République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahlab Blida

Faculté des Sciences

Département d'Informatique

MÉMOIRE DE MASTER

POUR L'OBTENTION DU DIPLÔME DE MASTER EN INFORMATIQUE

OPTION : SYSTEM D'INFORMATION ET RESEAUX

THÈME :

Un outil d'évaluation des systèmes de la gestion des clés cryptographiques dans les réseaux ad hoc

PRÉSENTÉ PAR : REZOUG Safaa KESSOUM Nacerin

ENCADRÉ PAR : Dr Nasri Ahlem

Devant le jury composé de :

Président de jury : Dr Yasmine GHEBGHOUB. Université Blida.

Examinateur : Dr Abderrazak KHEDHIRI. Université Blida.

Promotion 2021-2022

Dédicace

A mes très chers parents, nulle dédicace n'est susceptible de vous exprimer ma profonde affection
A mon mari pour son soutien
A mes enfants
A mes frères
A Nesrine
Safaa

Je dédie ce modeste travail

A la mémoire de mon père que dieu lui garde dans son vaste paradis

A ma très chère mère quoi que je fasse ou que je dise je ne saurai point de remercier comme elle se doit. Ton affection me couvre ; la bienveillance me guide et ta présence à mes côtés a toujours été ma source de force pour affronter les différents obstacles.

A L'homme de ma vie ; à mon soutien moral et source de joie et de bonheur mon marie pour l'encouragement et l'aide qu'il m'a toujours accordé

A mes sœurs ; mes frères pour leurs soutiens et

A ma fille RACHA

A mon binôme

Nasrine

Remerciement

Tout d'abord, nous remercions ALLAH pour la volonté, la force, la santé et la patience qu'il nous a donné afin de réaliser ce travail.

Nos remerciements et toute nos reconnaissances vont à tous les employés administratifs et les enseignants du département informatique, tout particulièrement

A notre encadreur

Docteur NASRI Ahlem

Pour nous avoir proposé le thème de ce travail et nous avoir encadrer tout le longue de sa préparation

Mme NASRI Ahlem n'a ménagé aucun effort pour nous guider et nous encourager à tenir jusqu' au bout

Quelle trouve ici le témoignage de nous profond respect et de toute nos gratitudes

Merci chaleureusement madame.

A madame la présidente de jury

Dr GHEBGHOUB Yasmine

Qui nous fait un grand bonheur de présider ce jury.

Quelle trouve ici l'expression de nos profonds respects.

A monsieur le membre de jury

Dr KHEDHIRI Abderrazak. Examinateur

Qui a accepté de juger ce travail, qu'il trouve ici l'expression de notre gratitude.

Enfin, nous remercions Toute personne qui a à des degrés divers, contribué sur le plan intellectuel, technique, moral, affectif ou encore matériel à l'achèvement de ce travail.

Merci

1 Table des matières

Résumé i

Introduction générale ii

Chapitre 1 1

1.1 Introduction 1

1.2 Les réseaux sans fil 1

1.2.1 La classification des réseaux sans fil selon l'infrastructure 2

1.2.2 La classification des réseaux sans fil selon la couverture 3

1.2.3 Technologies de communication sans fil 4

1.3 Les réseaux Ad hoc 4

1.3.1 Historique 4

1.3.2 Définition 4

1.3.3 Contraintes liées aux nœuds 5

1.3.4 Caractéristiques des réseaux Ad Hoc 6

1.3.5 Domaines d'application des réseaux ad hoc 7

1.3.6 Les différentes formes du réseau Ad Hoc 7

1.4 La Sécurité dans les réseaux ad hoc 18

1.4.1 Pourquoi la sécurité est difficile dans les réseaux Ad Hoc ? 18

1.4.2 Exigences de sécurité des réseaux ad hoc sans fil 19

1.4.3 Vulnérabilités des réseaux ad hoc sans fil 20

1.4.4 Types d'Intrusion dans les réseaux ad hoc sans fil 21

1.5 Conclusion 22

Chapitre 2 23

2.1 Introduction 23

2.2 Cryptographie 23

2.2.1 Concepts de base 24

2.2.2 les états et la transition de la clé 26

2.3 Tiers de confiance (TTP) 31

2.3.1 Modèle de confiance centralisé 31

2.3.2 PTT dans les systèmes de gestion de clés symétriques 32

2.3.3 Infrastructure à clé publique (PKI) 33

2.3.4 Modèle "web-of-trust " 34

2.3.5 Modèle de confiance décentralisé 34

2.4 Gestion des clés 34

2.4.1 Concepts de base de la gestion des clés 34

2.4.2 Classification des clés par type d'algorithme et utilisation prévue....37
2.4.3 Approches de la gestion des clés....39
2.4.4 Phases et fonctions de la gestion des clés....42
2.4.5 États et phases clés de gestion....46
2.5 Conclusion....47
Chapitre 3 48
3.1 Introduction....48
3.2 Schémas de gestion des clés dans les réseaux WANET....48
3.2.1 Schémas d'établissement de clés dans les réseaux ad hoc....49
3.3 Propriétés du système de gestion des clés....52
3.4 Taxonomies existantes....54
3.5 Travaux connexes....58
3.6 Conclusion....60
Chapitre 4 61
4.1 Introduction....61
4.2 Conception....61
4.2.1 Architecture de notre système....62
4.2.2 Les KMS utilisés....63
4.2.3 Les métriques d'évaluation utilisées....63
4.3 Environnement logiciel....64
4.3.1 Le Choix du simulateur OMNet++ :....64
4.3.2 Présentation OMNet++....65
4.3.3 Les plates formes OMNet++....65
4.3 Implémentation....66
4.4 Performance....69
4.4 Conclusion....71
Conclusion générale....72
Bibliographie....72

Table de illustrations

Figure1 1: Mode avec infrastructure BSS (1) 2
Figure1 2: Mode sans infrastructure (8).....3
Figure1 3: Couverture des réseaux sans fil (2) 3
Figure1 4: Communication un saute et multi-sauts des nœuds i et j (51) 5
Figure1 5: Architecture d'un réseau de capteur sans fil (5) 8
Figure1 6: changement de la topologie a cause de la mobilité (9) 10
Figure1 7 : Véhicule intelligent (9)**.** 13
Figure1 8: Les réseaux véhiculaire en mode ad hoc (44).....13
Figure1 9: Les réseaux ad hoc volants (FANET)(24) 15
Figure1 10 : Architecture de MANET,VANET et FANET (49).....16
Figure1 11: Le réseau des capteurs sous-marins (11).....17

Figure 2 1: Cryptographie symétrique (12) 25
Figure 2 2:Cryptographie symétrique (12) 26
Figure 2 3:Exemple d'état de transmission de clé (45).....27
Figure 2 4:Tiers en ligne et hors ligne (13).....31
Figure 2 5: Etablissement de la clé de session a l'aide de KTC ou DC (12).....32
Figure 2 6 : Principaux composant d'une PKI (9) 33
Figure 2 7:Types d'algorithmes couramment utilisés pour atteindre des objectifs spécifiques (13)......38
Figure 2 8: Protocole à trois passages de Shamir (14)......39
Figure 2 9: Échange de clés Diffie-Hellman (18) 40
Figure 2 10: Tiers en ligne, en ligne et hors ligne (22) 41
Figure 2 11: Phases et fonctions de la gestion des clés (4).....46
Figure 2 12: Principaux états et phases de gestion de clé (4).....47

Figure 4 1: Architecture de notre système.....62
Figure 4 2: Mise œuvre des KMS 66
Figure 4 3: Implémentation des KMS.....67
Figure 4 4: Création d'une simulation avec OMNET++.....69
Figure 4 5: Nombre de liens établis (forme textuelle).....70
Figure 4 6: Nombre de liens établis dans chaque phase par chaque KMS 70
Figure 4 7:la taille mémoire de chaque KMS 71

Résumé

Les réseaux ad hoc connaissent actuellement un grand succès, avec notamment la possibilité d'accéder à l'information et aux services indépendamment de sa position géographique. Ils ont montré leurs importances parce qu'ils sont mieux adaptés que leurs homologues filaires pour de nombreuses utilisations civiles ou militaires. Le système de gestion des clés cryptographiques (CKMS) est la pierre angulaire de la construction de la sécurité du réseau. Il est plus intéressant, plus difficile et fait face à de nouveaux défis dans les réseaux sans fil ad hoc que dans leurs analogues câblés. Dans cette thèse, notre objectif est de proposer un outil pour simuler et évaluer les schémas existants pour les réseaux ad hoc. Les métriques d'évaluation ont été simulées et évaluées pour aider le concepteur de réseau à choisir les meilleurs schémas de gestion des clés de sécurité pour son réseau.

Mots-clés : réseaux ad hoc sans fil, système de gestion de clés cryptographiques, schémas de gestion de clés, métriques d'évaluation, simulation à événement discrets.

Abstract

Wireless ad hoc networks are currently experiencing great success, including the ability to access information and services regardless of geographical location. They have shown their importance because they are better suited than their wired counterparts for many civilian or military uses. The Cryptographic Key Management System (CKMS) is the cornerstone of building network security. It is more interesting, more difficult and faces new challenges in ad hoc wireless networks than in their wired analogues. In this thesis, our goal is to propose a tool to simulate and evaluate existing schemes for ad hoc networks. Evaluation metrics were simulated and evaluated to help the network designer to choose the best security key management schemes for network.

Keywords: Wireless Ad hoc networks, Cryptographic Key Management System, Key Management Schemes, Properties, Evaluation Metrics

Introduction générale

1. Contexte du travail

Au cours de la dernière décennie, les réseaux ad hoc ont connu une énorme montée en popularité, et leur utilisation est montée en flèche. Par définition, un réseau ad hoc est simplement formé d'un ensemble de nœuds sans fil qui peuvent se déplacer librement et communiquer sans la présence d'une infrastructure préétablie ou d'une administration centralisée. Ces réseaux ont donc des capacités d'autoconfigurations et d'auto-organisation. La simplicité, la rapidité de déploiement, la robustesse, l'indépendance vis-à-vis de toute infrastructure et le faible coût sont les principales raisons de la supériorité des réseaux ad hoc sur les réseaux d'infrastructure.

L'une des principales préoccupations d'un réseau ad hoc est la sécurité. La complexité de la sécurité des réseaux ad hoc a défié des générations de chercheurs depuis leur apparition. La plupart de ces types de réseaux sont devenus des cibles précieuses pour les attaquants en raison de leurs activités importantes et de leurs informations sensibles qu'ils collectent et transmettent. Le souci de sécurité est plus sérieux dans les applications liées au militaire et à la e-santé.

Il existe de nombreuses méthodes d'assurer la sécurité, et de toutes ces méthodes, la cryptographie est la plus importante. La cryptographie est basée sur des clés secrètes. Ces clés sont établies et gérées par un système de gestion de clés (KMS). Par conséquent, il existe aujourd'hui de nombreux types de KMS qui sont pris en charge par le réseau ad hoc pour renforcer la sécurité. Certains d'entre eux peuvent ne pas être adaptés à un réseau donné. Cependant, il n'existe pas d'outils pour évaluer les schémas existants.

Dans cette thèse, notre objectif est de proposer un outil pour évaluer les schémas existants de réseaux en se basant de leurs propriétés.

2. Problématique et objectifs

Le système de gestion des clés cryptographiques (CKMS) est la pierre angulaire de la construction de la sécurité réseau. Il est d'un grand intérêt, il est plus complexe, et fait face à de nouveaux défis dans les réseaux sans-fil que dans les analogues câblés. Plusieurs CKMS ont été proposés dans la littérature, et certains sont génériques, tandis que d'autres sont spécifiques à certains types de réseaux. Ils ne considèrent pas souvent l'ensemble du processus de gestion et ne sont discutés que théoriquement sans donnant une idée claire sur les implémentations pratiques et leur utilisation.

D'un point de vue pratique, adopter un CKMS est une décision difficile qui doit être prise avec précaution car il y a tellement de paramètres à prendre en compte. Telles que les caractéristiques du réseau : débit, taux d'erreur, taux de perte de paquets, plage de communication, énergie initiale du nœud et le taux de consommation d'énergie, ainsi que le taux de défaillance des nœuds .la zone de déploiement et la densité des nœuds sont d'une grande importance. De plus, d'autres paramètres caractérisent les menaces possibles, comme le temps compromettre d'un nœud, la probabilité et la fréquence des attaques.

Notre objectif est de mettre en œuvre un simulateur d'évaluation des schémas de gestion des clés cryptographiques pour les réseaux sans fil ad hoc MANET, ce simulateur permet aux utilisateurs de choisir le bon schéma permis plusieurs, en basant sur les résultats obtenus. L'adoption d'un schéma particulier sera bien justifiée selon les critères du réseau et les métriques choisisses, cette opération permet d'éviter les alternatives nocives. De plus, elle permet aux concepteurs de tels schéma de valider leurs approches dans divers scénarios.

3. Organisation du mémoire

Ce manuscrit est formé en quatre (04) chapitres Il est organisé comme suit : le premier chapitre est réservé à la présentation du réseau ad hoc avec leurs caractéristiques et leurs types, le deuxième chapitre était réservé aux schémas de gestion de clés avec tous les concepts liés à ce sujet. Le troisième chapitre a illustré les schémas de gestion des clés dans les réseaux ad hoc. Dans ce chapitre, nous proposons une classification de tous les schémas de gestion de clés existants pour les réseaux ad hoc. Enfin, le chapitre quatre présente la conception et la mise en œuvre de l'outil proposé dans cette mémoire.

Chapitre 1 : Introduction au Réseaux Ad Hoc

Chapitre 1 1

1.1 Introduction 1

1.2 Les réseaux sans fil 1

1.2.1 La classification des réseaux sans fil selon l'infrastructure 2

1.2.2 La classification des réseaux sans fil selon la couverture 3

1.2.3 Technologies de communication sans fil 4

1.3 Les réseaux Ad hoc 4

1.3.1 Historique 4

1.3.2 Définition 4

1.3.3 Contraintes liées aux nœuds 5

1.3.4 Caractéristiques des réseaux Ad Hoc 6

1.3.5 Domaines d'application des réseaux ad hoc 7

1.3.6 Les différentes formes du réseau Ad Hoc 7

1.3.6.6 Comparaison entre les MANETs, VANETs et FANETs 16

1.4 La Sécurité dans les réseaux ad hoc 18

1.4.1 Pourquoi la sécurité est difficile dans les réseaux Ad Hoc ? 18

1.4.2 Exigences de sécurité des réseaux ad hoc sans fil 19

1.4.3 Vulnérabilités des réseaux ad hoc sans fil 20

1.4.4 Types d'Intrusion dans les réseaux ad hoc sans fil 21

1.5 Conclusion 22

Chapitre 1

Introduction au Réseaux Ad Hoc

Dans ce chapitre, nous présentons les réseaux sans fil ainsi que les idées clés associées. Nous allons faire La distinction entre le mode infrastructure et le mode sans infrastructure. Nous introduisons ensuite le concept des réseaux Ad Hoc avec leurs caractéristiques, inconvénients et avantages. Enfin nous abordons les domaines d'application les plus prometteurs et les différents types de réseaux ad hoc, ainsi que les caractéristiques de chaque type.

1.1 Introduction

L'émergence actuelle des appareils de calcul portables (ordinateur, téléphone, smartphones...), l'utilisation illimitée d'internet, sont autant d'éléments qui exigent des nouveaux besoins dans le domaine de la communication tel que la possibilité d'être mobile tout en restant connecté c'est à dire communiquer avec d'autres usagers, accéder à des services en tout lieu, à tout instant et depuis n'importe quel équipement mobile ou immobile. Le progrès récent de la communication sans fil a rendu ce défi possible.

Dans ce contexte beaucoup de solutions de communication sans fil de plus en plus performantes et évoluées sont apparues, Par ailleurs, les réseaux Ad Hoc, caractérisés par une structure dynamique, une facilité et une rapidité de déploiement, suscitent un intérêt particulier. Ce genre de réseaux a été conçu spécifiquement dans le but d'établir des communications dans des circonstances où l'installation d'une infrastructure de réseau filaire serait extrêmement difficile voire impossible. Au contraire des réseaux de communication avec infrastructure, aucune administration centralisée n'est disponible ou même nécessaire dans ce type de réseau.

1.2 Les réseaux sans fil

Les réseaux sans fil (en anglais Wireless network) permettent à ses utilisateurs d'accéder à l'information indépendamment de leurs positions géographiques. Les réseaux sans fil, sont des réseaux dans lesquels les machines participantes (ordinateur portable, téléphone mobile, PDA, etc.) peuvent communiquer sans liaison filaire. Ils sont basés sur des liaisons utilisant des ondes radioélectriques (radio ou infrarouge) à la place des câbles habituels. Ce genre de réseaux a été conçu essentiellement ; afin de pouvoir mettre en place assez rapidement un réseau de

communication et sans avoir besoin préalablement une infrastructure ; et dans le but est d'assurer une liaison indépendante de l'emplacement des entités qui constitues ce réseau.

1.2.1 La classification des réseaux sans fil selon l'infrastructure

Deux classes principales distingues le mode sans fil : les réseaux sans fil avec infrastructure et les réseaux sans fil sans infrastructure**.** (1)

1.2.1.1 *Les réseaux sans fil avec infrastructure*

Dans ce type de réseaux sans fil les unités mobiles (UM) appelée aussi nœuds communiquent directement avec des sites fixes appelés stations de base (SB) via des interfaces de communication sans fil, localisés dans une zone géographique limitée, appelée cellule comme le montre la figure 1.1. Le réseau est constitué d'une ou plusieurs cellules appelées BSS (Basic Service Set).

Chaque cellule correspond à une SB à partir de laquelle des UMs peuvent émettre et recevoir des messages. Les sites fixes (SB) sont interconnectés entre eux à travers un réseau de communication filaire mais peut être aussi sans fil. Le réseau GSM est un exemple typique des réseaux sans fil avec infrastructure.

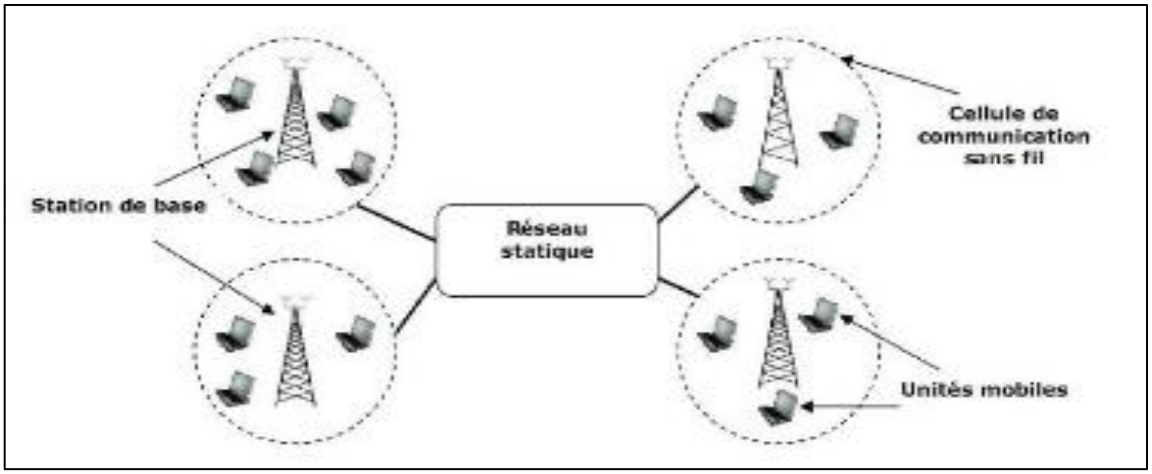


Figure1 1: Mode avec infrastructure BSS (1)

1.2.1.2 Réseau mobile sans fil sans infrastructure

Dans ce type appelé aussi mode Ad hoc ou IBSS (Independent Basic Service Set) les nœuds sont mobiles et communiquent entre eux directement sans faire appel à un point d'accès comme illustré sur la figure 1.2 chaque nœud peut communiquer avec les autres nœuds qui se trouvent dans sa zone de couverture.

L'absence de l'infrastructure ou des SBs, oblige les nœuds à se comporter comme des routeurs en participant à la découverte et la maintenance des chemins pour les autres nœuds du réseau.

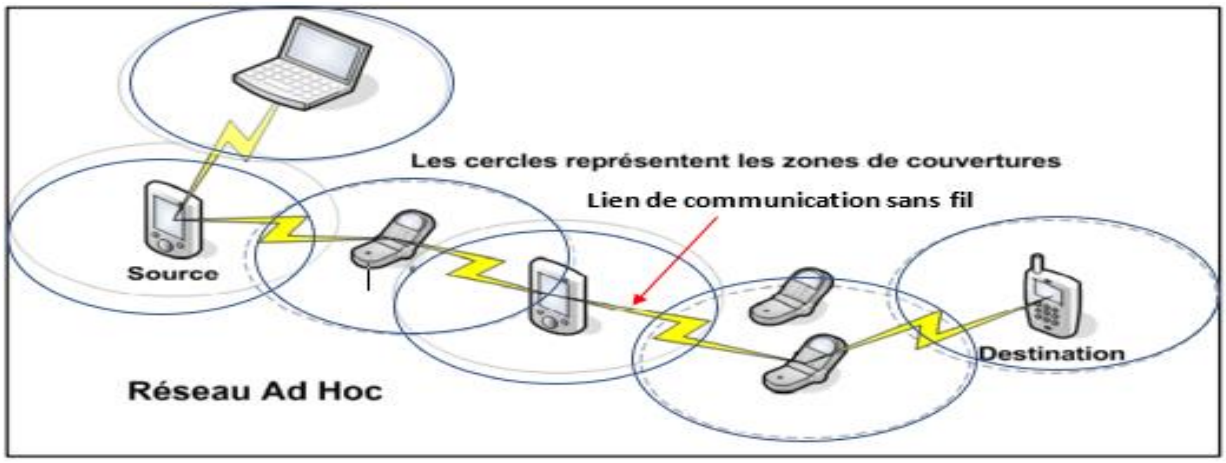


Figure1 2: Mode sans infrastructure *(8)*

1.2.2 La classification des réseaux sans fil selon la couverture

Les réseaux sans fil peuvent être regroupés selon le domaine d'application en quatre groupes spécifiques : Réseaux personnels sans fil (**WPAN**) utilisés en court distances entre un groupe privé d'appareils, les réseaux locaux sans fil (**WLAN**) utilisés dans des zones limités telles qu'une maison, un bureau ou un groupe de bâtiments, les réseaux métropolitains sans fil (**WMAN**) pour plusieurs blocs de bâtiments vers des villes entières et des réseaux étendus sans fil(**WWAN**) pour les régions et les pays. Ces quatre catégories sont illustrées à la figure 1.3.

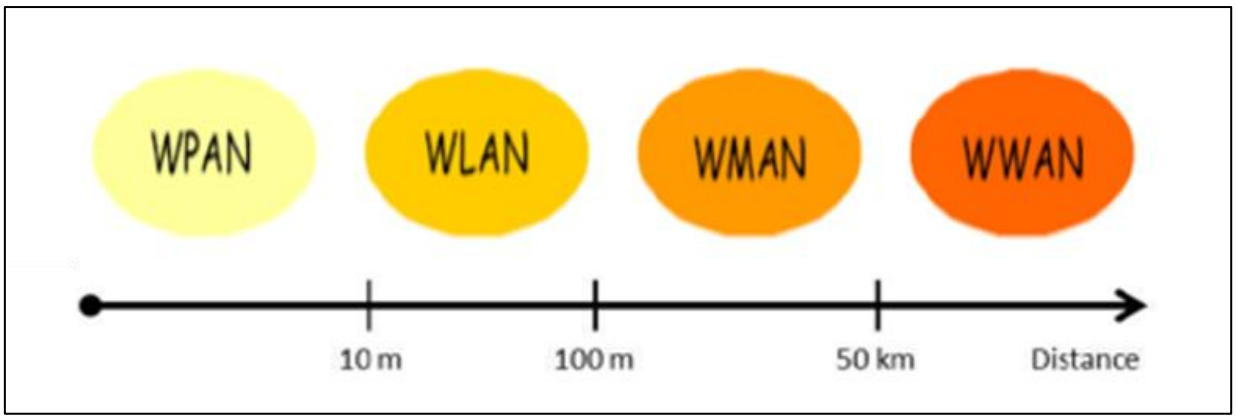


Figure1 3: Couverture des réseaux sans fil (2)

1.2.3 Technologies de communication sans fil

- ✓ **Le WPAN**, plusieurs technologies sont utilisées pour le réalisé tel que le Bluetooth (IEEE 802.15.1) et Zigbee (IEEE 802.15.4).

- ✓ **Le WLAN**, Ce réseau permet de connecter deux terminaux présents dans sa zone de couverture en utilisant diverses technologies à savoir le WiFi ou IEEE 802.11 et hiperLAN2.

- ✓ **Le WMAN,** est fondé sur la norme IEEE 802.16, dont la WiMAX (Worldwide Interoperability for Microwave Access) est la technologie sans fil la plus prometteuse qui permet d'obtenir des débits de l'ordre 70 Mbit/s et une couverture de plusieurs kilomètres.

- ✓ **Le WWAN**, permet ainsi de crée un réseau sans fil de couverture théoriquement illimité à l'aide de différentes technologies : GSM (Global System for Mobile Communications), GPRS (General Packet Radio Service), UMTS (Universal Mobile Télécommunications System).

1.3 Les réseaux Ad hoc

1.3.1 Historique

Le début des années 1970 voit, au sein du projet militaire Américain DARPA (The Défense 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 du protocole 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**.** (2)

1.3.2 Définition

Le dictionnaire français Larousse donne la définition suivante du mot Ad Hoc :
"Locution adjectival (mots latins signifiant pour cela), Se dit d'une personne qui convient parfaitement à une situation, à un usage, à un moment précis".

Cela signifie dans le domaine des réseaux informatique que le réseau Ad Hoc a été fait pour un but précis, souvent inattendu, comme sur un champ de bataille ou lors d'une catastrophe...

