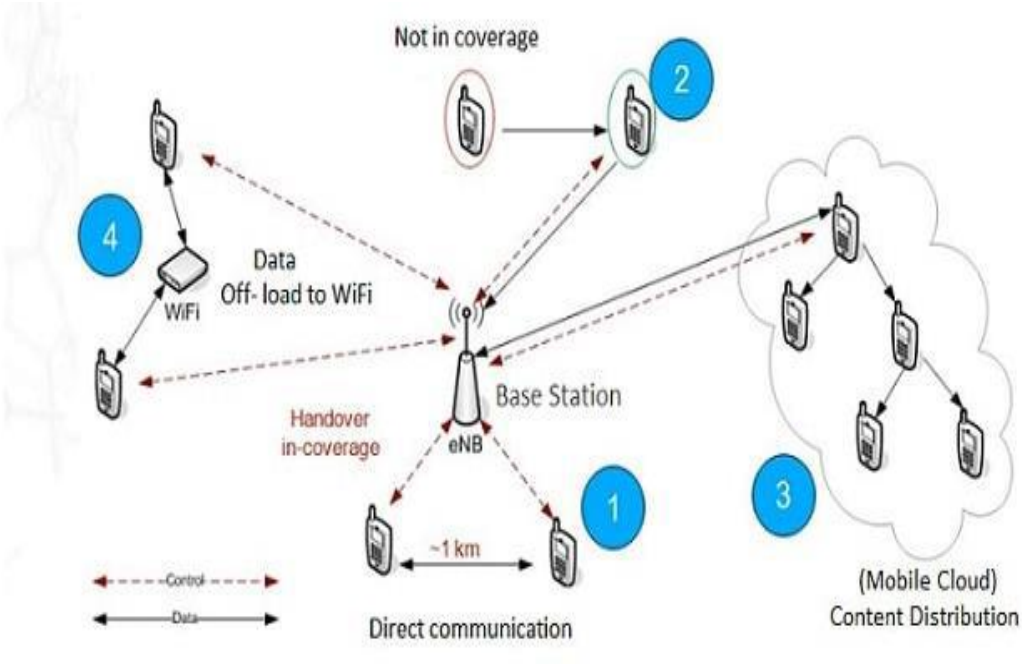

Figure 1 4: Scénarios de communication D2D

Scénario 1: Si deux périphériques se trouvent à proximité, ils peuvent commencer la communication, par exemple en partageant des données. Cela contribue à améliorer le débit de données, à réduire la consommation d'énergie des périphériques et à réduire la charge totale des stations de base. Le contrôle sera géré par la station de base.

Scénario 2: En l'absence de connexion réseau mobile active ou de réception de signaux insuffisante, les périphériques compatibles D2D peuvent établir une interface de communication alternative avec les périphériques environnants qui sont des stations de base mobiles connectés. Cela aidera le nœud sans couverture à maintenir une connexion au réseau mobile.

Scénario 3: Plusieurs périphériques peuvent se connecter à un périphérique disposant d'une connexion active à la station de base, puis étendre ce réseau en ajoutant une connexion à

plusieurs périphériques. Tous les appareils de ce petit Cloud mobile recevront les mêmes données sous forme de publicité ou de messages de la source.

Scénario 4: dans ce cas, plusieurs périphériques sont déchargés vers une connexion de données Wi-Fi pour la communication. Les signaux de commande destinés aux appareils seront traités par la station de base. Le déchargement Wi-Fi offre un débit de données beaucoup plus élevé, une moindre consommation d'énergie et évite les surcharges de trafic des stations de base.

Autres scénarios: La communication entre périphériques peut être efficacement mise en œuvre pour une communication entre machines, chaque machine pouvant communiquer avec d'autres machines à proximité. La communication entre dispositif (D2D) est utilisée de la même manière dans les communications entre véhicules (V2V) et dans les applications de communication entre homologues. Dans tous ces cas, un nœud se connecte à la station de base principale (station émettrice) et les autres périphériques forment un petit réseau pour communiquer entre eux.

1.3.4. Types de communication D2D

La communication D2D se divise fondamentalement en deux types, à savoir Inband et Outband [10] [11], comme le montre la figure 1.5.

Figure 1 5: Communication D2D In-Band et Out-Band

- **Communication en Bande (In-Band)**

En communication Inband, le D2D partage le spectre cellulaire sous licence avec d'autres utilisateurs cellulaires du réseau LTE-A. L'infrastructure réseau, c'est-à-dire que eNB (Evolved NodeB) contrôle totalement ou partiellement les utilisateurs de D2D. L'eNB est la responsable de la découverte des équipements D2D potentiels, de l'établissement de la liaison sur la base des informations sur l'état du canal, de l'affectation des ressources radio, en liaison montante ou descendante, du contrôle de l'alimentation en fonction de certain niveau seuil prédéfini, ainsi que la coordination des interférences entre les utilisateurs cellulaires et les utilisateurs de D2D.

- **Communication D2D hors Bande (Out-Band)**

La communication D2D hors bande exploite la bande de fréquence ISM (Industrielle, Scientifique et Médicale) sans licence pour ses opérations. Ceci est similaire à la bande de fonctionnements des technologies WLAN et Bluetooth. Le principal avantage de cette catégorie de D2D est qu'elle élimine le problème d'interférences entre les liaisons cellulaires et les liaisons D2D. En outre, l'allocation de ressources devient plus facile, car le planificateur n'a pas besoin de prendre en compte la fréquence, l'heure et l'emplacement des utilisateurs lors de l'attribution de blocs de ressources aux utilisateurs D2D et cellulaires. En outre, les utilisateurs peuvent simultanément gérer des connexions cellulaires et D2D à l'aide des deux interfaces radio. Cependant, l'inconvénient majeur est son interférence inter-système incontrôlable due à la présence d'autres entités communicantes, par exemple, les périphériques Wi-Fi et Bluetooth qui fonctionnent dans la même bande sans licence. Par conséquent, le partage de spectre sans licence ne pourrait pas fournir un environnement contrôlable stable, et entraînerait une congestion et une mauvaise expérience de la qualité de service, mais affecterait également le débit global du réseau. En outre, la sécurité de la transmission D2D et la coordination des communications sur deux bandes différentes avec des interfaces radio indépendantes posent un problème crucial de gestion de l'énergie.

1.3.5. Applications de la 5G D2D

Les applications de la 5G D2D incluent le service local, la communication d'urgence et l'amélioration de l'IoT [12] comme le montre la figure 1.6.

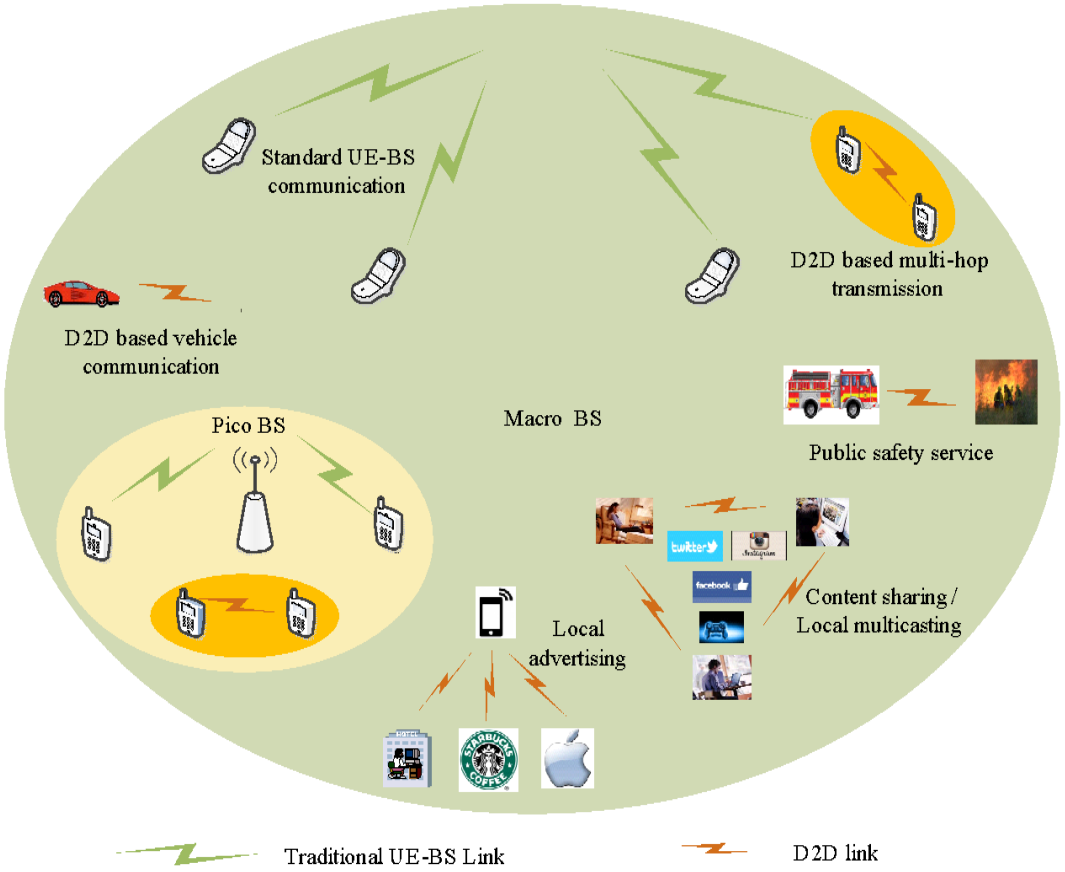

Figure 1 6: Les applications de la 5G D2D

- **service local**

En service local, les données utilisateur sont directement transmises entre les terminaux et ne transitent pas par le côté réseau. Le service local est généralement utilisé pour les applications sociales. Les applications sociales basées sur la fonctionnalité de proximité sont une application D2D de base. Grâce aux fonctions de découverte et de communication du D2D, un utilisateur peut trouver d'autres utilisateurs à proximité et partager des données ou jouer à des jeux avec eux.

Une autre application de base du service local est la transmission de données locale. Cette dernière exploite les fonctionnalités de proximité et de transmission directe de données du D2D

pour étendre les applications mobiles tout en économisant les ressources du spectre. Cela crée une nouvelle source de revenus pour les opérateurs. Par exemple, un service de publicité locale basé sur la proximité peut cibler avec précision les gens pour maximiser ses avantages. Un centre commercial peut envoyer des publicités, des remises et des promotions aux personnes qui entrent dans le centre commercial ou aux alentours, et un cinéma peut diffuser des informations sur les films et les séances aux personnes à proximité.

Une troisième application du service local est le déchargement du trafic cellulaire. À mesure que les services multimédias tels que les vidéos HD deviennent populaires, leurs flux de trafic massifs exercent une pression énorme sur les réseaux centraux et les ressources spectrales. Les services de médias locaux basés sur D2D peuvent aider les opérateurs à économiser leur cœur de réseau et leurs ressources spectrales. Dans les zones sensibles, les opérateurs ou les fournisseurs de contenu peuvent déployer des serveurs multimédias qui stockent des services multimédias populaires. Ces serveurs multimédias fournissent aux utilisateurs des services multimédias en mode D2D. Alternativement, les utilisateurs peuvent utiliser D2D pour obtenir le contenu multimédia des terminaux utilisateurs à proximité qui ont obtenu des services multimédias. De cette façon, la pression de transmission en liaison descendante des réseaux cellulaires d'opérateurs peut être atténuée. De plus, la communication cellulaire entre utilisateurs à courte distance peut être commutée en mode D2D pour décharger le trafic cellulaire.

- **Communication d'urgence**

Lorsque des catastrophes naturelles telles que des tremblements de terre se produisent, l'infrastructure de réseau de communication traditionnelle peut être endommagée et le réseau peut même s'effondrer. Cela entrave considérablement les efforts de sauvetage. Ce problème peut être résolu en introduisant la communication D2D. Bien que l'infrastructure du réseau de communication puisse être endommagée, un réseau sans fil peut toujours être configuré entre les terminaux en fonction de la connexion D2D. Cela signifie qu'un réseau ad hoc peut être établi sur la base du D2D à sauts multiples pour assurer une communication sans fil fluide entre les terminaux. Un réseau sans fil affecté par le terrain ou les bâtiments peut avoir des angles morts. Avec la communication D2D à un seul saut ou à plusieurs sauts, les utilisateurs dans les angles morts peuvent être connectés à des terminaux d'utilisateurs qui se trouvent dans des zones de couverture, puis être connectés au réseau sans fil.

- **Amélioration de l'IoT**

L'un des objectifs du développement de la communication mobile est d'établir un vaste réseau interconnecté contenant différents types de terminaux. C'est également l'un des points de départ pour le développement de l'Internet des objets (IoT) dans le cadre de la communication cellulaire.

Une application typique de l'amélioration de l'IoT basée sur D2D est la communication de véhicule à véhicule (V2V) dans l'Internet des véhicules (IoV). Lorsqu'il roule à grande vitesse, un véhicule peut avertir les véhicules à proximité en mode D2D avant de changer de voie ou de ralentir (Fig.1.7). Selon les avertissements reçus, les véhicules à proximité alertent les conducteurs ou même contrôlent automatiquement la conduite en situation d'urgence afin que les conducteurs puissent réagir plus rapidement pour réduire le nombre d'accidents de la circulation. De plus, grâce à la technologie de découverte D2D, les véhicules peuvent détecter et identifier de manière fiable des véhicules spécifiques à proximité, tels que les véhicules pouvant présenter un danger aux intersections et les véhicules spécifiques (autobus scolaires ou véhicules transportant des marchandises dangereuses) qui nécessitent une attention particulière[13].

