# Modélisation et Gestion de la Confiance dans les Réseaux Mobiles Ad hoc

Abdesselem Beghriche[1], Azeddine Bilami[2]

Département d'informatique, Université de Batna–Algérie.
05, avenue Chahid Boukhlouf, 05000 Batna–Algérie.
abdesselem_beghriche@hotmail.com, abilami@yahoo.fr

**Résumé** : Les réseaux mobiles Ad hoc annoncent les réseaux de communication du futur où la mobilité en est l'idée maîtresse. Ces réseaux devront être capable 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 ce papier notre approche consiste à modéliser et gérer la confiance dans une architecture Ad hoc hiérarchique distribuée. La solution envisagée est de faire reposer la prise de décision d'un échange sur la base de la confiance, sachant que chaque nœud ne pourra se protéger d'éventuels voisins malicieux qu'en faisant appel aux informations locales dont il dispose. Notre modèle de gestion de la confiance a donc pour objectif d'intégrer des mécanismes contrant les attaques actives, en forçant la coopération entre les nœuds, et détectant les comportements défaillants.

**Mots-clés :** Réseaux mobiles Ad hoc, Sécurité, Confiance, Réputation, Algorithmes distribués, Infrastructure à clé publique (PKI), Mécanisme de surveillance, IEEE 802.11 et Clustering.

## 1 Introduction

Les réseaux Ad hoc sont des réseaux sans fil sans infrastructure fixe. Les nœuds doivent donc collaborer pour organiser l'échange d'informations de contrôle et permettre l'acheminement du trafic. Ces réseaux doivent posséder la capacité de s'auto-configurer, sans intervention humaine. Suivant la définition de groupe MANET (*Mobile Ad hoc NETwork*) de l'IETF (*Internet Engineering Task Force*) [4], un réseau Ad hoc mobile, est un système autonome de nœuds mobiles reliés par des liens sans fil dont l'union forme un graphe arbitraire.

Un réseau MANET possède des exigences spécifiques en terme 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 Ad hoc mobiles sophistiqués et capables d'opérer dans des conditions difficiles, mais aussi vulnérables aux différents problèmes de sécurité, comme la gestion des clés de chiffrage, distribution des certificats, gestion de confiance entre les nœuds, la coopération, etc. Dans ces réseaux, le problème principal ne se situe pas au niveau du support physique, mais principalement dans le fait que tous les nœuds sont équivalents et potentiellement indispensables (fonction de routage) au fonctionnement du réseau. Les possibilités de

s'insérer dans le réseau sont grandes, la détection d'une intrusion ou d'un déni de service (DoS) est plus délicate en l'absence de centralisation.

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 Ad hoc mobiles est la gestion et la distribution des clés de chiffrage. 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. Le protocole ARAN [7] par exemple utilise une seul AC pour tout le réseau, si le nœud AC est compromis, tout le réseau sera compromis. Cette solution n'est seulement pas souhaitable, mais n'est en plus pas adaptée à la dynamique de la topologie du réseau. Il nous paraît nécessaire de traiter la sécurité dans les réseaux Ad hoc de manière plus globale en tenant compte des spécificités de ces réseaux.

La question de la confiance s'est appliquée dans le monde des télécommunications avec des modèles reposant sur la connaissance au préalable des identités. Si aucune information n'est transmise au préalable, la confiance ne s'établit pas, elle n'est pas adaptative [6]. C'est bien cette condition qui rend ces modèles contraignants et binaires, imposant aux entités communicantes qu'elles soient d'abord connues puis reconnaissables (identifiées et authentifiées) tout au long de l'échange (maintien de la confiance). Si la connaissance préalable des identités est possible pour des réseaux maîtrisés, elle ne peut pas naturellement s'imposer à des réseaux dont les caractéristiques sont tout le contraire : topologie réseaux fortement dynamique, passage à l'échelle incontrôlé et population anonyme.

Dans ce papier, nous allons concentrer sur notre architecture de sécurité proposée dans [13], pour développer les systèmes dynamiques de gestion de clés adaptés aux caractéristiques du réseau Ad hoc. Nous proposons un modèle de confiance probabiliste basé sur le principe de la réputation pour définir la connectivité entre les nœuds de confiance, afin de mettre en place un bon modèle de gestion de la confiance a pour objectif d'évaluer la robustesse de notre nouvelle architecture dans le but de sécuriser les réseaux MANETs.