Ad Hoc ou WANET (Wireless Ad hoc Network) est un type de réseau sans fil décentralisé, ça veut dire il ne s'appuie pas sur une infrastructure préexistante, comme des routeurs dans les

réseaux filaires ou des points d'accès dans les réseaux sans fil administrés. Au lieu de cela, chaque nœud participe au routage en retransmettant les données aux autres nœuds(1)

Si deux nœuds i et j par exemple dans un réseau Ad Hoc sont dans la portée de transmission immédiate l'un de l'autre, ils peuvent directement échanger des messages. Cela est appelé la communication à un saut, tandis que la communication avec un nœud situé en dehors de la zone de transmission se fait par l'intermédiaire de plusieurs nœuds c'est ce qu'on appelle la transmission multi-sauts comme illustré sur la figure 1.4 Dans ce cas-là chaque nœud peut jouer le rôle d'un routeur et participe dans la découverte et la maintenance des routes. (3)

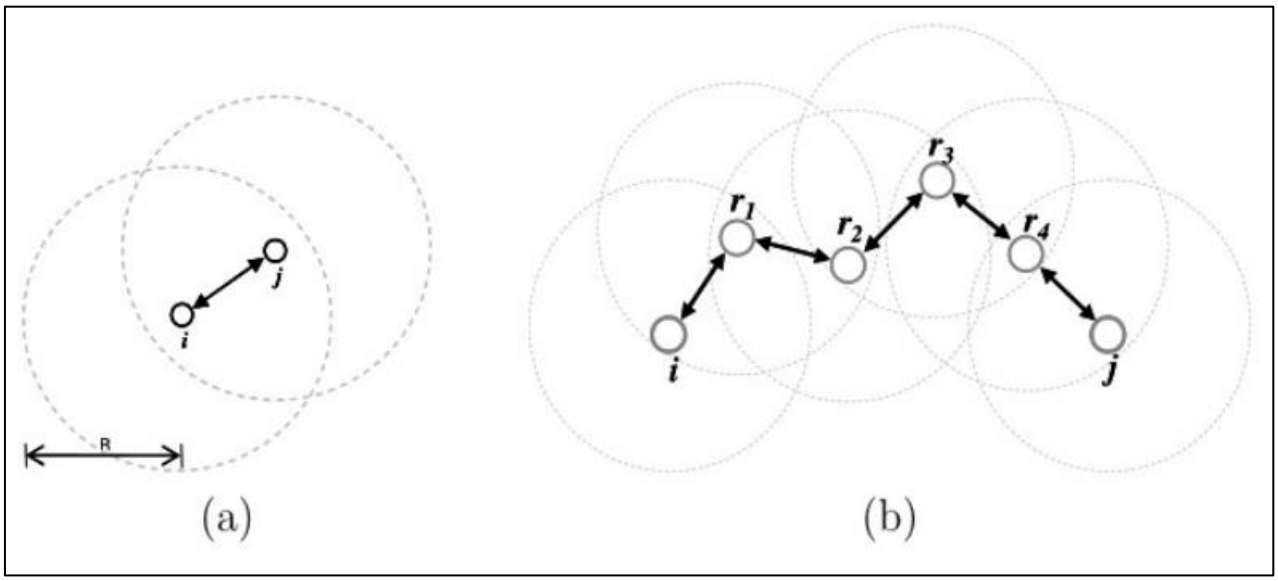


Figure1 4: Communication un saute et multi-sauts des nœuds **i et j** *(51)*

1.3.3 Contraintes liées aux nœuds

Les nœuds typiques d'un réseau Ad Hoc sont des ordinateurs portables, des assistants personnels, des téléphones cellulaires ou d'autres dispositifs mobiles sans fil. Présentant des contraintes similaires, car aucun serveur, routeur ou autre entité puissante n'est déployée ou accessible. Ces caractéristiques communes des dispositifs conduisent à plusieurs contraintes dont les quelles Selon (4) :

1. Puissance CPU limitée.
2. Mémoire limitée.
3. Charge de la batterie limitée.
4. Faible protection physique.

Ces contraintes réduisent fortement les capacités de calcul et de communication des appareils et donc de l'ensemble du réseau ad hoc.

1.3.4 Caractéristiques des réseaux Ad Hoc

Ce type de réseau présente plusieurs caractéristiques qui ne sont pas présentes dans les réseaux filaires, à savoir (3) (4):

- **Liaisons sans fil** : Le seul moyen de communication entre les nœuds mobiles au sein d'un réseau ad hoc est l'utilisation d'un canal radio. Malgré des progrès très importants, les performances des technologies sans fil restent et resteront en deçà de celles des technologies filaires. En effet, les liaisons sont à débits variables et la bande passante est assez limitée.

- **L'absence d'infrastructure :** Les réseaux ad hoc se distinguent des autres réseaux sans fil par l'absence d'infrastructure préexistante et la non disponibilité d'une administration centralisée. Les nœuds mobiles sont responsables de l'établissement et du maintien de la connectivité du réseau de manière continue.

- **La mobilité des nœuds** : la mobilité continue des nœuds crée un changement dynamique de topologie. Des liens peuvent se créer et disparaître très souvent. Ce déplacement a naturellement un impact sur la morphologie du réseau et peut modifier le comportement du canal de communication.

- **Auto-organisation :** Les réseaux ad hoc s'organisent automatiquement pour un déploiement facile, ils sont opérationnels de façon rapide. Ils s'adaptent aux conditions de propagation, au trafic et à la mobilité des nœuds.

- **Multi-sauts** : La topologie du réseau repose sur l'emplacement des différents nœuds qui change avec le temps. C'est pourquoi chaque nœud peut nécessiter la coopération d'autres nœuds pour acheminer un paquet vers sa destination finale.

- **L'hétérogénéité des nœuds :** un nœud mobile peut être équipé d'une ou plusieurs interfaces radio ayant des capacités de transmission variées et opérant dans des plages de fréquences différentes. Cette hétérogénéité de capacité peut engendrer des liens asymétriques dans le réseau. De plus, les nœuds peuvent avoir des différences en termes de capacité de traitement (CPU, mémoire), de logiciel, de taille mémoire (petite, grande) et de mobilité (lent, rapide).

- **Ressources énergétiques limitées** : Les équipements mobiles disposent de batteries limitées, et par conséquent d'une durée de traitement réduite. Cela limite les services et les applications supportées par chaque nœud, autrement dit l'épuisement de ses batteries engendre l'incapacité des nœuds à garantir la tâche de routage ce qui rend des parties de ce réseau inaccessible.
- **Vulnérabilité :** Les réseaux sans fil sont par nature plus sensibles aux problèmes de sécurité qui consistent les attaques menacent les données transmises et la vulnérabilité du support de communication partagé à l'écoute et au brouillage.

1.3.5 Domaines d'application des réseaux ad hoc

Les premières applications des réseaux ad hoc concernaient les communications et les opérations dans le domaine militaire. Cependant, avec l'avancement des recherches dans le domaine des réseaux et l'apparition des technologies sans fil d'autres applications civiles sont apparues. Selon (3) (4) les principales applications sont :

- **Etendre les réseaux :** Un des major problèmes des réseaux avec infrastructure est la couverture limitée. Les réseaux Ad Hoc sont sollicités afin d'étendre la couverture de ses réseaux.

- **Réseau domestiques :** réseaux Ad Hoc sont déployés aussi pour contribuer au confort domestique en transformant les logements personnels en environnements intelligents qui s'adaptent automatiquement au comportement des utilisateurs à l'aide des différents capteurs qui peuvent être installés facilement et évitent le câblage à la maison.

- **Situations d'urgence** : Opérations de recherche, de secourisme et de sauvetage durant les catastrophes naturelles.

- **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.

- **Le travail collaboratif :** Assurer les communications dans des entreprises ou bâtiments dans le cadre d'une réunion ou d'une conférence par exemple.

- **Domaine médical :** Garder un œil sur les patients et cela par la possibilité de recevoir des images en temps réel en utilisant la technologie biomédicale de manière plus ambitieuse. Par exemple : surveiller les organes, détecter les cancers avant qu'ils ne se propagent.la surveillance de la glycémie …

- **Domaine environnemental :** Réseaux de capteurs WSN utilisés dans le domaine environnemental afin de collecter les données métrologiques ou suivie des différents phénomènes naturels (les tsunamis, les feux de forêts, la pollution, le climat, etc.).

- **Transport :** Pour la gestion du trafic.

1.3.6 Les différentes formes du réseau Ad Hoc

Les réseaux ad hoc ou WANET (**W**ireless **A**d hoc **NET**work) sont classés en fonction de leurs exigences d'application, de leur objectif, du type d'équipement utilisé et de l'environnement physique en plusieurs catégories.

Dans ce qui suit, nous discuterons les types les plus couramment utilisés.

1.3.5.1 Réseaux de capteurs sans fil (RCSF)

1.3.5.1.1 Définition

Les réseaux de capteurs sans fil ou Wireless sensor networks (WSN) sont un ensemble de dispositifs souvent très petits, nommés "nœuds capteurs", formant un réseau sans infrastructure. Dont chaque nœud est capable de détecter des phénomènes et de traiter l'information au niveau local ou de l'envoyer à un ou plusieurs points de collectes.

Les WSN sont utilisés pour mesurer certains phénomènes physiques, tels que la température, la pression, l'humidité, la lumière, le mouvement, etc. C'est une technologie très utilisée pour des besoins militaires comme le suivi des troupes dans les champs de bataille. Les RCSFs peuvent être utilisés aussi pour assurer une surveillance permanente des organes vitaux de l'être humain (la détection de cancer, surveillance de glycémie, température corporelle, etc) grâce à des micro-capteurs qui peuvent être implanté sous la peau. La figure 1.5 illustre un réseau de capteurs sans fil.

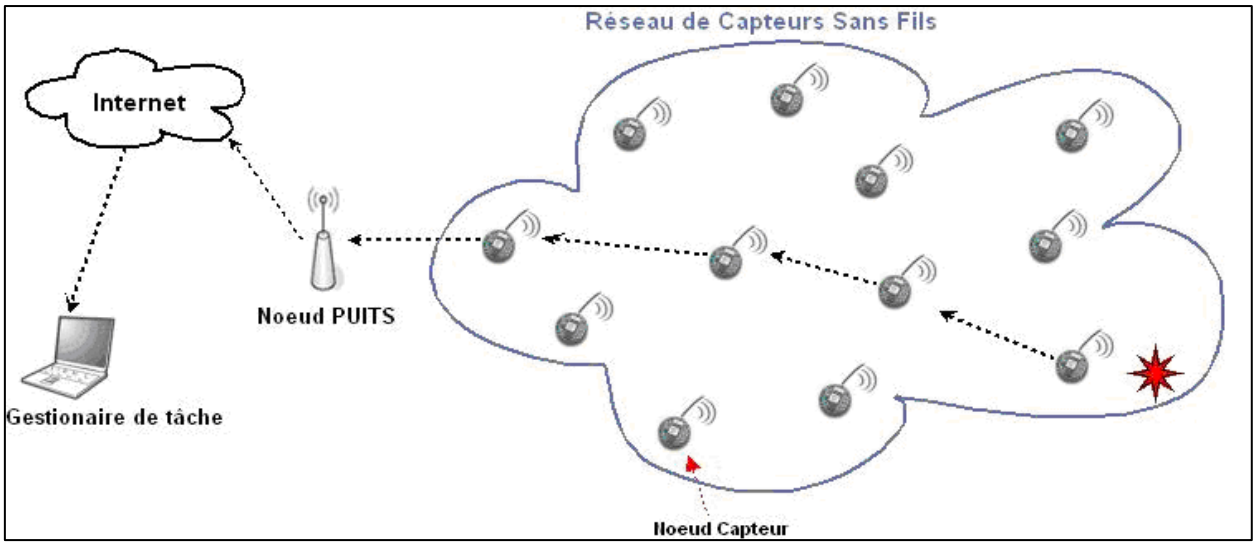


***Figure1 5: Architecture d'un réseau de capteur sans fil** (5)*

1.3.5.1.2 Contraintes et défis du RCSFs

Les RCSFs partagent certaines caractéristiques des réseaux ad hoc mais aussi possèdent des propriétés et des contraintes qui leurs sont propres parmi lesquelles (6):

- **La consommation d'énergie :** L'énergie est considérée comme la contrainte principale dans un réseau de capteurs. Il est important de tenir compte de cette contrainte car la plupart

des machines fonctionnent sur batterie. Après la décharge de la batterie, l'utilisateur est obligé de trouver une source électrique pour la recharger. Cependant, dans les réseaux de capteurs, il est pratiquement impossible de recharger de par le nombre élevé de capteurs par installateur et de par la difficulté de l'environnement dans lesquels ils peuvent se trouver. Une fois la batterie est vide, le capteur est considéré comme mort ou hors service. L'objectif à atteindre devient l'augmentation de la durée de vie du réseau de capteurs.

- **L'échelle :** Le nombre de nœuds déployés pour un projet peut atteindre le million. Un nombre aussi important de nœuds engendre beaucoup de transmissions inter nodales et nécessite que le puits "sink " soit équipé de beaucoup de mémoire pour stocker les informations reçues.

- **L'auto-organisation :** la mobilité et l'évolutivité des capteurs modifient fréquemment la topologie des WSN ce qui conduit à une auto réorganisation du réseau.

- **La fiabilité et la disponibilité :** les capteurs peuvent tomber en panne et fournir des informations erronées vers d'autres nœuds. Cela est dû aux conditions environnementales difficiles. Ils sont impactés par les vibrations, les environnements hautement corrosifs, L'humidité, la saleté ou la poussière qui dégradent leurs performances.
- **Mécanismes de sécurité adaptés :** Dans une architecture distribuée décentralisée, tous les nœuds sont similaires et personne n'est responsable de la réalisation des services réguliers, tout nœud peut rejoindre ou disjoindre le réseau à toute heure. Cela implique différents défis de sécurité, tels que l'absence d'un tiers de confiance partie, stockage de clés et capacités de traitement relativement petites.

1.3.5.1.3 Les avantages du RCSFs

Un WSN présente de nombreux avantages par rapport au système de surveillance traditionnel par câble :

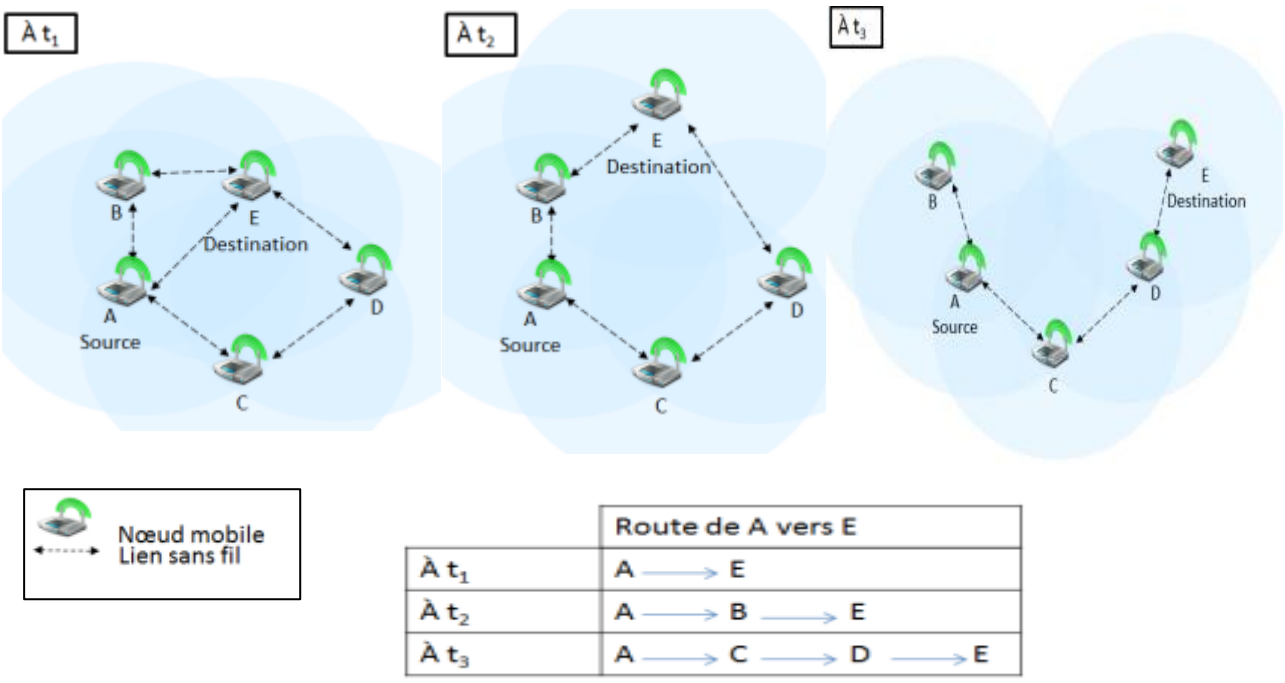
- Il est adaptable et flexible, permettant des partitions physiques.
- Les WSN ont un large éventail d'applications.
- Tous les nœuds WSN sont accessibles via un système de surveillance centralisé.
- Il est évolutif, il peut donc accepter de nouveaux nœuds ou appareils à tout moment.

1.3.6.2 Les MANETs

1.3.5.1.4 Définition

Mobile **A**d hoc **NET**work, est un ensemble de nœuds mobiles reliés entre eux par des connexions sans fil qui forment un réseau temporaire et dont la gestion de la communication s'effectue d'une façon autonome sans administration centralisée. Le fait que les nœuds sans en perpétuel mouvement rend la

topologie du réseau dynamique, comme illustré sur la figure 1.6. On peut trouver les Manet dans différents domaines à cause de la facilité de leur mise en œuvre. La mobilité des terminaux est l'avantage indéniable des Manets.



	Route de A vers E
À t_1	A → E
À t_2	A → B → E
À t_3	A → C → D → E

Figure1 6: changement de la topologie a cause de la mobilité *(9)*

1.3.6.2.2 Contraintes et défis du MANETS :

Les caractéristiques de MANET introduisent plusieurs défis qui doivent être étudiés attentivement avant qu'un large déploiement puisse être attendu (7). Ceux-ci inclus :

- **Contraintes de ressources :** l'utilisation des dispositifs mobiles à faible puissance (une bande passante, une énergie et un processeur limités, ainsi que de faibles capacités de mémoire). Cela engendre l'incapacité des nœuds à garantir la tâche de routage ce qui rend des parties de ce réseau inaccessible.
  Toutes les opérations qu'effectuent ces nœuds consomment de l'énergie (déplacement, envoi, réception, ...), il faudrait prendre en considération cela à tous les niveaux de conception afin de maintenir le réseau en activité le plus de temps possible, ainsi que les fonctions liées à la communication et au routage doivent être optimisées pour la consommation de la taille de stockage.

- **Manque de l'infrastructure :** le MANET n'a pas de serveur de surveillance centralisé. L'absence de gestion centralisée rend la détection d'attaques difficile car il n'est pas facile

de surveiller le trafic dans un réseau ad hoc hautement dynamique et à grande échelle. L'absence de gestion centralisée entravera la gestion de la confiance pour les nœuds.

- **Topologie dynamique :** La mobilité aléatoire et inattendue des nœuds provoque des changements fréquents et dynamiques dans la topologie du réseau. Le protocole de routage doit être capable de faire face cette dynamique.

- **Sécurité physique limitée :** l**es** réseaux sans fil sont plus sensibles aux attaques que les réseaux filaires**.** De plus les mécanismes de sécurité utilisée pour les réseaux traditionnels ne peuvent pas être appliqués dans les réseaux Ad Hoc tel que les certificats numériques. Cela conduit au développement de divers schémas de sécurité et d'authentification.

- **Routage multi-saut :** Dans les MANETs le paquet doit être acheminé via un ou plusieurs nœuds intermédiaires afin d'atteindre sa destination. Figure *1.5*. Les nœuds commencent par découvrir leur voisinage (les nœuds qui sont à l'intérieur de leur zone de couverture) et à chaque fois que l'un d'entre eux souhaite communiquer, il envoie son message à ses voisins qui à leurs tours l'envoient à leurs voisins et ainsi de suite. Puisque la topologie du réseau change aléatoirement des liens peuvent se créer et disparaître très souvent. Le problème d'acheminement des paquets dans ces conditions doit être géré efficacement par le protocole de routage pour maintenir une vision correcte de la topologie.

1.3.6.2.3 Les avantages des MANETs

- Fonctionne sans aucune infrastructure.
- Offre une grande mobilité.
- Fournit un accès à l'information et aux services quelle que soit la zone géographique.
- Peu coûteux.
- Le réseau peut être configuré à n'importe quel endroit et à tout moment.
- Tolérance aux pannes.

1.3.6.3 Comparaison des RCSF et MANET

Le tableau 1.1 résume les différences entre les réseaux de capteurs et les réseaux MANET selon. (8)

Paramètres	**MANET**	**RCSF**
Normes	IEEE 802.11	IEEE 802.15.4
Nombre de nœud	Moins que RCSF	Très grand
Mouvement des nœuds	Décentralisé	Centralisé
Fonctionnement des nœuds	Chaque nœud a son propre objectif.	Nœuds collaborent pour remplir un objectif

Interaction	Avec les humains	Avec l'environnement
Objectif principal	Informatique distribuée	Collecte d'informations
Équipement	Plus cher	Moins cher que MANET
Échelle	Plus grande	Beaucoup plus grande
Bande passante	Déficiente plus que RCSF	Parfois déficitaire
Défaillance dans les nœuds	Moins que le RCSF	Plus susceptibles aux pannes
Capacité des nœuds	Des nœuds ayant plus de capacité de traitements et de stockage	Des petits nœuds avec moins de capacité de traitement et de stockage
Redondance des données	Non	Oui
Protocoles de routage	Proactif, réactif, hybride,	Hiérarchique, basé sur l'emplacement , routage a plat
Taille du réseau	Dépend des utilisateurs actifs	Dépend de l'extension du zone observée
Mode de communication	Any-to-any	Many-to-one
Identification	Une adresse unique pour chaque nœud, utilisée pour réaliser la communication entre les nœuds.	Souvent pas d'adresses uniques, les requêtes sont envoyées à tous les nœuds.

***Tableau 1-1 : Différence fondamentale entre RCSF et MANET** (8) .*

1.3.5.2 Les VANETs

1.3.6.4.1 Définition

Vehicular **A**d hoc **NET**works, Les réseaux véhiculaires sont une particularité des réseaux MANETs où les nœuds mobiles sont des véhicules intelligents (figure 1.7) équipés de calculateurs, de carte réseaux et de capteurs. Ils permettent d'établir des communications entre les véhicules de 300 m à 1 km (pour échanger les informations sur le trafic par exemple) ou avec les stations de base placées tout au long des routes (pour demander des informations ou accéder à internet…) (9) (10).

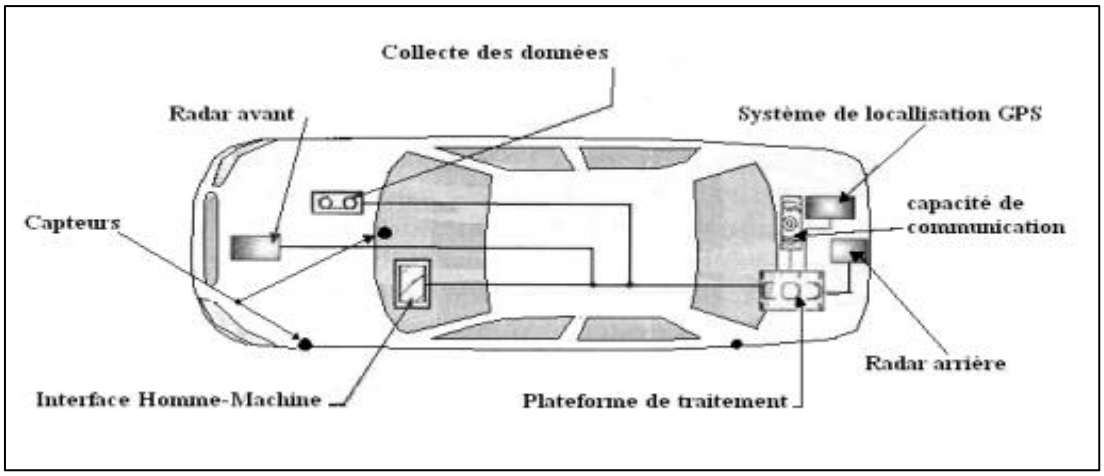


***Figure1 7 : Véhicule intelligent** (9).*

Les VANETs sont devenues l'une des technologies sans fil les plus pertinentes. Ils regroupent deux classes d'applications, à savoir les applications qui permettent l'implémentation des systèmes de transport intelligents (ITS : Intelligent Transport Systems) et celles liées au confort ou à la sécurité routière du conducteur et des passagers (10).

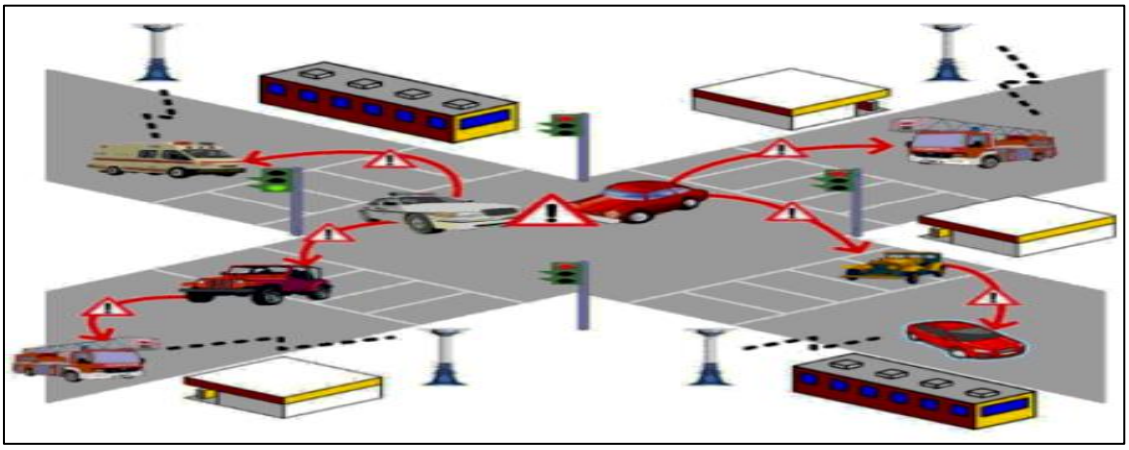


***Figure1 8: Les réseaux véhiculaire en mode ad hoc** (44)*

1.3.6.4.2 Contraintes et défis du VANETS

VANET est une application de MANET, mais il a ses propres caractéristiques et ces fonctionnalités présentent des problèmes et des défis distinctes qui peuvent se résume, selon (10), comme suit :

- **Traitement en temps réel :** les VANET permettent à un véhicule d'avertir automatiquement les autres véhicules à proximité sur ses mouvements (freinage, changement de voie, etc.) permettent également d'envoyer des annonces sur les conditions de la route (embouteillages, accidents) à d'autres véhicules afin que ces derniers puissent en profiter des informations

pour sélectionner des itinéraires évitant les points gênants. Ces messages d'alerte nécessitent un traitement en temps réel (cet échange doit être fait en des délai très courts). Puisque les situations qui y sont reliées sont critiques.

- **Sécurité :** La sécurité est un défi majeur ayant un grand impact sur le déploiement des réseaux véhiculaires. En raison de la sensibilité des domaines d'utilisation de ses réseaux, une fausse annonce de trafic aurait des conséquences et des dommages graves sur l'ensemble des véhicules interconnectés (un criminel peut diffuser de fausses notifications à d'autres véhicules afin de bloquer les voitures de police). Ainsi, le mécanisme d'authentification, confidentialité et de sécurité fiable s'avère nécessaire.

- **Volatilité du réseau :** la volatilité du réseau est un autre facteur qui augmente la difficulté de sécurisation des VANET. La connectivité entre les véhicules peut souvent être très transitoire en raison de leur grande mobilité, la connexion peut être intermittente d'où la possibilité de perte de paquets est élevée.

- **Évolutivité :** le système doit gérer des (dizaines de) millions de nœuds, dont certains peuvent rejoignez ou quittez occasionnellement le VANET. De plus, en cas de forte densité de véhicules dans les zones chaque nœud peut être inondé par un grand nombre de messages entrants nécessitant une vérification.

1.3.6.4.3 Les avantages des VANETs

- Contrairement à d'autres réseaux, les nœuds VANET n'ont aucun problème d'énergie.
- Offre une grande mobilité.
- Plus de bande passante.
- Portée supérieure (jusqu'à 600 m).
- Grande fiabilité.

1.3.6.5 Les FANETs

1.3.6.5.1 Définition

Fling **A**d-Hoc **Ne**twork C'est une sous-classe de MANET qui peut être constituée d'une multitude de petits appareils volants sans pilote UAV (Unmanned Aerial Vehicles). Généralement appelés drones. Équipés d'un caméra, capteur et système GPS. Les UAV volent dans le ciel et communiquent les uns avec les autres à l'aide d'un satellite ou d'une station de base et créent ainsi un réseau ad-hoc.

Chaque UAV est conscient des UAV volant à proximité pour éviter les collisions comme le montre la figure 1.9 Ils sont placés sur un même plan ou organisés à différentes altitudes. Les drones sont chargés de surveiller une zone en capturant des images et en les envoyant à une station de base.