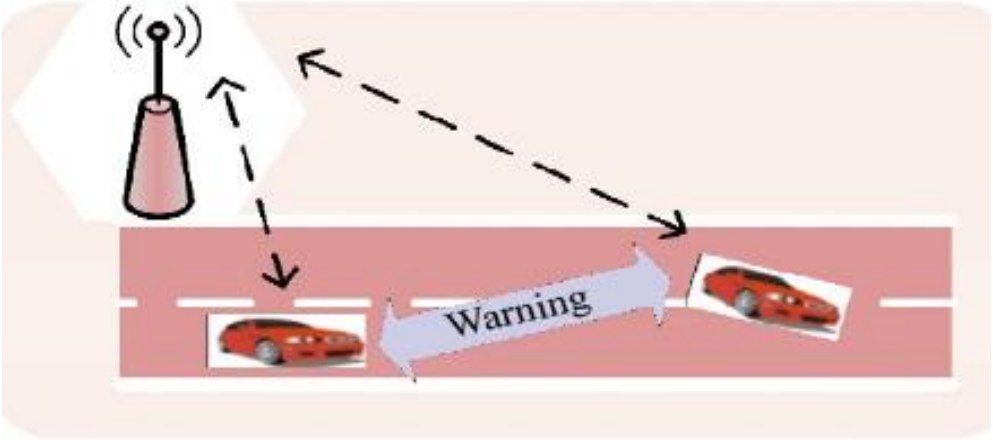

Figure 1 7: Application IoV basée sur D2D

1.3.6. Avantages de la communication D2D

La communication D2D permet d'augmenter l'efficacité spectrale, d'améliorer l'expérience utilisateur et d'étendre les applications de communication [12].

➢ **Augmentation de l'efficacité spectrale**

Dans les communications D2D, les données utilisateur sont directement transmises entre les terminaux sans routage via un réseau cellulaire et entraînent ainsi un gain de saut. De plus, les ressources entre les utilisateurs D2D et entre les réseaux D2D et les réseaux cellulaires peuvent être réutilisées, ce qui entraîne un gain de réutilisation des ressources. Avec le gain de saut et le gain de réutilisation des ressources, l'efficacité spectrale sans fil et le débit du réseau peuvent être augmentés.

➢ **Amélioration de l'expérience utilisateur**

À mesure que les services et technologies mobiles se développent, le partage de données à courte distance entre les utilisateurs à proximité, les activités sociales et commerciales à petite échelle et les services de localisation pour les utilisateurs locaux deviendront une source importante de croissance commerciale sur la plateforme sans fil. La technologie D2D basée sur la découverte d'utilisateurs à proximité améliorera l'expérience utilisateur dans ces modes de service.

➢ **Extension des applications de communication**

Les réseaux sans fil traditionnels exigent une infrastructure de communication. Le système de communication peut s'effondrer si les installations du réseau principal ou les périphériques d'accès au réseau sont endommagés. Cependant, la communication D2D permet aux terminaux de communication cellulaire de mettre en place des réseaux ad hoc. Si l'infrastructure sans fil est endommagée ou que les terminaux ne sont pas couverts par un réseau sans fil, le D2D à sauts multiples peut être utilisé pour la communication poste à poste ou même l'accès aux réseaux cellulaires. De cette façon, le nombre d'applications sans fil peut être étendu.

1.4. Conclusion

Ce premier chapitre a été consacré à la présentation du réseau 5G et la communication D2D. Nous avons commencé par décrire la 5ème génération, ses avantages et ses inconvénients ainsi que ses opportunités. Nous avons également vu l'évolution de la communication D2D à travers ces générations, et nous avons décrit son principe général et son fonctionnement. Par la suite, nous avons présenté les types de communications D2D qui sont classée en fonction du spectre Inband et Outband, puis nous avons expliqué les applications de la 5G D2D dont le service local, la communication d'urgence et l'amélioration de l'IoT. Enfin, nous avons cité ses avantages. Dans le chapitre qui suit nous présenterons les réseaux mobiles AD-HOC.

Chapitre 2

CHAPITRE 2 : Réseaux mobiles Ad-Hoc

2.1. Introduction

De nos jours, le domaine de télécommunication à pris un nouvel envol grâce à l'évolution technologique. De plus en plus, les environnements de communication utilisent les réseaux sans fil (réseaux ad hoc) plutôt qu'une infrastructure câblée pour communiquer.

Ce chapitre a pour but de définir les réseaux mobiles ad hoc, et de présenter ses principales caractéristiques et applications. Nous citerons également, ces avantages et ces inconvénients. Par la suite, nous allons classifier les protocoles les plus connus proposés pour effectuer le routage dans les réseaux ad hoc. Comme nous allons voir les concepts de base de leurs sécurités où nous définirons la cryptographie en générale. Puis, nous présenterons quelques protocoles de gestions de clés.

2.2. Réseaux Ad-Hoc

Un réseau mobile Ad-Hoc (ou MANET) est un réseau d'appareils mobiles sans fil. Les MANETs sont étudiés depuis de nombreuses années et ce sont des réseaux formés uniquement à partir d'équipements utilisateur mobiles (UE). Un nœud peut être un ordinateur portable, un téléphone mobile ou tout autre appareil mobile ayant la capacité de communiquer et qui coopèrent pour échanger des données dans un environnement sans infrastructure. Ce type de réseau peut être utilisé pour de nombreuses applications: les opérations tactiques de pointe, les zones désastreuses et dans les environnements encombrés comme les campus et les stades où de nombreux utilisateurs sont prêts à échanger des informations directement entre eux ou utiliser les appareils des autres en tant que routeurs.

2.2.1. Bref historique

Le début des années 1970 voit, au sein du projet militaire Américain DARPA (The Defense Advanced Research Projects Agency), la naissance des premiers réseaux utilisant le médium radio. Ces réseaux disposaient déjà d'une architecture distribuée, partageaient le canal de diffusion en répétant des paquets pour élargir la zone de couverture globale. Par la suite, en 1983, *les SUr vivable RAdio Networks* (SU RAN) furent développés par le DARPA. L'objectif était de

dépasser les limitations (en particulier permettre le passage à des réseaux comportant énormément des nœuds, gérant la sécurité, l'énergie). Mais les recherches sur ces réseaux restaient exclusivement militaires. Ce n'est qu'avec l'arrivée de la norme 802.11 de l'IEEE (Institute of Electrical and Electronics Engineers) qui permet de bâtir des réseaux sans fil autour de bases fixes, que la recherche civile s'empare à la fin des années 90 des problématiques liées à ces réseaux [14].

2.2.2. Définition des réseaux mobiles Ad-Hoc

Un réseau mobile Ad-Hoc, appelé généralement Mobile Ad hoc NETwork (MANET), est un ensemble de nœuds mobiles qui se déplacent dans un territoire quelconque d'une manière autonome et coopérative, sans l'utilisation d'une infrastructure préexistante ou d'une administration centralisée. Les "ondes radio" qui se propagent entre les différents nœuds mobiles sont le seul moyen de communication [15]. Dans un réseau Ad-Hoc, un nœud peut communiquer directement (mode point-à-point) avec n'importe quel nœud s'il est situé dans sa zone de transmission, tandis que la communication avec un nœud situé en dehors de sa zone de transmission s'effectue via plusieurs nœuds intermédiaires (mode multi-sauts) [16]. Les réseaux Ad-Hoc sont la réponse au défi que nous pose l'apparition de nombreux objets communicants dans notre environnement de tous les jours.

La figure 2.1 est une illustration adéquate du concept du réseau ad-hoc

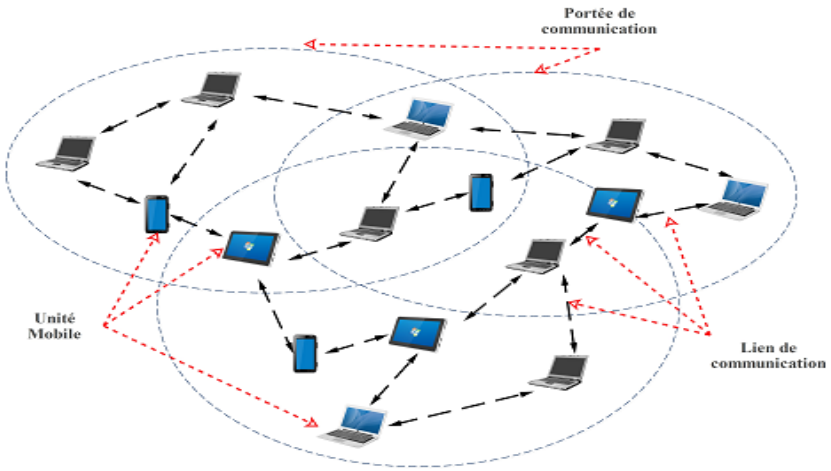

Figure 2 1: Réseau Ad-Hoc

2.2.3. Caractéristique des réseaux Ad Hoc

Les réseaux mobiles Ad-Hoc sont caractérisés par ce qui suit [17]:

- **Sans infrastructure:** les nœuds d'un réseau Ad-Hoc travaillent dans un environnement totalement distribué, ce qui leur permet de se déplacer librement. Cette caractéristique donne plus de liberté aux nœuds mais ces derniers doivent assurer des fonctionnalités supplémentaires par rapport aux nœuds d'un réseau sans fils avec infrastructure, puisqu'ils doivent agir en tant que routeurs pour relayer la communication d'autres nœuds.
- **Mobilité et topologie dynamique:** les unités mobiles du réseau se déplacent d'une façon libre et arbitraire. Par conséquent, la topologie du réseau peut changer, à des instants imprévisibles, d'une manière rapide et aléatoire. Les liens de la topologie peuvent être unis ou bidirectionnels.

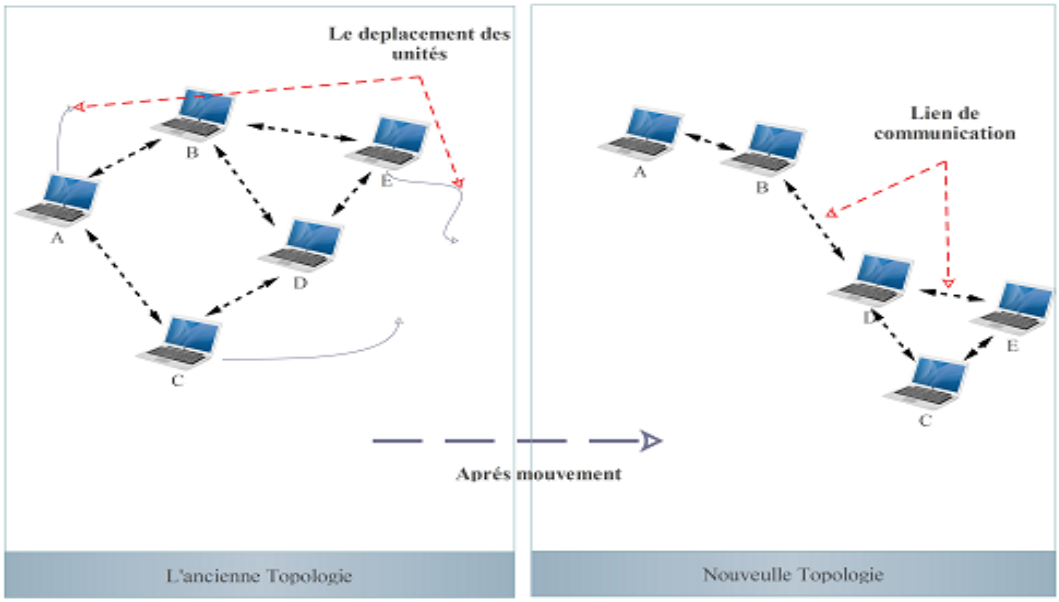

Figure 2 2: Changement de la topologie d'un réseau Ad-Hoc

- **Contraintes de ressources:** les nœuds disposent de ressources d'alimentation et de capacités de calcul et de stockage limitées. D'où une gestion efficace est nécessaire pour avoir une longue durée de vie, le trafic de routage devrait être maintenu à un minimum.
- **Bande passante limitée:** la communication dans les réseaux Ad-Hoc se base sur le partage d'un médium sans fil (onde radio). Ce qui induit une bande passante modeste, pour chaque hôte du réseau.

- **Interférences:** dans un réseau Ad-Hoc, les liens radio ne sont pas isolés. Ceci peut impliquer que deux transmissions simultanées sur une même fréquence ou sur des fréquences proches peuvent interférer et provoquer des erreurs de transmission. Un grand nombre de paquets peuvent être endommagés et perdus lors du transfert.
- **Sécurité physique limitée:** les terminaux ne sont pas protégés, ils sont menacés de vol ou de destruction. Donc les nœuds d'un réseau Ad-Hoc n'ont pas la même protection physique que les nœuds d'un réseau filaire. En effet, ceux d'un réseau Ad-Hoc sont censés être mobiles et parfois complètement autonomes, c'est notamment le cas des réseaux de capteurs où les nœuds sont souvent lâchés, dans un environnement particulier et parfois hostile, sans aucune surveillance particulière.
- **Sécurité et vulnérabilité:** les réseaux sans fil sont par nature plus sensibles aux problèmes de sécurité que les réseaux filaires. Pour les réseaux Ad-Hoc, le principal problème ne se situe pas tant au niveau du support physique mais principalement dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau.

2.2.4. Domaines d'applications

La particularité du réseau Ad-Hoc est qu'il n'a besoin d'aucune installation fixe, ceci lui permettant d'être rapide et facile à déployer. Les applications tactiques comme les opérations de secours, militaires ou d'explorations trouvent en Ad-Hoc, le réseau idéal. La technologie Ad-Hoc intéresse également la recherche, des applications civiles sont apparues.
On distingue [18]:

- **Services d'urgence:** opération de recherche et de secours des personnes, tremblement de terre, feux, dans le but de remplacer l'infrastructure filaire.
- **Travail collaboratif et communications dans des entreprises ou bâtiments**: dans le cadre d'une réunion ou d'une conférence par exemple.
- **Applications commerciales:** pour un paiement électronique distant (taxi) ou pour l'accès mobile à l'Internet, où service de guide en fonction de la position de l'utilisateur.
- **Réseaux de capteurs:** les capteurs, chargés de mesurer les propriétés physiques des environnements (comme la température, la pression...), sont dispersés (le plus souvent lâchés d'un avion ou d'un hélicoptère) par centaines, voire par milliers sur le site,

effectuent leurs mesures et envoient les résultats à une station par l'intermédiaire d'un routage ad hoc à travers le réseau.

