**République Algérienne Démocratique et Populaire**
**Ministère de l'Enseignement Supérieur et de la Recherche Scientifique**
*Université Abderrahmane Mira Béjaïa*
Faculté des Sciences Exactes
Département Informatique


## Mémoire de fin de Cycle

En vue de l'obtention du Diplôme de Master Recherche en Informatique

**Option : Réseaux et Systèmes Distribués**

*Thème*

# Sélection des nœuds de confiance dans les réseaux mobiles

*Réalisé par :*

**BENNOUCHEN Boudiaf** et **TAMINDJOUTE Hocine**

*Encadré par :*

M. **SADI Mustapha**

| | | |
|---|---|---|
| **Président :** | M. **AISSANI Sofiane** | Université de Béjaïa |
| **Examinateur :** | Mme. **CHEKRID Mohamed** | Université de Béjaïa |
| **Examinateur :** | Mlle. **CHERIFI Feriel** | Université de Béjaïa |

2016-2017

# *Remerciements*

Nous tenons à exprimer nos vifs remerciements et notre profonde gratitude à notre encadreur monsieur Sadi Mustapha et à l'ensemble du personnel du département d'informatique de l'université de Béjaia, et à tous ceux qui ont contribué à la réalisation de ce travail.

Un grand merci à nos familles et nos amis, pour leur soutien permanent et indéfectible.

# *Dédicaces*

**On dédie ce travail :**

*À nos familles, nos parents,*

*À nos amis,*

*À tous ceux qui nous ont aidé et soutenu.*

# Table des matières

# Table des figures

# Liste des tableaux

# Liste des abréviations

| | |
|---|---|
| **AC** | Autorité de Certification. |
| **AKM** | Autonomous Key Management. |
| **BCA** | Backup erification Authority. |
| **CH** | Cluster Head. |
| **CPU** | Central Process Unit. |
| **CRL** | Certificate Revocation List. |
| **DoS** | Denial of Service. |
| **GSM** | Global System for Mobil communication. |
| **GPRS** | General Packet Radio Service. |
| **MANET** | Mobile Ad hoc NETwork. |
| **NCA** | Number of times that a node acted as a CA. |
| **NREJ** | Number of rejects. |
| **NTC** | Neighborhood Trustworthy Certifier. |
| **PGP** | Pretty Good Privacy. |
| **PKI** | Public Key Infrastructure. |
| **RSA** | Rivest-Shamir-Adleman. |
| **SEKM** | Secure and Efficient Key Management. |
| **TC** | Trust Chain : chaine de confiance. |
| **TTL** | Time To Live. |
| **TV** | Trust Value. |
| **UMTS** | Universal Mobile Telecommunications System. |
| **WLAN** | Wireless Local Area Network. |
| **WMAN** | Wireless Metropolitan Area Network. |
| **WWAN** | Wireless Wide Area Network. |
| **WPAN** | Wireless Personal Area Network. |

# Introduction générale

Les avancées remarquables de la technologie ont favorisé le développement des réseaux mobiles de façon prodigieuse. Les réseaux mobiles Ad hoc sont l'une des principales catégories de réseaux mobiles. Un réseau mobile Ad hoc est un système distribué, composé de plusieurs entités autonomes capables de communiquer entre elles sans l'existence d'une infrastructure centralisée. Ces noeuds communiquent via des fréquences radio et peuvent s'auto-organiser et coopérer pour fournir des services.

L'élargissement du domaine d'application des réseaux mobiles Ad hoc nécessite plus de sécurité pour assurer l'intégrité et la confidentialité des données qui circulent dans le réseau. En effet, les réseaux mobiles Ad hoc sont confrontés à de nombreux problèmes liés à leurs caractéristiques qui rendent les solutions de sécurité développées pour les réseaux filaires ou sans fil avec infrastructure inapplicables dans le contexte des réseaux mobiles Ad hoc. Parmi les vulnérabilités qui touchent les réseaux mobiles Ad hoc nous pouvons citer : L'absence d'infrastructure, la topologie réseau dynamique, la vulnérabilité des noeuds, la vulnérabilité du canal, les ressources limitées.

Pour remédier à ces vulnérabilités, plusieurs architectures de sécurité ont été proposées pour distribuer les clés de chiffrement ainsi que les certificats dans le but de sécuriser la communication entre les noeuds. Cependant, la plupart de ces architectures ne respectent pas les caractéristiques des réseaux mobiles Ad hoc : soit elles adoptent un schéma centralisé soit elles ne supportent pas la mobilité et la dynamique de la topologie des noeuds, soit elles ne possèdent aucun modèle de confiance dynamique et se limitent à un réseau fermé. L'objectif de notre travail est de faire une étude des différents protocoles d'établissement de confiance dans les MANETs (Mobile Ad hoc Networks) et par la suite définir une architecture sécurisée adapté aux réseaux sans fil ad hoc, pour cela notre mémoire commence avec une introduction générale et s'articule autour de trois chapitres.
Dans le premier chapitre nous donnons une généralité sur les réseaux sans fil, par la suite

nous définissons les réseaux Ad hoc, après nous citions quelques défis de sécurité dans les réseaux Ad hoc. A la fin un aperçu sur la gestion de confiance.
Le chapitre 2 est consacré à l'état de l'art sur la sélection des noeuds de confiance dans les réseaux mobiles. Nous présentons une étude et une analyse de quelques travaux liés à la gestion de confiance dans les réseaux mobiles.
Dans le chapitre 3, nous allons proposer un schéma qui permettra d'organiser le réseau en clusters afin de décentraliser le role de l'autorité de certification et offrir une gestion robuste et sécurisée des certificats en introduisant la cryptographie à seuil à base de RSA (Rivest-Shamir-Adleman) adaptée au contexte des MANET.
Et en fin nous concluons notre mémoire par une conclusion générale et perspectives.

# Chapitre I

# Généralités sur les réseaux sans fil

## Introduction

Ces dernières années, les réseaux ont connu un essor spectaculaire et s'imposent de façon indéniable, grâce à l'adoption des technologies de communication sans fil. Un succès dû principalement à la vulgarisation des équipements mobiles offrant plus de souplesse, plus de rapidité et moins de frais. Les réseaux mobiles sans fil peuvent être classés en deux catégories : les réseaux avec infrastructure ou cellulaires qui nécessitent généralement l'installation des stations de base et les réseaux sans infrastructure ou Ad Hoc caractérisés par leur dynamisme, facilité et rapidité de déploiement. Ces caractéristiques les rendent utilisés dans plusieurs applications à savoir la téléphonie, les applications militaires, les applications commerciales et la sécurité routière.
Dans ce chapitre nous allons décrire en premier lieu les réseaux sans fil et les réseaux Ad hoc, et les contraintes liées à ces derniers, et ensuite un aperçu sur la gestion de confiance et finir par une description de la cryptographie à seuil.

## I.1 Les réseaux sans fil

### I.1.1 Environnement sans fil

La croissance rapide des réseaux sans fil a permis l'émergence des communications sans fil. Les réseaux sans fil se sont développés essentiellement avec la téléphonie mobile. L'un des principaux avantages du déploiement des réseaux sans fil réside dans leur flexibilité d'emploi. En effet, ils permettent la mise en réseau d'unités sans fil évitant ainsi l'utilisation de câblages aux coûts onéreux ou impossibles à mettre en place à cause de la présence

d'unités mobiles par exemple. La recherche et le développement dans le domaine sans fil font des avancées considérables. Les utilisateurs sont passés en peu de temps de l'utilisation du GSM (Global System for Mobil communication) le standard de téléphonie mobile du 21ème siècle au GPRS (General Packet Radio Service) et actuellement à l'UMTS qui est la téléphonie mobile avec accès à internet (Universal Mobile Telecommunications System). Les réseaux sans fil utilisent les ondes radio pour communiquer. Ces dernières sont plus exposées aux perturbations et aux interférences que ne le sont les communications filaires [1].

### I.1.2 Les catégories des réseaux sans fil

Dans les réseaux sans fil, on peut distinguer, selon le périmètre géographique ou la zone de couverture, quatre catégories, illustrées sur la figure qui suit :

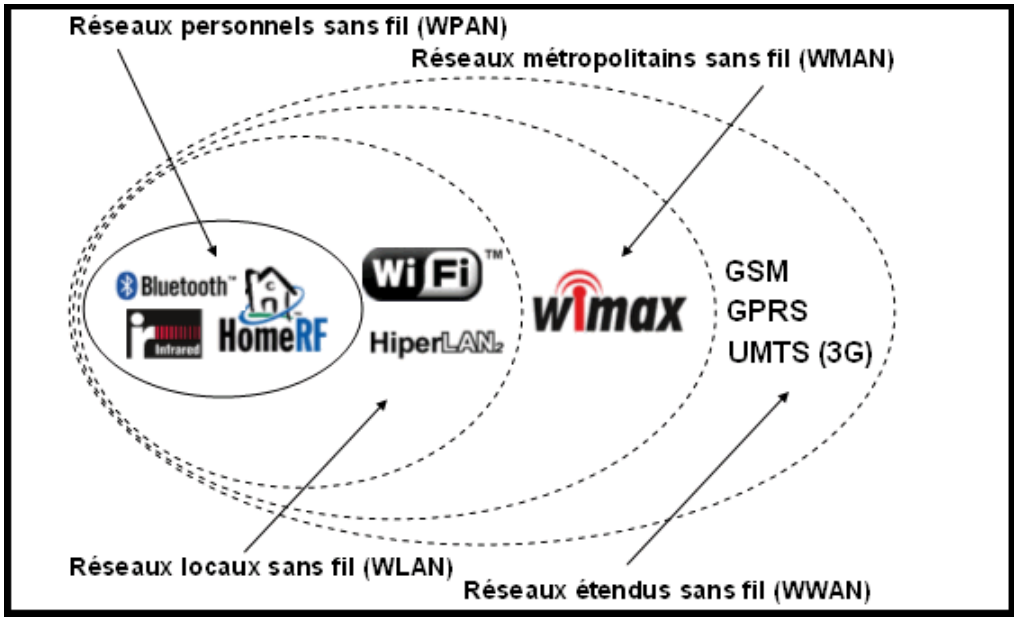


FIGURE I.1 – Catégories des réseaux sans fil [2].

#### A) Réseau personnel sans fil WPAN

Le réseau personnel sans fil (noté WPAN pour Wireless Personal Area Network) concerne les réseaux sans fil d'une faible portée, de l'ordre de quelques dizaines de mètres. Plusieurs technologies sont utilisées pour les WPAN, et la principale technologie est la technologie

Bluetooth, lancée par Ericsson en 1994, proposant un débit théorique de 1 Mbps pour une portée maximale d'une trentaine de mètres [2].

### B) Réseau local sans fil WLAN

Le réseau local sans fil (noté WLAN pour Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre-eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes : Le Wifi (ou IEEE 802.11), soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres [2].

### C) Réseau métropolitain sans fil WMAN

Le réseau métropolitain sans fil (WMAN pour Wireless Metropolitan Area Network) est connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication. La norme de réseau métropolitain sans fil la plus connue est le WiMAX (Worldwide Interoperability for Microwave Access), permettant d'obtenir des débits de l'ordre de 70 Mbit/s sur un rayon de plusieurs kilomètres [2].