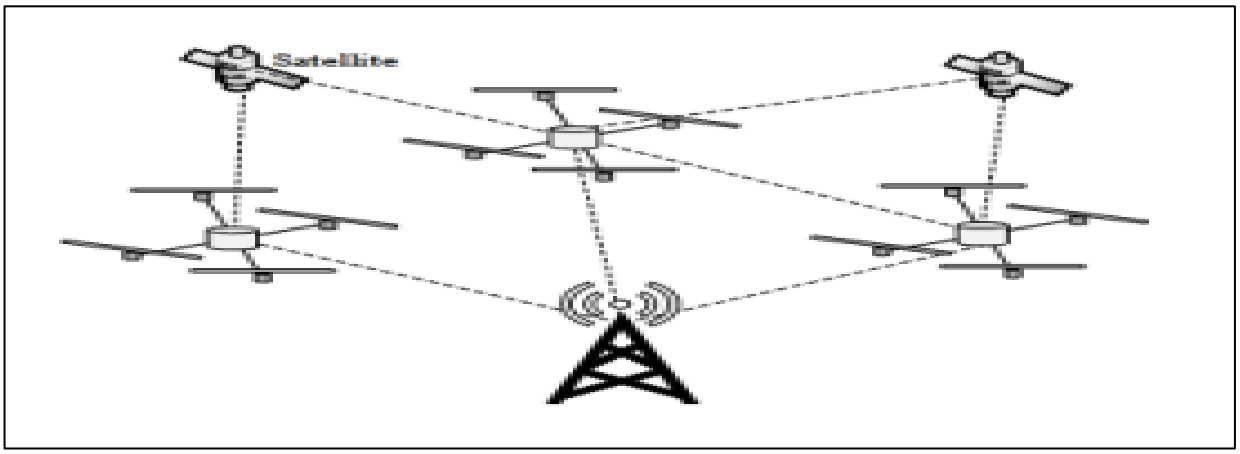


Figure1 9: Les réseaux ad hoc volants (FANET)*(24)*

Cela en fait une technologie très attrayante pour de nombreuses applications civiles et militaires. Les FANETs sont utilisés dans des environnements hostiles pour la surveillance ou l'inspection de sites dangereux ou inconnus, dans les opérations de recherche et de secourismes après une catastrophe naturelle, la détection et la poursuite de cibles militaires, la surveillance de feux de forêts, la télédétection agricole, etc. Ils peuvent être également utilisés pour suivre et filmer des événements spéciaux comme une course de vélos ou un match de football.

1.3.6.5.2 Contraintes et défis du FANETS

Les contraintes des FANET diffèrent de celles des autre réseaux, tels que le réseau mobile ad hoc (MANET) ou le réseau ad hoc pour véhicules (VANET), nous pouvons les résumées, selon (8), comme suit :

- **Faible énergie résiduelle :** Les FANETs nécessitent une attention particulière en ce qui concerne l'économie d'énergie des UAV dont les ressources en énergie sont limitées, les drones sont alimentés par batterie, alors qu'ils ont beaucoup de taches à effectuer tel que le routage, et la transmission des paquets, en prenant en considération la distance relativement longue entre les drones.

- **Position des UAV :** positionner les UAV de la manière la plus appropriée pour surveiller les régions, en minimisant les coûts et en maximisant la performance du réseau.

- **Dynamique élevée dans les FANET :** réduire les effets négatifs de la haute mobilité des drones et des changements de topologie. Cela peut compromettre la communication entre les drones et les performances du réseau.

1.3.6.5.3 Les avantages des FANETs (8)

- Réduction du temps d'accomplissement des missions : les missions peuvent être accomplies plus rapidement selon le nombre des drones utilisés.
- Réduction du coût de maintenance total : au lieu d'utiliser un seul grand UAV
- Coûteux, il vaut mieux d'utiliser plusieurs mini-drones dont le coût de maintenance de chacun est minimal.
- Scalabilité (Passage à l'échelle) : le théâtre des opérations peut être facilement élargi en incorporant tant de drones que nécessaire.
- Réduction de la détectabilité par les radars : c'est une propriété importante pour les applications militaires.

1.3.6.6 Comparaison entre les MANETs, VANETs et FANETs

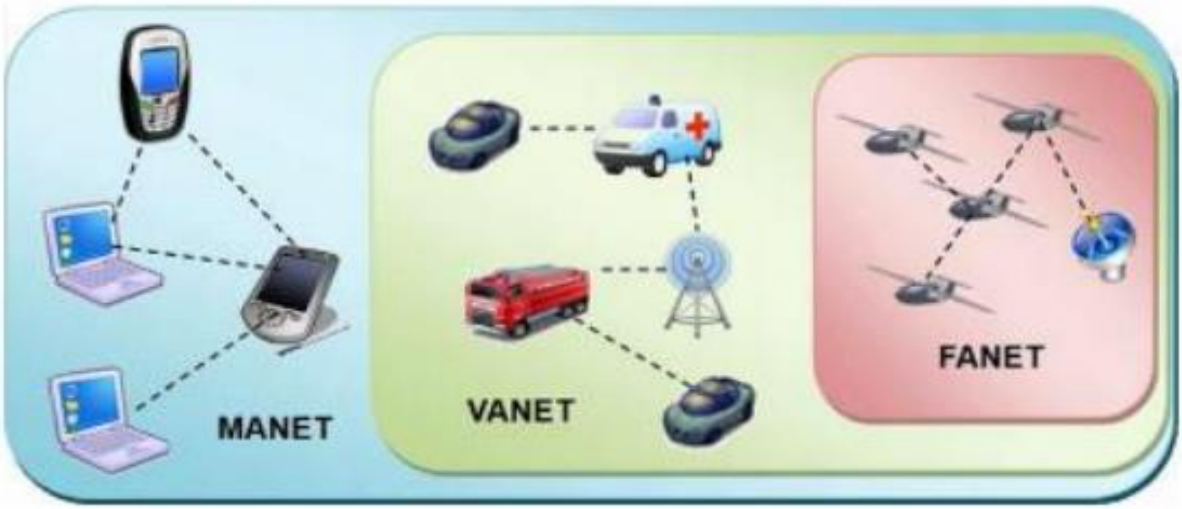


***Figure1 10 : Architecture de MANET,VANET et FANET** (49)*

Malgré la similitude du type de réseau, les réseaux ad hoc diffèrent les uns des autres,

Voici quelques différences qui sont indiqués dans le tableau 1.2:

Paramètres	MANET	VANET	FANET
Densité des nœuds	Forte	Moyenne	Très faible
Modelé de mobilité	Aléatoire	Régulier	Aléatoire
Vitesse de mobilité	Plus faible	Moyenne	Forte
Nature de mobilité	Trieste-Bidimensionnel	Trieste-Bidimensionnel	Espace - Tridimensionnel
Degré de mobilité	Faible	Moyen	Elevé
Contrainte d'énergie	Moyenne	Faible	Élevée
Méthode de localisation	GPS Précision 10 a 5 m	AGPS Précision 10 cm	Unité de mesure inertielle
Propagation radio	NLOS	NLOS dans certains cas	LOS
Changement de topologie	Lent	Rapide	Rapide

Le tableau 1.2 : comparaison entre les déférents types de réseau Adhoc

1.3.5.3 Les RCSF-SM

1.3.6.5.1 Définition

Le réseau de capteurs sous-marins ou UWSN (Under water Wireless Sensor Network) se compose d'un nombre de nœuds capteurs et des véhicules déployés sous l'eau (figure 1.11.) Chaque nœud est capable d'échanger des messages entre les nœuds du réseau, et de relayer des messages vers d'autres nœuds pour atteindre une station de base, Les capteurs sous-marins peuvent mesurer différentes grandeurs telles que la qualité d'eau et étudier ses caractéristiques, la température, la densité, la salinité, l'acidité, les produits chimiques, la conductivité, le pH, l'oxygène, l'hydrogène…

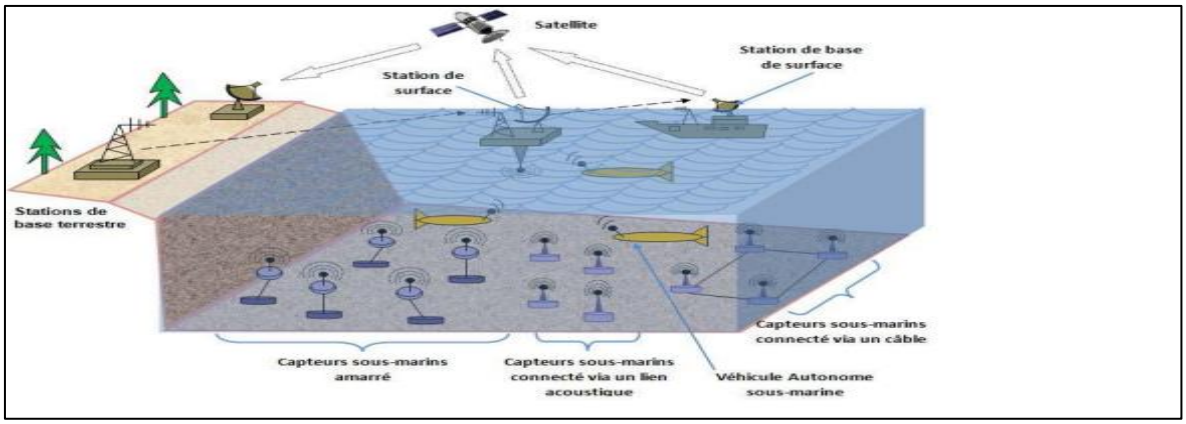


Figure1 11: Le réseau des capteurs sous-marins (11)

1.3.6.5.2 Contraintes et défis du RCSF-SM

L'environnement sous-marin est très différent de l'environnement terrestre et un certain nombre de problème ont été abordés tout en utilisant les réseaux de capteurs comme une technologie efficace pour les systèmes sous-marins nous pouvons les résumées, selon (11), comme suit :

- **Salinité de l'eau :** En raison de l'eau salée très dense, les signaux électromagnétiques et optiques ne peuvent pas être transmis pendant longues distances dans l'océan. Certains des défis de la communication sous-marine sont le délai de propagation, taux d'erreur binaire élevé et bande passante limitée.
- **Consommation d'énergie :** L'objectif principal des protocoles de routage est livraison efficace d'informations entre les nœuds de capteur et le puits. Ainsi, la consommation d'énergie peut être une préoccupation majeure dans la conception du protocole de routage dans les RCSF.

- **Changement d'emplacement :** Les RCSF-SM sont par nature des RCSF mobiles. Lorsqu'il y a des courants d'eau, les capteurs RCSF-SM peuvent se déplacer et souffrir de changements de topologie de réseau dynamique. Il est difficile de faire face aux changements dynamiques des réseaux sous-marins.

- **Capacité de stockage :** Les capteurs doivent avoir des capacités plus importantes pour la mise en cache des données sous-marines.

1.4 La Sécurité dans les réseaux ad hoc

Les réseaux Ad Hoc présentent une technologie pionnière dans le domaine de la communication sans fil. Cependant la sécurité reste dans ce type de réseau un véritable défi. Effectivement, les réseaux ad hoc sont connus pour leur manque d'infrastructure préexistante et d'administration centralisée, ils sont de ce fait considérés comme difficiles à sécuriser. Nous avons déjà signalé que les opérations de gestion de communication dans les réseaux ad hoc sont gérées d'une manière très différente que celles des réseaux traditionnels, il en est de même pour leurs sécurités.

1.4.1 Pourquoi la sécurité est difficile dans les réseaux Ad Hoc ?

Les réseaux Ad Hoc se distinguent par des propriétés et caractéristiques spécifiques qui empêchent les solutions traditionnelles de sécurité d'être directement appliquées. Nous présentons ci-après quelque de ces caractéristiques inhibitrices :

- Les communications sans fil sont intrinsèquement moins sécurisées que leurs homologues filaires. Car Dans les réseaux sans fil, les signaux sont transmis via des médias ouverts et

partagés sans protection, toute personne se trouvant dans la portée de transmission de l'expéditeur peut intercepter le signal de l'expéditeur.

- Les appareils sans fil mobiles ont généralement des ressources limitées, telles que la bande passante, l'espace de stockage, la capacité de traitement et l'énergie.
- La topologie dynamique du réseau aboutit à un changement permanent dans les relations de confiance entre les nœuds. Ainsi, l'implémentation de sécurité basée sur la confiance fait face à de grands défis et les solutions statiques ne s'appliquent pas dans un tel environnement dynamique.
- Les liaisons entre les nœuds ne sont pas garanties, ce qui peut avoir un impact important sur la communication et qui affecte aussi la mise en œuvre de mécanismes de sécurité.
- Exigence de coopération, en raison du manque d'une infrastructure les fonctions de base de gestion du réseau doivent être effectuées d'une façon distribuée par la collaboration d'un ensemble de nœuds ordinaires. Ainsi, l'exécution des opérations de base du réseau peut être fortement affectée par manque malveillant ou accidentel de coopération.

1.4.2 Exigences de sécurité des réseaux ad hoc sans fil

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. Elle regroupe un ensemble de critères s'ils sont remplis dans un réseau nous pouvons le considérer comme sûr.

Ces critères de sécurité sont les suivants :

- **Disponibilité :** Les services fournis par le réseau doivent être toujours disponibles (souvent en temps opportun), malgré tout dysfonctionnement du système. La principale classe d'attaques visant à subvertir cette propriété sont les attaques d'épuisement des ressources. La résistance à de telles attaques revêt donc une importance primordiale.
- **Intégrité :** veut dire que les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.
- **Confidentialité :** seuls les nœuds autorisés peuvent avoir accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché. Les outils cryptographiques sont les typiques, mais pas uniques, aux menaces de confidentialité.
- **Authenticité :** C'est un mécanisme pour sectionner les attaques d'usurpation d'identité pendant la communication. Le nœud expéditeur et le nœud destinataire des messages doivent prouver leur identité à l'aide de mécanisme d'authentification lors du transfert des messages. Cela permet de gérer les droits d'accès aux ressources concernées et maintenir la confiance dans les relations d'échange.

- **Non-répudiation :** elle garantit que l'expéditeur et le destinataire ne peuvent pas renier les messages qu'ils ont envoyés ou reçus. Ainsi, les nœuds compromis envoyant des messages erronés peuvent être identifiée si la non-répudiation est assurée.
- **Anonymat :** L'anonymat assurait la confidentialité des nœuds. Lorsque l'identité du propriétaire d'un nœud n'est pas distribuée par le nœud ou le logiciel système (6).

1.4.3 Vulnérabilités des réseaux ad hoc sans fil

Les vulnérabilités suivantes doivent toujours être gardées à l'esprit lors de la proposition des solutions sécuritaires pour l'environnement ad hoc sans fil :

- **Absence de frontières sécurisées :** contrairement aux réseaux câblés, les attaquants dans un environnement ad hoc sans fil peuvent facilement faire partie du réseau, pour cela il suffit de se trouver dans la portée radio de n'importe quel nœud participant. L'accès direct à la liaison sans fil rend un réseau ad hoc sans fil susceptible de divers types d'attaques, telles que l'écoute passive, l'interférence active et la fuite d'informations secrètes, de falsification de données, de relecture de messages, de contamination de messages et déni de service (6).
- **Initiés malveillants :** le terme d'initiés malveillants fait référence aux nœuds qui ont été compromis pour un comportement malin, il devient très difficile de distinguer un comportement anormal d'une malignité. Le comportement peut être classé en utilisant soit la détection basée sur la signature, soit la détection basée sur les anomalies détectées (6).
- **Pas d'installation de gestion centralisée :** l'administration du réseau devient d'autant plus difficile pour l'environnement ad hoc sans fil, car l'architecture même des réseaux sans-fil est distribué. Cela entraîne des vulnérabilités supplémentaires, comme suit :
  - Surveillance du trafic, des nœuds sans fil et des liaisons variables dans le temps, est très difficile dans un réseau ad-hoc sans fil à grande échelle. Contrairement à un réseau avec serveur central qui peut surveiller facilement l'ensemble de l'environnement réseau.
  - Établir une ligne de défense sécurisée n'est pas possible sans une architecture centralisée. La décentralisation peut être exploitée par des intrus pour lancer des attaques collaboratives qui affectent les performances du réseau. La coopération entre les nœuds devient obligatoire pour exécuter certains protocoles spécifiques qui sont spécialement conçu pour l'environnement de réseau mobile sans fil ad hoc.
- **Contraintes énergétiques :** les nœuds d'un réseau sans fil fonctionnent sur batterie, si la charge de la batterie se vide, il devient obligatoire de la recharger. Cela pose plusieurs problèmes lorsque le nœud est en mouvement. Les problèmes associés à l'énergie limitée des nœuds sans fil sont le déni de service (DoS) et comportement égoïste.

Une attaque DoS peut épuise la charge stockée dans les batteries des nœuds sans fil, ont lançant un travail inutile tel que le routage d'une infinité de paquets factices.

Un autre comportement malveillant, plus facile à réaliser, mais tout aussi néfaste pour le bon fonctionnement du réseau est le comportement dit égoïste d'un nœud (7). Autrement dit, certains nœuds pourraient refuser de router les paquets des autres afin de préserver leurs ressources matérielles.

Évolutivité : L'une des caractéristiques les plus intéressantes des réseaux ad hoc sans fil est l'évolutivité. Cette caractéristique particulière des réseaux ad hoc sans fil a un impact important sur la sécurité, elle peut expose le réseau a des menaces auxquelles. Etant donné que les différents nœuds peuvent rejoindre le réseau à la volée, tous les algorithmes de gestion du réseau, tels que le routage et le contrôle d'accès, doivent également pouvoir s'adapter à ces changements.

1.4.4 Types d'Intrusion dans les réseaux ad hoc sans fil

1.4.4.1 Classement des intrusions (9)

Les intrusions dans les réseaux ad hoc sans fil peuvent être globalement classées en deux catégories différentes

1. **Interne/Externe :** Un attaquant interne est celui qui arrive à contrôler un nœud ayant le statut de membre à part entière du réseau et qui dispose donc de l'ensemble de connaissances associées à ce statut (clés secrètes, table de routage, etc.), Par opposition, un attaquant externe ne dispose pas a priori de ces connaissances. En particulier, il est capable de provoquer des congestions, de falsifier le routage ou bloquer les ressources du réseau...

Il est a noté que les attaques internes sont plus graves que les attaques externes dans la mesure où les premières permettent aux intrus d'utiliser les ressources du réseau avec les mêmes privilèges d'accès qu'un nœud normal.

2. **Actif/Passif :** Un attaquant passif va se restreindre à écouter les flux de communication et essayer uniquement par ces écoutes d'obtenir et stocker des informations qu'il n'est pas supposé connaître ou garder. Un attaquant actif quant à lui pourra supprimer, modifier ou injecter des paquets, et de façon plus générale modifier son comportement de façon arbitraire par rapport au comportement normal dans les différents protocoles dans lesquels il sera engagé. Un tel attaquant pourra ainsi non seulement obtenir plus d'informations qu'un attaquant passif, mais aussi il pourra modifier significativement le fonctionnement d'un protocole ou en empêcher son exécution. Dans un environnement collaboratif comme celui des réseaux ad hoc, un tel attaquant peut en pratique être extrêmement nuisible, en particulier s'il contrôle un ou plusieurs nœuds du réseau.

1.4.4.2 Les principales attaques

Les principaux types d'attaques qui se produisent dans les réseaux ad hoc sans fil sont les suivants :

• **Déni de service (DoS)** : les techniques utilisées par les agents DoS pour bloquer les ressources réseau sont : brouillage de la liaison sans fil et épuisement de la batterie, et par conséquent empêcher le réseau de fournir les services souhaités.

• **Usurpation d'identité** : l'absence de mécanismes d'authentification appropriés peut permettre à des intrus de rejoindre un réseau ad hoc sans fil avec les mêmes droits d'accès qu'un nœud normal. Les services réseau commencent à mal fonctionner lorsque les intrus lancent des attaques spécifiques sur le réseau.

• **Eavesdropping :** ou écoute clandestine, ce type d'attaque tente de déchiffrer des informations confidentielles d'une communication sans fil. Ces informations peuvent inclure des mots de passe et des informations publiques ou privées.

1.5 Conclusion

Nous avons montré dans ce chapitre que les réseaux ad hoc, qui font partie intégrante du sans-fil réseaux, ne nécessitent aucune infrastructure fixe à créer et à organiser. Malgré les progrès fait dans ce domaine, pour atteindre les objectifs de ces réseaux, beaucoup reste à faire.

Les caractéristiques de ces réseaux posent de réels enjeux. Les réseaux ad hoc sont soumis à de nombreuses menaces en raison de leurs vulnérabilités. Les canaux de communication entre n'importe quelle paire des nœuds à l'intérieur d'un réseau ad hoc sans fil doivent être protégés pour éviter les attaques des entités externes.

La cryptographie est un moyen très puissant de faire face à la plupart de ces menaces. Mais à assurer une sécurité digne de ce nom, les systèmes cryptographiques doivent être associés à des gestions des clés. La gestion des clés est l'un des problèmes les plus difficiles dans la conception de réseaux ad hoc, car leurs nœuds sont limités en ressources. Ces sujets seront abordés dans plus de détails dans les chapitres suivants.

Chapitre 2

Chapitre 2.....23
2.1 Introduction.....**23**
2.2 Cryptographie.....**23**
2.2.1 Concepts de base.....**24**
2.2.2 les états et la transition de la clé.....**26**
2.3 Tiers de confiance (TTP).....**31**
2.3.1 Modèle de confiance centralisé.....**31**
2.3.2 PTT dans les systèmes de gestion de clés symétriques.....**32**
2.3.3 Infrastructure à clé publique (PKI).....**33**
2.3.4 Modèle “web-of-trust ".....**34**
2.3.5 Modèle de confiance décentralisé.....**34**
2.4 Gestion des clés.....**34**
2.4.1 Concepts de base de la gestion des clés.....**34**
2.4.2 Classification des clés par type d'algorithme et utilisation prévue.....**37**
2.4.3 Approches de la gestion des clés.....**39**
2.4.4 Phases et fonctions de la gestion des clés.....**42**
2.4.5 États et phases clés de gestion.....**46**
2.5 Conclusion.....**47**

Chapitre 2

Gestion des clés

Ce chapitre examine les concepts de base de la cryptographie, les états clés et les transitions, les classifications des clés par type d'algorithme et l'utilisation prévue. Ensuite, nous présentons les concepts de base de la gestion des clés, l'approches de gestion des clés, le tiers de confiance, la gestion des clés phases et fonctions, et enfin, la combinaison des états clés et des phrases clés.

2.1 Introduction

Les nœuds d'un réseau doivent pouvoir communiquer entre eux en toute sécurité. La nature sans fil et dynamique de l'environnement ad hoc ajoute un nouveau défi à la sécurité réseau, ainsi que l'absence de l'infrastructure le rend plus vulnérable aux attaques de sécurité que les réseaux câblés traditionnels.

L'espionnage, l'insertion de messages, le déni de service et les attaques de décharge de batterie sont inhérents à l'environnement ad hoc et faciles à réaliser. D'autres nœuds agissant comme routeurs et les terminaux de communication ne sont pas forcément fiables.

Les techniques cryptographiques sont essentielles pour protéger les informations de routage et les données. Les clés cryptographiques servent de preuve de confiance pour authentifier les nœuds en tant que membres légitimes du réseau. Ils sont également utilisés pour garantir la confidentialité et l'intégrité.

La gestion efficace des clés cryptographiques est cruciale pour un service réseau fiable surtout pour le succès des réseaux ad hoc sans fil.

2.2 Cryptographie

Cryptographie est l'art de rendre inintelligible, de crypter, et de coder un message pour ceux qui ne sont pas habilités à en prendre connaissance. Le mot cryptographie est un mot d'origine grecque composé de deux parties : "crypto" (krup tos) qui signifie cacher et « graphie » (graphein) qui signifie écrire. La cryptographie est l'étude des techniques mathématiques liées aux aspects de la sécurité de l'information telles que la confidentialité, l'intégrité des données, l'authentification de l'entité et l'authentification de l'origine des données.

2.2.1 Concepts de base

Clé cryptographie : un paramètre constitué d'une séquence de symboles utilisé en conjonction avec un algorithme cryptographie qui détermine son fonctionnement de manière à ce qu'une entité connaissant la clé puisse reproduire, inverser ou vérifier l'opération alors qu'une entité sans connaissance de la clé ne peux pas le faire. La clé cryptographique a pour caractéristiques les éléments suivants :

1. La transformation de données en clair en données chiffrées,

2. La transformation de données chiffrées en données en clair,

3. Le calcul d'une signature numérique à partir de données,

4. La vérification d'une signature numérique sur les données,

5. Le calcul d'un code d'authentification à partir des données,

6. La vérification d'un code d'authentification à partir des données et d'un code d'authentification reçu ou récupéré, et

7. Le calcul d'un secret partagé qui est utilisé pour dériver le matériel de chiffrement.

Cryptage : aussi appelé chiffrement est le processus de transformation du texte en clair en texte chiffré à l'aide d'un algorithme cryptographique et une clé.

Crypter : synonyme de "chiffrer".

Texte en clair : des données intelligibles qui ont du sens et peuvent être comprises sans l'application de décryptage.

Texte chiffré : Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.

Clé symétrique ou clé secrète : Une clé secrète est également appelée clé symétrique c'est-à-dire qu'elle n'est pas publique (la clé est gardée secrète).

L'utilisation du terme "secret" dans ce contexte n'implique pas un niveau de classification, mais implique plutôt le besoin de protéger la clé de la divulgation.

Algorithme cryptographique : est l'ensemble des fonctions (mathématiques ou non) utilisées pour le chiffrement et le déchiffrement.

Algorithme de cryptographie à clé publique (clé asymétrique) : algorithme cryptographique qui utilise deux clés liées : une clé publique et une clé privée. Les deux clés ont la propriété que la détermination de la clé privée à partir de la clé publique est irréalisable par calcul.

Cryptanalyse : Contrairement à la cryptographie, la cryptanalyse est l'art de décrypter des messages sans savoir les clés de déchiffrement. Les méthodes de cryptanalyse sont bien sûr très nombreuses et largement dépendent du type d'algorithme auquel il est confronté.

La cryptanalyse a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.

Cryptologie : La science qui englobe la cryptographie et la cryptanalyse. C'est la science mathématique des messages secrets.

Généralement, la cryptographie consiste en un couple (e, d) d'opérations. La première opération e est cryptage (également appelé chiffrement). Il permet de convertir un texte initial M, dit texte clair, en un autre texte C, dit texte crypté, supposé incompréhensible. La forme C dépend sur un paramètre K appelé clé de chiffrement. La deuxième opération d est le déchiffrement, (aussi appelé décryptage). Le déchiffrement reconstruit le texte en clair à partir du texte chiffré. Cette reconstitution nécessite une deuxième clé, K-1 appelée clé de déchiffrement., dépendante de la clé de chiffrement K.

Système cryptographique : La définition du couple (e, d) constitue un système cryptographique. Il peut être classés en deux types : système cryptographique à clé symétrique et système cryptographique à clé asymétrique (avec clé publique).

2.2.1.1 Cryptographie à clé symétrique

En cryptographie symétrique, aussi appelée cryptographie à clé secrète, une seule et même clé K est utilisée pour le chiffrement et le déchiffrement du message M (voir Figure 2.1)

En général, ce système est utilisé pour assurer la confidentialité des données. Pour cela, chaque interlocuteur qui souhaite communiquer des données confidentielles doit partager une clé secrète avec son partenaire.