- **Le cadre informatique:** dans le cadre de l'informatique, les réseaux ad hoc peuvent servir à établir des liens entre ses différents composants. Dans ce cas, on parle non plus de LAN (Local Area Network) mais de PAN (Personnal Area Network).

2.2.5. Avantages et inconvénients des réseaux Ad-Hoc

❖ **Avantages**

Le mode de fonctionnement des réseaux Ad-Hoc présente de nombreux avantages [19]:

- L'avantage principal d'un tel réseau est son déploiement rapide (en effet, il est possible d'utiliser un réseau dans des situations d'urgence, par exemple, pour organiser les secours lors d'une catastrophe naturelle), sa robustesse, sa flexibilité et le support de la mobilité.
- Possibilité de créer un réseau local mobile: en effet, un ensemble de personnes se déplaçant peuvent créer un réseau local mobile. On peut, par exemple, imaginer l'utilisation d'un réseau ad hoc pour relier entre eux au cours d'un trajet, les camions d'un convoi routier.
- Facilité d'installations temporaires: telles que les stands de foire, les expositions ou salles de conférences.
- Installation plus économique du réseau dans les endroits difficiles à câbler.
- adapté aux environnements dynamiques nécessitant des transformations fréquentes grâce au coût minimum du câblage.

❖ **Inconvénients**

Le mode de fonctionnement des réseaux Ad-Hoc présente de nombreux inconvénients[19] :

- bruits et interférences: Accroissent le nombre d'erreurs sur la transmission et amoindrissent d'autant les performances d'un lien radio.
- perte de paquets.

- débits plus faibles que filaires, les nœuds sont souvent peu puissants, problème de consommation d'énergie.
- faible en termes de sécurité.
- liens asymétriques : ces liens n'accueillent que des communications à sens unique entre un émetteur et un récepteur.
- mobilité des nœuds : modification de la topologie du réseau, et la transformation du tracé des routes lors des échanges des paquets.

2.2.6. Routage dans les réseaux Ad-Hoc

Tous les types de systèmes de communication exécutent le processus de communication en utilisant un mécanisme appelé routage. Le routage est un ensemble de règles ou d'algorithmes permettant de traiter et de déplacer des données d'un nœud à un autre dans le réseau. Cette règle détermine le «meilleur» chemin sur lequel les données sont transmises. Les réseaux MANETs ne peuvent pas être utiles sans l'utilisation d'un protocole de routage fiable pour le maintien d'une route appropriée qui lui permet d'entamer le processus de communication. Un protocole de routage dans MANET utilise un algorithme pour déterminer le transfert optimal des données réseau et les chemins de communication entre les nœuds du réseau. En même temps, un protocole de routage est responsable de la maintenance et, si nécessaire, de la réparation de tous les chemins. La mobilité des nœuds dans les réseaux ad hoc rend le routage plus complexe [20].

Le groupe de travail IETF (Internet Engineering Task Force) a défini trois types de protocoles de routage selon la procédure utilisée pour établir et maintenir les routes: la famille de protocoles réactifs (à la demande), la famille des protocoles proactifs (vu global du réseau), et la famille des protocoles hybride.

2.2.6.1. Classification des protocoles de routage

Les protocoles de routage peuvent être classés en différentes familles selon le moment auquel ils initient la découverte de route, ou la manière dont les nœuds d'un réseau se partagent le travail de routage et selon la manière dont les informations de routage sont échangées. Dans ce qui suit, nous expliquons le principe de chacune de ces classes et nous citons quelques protocoles les plus connus dans chaque famille, comme illustré dans la figure 2.3. [7].

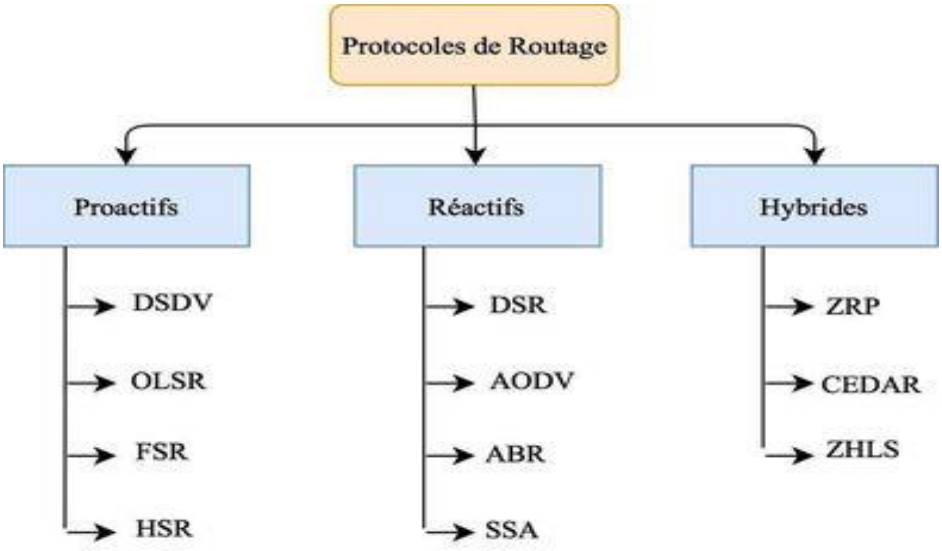

Figure 2 3: Types de protocoles de routage

a. Protocoles de routage proactifs

Les protocoles de routage proactifs diffusent des messages de contrôle périodiques pour la création, la maintenance et la mise à jour des routes, et ce en parallèle de la transmission des données. Même s'il n'y a pas de trafic, cette maintenance reste toujours active. Cette classe de protocole est basée sur les mêmes méthodes utilisées pour les protocoles de routage dans les réseaux filaires. Les deux principales méthodes sont: la méthode à État de Liens (Link State) et la méthode du Vecteur de Distances (Distance Vector). Ces deux méthodes reposent sur la technique de plus court chemin ce qui permet à une source de trouver le chemin le plus court vers une destination, exemples: DSDV, FSR, HSR, OLSR,…etc.

b. Protocoles de routage réactifs

Comme nous l'avons mentionné au cours du paragraphe précédent, les protocoles de routage proactifs essaient de maintenir les meilleurs chemins vers toutes les destinations du réseau par l'échange périodique de messages de contrôle de mise à jour. Les routes sont sauvegardées même si elles ne sont pas utilisées ce qui induit un contrôle excessif surtout dans le cas des réseaux denses. Les protocoles de routage réactifs créent et maintiennent les routes selon les besoins des émetteurs et de leurs applications. Dans ce cas, une procédure de découverte globale de routes est lancée qui permet d'avoir une information bien spécifique mais inconnue au préalable. Les protocoles basés sur ce principe, dits aussi à la demande, sont entre autres : DSR, AODV, ABR, SSR,…etc.

c. Protocoles de routage hybrides

Ces protocoles utilisent l'approche proactive pour déterminer le voisinage à deux sauts ou trois sauts. De cette manière, les routes dans le voisinage sont définies. Au-delà de cette zone prédéfinie, les protocoles hybrides utilisent l'approche réactive pour la recherche de route. De ce fait, le réseau est découpé en plusieurs zones. À la réception d'une requête de recherche de route réactive, le nœud peut signaler si la destination est dans son voisinage ou non pour renvoyer la requête vers les autres zones. Les protocoles de routage ZRP (Zone Routing Protocol), CEDAR, ZHLS présentent des exemples de cette catégorie. Les protocoles hybrides s'adaptent bien aux grands réseaux, cependant, ils comportent aussi les inconvénients des protocoles proactifs et réactifs tels que: les messages de contrôle périodiques, plus le coût de recherche d'une nouvelle route.

2.2.6.2. Problème du routage dans les réseaux Ad-Hoc

La topologie du réseau continue de changer au fil du temps, car les nœuds peuvent se déplacer, de nouveaux nœuds peuvent rejoindre le réseau et d'autres se désengagent du réseau. Le réseau est créé, géré et organisé uniquement par les nœuds eux-mêmes sans l'aide d'aucun tiers centralisé ou infrastructure fixe. Par conséquent, la coopération des nœuds entre eux est la plate-forme sur laquelle ce réseau est construit. Un nœud utilise non seulement le réseau pour communiquer avec d'autres nœuds, mais prend également en charge le réseau en effectuant des fonctions de routage. Un nœud qui souhaite communiquer avec un autre nœud qui ne se trouve

pas dans sa zone de communication prend l'aide des nœuds intermédiaires pour relayer son message [21].

Le problème qui se pose dans le contexte des réseaux ad hoc est l'adaptation de la méthode d'acheminement utilisée avec le grand nombre d'unités existant dans un environnement caractérisé par de modestes capacités de calcul et de sauvegarde et de changements rapides de topologies [22].

MANET est bien connu en raison du fait que ces réseaux sont puissants, sans infrastructure et évolutifs et aussi une technologie avec une grande variété de domaines d'application. Malgré sa réputation, les hyperliens Wi-Fi rendent également le MANET plus vulnérable aux attaques, ce qui simplifie l'accès de l'ennemi au réseau. La sécurisation de MANET reste aussi un problème difficile, en raison de la nature du réseau sans fil. Par conséquent, de nombreux protocoles de routage sécurisés ont été proposés [21].

2.3. Concepts de sécurité

2.3.1. Risques liés à la sécurité

Afin d'appréhender la problématique de la sécurité dans les réseaux sans fil les concepteurs, les administrateurs et les utilisateurs de ce dernier doivent effectuer une analyse de risques afin de déterminer les parties critiques, en terme de sécurité. Cette analyse suit les étapes suivantes [14] présenté dans la figure 2.4.

- détermination des fonctions et données sensibles des réseaux sans fil Ad-Hoc.
- recherche des exigences de sécurité par le biais des critères de sécurité que sont l'authentification, l'intégrité, la confidentialité, l'anonymat et la disponibilité.
- études des vulnérabilités.
- études des menaces et quantification de leur probabilité d'occurrence ou de leur faisabilité.
- mesure du risque encouru en fonction des vulnérabilités mises en lumière et des menaces associées.

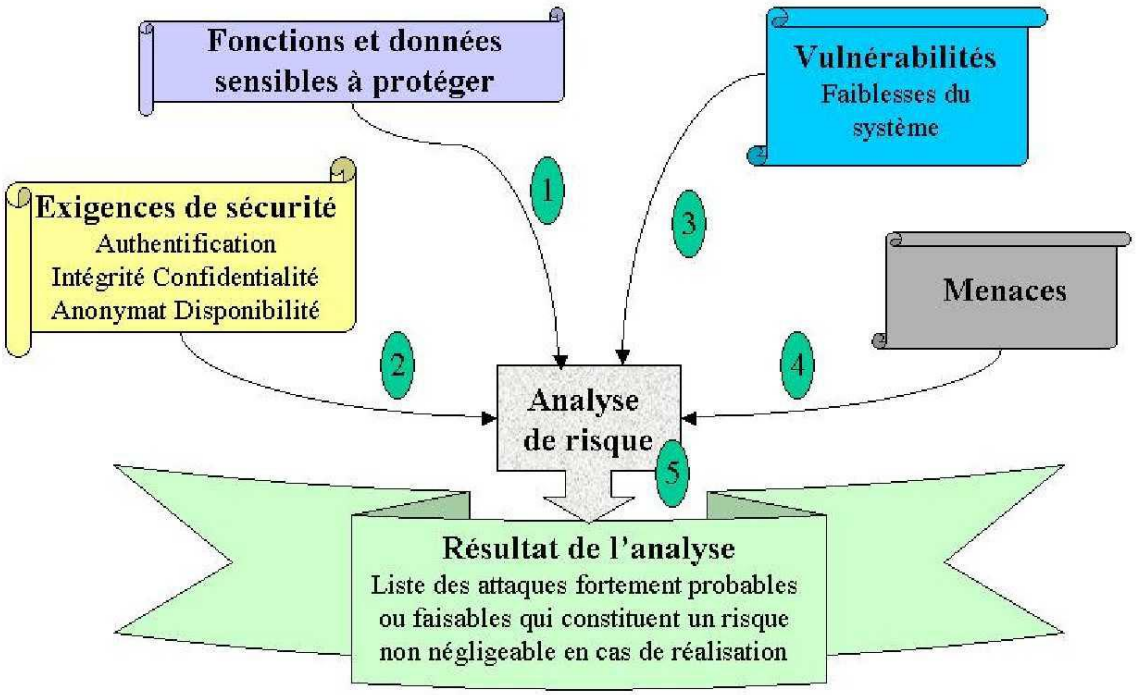

Figure 2 4 : Etapes d'analyse de risque

1. Fonctions et données sensibles

Les fonctions sensibles des nœuds d'un réseau sans fil Ad-Hoc sont le routage, la configuration, la gestion d'énergie, et les mécanismes de sécurité. La plupart des données sensibles sont directement liées à ces fonctions puisqu'il s'agit :

- des données relatives au routage (tables de routage et données de configuration des mécanismes de routage).
- des mesures et données de configuration pour la gestion de l'énergie.
- des données relatives à la sécurité (clés cryptographiques, mots de passe, certificats, etc.).
- d'une manière générale tout ce qui concerne les données de configuration. Les informations personnelles des utilisateurs doivent aussi être considérées comme des données sensibles.

2. Exigences de sécurité des réseaux sans fil Ad-Hoc

Déterminer les exigences de sécurité d'un système nécessite d'appréhender l'ensemble des contraintes qui pèsent sur ce système. Cette étape permet par la suite de quantifier les critères de sécurité. Les spécificités des réseaux sans fil Ad-Hoc sont multiples et traitant de manière générale: les caractéristiques des nœuds, la gestion de l'énergie, les caractéristiques du réseau, les technologies sans fil sous-jacentes, la mobilité et la configuration.