### d) Réseau étendu sans fil WWAN

Le réseau étendu sans fil (WWAN pour Wireless Wide Area Network) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Les principales technologies sont [2] :

- **Le réseau GSM :** Noté GSM pour Global System for Mobile communications, autorise un débit maximal de 9,6 kbps, ce qui permet de transmettre la voix ainsi que des données numériques de faible volume, par exemple des messages textes (SMS, pour Short Message Service) ou des messages multimédias (MMS, pour Multimedia Message Service). Il s'agit d'un standard de téléphonie dit "de seconde génération" (2G) car, contrairement à la première génération de téléphones portables, les communications fonctionnent selon un mode entièrement numérique.

- **Le standard GPRS :** Noté GPRS pour General Packet Radio Service est une évolution de la norme GSM, ce qui lui vaut parfois l'appellation GSM++(ou GMS 2+). Etant donné qu'il s'agit d'une norme de téléphonie de seconde génération permettant de faire la transition vers la troisième génération (3G), on parle généralement de 2.5G pour classifier le standard GPRS. Le GPRS permet d'étendre l'architecture du standard GSM, afin d'autoriser le transfert de données par paquets, avec des débits théoriques maximums de l'ordre de 171,2 kbit/s (en pratique jusqu'à 114 kbit/s).

- **Le réseau UMTS :** Le réseau UMTS (universel mobile telecomminications system) vient se combiner aux réseaux déjà existants. L'UMTS est ainsi une extension du GPRS et fonctionne également en mode paquet. La vitesse de transmission offerte par les réseaux UMTS atteint 2 Mb/s.

- **Le réseau LTE :** Les réseaux mobiles LTE(Long Term Evolution) sont commercialisés sous l'appellation " 4G " par les opérateurs de nombreux pays, par exemple : Free Mobile en France, Algérie Télécom en Algérie etc. Le LTE utilise des bandes de fréquences hertziennes d'une largeur pouvant varier de 1,4 MHz à 20 MHz dans une plage de fréquences allant de 450 MHz à 3,8 GHz selon les pays. Il permet d'atteindre (pour une largeur de bande de 20 MHz) un débit binaire théorique de 300 Mbit/s en "liaison descendante" (downlink, vers le mobile). La " vraie 4G ", appelée LTE Advanced offrira un débit descendant pouvant atteindre ou dépasser 1 Gbit/s.

### I.1.3 Classification des réseaux selon l'infrastructure

Les réseaux sans fil peuvent être classifiés en deux catégories : les réseaux avec une infrastructure et les réseaux sans infrastructure [1].

#### A) Les réseaux avec infrastructure

Ce type de réseaux demande une infrastructure logistique et matérielle fixe. Cette infrastructure est représentée par un ou plusieurs points d'accès appelé(s) stations de base auxquelles sont connectées les unités mobiles. Ce type de réseau utilise un modèle de communication cellulaire (exemple les réseaux : GSM). Toutes les communications sont gérées par un ou plusieurs points d'accès (une station de base). Toutes les données qu'un hôte (unité mobile ou utilisateur mobile) peut émettre sont transmises au point d'accès (la station de base). Seul le point d'accès renvoie les données aux autres membres du

réseau. Plusieurs points d'accès peuvent être reliés ensemble (par câble ou par relais wifi). En d'autres termes une unité mobile du réseau ne peut pas communiquer directement avec une autre unité mobile donc une gestion centralisée des unités mobiles est nécessaire. L'unité mobile doit tout d'abord passer par le point d'accès de sa cellule [1].

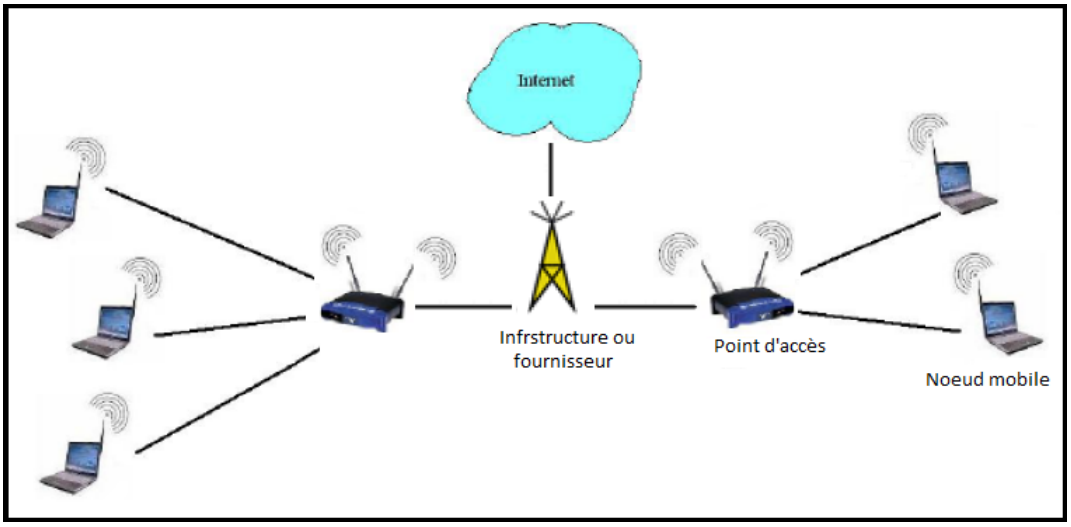


FIGURE I.2 – Réseau avec infrastructure [5].

### B) Les réseaux sans infrastructure

Dans ce type de réseaux (appelé aussi réseau ad hoc) il n'y a pas de gestion centralisée par un point d'accès (ou une station de base). Chaque membre du réseau retransmet les informations qu'il reçoit aux autres membres du réseau constituant ainsi un réseau point à point (Figure I.3). En d'autres termes c'est un réseau dans lequel chaque unité joue en même temps le rôle de client (hôte) et de point d'accès. Il n'y a pas d'infrastructure préexistante, c'est un ensemble d'unités inter-connectées à travers une interface sans fil sans administration ni support fixe [1].

## I.2 Les réseaux ad hoc

Un réseau ad hoc mobile aussi appelé MANET pour Mobile Ad hoc NETwork est une collection de nœuds mobiles connectés via des liaisons sans fil. Il n'a pas d'infrastructure fixe. Les nœuds mobiles dans ce réseau établissent un routage entre eux pour construire leur propre réseau de façon indépendante [4].

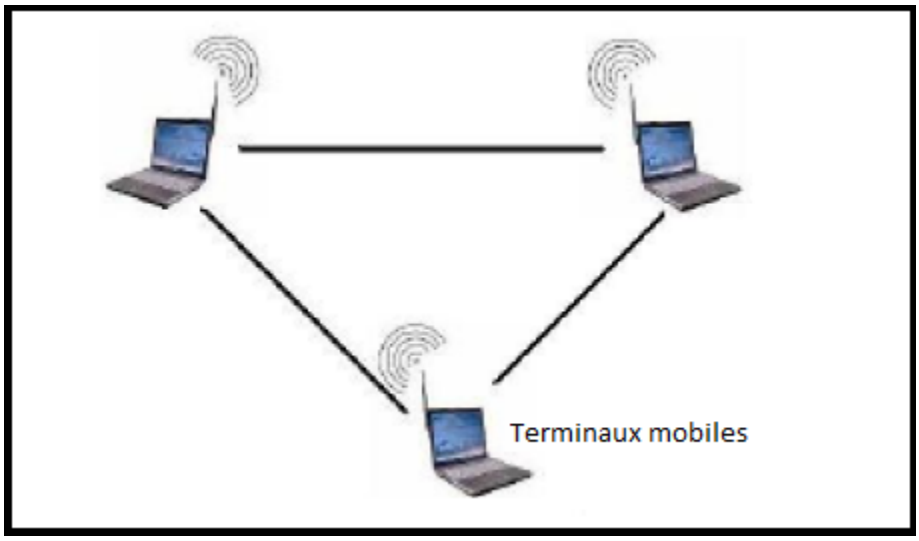


FIGURE I.3 – Réseau sans infrastructure [3].

### I.2.1 Description des réseaux ad hoc

Dans un MANET chaque nœud communique directement avec son nœud voisin. Pour communiquer avec des nœuds plus éloignés il lui est nécessaire de collaborer avec d'autres nœuds qui se chargeront de l'acheminement des données vers le nœud destination. Chaque nœud se comporte comme un routeur. Chaque nœud assure les tâches qui sont réalisées par l'administration centrale fixe dans les réseaux avec infrastructure. En effet, chaque nœud prend ses décisions en fonction de la situation actuelle du réseau car le réseau est formé dynamiquement et aucune pré-installation relative aux rôles de chaque nœud n'est requise au préalable. A un instant donné en fonction de la position des nœuds, de la configuration de leur émetteur-récepteur, des niveaux de puissances de transmission et des interférences entre les canaux il y a une connectivité sans fil qui existe entre les nœuds [1].

### I.2.2 Application des réseaux ad hoc

Aucune infrastructure préalable n'étant nécessaire à leur déploiement, les réseaux ad hoc peuvent être mis en place dans des environnements hostiles de manière simple et rapide. Leur flexibilité leur ouvre un large éventail d'applications. Les premiers travaux ont été effectués dans le domaine militaire. Leur utilisation s'est répandue dans beaucoup d'autres domaines : application commerciale, secourisme etc. Ils peuvent être utilisés dans toutes les situations où les infrastructures de communication sont absentes [1].

### I.2.3 Caractéristiques et contraintes liées aux réseaux ad hoc

- **Absence d'infrastructure :** Les MANET ne dépendent donc pas d'une infrastructure préétablie, chaque nœud opère comme un routeur indépendant. L'organisation du réseau doit donc être distribuée à tous les nœuds, ce qui rend la détection d'erreur et la gestion du réseau complexes [3].

- **Topologie dynamique :** Les nœuds se déplaçant arbitrairement, la topologie change fréquemment et de façon aléatoire. Cela implique que les routes entre les nœuds changent et des paquets peuvent ainsi être perdus [3].

- **Connexions variables :** Les nœuds peuvent avoir plusieurs interfaces radios, présentant des propriétés de débit ou de fréquences différentes. Ces variations donnent naissance à des connexions asymétriques [3].

- **Contraintes d'énergie :** Les batteries utilisées par les nœuds ne sont pas illimitées, les services supportés par ces nœuds sont donc restreints. C'est un problème d'autant plus important que les nœuds sont responsables du routage des paquets dans le réseau, ce qui consomme beaucoup d'énergie [3].

- **Nœud caché :** Ce problème survient quand une ou plusieurs stations ne peuvent se détecter (A et C sur la figure I.4), car elles se trouvent hors de leurs portées respectives, mais leurs zones de transmission ne sont pas disjointes. Une collision peut se produire quand les stations A et C envoient des informations à la station B simultanément.

  Un mécanisme a été pensé afin d'éliminer ce problème : avant l'envoi d'information, l'émetteur transmet un paquet RTS (Request To Send) au récepteur, lui annonçant ainsi une demande de transmission. Le récepteur renvoie un paquet CTS (Clear To Send) s'il est libre. Cette technique permet donc d'obtenir une certaine visibilité de la station cachée [3].