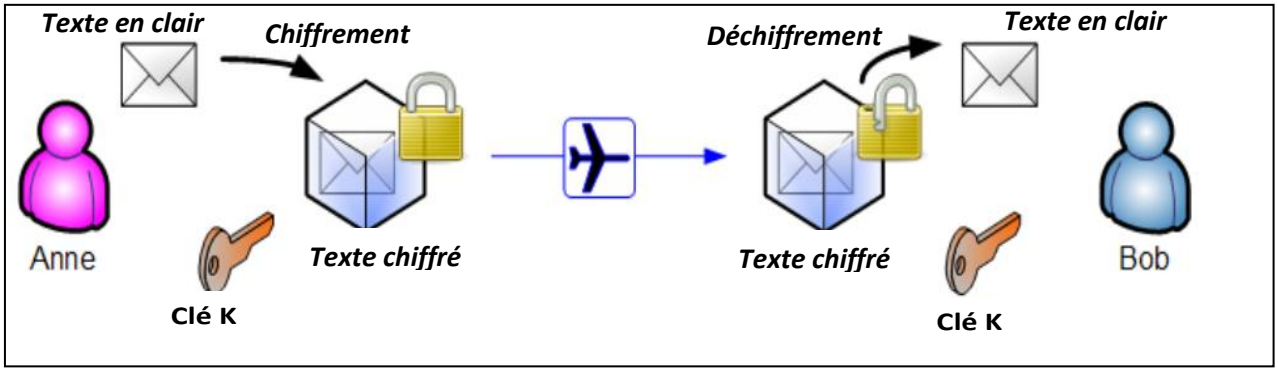


Figure 2 1: Cryptographie symétrique (12)

Cette clé est utilisée par l'expéditeur pour chiffrer le message avant de l'envoyer, et par le destinataire pour décrypter le message reçu.

Ce type de cryptographie a l'avantage d'être rapide car le nombre de clés et les calculs sont réduits. Mais le problème majeur de la cryptographie symétrique reste la distribution de la clé et l'envoi de cette clé unique de chiffrement et de déchiffrement à tous les utilisateurs d'une manière sécurisée.

Des exemples d'algorithmes de chiffrement symétriques incluent DES (Data Encryptions Standards), AES (Advanced Encryption Standards), IDEA, Blowfish et bien d'autres.

2.2.1.2 Cryptographie asymétrique

La cryptographie asymétrique, également appelée cryptographie à clé publique, est un processus utilisant une clé paire (clé privée et clé publique), la clé publique sert à chiffrer les messages à envoyer, et la clé secrète (privée) pour déchiffrer les messages reçus (voir Figure 2.2). La clé privée reste secrète, et la clé publique peut être connue des autres interlocuteurs.

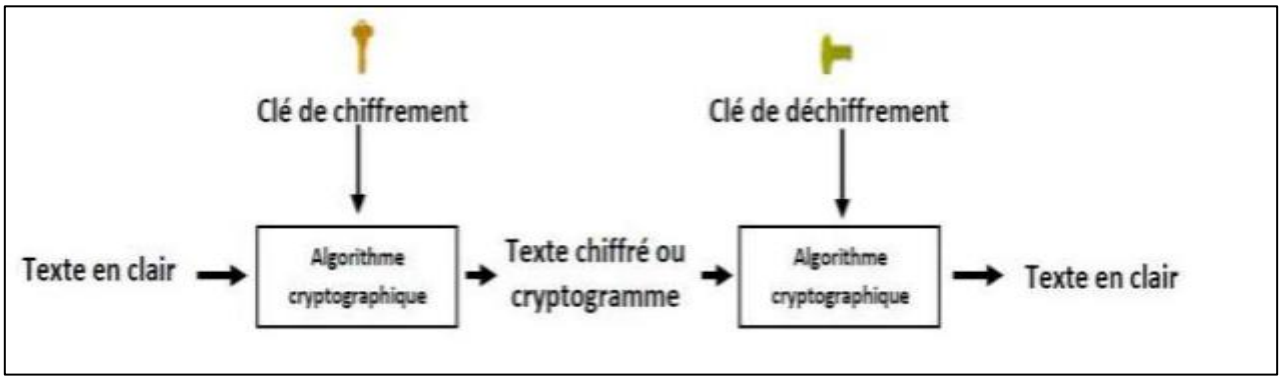


Figure 2 2:Cryptographie symétrique (12)

La cryptographie asymétrique n'est pas seulement utilisée pour assurer la confidentialité, mais aussi pour assurer d'autres propriétés telles que l'authentification, qui repose sur l'utilisation d'un mécanisme cryptographique appelé signature numérique qui prouve l'origine des données. Les algorithmes de cryptographie asymétrique les plus connus est le RSA (Rivest-Shamir-Adleman) nommé par les initiales de ses trois inventeurs il se base sur des concepts mathématiques, ElGamal qui se base sur le problème des logarithmes discrets, ou encore le problème du sac à dos de Merkel-Hellman.

Le principal avantage de la cryptographie asymétrique est de permettre l'échange de données de manière sécurisée. La distribution des clés est beaucoup plus facile car l'échange de clés secrètes n'est plus nécessaire. Chaque utilisateur conserve sa clé secrète sans jamais la divulguer. Seule la clé publique devra être distribuée.

2.2.2 les états et la transition de la clé

Selon son état une clé peut être utilisée différemment durant son cycle de vie. La transition entre les états nécessite souvent l'enregistrement de l'événement. Les endroits

appropriés pour de tels enregistrements sont les journaux d'audit et les métadonnées de la clé. La Figure 2.3 illustre un exemple des états qu'une clé pourrait supposer et les transitions entre eux.

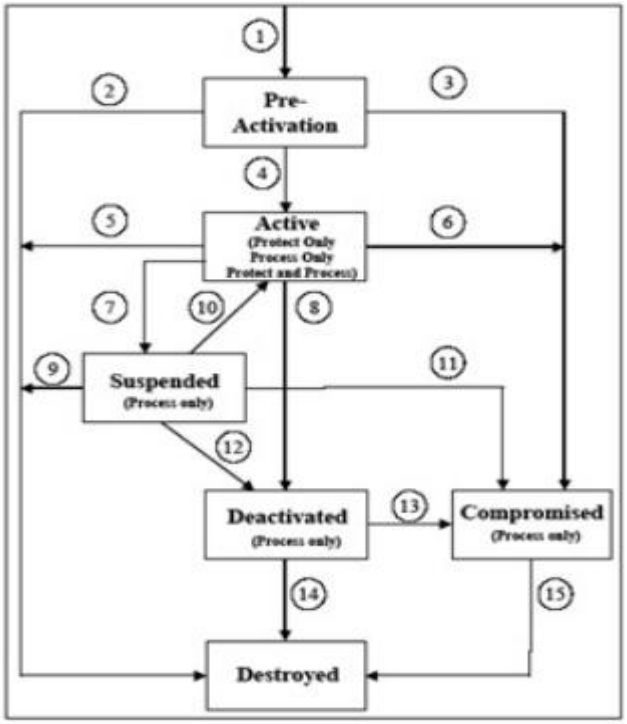


Figure 2 3:Exemple d'état de transmission de clé (45)

2.2.2.1 État de pré-activation (Pre-activation State)

Dans cet état, la clé a été générée mais n'a pas été encore autorisée à être utilisée.

1. Immédiatement après sa génération, la clé entre dans l'état de pré-activation. Toutes les informations sur la génération de la clé doivent être enregistrée.

2. La clé doit passer directement de l'état de pré-activation à l'état détruit, si elle a été jugée comme non essentielle à l'avenir.

3. La clé doit passer de l'état de pré-activation à l'état compromis, lorsque son intégrité et sa confidentialité sont devenu suspectes c'est-à-dire la clé elle-même nécessitant une protection de sa confidentialité.

4. La clés doit passer de l'état de pré-activation à l'état actif si elle deviendra disponible pour l'utilisation. Cette transition peut se produire lorsqu'une date d'activation est atteinte ou peut survenir en raison d'un événement extérieur. Dans le cas où des clés sont générées pour utilisation immédiate, la transition se produit immédiatement après l'entrée dans l'état de pré-activation

Dans le cas des clés asymétriques, les deux clés de la paire de clés doivent avoir le même état dans les transitions.

2.2.2.2 État actif (Active State)

Dans l'état actif, la clé est utilisée pour : protéger les informations de manière cryptographique (générer une signature numérique ou crypter un texte brut), pour les traiter précédemment de manière cryptographique (décrypter un texte chiffré ou vérifier une signature numérique), ou les deux à la foi, la protection et le traitement, selon son genre.

5. Plusieurs types de clés passent directement de l'état actif à l'état détruit dans les cas suivant :

- Si elle n'a pas été déterminée, ou la crypto-période de la clé est atteinte.
- À la fin de leurs périodes d'utilisation respectives par l'expéditeur, les clés de signature privées asymétriques et les clés d'authentification privées passent à l'état détruit, et les clés publiques passent à l'état désactivé à ce moment.
- Une clé symétrique doit passer à l'état détruit lorsqu'elle est remplacée par une nouvelle clé ou lorsqu'elle n'est plus utilisée.
- Les clés symétriques et les clés d'autorisation symétriques doivent passer à l'état détruit à la fin de leurs périodes d'utilisation respectives.
- Les clés d'accord entre les clés éphémères privées asymétriques et les clés publiques correspondantes doivent passer immédiatement à l'état détruit à la fin de leurs utilisations.

6. La clé ou la paire de clés dans le cas de paires de clés asymétriques est révoquée lorsque l'intégrité de la clé symétrique ou la confidentialité de la clé asymétrique nécessitant la protection de la confidentialité devient suspectes. Dans ce cas, une clé symétrique ou la paire de clés asymétrique doit passer de l'état actif à l'état compromis.

7. Une clé symétrique ou une paire de clés doivent passer de l'état actif à l'état suspendu si la clé ou la paire de clés ne devra pas être utilisée pendant un certain temps, par exemple : une clé de signature privée peut être suspendue parce que l'entité associée à la clé est en congé ou si l'on soupçonne que la clé a été compromise .la suspension permet de faire une enquête sur l'état de la clé avant de commencer le processus de révocation ou de remplacement.

8. Le passage de l'état actif à l'état désactivé peut être dû au fait qu'une clé n'est pas assez longue pour être utilisée à la protection cryptographique des données, et la clé symétrique a été remplacée ou elle a atteint la fin de sa période d'utilisation par l'expéditeur.
La transition doit être enregistrée et si la clé ou la paire de clés est connue de plusieurs entités, une notification indiquant la transition et sa raison doit être générée.

2.2.2.3 État suspendu (Suspended State)

Il s'agit d'un état de clé dans lequel l'utilisation d'une clé ou d'une paire de clés peut être suspendue pendant une période, la clé peut être suspendue pour plusieurs raisons possibles si, la clé ou la paire de clés ne doit pas être utilisée pendant un certain temps. Par exemple, une clé de signature privée peut être suspendue car l'entité associée à la clé est en congé ou l'on soupçonne que la clé peut avoir été compromise, dans ce cas, la suspension peut être prononcée pour laisser le temps d'enquêter sur la situation avant d'engager des processus coûteux de révocation et de remplacement.

9. Si aucun compromis n'a été déterminé, plusieurs types de clés passent de l'état de suspension à l'état détruit. Les clés privées de signature et les clés privées d'authentification passent de l'état suspendu à l'état détruit à la fin de leurs périodes d'utilisation par l'expéditeur, tandis que les clés publiques correspondantes passent à l'état désactivé à ce moment-là. (Transition 12).

Les clés d'autorisation symétriques passent de l'état suspendu à l'état détruit à la fin de leurs périodes d'utilisation par l'initiateur.89 Les clés d'autorisation privées doivent passer de l'état suspendu à l'état détruit à la fin de leurs périodes d'utilisation par l'expéditeur. Les clés d'autorisation publique doivent passer à l'état détruit lorsque les clés privées correspondantes sont détruites.

10. Une clé ou une paire de clés passe de l'état suspendu à l'état actif lorsque la raison de la suspension n'existe plus et que la fin de la période d'utilisation de l'expéditeur n'a pas été atteinte. Dans le cas de clés symétriques, la transition doit être effectuée avant la fin de la période d'utilisation de la clé par l'expéditeur. Pour les clés asymétriques, la transition doit être effectuée, par exemple, avant la date " not After " sur le dernier certificat délivré pour la clé publique Clé publique.

11. La clé passe de l'état suspendu à l'état compromis lorsque son intégrité et sa confidentialité nécessitant une protection c'est-à-dire sa confidentialité devienne suspecte. Dans ce cas, la clé ou la paire de clés est révoquée.

12. Si aucun compromis n'a été trouvé et que la suspension n'est plus nécessaire, plusieurs les types de clé passent de l'état suspendu à l'état désactivé.

Les clés d'authentification symétriques**,** les clés symétriques de cryptage/décryptage de données, les clés symétriques d'accord sur les clés**,** et les clés symétriques d'enveloppement passent à l'état désactivé lorsque la fin de la période d'utilisation par l'expéditeur a été atteinte**,** mais que la fin de la période d'utilisation par le destinataire n'a pas été atteinte.

Les clés publiques de vérification de signature**,** les clés publiques d'authentification et les paires de clés statiques privées/publiques91 passent à l'état désactivé à la fin de la période d'utilisation par l'expéditeur de la clé privée (par exemple, lorsque la date "not After" est atteinte sur le dernier certificat émis pour la clé publique). Les clés publiques éphémères d'accord sur les clés et les clés publiques d'autorisation passent à l'état désactivé si elles n'ont pas été détruites lorsque les clés privées correspondante ont été détruites (voir transition d'état 9**).** Une paire de

clés privée/publique passe à l'état désactivé à la fin de la période de cryptage de la paire de clés **(**par exemple, lorsque la date " not After " est atteinte sur le dernier certificat émis pour la clé publique).

Dans le cas des paires de clés asymétriques, les clés publique et privée doivent passer à l'état désactivé en même temps**.** La transition doit être enregistrée**.** Si la clé est connue par plusieurs entités, et un avis de révocation doit être généré.

2.2.2.4 État désactivé (Deactivated State)

Dans cet état, les clés ne sont pas utilisées pour appliquer une protection cryptographique **(**par exemple, chiffrer**)** mais dans certains cas, sont utilisées pour traiter des informations protégées par cryptage (par exemple, déchiffrer).

Les clés à l'état désactivé peuvent passer à l'état compromis ou détruit à un moment donné.

13. Une clé passe de l'état désactivé à l'état compromis lorsque l'intégrité ou la confidentialité d'une clé nécessitant une protection de la confidentialité devient douteuse**.** Dans ce cas, la clé ou la paire de clés est révoquée**.**

14. Les clés privées symétriques (secrètes) et asymétriques à l'état désactivé passent à l'état détruit lorsqu'elles ne sont plus nécessaires (c'est-à-dire lorsqu'elles ne sont plus utilisées) ; **(**par exemple, pour déchiffrer des données**).** Les clés publiques à l'état désactivé passent à l'état détruit dès qu'elles ne sont plus nécessaires. Que les clés publiques soient détruites ou non, les métadonnées doivent être conservées à des fins d'audit.

2.2.2.5 État compromis (Compromised State)

En général, les clés sont compromises lorsqu'elles sont fournies à une entité non autorisée ou déterminées par elle**.** Une clé compromise ne doit pas être utilisée pour appliquer une protection cryptographique à des informations.
Cependant, dans certains cas, une clé symétrique compromise ou une clé publique qui correspond à une clé privée compromise d'une paire de clés peut être utilisée pour traiter des informations cryptographiques**.** Par exemple, une signature peut être vérifiée pour déterminer l'intégrité de données signées si sa signature a été physiquement protégée depuis un moment avant que la compromission ne se produise ou si un horodatage fiable a été inclus dans les données signées**.** Ce traitement doit être effectué uniquement dans des conditions hautement contrôlées**,** où les utilisateurs de l'information sont pleinement conscients des conséquences possibles**.** Ces clés extraites d'une archive peuvent être à l'état compromis.

15. Une clé privée symétrique (secrète) ou asymétrique passe à l'état détruit, et la clé publique doit également passer à l'état détruit lorsque son utilisation n'est plus autorisée ou nécessaire**.** Que les clés publiques soient détruites ou non, les métadonnées doivent être conservées à des fins d'audit**.**

2.2.2.6 État détruit (Destroyed State)

État de la clé vers lequel une clé passe lorsqu'elle est détruite**.** Bien que la clé n'existe plus lorsqu'elle se trouve dans cet état**,** certaines métadonnées **(**par exemple, l'historique des transitions de l'état de la clé, le nom de la clé, son type, et période de cryptage**)** peuvent être conservées à des fins d'audit**.**

La séquence d'états par laquelle le matériel de codage évolue au cours de sa vie est appelée le cycle de vie de la gestion des clés. Les étapes du cycle de vie peuvent comprendre la génération, la pré-activation, l'activation, la récupération et la révocation**.**

2.3 Tiers de confiance (TTP)

2.3.1 Modèle de confiance centralisé

Le TTP est considéré comme une entité de confiance pour le modèle de confiance centralisé**.** Il s'agit d'une entité de confiance de tous les communicants du système (12)**.** En fonction de leurs interactions en temps réel avec d'autres entités**,** les TTPs peuvent être classés en trois catégories : en ligne, en ligne ou hors ligne Voire la figure 2.4

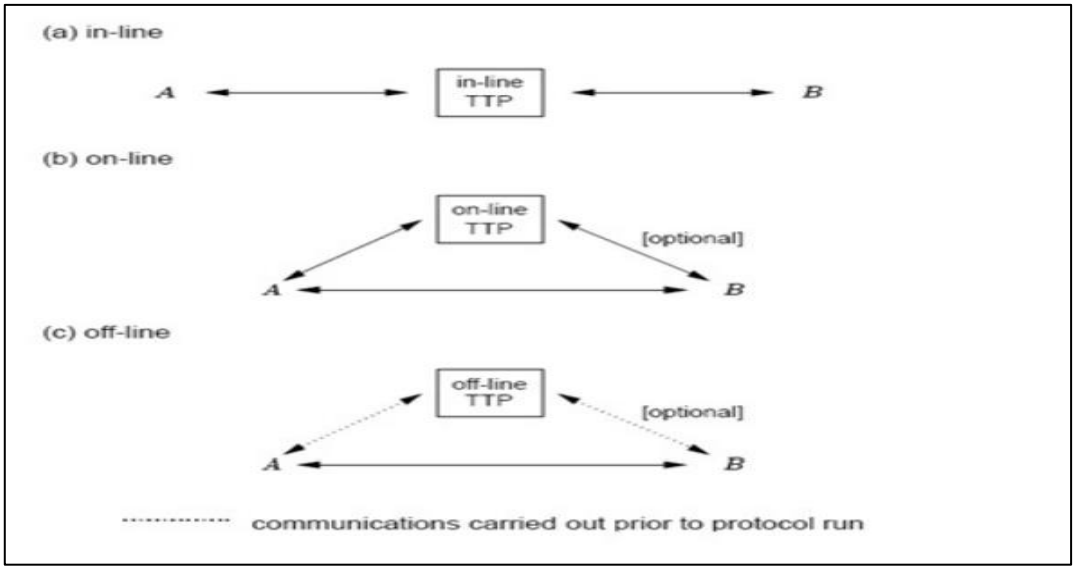


Figure 2 4:Tiers en ligne et hors ligne (13)

1. En la ligne : Le TTP sert de moyen en temps réel et participe activement à la communication de deux utilisateurs A et B.

2. En ligne : Le TTP est impliqué en temps réel et participe activement, mais uniquement à des fins de gestion, car les deux parties communiquent directement entre elles.

3. Hors ligne : Le TTP n'est pas impliqué en temps réel, mais communique avec les utilisateurs apriori et reste hors ligne pendant le fonctionnement du réseau.

2.3.2 PTT dans les systèmes de gestion de clés symétriques

Des PTTs ont été réalisées dans des systèmes de gestion de clés symétriques et asymétriques. Dans les systèmes de gestion de clés publiques, le PTT est l'autorité de certification (AC), et dans les systèmes de gestion de clés cryptographiques symétriques, les PTTs sont les centres de distribution (KDC)et les centres de traduction de clés (KTC). Où se situe le rôle des KDC et KTC dans la simplification de la gestion des clés symétriques puisque chaque utilisateur ne doit pas partager une clé secrète avec tous les autres utilisateurs, il suffit de partager une clé avec le TTP. Cela minimise le nombre total de clés qui doit être géré de n(n-1) /2 à n, où n est le nombre total d'utilisateurs. Le protocole en mettant en œuvre KDC ou KTC est illustré à la figure 2.5.

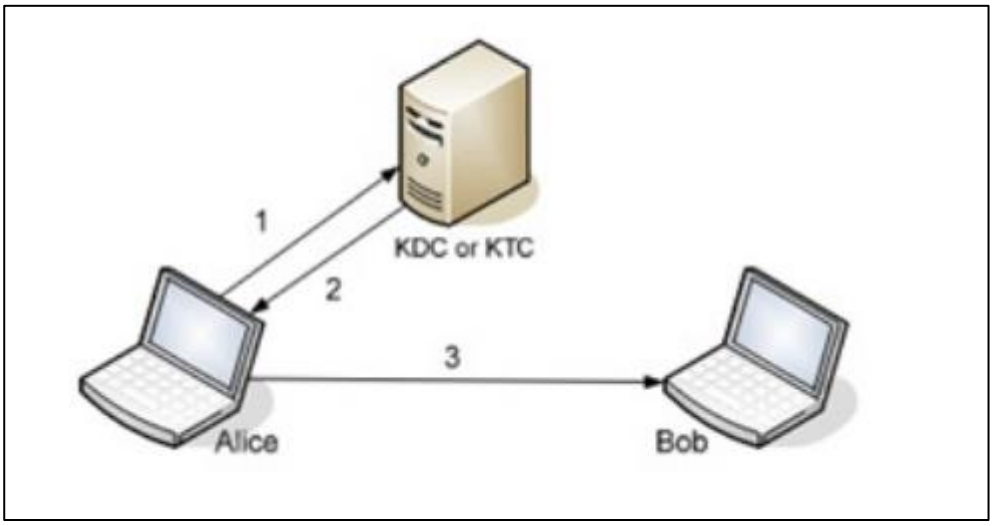


Figure 2 5: Etablissement de la clé de session a l'aide de KTC ou DC (12)

1. Alice demande à partager une clé secrète avec Bob. Le TTP génère (KDC) ou acquiert (Alice la fournit) une clé, la clé secrète partagée entre Alice et le TTP est utilisée pour chiffrer le message.

2. La clé qu'elle a partagée avec Bob est utilisée pour chiffrer la clé de session par le TTP et la retourne à Alice.
3. Alice envoie la clé de session cryptée à Bob, qui peut la décrypter et l'utiliser ensuite pour communiquer en toute sécurité avec Alice.

2.3.3 Infrastructure à clé publique (PKI)

Une infrastructure à clé publique (PKI) fournit les mécanismes nécessaires à la gestion des certificats, car l'utilisation de la cryptographie à clé publique exige que l'authenticité des clés publiques puisse être établie. Un certain cadre de confiance doit être présent pour vérifier la propriété d'une clé publique. Une approche simple exige que deux utilisateurs souhaitant communiquer échangent leurs clés publiques de manière authentifiée, ce qui nécessiterait la distribution initiale de n(n-1) clés publiques. Cependant, si un tiers de confiance délivre des certificats à tous les utilisateurs, seule la clé publique du TTP doit être distribuée à chacun des utilisateurs. Les PKI est constituée des composants illustrés à la figure 2.6. (12).

L'autorité de certification (CA) est le composant responsable de l'émission et de la révocation des certificats, tandis que l'autorité d'enregistrement (RA) est responsable de l'établissement de l'identité du sujet du certificat et de la correspondance entre l'objet et sa clé publique**.** Le site **RA** est un composant facultatif**,** car l'autorité d'enregistrement et l'autorité de certification peuvent être mises en œuvre en tant que composant unique**.**

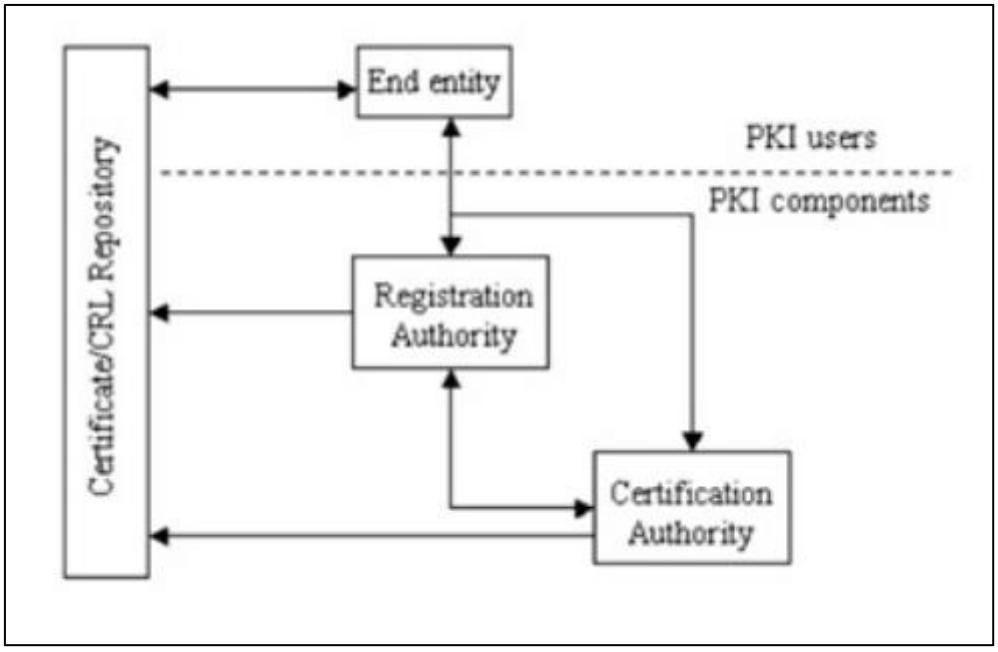


Figure 2 6 : Principaux composant d'une PKI (9)

Les composants de l'PKI fournissent des services de base, tels que l'enregistrement, l'initialisation, la certification, la mise à jour des clés, la révocation, la récupération des clés, la certification croisée, etc.

2.3.4 Modèle “web-of-trust "

Dans le modèle "web-of-trust", il n'existe pas de TTP auquel tous les nœuds du réseau font confiance. D'un autre côté, les nœuds pairs peuvent se délivrer des certificats les uns aux autres et également alimenter le graphe de ce certificat.
L'authentification du certificat peut donc se faire par chaînage de certificats. Pour cela, on parle aussi de chaînage de certificats, chaque nœud joue le même rôle et a la même responsabilité.

Contrairement au modèle de confiance centralisé, dans ce modèle il n'y a pas d'infrastructure lourde, ou de procédures complexes d'amorçage ; mais la confiance globale pour le certificat peut être relativement faible en raison de deux limitations majeures. Premièrement, la demande d'authentification ne peut pas être satisfaite si un graphique de certificat n'est pas suffisamment qualifié pour fournir des chaînes de certificats pour les nœuds pairs donnés.

Deuxièmement, sans TTP, la relation repose sur les comportements corrects et la bonne volonté de tous les nœuds ; nous ne pouvons pas déterminer si une chaîne de certificats inclut des nœuds qui se comportent mal.

2.3.5 Modèle de confiance décentralisé

Dans les réseaux ad hoc, un cadre pour la gestion des clés ne repose pas sur un mode entièrement centralisé, car l'entité centrale devient un point de chute des attaques. Parmi les solutions possibles est de distribuer la confiance centrale à de nombreux nœuds ou à tous les nœuds sur la base d'un schéma de partage de secrets. Dans le schéma de gestion décentralisée de la clé publique, du système est distribuée à tous les nœuds, mais la clé privée du système est divisée en plusieurs morceaux et distribuée à certains (ou tous) les nœuds.

Le sous-ensemble de nœuds du groupe crée une vue d’un AC et fonctionne comme un AC en combinaison (12).