Le présent papier est organisé comme suit : nous décrivons dans la section 2, les solutions proposées dans la littérature, qui traitent de la distribution et de la gestion des clés dans l'environnement des réseaux MANETs. Dans la section 3, nous présentons notre architecture de sécurité en expliquant les objectifs de notre modèle de confiance et les modules de surveillance et gestion de groupe. Enfin, et avant de conclure, nous discutons et commentons dans la section 4, les résultats obtenus par simulation de la solution proposée.

## 2 Positionnement bibliographique

Un cadre de gestion de la confiance doit permettre à une entité de prendre une décision en fonction de son expérience et d'une analyse des risques encourus. L'idée principale est d'évaluer le trait prévisible d'une autre entité et d'établir le niveau de confiance qu'il lui est porté, c'est-à-dire paraît-il digne de confiance ? Est-il honnête dans les réponses aux requêtes? Dans [1] les auteurs montrent qu'un tel cadre de gestion de la confiance peut revêtir trois formes :

- Les systèmes de *Credentials* (à base de certificats).
- Les systèmes de réputation et de recommandation.
- Et les systèmes développés à partir du réseau social de l'utilisateur.

Les deux premiers systèmes reposent en général sur une infrastructure à clefs publiques et sont aujourd'hui les plus répandus. Ils garantissent l'identité de chaque entité par l'émission d'un certificat. L'autorité peut se répartir suivant deux modèles : centralisé ou distribué. Le modèle distribué offre une meilleure disponibilité du service du fait de la décentralisation des informations de confiance mais se heurte cependant à la difficulté de répartir la clef privée avec cohérence entre chaque membre. Dans le modèle distribué, l'autorité est distribuée en plusieurs entités de certification, La cryptographie à seuil est en charge de la problématique de la distribution des clefs privées.

Les modèles partagés ne gèrent pas l'identité des entités, et sont statiques. Le secret, distribué au préalable, identifie le groupe et se partage entre l'ensemble des membres. L'authentification s'effectue sur la connaissance du secret partagé. La compromission d'un seul membre met en danger l'ensemble du groupe.

Les modèles coopératifs ne nécessitent pas la présence du tiers de confiance. Chaque entité contribue au calcul du secret du groupe.

### 2.1 Le système de Credentials

Ce cadre repose sur la mise en place d'une ou plusieurs politiques de sécurité et d'un système de certificats : les nœuds utilisent la vérification des certificats pour établir un lien de confiance avec les autre nœuds [2]. Le principal but de tels systèmes est de permettre le contrôle d'accès. En conséquence, leur concept de gestion de la confiance se limite aux règles de politiques définies par chaque application [3].

Un nœud rendra accessible à un autre nœud un service dont l'accès est normalement restreint seulement si ce dernier peut lui prouver la validité d'un certificat.

### 2.2 Le système de réputation et de recommandation

Dans ce cadre, la gestion de la confiance repose sur un modèle de réputation et/ou de recommandation. La réputation peut-être vue comme l'espérance portée dans la réalisation d'un objectif fictif. La recommandation serait la qualité supposée d'un nœud qu'il détiendrait d'un tiers et qu'il présenterait à un autre nœud. De tels systèmes fournissent un mécanisme pour lequel un nœud demandant une ressource peut évaluer la confiance qu'il porte au fournisseur à la lui fournir, Chaque nœud établit ainsi des relations de confiance avec les autres nœuds et assigne des valeurs de confiance à ses relations [14]. La valeur assignée à la relation de confiance est fonction d'une combinaison entre la réputation globale du nœud et l'évaluation de la perception du nœud, c'est-à-dire basée sur son expérience propre.

### 2.3 Confiance à partir d'un réseau social

Enfin dans ce cadre, le réseau social sous-jacent conditionne le cadre de gestion de la confiance. Les relations sociales sont utilisées pour calculer les valeurs de réputation et

de recommandation entre chaque nœud. De tels systèmes analysent le réseau social qui représente les relations existantes dans chaque communauté dans le but de tirer des conclusions sur les niveaux de confiance à accorder aux autres nœuds, Ils reposent sur des mécanismes de réputation, de crédibilité, d'honnêteté et également des procédés de recommandations. Les exemples de tels systèmes de gestion inclus Regret [11] qui identifie les différents groupes en utilisant directement le réseau social et NodeRanking [10] qui tente d'identifier des experts par le biais du réseau social.