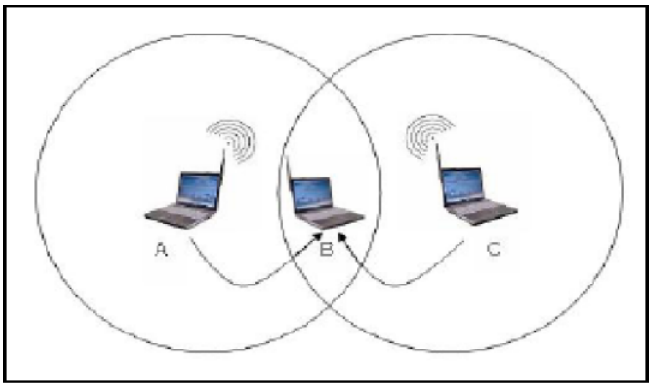


FIGURE I.4 – Exemple sur les nœud cachés [3].

- **Nœud exposé :** Ce problème survient quand un nœud veut établir une transmission avec un deuxième, mais doit la retarder car il y a une transmission en cours entre deux autres nœuds se trouvant dans son voisinage. La figure I.13 décrit un scénario typique.

  Supposons que les stations A et C peuvent entendre les transmissions de B, mais que A n'entend pas C (et vice-versa). Supposons aussi que B est en train d'envoyer des données Vers A et que, au même moment, C veut communiquer avec D. En suivant la logique CSMA/CA, le nœud C va commencer par déterminer si le support est libre. Á cause de la communication entre B et A, C trouve le support occupé et il retarde son envoi bien que celui-ci n'aurait pas causé de collisions [3].

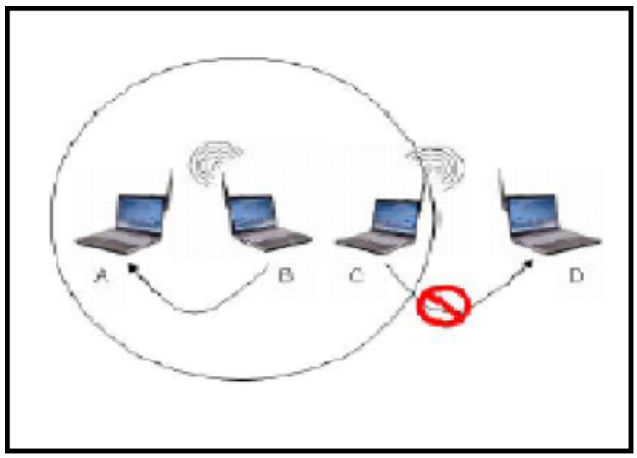


FIGURE I.5 – Exemple sur les nœud exposés [3].

- **Sécurité physique limitée :** Les réseaux mobiles ad hoc sont très sensibles aux at-

taques extérieures par rapport aux réseaux filaires classiques. Les données envoyées transitent par des équipements d'utilisateurs inconnus ce qui pose un problème de confidentialité et nécessite l'utilisation d'outils de cryptage et de sécurisation des données [5].

## I.3 Défis de sécurité

### I.3.1 Risques liés à la sécurité informatique

Afin d'appréhender la problématique de la sécurité dans les réseaux sans fil les concepteurs, les administrateurs et les utilisateurs de ce dernier doivent effectuée une analyse de risques afin de déterminer les parties critiques, en terme de sécurité. Cette analyse suit les étapes suivantes [6] :

— Détermination des fonctions et données sensibles des réseaux sans fil ad hoc.

— Recherche des exigences de sécurité par le biais des critères de sécurité que sont l'authentification, l'intégrité, la confidentialité, l'anonymat et la disponibilité.

— Études des vulnérabilités.

— Études des menaces et quantification de leur probabilité d'occurrence ou de leur faisabilité.

— Mesure du risque encouru en fonction des vulnérabilités mises en lumière et des menaces associées.

### I.3.2 Exigences de sécurité dans les réseaux sans fil

Déterminer les exigences de sécuritaire d'un système nécessite d'appréhender l'ensemble des contraintes qui pèsent sur ce système. Cette étape permet par la suite de quantifier les critères de sécuritaire. Les spécifications des réseaux sans fil sont multiples. On peut les repartir en six grands termes traitant des caractéristiques des nœuds, de la gestion de l'énergie, des caractéristiques du réseau, des technologies sans fil sous adjacentes, de la mobilité et de la configuration [7].

**• Caractéristiques des Noeuds**

- Les participants peuvent posséder des systèmes hétérogènes qui doivent s'interconnecter facilement.
- Certains éléments peuvent avoir de faibles capacités de calculs.

- **Gestion de l'énergie**

  - L'énergie doit être conservée au maximum pour éviter d'incessantes recharges du système qui diminuent sa mobilité - Les nœuds chercheront donc à se mettre en veille le plus souvent possible, ce qui provoquera alors une diminution de réactivité de l'ensemble du réseau [7].

- **Mobilité**

  - Les éléments étant fortement mobiles, leur sécurité physique est moins assurée que pour un poste de travail fixe, dans un bureau par exemple. Leur valeur marchande peut être d'importance non négligeable. - La topologie du réseau peut changer d'autant plus rapidement que les nœuds sont mobiles. - Des liens asymétriques peuvent se créer lorsqu'un élément muni d'un récepteur particulièrement sensible est capable de capter les émissions d'un autre nœud qui est hors de portée du premier élément [7].

- **Authentification / Intégrité / Confidentialité / Disponibilité**

  Coopérer au sein de tels réseaux présente un risque s'il n'y a aucun contrôle des participants. L'authentification des parties apparait donc comme la pierre angulaire d'un réseau sans fil ad hoc sécurisée. En effet, comment assurer une quelconque confidentialité et intégrité des messages échangés si, dès le départ, on n'est pas sûr de communiquer avec la bonne entité. Contrairement au réseau filaire, il n'est pas nécessaire de pénétrer dans un local physique pour accéder au réseau. Si l'authentification est mal gérée, un attaquant peut s'attacher au réseau sans fil et injecter des messages erronés. L'intégrité des messages échangés est donc une exigence importante pour ces réseaux.

  Une fois les parties authentifiées, la confidentialité reste un point important étant donné que les communications transitent via les airs et sont donc potentiellement accessibles à tout possesseur du récepteur adéquat.

  La disponibilité est une propriété difficile à gérer dans les réseaux sans fil étant données les contraintes qui pèsent sur ces réseaux.

# I.4 Aperçu sur la gestion de confiance et la cryptographie à seuil

## I.4.1 La gestion de confiance dans les réseaux mobile

Dans les réseaux sans fil les nœuds doivent s'organiser, collaborer pour organiser l'échange de l'information et l'acheminement du trafic, donc ces réseaux doivent posséder la capacité de s'autoconfigurer sans aucune intervention de l'extérieur, étant donné que ces réseaux sont sans infrastructure, et possèdent des exigences spécifiques en termes de sécurité, du fait de ses particularités : liens sans fil, contraintes d'énergie, limitation de la bande passante et de la puissance de calcul, connectivité non permanente d'un nœud avec les autres nœuds. Ces caractéristiques rendent les réseaux sans fil mobiles sophistiqués et capables d'opérer dans des conditions difficiles, mais aussi vulnérables aux différents problèmes de sécurité, comme la gestion des clés, distribution des certificats. Les solutions de sécurité doivent proposer certains services de base comme : l'authentification, le contrôle de l'intégrité, la confidentialité, la disponibilité et la non répudiation. La majorité des solutions de sécurité proposées dans la littérature sont basées sur la cryptographie symétrique ou asymétrique. Mais le problème majeur de ces solutions dans l'environnement des réseaux fil mobiles est la gestion et la distribution des clés. Proposer une seule autorité de certification (AC) pour tout le réseau n'est pas une solution souhaitable car cette conception est vulnérable aux attaques de type (DoS) sur l'AC, et en plus les nœuds dynamiques et autonomes [8].

## I.4.2 Cryptographie à seuil

Le partage de secret repose sur le concept de détention d'une portion d'une information secrète par plusieurs entités. La cryptographie à seuil permet le partage d'une valeur secrète S à un ensemble de n serveurs, sans que chacun d'eux connaisse sa valeur. A partir d'au moins k serveurs on peut reconstruire le secret ($k \leq n$). Si le nombre de serveurs est inférieur à k, aucune information n'est obtenue sur le secret S. La cryptographie à seuil s'exécute en deux étapes :

1) **Le partage du secret** :

Cette étape permet de mettre en commun un secret S entre n serveurs. On crée un polynôme F(x) avec des coefficients arbitraires en mettant $a_0 = S$.

On choisit ensuite publiquement n points distincts $x_i$, et on distribue secrètement 'a chaque serveur une part privée ($x_i$, $F(x_i)$). Le point xi pourrait être n'importe quelle valeur pu-

blique qui identifie le serveur si d'une manière unique. Pour simplifier la notation, on met $x_i$ = i, par conséquent les parts privées sont dénotées par F(1), F(2), ..., F(n) [10].
2) **La reconstruction du secret** :
Cette étape permet de reconstruire le secret S à partir d'un sous-ensemble de k parts : F(1), F(2), ..., F(k). Étant donné k points distincts (i, F(i)), il existe un polynôme unique F(x) passant par tous les points. Ce polynôme peut être calculé à partir des points (i, F(i)) en utilisant l'interpolation de Lagrange [10].

# Conclusion

Dans ce chapitre nous avons présenté les notions de base sur les réseaux sans fil, et cela en définissant les concepts rencontrés dans la littérature ou dans le modèle que nous avons étudié. Le chapitre suivant sera consacré à l'étude de quelques travaux récents réalisés dans le contexte de la sélection des nœuds de confiance dans les réseaux mobiles sans fil.

# Chapitre II

# État de l'art sur la sélection des nœuds de confiance dans les réseaux mobiles

## Introduction

Les réseaux mobiles annoncent les réseaux de communication du futur où la mobilité en est l'idée maîtresse. Ces réseaux devront être capables d'interconnecter des mobiles, à la volée et de bout en bout, pour leur fournir des services de manière omniprésente. Ils sont de ce fait plus vulnérables à de nombreux types d'attaques. Leur succès dépendra sans aucun doute de la confiance qu'ils apporteront à leurs usagers. Les modèles de confiance traditionnels ne répondent pas aux nouvelles exigences de tels réseaux dont les caractéristiques les rapprochent de plus en plus des modèles sociaux. Dans le chapitre ci-présent nous avons étudié les différentes solutions proposées pour assurer la sélection des noeuds de confiance dans les réseaux mobile, afin d'en faire un critère de base que nous utiliserons par la suite dans notre proposition, pour ce faire, nous avons commencé ce chapitre par des définitions des critères d'analyse des différentes approches proposés, ensuite nous avons fait une classification des solutions proposés pour enfin finir par une synthèse qui englobe les avantages et les désavantages de chaque solution proposé.

# II.1 Critères d'analyse des solutions existantes

## II.1.1 Consommation d'énergie

Les nœuds d'un réseau mobile peuvent être sévèrement limités en termes de mémoire, CPU ainsi que de capacités énergétiques. De ce fait les protocoles du service de certification doivent être à moindre consommation d'énergie [10].

## II.1.2 Scalabilité

Les opérations de service de clé et certification devraient finir d'une façon opportune en dépit d'un nombre variable de nœuds et de densité de nœuds. La fraction de la bande passante disponible occupée par le trafic de gestion de réseau devrait être maintenue aussi réduite que possible. N'importe quelle augmentation du trafic de gestion réduit la bande passante disponible pour des données de charge utile. Par conséquent, le passage à l'échelle des protocoles de gestion de certification est crucial [10].