2.4 Gestion des clés

2.4.1 Concepts de base de la gestion des clés

Avant d'aborder en détail le concept de système de gestion des clés cryptographiques, les définitions, les bases, et les concepts essentiels seront d'abord introduits.
Gestion des clés C’est l’ensemble de techniques et de procédures permettant d'établir et de maintenir des relations de clé entre les parties autorisées. La gestion des clés englobe les techniques et les procédures permettant de :

1. L'initialisation des utilisateurs du système dans un domaine ;

2. La génération, la distribution et l'installation de matériel de clé ;

3. Contrôle de l'utilisation du matériel de codage ;

4. Mise à jour, révocation et destruction du matériel de codage ; et

5. Stockage, sauvegarde/récupération et archivage du matériel de codage.

Relation de codage : c'est l'état dans lequel les entités communicantes partagent des données communes (matériel de codage) pour faciliter les techniques cryptographiques. Ces données peuvent comprendre des clés publiques ou secrètes, des valeurs d'initialisation et d'autres paramètres non secrets.

Matériel de clé : comprend une clé cryptographique et d'autres éléments (par exemple, un vecteur d'initialisation ou des paramètres de domaine.) à utiliser pendant l'exécution d'un algorithme cryptographique

Métadonnées : ce sont les informations associées à une clé qui décrivent ses caractéristiques spécifiques, contraintes, utilisations acceptables, propriété, etc. Certaines parties des métadonnées peuvent être secrètes. Les éléments suivants sont des métadonnées typiques :

1. **Étiquette de la clé** : il s'agit d'une chaîne de texte qui fournit un ensemble de descripteurs pour la clé, lisible par l'homme et peut-être par la machine,
2. **Identificateur de clé :** utilisé pour sélectionner une clé spécifique dans une collection de clés. Un identificateur de clé est généralement unique dans un domaine de sécurité.

3. Identificateur du propriétaire : Cet élément spécifie les identifiants des entités qui possèdent la clé.

4. **État du cycle de vie de la clé** (Key Life cycle State).

5. Spécifier le format de clé : Ce format spécifie les séquences dans lesquelles les identifiants d'objets et les structures de clés connexes sont définis sont stockés et le format dans lequel chaque valeur est codée.

6. Produit utilisé pour créer la clé : Cet élément précise quel produit cryptographique a été utilisé pour créer ou générer la clé, la source du matériel de clé (c'est-à-dire l'entité qui a fourni la clé).

7. Algorithme cryptographique utilisant la clé : Cet élément précise l'algorithme cryptographique qui est destiné à utiliser la clé ou l'algorithme à utiliser avec la clé.

8. Schémas ou modes de fonctionnement : Cet élément définit les schémas ou modes d'opération applicables à l'exécution d'une fonction cryptographique à l'aide d'une clé.

9. Paramètres de la clé : Cet élément précise les paramètres, le cas échéant d'une clé.

10. Longueur de la clé : Cet élément spécifie la longueur de la clé en bits (ou en octets).

11. Niveau de sécurité de la paire clé/algorithme : Cet élément est un nombre indiquant la quantité de travail (c'est-à-dire le logarithme de base 2 du nombre d'opérations) qui est nécessaire pour casser (cryptanalyse) l'algorithme cryptographique.

12. Type de clé : Cet élément identifie le type de clé (par exemple, une clé privée de signature, une clé de chiffrement ou une clé maîtresse).

13. Applications appropriées pour la clé : Cet élément précise les applications pour lesquelles la clé peut être utilisée, (par exemple, les achats ou le courrier électronique).

14. Identificateur de la politique de sécurité de la clé : Cet élément identifie la politique de sécurité applicable à la clé, c'est-à-dire un ensemble de contrôles de sécurité utilisés pour protéger la clé ou le type de clé pendant le cycle de vie de la clé, de sa création à sa destruction.

15. Liste de contrôle d'accès aux clés : Une liste de contrôle d'accès identifie les entités qui peuvent accéder et/ou pour utiliser les clés selon les contraintes imposées par les fonctions de gestion des clés et des métadonnées.

16. Compteur d'utilisation des clés : Cet élément indique le nombre de fois que la clé a été utilisée.

17. Clé parent : Cet élément indique la clé à partir de laquelle la clé associée à cette métadonnée est dérivée (identificateur de clé et nature de la relation).

18. Sensibilité de la clé : Cet élément indique la sensibilité ou l'importance de la clé. Il peut s'agir d'un niveau de risque (par exemple, faible, modéré ou élevé) ou d'un niveau de classification (par exemple, confidentiel, secret ou très secret),

19. Protection des clés : Cet élément spécifie les protections d'intégrité, de confidentialité et d'authentification de la source appliquées à la clé.

20. Protection des métadonnées : Cet élément spécifie les mécanismes utilisés pour assurer l'intégrité, la confidentialité et l'authentification à la source des métadonnées associées, en particulier si la clé et les métadonnées sont transmises ou stockées ensemble.

21. Protections de l'association de confiance : Ces informations sont implicitement fournies si la clé et les métadonnées sont protégées en tant qu'un seul élément agrégé à l'aide des protections énumérées au point ci-dessus.

22. Dates et heures : Il existe plusieurs dates-horaires importantes pour les transitions d'état du cycle de vie d'une cle (par exemple, la date de génération, la date d'association, la date d'activation, la date d'activation future, la date de désactivation . . .).

23. Motif de révocation : si une clé est révoquée, cet élément précise le motif de la révocation. Il peut s'agir, par exemple, d'une compromission due au fait qu'un adversaire possède la clé, compromission due au fait qu'un adversaire possède le module cryptographique contenant la clé, perte de la clé, perte du module cryptographique contenant la clé. Le propriétaire de la clé a quitté l'organisation commanditaire, et une mauvaise utilisation de la clé par le propriétaire.

Information sur la clé : information sur une clé particulière qui comprend tout le matériel de chiffrement associé à cette clé et les métadonnées associées.

Clé de chiffrement des données : une clé utilisée pour chiffrer et déchiffrer des données autres que des clés.

Établissement de la clé : une fonction du cycle de vie d'une clé cryptographique ; le processus par lequel les clés cryptographiques sont établies de manière sécurisée entre les entités à l'aide

de méthodes de transport manuelles (par exemple, chargement de clés), des méthodes automatisées (par exemple, des protocoles de transport et/ou d'accord sur les clés), ou une combinaison de méthodes automatisées et manuelles.

Distribution de clés : Le transport d'une clé et d'autres éléments de chiffrement à partir d'une entité qui possède, génère ou acquiert d'une autre manière la clé, à une autre entité destinée à l'utiliser.

Destruction de la clé : Suppression de toutes les traces d'une clé cryptographique afin qu'elle ne puisse pas être récupérée par des moyens physiques ou électroniques.

Clé de dérivation de clé : Une clé utilisée avec une méthode de dérivation de clé pour dériver des clés supplémentaires. Parfois appelée clé maîtresse.

Méthode de dérivation de clé : Une fonction de dérivation de clé ou toute autre procédure approuvée pour dériver des clés.

Système de gestion des clés : Système de gestion des clés cryptographiques et de leurs métadonnées (par exemple, génération, distribution, stockage, sauvegarde, archivage, récupération, utilisation, révocation et destruction). Un système automatisé de gestion des clés peut être utilisé pour superviser, automatiser et sécuriser le processus de gestion des clés.

Crypto période : Période de temps pendant laquelle l'utilisation d'une clé spécifique est autorisée, ou pendant laquelle les clés d'un système ou d'une application donnée peuvent rester en vigueur.

2.4.2 Classification des clés par type d'algorithme et utilisation prévue

La terminologie de clé privée, clé publique et clé secrète (clé symétrique) est utilisée en référence au matériel de codage.

1. **Un système cryptographique symétrique** : c'est un système qui implique deux transformations, une pour l'émetteur et l'autre pour le destinataire, qui utilisent toutes deux la même clé secrète (clé symétrique) ou deux clés facilement calculées l'une à partir de l'autre.

2. **Un système cryptographique asymétrique** : est un système impliquant deux transformations liées, l'une définie par une clé publique (la transformation publique), et l'autre définie par une clé privée (la transformation privée), avec la propriété qu'il est infaisable du point de vue du calcul de déterminer la transformation privée à partir de la transformation publique.

La figure 2.7 montre divers types d'algorithmes couramment utilisés pour atteindre les objectifs cryptographiques spécifiés. Les clés associées à ces algorithmes peuvent être classées en conséquence, dans le but de contrôler l'utilisation des clés. La classification donnée nécessite

la spécification le type d'algorithme (par exemple, chiffrement ou signature) et l'utilisation prévue (par exemple, confidentialité ou authentification d'une entité).

↓ Cryptographic objective (usage)	Algorithm type	
	public-key	symmetric-key
confidentiality†	encryption	encryption
data origin authentication‡	signature	MAC
key agreement	Diffie-Hellman	various methods
entity authentication (by challenge-response protocols)	1. signature 2. decryption 3. customized	1. MAC 2. encryption

†May include data integrity, and includes key transport.
‡Includes data integrity; and in the public-key case, non-repudiation.

Figure 2 7:Types d'algorithmes couramment utilisés pour atteindre des objectifs spécifiques (13).

La gestion des clés symétriques peut être plus ou moins simple selon les applications. Dans les systèmes de chiffrement symétrique, la clé de déchiffrement est facilement obtenue à partir de la clé de chiffrement.
Une durée de vie maximale, appelée crypto période, est également associée à chaque clé. Cette durée de vie peut être représentée par une date limite d'utilisation ou par un compteur du nombre d'utilisations qui ne doit pas dépasser une certaine limite.

Une telle limitation de la durée de vie des clés est généralement destinée à réduire l'effet d'une éventuelle compromission des clés. Il est important de comprendre que dans un système cryptographique bien conçu, il ne devrait pas y avoir de phénomène d'"usure" des clés, limitant leur durée d'utilisation des clés, limitant leur durée d'utilisation.

2.4.2.2 Gestion des clés asymétriques

La gestion des clés en cryptographie asymétrique est à la fois plus simple et plus complexe que dans le cas symétrique Plus simple, mais aussi plus sûre, car il n'est plus nécessaire de partager des secrets avec plusieurs personnes. Parce que dans les systèmes de chiffrement à clé publique, il est infaisable sur le plan informatique (en d'autres termes, pratiquement impossible) de déterminer en d'autres termes, pratiquement impossible) de déterminer la clé de décryptage à partir de la clé de cryptage. Ainsi, la clé privée ne doit être connue que de son seul détenteur et en aucun d'autres personnes. En théorie, il n'est pas nécessaire que ces clés soient générées par un tiers, ce qui pose problème, cependant, réside dans la nécessité d'associer une clé publique à l'identité de son détenteur légitime. Cette certification de la clé publique peut être effectuée par la signature d'un certificat par une autorité, qui certifie ainsi que cette clé est bien celle du détenteur légitime, qui certifie ainsi que cette clé publique appartient bien à cette personne ou à cette entité. Le problème qui se pose alors est celui de la vérification de cette signature, qui

nécessitera à son tour de la connaissance de la clé publique de l'autorité. Afin de certifier cette clé, on peut imaginer qu'une autorité supérieure génère un nouveau certificat, et ainsi de suite.

2.4.3 Approches de la gestion des clés

L'objectif de la gestion des clés est d'établir une clé secrète partagée entre tous les dispositifs participants. Nous allons examiner plusieurs méthodes pour y parvenir.

2.4.3.1 Pré-distribution de clés

Dans la pré-distribution de clés, le système commence par spécifier les dispositifs participant à la communication et distribue des clés à tous ces dispositifs. (14).

2.4.3.2 Transport des clés

Dans les méthodes de transport de clés, la clé est transmise uniquement en cas de besoin. Le dispositif initial génère une clé, qui est ensuite envoyée aux destinataires. En général, la clé envoyée est cryptée à l'aide d'une clé de cryptage partagée (KEK). Dans ces méthodes, les dispositifs doivent connaître la clé KEK et l'infrastructure à clé publique (PKI). Les clés publiques des destinataires peuvent être utilisées pour envoyer la clé. Mais, dans les réseaux ad hoc, l'infrastructure à clé publique ne peut pas être utilisée.

Le protocole à trois passages de Shamir est l'une des méthodes possibles pour le transport des clés à l'aide de la clé de chiffrement (voir la figure 2.8). Il est basé sur des fonctions inversibles f et g qui se commutent, c'est-à-dire que f(g(x)) = g(f(x)).

1. D_1 generates random key K and encrypts it using f with random key x and sends the value to D_2
   $D_1 \rightarrow D_2$: $f_x(K)$
2. D_2 encrypts the received message using g and a random key y and sends the value to D_1
   $D_1 \leftarrow D_2$: $g_y(f_x(K))$
3. D_1 decrypts the received value using f^{-1} and x and sends the value to D_2
   $D_1 \rightarrow D_2$: $f^{-1}(g_y(f_x(K))) = f_x^{-1}(f_x(g_y(K))) = g_y(K)$
4. D_2 decrypts the received value using g^{-1} and y.

Figure 2 8: Protocole à trois passages de Shamir (14).

2.4.3.3 Arbitrage de clé

Dans l'arbitrage des clés, un dispositif est utilisé pour générer et transmettre des clés aux autres. Ce dispositif central doit être accessible à tous les autres nœuds à tout moment, ce qui rend les méthodes d'arbitrage de clés très adaptées aux réseaux câblés et totalement opposées aux réseaux ad-hoc (14).

2.4.3.4 Accord de clé

Un protocole d'accord de clé est un protocole dans lequel deux parties ou plus peuvent se mettre d'accord sur une clé. Un algorithme asymétrique est utilisé pour négocier la clé dans les protocoles d'accord de clé.

Le protocole d'accord de clé Le Diffie-Hellman a été le premier à fournir un accord de clé non authentifié, permettant à un attaquant actif de se faire passer pour un homme du milieu et de participer à l'accord de clé sans que les dispositifs légitimes ne le remarquent. Le protocole est illustré à la figure 2.9.

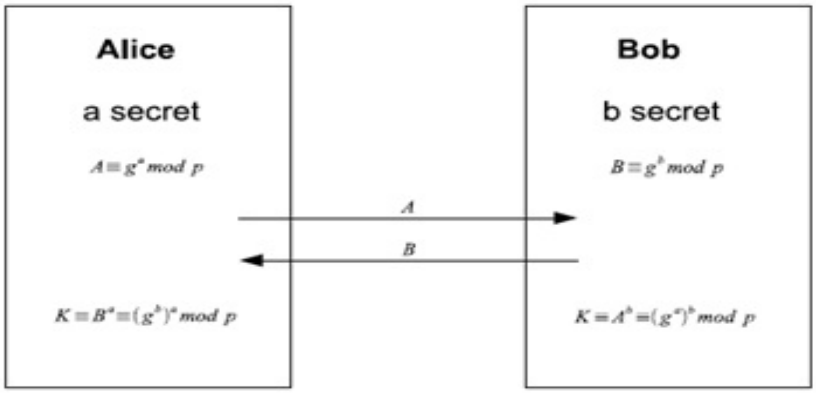


Figure 2 9: Échange de clés Diffie-Hellman (18)

2.4.3.5 Distribution de clés

La distribution de clés n2 : Par exemple dans un système avec n utilisateurs se rapportant à des techniques de clé symétrique et chaque paire doit partager une clé secrète spéciale, Dans ce cas, chaque partie doit avoir n - 1 clés secrètes ; le nombre total de clés dans le système, est alors n(n - 1)/2, soit environ n2. Ce nombre devient très grand chaque fois que la taille d'un système augmente, et il peut doubler parce qu'il peut y avoir une sauvegarde centrale.

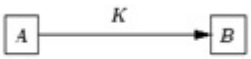
La solution dans ce cas est d'utiliser des serveurs de clés centralisés avec un tiers de confiance au centre ou le moyeu des communications comme une étoile ou une roue à rayons, ce qui résout le problème de la distribution de n2 clés.

Gestion des clés point à point et centralisée : Exemples de modèles de distribution de clés simples (impliquant au plus un tiers) pertinents pour les systèmes à clés symétriques : les communications point à point et la centralisation des gestions des clés, en utilisant des centres de distribution de clés ou des centres de traduction de clés. C'est ce qui est décrit ci-dessous et illustré à la Figure 2.10, où Kxy désigne une clé symétrique partagée par x et y.

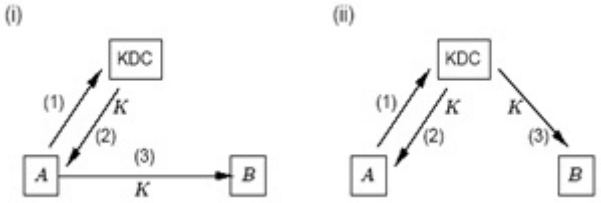
a) **Mécanismes point à point** : Ils impliquent une communication directe entre deux parties.

b) **Centres de distribution de clés (KDC)** : Le KDC est utilisé pour distribuer les clés entre les communicants qui partagent des clés spéciales avec le KD, et non entre eux. Le processus se déroule comme suit : Une demande de partage de clé avec B, le KDC T génère ou acquiert une clé K, après son chiffrement KAT, il l'envoie à A, avec une copie de K chiffrée sous KBT.

(a) Mécanismes point à point



(b) Centres de distribution de clés (KDC)



(c) Les centres de traduction clés (KTC)

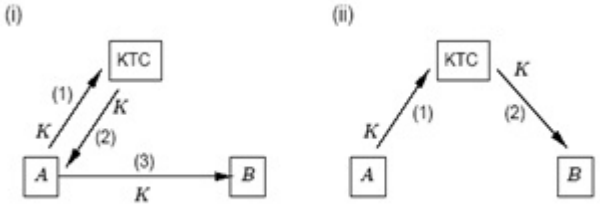


Figure 2 10: Tiers en ligne, en ligne et hors ligne *(22)*

Le principe et les objectifs des KTCs sont similaires à ceux des KDCs , mais ici la clé de session est fournie par l'une des parties (par exemple A) plutôt que par le centre de confiance. Le processus se déroule comme suit : A envoie une clé K au KTC T chiffrée sous KAT, le KTC renvoie K à A (pour le relayer à B) après l'avoir décryptée et réencryptée sous KBT, ou l'envoie directement à B.

Les KDCs et les KTCs sont des techniques centralisées qui font intervenir un serveur de confiance en ligne, dans lesquelles Les KDCs génèrent les clés, mais les KTCs les distribuent (13).

2.4.4 Phases et fonctions de la gestion des clés

Le cycle de vie de la gestion des clés cryptographiques peut être divisé en quatre phases. Pendant chaque phase, les clés se trouvent dans certains états spécifiques, comme nous l'avons déjà vu. En outre, dans chaque phase, certaines fonctions de gestion des clés sont généralement exécutées. Ces fonctions sont nécessaires à la gestion des clés et des métadonnées qui leur sont associées. Les informations relatives à la gestion des clés sont appelées métadonnées. Les métadonnées nécessaires à la gestion des clés peuvent comprendre l'identité d'une personne ou d'un système associé à cette clé ou les types d'informations auxquels cette personne est autorisée à accéder. Les applications utilisent les métadonnées pour sélectionner la ou les clés cryptographiques appropriée(s) pour un service particulier. Bien que les métadonnées n'apparaissent pas dans les algorithmes cryptographiques, elles sont cruciales pour la mise en œuvre des applications et des protocoles d'application.

Les quatre phases de gestion des clés sont les suivantes :

1. **Phase pré-opérationnelle** : Pour les opérations cryptographiques normales, le matériel de clé n'est pas encore disponible. Les clés ne sont peut-être pas encore générées ou sont à l'état de pré-activation. Les attributs du système ou de l'entreprise sont également établis au cours de cette phase.

2. **Phase opérationnelle** : Le matériel de chiffrement est disponible et utilisé normalement. Les clés sont à l'état actif ou suspendu. Les clés à l'état actif peuvent être désignées comme protection uniquement, traitement uniquement, ou à la fois protection et traitement ; les clés à l'état suspendu peuvent être utilisées pour le traitement uniquement.

3. **Phase post-opérationnelle** : Le matériel de codage n'est plus utilisé normalement, mais l'accès au matériel de codage est possible. Mais il est possible d'y accéder et de l'utiliser pour traiter des informations protégées. Les clés sont à l'état désactivé ou compromis. Les clés en phase post-opérationnelle peuvent se trouver dans une archive.

4. Phase de destruction : Les clés ne sont plus disponibles. Les enregistrements de leur existence peuvent avoir été supprimés. Les clés sont dans l'état détruit. Bien que les clés elles-mêmes peuvent avoir été détruites, les métadonnées de la clé (par exemple, le nom de la clé, le type, la crypto période et la période d'utilisation) peuvent être conservées.

Un diagramme de flux pour les phases de gestion des clés est présenté à la Figure 2.11. Sept transitions de phase sont identifiées dans le diagramme. Une clé ne doit pas pouvoir être transférée à une phase précédente.

1. Une clé est dans la phase pré-opérationnelle lors de sa génération (état de pré-activation).

2. Si des clés sont produites mais jamais utilisées, elles peuvent être détruites en passant directement de la phase pré-opérationnelle à la phase de destruction.

3. Lorsqu'une clé en phase pré-opérationnelle est compromise, elle passe à la phase post-opérationnelle (état compromis).

4. Une fois que les métadonnées requises ont été établies, le matériel de clé est généré, et que les métadonnées sont associées à la clé pendant la phase pré-opérationnelle, la clé est prête à être utilisée par les applications et passe à la phase opérationnelle au moment approprié.

5. Lorsqu'une clé en phase opérationnelle est compromise, elle passe à la phase post-opérationnelle (état compromis).

6. Lorsque les clés ne sont plus nécessaires pour une utilisation normale (c'est-à-dire qu'à la fin de la crypto période a été atteinte et la clé n'est plus "active") mais que l'accès à ces clés doit être maintenu, la clé passe à la phase post- opérationnelle.

7. Certaines applications exigent que l'accès soit préservé pendant un certain temps, le matériel de codage peut être détruit. Lorsqu'il est clair qu'une clé en phase post-opérationnelle n'est plus nécessaire, elle peut passer à la phase de destruction.

2.4.4.1 Phases pré-opérationnelles

Pendant la phase pré-opérationnelle de la gestion des clés, le matériel de clé n'est pas encore disponible pour les opérations cryptographiques normales.

1. **Fonction d'enregistrement des entités** : Identification de l'entité qui interagit pour devenir membre autorisé d'un domaine de sécurité, c'est ainsi qu'elle s'inscrit dans un système de gestion de clés.
2. **Fonction d'initialisation du système** : L'initialisation du système implique la configuration ou la mise en place système pour un fonctionnement sécurisé, ce qui peut inclure des préférences d'algorithme, l'identification des parties de confiance, et la définition des politiques de paramètres de domaine et de tout paramètres fiables.

3. **Fonction d'initialisation** : Il s'agit de l'installation ou de l'utilisation des clés initiales qui peuvent être obtenues lors de l'enregistrement de l'entité.

4. **Fonction d'installation du matériel de chiffrement** : Cette fonction est essentielle à la sécurité d'un système ; le matériel de chiffrement est installé pour une utilisation opérationnelle dans le logiciel d'une entité, logiciel, le matériel, le système, l'application, le module cryptographique ou le dispositif d'une entité en utilisant diverses techniques.

5. **Fonction d'établissement des clés** : L'établissement des clés implique la génération et la distribution ou l'accord de matériel de clé pour la communication entre entités.

6. **Fonction d'enregistrement des clés** : L'enregistrement des clés permet de lier le matériel de codage aux l'information associée à une entité particulière.

2.4.4.2 Phase opérationnelle

La récupération des clés consiste à reconstruire le matériel de codage utilisé pendant la période de cryptage d'une clé à partir une archive ou une sauvegarde est souvent stockée pour être accessible en cas de besoin. Le système doit être conçu pour permettre la reconstruction ou la re-dérivation du matériel de codage.

1. **Fonction de stockage opérationnel normal** : L'un des objectifs de la gestion des clés est de faciliter la disponibilité opérationnelle du matériel de codage à des fins cryptographiques standard. Dans le cadre d'une utilisation opérationnelle normale, le matériel de clé est disponible dans le dispositif ou le module en tant que RAM ou dans un support de stockage immédiatement accessible tel que le disque dur local, ou le matériel de clé peut être stockée dans le module cryptographique qui ajoute, vérifie ou supprime la protection cryptographique de l'information.

2. **Fonction de continuité des opérations** : Les clés peuvent être compromises ou perdues et inutilisables en raison d'un dommage matériel, l'utilisateur doit être en mesure de récupérer le matériel de clé à partir d'un stockage de sauvegarde et une nouvelle clé doit être disponible pour remplacer l'ancienne pour assurer la continuité des opérations.

3. **Fonction de changement de clé** : La clé est remplacée par une autre clé au cours de deux processus : le Rekeying si elle est générée d'une manière totalement indépendante de la "valeur" de l'ancienne clé, et la Fonction de mise à jour de la clé si la "valeur" de la nouvelle clé dépend de la valeur de l'ancienne clé.

4. **Méthodes de dérivation des clés** : Les clés cryptographiques peuvent être dérivées d'une valeur secrète avec d'autres informations. Trois cas de dérivation de clés sont couramment utilisés : Deux parties dérivent des clés communes à partir d'un secret partagé commun, des clés dérivées d'une clé de dérivation (clé maîtresse) et des clés dérivées d'un mot de passe.

2.4.4.3 Phase post-opérationnelle

Dans la phase post-opérationnelle, le matériel de codage n'est plus utilisé de manière opérationnelle, mais l'accès au matériel de codage peut encore être possible.

1. **Archives des clés et fonctions de récupération des clés** : Une archive de clés est un dépôt contenant les clés et les informations qui leur sont associées pour une récupération au-delà de la période de cryptage des clés.

2. **Fonction de désenregistrement des entités** : Lorsqu'une entité cesse de faire partie d'un domaine de sécurité, la fonction de désenregistrement des entités supprime les autorisations d'une entité à participer à un domaine de sécurité, ceci afin d'empêcher d'autres entités de s'appuyer sur ou d'utiliser le matériel de clé de l'entité radiée.

3. **Fonction de désenregistrement de la clé** : le matériel de clé doit être désenregistré lorsque le matériel de clé n'est plus nécessaire ou que les informations associées ne sont plus valides.

4. **Fonction de destruction de la clé** : toutes les copies d'une clé privée ou secrète (symétrique) seront détruites dès qu'elles ne seront plus nécessaires., afin de minimiser le risque de compromission.

5. **Fonction de révocation des clés** : La révocation d'une clé est utilisée dans les cas où : l'utilisation autorisée d'une clé doit prendre fin avant la fin de la période de cryptage établie pour cette clé, ou une clé dont la période d'utilisation a expiré a été compromise. Dans les deux cas, une clé cryptographique est révoquée dès que possible après que le besoin de révocation a été déterminé.

2.4.4.4 Phase détruite

La clé n'existe plus. En général, tous les enregistrements de son existence ont été supprimés, sauf dans certains cas, un enregistrement des métadonnées des clés détruites et compromises, à des fins d'audit, c'est-à-dire pour savoir quelles clés sont passées par un cycle de vie normal et quelles clés ont été compromises à un moment donné au cours de leur cycle de vie.

2.4.5 États et phases clés de gestion

Les sous-sections précédentes traitent des fonctions qui sont mises en œuvre dans chaque phase de la gestion des clés. Le système de gestion des clés peut remplir un grand nombre de ces fonctions, mais il ne peut pas avoir toutes les fonctions différentes, car certaines d'entre elles peuvent ne pas être appropriées. Dans certains cas, il peut être combinées une ou plusieurs fonctions, ou les fonctions peuvent être exécutées dans un ordre différent.

Alors que le système peut tolérer les fonctions de la phase post-opérationnelle si les clés sont immédiatement détruites, lorsqu'elles ne sont pas utilisées pour appliquer une protection cryptographique ou sont compromises. Dans ce cas, les clés passent directement de la phase opérationnelle à la phase de destruction.