L'objectif de la sécurité est d'assurer les cinq principes clés suivants [23] :

- **authentification:** s'assurer de l'identité des entités en cours de communication. Avec l'authentification, le destinataire sera sûr que le message provient de la source prétendue.
- **confidentialité:** assurer que l'information ne peut pas être interprétée par des tiers non autorisés. Les informations de routage doivent aussi, dans certains cas, rester secrètes.
- **intégrité:** assurer que la modification des données transmises sera détectée. On utilise souvent les fonctions de hachage pour assurer l'intégrité.
- **disponibilité:** assurer la présence des services du réseau même en présence d'attaques de déni de service. Ces attaques peuvent se présenter au niveau de différentes couches d'un réseau ad hoc. La disponibilité donne aussi une assurance sur la réactivité et le temps de réponse du réseau.
- **non-répudiation:** empêcher un nœud de nier l'envoi ou bien la réception d'un message.
- **contrôle d'accès:** service de sécurité permettant de déterminer, après avoir authentifié un utilisateur, quels sont ses privilèges et de les appliquer. Ce service a pour but d'empêcher l'utilisation d'une ressource (réseau, machine, données, etc.) sans autorisation appropriée.

3. Vulnérabilités

La première vulnérabilité de ces réseaux est liée à la technologie sans fil sous-jacente. Quiconque possédant le récepteur adéquat peut potentiellement écouter ou perturber les messages échangés. Et ceci, même s'il se trouve dans un lieu public, à l'extérieur du bâtiment où se déroulent les échanges:

- les nœuds eux-mêmes sont des points de vulnérabilités du réseau car un attaquant peut compromettre un élément laissé sans surveillance.

- l'absence d'infrastructure fixe pénalise l'ensemble du réseau dans la mesure où il faut faire abstraction de toute entité centrale de gestion pour l'accès aux ressources.
- les mécanismes de routage sont d'autant plus critiques dans les réseaux Ad-Hoc que chaque entité participe à l'acheminement des paquets à travers le réseau. De plus, les messages de routage transitent sur les ondes radio.

4. Menaces

On distingue les menaces de type passif, où l'attaquant est limité à l'écoute et l'analyse du trafic échangé, et les menaces de type actif. Dans ce dernier mode, l'attaquant se donnera les moyens d'agir sur la gestion, la configuration et l'exploitation du réseau. Il peut injecter son propre trafic, modifier le fonctionnement d'un nœud, usurper l'identité d'un élément valide, rejouer des messages, modifier des messages transitant sur le réseau ou provoquer un déni de service. L'attaque passive prive le réseau de la confidentialité des messages échangés. Éventuellement, l'analyse du trafic représente un risque pour l'anonymat des participants et le respect de leur vie privée.

5. Résultat de l'Analyse de Risque

Après l'étude des besoins et exigences des réseaux sans fil Ad-Hoc en termes de sécurité, puis corrélation avec les risques issus des vulnérabilités et menaces s'appliquant à ces réseaux, nous avons pu trouver qu'il existe cinq formes d'attaque que nous détaillerons comme suit [24] :

- **attaque passive** : tout acte qui nous permet de faire, la surveillance, l'analyse et le décryptage des communications ainsi que la capture des informations d'authentification du trafic réseau, représente une attaque passive. Cette dernière peut entraîner la divulgation des informations ou des données à un attaquant sans que la victime soit consciente. À titre d'exemple l'interception du mot de passe, numéros de carte de crédit, des emails représente tous des attaques passives.
- **attaque active**: toute tentative ayant pour but de contourner ou arrêter les fonctions de protection, introduire un code malveillant et de voler ou modifier des informations représente une attaque active.
- **attaque externe**: représente l'utilisation de la proximité physique du réseau ou du système qui a été obtenu grâce à l'entrée clandestine ou un accès ouvert afin de modifier, collecter ou refuser l'accès à l'information.

- **attaque interne:** sont de deux genres :
  - ❖ intentionnelles: représentent les tentatives d'espionnage, de voler ou d'endommager des informations, utiliser l'information de manière frauduleuse, ou interdire l'accès à d'autres utilisateurs autorisés.
  - ❖ non intentionnelles: représentent le résultat d'une mauvaise manipulation, la négligence ou le manque de connaissances.
- **attaque de distribution**: toute modification malveillante du matériel ou du logiciel en usine ou lors de la distribution représente une attaque de distribution, qui consiste à introduire un code malveillant dans un produit comme un port dérobé pour obtenir un accès non autorisé à des informations ou une fonction système.

2.3.2. Outils cryptographiques

Les exigences de sécurité des réseaux sans fil Ad-Hoc décrits précédemment, peuvent être assurées en utilisant différentes techniques cryptographiques :

2.3.2.1. Le cryptage symétrique (ou à clé secrète)

On parle de cryptage symétrique, lorsqu'on utilise une même clé pour crypter et décrypter les messages (figure 2.5). Le principal inconvénient de ce système est la difficulté de la distribution de la clé de manière sécurisée. Car il suffit qu'une personne puisse intercepter cette clé durant son envoi au destinataire pour qu'elle puisse décrypter tous les messages cryptés avec cette clé [25].

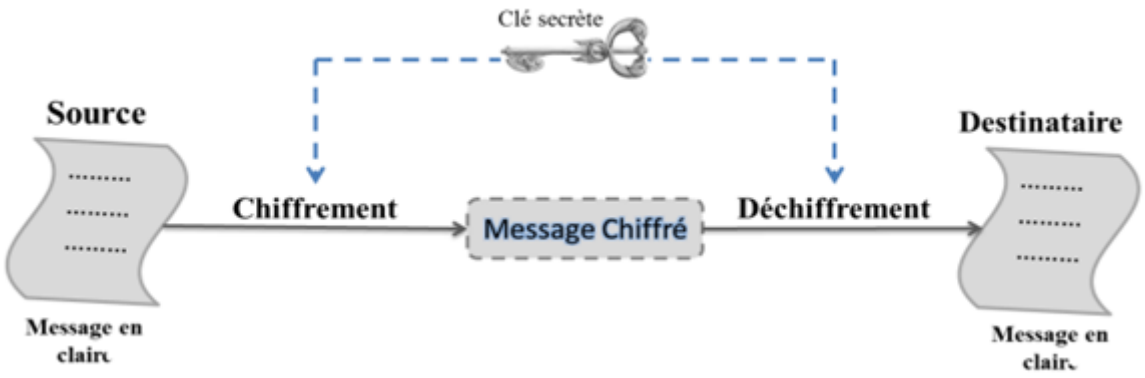

Figure 2 5: Chiffrement symétrique

2.3.2.2. Le cryptage asymétrique (ou à clé publique)

La cryptographie asymétrique appelée aussi la cryptographie à clé publique, est un procédé utilisant une paire de clé (clé privée et clé publique), la clé publique c'est pour chiffrer les messages à envoyer, et clé secrète (privée) pour déchiffrer les messages reçus (figure 2.6). La clé privée reste secrète et la clé publique peut être connue par les autres interlocuteurs. La cryptographie asymétrique n'est pas seulement utilisée pour assurer la confidentialité, mais aussi pour assurer d'autres propriétés comme l'authentification qui est basée sur l'utilisation d'un mécanisme cryptographique appelé la signature numérique qui prouve l'origine des données [26].

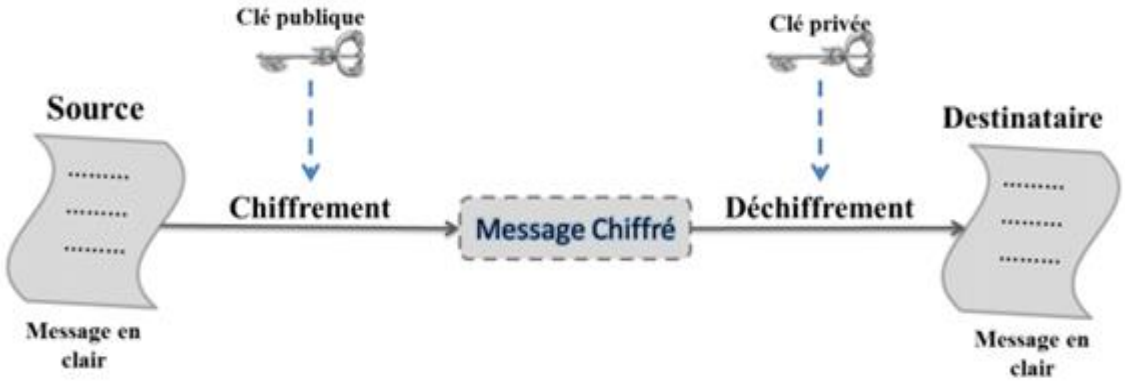

Figure 2 6: Chiffrement asymétrique

2.3.3. Fonctions de hachage

Une fonction de hachage est une fonction permettant d'obtenir un condensat à partir d'un message, c'est-à-dire une suite de caractères assez courte représentant le message à envoyer. La fonction de hachage associe un et un seul condensat à un message en clair (cela signifie que la moindre modification du message entraîne la modification de son condensat) [27].

En expédiant un message accompagné de son condensat, il est possible de garantir l'intégrité de ce message, c'est-à-dire que le destinataire peut vérifier que le message n'a pas été altéré (intentionnellement ou accidentellement) durant la communication.

2.3.4. La signature numérique

La façon la plus simple pour signer un message consiste à chiffrer celui-ci à l'aide d'une clé privée: seul le possesseur de cette clé est capable de générer la signature, mais toute personne ayant accès à la clé publique correspondante peut la vérifier. Dans la pratique, cette méthode est peu utilisée du fait de sa lenteur [28].

Pour cette raison, une autre méthode est utilisée pour signer, consiste à calculer un condensat du message à signer et à ne chiffrer que ce condensat. Le résultat obtenu s'appelle la signature numérique (figure 2.7). Le destinataire reçoit le message et la signature. Il décrypte d'abord la signature à l'aide d'une clé publique fournie par l'expéditeur au préalable. Il obtient ainsi un condensat. A partir du message, il exécute le même algorithme de hachage que l'expéditeur pour obtenir un condensat. Si les deux condensats ainsi obtenus sont identiques, l'expéditeur aura la certitude que le message est authentique (sous la condition que la clé publique utilisée soit bien celle envoyée par l'expéditeur).

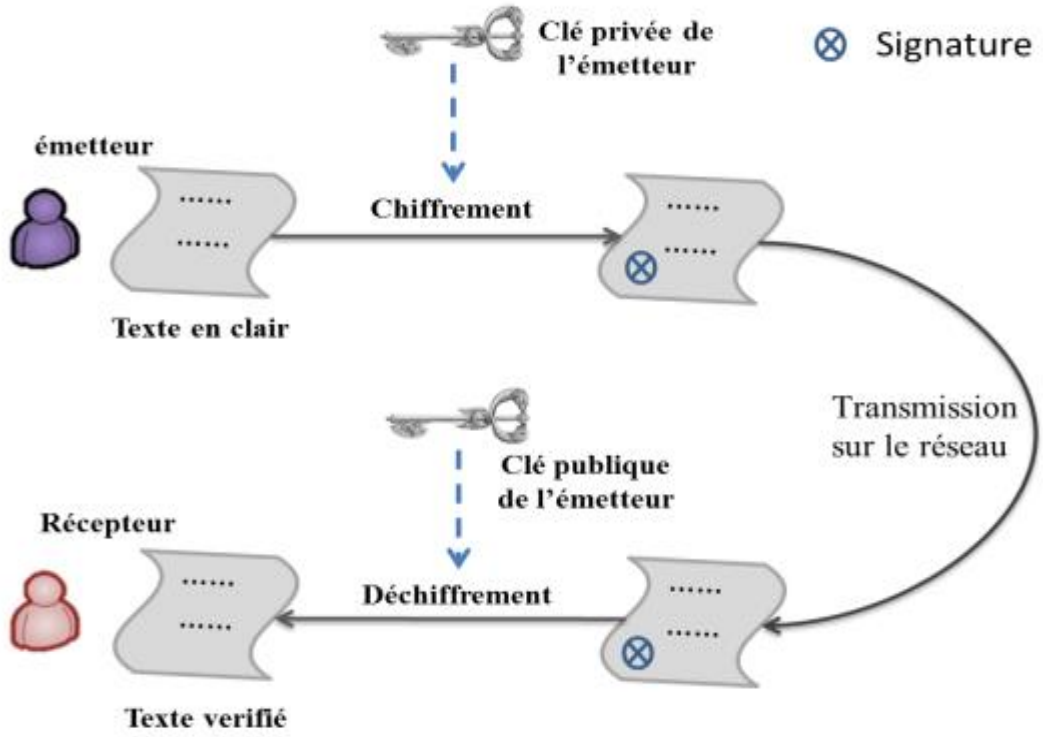

Figure 2 7: Signature Numérique

2.3.5. Solutions pour l'Authentification

Les protocoles de gestion efficaces des clés de groupe devraient prendre compte de besoins divers et des exigences qui peuvent êtres résumées en quatre points de vue: sécurité, qualité de service, ressources de KS et les ressources des membres du groupe [29].

1. le secret de transmission exige que les utilisateurs qui ont quitté le groupe n'aient aucun accès à aucune future clé. Cela garantit qu'un membre ne peut pas décrypter les données après avoir quitté le groupe. Pour assurer le secret de retransmission, une régénération de-clés du groupe avec une nouvelle clé est nécessaire après qu'un nœud quitte le réseau.

2. lorsqu'un nouvel utilisateur rejoint la session ; il ne doit avoir accès à aucune ancienne clé. Cette garantie permet qu'un membre ne puisse pas décrypter les données envoyées avant de rejoindre le groupe. Pour assurer le secret passé, un changement de clé de groupe avec une nouvelle TEK est nécessaire après chaque addition de nouveaux nœuds.

3. La liberté de collusion exige que tout ensemble des utilisateurs ne doive pas pouvoir déduire le trafic actuel clé de cryptage.

4. Indépendance des clés: un protocole est dit indépendant de clés si la divulgation d'une clé ne compromet pas d'autres clés.