## II.1.3 Disponibilité

Dans les réseaux ad hoc, il est difficile de maintenir une autorité de confiance centrale fixe pour tout le réseau, à cause des déconnexions et ruptures de liens radio fréquente dues principalement à la mobilité des nœuds et leurs ressources limitées. Par ailleurs, une telle autorité centrale serait un point de défaillance singulier, ce qui entraverait la disponibilité des services de sécurité. Ainsi, l'une des exigences fondamentales est que le service de certification puisse assurer la disponibilité du service malgré les éventuelles déconnexions voir partitionnement du réseau [10].

## II.1.4 Robustesse

La robustesse est une condition nécessaire pour tout système de sécurité. Un système de gestion de clés robuste doit assurer une tolérance aux intrusions cela signifie qu'un système de sécurité ne devrait pas succomber à un simple, ou à quelques nœuds compromis. Le système de gestion de clés devrait survivre en dépit des attaques de déni de service et des nœuds indispensables. Les opérations de gestion de clés devraient pouvoir être accomplies en présence des nœuds compromis et des nœuds montrant le comportement malveillant [10].

### II.1.5 Révocation

la révocation d'un certificat consiste à annuler le certificat avant la date de son expiration. Après la révocation le certificat n'est plus utilisable, le certificat change de statut, il passe de valide à révoqué.

### II.1.6 Renouvellement

Renouvellement concrne le renouvellemnt des clés privés si elles sont divulgué et les certificats lors de leur expiration.

## II.2 Les techniques de gestion de confiance

Dans les réseaux mobiles ad hoc, un nœud peut faire confiance à un autre nœud seulement si ce dernier se comporte d'une façon correcte. Cette définition a donné naissance à deux modèles de confiance :

### II.2.1 Le modèle de confiance à base de coopération

Qui se base sur la réputation d'un nœud, qui augmente quand ce dernier effectue correctement les taches qui correspondent au bon fonctionnement du réseau, tel que le routage. Chaque nœud observe le comportement de ses voisins et déclare une accusation si l'un de ses voisins se comporte d'une manière incorrecte.

### II.2.2 Le modèle de confiance à base de certification

Dans cette catégorie de modèles la mise en œuvre de la confiance est basée sur la notion de certificat. Un nœud peut faire confiance à un autre si et seulement si ce dernier est certifié par un tiers nœud auquel le premier fait confiance. Ainsi, les nœuds utilisent la vérification des certificats pour établir des liens de confiance avec les autre nœuds. En effet, un certificat est une structure de données dans laquelle une clé est liée à une identité (et éventuellement à certain autre attributs) délivrée par une une tierce partie de confiance. Si cette dernière estime qu'un nœud est digne de confiance, elle lui de délivre un certificat qui va lui permettre de prouver sa légitimité envers les autres nœuds du réseau.

### A) Infrastructure à clé publique non auto-organisée

Elle permet de distribuer les fonctionnalités de AC parmi les différents nœuds du réseau en utilisant l'approche de la cryptographie à seuil. Il existe deux possibilités pour distribuer AC. La première est appelée " AC partiellement distribuée " : seuls certains nœuds spécifiques sont capables d'assumer le rôle de AC. La deuxième possibilité est appelée " AC complètement distribuée " : tous les nœuds ont la possibilité de jouer le rôle de AC.

#### A.1 Autorité de certification partiellement distribuée

Pour des raisons de sécurité, la distribution de la fonctionalité de AC est limitée à certains noeuds nous citons certains protocoles basés sur la distribution partielle de AC :

— **Solution de Zhou et Haas**

Zhou et Haas [11] proposent un protocole nommé Securing Ad hoc Networks, dans lequel les auteurs présentent un service distribué de gestion de clé publique pour les réseaux ad hoc, qui s'appuie sur la cryptographie à seuil. Ils ont proposé l'existence d'une autorité de certification centrale distribuée sur un ensemble de serveurs suivant un schéma de cryptographie à seuil (n,t). L'autorité de certification possède une paire de clé publique / privée (K/k), qui est utilisée pour vérifier / signer les certificats pour les clés publiques des nœuds clients du réseau. Ils ont supposé encore que tous les nœuds connaissent la clé publique K du AC et font confiance à tous les certificats signés par la clé privée correspondante k, cette clé n'est connue par aucun nœud du réseau. Les nœuds clients peuvent envoyer des requêtes pour récupérer les clés publiques. Le Schéma (n, t+1) de cryptographie à seuil permet à n nœuds spéciaux appelés serveurs de partager la capacité de signer les certificats partiels, la clé privée de AC est divisée en n secrets partagés sur n serveurs (s1,s2,....sn) présents dans le réseau ad hoc, chaque serveur est capable de produire une signature partielle en utilisant sa part privée. Pour créer un certificat, chaque serveur génère une signature partielle pour le certificat et l'envoie au combinateur, qui doit rassembler au moins (t+1) signatures partielles correctes pour pouvoir générer la signature valide pour le certificat. L'application de la cryptographie à seuil (n,t+1) garantit que le système peut tolérer un certain nombre $t < n$ de serveurs compromis dans le sens que (t+1) de signatures partielles correctes sont nécessaires pour générer une signature valide, avec au plus de t serveurs compromis, le combinateur peut encore générer des certificats valides. Le combinateur peut vérifier la validité de la signature partielle des serveurs, si l'un d'eux envoie une signature partielle incorrecte, le combinateur la rejette et continue à rassembler les signatures jusqu'à ce qu'il arrive à construire une signature

valide pour le certificat et transmettre ce dernier au nœud client. Pour s'adapter aux changements topologiques et assurer une meilleure protection du réseau, un système de rafraichissement permet aux serveurs de renouveler leurs secrets qui sont utilises pour générer des certificats.

Zhou et haas ont proposé une solution, ou ils emploient un schéma à seuil (n,t) pour distribuer les services d'autorité de certification à un ensemble spécial de nœuds. Le système contient trois types de nœuds : nœuds client, serveurs, et combinateurs. Quand un nœud souhaite renouveler son certificat, il doit demander le renouvellement auprès d'un minimum de t serveurs. Cependant, les auteurs n'ont pas explicité diverses opérations. Entre autre, comment un nœud exécute le protocole de certification avec t serveurs quand les serveurs sont dispersés dans un large réseau ? Et comment maintenir au moins t serveurs disponibles pour chaque nœud client ? Et comment les nœuds localisent les serveurs. Également, les auteurs n'ont pas discuté la valeur optimale du seuil t, qui influence fortement sur deux paramètres : la disponibilité et la robustesse du service de certification. En effet, si la valeur de t est petite, ce sera relativement moins difficile de compromettre les parts privées du service de certification. Dans ce cas, la robustesse du système diminue, mais la disponibilité du service devient de plus en plus forte. Alors que si la valeur de t est grande, l'adversaire devra compromettre un nombre important de serveurs pour pouvoir compromettre la clé privée de certification, ce qui rend le système plus robuste, mais affaiblit la disponibilité du service de certification puisque les nœuds devront solliciter un nombre important de serveurs pour pouvoir satisfaire leurs requêtes.

— **Protocle Wu et al**

Une méthode permettant de distribuer la confiance sur un ensemble de nœuds appelés serveurs est présentée par Wu et al [16]. En effet, les auteurs proposent Secure and efficient Key management (SEKM) adapté aux réseaux mobiles ad hoc. SEKM construit une infrastructure publique PKI en appliquant un schéma de secret en utilisant un groupe de serveurs pour les multicast. Deux types de nœuds sont présents dans le réseau, les serveurs et les non-serveurs.

La communication entre les serveurs, appelé aussi groupe multicast se fait en diffusant des requêtes de recherche des autres serveurs et le but de cette diffusion est d'élire les nœuds réguliers de tous les serveurs par le plus court chemin. La topologie des serveurs forme une structure de maille permettant de mieux extraire les capacités du réseau : plusieurs chemins sont possibles entre les serveurs, ce qui diminue le cout de la recherche d'un serveur si un chemin devient invalide. Une étape aussi

importante consiste à rafraichir le secret partagé. Dans ce cas t serveurs parmi le groupe multicast initialisent une étape de mise à jour du secret partagé. Ces serveurs actifs génèrent de nouvelles portions, puis ils envoient aux serveurs correspondant. La formation, la maintenance du groupe multicast et du secret partagé serviront pour la signature et la mise à jour de certificat à clé publique, un certificat expire après un laps de temps. Il suffit de regrouper t certificats partiels pour reconstruire un certificat valide. Un nœud attache un ticket à sa requête de mise à jour et l'envoie à t (c'est une marge de sécurité s'il y'a corruption de certains certificats partiels). Un certificat peut être révoqué pour de nombreuses raisons :

- Un noeud refuse de générer des certificats partiels.
- Un serveur compromis génère des portions incohérente.
- Un serveur relais se conduit mal face à la retransmission des requêtes/réponses pour la maintenance du groupe multicast.

Par conséquent le serveur marque le certificat du nœud suspecté. Le certificat contient aussi un compteur TTL (Time To live). Le compteur décroit avec le temps. S'il atteint un certain seuil, les t serveurs peuvent révoquer le certificat, l'ajouter à une liste de révocation des certificats CRL (Certificate Revocation List) et la diffuser sur tout le réseau.
SEKM construit une infrastructure à clé publique PKI en utilisant la technique de partage de secret. Certain des noeuds du réseau sont définit serveurs, génèrent les certificats partiels pour construire les certificats valides. La révocation du certificat se fait pour plusieurs raisons par exemple si un serveur est corrompu et génère des portions incohérente.

— **Protocole de Chang et al**

Chang et al [15] ont proposé une approche d'authentification sécurisée en deux étapes pour les MANET de multidiffusion. Tout d'abord, un modèle de confiance en chaîne de Markov est proposé pour déterminer la valeur de confiance (TV) (Trust value) pour chaque voisin d'un seul saut. Le TV d'un nœud est analysé à partir de sa confiance antérieure qui a été effectuée dans ce groupe. Le modèle de confiance proposé est éprouvé en tant que modèle de chaîne Markov à temps continu ergodique. Deuxièmement, le nœud avec le TV le plus élevé d'un groupe sera sélectionné en tant que serveur CA qui gère La table de confiance du groupe, le nombre de fois qu'un nœud agit en tant que CA est définis par NCA. Pour augmenter la fiabilité, le nœud

avec le deuxième TV le plus élevé sera sélectionné en tant que serveur BCA (CA de secours) qui prendra le rôle de CA lorsque CA échoue.
Le modèle d'analyse de la chaîne de Markov est utilisé pour déterminer le TV de chaque nœud dans un groupe de multidiffusion. La première phase se compose de quatre étapes :

— Étape 1. Création de la relation de confiance entre les membres.

— Étape 2. Définition des événements de confiance pour transiter l'état de confiance d'un nœud.

— Étape 3. Déterminez le TV de chaque membre.

— Étape 4. Analyser les frais généraux de l'établissement de confiance.

Ensuite, la phase de gestion de CA, d'authentification, et de gestion des clés.
Le modèle adopte l'infrastructure de clé publique, qui repose sur L'algorithme de cryptage RSA. le Modèle de confiance, fournit ainsi plusieurs procédures de confiance sécurisées pour empêcher les intrusions :

1. Phase initiale du groupe :
Initialement un nœud est choisi en tant que chef de groupe et en tant que CA provisoire.

2. Phase de jointure d'un nœud :
Lorsqu'un nœud veut rejoindre un groupe, il initialise un JoinReq Message et effectue l'authentification de confiance.