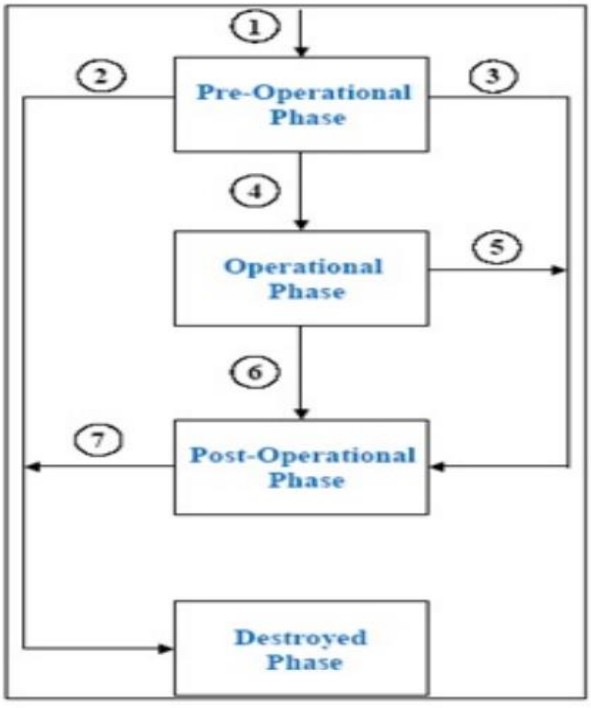


Figure 2 11: Phases et fonctions de la gestion des clés *(4)*

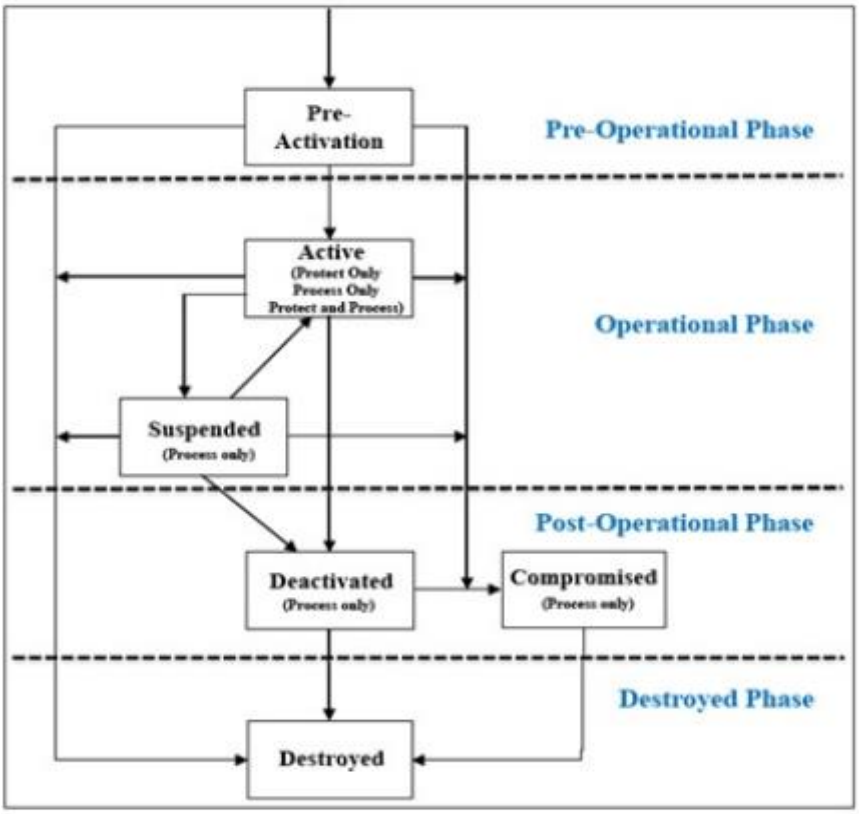


Figure 2 12: Principaux états et phases de gestion de clé *(4)*

2.5 Conclusion

La gestion des clés fournit des mécanismes efficaces, sûrs et stables pour gérer les clés utilisées dans les opérations cryptographiques. Ainsi, la gestion des clés est un service essentiel pour la sécurité de tout système basé sur la communication, car la plupart des attaques visent le niveau de la gestion des clés plutôt que l'algorithme cryptographique lui-même. Est de maintenir les relations de clé et le matériel de clé d'une manière qui contrecarre les menaces pertinentes. En pratique, un objectif supplémentaire est la conformité à une politique de sécurité pertinente. Il s'agit de l'un des aspects les plus difficiles de la mise en place d'un système de sécurité cryptographique. Il s'agit de générer les clés et de les distribuer en toute sécurité aux utilisateurs, ou d'offrir à l'utilisateur un moyen de les générer. Il doit également être en mesure d'enregistrer et de gérer ses clés publiques et privées de manière sécurisée.

Chapitre 3 : Gestion des clés dans les réseaux sans fil ad-hoc

Chapitre 3 48

3.1 Introduction **48**

3.2 Schémas de gestion des clés dans les réseaux WANET **48**

3.2.1 Schémas d'établissement de clés dans les réseaux ad hoc **49**

3.3 Propriétés du système de gestion des clés **52**

3.4 Taxonomies existantes **54**

3.5 Travaux connexes **58**

3.6 Conclusion **60**

Chapitre 3

Gestion des clés dans les réseaux sans fil ad-hoc

Dans ce chapitre, nous présenterons les schémas de gestion des clés dans les réseaux ad hoc sans fil, leurs propriétés et les mesures permettant d'évaluer leur qualité, les taxonomies existantes, et enfin les outils d'évaluation.

3.1 Introduction

La gestion des clés est un service cryptographique de base nécessaire avant de déployer tout autre service de sécurité dans le réseau. Les caractéristiques des réseaux ad hoc sont une arme à double tranchant. Certes, ils permettent une grande facilité de production et de déploiement, mais ils rendent le système de communication global assez " fragile “ pour un certain nombre de défaillances. Pour que cette technologie soit largement déployée, il est nécessaire de surmonter ces problèmes de sécurité à différents niveaux de l'architecture du réseau ad hoc. Sous les contraintes d'un réseau ad hoc, la gestion des clés est l'une des questions les plus difficiles dans la conception des réseaux ad hoc, car leurs nœuds sont limités en ressources, ce qui en fait un terrain fertile pour la recherche.

3.2 Schémas de gestion des clés dans les réseaux WANET

Les systèmes de gestion des clés sont les premiers éléments constitutifs des systèmes de sécurité. En manipulant les matériaux de clé cryptographique de la bonne manière. De nombreux schémas sont proposés, avec différents objectifs et techniques. Leurs propriétés, taxonomies et évaluations ont été déterminées par les développeurs et les chercheurs afin de faciliter la navigation dans ces systèmes.

3.2.1 Schémas d'établissement de clés dans les réseaux ad hoc

Au cours de la dernière décennie, divers schémas ont été proposés pour tous les types de réseaux ad hoc, comme les WSNs, les MANETs et les VANETs. Généralement, deux schémas, la pré-distribution de clés par paire et la pré-distribution de la clé maîtresse, sont considérés comme essentiels dans ce domaine, où chaque nœud partage une clé secrète unique avec tous les autres nœuds (15).

La pré-distribution de clés par paire est la solution parfaite du point de vue de la sécurité, car chaque nœud capturé ne révèle que les clés des liens dont il faisait partie. En raison de ses caractéristiques d'évolutivité et d'insensibilité, pour n nœuds dans le réseau ad hoc, chaque nœud doit stocker n - 1 clés et l'ajout de nouveaux nœuds au réseau nécessite une mise à jour de chaque nœud ou le pré chargement de clés supplémentaires pour les futurs nœuds à venir.

La pré-distribution de la clé maîtresse KMS, du point de vue de l'efficacité**,** est considérée comme la plus basique et la plus parfaite**.** En effet, tous les nœuds partagent une seule et même clé secrète**.** Dans un tel schéma, la mémoire est utilisée avec parcimonie, aucun calcul ou communication n'est nécessaire et l'évolutivité est parfaite. D'un autre côté, si un attaquant capture un nœud, il peut directement lire la clé et ainsi révéler toute communication protégée par cette clé**.**

Pour les besoins de cette étude, nous donnons un aperçu des schémas les plus utilisés et les plus cités.

1. SPINS (16) : proposé en 2001 par Perrig et al, les Protocoles de sécurité pour les réseaux de capteurs utilise 2 blocs de construction sécurisés, qui sont SNEP et µTesla**.** SNEP offre une

confidentialité, l'authentification des données par deux parties et la preuve de la fraîcheur des données**,** tandis que µTESLA fournit une diffusion authentifiée pour les environnements fortement limités en ressources**.** Dans ce schéma**,** la station de base partage une clé par paire avec chaque nœud du réseau avant le déploiement**.** Lorsque deux nœuds ont besoin d'une clé par paire, ils en demandent une à la station de base**.**

2. BROSK (17): proposé par B. Lai et al en 2002. Il est basé sur une seule clé maîtresse à l'échelle du réseau kM qui est préchargée dans tous les nœuds. Après le déploiement**,** les nœuds commencent à diffuser leur identifiant ainsi qu'un nouveau nonce**.** Le nœud A avec l'identifiant IDA**,** le nonce nA diffuse ensuite un message IDA | nA | hkM(IDA | nA), où hkM est une fonction MAC paramétrée par la clé maîtresse kM**.** Après avoir reçu un message similaire du noeud B**,** le noeud A peut calculer une nouvelle clé partagée kAB à partir des deux noeuds**,** par exemple, comme kAB) = hkM(nA |nB**). BROSK** est très évolutif car le temps nécessaire pour terminer **l**a négociation de la clé ne dépend pas du nombre de nœuds de capteurs**,** et économise de l'énergie en réduisant le nombre de transmissions**.** D'autre part, la clé principale sera stockée pendant toute la durée de vie du réseau et donc le schéma reste vulnérable à l'attaque de capture de nœud**.**

3. EG (22)**:** Eschenauer et Gligor ont proposé en 2002 la pré-distribution de clés aléatoires**.** Le

Principe de base est de générer un grand pool de P clés**, de tirer** aléatoirement k clés et de les charger comme porte-clés à chaque nœud indépendamment**.** Après le déploiement, les nœuds

diffusent les identifiants des clés stockées et établissent des clés partagées**,** soit en tant que clé partagée unique, soit en calculant une nouvelle clé partagée à partir **de** toutes les clés partagées**.** Ensuite, et pour augmenter la capture de nœuds la résilience de ce schéma**.** Chan et al (9)en 2003, ont proposé le schéma q-composite, en exigeant que q > 1 clés communes soient partagées au lieu d'une seule.

4. DKPS (13)**:** Aldar C-E Chan a introduit un schéma de gestion de clés symétriques distribuées **pour** les réseaux mobiles ad hoc en 2004**,** le Distributed Key Pre-distribution Scheme (DKPS**).**

Il est basé sur trois phases principales. Premièrement, la sélection de clé distribuée (DKS) dans **c**ette phase chaque nœud utilise la propriété d'exclusion pour obtenir la clé aléatoire de l'ensemble universel**,** L'évaluation de la propriété d'exclusion dépend du concept de famille sans couverture (CFF**).**et utilise la méthode probabiliste pour faire la CFF de manière distribuée**,** ce qui supprime le besoin de TTP (tiers de confiance) et rend le MANET plus dynamique, deuxième Découverte sécurisée de clés partagées (SSD) : il s'agit de la deuxième phase de DKPS, dans laquelle chaque nœud ayant une clé partagée avec un autre nœud est en mesure d'accéder à la clé. Cette étape est importante car l'écoute clandestine peut se produire dans la phase DKS. Enfin, le test de propriété d'exclusion de clé (KEPT), dans la dernière phase, une matrice d'incidence est utilisée pour présenter la relation entre les clés des nœuds mobiles et les clés partagées. Elle utilise des valeurs binaires pour construire la matrice. DKPS nécessite moins de stockage que l'approche d'accord de clé par paire. Ce schéma est plus efficace par rapport à l'accord de clé de groupe. De plus, il minimise les exigences sur les réseaux sous-jacents et peut être facilement appliqué aux scénarios de réseaux ad hoc.

5. **GicheolWang et al** (18) ont proposé en 2005 un schéma d'établissement de clés par paire sans distribution préalable de clés pour les réseaux ad hoc. Ce schéma est basé sur le protocole d'échange de clés Diffie-Hellman, et pour empêcher la falsification des valeurs Diffie-Hellman, il utilise uniquement le mot de passe à usage unique. De plus, pour fournir une authentification mutuelle, il oblige chaque nœud à prouver la propriété de sa clé secrète à long terme. Il peut réduire le nombre de messages à échanger par rapport au schéma de pré-distribution probabiliste des clés.

6. **PIKE** (7): Chan et Perrig ont introduit un schéma d'accord de clé symétrique pour les capteurs en 2005, afin de résoudre les problèmes d'extensibilité et de point de défaillance unique de SPINS. Pair

Intermédiaires pour l'établissement de clés (PIKE), ce modèle utilise le concept de pré-distribution aléatoire de clés. L'idée de base de leur approche est que chaque nœud partage une clé unique avec un ensemble de nœuds en 2 dimensions (horizontale et verticale et peut être étendue à 3 dimensions). Par conséquent, toute paire de nœuds peut compter sur au moins un nœud intermédiaire pour établir la clé commune. Dans un MANET, chaque paire de nœuds mobiles partage une clé secrète commune avec au moins un ou plusieurs intermédiaires. Les caractéristiques de ce modèle sont de bons services de sécurité et une évolutivité à échelle équitable.

7. **Richard Yu et al** (19) ont proposé en 2010 un schéma de gestion des clés hiérarchique basé sur l'identité dans les réseaux mobiles ad hoc tactiques. Les auteurs ont présenté une technique de gestion des clés dans un réseau hiérarchique distribué, dans lequel les nœuds peuvent obtenir leurs clés soit à partir d'un seuil de frères et sœurs, soit à partir de leur parent. La technique de sélection

dynamique des nœuds est formulée comme un problème stochastique. Les meilleurs nœuds à utiliser en tenant compte de leurs conditions de sécurité et de leurs états énergétiques.

8. SCKD (10) **:** Daeinabi et al ont suggéré un schéma pour VANETs en 2014, basé sur le clustering et la distribution de clé (SCKD)entre les nœuds et les têtes de cluster dans les VANET. Ce site

permet de réduire le coût et le temps de calcul de la génération et de la distribution des clés.

L'algorithme appliqué a utilisé la surveillance des véhicules malveillants (MMVs) pour isoler

véhicule malveillant. Les exigences de sécurité, telles que l'authentification, la non-répudiation, les données, etc. inteschenauer2002keyrity et la capacité de forgeage sont satisfaites dans ce schéma.

9. LDGKA (20) **:** Wang et al ont proposé le schéma d'accord de clé de groupe distribué en fonction de l'emplacement (LDGKA) pour les VANET en 2014. Ce protocole gère les entrées et sorties de groupe dynamiques. La reconstruction d'une dérivation à sens unique nécessite seulement O(log(n)) opérations,réduisant le surcoût de communication associé à la distribution de nouvelles clés aux véhicules membres. Il n'y a pas d'autorité centrale, il n'y a donc pas de point de défaillance unique ou de goulot d'étranglement.

10. Kumar et al (21)**:** les auteurs ont proposé en 2015, une infrastructure de clé publique décentralisée (PKI) pour VANETs. L'algorithme utilisé pour préserver la confidentialité et l'intégrité des messages utilise les concepts de Bayesian Coalition Game (BCG) et d'automates d'apprentissage (LA). Les automates d'apprentissage sont diffusés sur chaque véhicule, et à l'aide de certificats qui leur sont distribués par une autorité de certification, ils peuvent échanger des informations et coopérer entre eux, formant ainsi une coalition dynamique à l'aide d'un chiffrement à clé symétrique et d'une authentification des messages par hachage.Les certificats des nœuds qui se comportent mal seront révoqués.

11. Shuaiqi Hu et al (27): a proposé en 2015, un schéma de gestion de clé hiérarchique pour les réseaux de capteurs sans fil en utilisant le chiffrement basé sur l'identité. et les méthodes de base Boneh-Franklin et l'algorithme Diffie-Hellman (DH) pour résoudre la grande consommation d'énergie dans la communication et le calcul.

12. Zahid et al (28): ont proposé, en 2017, un schéma de gestion efficace des clés (EKM) pour les scénarios basés sur la communication multipartite. Pour résoudre le problème des valeurs polynomiales dans les schémas d'établissement de clés basés sur la distribution polynomiale, qui entraînent soit un stockage intensif, soit des opérations infaisables lorsque de grandes valeurs sont multipliées. Réduire le calcul et le coût lorsque ces polynômes sont régénérés de manière dynamique à chaque fois qu'un nœud se joint ou se retire, et à chaque fois que la clé est rafraîchie dans le schéma Emu le protocole de gestion des clés de session proposé est établi en appliquant un polynôme symétrique aux membres du groupe., et la tête du groupe agit comme un nœud responsable. La méthode de génération du polynôme utilise des justificatifs de sécurité et une fonction de hachage sécurisée. Les paramètres cryptographiques symétriques sont efficaces en termes de calcul, de communication et stockage requis.

13. Md Samsul et al (29) ont proposé en 2018, une structure hiérarchique pour la distribution des clés et le partage d'informations pour assurer la confidentialité et augmenter la sécurité globale des

véhicules aériens sans pilote (UAV). Ce schéma offre une flexibilité au réseau en permettant aux nœuds de servir alternativement de têtes de cluster. Les nœuds de grappe ordinaires utilisent le chiffrement basé sur l'identité (IBE) pour créer la confiance et négocier les clés avec la tête de cluster. Les schémas de gestion des clés sont un élément de base de tout système de gestion des clés sûr, robuste et efficace.

3.3 Propriétés du système de gestion des clés

Comme pour tout système, nous pouvons évaluer la qualité d'un schéma de gestion des clés en évaluant ses propriétés. Ses propriétés. Selon (30), nous pouvons identifier les exigences et les mesures suivantes pour les solutions de gestion des clés dans les réseaux ad hoc sans fil (WANET), classées en trois groupes **:**

- ***Métriques de sécurité***

  - **Authentification du nœud** : Une caractéristique d'un KMS permettant la vérification des nœuds entre eux.

  - **Résilience :** Cette propriété exprime l'impact qu'un attaquant aurait sur le réseau en capturant un nœud ou un ensemble de nœuds. Comme les nœuds ad hoc sans fil sont considérés comme physiquement peu sûrs, un attaquant qui capture un nœud peut facilement accéder à toutes ses données confidentielles**.** En capturant un nœud avec un bon KMS, seuls les liens de ce nœud qui sont concernés devraient être compromis**.**

  - **Révocation des nœuds :** Fonctionnalité d'un KMS permettant la révocation des clés et des nœuds compromis ou périmés et des nœuds du réseau.

- ***Mesures d'efficacité***

  - **Mémoire :** D'après les spécifications techniques de la plupart des types de nœuds ad-hoc sans fil, leur mémoire est considérablement limitée**.** Ainsi, il est souvent important de minimiser la quantité de données stockées ainsi que le code d'infrastructure réel, également stocké dans la mémoire.

  - **Vitesse de traitement :** les microcontrôleurs les plus couramment utilisés fonctionnent à des fréquences si basses que l'exécution d'une opération exigeante en termes de calcul.

  - **Bande passante** : les frais généraux de communication sont l'un des principaux points d'intérêt des protocoles ad hoc sans fil actuels. La latence de la transmission des informations et la consommation la consommation d'énergie sont considérablement affectées par des messages plus longs et plus fréquents. La transmission et la réception des messages constituent le principal facteur de consommation d'énergie des nœuds. Le meilleur KMS pour les réseaux ad hoc sans

fil devrait transmettre autant de messages que possible. L'idéal est qu'il soit préchargé avec tous les secrets partagés et qu'il n'y ait aucun besoin de communication supplémentaire. Par conséquent, l'exécution de calcul sur microcontrôleur peut réduire la durée de vie du nœud.

- **L'énergie :** L'énergie est l'une des propriétés les plus souvent limitées de la plupart des types de réseaux ad hoc sans fil est la restriction de l'énergie**.** La propriété énergétique décrit combien d'énergie est nécessaire à un KMS pour établir des secrets partagés**.** Le KMS choisi doit effectuer le moins de calculs et transmettre le moins de données possible afin de préserver la quantité maximale d'énergie sur le nœud**.** Cette propriété peut également être considérée comme une bande passante et une vitesse de traitement communes.

- **Connectivité de la clé** : caractéristique d'un KMS décrivant la capacité de deux nœuds (sommets) d'établir un secret partagé (une connexion). Des propriétés de connectivité plus spécialisées sont **:**

  - **Connectivité locale :** Décrit la probabilité de deux nœuds voisins quelconques partagent un secret.
  - **Connectivité globale :** Décrit la probabilité qu'un chemin sécurisé entre n'importe quels deux nœuds soit établi**.**
  - **Connectivité des nœuds** : Décrit la probabilité pour que deux nœuds quelconques du réseau partagent un secret.

- ***Métriques de flexibilité***

- **Manque de connaissances préalables sur le déploiement :** Les solutions plus flexibles ne tirent pas avantage des connaissances préalables sur le déploiement**.** Cependant, d'un autre côté, les KMS utilisant de telles connaissances peuvent être plus efficaces, principalement en ce qui concerne les mesures d'efficacité**.**

- **Évolutivité** : Un réseau ad hoc peut être d'une taille arbitraire. Cette propriété exprime le nombre de ressources (matériel de clé, temps de calcul, communication, **. . .** etc) sont nécessaires pour un nœud ou pour l'ensemble du réseau en fonction de la taille du réseau.

Dans (19), bien que la propriété d'extensibilité soit englobée dans la propriété d'extensibilité, et la propriété de latence dans la propriété de vitesse de traitement, il a préféré les inclure en tant que deux propriétés de base, la mise à jour principale étant souvent discutée.

L'auteur énumère ces trois propriétés :

- **Extensibilité :** c'est la capacité d'établir des clés avec un nombre arbitraire de nouveaux nœuds et d'établir des secrets partagés pendant sa durée de vie**,** tandis que l'extensibilité est la capacité de faire face à un grand nombre de nœuds dans le réseau.

- **Latence** : la latence décrit le temps requis par l'ensemble du réseau pour terminer la phase d'initialisation. Cette valeur est de 0s lorsqu'aucune phase d'initialisation n'est

nécessaire**.** Alors que la vitesse de traitement décrit le temps nécessaire pour terminer le calcul, soit sur le site de pré-calcul, soit sur un seul nœud.

- **Mise à jour des clés :** décrit la fréquence et les coûts, en termes de communication et de calcul, de l'opération de mise à jour des clés sur un seul nœud et sur l'ensemble du réseau.

Enfin, pour choisir un schéma de gestion des clés adapté aux exigences du scénario de réseau ad hoc sans fil**,** la proposition de gestion des clés doit être évaluée en fonction des toutes les propriétés susmentionnées.

3.4 Taxonomies existantes

De nombreuses taxonomies pour les KMSs ont été présentées. Elles peuvent être classées de plusieurs façons ; de nombreuses propositions dépendent du point de vue, ce qui rend difficile la granularité et le recouvrement des classes.

Dans (31), l'auteur a proposé deux taxonomies. La première est basée sur la structure du réseau, et la seconde est basée sur la probabilité de partage de clés. Pour ceux basés sur la structure du réseau, les auteurs divisent les systèmes en systèmes à clé centralisée et systèmes à clé distribuée. Dans les schémas centralisés les tâches de génération et de distribution des clés sont accomplies par une seule entité appelée centre de distribution de clés (KDC). L'approche basée sur la probabilité de partage des clés différencie les systèmes de clés probabilistes des systèmes de clés déterministes.

Cependant, certains proposent une catégorie mixte. Sa taxonomie est présentée comme suit :

- Structure de réseau :

  - Schéma de clé centralisé,
  - Schéma de clé distribué.

- Probabilité de partage des clés :

  - Schéma de clé probabiliste,
  - Schéma de clé déterministe.

L'auteur de (32) a proposé deux taxonomies. La première est basée sur le mécanisme d'établissement de la clé, qui est fortement orienté vers la cryptographie à clé symétrique et néglige les schémas basés sur la cryptographie à clé publique. La seconde, basée sur le modèle de l'attaquant, définit quatre modèles d'attaquants et font correspondre les classes de mécanismes d'établissement de clés précédemment définies au modèle d'attaquant le plus fort pour lequel ils sont encore sûrs.

- Basé sur le mécanisme d'établissement des clés :

  - Pré-distribution de clés par paires.
  - Pré-distribution basée sur la clé principale.

- Participation de la station de base.
- Pré-distribution probabiliste des clés.
- Pas de pré-distribution de clés.

➡ Basé sur le modèle d'attaquant

➡ Modèle de l'attaquant 1

∗ Après l'établissement de la clé, l'attaquant peut surveiller la communication mais ne peut lancer aucune attaque pendant la durée de vie du réseau.

➡ Modèle d'attaquant 2

∗ Lors de la configuration de la clé, la surveillance par un adversaire est un scénario rare. Après la configuration de la clé, des attaques actives telles que la capture de nœud peut se produire.

∗ Sous ce modèle d'attaquant, le schéma d'infection en tant que "Pas de pré-distribution de clé" est considéré comme sécurisé.

➡ Modèle d'attaquant 3

∗ Juste après le déploiement, la surveillance de la communication est possible, mais des attaques actives ne peuvent apparaître qu'après la configuration des clés.

∗ Selon ce modèle, le protocole LEAP est représentatif des schémas sécurisés.

➡ Modèle d'attaquant 4 :

∗ Dès le déploiement des nœuds, l'écoute et les attaques actives sont toutes deux possibles.

∗ Les schémas de pré-distribution de clés par paires, ainsi que la participation de la station de base le protocole SPINS, sont jugés parfaitement sûrs et appropriés pour cette classe. De plus, les schémas probabilistes de pré-distribution de clés, tels que EG, offrent une grande résistance élevée à la capture de nœuds à ce niveau.

Dans (33), les auteurs présentent une étude des schémas de gestion des clés existants et les classent selon le type de mécanisme de clé de chiffrement utilisé dans le schéma. En outre, chaque classe est divisée en sous-classes basées sur le mécanisme de pré-distribution et d'établissement.

Les principales classes sont les suivantes :

➡ Les schémas de gestion de clés symétriques.

➡ Schémas de gestion de clés asymétriques.

➡ Schémas hybrides.

Cette division concerne tous les types de réseaux ad hoc sans fil. Pour améliorer la granularité de la taxonomie, la première classe est divisée en huit sous-classes et la seconde en trois sous-

classes. Les noms de chaque classe illustrent l'approche de l'établissement de clés et indiquent certaines caractéristiques du système, telles que des coûts de calcul et de mémoire plus élevés.

Les schémas de gestion des clés symétriques nécessitent un faible coût de traitement et une petite quantité de mémoire nécessaire au stockage des clés. Pour ces raisons, ils sont très répandus dans la littérature.

Dans (33), les premières sous-classes sont :

- Les schémas basés sur les entités ou arbitrés :
  - Schéma de pré-distribution basé sur la clé maîtresse,
  - Schéma de participation de la station de base,
  - Schéma basé sur un troisième nœud de confiance.
- Schéma de pré-distribution de clés par paires.
- Schémas de pré-distribution de clés purement probabilistes.
- Schémas de pré-distribution de clés à base polynomiale.
- Schémas de pré-distribution de clés basés sur des matrices.
- Schémas de pré-distribution de clés basés sur des arbres :
  - Schémas de pré-distribution de clés basés sur des arbres en étoile,
  - Schémas de pré-distribution de clés basés sur des arbres logiques.
- Schémas de pré-distribution de clés basés sur la conception combinatoire.
- Schémas de pré-distribution de clés basés sur un système de base d'exclusion.