5. Confiance minimale: le système de gestion des clés ne doit pas faire confiance à un grand nombre d'entités. Sinon, le déploiement efficace du régime ne sera pas facile.

2.3.6. Classification des protocoles de gestion des clés dans les MANETs

Les protocoles de gestion des clés peuvent être classés de différentes façons. Ils peuvent être regroupés en deux grandes catégories : les systèmes contributifs et les systèmes distributifs. Comme illustré dans la figure 2.8.

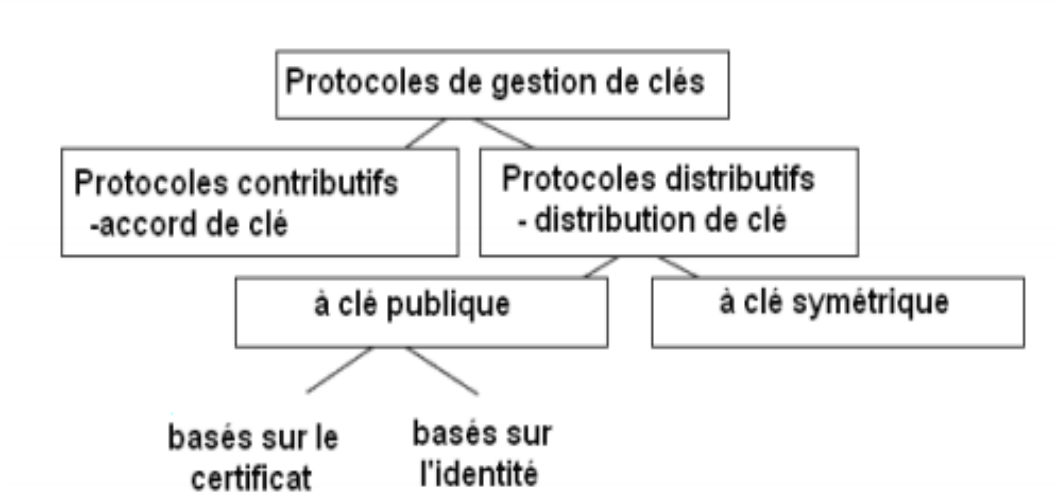

Figure 2 8: Protocoles de gestion des clés

2.3.6.1. La catégorie distributive

Elle englobe les protocoles selon lesquels chaque clé provient d'un seul nœud. Les nœuds peuvent très bien coopérer au cours de la distribution des clés, mais chacune d'elle provient d'une source unique. Les systèmes distributifs peuvent être centralisés, ou semi-distribués. Dans ce dernier cas, il existe des contrôleurs locaux qui aident le centre de distribution, ce dernier peut être à tout moment chargé ou point central de défaillances.

2.3.6.2. La catégorie contributive

Dans les systèmes contributifs, la clé est le résultat d'un effort de collaboration de plusieurs nœuds. Ce mode oblige chaque membre à calculer la clé de groupe en utilisant le protocole d'échange de clé de groupe Diffie-Hellman.

Le schéma d'accord de groupe est basé sur le système contributif, appelé accord de clé (ou Group Key Agreement) dans laquelle tous les nœuds coopèrent pour former une nouvelle clé de groupe.

Kumar et al. [30] Proposent un protocole contributif régional (région-based group-Key agreement protocol) qui utilise GECDH (The Group Elliptic Curve Diffie-Hellman Protocol) et utilise aussi TGECDH (Tree based Group Elliptic Curve Diffie Hellman Protocol). Dans ce cas, les membres du groupe sont organisés en un arbre binaire comme illustrer dans la figure 2.9.

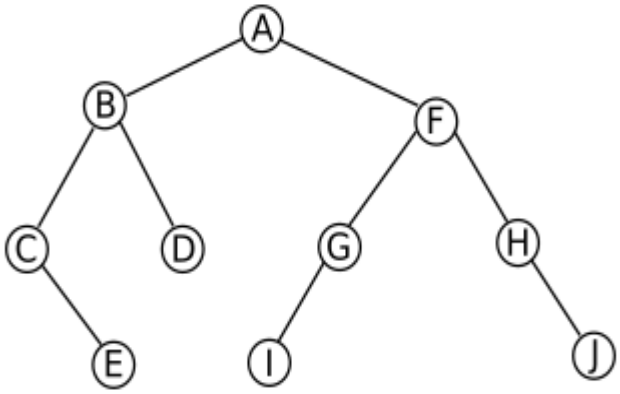

Figure 2 9: Arbre binaire

Dans cette proposition, le groupe de nœuds est organisé en sous-groupes régionaux, chacun avec un leader différent. Chaque sous-groupe régional a sa propre clé de groupe, et les leaders se communiquent à l'aide d'une clé de groupe externe. Ainsi, s'il y a un changement d'appartenance à un groupe spécifique, seule la clé de ce groupe est mise à jour. Pendant ce temps, si un leader quitte le réseau donc la clé du leader et la clé de groupe externe sont mises à jour. Bien que cette proposition soit sur les régions, il n'existe aucun mécanisme sur la répartition du réseau en régions ou comment élire les leaders n'est mentionné. De plus, le protocole suppose que des informations telles que le nombre de nœuds ou le moment où un membre quitte le réseau

est connu, mais aucun mécanisme de diffusion de ces données n'est prévu. Selon les auteurs, l'inconvénient de cette proposition est qu'il faut du temps pour générer une nouvelle clé de groupe. Un défi pour la plupart des propositions d'accord de clés est d'établir l'ordre des nœuds pour établir la clé de groupe et pour spécifier quel nœud est le nième nœud. En outre, la plupart des mécanismes d'accord de clés supposent que tous les nœuds connaissent les uns aux autres, ce qui est une hypothèse forte. Si nous prenons en considération le cas d'une clé de groupe pour un routage sécurisé dans les réseaux ad hoc. Dans cette situation, les nœuds ne connaissent aucune route, car ils ne sont pas en mesure d'échanger des messages de contrôle avant d'établir une clé de groupe. Par conséquent, toutes les clés contributives doivent être inondées dans le réseau.

Dans [31], Younchan Jung, Enrique Festijo et Marnel Peradilla proposent un protocole qui établit une clé secrète commune par le système contributif au lieu de la méthode de distribution de clé. Ils partent du principe que dans le réseau 5G, les appareils sans fils peuvent communiquer directement et gérer la plupart du trafic local au sein des réseaux D2D ad hoc. Ensuite, ces appareils sans fils en 5G répondront aux futures exigences d'Internet d'une manière à économiser de l'énergie et le coût. Ils proposent et précisent l'utilisation du protocole D2D ad hoc pour contrôler le réseau et gérer la clé de groupe dans un environnement ad hoc.

Ensuite, le processus d'accord de clé de groupe peut être combiné avec le processus de contrôle de routage. L'accord clé du groupe est déclenché pour mettre à jour la clé de groupe dans deux cas: chaque fois qu'un nœud rejoint le réseau ou lorsque deux réseaux se fusionnent en un seul réseau. D'un autre côté, le contrôle de routage a lieu lorsqu'un lien change d'état. Le contrôle de routage est responsable de l'inondation des informations à d'autres nœuds et le gestionnaire de transactions lance la procédure d'accord de groupe clé. Cette proposition est bien adaptée avec les caractéristiques ad hoc de la 5G, telles que l'absence des stations de base, la composition très dynamique du groupe et le changement fréquent de liaison, des nœuds et du réseau.

Dans ce protocole proposé, tous les nœuds n'ont besoin que d'une paire de clés publiques/privées et d'un certificat établi par une autorité central. Un certificat est une structure de données dans laquelle une clé est liée à une identité (et éventuellement à certains autres attributs) qui est délivré par une tierce partie de confiance. Si cette dernière estime qu'un nœud donné est digne de confiance, elle lui délivre un certificat qui va lui permettre de prouver sa légitimité envers les autres nœuds du réseau [26].

Dans [32], les auteurs proposent le protocole Two Round Key Agreement Protocol nommé TRP qu'on va utiliser dans notre simulation dans le prochain chapitre.

Dans TRP, l'initiateur du protocole devient le leader de groupe. Le leader commence par diffuser un message INIT pour lancer le processus de calcul de clé. Puis, le protocole a besoin de deux Tours :

Tour 1 : Chaque participant i, répond à la demande INIT en choisissant un secret r_i et en envoyant sa clé publique g^{ri} à l'initiateur.

Tour 2 : Le leader de groupe élève à la puissance de la clé publique de chaque membre se joignant à son secret r_i et les diffuse avec les contributions originales au groupe, c'est-à-dire il envoie $\{g^{ri}, g^{rl\,ri}\}$ pour tout i = 1, n et i≠l, n est le nombre de participants. Puis, chaque membre i vérifie si sa contribution est incluse correctement, enlève son secret r_i de $g^{rl\,ri}$ pour obtenir g^{rl} et calcule la clé de groupe :

$$TEK = g^{ri} * \prod_{i=1,n}^{i\neq l} g^{rl\,ri} = g^{rl(1+\sum_{i=1,n}^{i\neq l} ri)}$$

2.4. Conclusion

Nous avons vu dans ce chapitre, le principe général des réseaux mobiles ad hoc qui sont un type particulier de réseaux sans fil, ne nécessitant aucune infrastructure fixe pour se créer et s'organiser. Malgré les progrès réalisés dans ce domaine, pour atteindre les objectifs de ces réseaux, beaucoup de travail reste à faire. Les caractéristiques de ces réseaux constituent de réels défis. Le caractère fortement dynamique des réseaux ad hoc, nécessite l'implémentation de protocoles plus complexes que ceux des réseaux fixes ou des réseaux avec points d'accès. A cause de leurs vulnérabilités, les réseaux ad hoc sont sujets à de très nombreuses menaces. Pour faire face à la plupart de ces menaces, plusieurs protocoles de sécurité en étaient proposés.

Dans le chapitre suivant, nous intéresserons au protocole TRP afin d'évaluer le coût énergétique d'une communication lors de la génération de clés.

.

Chapitre 3

Chapitre 3: Simulation de l’énergie de communication

3.1. Introduction

L'économie d'énergie est une des problématiques majeures dans les réseaux Ad-Hoc. En effet, la recharge des sources d'énergie est souvent trop coûteuse et parfois impossible. Pour faire face a ce problème, la subdivision du réseau devrait être prise en compte pour que les capteurs économisent au maximum l'énergie afin de pouvoir fonctionner et d’avoir une longue durée de vie.

Ce chapitre est consacré à l’évaluation du coût énergétique d’une communication lors de la génération de clé en utilisant le protocole TRP dans le cadre des réseaux Ad-Hoc. Nous présenterons d’abord l’environnement de simulation python qui a été utilisé. Ensuite, nous proposerons deux modèles d’architectures que nous utiliserons dans notre simulation. Enfin, nous donnerons quelques résultats.

3.2. L’environnement de simulation

Python : un langage de programmation qui a été crée en 1989 par Guido van Rossum, aux Pays-Bas, sa 1er version publique a et e publiée en 1991. Et sa dernière version est la version 3 (version 3.7, a été publiée en juin 2018). La `Python Software Fondation est l'association qui organise le développement de Python et anime la communauté de développeurs et d'utilisateurs. Parmi ses avantages on cite :

- **Multiplateforme :** fonctionne sur de nombreux systèmes d'exploitation (Windows, Mac OS, Linux, Android, iOS), depuis les mini-ordinateurs jusqu'aux les supercalculateurs ;
- **Gratuit :** vous pouvez l'installer sur autant d'ordinateur que vous voulez ;
- **Un langage de haut niveau :** Il demande relativement peu de connaissance sur le fonctionnement d'un ordinateur pour être utilisé ;
- **Un langage interprété :** Le programme n'a pas besoin de compiler son programme pour pouvoir l'utiliser, contrairement à des langages comme le C ou le C++;

- **Orienté objet :** possible de créer en Python des entités qui ont un sens dans le monde réel (une cellule, une protéine, un atome) avec un certains nombres de fonctionnement et d'interaction ;
- Il est relativement simple à prendre en main.

Quelques bibliothèques que nous avons utilisées sous le python :

i) Matplotlib : permet de dessiner des graphiques depuis Python, nous avons importée Numpy sous une abréviation, comme suit :

> import matplotlib.pyplot as plt;

ii) Math : Permet de disposer des fonctions mathématiques usuelles. On peut importer juste les fonctions nécessaires par (from math import cos, log) ou toutes les fonctions Mathématiques par (from math import *).

3.3. Architecture des schémas proposés

Schéma 1 :

La figure 3.1 représente une zone géographique basée sur une couverture hexagonale qui se compose d'un hotspot et de plusieurs nœuds mobiles où une connexion entre la source (SN) et la destination (DN) est établie à travers un chemin à plusieurs sauts.

Graphiquement, on représente une cellule par un hexagone car cette forme approche celle d'un cercle. Cependant, en fonction de la nature du terrain et des constructions, les cellules n'ont pas une forme circulaire.

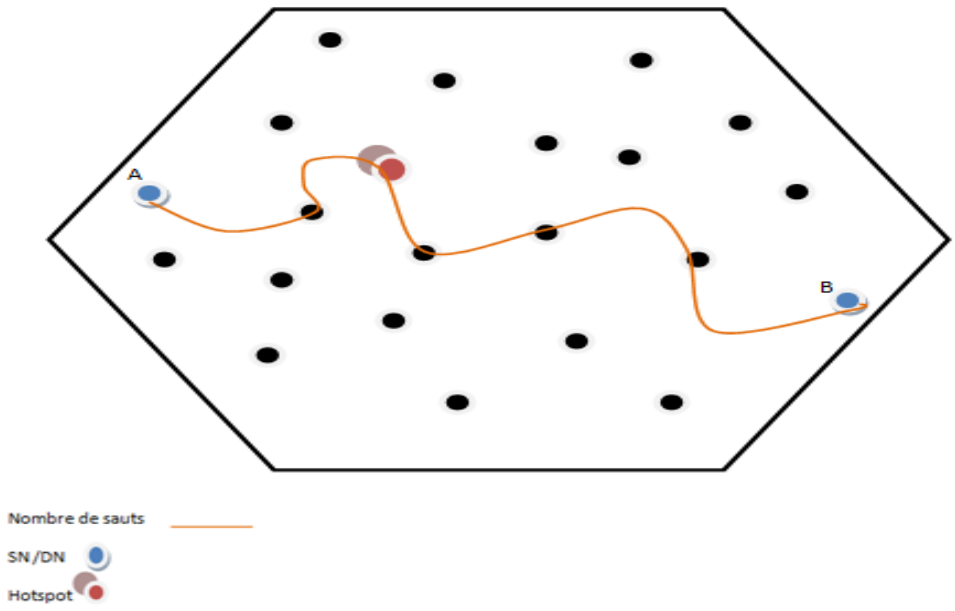

Figure 3. 1: Une zone géographique basée sur le modèle de couverture hexagonale.