3. Phase de départ des membres :
Lorsqu'un membre veut quitter un groupe, il initialise un Message LeaveReq. Ensuite, le nœud CA exécute une Régénération de clé de groupe pour garantir la sécurité du groupe.

4. Phase de sortie de CA :
Lorsque le nœud CA veut quitter un groupe, il notifie le nœud BCA Pour être le

nouveau nœud CA.
5. Phase de sortie de BCA :
Lorsque le nœud BCA veut quitter un groupe, il informe le CA de sélectionnez un nouveau BCA.

6. Phase de départ du leader de groupe :
Dans les MANET de multidiffusion, un chef de groupe (c'est-à-dire l'expéditeur) est le premier membre qui initialise le groupe. Si le chef du groupe quitte le groupe, le groupe disparaît. Dans la groupe-leader Phase, quand le leader décide de quitter le groupe il envoie un message LeaderLeave à tous les membres du groupe, Le message est chiffré par la clé privée KR. Seuls les membres du groupe peuvent décrypter le message en utilisant la clé publique KP. Ainsi, les propriétés de l'intégrité, l'authenticité, la confidentialité et la non-répudiation sont satisfaites.
L'approche de Chang et al réalise une authentification sécurisée dans les MANET multicast. Les résultats ont démontré qu'un nœud doté d'un TV élevé produit un NCA élevé et un NREJ (Nombre de rejets ) faible, et vice versa.
Les auteurs ont aussi démontré que leur protocole pouvait résister à plusieurs attaques comme :
L'attaque marche-arrêt quand un nœud malveillant alternativement accomplit des bonnes et mauvaises manières, l'attaque des nouveaux arrivants, quand un mauvais nœud tente d'enlever ses enregistrements de mauvaise confiance en se réenregistrant comme un nouveau nœud qui n'a pas encore rejoint le groupe, La fausse attaque, quand un nœud malveillant utilise un faux ID de nœud pour attaquer le groupe.

— **Protocole de Jenitha et Jayashree**
Jenitha et Jayashree [4] ont amélioré le mécanisme de sélection des nœuds de confiance qui participera au processus de génération de clés pour la communication de groupe sécurisée dans un environnement distribué. La sélection est proposée en deux étapes : La première étape adopte la technique de regroupement pour identifier les nœuds dignes de confiance à travers le réseau et la deuxième phase utilise l'approche de recul dans le problème de N-Queen pour réduire la liste des nœuds fiables et pour s'assurer que les nœuds sont répartis sur tout le réseau. Cette distribution de nœuds aide à la génération des clés distribuées par le biais du protocole de partage de clé secrète. Jenitha et Jayashree ont proposé un schéma distribué pour une sélection de nœud de confiance efficace dans les MANET. Les nœuds sont regroupés dans des

clusters différents, les nœuds dignes de confiance dans les clusters sont sélectionnés en fonction du problème de N-Queens, la clé secrète de groupe est calculée en combinant les actions obtenues auprès des différents actionnaires. Les fonctionnalités sont : la formation des clusters, la sélection des nœuds de confiance, la génération de clés, l'extraction des clés et la révocation des clés.

Les nœuds dignes de confiance sont sélectionnés en fonction du rapport d'envoi et de réception des paquets.

La formation des clusters : Les nœuds dans un cluster sont similaires et les noeuds dans des clusters différents sont différents. Les clusters sont formé s en fonction du temps de calcul de la tête du cluster qui est sélectionnée de manière aléatoire en fonction de la faible mobilité, du rapport d'envoi, de réception des paquets, de l'énergie et de la connectivité. La sélection des nœuds de confiance : La valeur de confiance des nœuds est calculée par rapport au nombre d'envoi et de réception des paquets, retard et aussi le nombre de paquets manqués. Après la sélection des nœuds dignes de confiance pour une communication de groupe, ce fait la sélection d'un sous-ensemble de manière à ce que les nœuds de confiance soient distribués de manière égale. Pour la formation des sous-ensembles, les nœuds sont sélectionnés en fonction du problème de N-Queen. Dans le problème de N-Queens, pas deux reines ne partagent la même ligne, colonne ou diagonale. De la même manière, les nœuds qui se situent dans la plage de la cellule sont sélectionnés de sorte que différents sous-ensembles sont formés en fonction du nombre de façons possible pour placer les reines dans la cellule. Enfin, le sous-ensemble qui a le nombre maximal de nœuds de confiance est sélectionné. Ce processus réduit les attaques possibles en phase d'extraction principale. Lorsque les nœuds de confiance sont distribués dans la nature, il sera facile pour un nouveau nœud de partager les membres fondateurs et de générer la clé. Jenitha et Jayashree ont proposé un schéma distribué pour la sélection des nœuds de confiance basée sur le problème des N-Queen. Ils ont démontré que le schéma proposé pourrait réduire le coût et améliorer la sécurité des réseau mobile de manière significative. Ainsi, le travail proposé augmente considérablement la sécurité du système. Cependant les auteurs pourraient ce basé un peu plus sur la cryptographie afin de fournir une communication plus sûre.

| Modèle | Disponibilité | Ressources | Renouvellement | Révocation | Robustesse |
|---|---|---|---|---|---|
| Zhou et Haas | Moyenne | Les serveurs stockent les certificats | Oui | Oui | Non |
| Wu et al | Moyenne | Les serveurs sont puissants en termes de capacité de traitement. Le reste des nœuds maintient seulement une table de routes vers les serveurs | Oui | Oui | Oui |
| Chang et al | Élevée | L'analyse de la confiance des nœuds voisins, et la procédure de départ du nœud CA génère un grand trafic. | Oui | Oui | Oui |
| Jenitha et Jayashree | Élevée | Les auteurs ont démontré que leurs modèle réduit les coûts | Non | Oui | Oui |

TABLE II.1 – Comparaison des modèles à autorité de certification partiellement distribuée

### A.2 Autorité de certification complètement distribuée

Contrairement aux modèles précédents qui fixent un ensemble de serveurs, dans ce modèle, le service de certification est distribué sur tous les noeuds du réseau, comme exemples de protocole de cette approche :

— **Protocole de Raghani et al**

Dans [9], Raghani et al proposent un protocole Dynamic support for distributed certification authority in Mobile Ad hoc Networks, ils ont présenté une autorité de certification complètement distribué où le service de certification est distribué sur tous les nœuds du réseau. Cependant, afin d'assurer une forte disponibilité de ce service, ils ont proposé de maintenir la valeur du seuil t dynamique, ajustable systématiquement selon le nombre moyen de voisins directs de chaque nœud du réseau. Chaque nœud exécute périodiquement un protocole de découverte de voisinage, calcule le nombre de ses voisins directs, et envoie cette information à un nœud spécial, nommé leader. Ce dernier, en recevant le nombre de voisins directs de chaque nœud spécial, calcule le degré moyen d du réseau. S'il est inférieur à la valeur actuelle du seuil t, le leader recalcule une nouvelle valeur de t. Quand le leader décide de changer la valeur du seuil, il diffuse cette dernière à tous les nœuds du réseau. Ensuite les nœuds mettent à jour leurs parts privées correspondantes à la nouvelle valeur de t.
Raghani et al proposent un schéma de AC distribué où un nœud obtient son certificat en communicant avec ses voisins à un seul saut. Avec une telle approche, quand le degré d'un nœud dans le réseau diminue au-dessous du seuil, il y a une augmentation substantielle de la latence du service de certification. Pour résoudre ce problème, le schéma proposé offre un support dynamique pour une AC distribuée en lui permettant de modifier dynamiquement la valeur du seuil en cas de besoin ce qui permet de réduire la latence du service de certification. La disponibilité du service de certification est amélioré grâce à la flexibilité du seuil t. Cependant, cette solution provoque une charge importance de transmission. En effet, à chaque changement du degré moyen du réseau, ce qui est fréquent dans le réseaux ad hoc, une nouvelle valeur de t est diffusée. En plus, cette opération sera suivie par le recalcul des parts privées de chaque nœud, ce qui implique également une charge importante et périodique de traitement. Il reste à signaler qu'il existe un autre cas très important qui nécessite le changement de la valeur du seuil, qui est lié à la robustesse du service de certification. Par exemple, quand le nombre de nœuds malveillants augmente dans le réseau, la valeur du seuil doit être augmentée, afin de rendre le système résistible face aux faux certificats partiels générés. Une telle mesure n'a pas été envisagée dans ce modèle.

— **Protocole de Zhu et al**

Zhu et al [13] ont proposé une technique Efficient and Robust Key Management for Large Mobile Ad Hoc Networks appelée aussi AKM (Autonomous Key Management) qui fournit un service de AC complètement distribué en se basant sur la cryptographie à seuil. Lorsque le nombre de nœuds augmente, le protocole introduit une hiérarchie de clés secrètes partagées, pour s'adapter aux MANET avec un grand nombre de nœuds. Ce schéma permet d'établir des certificats avec différents niveaux de sécurité. La clé privée de la AC est initialement partagée par un groupe de nœuds voisins, ensuite chaque nœud des N voisins choisit une valeur secrète Si, et distribue les parts partiels de cette valeur secrète aux autres voisins. La somme des valeurs secrètes individuelles S =($S_1$+$S_2$+$S_3$+...+$S_n$) représente la clé privé de la AC. Les nœuds $N_1$...$N_6$ et leurs parts secrètes (clés partielles f($N_i$)), peuvent être vu comme des niveaux d'une structure arborescente. La probabilité de la compromission augmente avec l'accroissement du nombre des nœuds possédants les clés partielles de la clé privée de la AC. Ainsi lorsque le nombre de possesseurs de clés partielles atteint un certain niveau, les nœuds sont divisés en petits groupes pour installer une nouvelle valeur secrète de ce groupe. Les certificats signés par un groupe situé au bas niveau de l'arborescente a moins d'assurance que ceux signés par un groupe situé au bas niveau. Avant de se diviser, les nœuds $N_1$...$N_6$ possèdent les clés partielles f($N_1$)...f($N_6$) de la clé privée de la CA. Supposons que $N_1$,$N_2$,$N_3$ décident de former un nouveau groupe et $N_4$,$N_4$,$N_6$ un autre, $N_1$ distribue une part de la valeur secrète f($N_1$) aux autres nœuds dans le même groupe, les autres font la même chose, la nouvelle valeur privée qui sera partagée par les nœuds $N_1$, $N_2$, $N_3$ est la somme de leurs parts S' = f($N_1$)+f($N_2$)+f($N_3$). Lorsque le nombre de nœuds appartenant à la même région (groupe) atteint le seuil spécifie, ce groupe sera encore divisé. Cette technique augmente la robustesse et la tolérance aux intrusions au prix du cout des communications, les nœuds sont supposés être capable de quitter un groupe et appartenir à un autre lorsqu'il se déplace d'une région à une autre dans le réseau. Implicitement, les nœuds doivent maintenir une vue sur l'hiérarchie de clé et être capables de détecter les frontières de la nouvelle région. Cette technique gère les MANET qui peuvent changer en fonction de l'augmentation ou diminution de nœuds, et les différentes parties de la structure ont la liberté d'établir les configuration appropriées pour faire face à différents niveaux de risques. AKM permet également, de délivrer des certificats avec différents niveaux de sécurité et aussi avec l'aide d'un nombre relativement restreint de nœuds.

| Modèle | Disponibilité | Ressources | Révocation | Scalabilité | Robustesse |
|---|---|---|---|---|---|
| Raghani et al | Élevée | Un nombre de message important transmis périodiquement pour les pour valeurs de seuil suivi par une mise à jour, donc une charge importante de calculs | Oui | Non | Oui |
| Zhu et al | Élevée | Une charge importante de transmission et de calculs afin de maintenir la structure d'arborescence qui peut changer en fonction de l'augmentation ou diminution de nœuds. De nouvelles portions impliquant une charge importante de calculs. | Oui | Oui | Oui |

TABLE II.2 – Comparaison entre les modèles à autorité de certification complètement distribuée.