Les secondes sous-classes sont :

- Système de cryptage asymétrique basé sur RSA,
- Système de cryptage asymétrique basé sur ECC,
- Schémas d'accord de clé basée sur l'ID.

Dans un travail similaire (34), l'auteur a proposé la taxonomie suivante :

- Schémas de gestion des clés symétriques :
  - Schéma de pré-distribution des clés,
  - Schéma d'accord de clé.
- Schémas de gestion de clés asymétriques :
  - PKI basée sur les certificats,
  - Schémas PKI basés sur l'ID,

- Schémas PKI sans certificat.

- Schéma hybride.

Dans (35), après avoir analysé les études précédentes, les auteurs ont proposé une taxonomie des protocoles KMS en quatre catégories comme suit :

- **Cadre de pool de clés :** comprend les protocoles KMS basés sur l'idée d'un pool de clés global, comme dans le schéma EG.

- **Cadre mathématique :** comprend les conceptions polynomiales, matricielles et combinatoires.

- **Cadre de négociation :** comprend des approches telles que l'infection de la clé**.**

- **Cadre de la clé publique.**

Dans (6), l'auteur a proposé une classification des schémas de gestion des clés de groupe en trois catégories principales.

Dans (36), l'auteur divise deux classes en sous classes basées sur les techniques de clé de chiffrement du trafic (TEK).

- Les catégories de systèmes de gestion de clés de groupe sont les suivantes
- Gestion centralisée des clés de groupe,
- Gestion décentralisée des clés de groupe,
- Gestion des clés de groupe distribuées.

Dans le cas de la gestion centralisée des clés de groupe, une entité garantit la fonction de distribution des clés et génère des clés chaque fois que nécessaire. Les membres du groupe coopèrent pour atténuer les besoins de stockage et d'augmenter l'utilisation de la puissance de calcul et de la capacité de transfert de données, tant du côté du client que du côté du serveur.

Dans un plan décentralisé, le grand groupe est réparti entre les gestionnaires de sous-groupes afin de résoudre les problèmes liés à un gestionnaire unique et à un point de défaillance unique**.** Lorsque chaque membre d'un groupe fournit des informations pour obtenir la clé de groupe**,** on parle de gestion de clé de groupe

Les auteurs de (37)présentent trois taxonomies basées sur les modèles de réseau**,** la probabilité de partage des clés et les modèles de communication.

1. Basée sur le modèle de réseau :

- Distribué,
- Hiérarchique ou en grappe.

2. Basé sur la probabilité du partage des clés :

- Probabiliste,
- Déterministe,
- Hybride.

3. Basé sur le modèle de communication :

- Unicast ou Point-to-point dans lequel il y a une source et une destination**,**
- Multicast ou multipoint, qui permet d'envoyer un message à plusieurs destination (groupe de nœuds),
- Broadcast ou diffusion permet d'envoyer un message à tous les nœuds du réseau**.**

Enfin, nous avons pensé à une catégorisation complète et valide de tous les types de réseaux ad hoc**,** où, pour assurer la sécurité de ces réseaux**,** le cryptage doit être utilisé dans le réseau.

Sur cette base, nous avons divisé les classifications en deux phases basées sur les composants du réseau et la relation entre les nœuds, et sur la base des techniques de cryptage utilisées dans la gestion et le partage des clés**.** La classification basée sur la cryptographie utilisée, le mécanisme d'établissement des clés, le modèle de réseau, le modèle de communication, la probabilité de partage des clés et la gestion des clés de groupe.

3.5 Travaux connexes

Les schémas de gestion des clés ont été largement étudiés dans la littérature et divers schémas ont été présentés. Chaque groupe de schémas s'applique à un type particulier de réseau. Tous ces systèmes de gestion des clés ont leurs propres avantages et inconvénients**.** Tous peuvent convenir à des besoins différents.

Xiao et al. (2007) (38) ont étudié le schéma de clés aléatoire par paire qui est une variante du schéma de clés par paires (Du et al., 2005) La principale différence entre les deux schémas est qu'ici nous utilisons moins de N-1 clés pour avoir un graphique connexe avec une forte probabilité. Ce régime a également trois phases : phase d'initialisation, phase de configuration de la clé et phase de partage des clés.

Al-Haija (2010) (38), a récupéré les quatre approches probabilistes de gestion des clés qui ont été largement utilisées dans les WSN. Ces approches sont : Schème de prédistribuions aléatoire

de clé, schéma de clé Q-composite, MultiPath Schéma de renforcement et clés aléatoires par paires. Il a également fourni une analyse probabiliste du modèle d'évaluation pour évaluer ces protocoles individuellement.

Le modèle comprend plusieurs facteurs qui doivent être soigneusement examiné avant de déployer le WSN. Les facteurs sont : l'évolutivité, la confidentialité, la mémoire, complexité de la communication et puissance consommation. Les résultats ont montré que schéma de paires de clé peut être adapté dans divers environnements satisfaisant la plupart des facteurs de notre étude.

Kuchipudi et Basha (2012) (38) ont proposé plusieurs systèmes de gestion qui ne peuvent pas offrir de solide résilience contre les attaques de capture de nœuds, ou nécessitent beaucoup de mémoire pour obtenir la connectivité souhaitée. Leur l'algorithme de Bloms proposé surpasse les autres en termes de résilience contre la capture de nœuds. Le schéma de distribution des clés Bloms avec connaissance du déploiement offre une plus grande connectivité avec une portée de transmission la plus courte avec une capacite de mémoire minimum

Filip Jurnecka (2013) (9)a présenté un outil basé sur OMNeT++ et construit sur MiXiM**.** Il est destiné à l'évaluation automatique des schémas de gestion des clés dans les réseaux de capteurs sans fil (WSNs). Son but est d'unifier le processus d'évaluation de manière à ce que toutes les évaluations futures pourront utiliser un seul point de référence au lieu d'utiliser une évaluation analytique ou manuelle. Il permet une comparaison des schémas en sélectionnant les valeurs appropriées pour chaque schéma. Dans son cadre, il a utilisé un sous-ensemble de paramètres d'évaluation, à savoir : le débit de communication, la connectivité, la résilience du réseau et l'énergie consommée, qu'il considère comme des métriques mesurables**.** Dans sa thèse, les métriques d'évaluation proposées ont été simulées sur les principaux schémas pour les réseaux sans fil, à savoir : la pré-distribution de la clé maîtresse, la pré-distribution par paire, BROSK, la pré-distribution aléatoire d'Eschenauer-Gligor (EG), et PIKE**.** Ce cadre ajoute trois grands groupes de composants à MiXiM : la bibliothèque de schémas de gestion de clés, le support d'évaluation de KMS et le support KMS**.** Cependant, il n'est pas gratuit et n'est pas open source.

Qasem Abu Al-Haija (2013) (9**)** a proposé un outil logiciel pour simuler et évaluer les six mesures d'évaluation présentées pour un réseau de capteurs sans fil non déterministe. Qui sont : L'évolutivité, la connectivité des clés, la capacité de la mémoire, la complexité de la communication**,** la consommation d'énergie et la confidentialité**.** Les mesures d'évaluation ont été simulées et évaluées pour aider le concepteur du réseau à choisir la meilleure gestion probabiliste des clés de sécurité. Cet algorithme est destiné à un réseau sensoriel distribué de façon aléatoire. Il est programmé et implémenté dans le langage de programmation VB.NET**.** Ce simulateur définit deux méthodes d'évaluation**,** ces méthodes sont : Une approche d'évaluation et des approches comparatives**.** Dans l'évaluation d'une approche nous pouvons choisir une approche à utiliser dans les calculs de métriques**,** et nous pouvons également entrer toutes les spécifications de votre réseau pour tester le comportement de l'approche sélectionnée du point de vue d'une métrique parmi les six métriques présentées**.** Dans la comparaison des approches les quatre approches seront comparées qui sont **:** Clé aléatoire, Q-composite aléatoire, Random Multi-path, et Aléatoire par paire **;** ensuite vous choisissez les métriques requises pour être calculées.

3.6 Conclusion

Plusieurs schémas de gestion de clés sont proposés dans les réseaux ad hoc. Dans ce chapitre, nous avons présenté les schémas les plus importants avec leurs classifications et taxonomies. Les propriétés des schémas de gestion de clés proposés sont discutées. Enfin, les outils d'évaluation existants pour les systèmes de gestion de clés sont présentés et discutés.

Chapitre 4 : Conception, mise en œuvre et performances

Chapitre 4 61

4.1 Introduction **61**

4.2 Conception **61**

4.2.1 Architecture de notre système **62**

4.2.2 les KMS utilisés **63**

4.2.3 Les métriques d'évaluation utilisées **63**

4.3 Environnement logiciel **64**

4.3.1 Le Choix du simulateur OMNet++ : **64**

4.3.2 Présentation OMNet++ **65**

4.3.3 Les plates formes OMNet++ **65**

4.4 Implémentation **66**

4.5 Performance **69**

4.4 Conclusion **71**

Chapitre 4

Conception, mise en œuvre et performances

4.1 Introduction

Dans ce chapitre, nous présenterons et expliquerons notre proposition d'outil pour évaluer certains schémas choisis, et fournir une description détaillée de mise en œuvre. Une évaluation automatique de certains schémas de gestion des clés sera menée, et une étude comparative sera faite à la lumière des résultats obtenus.

4.2 Conception

Notre objectif est d'évaluer les schémas de gestion des clés cryptographiques pour les applications des réseaux sans fil ad hoc. Pour aider les utilisateurs à choisir le schéma approprié et à l'appliquer dans des scénarios réels. Comme pour tout système, nous pouvons évaluer la qualité d'un schéma de gestion de clés en évaluant ses propriétés. Pour cela, nous proposons le système présenté dans la Figure 4.1.

Notre système nécessite en entrée les exigences suivantes : le modelé du réseau et les schémas de gestion de clé a appliqué et produit en sortie les résultats de calcul des métriques d'évaluation par rapport à chaque schéma. Ces exigences sont mises en œuvre sous forme des modules indépendants comme suit :

1. **Réseau** : Pour évaluer les KMS choisis, nous devrons les appliquer à un modèle de réseau. Nous commençons d'abord par définir le modelé de ce réseau qui sera simulé par la suite pour obtenir les résultats attendus

2. **Schémas Gestion des clés Adhoc** : ce module présente les schémas qui seront évalués. Ces schémas sont appliqués à un réseau qui sera définis par l'utilisateurs. À chaque itération, l'utilisateur peut en sélectionner un parmi l'ensemble de schémas à appliquer.

4.2.1 Architecture de notre système

Notre architecture se concentre sur trois étapes :

- La première est l'étape de simulation dans laquelle le modèle du réseau est simulé avec le schéma de gestion de clé sélectionné et il sera évalué à chaque itération de simulation.
- La deuxième étape est l'étape de calcul des métriques.
- La troisième étape est réservée à la comparaison des résultats obtenus dans l'ensemble des itérations.

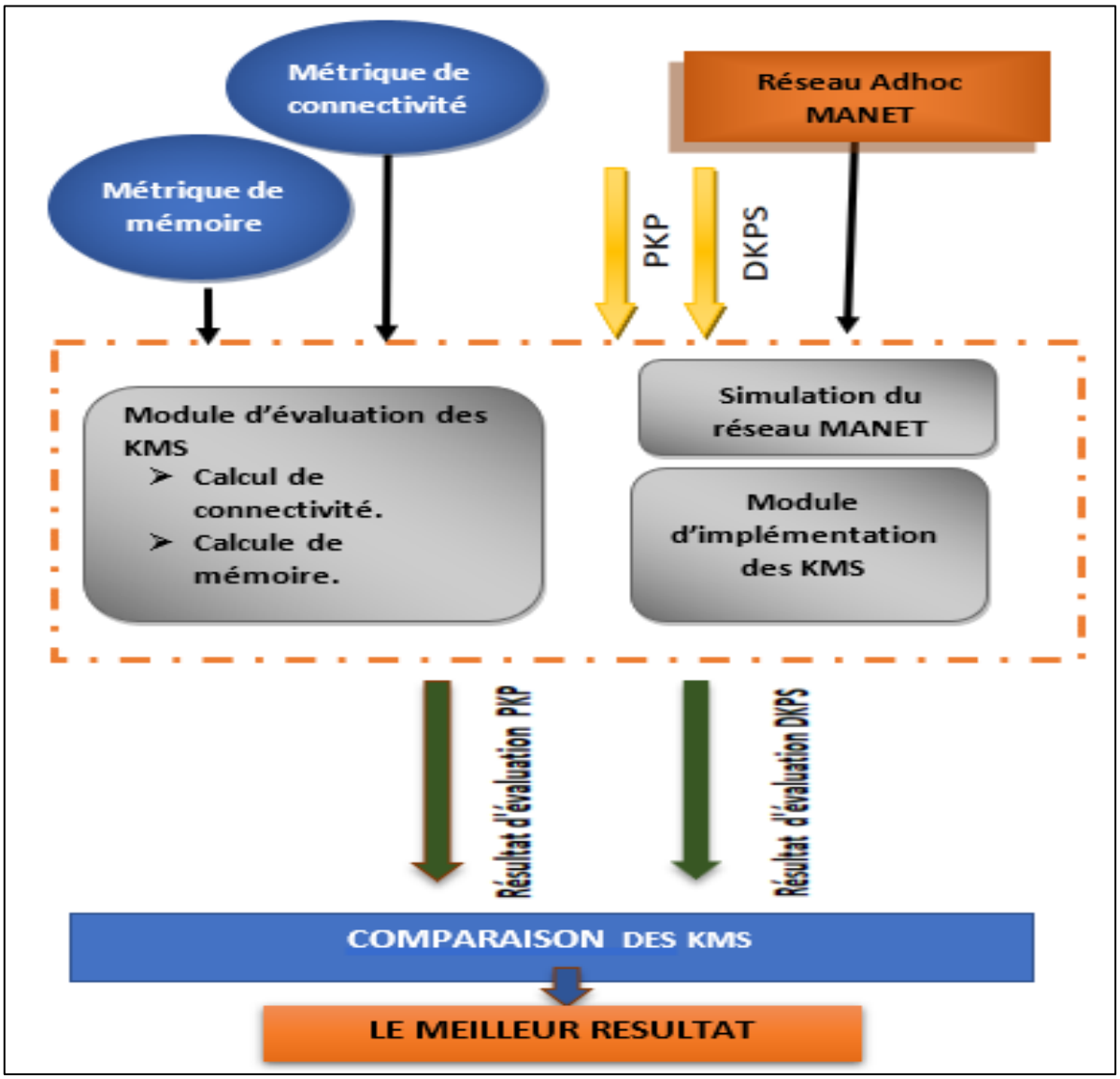


Figure 4 1: Architecture de notre système

4.2.2 Les KMS utilisés

Les deux KMS basés sur la cryptographie symétrique utilisés dans notre architecture sont : le schéma de pré distribution de la clé distribuée DKPS, et le schéma de la pré distribution de la clé par paire. Ces KMS sont jugés les plus simple et efficaces dans le monde de la sécurité des réseaux Adhoc.

L'évaluation de ces deux schémas est indispensable à la comparaison des deux KMS et à l'orientation du choix de l'utilisateur vers le KMS le plus efficace pour le modèle du réseau simulé**.**

- **Schéma de Pré-distribution de clé par paire (*Pair-wise key pre-distribution*)** est la solution idéale et la plus simple du point de vue de la sécurité, car chaque nœud capturé ne révèle que les clés des liens dont il faisait partie. Du fait de ses caractéristiques de scalabilité et d'insensibilité, pour n nœuds du réseau ad hoc, chaque nœud doit stocker n − 1 clés, et l'ajout de nouveaux nœuds au réseau nécessite une mise à jour sur chaque nœud ou un pré-chargement des clés supplémentaires pour les futurs nœuds à venir.

- **Schéma de pré distribution de clé distribuée *DKPS* (*Distributed Key Pre-distribution Scheme*)** (13) : introduit en 2004 par Aldar CE Chan, est un schéma de gestion de clé symétrique distribué pour les réseaux mobiles ad hoc (MANETs), Il repose sur trois phases principales. Tout d'abord, la sélection de clé distribuée (Distributed Key Selection- DKS), dans cette phase, chaque nœud utilise la propriété d'exclusion pour obtenir la clé aléatoire de l'ensemble universel, car l'évaluation de la propriété d'exclusion dépend du concept de Cover Free Family (CFF) et utilise la méthode probabiliste pour faire CFF de manière distribuée, ce qui supprime le besoin de TTP (tiers de confiance) ce qui rend les MANETs plus dynamique. Deuxièmement, Secure Shared-key Discovery (SSD). Il s'agit de la deuxième phase de DKPS, dans laquelle chaque nœud a une clé partagée avec un autre nœud dans le réseau. Cette étape est importante car les attaques peuvent se produises dans la phase DKS. Enfin, Key Exclusion Property Testing (KEPT), dans la dernière phase, une matrice d'incidence est utilisée pour présenter la relation entre la clé des nœuds mobiles et les clés partagées. Il utilise des valeurs binaires pour construire la matrice. DKPS nécessite moins de stockage et plus efficace que d'autres approches, il minimise les exigences posées aux réseaux sous-jacents et peut être facilement appliqué aux scénarios de mise en réseau ad hoc.

4.2.3 Les métriques d'évaluation utilisées

Une métrique est une quantité numérique précise qui peut être utilisée pour évaluer les propriétés. Nous avons choisi deux métriques d'évaluation des KMS dans notre système :

- **Calcule de connectivité** : c'est le calcul du nombre du liens physiques établis entre les nœuds du réseau.

- **Calcule de la mémoire nécessaire pour le stockage :** c'est le calcul de la quantité de données stockées par un KMS et la taille de l'implémentation KMS elle-même sur la mémoire de stockage.

4.3 Environnement logiciel

Notre projet a été réalisé dans l'environnement logiciel suivant :

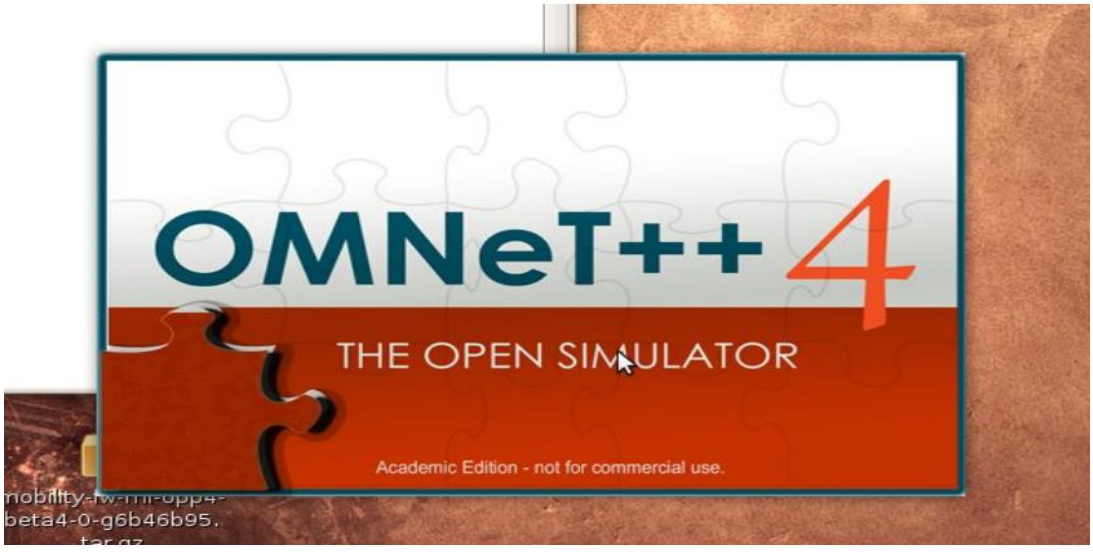
Système d'exploitation WINDOWS ; Simulateur OMNET++ ; MIXIM ; INET.

4.3.1 Le Choix du simulateur OMNet++ :

Le déploiement d'un réseau exige une étape de simulation, cette simulation permet de tester à moindre cout les performances d'une solution .OMNet++ est environnement de simulation à événements discrets basé sur le langage C++.il est totalement programmable, paramétrable et modulaire ainsi grâce a son architecture flexible et générique il a été utilisé avec succès dans divers domaines notamment :

- La modélisation de réseau de file attente.
- La modélisation de protocole de communication.
- La validation des architectures hardware.
- L'évaluation de performances pour des systèmes software complexes.

OMNet++ sera notre environnement de simulation, grâce à son architecture modulaire.



4.3.2 Présentation OMNet++

OMNET++ : est une plateforme de simulation, modulaire, open source, orienté objet et à événements discrets écrit en C++, Elle offre un environnement d'exécution graphique, elle a été conçue pour fournir un environnement complet pour la construction et la simulation des réseaux. Les modèles de simulation sont mis en œuvre par des cadres de simulation tels que MiXiM, Castalia et INET. OMNeT++ n'est pas un simulateur, mais fournit une infrastructure et des outils pour écrire des simulations. L'architecture des composants permet de construire des simulations à partir de modules de composants réutilisables. Les modules ont des paramètres pour personnaliser leur comportement et communiquer entre eux par message. La fonctionnalité est implémentée dans des modules dits simples, qui sont programmés en C++ et utilisent l'API OMNet++. Les simulations peuvent être exécutées sous une interface utilisateur graphique ou en ligne de commande.

4.3.3 Les plates formes OMNet++

Il existe plusieurs extensions, plateforme et simulateurs basé sur OMNET++.

Nous avons utilisé.

- **MiXiM** (simulateur mixte) est utilisée pour déterminer les propriétés et calculer les métriques afin d'évaluer les schémas de gestion des clés.

  MiXiM est un cadre de modélisation OMNeT ++ créé pour les réseaux mobiles sans fil et fixes tels que les réseaux de capteurs sans fil, les réseaux corporels et les réseaux ad hoc. Il propose des modèles de propagation des ondes radio, d'estimation des interférences, de consommation d'énergie des émetteurs-récepteurs radio et des protocoles MAC sans fil.

  Mixim donne pour omnet++ de brefs protocoles et un cadre pour de nombreux réseaux. Il aide les chercheurs à comparer leur propre idée avec celle déjà mise en œuvre.

  Les cinq KMS basés sur la cryptographie symétrique mis en œuvre sont : la prédistribuions de clé principale, la prédistribuions par paires, BROSK, la prédistribuions aléatoire Eschenauer-Gligor et PIKE. Ces régimes sont évalués à l'aide de cet outil pour faire une comparaison et orienter le choix du plus efficace. La figure 4.2 illustre les schémas implémentés dans OMNet++.

.

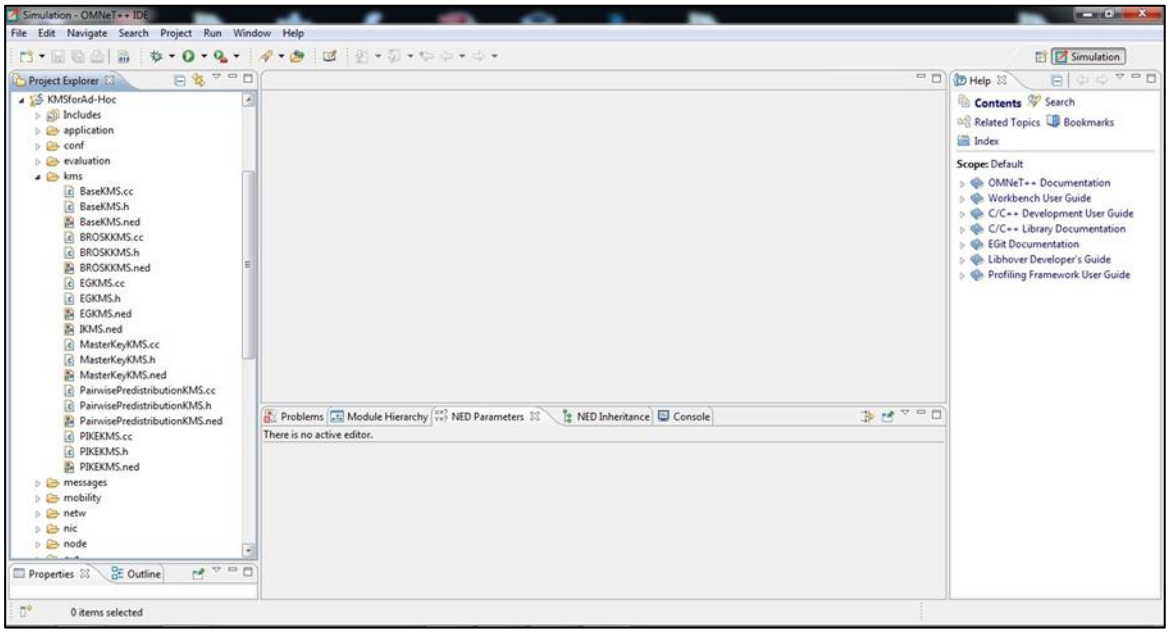


Figure 4 2: Mise œuvre des KMS .

- **INET Framework** est une bibliothèque de modèles open source pour l'environnement de simulation OMNeT++. Il fournit des protocoles, des agents et d'autres modèles pour les chercheurs et les étudiants travaillant avec des réseaux de communication. INET est particulièrement utile lors de la conception et de la validation de nouveaux protocoles ou de l'exploration de scénarios nouveaux ou exotiques.

  INET contient des modèles pour la pile Internet (TCP, UDP, IPv4, IPv6, OSPF, BGP, etc.), les protocoles de couche de liaison filaire et sans fil (Ethernet, PPP, IEEE 802.11, etc.), la prise en charge de la mobilité, les protocoles MANET, DiffServ, MPLS avec signalisation LDP et RSVP-TE, plusieurs modèles d'application et de nombreux autres protocoles et composants.

- **Crypto++** est une bibliothèque de chiffrement fournissant une interface C++ relativement moderne. Crypto++est utilisée pour définir les schémas de gestion des clés.

4.3 Implémentation

L'outil proposé est composé de trois grands modules :

1. **Un module de simulation :** pour simuler le modèle de réseau sur lequel nous allons implémenter les KMS.

2. **Un module pour l'implémentation des KMS *:*** ce module contient l'implémentation des algorithmes des KMS. Il offre également la possibilité de l'implémentations publiques et l'amélioration de celles existantes. Ce module dépend fortement de *MiXiM*. La plupart des composants de cet outil étendent les classes de base de MiXiM. Par conséquent, bien

que les paramètres sous-jacents puissent être radicalement modifiés ou même complètement supprimés, MiXiM est requis pour exécuter cet outil.

Parmi les méthodes les plus importantes qu'on a utilisées pour l'évaluation des KMS : ***getNumberOfKeys()*** : pour récupérer le nombre des clés partager par un nœud.

getKey() et ***setKey() :*** est utilisé par l'entité de pré-distribution pour charger les clés avant le déploiement.

demandKey() : est utilisée pour établir une nouvelle clé avec un nœud du réseau avec lequel ce nœud ne partage pas encore de clé.

updateKey() : utilisée pour la mise à jours une clé existante.

updateKey() : est utilisée pour révoquer une clé éventuellement compromise ou mise à jour.

3. **Un module d'évaluation des KMS :** fonctionne partiellement en conjonction avec le module implémentation des KMS afin d'évaluer leurs diverses caractéristiques du KMS. C'est dans ce module que nous avons implémenté les différentes méthodes pour le calcul des métriques d'évaluations des KMS.

   Ce module est basé sur la méthode ***BaseEal().*** Il ne fait pas partie d'un nœud mais plutôt de la simulation entière afin de garder les modèles d'évaluation logiquement séparés. Cependant, les interactions avec les nœuds sont nécessaires pour pouvoir recueillir des informations.