Schéma 2 :

Nous présentons une architecture basé sur les communications D2D Ad-Hoc, comme illustré sur la figure 3.2. Le réseau est constitué d'une cellule qui est décomposé en petites cellules de forme hexagonales de différents niveaux. Chaque petite cellule mobile est contrôlée par un hotspot (ou cluster-head). Il s'agit d'un nœud mobile (appareil) au sein du cluster de nœuds mobiles qui est sélectionné pour devenir le gestionnaire radio local pour contrôler et maintenir le cluster. De plus, Grâce à la coopération, ces hotspots forment un réseau sans fil de petites cellules mobiles qui ont plusieurs passerelles / points d'entrée au réseau mobile. Le trafic de données entre les nœuds mobiles est établi via les communications D2D Ad-Hoc qui est sécurisé par le protocole TRP.

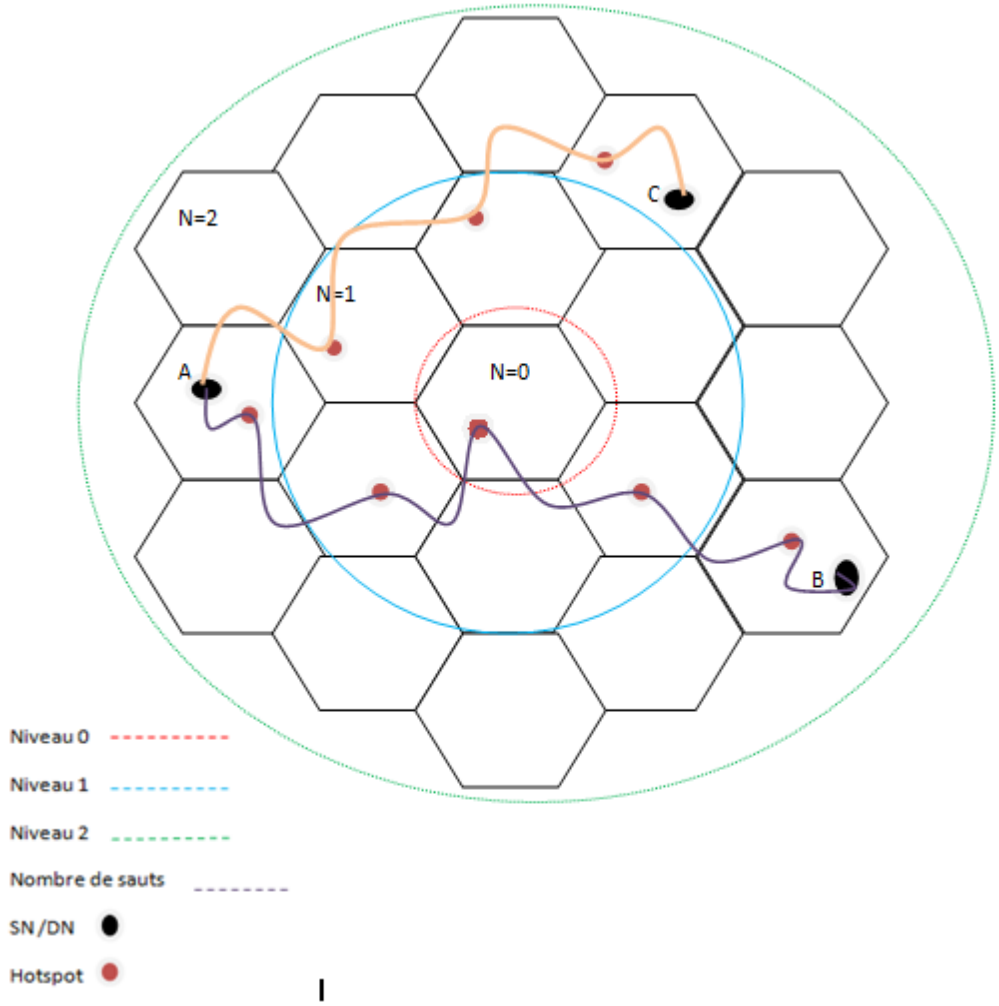

Figure 3. 2: Une zone géographique divisée en 3 niveaux basée sur le modèle de couverture hexagonale.

Supposons qu'un nœud mobile A souhaite partager un fichier multimédia avec un nœud mobile B. Le nœud mobile en possession du fichier multimédia, le nœud source (SN), envoie ce fichier aux nœuds mobiles sollicitant le fichier, les nœuds de destination (DN). Notez que ces nœuds mobiles ne sont pas tenus d'être dans la même petite cellule mobile, comme illustré sur la figure 3.2. Grâce aux communications D2D Ad-Hoc le fichier multimédia utilisant plusieurs sauts est acheminé par des nœuds mobiles, à travers le réseau de petites cellules mobiles du SN aux DN.

3.4. Analyse de l'énergie en fonction du protocole TRP

En générale le coût de consommation d'énergie E_{Tx} (B) pour B bits peut être calculé en utilisant la formule suivante [33]

$$\boldsymbol{E}_{\mathrm{Tx}}(\boldsymbol{B}) = \boldsymbol{B} \,.\, \boldsymbol{\varepsilon Tx} \qquad (3.\ 1)$$

Où $\boldsymbol{\varepsilon Tx}$ désigne l'énergie consommée par la radio de communications pour transmettre un bit .Un modèle plus détaillé pour la transmission est donnée dans [34].Pour transmettre un message B-bits sur une distance d, la radio dépense :

$$\boldsymbol{E}_{\mathrm{TX}}(\boldsymbol{B}, \boldsymbol{d}) = \boldsymbol{B} \,.\, \boldsymbol{\varepsilon Tx} + \boldsymbol{B}.\ \boldsymbol{d}^2 . \boldsymbol{\varepsilon Tx}_{\mathrm{a}}\, \boldsymbol{mp} \qquad (3.\ 2)$$

Où $\varepsilon Tx_{\mathrm{a}}\, mp$ désigne l'énergie consommé par bit par mettre carré ($J/bit/m^2$)

Le coût de la consommation d'énergie lors de la réception est donné par la fonction suivante :

$$\boldsymbol{E_{Rx}}(\boldsymbol{B}) = \boldsymbol{B} \,.\, \boldsymbol{\varepsilon Rx} \qquad (3.\ 3)$$

Où εRx se réfère à l'énergie consommée par la radio de communication pour recevoir un bit.

Dans notre modèle le coût de consommation de l'énergie lors d'un flux multicast peut être représenté par la fonction suivante :

$$\boldsymbol{EC_{TX}}(\boldsymbol{B}) = \boldsymbol{\beta}\mathrm{q} \qquad (3.\ 4)$$

Où β représente le coût énergétique consommé lors de l'envoi d'un flux multicast où

$$\boldsymbol{\beta = B.\varepsilon Tx} \quad (3.\ 5)$$

Quant à la réception la fonction est comme suit :

$$\boldsymbol{EC_{Rx}(B) = \beta', où\ \beta' = (B.\varepsilon Rx)\ (n-1)} \quad (3.\ 6)$$

Donc le coût énergétique d'une communication est :

$$\boldsymbol{EC_{com}(B) = EC_{TX}(B) + EC_{Rx}(B)} \quad (3.\ 7)$$

Par contre dans un réseau, le coût de consommation d'énergie augmente avec l'augmentation des nœuds, cela est dû au fait que certain nœuds ne sont pas à portée l'un de l'autre, ce qui fait que lors d'une transmission le message parcourt X stations avant d'arriver à la station destinatrice cela implique que le coût de consommation d'énergie augmente, dans ce cas il sera donné par cette fonction :

$$\boldsymbol{E_{TX}(B) = \beta.X + \beta} \quad (3.\ 8)$$

Le coût énergétique de la réception est comme suivant :

$$\boldsymbol{EC_{Rx}(B) = \beta', où\ \beta' = (B.\varepsilon Rx)\ (n-1)} \quad (3.\ 9)$$

Donc le coût énergétique d'une communication est :

$$\boldsymbol{E_{com}(B) = E_{TX}(B) + E_{Rx}(B)} \quad (3.\ 10)$$

Dans notre étude, on suppose que A initie la découverte des membres du groupe et seulement 4 membres (B C D E) montrent un intérêt mais en raison des contraintes de

connectivité, seulement B et C s'intègrent en choisissons un secret r_B, r_C et envoyant leurs clé publique g^{rB} , g^{rC} à l'initiateur A avec une génération de B= 1024 bits pour chaque clé.

Puis l'initiateur A envoie une paire de clés $\{g^{rB}, g^{rA\,rB}\}$ pour le membre B et $\{g^{rC}, g^{rA\,rC}\}$ pour C avec une génération de 2B pour chaque paire de clés. Ensuite B et C vérifient si leurs contributions sont incluses correctement, enlèvent leurs secret r_B , r_C de $g^{rA\,rB}$, $g^{rA\,rC}$ respectivement pour obtenir g^{rA} et calculent la clé de groupe TEK.

Donc le coût énergétique d'une communication lors de la génération de clé est :

$$\boldsymbol{E_{com}(3B) = E_{TX}(3B) + E_{Rx}(3B)} \qquad (3.\ 11)$$

3.5. Simulation et discussion des résultats

3.5.1. Modèle de simulation

Avant de lancer la simulation, nous devons fixer certains paramètres qui vont constituer le contexte de notre simulation. Le réseau est composé de 100 nœuds, déployé sur une surface de 1000 m^2 décomposé en plusieurs niveaux (N=0, N=1, N=2…etc.)
La figure 3.3 montre un réseau Ad-Hoc sans subdivision et la figure 3.4 montre réseau Ad-Hoc avec subdivision en N niveau.