### B) Infrastructure à clé publique auto-organisée

Un réseau mobile Ad hoc est dit complètement auto-organisé du point de vue de la sécurité, si et seulement si il n'a aucune infrastructure, aucun serveur centralisé et aucun secret partagé. L'approche PGP (Pretty Good Privacy) est la plus répandue dans la PKI auto-organisé sur internet. Le principe de cette approche est que tout utilisateur puisse certifier (signer) la clé publique d'un autre utilisateur s'il lui fait confiance. L'ensemble des signatures générées par les uns et les autres forment des relations de confiance entre les entités du réseau. Parmi les protocoles auto-organisés basés sur cette approche :

— **Protocole de Maheswaran et al**

L'approche décrite dans [14] se base sur le modèle hiérarchique, et il est décentralisé du fait que les MANET ne peuvent pas contenir d'entité centralisée. Il permet aux nœuds des MANET de retirer les certificats des nœuds malicieux, il se base sur l'utilisation de l'approche self-healing qui permet l'observation des nœuds, et exige aux participants du protocole de compléter et de maintenir des données qui se réfèrent à la diffusion des informations d'accusation de tous les nœuds du réseau. La collection de données est utilisée pour assigner une valeur à la fidélité d'un nœud. Les accusations pèsent par rapport au degré de fidélité de l'accusant, plus son poids de fidélité est grand, plus le poids de son accusations est grande et vice versa. Le certificat d'un nœud est révoqué si la valeur de la somme de poids des accusations faites contre lui est plus grande à un seuil configurable. Le but de ce protocole est que les nœuds ont tous les informations consistantes en ce qui concerne le statut des certificats de leur réseau.

Les auteurs ont proposé un protocole se basant sur le modèle hiérarchique pour assurer l'authentification, il utilise des valeurs hachées générées par des fonctions de hachage. Le processus d'identification des nœuds malicieux n'est pas évoqué dans ce protocole. L'avantage est que ce protocole est approprié aux MANET par ce qu'il est décentralisé. Il permet aux nœuds des MANET d'annuler les certificats des nœuds malicieux et d'empêcher les nœuds malveillants de pouvoir employer les accusations injustifiées qui annulent les certificats des nœuds bienveillants. La complexité du protocole est linéaire.

Comme le protocole est basé sur le nombre de nœuds malicieux, quand ce nombre est plus grand que le nombre de nœud bienveillants, le protocole devient non résistant aux attaques et inefficace pour retirer les certificats des nœuds malicieux.

— **Protocole de Omar et Al**

Omar et al [10], ont proposé un modèle appelé Reliable and fully distrubuted trust model for mobile ad hoc network. Ce modèle permet aux nœuds de générer, stocker, distribuer leurs certificats. Tous les nœuds ont un rôle identique, de telle sorte qu'aucune fonction spéciale n'est assignée à un ensemble de nœuds. Dans ce modèle, la paire de clés $k_i^{-1}/k_i$ (privé/publique) de chaque utilisateurs i est créée localement par l'utilisateur lui même, l'authentification des clés publiques est établie à travers la vérification des chaines de certificats et aussi dans ce modèle les certificats sont stockés et distribués par les nœuds mobiles au lieu d'utiliser des serveurs centralisés. L'idée principale de ce modèle est l'intégration d'un schéma de cryptographie à seuil (n,t) au graphe de confiance. Pendant l'initialisation du système, chaque nœud u reçoit une part privée $S_i$ de la clé privé du service de certification, noté par $k_{sys}^{-1}$ qui est maintenue secrètement par l'administrateur du système. Dans ce modèle, au lieu d'utiliser les clés privées pour la signature des certificats, les utilisateurs utilisent leurs parts privées en générant des certificats partiels. La génération de ces derniers va permettre de produire un graphe de confiance (graphe de confiance partielle). Cette nomination vient du fait que les nœuds du réseau ont un pouvoir limité de certification, de telle sorte que si un nœud A estime que B est digne de confiance, il lui délivre seulement un certificat partiel. Ce certificat ne sera pris en considération que si le nœud B est estimé digne de confiance auprès d'au moins t nœuds. Ainsi pour authentifier le nœud B , on combine l'ensemble des certificats partiels qu'on lui a délivrés. Les auteurs ont mis au point un système de collection de certificats partiels où périodiquement chaque paire de voisins s'échange les certificats partiels qu'ils détiennent. Ainsi, les nœuds sont entièrement indépendants des nœuds collaborateurs en collectant les certificats partiels directement à partir de leurs dépôts.
Le modèle proposé par Omar et al est basé à la fois sur les graphes de confiance et la cryptographie à seuil. Ce modèle a plusieurs avantages :
- Le service est complètement autonome, et qui supporte la mobilité et la défaillance des nœuds.
- Le service de certification est toujours disponible même si le réseau subit des partitionnements s'il y ait au moins k nœuds dans sa partition. - Le processus d'authentification permet la combinaison de tous les certificats partiels, et ainsi suspendre ceux qui ne vérifient pas le schéma de cryptographie à seuil. Ceci permet de résister aux comportements malveillants de certains nœuds qui délivrent des certificats partiels corrompus, ce qui met en valeur le critère de la robustesse. Cependant les auteurs n'ont pas discuté la révocation des certificats et renouvellement des parts privées.

— **Protocole de Jin-Hee et al** Jin-Hee et al [12] ont proposé un modèle de gestion de confiance à base de clé publique CTPKM pour les réseaux mobile ad hoc sans utiliser une autorité de confiance centralisé CA. En considérant 3 dimensions de confiance différente à savoir la compétence, l'intégrité et le contacte social, CTPKM permet à un nœud de prendre des décisions quand il interagit avec d'autre nœud. CTPKM est un algorithme de distribution de clés, ou chaque nœud génère sa paire de clés périodiquement, mais cette paire doit être certifiée par une tierce partie de confiance qui génère le certificat de la clé publique. et puisque CTPKM n'assumais pas l'existence d'une tierce patrie de confiance, chaque nœud se doit de trouver un nœud de tierce partie digne de confiance parmi ses 1-saut voisins, appelé "neighborhood trustworthy certifier NTC", qui peut certifié les clés auto générer, à condition qui est une certaine confiance entre les deux. le minimum de conditions pour être un NTC est d'avoir une valeur de confiance supérieur au seuil de confiance donné. Après qu'un nœud est obtenue son certificat, il diffuse la clé publique avec le certificat à un sous-ensemble de ses voisins à un saut dont les valeurs de confiance ne sont pas inférieures à T pour les trois composantes de confiance. CTPKM est conçu sur la conception optimale du protocole TC (trust chain) chaine de confiance qui est mesuré par les performances suivantes :
-Fraction des clés publiques correctes (efficacité) (F) : Moyenne des clés valide par-rapport au totale des clés maintenues par tous les nœuds du réseau.
-Service de disponibilité (A) : La période de temps moyen qu'une clé valide d'un nœud est maintenue par les autre nœuds.
-le risque d'informations (R) : Indique le nombre de paquets de transmission moyen en utilisant une clé compromise durant toute une session.
-Le coût de communication (C) : Compte le nombre de messages de sauts par unité de temps.
CTPKM filtre des messages ou des opérations non fiables, ainsi il minimise la vulnérabilité de sécurité tout en obtenant une haute disponibilité, sans encourir de coûts de communication élevés, mais dans le protocole de Jin-Hee et al pour obtenir un certificat chaque nœud se doit de trouver un nœud NTC parmi ces un 1-saut voisins ce qui n'est pas toujours probable.

| Modèle | Disponibilité | Ressources | Renouvellement | Révocation | Robustesse |
|---|---|---|---|---|---|
| Maheswaran et al | Élevée | Chaque nœud maintient un dépôt contenant un nombre important de certificats. | Oui | Oui | Oui |
| Omar et al | Élevée | Chaque nœud maintient un dépôt contenant un nombre important de certificats partiels. | Non | Non | Oui |
| Jin-Hee et al | Oui | Afin de réduire la vulnérabilité, CTPKM génère un coûts de communication élevés | Oui | Non | Oui |

TABLE II.3 – Exposition des dimensions dans les infrastructures à clé publique auto-organisée

### II.2.3 Synthèse

Un réseau mobile Ad hoc peut être formé de deux ou plusieurs nœuds mobiles capables de communiquer entre eux via des liens sans fil, sans infrastructure pré-déployé, ainsi, constitue une topologie dynamique. Ces caractéristiques rendent ce type de réseaux facile à mettre en place et capables d'opérer dans des conditions difficiles, mais aussi vulnérables aux différents problèmes de sécurité, comme la gestion des clés de chiffrement, la distribution des certificats, la gestion de confiance. Cependant, la plupart des travaux dédiés à résoudre le problème de gestion confiance dans les réseaux ad hoc visent à décentralisé le rôle de l'AC, du moins leurs principe, et ceux est dû à la mobilité de ses composantes et leurs ressources limitées, Zhou et Haas [11] ont été les premiers à proposé une architecture partiellement distribuée pour tenir le rôle de l'AC, mais cette architecture ne pouvait pas assurer son rôle à cause de l'indisponibilité des serveurs de certification décrit dans cette solution, entre autre comment un nœud exécute le protocole de certification avec k serveurs quand les serveurs sont dispersés dans un large réseau. Depuis, des améliorations ont était apportées, nous citons Wu et al [16] avec leur protocoles SEKM qui construit une infrastructure à clé publique en utilisant la technique de partage de secret technique, mais la disponibilité du service de certification reste moyenne et le protocole et assez gourmand en terme de ressources. Chang et al [15] ont aussi proposé une approche d'authentification sécurisée dans les MANET multicast, avec un modèle de confiance en chaine de Markov pour déterminer la valeur de confiance pour chaque voisins d'un seul saut, le nœud avec le seuil de confiance le plus élevé sera sélectionnée en tant que CH du groupe qui va géré la table de confiance du groupe. Les auteurs ont aussi démontré que leur protocole pouvait résister à plusieurs attaques comme : L'attaque marche-arrêt.