KMSApplication.h

```
    KMSApplication();
    virtual ~KMSApplication();

    /** @brief Message kinds used by this layer.*/
    enum KMSApplMessageKinds {
        NEIGHBOURS_TIMER = LAST_BASE_APPL_MESSAGE_KIND,
        NETWORK_TIMER,
        LAST_KMS_APPL_MESSAGE_KIND
    };
private:
    /** @brief Copy constructor is not allowed.
     */
    KMSApplication(const KMSApplication&);
    /** @brief Assignment operator is not allowed.
     */
    KMSApplication& operator=(const KMSApplication&);

protected:
    int numNodes;

    /** @brief if the KMS requires some initialization period before evaluation. */
    int initPhaseLength;
    int neighboursPhaseLength;
    int networkPhaseLength;

    /** @brief Timer message for scheduling next message.*/
    cMessage *neighboursTimer;
    /** @brief Timer message for scheduling next message.*/
    cMessage *networkTimer;

    cModule::GateIterator * stateNeighbour;
    int stateNetwork;

    /** @brief Enables debugging of this module.*/
    bool coreDebug;
```

Figure 4 3: Implémentation des KMS

Le calcul des métriques est effectué au niveau de ce module.

- **Évaluateur de connectivité**

Pour calculer le rapport de connectivité des nœuds, nous avons utilisé un algorithme de graphe simple pour l'évaluation de la connectivité, connu sous le nom d'algorithme de FloydWarshall. Il fournit la matrice des coûts chemins à partir de laquelle nous pouvons calculer le taux de connectivité réussi.

L'algorithme de Floyd-Warshall (39): permet de trouver le plus court chemin entre toute paire de sommets. Il fait partie de la famille des algorithmes à correction d'étiquettes, mais comme il permet de calculer le plus court chemin pour tout couple (x, y)de sommets du graphe, les étiquettes ne sont plus un tableau (une étiquette par sommet), mais une matrice Mde taille $N \times N$où l'entrée $M_{i,j}$correspond au plus court chemin entre les sommets $i$et j. Cet algorithme est valable quelles que soient les valuations des arcs, y compris si cela implique des circuits négatifs (l'algorithme permet de prouver l'existence ou l'inexistence de tels circuits). L'algorithme est constitué de Nitérations principales ; pour chaque itération k, on calcule les plus courts chemins entre toute paire de sommets avec des sommets intermédiaires appartenant uniquement à l'ensemble $\{1, 2, \ldots, k\}$. A l'initialisation, on calcule le plus court chemin entre toute paire de sommets n'ayant pas de sommets intermédiaires, donc il suffit de prendre la longueur des arcs qui existent et mettre un poids infini si l'arc n'existe pas. Par la suite, si on note la valeur du plus court chemin dont les seuls sommets intermédiaires sont dans l'ensemble, alors on a l'égalité suivante :

$$M_{i,j}^{k} = \min\left(M_{i,j}^{k-1}, M_{i,k}^{k-1} + M_{k,j}^{k-1}\right)$$

Cette formule est à la base de l'algorithme, qui est détaillé ci-dessous (39).

Algorithme 11: Algorithme de Floyd

```
Données : Un graphe orienté pondéré G = (X, A, W)
Résultat : Le plus court chemin entre toute paire de sommets de G
// M : matrice des plus courts chemins
// P : matrice des prédécesseurs pour les plus courts chemins
Initialiser M à +∞
Initialiser P à 0
pour i allant de 1 à N faire
    M_{i,i} ← 0
    P_{i,i} ← i
    pour tout successeur j de i faire
        M_{i,j} ← W[i, j]
// Calcul des matrices successives
pour k allant de 1 à N faire
    pour i allant de 1 à N faire
        pour j allant de 1 à N faire
            si M_{i,k} + M_{k,j} < M_{i,j} alors
                M_{i,j} = M_{i,k} + M_{k,j}
                P_{i,j} = P_{k,j}
si ∃i | M_{i,i} < 0 alors
    retourner Il existe un circuit de longueur négative passant par i
sinon
    retourner M
```

➢ **Évaluateur de mémoire**

Dans ce module d'évaluation de la mémoire, nous mesurons la quantité de données stockées par un KMS et la taille de l'implémentation KMS elle-même. Nous mesurons la taille des données stockées via deux méthodes **getNumberOfKeys()** et ***getSizeOfAdditionalData()*** avec la connaissance de la taille des clés stockées. La taille d'une implémentation KMS est très difficile à mesurer. Cependant, les mesures des fichiers de sortie compilés peuvent être comparées les unes aux autres pour produire des résultats relatifs.

.

4.4 Performance

➢**La simulation du réseau**

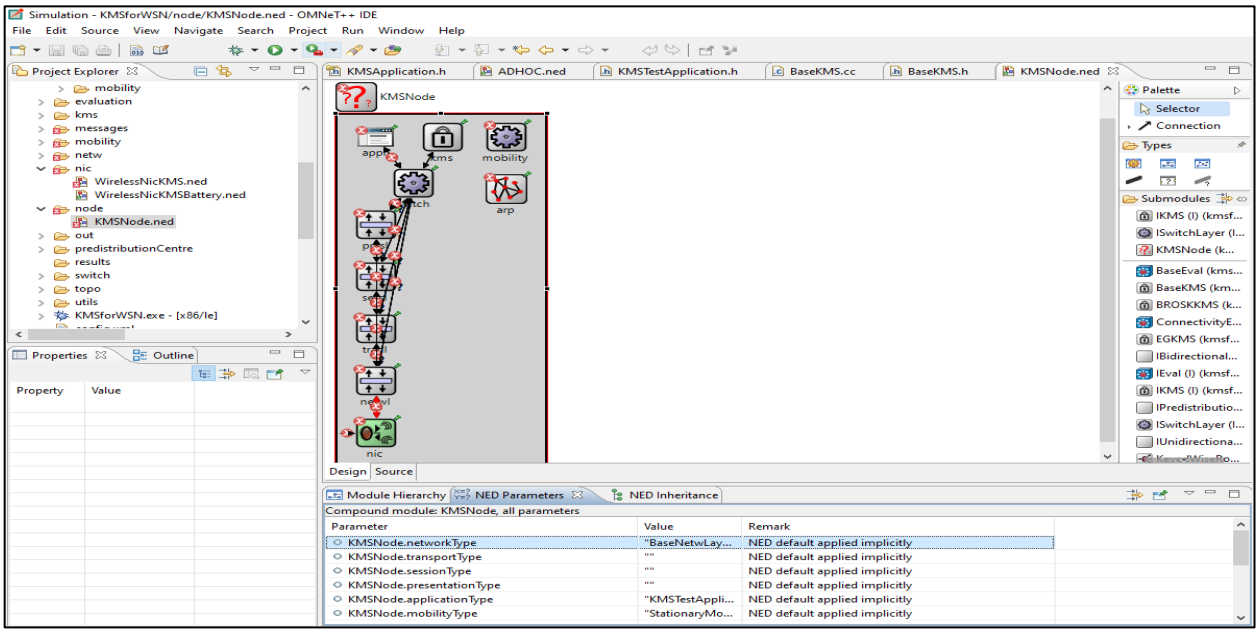


Figure 4 4: Création d'une simulation avec OMNET++

Les résultats obtenus de l'évaluation automatique des schémas proposés sur les métriques sont présentés sous forme textuelle *la figure 4.5* et graphique *La figure 4.6.*

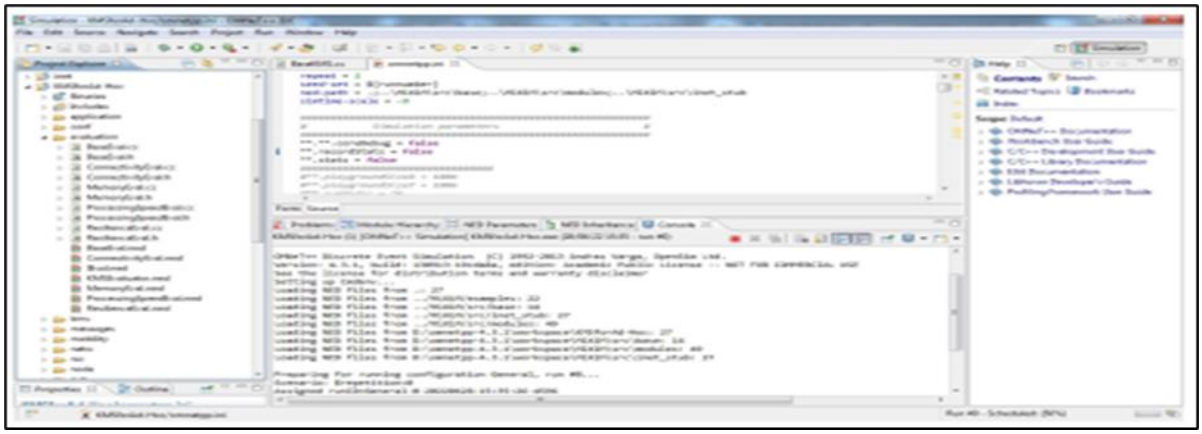


Figure 4 5: Nombre de liens établis (forme textuelle)

La figure 4.6 montre le nombre de liens établis dans chaque phase par chaque KMS sous forme de graphe.

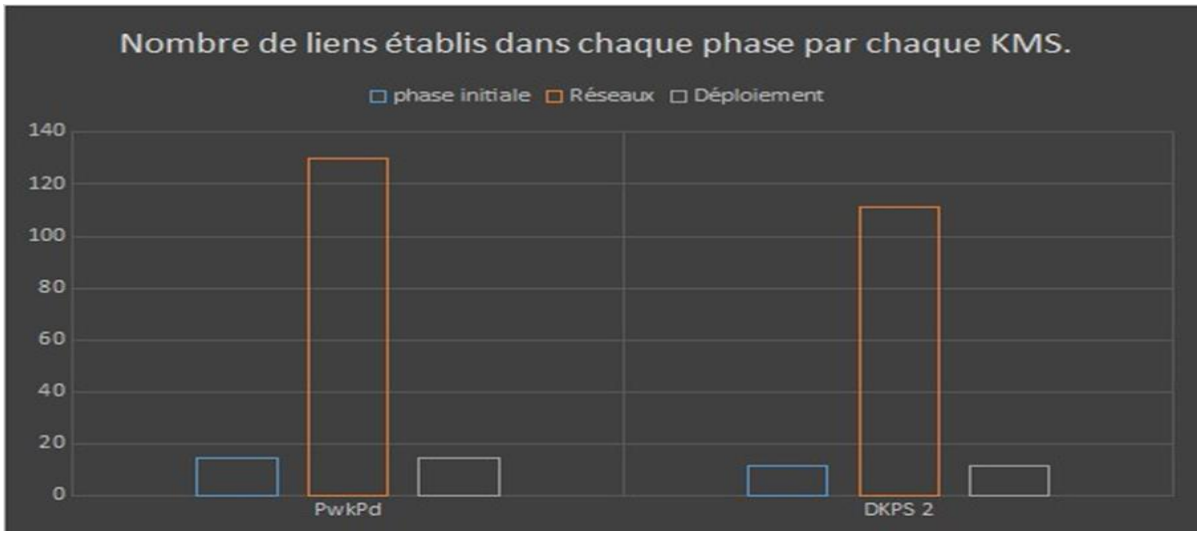


Figure 4 6: Nombre de liens établis dans chaque phase par chaque KMS

Dans ce graphe nous pouvons voir le nombre de liens, sécurisés par une clé partagée, établis par chaque KMS dans chaque phase pertinente de notre expérience (on a pris en compte seulement les deux phases : le nombre des liens dans la phase initiale et le nombre des liens dans le réseau). Plusieurs faits intéressants peuvent être observés.

Tout d'abord, nous pouvons voir la caractéristique de clé principale pour les deux KMS ***PwKPd*** et ***DKPS*** après le déploiement, où tous les nœuds partagent une clé unique. Ainsi, le nombre de liens sécurisés est égal au nombre de liens logiques dans le réseau. D'où la clé

principale reste après la phase d'initialisation, mais n'est plus utilisée directement sauf pour "uniquement" établir de nouvelles clés partagées.

Ainsi, le nombre de liens chute rapidement à 130 et 111 après la tentative répétée d'établir des clés avec tous les voisins après l'initialisation du réseau.

La figure 4.6 montre la taille de chaque schéma mis en œuvre dans notre cadre. Bien qu'il soit implémenté sur un simulateur fonctionnant sur un PC, une plate-forme sensiblement différente du matériel réel, les rapports approximatifs entre la taille des implémentations de chaque schéma devraient également tenir sur le matériel réel.

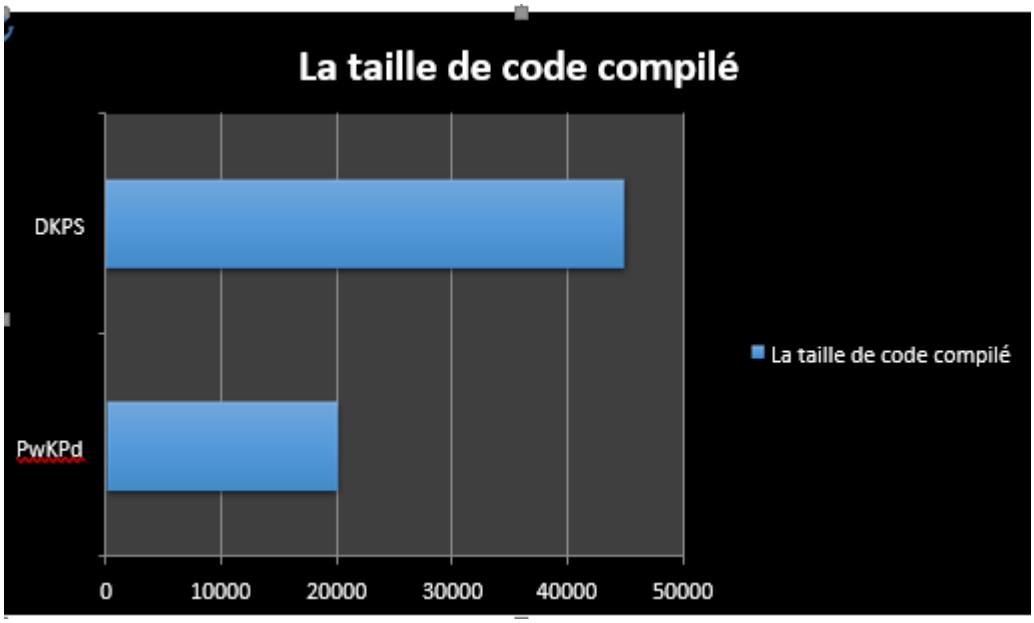


***Figure 4 7*:la taille mémoire de chaque KMS**

Un résultat légèrement surprenant de la figure 4.6 est la taille de DKPS. Vraisemblablement, la raison est l'ajout de cas de gestion logique avec plusieurs clés partagées et l'utilisation d'un conteneur de stockage supplémentaire dans l'implémentation du schéma, où une carte mappe des voisins aux clés partagées et une autre carte est utilisée pour attribuer des index aux clés préchargées.

4.4 Conclusion

Dans ce chapitre, nous avons présenté et expliqué l'outil développé pour évaluer certains schémas choisis, et fourni une description précise des principaux détails de mise en œuvre. Cet outil peut évaluer n'importe quel schéma. Les résultats de l'évaluation seront présentés et discutés, plus l'étude comparative qui sera menée.

Conclusion générale

Alors que les réseaux ad hoc deviennent de plus en plus populaires et utilisés dans différentes applications, la sécurité dans ces types de réseaux est le problème le plus important. Pour assurer la sécurité, plusieurs schémas de gestion de clés ont été proposés. Le travail présenté dans ce manuscrit a pour objectif de fournir un outil approprié pour évaluer les schémas de gestion de clés pour les réseaux ad hoc.

Nous avons commencé par une présentation générale des réseaux ad hoc avec leurs différents types et les caractéristiques. Afin de mieux comprendre la phase de chiffrement et le mécanisme de génération de clé, nous avons poursuivi en introduisant tous les concepts liés à ce sujet. Une étude de l'état actuel de l'art dans le domaine des schémas de gestion de clés, de leurs propriétés importantes et de leurs taxonomies a été présentée. Une nouvelle classification des schémas de gestion de clés exigeants pour les réseaux ad hoc a été élaborée. Un nouveau cadre d'évaluation automatique des schémas de gestion de clés pour les réseaux ad hoc utilisant la simulation a été développé et testé avec succès sur certains KMS.

L'outil est construit dans OMNet++ en plus du framework MiXiM. C'est hiérarchiquement construit comme un ensemble de modules d'évaluation. Les résultats de l'évaluation des schémas choisis sont présentés en tant que travail futur, notre objectif est de mettre en œuvre le maximum de schémas de gestion de clés. Ainsi, nous visons à fournir d'autres propriétés non mesurables pour évaluer les schémas de gestion de clés pour les réseaux ad hoc.

Bibliographie

1. **Mira Youcef et Djettou Brahim Khalil.** *Étude des Réseaux Ad hoc par la Théorie des Jeux .* université AKLI MOHAND OULHADJ-BOUIRA. ALGERIE : Mémoire de fin d'étude En vue de l'obtention du diplôme de Master 02, 2019.

2. **DOYI, Eric BOSASI.** *Gestion des ressources radios dans les réseaux sans fils cas d'un reseau wimax.* Khinshasa : Université de Khinshasa, 2010.

3. **Mr Daniel MABELE MONDONGA.** *" Etude sur les protocoles de routage d'un réseau sans fil en mode Ad Hoc et leurs impacts. Cas de protocoles OLSR et AODV".* CONGO : Institut supérieur d'informatique, programmation et analyse de KINSHASA., 2010.

4. **Mr BELKHIRA Sid Ahmed Hicham.** *" Optimisation de la QoS dans les Réseaux Adhoc Mobiles".* Université DJILLALI LIABES de Sidi Bel Abbés. ALGERIE : Thèse de Doctorat en Sciences Filière : Informatique,, 2020.

5. **IDRISS MAKHLOUF.** *" Gestion de clés basée identité pour les réseaux AD hoc".* Université LARBI BEN M'HIDI -OUM EL BOUAGHI : Mémoire de master pour l'obtention du diplôme de master en informatique option : architectures distribuées, Juillet 2019.

6. **Noureddine Lasla.** *La gestion de clés dans les réseaux de capteur sans fil.* Hamad bin Khalifa University : Thesis for : Magister, 2008.

7. **Challal, Yacine.** *Réseaux de Capteurs Sans Fils.* 17/11/2008.

8. **Priyanka Goyal, Vinti Parmar, Rahul Rishi.** *vulnerabilities, challenges, attacks, application.* s.l. : IJCEM International Journal of Computational Engineering & Management,pages 32-37, 2011.

9. **NASRI Radhia.** *Evaluation of cryptographic key management systems in wireless ad-hoc networks Presented for defense in a public examination.* Oum El Bouaghi:ALGERIE : Larbi Ben M'hidi University, July 3 th 2022.

10. **J. Bernsen and D.Manivannan.** *"Unicast Routing Protocols for Vehicular Ad Hoc Networks: A Critical Comparison and Classification".* s.l. : Elsevier Journal of Parvasive and Mobile Computing.page 1-18, 2009.

11. **R. Meraihi, M. Senouci and M. Djebri.** *"Réseau mobile Ad Hoc et réseaux de capteurs sans fil".* s.l. : chapitre de livre Edition Hermès, 2006.

12. **NASSIMA, ZEROUALI.** *LE ROUTAGE DANS LES RESEAUX DE CAPTEURS SANS FIL SOUS MARIN.* s.l. : UNIVERSITE ABOUBAKER BL KAID TELEMCEN, 2016.

13. **Wan Du, David Navarro, Fabien Mieyeville, and Frédéric Gaffiot. , .** *Towards a taxonomy of simulation tools for wireless sensor networks. .* s.l. : In Proceedings of the 3rd International ICST Conference on Simulation Tools and Techniquespages 1–7, 2010.

14. **Goffinet, Francois.** *Algorithmes de cryptographie symétrique.* 2021.

15. **https://librecours.net/module/culture/intro-chiffrement/pres/co/chiffrement-sym.html?mode=html.**

16. **Bing Wu, Jie Wu, and Mihaela Cardei.** *A survey of key management in mobile ad hoc networks. .* s.l. : In Handbook of research on wireless security, pages 479–499. IGI Global,, 2008. .

17. **Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone.** *Handbook of applied cryptography. .* s.l. : CRC press, 2018. 35, 41, 44, 2018.

18. **Valkonen., Jukka.** *Key management in ad-hoc networks. .* s.l. : Technical report, HelsinkiUniversity of Technology,, 2007. .

19. **Hu, Shuaiqi.** *A hierarchical key management scheme for wireless sensor networks based on identity-based encryption.* s.l. : IEEE International Conference on Computer and Communications (ICCC), pages 384–389. , 2015.

20. **Adrian Perrig, Robert Szewczyk, Justin Douglas Tygar, Victor Wen, and David E Culler.** *Security protocols for sensor networks. Wireless networks.* Spins : 8(5):521–534,, 2022.

21. **Neeraj Kumar, Rahat Iqbal, Sudip Misra, and Joel JPC Rodrigues.** *An intelligent approach for building a secure decentralized public key infrastructure in vanet.* s.l. : Journal of Computer and System Sciences, 81(6):1042–1058, , 2015.

22. **Gligor, Laurent Eschenauer and Virgil D.** *A key-management scheme for distributed sensor networks.* s.l. : In Proceedings of the 9th ACM Conference on Computer and Communications Security,pages 41–47, 2002.

23. **Gicheol Wang, Gihwan Cho, and Sangwon Bang.** *A pair-wise key establishment schemewithout predistributing keys for ad-hoc networks. I.* s.l. : n IEEE International Conference on Communications, 2005. ICC 2005. 2005, volume 5, pages 3520–3524. IEEE, , 2005.

24. **F Richard Yu, Helen Tang, Peter C Mason, and Fei Wang.** *A hierarchical identity based key management scheme in tactical mobile ad hoc networks.* s.l. : IEEE transactions on network/16811/mod_resource/content/0/Cours1/TI60_sensors_cours1.pdf, 2022.

25. **Eric Ke Wang, Yuming Ye, and Xiaofei Xu.** *Location-based distributed group key agreement scheme for vehicular ad hoc network.* s.l. : International Journal of Distributed Sensor Networks, 2014.

26. **Muhammad Fahad Khan, Kok-Lim Alvin Yau, Rafidah Md Noor, and Muhammad Ali Imran.** *Routing schemes in fanets.* s.l. : A survey. Sensors, 20(1):38, 2019.

27. **Ali Ghorbani, Kui Ren, Sencun Zhu, and Aiqing Zhang,.** *editors, Security and Privacy in Communication Networks, .* s.l. : Springer International Publishing. ISBN 978-3-319-78816-6., 2018.

28. **Zahid Mahmood, Huansheng Ning, and AtaUllah Ghafoor.** *A polynomial subset-based efficient multi-party key management system for lightweight device networks. .* s.l. : Sensors 17 (4):670, 2017.

29. **Chowdhury, Md Samsul Haque and Morshed U.** *A new cyber security framework towards secure data communication for unmanned aerial vehicle (uav).* s.l. : In Xiaodong Lin.

30. **Marcos A Simplício Jr, Paulo SLM Barreto, Cintia B Margi, and Tereza CMB Carvalho.** *A survey on key management mechanisms for distributed wireless sensor networks.* s.l. : Computer networks, 54(15):2591–2612, , 2010. .

31. **Yong Wang, Garhan Attebury, and Byrav Ramamurthy.** *A survey of security issues in wireless sensor networks. .* s.l. : IEEE Communications Surveys and Tutorials, 8(2):2–23, , 2006. .

32. **Bocheng Lai, Sungha Kim, and Ingrid Verbauwhede.** *Scalable session key construction protocol for wireless sensor networks In IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES).* s.l. : Citeseet, 2002.

33. **Varadharajan., Junqi Zhang and Vijay.** *Wireless sensor network key management survey and taxonomy.* . s.l. : Journal of network and computer applications, 33(2):63–75, 2010.

34. **Gill., Pooja Singh and Nasib Singh.** *A survey on key management schemes in wireless adhoc networks.* s.l. : International Journ al of Applied Engineering Research, 13(1):268–272, , 2018.

35. **Ricardo., Manuel P.** *Lecture notes in wireless networks and protocols.https://web.fe.* 2011.

36. **Challal., Saïd Gharout and Yacine.** *Group key management.* s.l. : Models & Optimisation and Mathematical Analysis Journal, 1(1):106–111,, 2012.

37. **Kant., P Raghu Vamsi and Krishna.** *A taxonomy of key management schemes of wireless sensor networks.* . s.l. : In 2015 Fifth International Conference on Advanced Computing &Communication Technologies, pages 690–696. IEEE, , 2015. .

38. **Qasem Abu Al-Haija, Mohamed H Shwehdi, and Muhammad Banat.** *Evaluation metrics for wireless sensor network security: Algorithms review and software tool.* s.l. : Journal of Computer Science, 9(5):635–645,, 2013. .

39. **Guére, Christelle.** *"Modèles et Algorithmes de Graphe" .* 2012.

40. **Fokine, Klas.** *Key management in ad hoc networks.* 2002.

41. **Teeb H Hadi. I, .** *Manet and wsn: What makes them different? .* s.l. : RACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), 7(6):23–28, 2017.

42. **Jurnecka., Filip.** *On automated evaluation of key management schemes in wireless sensor networks.* s.l. : PhD thesis, Masaryk University,Brno, 2014.

43. **Kaur, Prabhleen.** *An overview on manet-advantages, characteristics and security attacks. I.* s.l. : In International Journal of Computer Applications, 4th International Conference on Advancements in Engineering & Technology (ICAET 2016), 2016.

44. **Jin-Shyan Lee, Yu-Wei Su, and Chung-Chou Shen. .** *A comparative study of wirelessprotocols: Bluetooth, uwb, zigbee, and wi-fi.* s.l. : In IECON 2007-33rd Annual Conference ofthe IEEE Industrial Electronics Society, pages 46–51. Ieee, , 2007.

45. **Krishnamurthy, Prasant Mohapatra and Srikanth.** *AD HOC NETWORKS: technologies and protocols. Springer Science & Business Media.* , 2004. .

46. **Rodrigo Roman, Javier Lopez, Cristina Alcaraz, and Hsiao-Hwa Chen.** *Sensekey–simplifying the selection of key management schemes for sensor networks.* s.l. : In IEEE Workshops of International Conference on Advanced Information Networking and Applications, pages 789–794. IEEE, 2011.

47. **Singh., Manjyot Saini and Harjit.** *Vanet its characteristics attacks and routing techniques :.* s.l. : a survey. International Journal of Science and Research, 5(5):1595–1599, , 2016. .

48. **Soler., Jorge Salazar.** *Wireless networks,.* 2017. .

49. **Abdelmadjid Bouabdallah Yacine Challal, Hatem Bettahar. .** *Cours: Les réseaux de capteurs (wsn: Wireless sensor networks).* s.l. : https://moodle.utc.fr/pluginfile.php.

50. **Hassen DKHIL.** *Greedy perimeter stateless routing sur omnet++. PhD thesis.* Tunisie : Master's thesis, Ecole nationale supérieur d'informatique, V, 12, 2009.

51. **Elaine Barker.** *Recommendations for Key Management - Part 1 –.* s.l. : General. Federal Information.

52. **Sunil Maakar, Yudhvir Singh et Rajeshwar Singh.** *An Enhanced Gauss-Markov Mobility Model for Simulation of FANET in 3-D Environment .* Nov 2018.

53. **Dieynaba Mall, Karim Konate.** *Analyse des Protocoles de Gestion des Clés dans les Réseaux Mobiles Ad Hoc .* 2011.