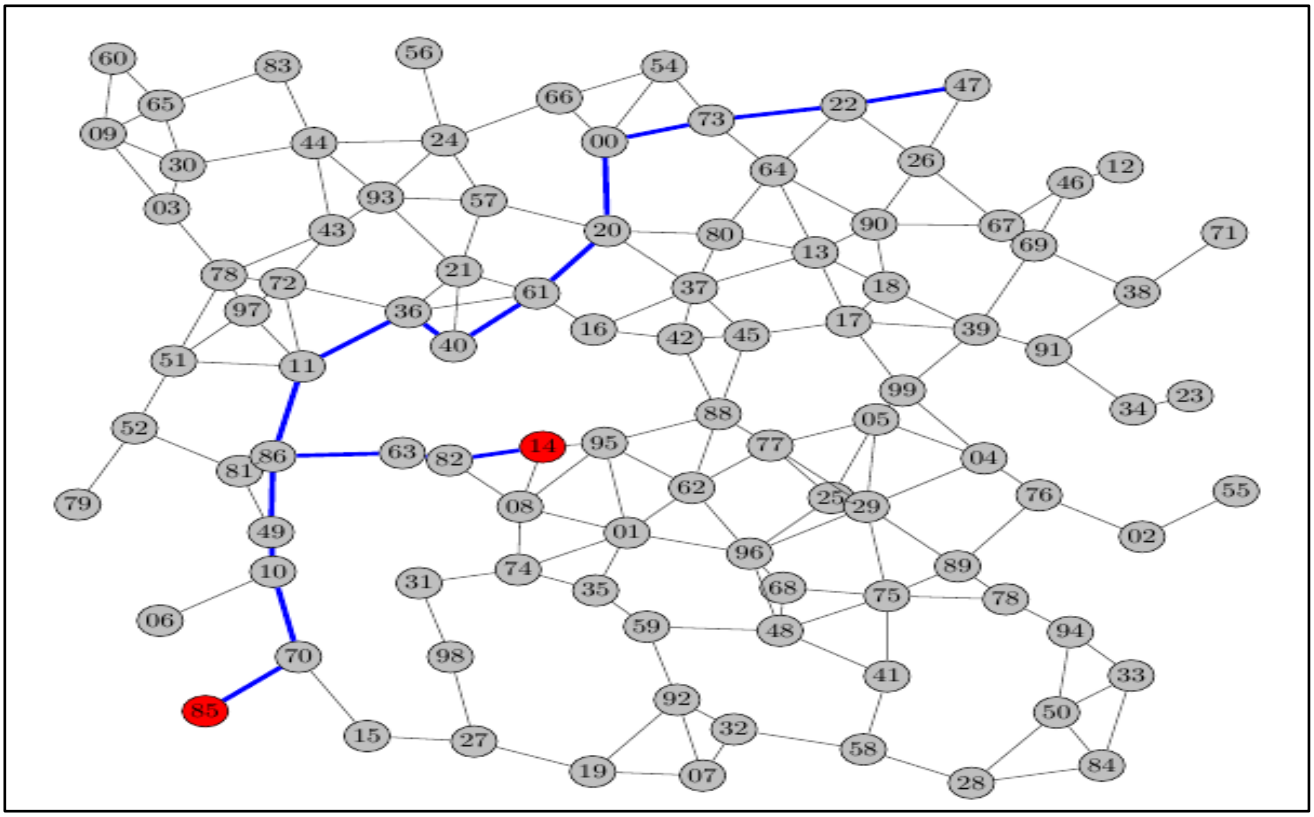

Figure 3. 3: Réseau Ad-Hoc sans subdivision

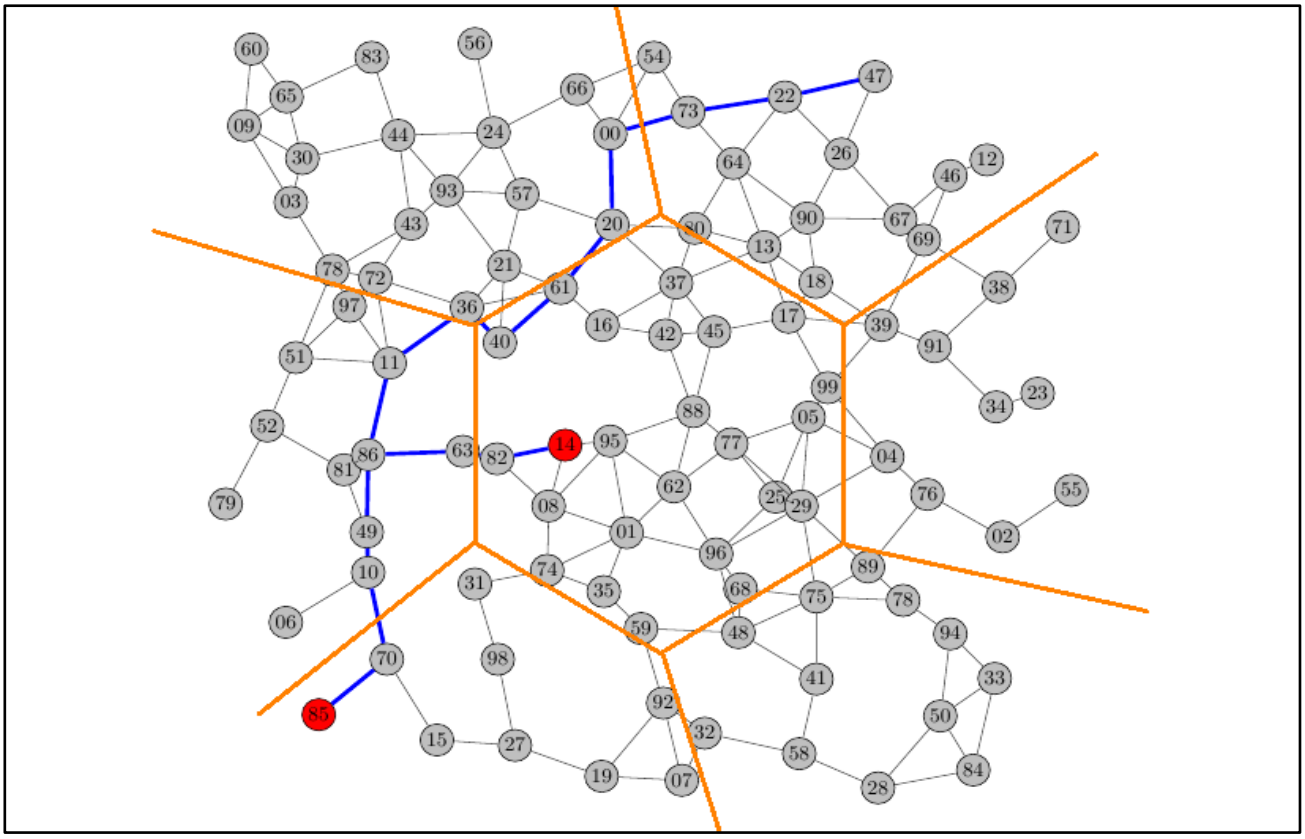

Figure 3. 4 : Réseau Ad-Hoc avec subdivision

On suppose que ce réseau utilise :

- un algorithme qui calcule le plus court chemin pour transporter l'information entre [A-B] et [A-C] (l'identifiant de A est 85, celui de B est 47 et celui de C est 14).
- Un protocole TRP comme un protocole d'accord de clé pour établir une communication sécurisée entre les nœuds.

La notation utilisée pour les formules mathématiques est illustré dans le tableau qui suit :

Paramètre	**Notation**
Nombre de bits	B
Nombre de niveau	N
La moyenne entre deux Hotspot	moy_d
Nombre de sauts pour B	d_1
Nombre de sauts pour C	d_2
le coût de consommation d'énergie	E_{TX}
Le coût énergétique de la réception	E_{Rx}
Le coût énergétique d'une communication	EC_{com}

Tableau 3. 1: Notation des paramètres

3.5.2. Paramètres de simulation

Soit le coût de consommation d'énergie pour l'envoi d'une donnée de 1024 bits est de 11.1 mJ, le coût de réception de cette donnée est de 7.69mJ [33] et dans notre cas pour générer 3B en utilisant les informations précédentes en appliquant le protocole TRP, on obtient 33.3 mJ pour l'énergie de consommation et 23.07 mJ pour l'énergie de réception.

Les paramètres de notre simulation sont résumés dans le tableau suivant :

Paramètres de simulation	**Valeur**
Zone de simulation	1000 m^2
Protocole d'accord de clé	TRP
Nombre de nœuds	100
Placement des nœuds	Aléatoire
Nombre de bits	1024
Energie pour l'envoie	33.3mj
Energie de réception	23.07mj

Tableau 3. 2: Paramètres de simulation

3.5.3. Résultats de simulation

Pour tracer les courbes sous python, nous avons importé la bibliothèque < matplotlib > destinée à tracer et visualiser des données sous formes de graphe.

3.5.3.1. Evaluation du coût énergétique de communication par rapport aux nombres de nœuds

En utilisant les formules précédentes, et en variant le nombre de nœuds sue une seul surface (sans subdivision), on obtient le graphe de la figure 3.5 qui illustre l'énergie de communication entre les nœuds [A-B] et [A-C] lors de la génération de clé en utilisant le protocole TRP.

- **Représentation graphique :**

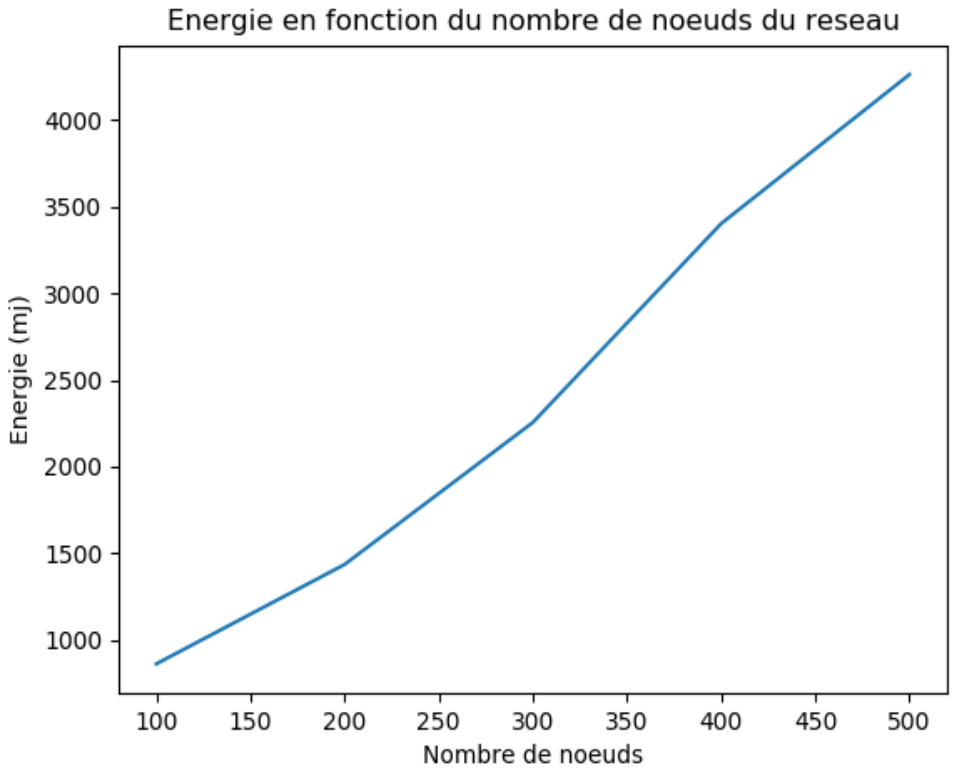

Figure 3. 5: Energie de communication en fonction de nombre de nœuds

Commentaire :

La courbe a été obtenue pour une variation de nombre de nœuds .Il est bien évident que le coût énergétique de communication augmente en fonction de nombre de nœuds, puisque dans ce cas les nœuds consomment leurs propre énergie en routant des données pour d'autre nœuds.

3.5.3.2. Evaluation du coût énergétique de communication par rapport aux nombres de niveaux

Dans notre simulation, on divise la surface en 6 niveaux (Tableau 3.3) et on suppose que :

- Pour N=1, la moyenne de sauts entre deux Hotspots égale à 5 ;
- Pour N=2, la moyenne de sauts entre deux Hotspots égale à 2 ;
- Pour N=3, la moyenne de sauts entre deux Hotspots égale à 1 ;
- Pour N>3, la moyenne de sauts entre deux Hotspots égale à 1 ;

Niveau N	0	1	2	3	4	5	6
moy_d	/	5	2	1	1	1	1
d_1	13	12	10	8	10	12	14
d_2	8	7	6	5	6	7	8

Tableau 3. 3: Nombre de sauts

- **Communication entre AB et AC**

En utilisant les formules précédentes, et en variant le nombre de niveaux (Tableau 3.3), on obtient le graphe de la figure 3.6 qui illustre l'énergie de communication entre les nœuds AB et AC lors de la génération de clé.

- **Représentation graphique :**

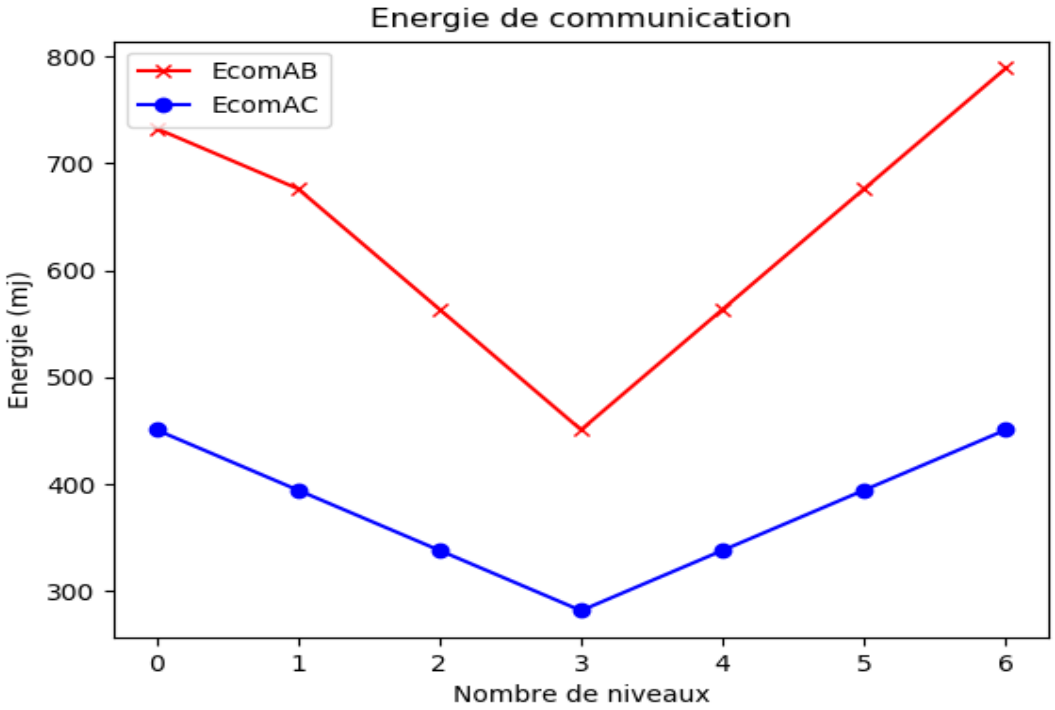

Figure 3. 6: Energie de communication en fonction de nombre de niveaux

Commentaire :

Les courbes ont été obtenues pour une variation de nombre de niveaux de 0 à 6. On constate qu'au niveau 0 l'énergie est maximale (sans subdivision, figure 3.3), de 0 à 3 l'énergie diminue vu que les communications passent directement via les hotspots. Autrement dit, ce n'est ^pas nécessaire de parcourir de longues distances, mais il suffit d'avoir un itinéraire plus direct via les hotspots et de 3 à 6 malgré la subdivision, l'énergie augmente de nouveau car le nombre de sauts augmente aussi.