Pour les architectures complètement distribuées contrairement au modèle précédent qui fixe un ensemble de serveurs, dans ce modèle, le service de certification est distribué sur tous les nœuds du réseaux comme exemples de protocoles de cette approche nous citons la solution de Zhu et al [13] qui ont proposé une technique appelée AKM qui fournit un service AC complètement distribué en se basant sur la cryptographie à seuil, et Raghani et al [9] qui ont proposé un schéma de AC distribué où un nœud obtient son certificat en communicant avec ses voisins à un seul saut, les auteurs ont démontré que leurs protocole offre une disponibilité élevé du service de certification, mais on signale que leur système est résistible face aux faux certificats partiels générés. Enfin nous abordons les protocoles à clé publique auto-organisés, nous citons le protocole de Maheswaran et al [14] qui ont proposé un protocole se basant sur le modèle hiérarchique pour assurer l'authentification, il utilise

des valeurs hachées générées par des fonctions de hachage. Le processus d'identification des nœuds malicieux n'est pas évoqué dans ce protocole. L'avantage est que ce protocole est approprié aux MANET par ce qu'il est décentralisé. Il permet aux nœuds des MANET d'annuler les certificats des nœuds malicieux et d'empêcher les nœuds malveillants de pouvoir employer les accusations injustifiées qui annulent les certificats des nœuds bienveillants. Comme le protocole est basé sur le nombre de nœuds malicieux, quand ce nombre est plus grand que le nombre de nœud bienveillants, le protocole devient non résistant aux attaques et inefficace pour retirer les certificats des nœuds malicieux. Puis nous citons le protocole de Omar et al [10] avec un modèle de confiance entièrement distribué pour les réseaux mobile ad hoc. Le régime permet au nœuds de générer, stocker et distribuer leurs certificats de clé publique sans serveur central ou tiers de confiance. L'avantage de ce modèle c'est qu'il est capable de découvrir et d'isoler un pourcentage élevé de nœuds malveillants, l'inconvénient c'est que les certificats partiels et leur combinaisons de chaque authentification sont stockés dans chaque nœud donc assez gourmand en ressources. Enfin nous citons le modèle de Jin-Hee et al [12], les auteurs ont proposé un modèle de gestion de confiance à base de clé publique pour les réseaux mobile ad hoc sans utiliser une autorité de certification centralisé CA, les auteurs on résolu le problème de l'existence d'une autorité centrale en introduisant un concept ou chaque nœud se doit de trouver un nœud de tierce partie de confiance parmi ces 1-saut voisins qui peut lui certifié les clés auto généré. Le protocole de Jin-Hee et al offre améliore la disponibilité du service de certification mais pour cela chaque nœud se doit de posséder un nœud de confiance parmi ces 1-saut voisins. Ces solutions se basent sur des algorithmes de cryptographie distribués, ce qui offre une résistance aux comportements malveillants de certains nœuds du réseau. Les architectures proposées rencontrent chacune des problèmes, soit la disponibilité du service de certification, la révocation des certificats ou la robustesse lorsque ces réseaux deviennes plus grands.

# Conclusion

Dans ce chapitre nous avons donné une vue générale sur les objectifs concernant la gestion de confiance dans les réseaux Ad hoc. Nous avons classifié les solutions existantes dans la littérature. Nous avons également présenté des comparaisons et discussions de l'ensemble des solutions.

# Chapitre III

# Modèle de confiance proposé

## Introduction

Pour gérer la confiance dans les réseaux mobile Ad hoc nous optons pour une architecture pseudo hiérarchique afin de définir le rôle de l'autorité de certification sur les nœuds que nous jugerons des nœuds de confiance. Dans notre architecture on va utiliser le concept de clusterisation qui consiste à diviser le réseaux on groupes, dans chaque groupe élire un chef de groupe (cluster head) au quel on affecte le rôle de l'autorité de certification. Pour cela les nœuds chefs doivent être des nœuds digne de confiance, et ensuite les nœuds passerelle ( les noeuds à un saut du CH ) et les noeuds mobile seront sélectionnés.

## III.1 Schéma proposé

Pour illustrer notre architecture, nous considérons que notre réseaux est représenté sous forme d'un graphe connexe dont les sommets sont les nœuds du réseau et les arrêtes sont des liens bidirectionnels entre ces nœuds. Et pour mieux distribuer le rôle de l'autorité de certification nous procédant à la cluestérisation de ce graphe. Notre proposition repose sur trois autres solutions, pour la clusterisation on a utilisé la valeur de confiance qui est calculer selon Jenitha et al [4], et pour la cryptographie à seuil, nous utliserons le schéma de Omar et al [10], ainsi que Jin-Hee et al [12].
Notre schéma est constitué de deux étapes :

## Étape 1 : Phase de clusterisation

On commence par divisé le réseau on des sous groupes (cluster), dans chaque cluster élire un chef de groupe (cluster head), l'élection du nœud CH se fait selon notre algorithme de clustering distribué. On suppose que tous les nœuds vont participer au bon fonctionnement de cet algorithme, et tous sera implémenté selon les critères suivants :

— Pour être candidat au titre de cluster head, les nœuds doivent avoir un SC = 1.
Chaque nœud dispose d'une table de confiance dans laquelle figure les valeurs de confiance des nœuds aux quels il a eu contact.
Pour les autres neouds, leurs valeurs de confiance sont calculées par transitivité. Le seuil de confiance SC est calculé par rapport au nombre d'envoi et de réception des paquets, retard et aussi le nombre de paquets manqué [4], il varie dans un intervalle de ]0,1].
Chaque nouveau nœud commence avec un seuil de confiance sc = 0.1 et ce dernier augmente au fur et à mesure que le nœud se montre digne de confiance au sein du réseau.

— Les nœuds se présentons au rôle de chef (cluster head) diffuse un message dans le réseau. Le message contient : l'identifiant du nœud (ID), nombre chromatique (NC), niveau d'énergie (NE).
— Les nœuds passerelles sont sélectionnés en fonction de leur valeur de confiance qui doit être comprise dans l'intervalle ]0.7,1], ils doivent se trouver à un 1-saut du CH (cluster head).
— Les nœuds non candidats au titre de chef doivent s'affilier à un seul CH (Cluster Head).

### L'algorithme d'élection du cluster head

Nous considérons que chaque nœud possède les variables suivantes :

— ID : un identifiant unique.
— Une table de confiance.
— état : candidat ou non-candidat.
— affilié : porte l'ID du CH auquel un nœud est affilier, ou null sinon.
— D : la distance entre un nœud et son CH (en nombre de sauts ).

On définit trois types de messages : message d'élection, message d'affiliation, message de départ quitter.

- Au début, chaque candidat au titre du CH diffuse un message élection (ID, NC, NE,), quand les nœuds reçoivent le message, nous pouvons distinguer trois cas :
  Cas N°1 : Le nœud n'est affilié à aucun CH cluster head, alors le nœud vérifie le seuil de confiance du candidat dans sa table de confiance si le sc du candidat = 1 alors le nœud s'affilie directement au candidat et calcul sa distance (D) par rapport à se dernier.
  Cas N°2 : Si le nœud est lui même candidat au titre du cluster head il ignore le message.
  Cas N°3 : Si le nœud est déjà affilié à un CH, il calcule sa distance par rapport au candidat. Puis la compare avec sa distance envers son CH si elle est inférieure alors, dans ce cas ce dernier peut se détacher de son CH et s'affilier au candidat.
- La sélection des nœuds passerelles (NP) se fait par les CH, qui désignent parmi leurs nœuds voisins à un seul saut qui ont un degré de confiance assez élevé ]0.7,1].
- Les nœuds qui ne sont ni des CH ni des NP sont appelés nœuds mobiles (NM).
- Quand un nouveau nœud intègre le réseau il diffuse un message "affiliation", les nœuds mobiles et les nœuds passerelles ignorent ce message, les CH recevant ce message calculent leurs distances par rapport au nouveau nœud $D_{NV}$ et l'envoie à ce dernier. Si le nouveau nœud reçoit une seule réponse de la part d'un CH, il s'affilie directement à lui, si il en reçoit plus d'une, il compare ces distances et s'affilie au cluster head dont la distance est la plus courte par rapport à lui.

**Algorithm 1** démarrer l'élection :

**if** ($sc_i = 1$) **then**
  $état_i$ := candidat ;
  diffuser élection ($ID_i$, $NC_i$, $NE_i$,) ;
**end if**
END

**Algorithm 2** Algorithme affiliation :

Lors de la réception de élection de j ($ID_j$, $NC_j$, $NE_j$,)
**if** ($état_i$ == candidat) **then**
  ignorer ;
**else if** (affilié == null) **then**
  affilié := $ID_j$ ;
  calculer D ;
**else**
  calculer d(distance entre le candidat et le nœud) ;
  **if** (d < D) alors **then**
    Envoyer quitter à affilié ;
    affilié = $ID_j$ ;
    D = d ;
  **end if**
**end if**
END

L'architecture ci dessous représente un exemple de notre schéma de clusterisation :

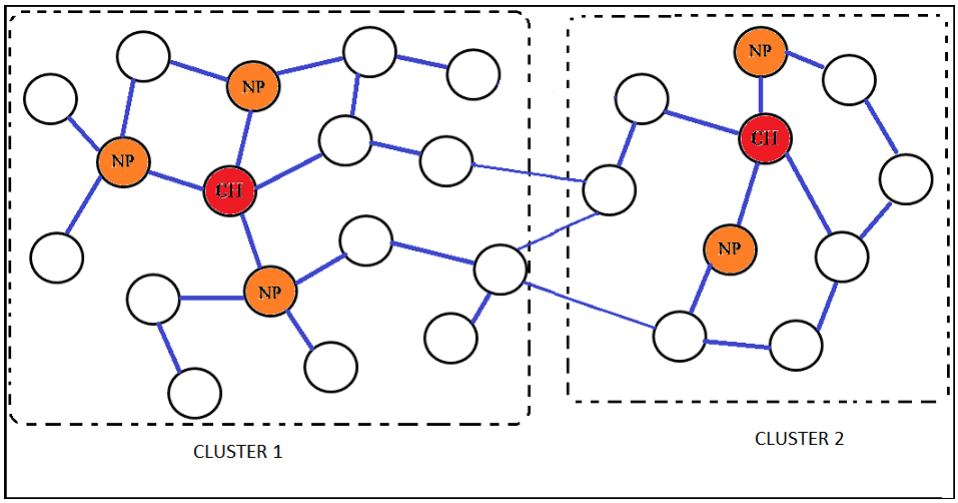


FIGURE III.1 – Architecture clusterisé.

## Étape 2 : Distribution du rôle de l'autorité des chefs de groupe sur les nœuds passerelle

Pour distribuer le rôle des chefs de groupes sur les nœuds passerelles on va intégrer la cryptographie à seuil [10] à base de RSA à notre architecture.
Au début, chaque chef de groupe génère sa paire de clé en suivant RSA :

- Choisir deux grands nombres premiers p et q et calculer
  n = p*q et $\phi$(n) = (p - 1) * (q - 1)
- Calculer une paire de clés (k,$k_p$) (privée, publique), telle que $k_p$ est premier avec $\phi$(n) et
  k * $k_p \equiv 1$ mod $\phi$(n)

Après avoir générer sa paire de clé chaque chef de groupe va partager son pouvoir de certification sur les nœuds passerelle, pour cela il attribue à chaque nœuds passerelle une parts privé et leur délivre un certificat. La génération des parts privé se fait à travers un polynôme :
f(x) = $a_0$ + $a_1$x2 + ... + $a_{t-1}x^{t-1}$ mod $\phi$(n) avec $a_0$ = K La part privé de chaque noeud passerelle i est notée comme suit : $S_i$ =f(i).

Chaque nœud passerelle d'un cluster possède une part de la clé privé du CH avec laquelle il peut délivrer des certificats partiels ($C_i$) aux nœuds mobile à un seul saut. La

génération des certificats partiels ($SP_i$) ce fait comme suit : $SP_i = C^{S_i}$ mod n.
Pour les nœuds à un seul saut des nœuds passerelles, leurs certificats sont délivrés en combinant t signatures partiels parmi n des nœuds passerelles. La combinaison des signatures partiels ce fait comme suit : Pour combiner l'ensemble des signatures partielles, nous calculons tout d'abord l'interpolation de lagrange pour chaque signature :

$L_i = \prod_{j=1 j \neq i}^{j=t} \frac{j}{j-i} \bmod \theta(n)$

Ensuite, on calcule la signature complète SC du certificat :
$\mathrm{SC} = \prod_{i=1}^{i=t} SP_i^{Li}$
pour les nœuds de plus d'un saut par rapport au nœud passerelles, ils doivent trouver un nœud digne de confiance (NVC) [12], parmi ses 1-saut voisins, qui va lui certifier un certificat partiel $SP_v$ avec sa propre clé privé, à condition qui est une certaine confiance entre les deux. Le minimum de condition pour être un NVC est d'avoir obtenu un certificat valide. Donc le certificat des nœuds de plus d'un saut par rapport au nœuds passerelles doivent contenir t signatures partielles parmi n des nœuds passerelles et une signature d'un voisin de confiance.

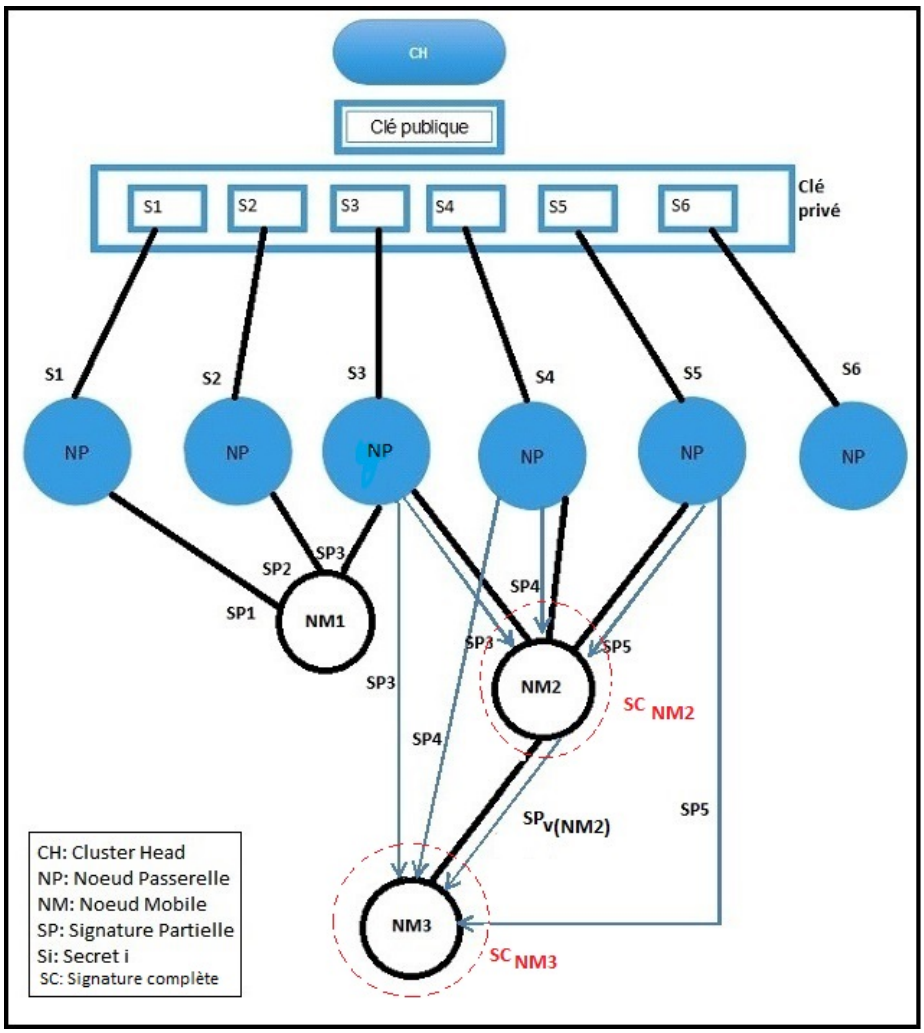


FIGURE III.2 – Shéma de certification.

**Discussions des valeurs des paramètre t et n lors de la combinaison des certificats partiels**

Notre réseaux est un graphe connexe non uniformément répartis, le choix des valeurs (n,t) doit être convenable.

Les cas particuliers du choix de t :

t =1 : La décision est partagée par les n noeuds passerelles , et n'importe lequel d'entre eux peut valider un certificat en utilisant seulement sa part privé. Ce schéma est semblable à une autorité unique et donc vulnérable au point de défaillance unique.

t = n : Le secret est partagé par tous les nœuds passerelles n et ils doivent tous participer avec leurs actions afin d'obtenir la validation. Ce système offre une sécurité maximale, mais nécessite l'accessibilité à tous les nœuds passerelles.

- 1 < t < n : Le choix du seuil t se fait d'une manière à ce qu'il y ait un équilibre entre la sécurité et la disponibilité .

**Révocation des certificats**

Les certificats peuvent être révoqués pour plusieurs raison :

- L'expiration de la période de validité (La révocation ce fait automatiquement).
- La divulgation de la clé privée du nœud(Ce qui sera suivi par la mise à jour de sa paire de clés).
- L'utilisateur n'est plus considéré digne de confiance (Par rapport à son comportement).

# Conclusion

Dans ce chapitre nous avons proposé un schéma de gestion de confiance pour les réseaux mobile. Tout d'abord une architecture clusterisé pour divisé le réseaux on groupes, dans chaque groupe élire un chef de groupe CH selon les paramètres : seuil de confiance,nombre chromatique et la niveau d'énergie, en vu de la difficulté de trouver une entité stable et permanente pour assurer la fonction de l'AC, une distribution de ce rôle sur certains noeud de confiance s'impose pour cela nous avons intégré à notre architecture la cryptographie à seuil à base de RSA pour distribuer les rôles d'autorité de certification sur les nœuds digne de confiance.

# Conclusion générale et perspectives

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

Ayant définit les motivations pour la conception d'un schéma de gestion de confiance pour les réseaux ad hoc, nous avons présenté un schéma de gestion de confiance basée sur une architecture en cluster dans laquelle nous avons introduit la cryptographie à seuil à base de RSA pour distribuer le rôle de l'autorité de certification sur les noeuds digne de confiance.
Notre modèle permet de décentraliser le service de certification ce qui augmente sa disponibilité, optimiser la charge du réseau et éviter le trafic à longue portée, assurer la tolérance aux pannes augmenter la durée de vie de réseaux au maximum.

En guise de perspectives, nous envisageons la simulation et l'évaluation des performances de notre schéma de gestion de clés en le comparant à d'autre schémas similaires, dans le but de le rendre plus performant et plus résistant contre tout comportement malveillant.

# Références bibliographique


[1] Sayad Maya, Energy Efficient Protocol (EEP) : un protocole de routage efficace en énergie pour réseaux de capteurs sans fil, Mémoire master, Ecole nationale Supérieure d'Informatique (ESI) Oued-Smar, Alger, 2009.

[2] `http://www.commentcamarche.net/contents`, articles 1308-1322, Janvier 2017, consulté le 6 Février 2017.

[3] Van der Meerschen Jérome, Hybridation entre les modes ad-hoc et infrastructure dans les réseaux de type Wi-Fi, mémoire de Master, Université Libre de Bruxelles, 2006.

[4] T. Jenitha, P. Jayashree, Distributed trust node selection for secure group communication in MANET, Fourth international conference on advances in computing and communications, India, 2014.

[5] Y. Meraihi, Routage dans les réseaux véhiculaires (VANET) cas d'un environnement type ville, mémoire de Master, Université M'hamed BOUGARA, Boumrerdes, 2011.

[6] B. Tharon, F. Dupont, L. Nuaymi, S. Gombault, V. Gayraud, La Sécurité dans les réseaux sans fil Ad Hoc», Conférence SSTIC03, France, 12 Juin 2003.

[7] F. Stajano, Security for Ubiquitous Computing, John Wiley and Sons, 2002, ISBN 0-470-84493-0, http ://www-lce.eng.cam.ac.uk/ fms27/secubicomp/.

[8] A. Beghriche, A. Bilami , Université de Batna–Algérie.

[9] S. Raghani, D. Toshniwal et R. Joshi, Dynamic support for distributed certification authority in mobile ad hoc networks. In Proceedings International Conference on

Hybrid Inforlation Technology IEEE Computer Society, Washington, 2006.

[10] M. Omar, Y. Challal et A. Bouabdallah, Reliable and fully distributed trust model for mobile ad hoc network, Computers & Security 28(3-4) : 199-214,2009.

[11] L. Zhou et Z. Hass, Securing ad hoc networks.IEEE Network : 24-29, 1999.

[12] J. Choa, I. Chenb, K. S. Chana, Trust Threshold based Public Key Management in Mobile Ad Hoc Networks, U.S. Army Research Laboratory, Adelphi,Department of Computer Science, 2016.

[13] B. Zhu, F. Bao, G. Wang et R. H. Deng, Efficient and Robust Key Management for Large Mobile Ad Hoc Networks, Computer Networks 48 : 657-682, 2005.

[14] M. Muthucumaru, G. Arboit, C. Crépeau et R. D. Cerlton, A Localised certificate Revocation Scheme for Mobile Ad Hoc Network, IEEE Trans, Mobile Computer, 2006.

[15] B. Chang, Markov Chain Trust Model for Trust-Value Analysis and Key Management in Distributed Multicast MANETs, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 4, MAY 2009.

[16] B. Wu, E. B. Fernandez, M. Ilyas ET S. Magliveras, Secure and efficient Key Management in Mobile Ad Hoc Networks, Computer Applications 30 : 973-954,2005.

# Résumé

Un réseau Mobile Ad hoc est une collection de noeuds mobile sans fil avec une portée et des ressources restreintes, aucune infrastructure fixe et une configuration rapide et facile. En raison de ces caractéristiques spéciales, ces réseaux sont plus vulnérables aux attaques que les réseaux filaires classiques. Le principal problème dans la sécurisation d'une session multicast dans un réseau ad hoc est la gestion de clés de groupe, elle ne prend pas toujours en considération le dynamisme des membres du groupe qui quittent ou rejoignent le réseau, ceci aboutit à des solutions parfois inefficaces pour une session multicast. L'objectif du travail consiste à étudier les solutions susceptibles d'assurer la sécurité dans les réseaux ad hoc et plus particulièrement la gestion de groupes et la distribution de clés. Dans ce cadre, un modèle de confiance adapté à la dynamique des groupes basée sur la clusterisation et la cryptographie à seuil est proposé.


**Mots clés :** Manet, Confiance, Clusterisation, Cryptographie à seuil.



# Abstract

Network Mobile Ad Hoc is a collection of wireless mobile nodes with restricted transmission range and resources, no fixed infrastructure and quick and easy setup. Because of special characteristics, these networks are more vulnerable to attacks compared to the classical wired networks. The main problem in securing a multicast session in an ad hoc network is the key management group, it does not always take into consideration the dynamism of the group members leaving or joining the network, this leads to solutions sometimes ineffective for a multicast session. The research objective is to explore solutions that can ensure security in ad hoc networks and especially the group management and key distribution. In this context, a trust model adapted to the dynamics of groups Based on clustering and threshold cryptography is proposed.


**Keywords-component :** Manet, Trust, Clustering, Threshold cryptography.