- **Communication globale (AB+AC)**

- **Représentation graphique :**

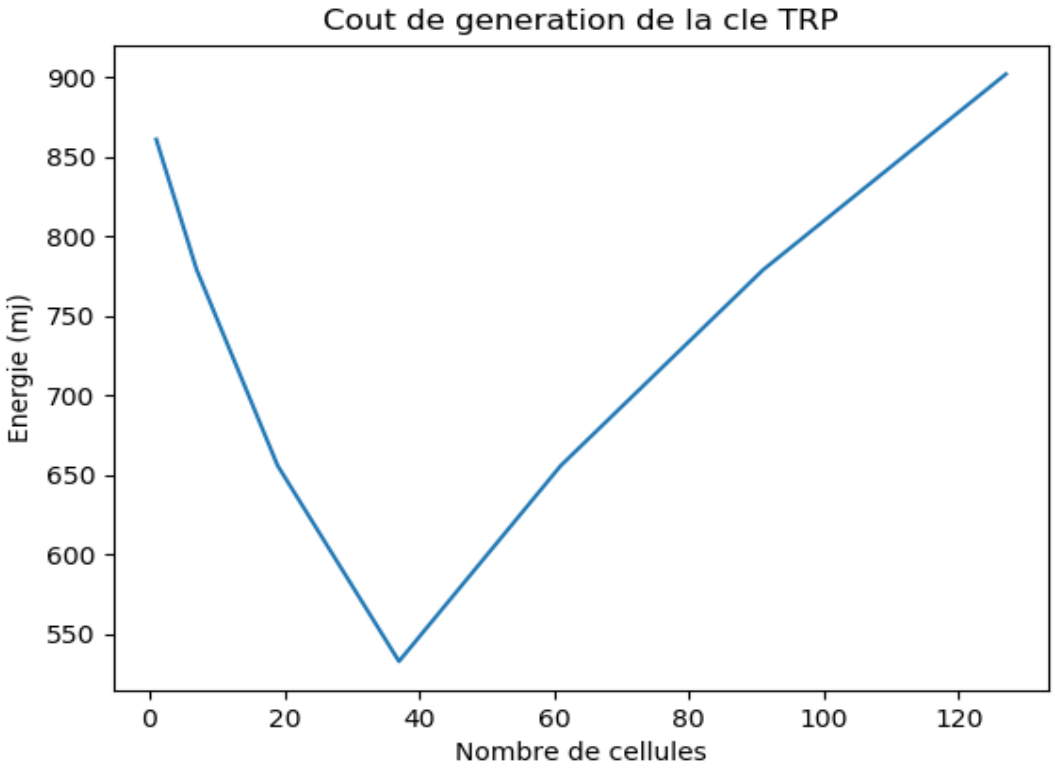

Figure 3. 7: Energie de communication globale en fonction de nombre de cellules

Commentaire :

-De 0 à 38 l'énergie diminue en augmentant le nombre de cellules.

-De 38à 12 L'énergie augmente en augmentant le nombre de cellules.

-Pour une valeur de 40 cellules on obtient l'énergie minimale.

3.5.4. Bilan des résultats

Le premier schéma est une surface sans subdivision où le nœud source choisit le chemin le plus court en effectuant des sauts jusqu'au nœud destination pour transmettre les données, dans ce cas le coût énergétique augmente avec l'augmentation de nombre de nœuds, ceci est dû au fait

que les nœuds consomment leurs propre énergie en routant des données vers d’autres nœuds. Pour éviter ce problème, nous avons proposé une subdivision du réseau qui répond à une meilleure conservation d’énergie. D’après nos résultats on a déduit qu’il existe une subdivision optimale qui permet une meilleure consommation.

En général, l’architecture du schéma 2 (fig.3.2) présente de multiples avantages par rapport à l'architecture du schéma 1 (fig.3.1). En autorisant les communications D2D Ad-Hoc à sauts multiples via un réseau de petites cellules mobiles, le trafic de données dans ce schéma n'a plus besoin d'être acheminé via plusieurs nœuds intermédiaires. Cela signifie que les données ne sont plus nécessaires pour parcourir les longues distances à destination, mais ont un itinéraire plus direct via les hotspots. Cela réduit considérablement la latence. Puisque les transmissions parcourent des distances plus courtes, les transmissions nécessitent moins d'énergie pour atteindre leur destination. Cela signifie que cette architecture permet également une transmission de données plus économe en énergie. Ce qui augmente la durée de vie du réseau.

3.6. Conclusion

Dans ce chapitre, à l'aide des expressions mathématiques de calcul du coût énergétique lors de la génération de clé en utilisant le protocole TRP dans deux modèles d’architectures proposés, nous avons effectué des simulations sous python. Pour illustrer l’énergie de communication en variant le nombre de niveaux, des résultats numériques sont visualisés.

Conclusion générale

Conclusion générale et perspectives

De nos jours, les activités humaines deviennent très dépendantes des services Internet mobiles. Les appareils sans fil 5G devraient répondre aux futurs besoins d'Internet d'une manière économe en énergie et en fonction des coûts en traitant directement le trafic local au lieu de transporter des données via une station de base

Dans l'évolution vers la 5G les indicateurs de performance traditionnels, tels que la capacité du réseau et l'efficacité spectrale doivent être continuellement améliorés. Une plus grande variété de modes de communication et d'applications doit être fournie pour améliorer l'expérience utilisateurs, c'est la où Ad-Hoc D2D intervient. Il est considéré comme une technologie émergente importante pour le cellulaire actuel et les réseaux. Il permet une communication directe entre utilisateurs, avec une amélioration de l'efficacité, et du débit du système.

Les réseaux mobiles ad hoc n'ont jamais cessé de susciter des préoccupations du fait qu'ils sont exposés à des menaces supplémentaires par rapport aux réseaux filaires. Ces menaces viennent généralement du fait que les communications sans fil sont transmises par ondes radios et peuvent être interceptées par des personnes non autorisées. La gestion de clés représente l'élément primordial pour assurer la confidentialité, l'intégrité et l'authentification des communications dans ce type de réseau.

La principale contrainte dans les communications sans fil est la durée de vie limitée des terminaux mobiles dont le support énergétique représente souvent une batterie dont la capacité est limitée. L'énergie est aujourd'hui l'un des critères les plus importants pour les réseaux Ad-Hoc.

Dans le cadre de ce mémoire, l'objectif était de réduire l'énergie de communication afin d'augmenter la durée de vie du réseau en effectuant l'évaluation sous le langage de programmation python.

Dans le premier chapitre, nous avons donné une vue globale sur la cinquième génération et le principe général de la communication D2D.

En second chapitre, nous avons présenté les réseaux ad hoc et ses concepts de sécurités.

Le dernier est destiné à des simulations, où nous avons évalué le coût énergétique de la communication lors de la génération de clés en utilisant le protocole TRP. Les résultats nous ont conduits à conclure que pour un certain nombre de subdivision on peut atteindre l'énergie optimale.

Perspectives

Le travail entrepris au cours de ce mémoire nous inspire plusieurs voies de recherche. Tout d'abord, il serait intéressant de poursuivre ce travail en effectuant des simulations sur des systèmes de taille plus importante. Il nous semble également important d'étudier la minimisation de la consommation d'énergie dans les réseaux ad hoc utilisant des protocoles de routage réactifs, proactifs ou hybrides. Enfin, étant donné le succès phénoménal des réseaux Ad-Hoc, Une expérience basée sur une implémentation de ces propositions dans un réseau ad hoc réel reste le meilleur moyen de tester leurs performances.

Bibliographie et Webographie

[1] Matthew Wall .Qu'est-ce que la 5G et qu'est-ce que cela signifie pour vous. [Online]. Available: https://www.bbc.com/afrique/monde-50223402

[2] Celik, Aslihan, Tetzner, Jessica, Sinha, Koushik, *et al.* 5G device-to-device communication security and multipath routing solutions. *Applied Network Science*, 2019, vol. 4, no 1, p. 1-24

[3] Olaobaju Abdulrahman, « device-to-device communication in 5g cellular networks», University of Vaasa. Mémoire Master, 2018.

[4] Rakotondrafara Nomena Tsiverilaza. Etude des performances du massif mimo avec la communication d2d dans le réseau 5 g. Mémoire master, Université d'Antananarivo, 2019.

[5] 5g: la technologie de la cinquième génération. [Online]. Available: https://www.bravotelecom.com/blog/5g-technologie-cinquieme-generation/#

[6] Youssef Lmoumen .Approche coopérative pour l'extension de la couverture cellulaire via une architecture d2d basée sur le protocole olsr. Université ibn tofail, Mémoire de magister, 2019

[7] Shen, Xuemin. Device-to-device communication in 5G cellular networks. *IEEE Network*, 2015, vol. 29, no 2, p. 2-3.

[8] Azni Cilia .Sélection du mode de communication d2d/d2i dans les réseaux 5g/lte .Mémoire Master, université a/mira-Bejaia, 2019.

[9] Mumtaz, Shahid et Rodriguez, Jonathan (ed.). *Smart device to smart device communication*. Switzerland: Springer International Publishing, 2014.

[10] Safdar, Ghazanfar Ali, UR-Rehman, Masood, Muhammad, Mujahid, *et al.* Interference mitigation in D2D communication underlaying LTE-A network. *IEEE Access*, 2016, vol. 4, p. 7967-7987.

[11] Masroor, R., Abrar, M., et Gui, X. Device to Device (D2D) Communication: Interference Management Perspective.

[12] Gandotra, Pimmy et JHA, Rakesh Kumar. Device-to-device communication in cellular networks: A survey. *Journal of Network and Computer Applications*, 2016, vol. 71, p. 99-117.

[13] Militano, Leonardo, Araniti, Giuseppe, Condoluci, Massimo, *et al.* Device-to-device communications for 5G internet of things. *EAI Endorsed Trans. Internet Things*, 2015, vol. 1, no 1, p. 1-15.

[14] Fatima Amezal.es technologies sans fil: le routage dans les réseaux ad hoc (olsr et aodv) .mémoire master, université de Bejaia, 2007.

[15] Sabrine Naimi. Gestion de la mobilité dans les réseaux ad hoc par anticipation des métriques de routage.Thèse de doctorat, Université Paris Sud, 2015. https://tel.archives-ouvertes.fr/tel-01208152

[16] Ilyas, Mohammad (ed.). *The handbook of ad hoc wireless networks*. CRC press, 2017.

[17] Boukhechem Nadhir. Routage dans les réseaux mobiles ad hoc par une approche à base d'agents. Mémoire master ,2017-2018.

[18] Daniel Mabele Mondonga. Etude sur les protocoles de routage d'un réseau sans fil en mode Ad-Hoc et leurs impacts, Mémoire Master, 2010.

[19] Ferroudj Sonia et Hadji Thiziri. Etude comparative des deux protocoles de routage dsdv et dsr dans le cadre des réseaux ad hoc. Mémoire de Master, Université A/Mira de Bejaïa, 2016.

[20] Saddiki, Kamel. *Denial of services attack in wireless networks*. 2019. Thèse de doctorat. University Djillali liabes of Sidi Bel Abbes.

[21] Security for mobile ad hoc networks, *2012*.[Online].Available :*https://www.sciencedirect.com/topics/computer-science/mobile-ad-hoc-network*

[22] Fatima Ameza. Les technologies sans fil : Le routage dans les reseaux ad hoc (OLSR ET AODV), Mémoire Master ,2007.

[23] O.Cheikhrouhou. Sécurité des réseaux ad hoc. Université de sfax, tunisie, 2005.

[24] BIBLE JR, Robert et BURNETT, Mark Steven. *Secured commercial transaction*. U.S. Patent No 6,856,976, 15 févr. 2005.

[25] Zimmermann, Philip R. et Zimmermann, Philip R. *The official PGP user's guide*. Cambridge : MIT press, 1995.

[26] Makhloufi Roza ,Baouch Immad .Gestion des clés publiques dans les réseaux mobiles ad hoc . Mémoire de Master, Université A. Mira de Bejaïa ,2012.

[27] Benhaoua Mohamed Kamel .Approche cryptographique basée sur les algorithmes génétiques pour la sécurité des réseaux ad hoc. Mémoire Master, Université d'Oran.

[28] Bidan, Christophe et Issarny, Valérie. *Un aperçu des problèmes de sécurité dans les systèmes informatiques*. IRISA, 1995.

[29] Challal, Yacine et SEBA, Hamida. Group key management protocols: A novel taxonomy. *International journal of information technology*, 2005, vol. 2, no 1, p. 105-118.

[30] K. Kumar, V. Sumathy, and J. Nafeesa Begum, Efficient Region -BasedGroup Key Agreement Protocol for Ad Hoc Networks using Elliptic Curve Cryptography, *2009.*

[31] Jung, Younchan, Festijo, Enrique, et Peradilla, Marnel. Joint operation of routing control and group key management for 5G ad hoc D2D networks. In : *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*. IEEE, 2014. p. 1-8.

[32] Augot, Daniel, Bhaskar, Raghav, Issarny, Valérie, *et al.* An efficient group key agreement protocol for ad hoc networks. In : *Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*. IEEE, 2005. p. 576-580.

[33] Teo, Joseph Chee Ming et Tan, Chik How. Energy-efficient and scalable group key agreement for large ad hoc networks. In: *Proceedings of the 2nd ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*. 2005. p. 114-121.

[34] Heinzelman, Wendi Rabiner, Sinha, Amit, Wang, Alice, *et al.* Energy-scalable algorithms and protocols for wireless microsensor networks. In: *2000 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings (Cat. No. 00CH37100)*. IEEE, 2000. p. 3722-3725.

Résumé

Les systèmes sans fil 5G promettent d'améliorer la technologie existante en fonction des futures demandes des utilisateurs. Ad-Hoc D2D est considérée comme une technologie prometteuse pour fournir des services à faible consommation d'énergie, à haut débit et à faible latence. L'un des objectifs majeurs de ces réseaux consiste à ce que les terminaux mobiles soient utilisés au maximum « n'importe où et n'importe quand ». Cependant, la principale contrainte dans les communications sans fil est la durée de vie limitée des terminaux mobiles dont le support énergétique représente souvent une batterie dont la capacité est limitée. Cette contrainte est beaucoup plus importante dans les réseaux Ad-Hoc. La sécurité des MANET représente un sujet de recherche ouvert et un défi majeur au regard de leur vulnérabilité aux différentes attaques. Dans ce mémoire, nous avons évalué le coût énergétique d'une communication lors de la génération de clés en utilisant le protocole TRP dans le cadre des réseaux Ad-Hoc.

Mots clés : 5G, Communication D2D, Réseau mobile Ad-Hoc, Energie, Sécurité.

Abstract

5G wireless systems promise to improve on existing technology based on future user demands. Ad-Hoc D2D is seen as a promising technology for delivering low power, high throughput and low latency services. One of the major goals for these networks is that mobile devices are used as much as possible "anywhere and anytime". However, the main constraint of wireless communications is the limited lifespan of mobile terminals whose energy support often represents a battery with limited capacity. This constraint is much more important in Ad-Hoc networks. The security of MANETs represents an open subject of research and a major challenge in view of their vulnerability to various attacks. In this work, we evaluated the energy cost of a communication during key generation using the TRP protocol within the framework of Ad-Hoc networks.

Keywords: 5G, D2D Communication, Mobile Ad-Hoc network, Energy, security.