## 3. Architecture Ad hoc sécurisée

Pour sécuriser les réseaux Ad hoc, nous envisageons une architecture hiérarchique [13] pour distribuer le rôle de l'autorité de certification (CA) sur les nœuds qui bénéficient d'un certain niveau de confiance pour la sécurité et d'une certaine stabilité pour optimiser la charge du réseau et augmenter la durée de vie du réseau. Cette architecture est composée d'un modèle de confiance sur lequel la sélection des chefs du groupe (leaders) est basée. Pour atteindre cet objectif nous proposons un algorithme d'élection distribué (AED) [13] qui consiste à diviser le réseau sous forme de groupes, avec un nœud chef de groupe pour chaque Cluster (groupe). Le rôle de l'autorité de certification est affecté au nœud chef de groupe qui doit disposer d'un certain niveau de confiance et une meilleure stabilité par rapport à ses nœuds voisins.

### 3.1 Description de l'architecture proposée

Le concept de sécurité proposé dans cette architecture repose sur les idées suivantes :

- Définir une architecture Ad hoc basée sur la division du réseau avec un seul chef par groupe (Cluster).
- Crée une atmosphère de confiance entre toutes les entités du groupe, en utilisant un modèle de confiance hybride, distribué et coopératif fondé sur des éléments que nous suggérons, et qui sont nourris par les interactions de l'entité communicante avec son environnement.
- Dans chaque groupe, élire un nœud chef (Cluster Head), parmi les nœuds qui disposent d'un niveau de confiance plus élevé.
- Mettre en ouvre *la cryptographie à seuil* pour sécuriser les interactions inter groupes.
- Maintenir l'architecture de sécurité le plus longtemps possible.

### 3.2 Modèle de confiance proposé

#### 3.2.1 Principe

Le modèle de confiance proposé consiste à fournir les mécanismes nécessaires pour associer un niveau de confiance à chaque nœud du système via sa table de routage. Un mécanisme basé sur la notion de réputation est mis en place. Toutefois, si un nœud réussi très régulièrement à acheminer un paquet de données avec un même nœud, sa réputation peut devenir importante et donc autoriser des accès à des services plus évolués dans le groupe (notamment le service d'authentification). Dans le type de ces réseaux la notion de réputation est limitée à des interactions de type un à un, et donc n'aura que très peu

d'impact sur le réseau. Pour augmenter la portée dans notre modèle, nous proposons d'introduire un autre mécanisme basé sur le principe de recommandation. La confiance locale pour une entité (nœud ou participant) peut donc être transmise, l'acceptation d'une recommandation étant assujettie également au degré de confiance accordé à l'entité qui propose cette recommandation.

Cependant, la question qui se pose ici, est comment publier la confiance dans notre modèle tout en garantissant sa validité ? Pour cela, on va définir quelques paramètres qui peuvent assurer le déroulement de notre modèle :

Nous supposons qu'il existe une relation sociale entre les nœuds dans le but d'établir des relations de confiance. Aussi chaque nœud possède une paire de clés privées/publiques. Initialement, les nœuds de confiance se connaissent entre eux (climat de confiance) (l'identité et la clé publique) et ils sont considérés comme des nœuds honnêtes qui ne doivent pas générer des faux certificats.

- Un seuil de confiance Sc (Sc : valeur continue dans l'intervalle : ]0, 1]), et une valeur de réputation (Vr) (Vr : valeur continue dans l'intervalle : [0, 1]).
- Un nœud (*i*) possède un seuil de confiance plus élevé (Sc (*i*) = 1), s'il est connu par d'autres nœuds de confiance et a échangé les clés via un canal sécurisé (rencontre physique par exemple) [13] avec un ou plusieurs nœuds de confiance. Un seuil de confiance très élevé, existe aussi si le nœud a prouvé sa totale coopération et son bon comportement (Vr = 1) (principe de réputation).
- Si un nouveau nœud est ajouté à la liste des nœuds de confiance par un ou plusieurs nœuds de confiance, les autres nœuds doivent mettre à jour leurs listes des nœuds de confiance.
- Chaque nœud dispose dans sa table de routage de deux tables (une table de confiance et une table de réputation), qui seront actualisées à chaque changement de Sc et/ou de Vr.
- Chaque nœud inconnu commence avec le plus bas seuil de confiance (Sc = 0.1) et le plus bas niveau de réputation (Vr = 0). L'idée de ce principe consiste à obliger les nœuds inconnus à coopérer et bien se comporter [8].
- Pour estimer le chemin de confiance entre deux nœuds, on propose de prendre la valeur minimum entre leurs deux seuils de confiance.

### 3.2.2 Fonctionnement :

Lorsque deux éléments d'un groupe veulent communiquer sans connaissance préalable, ils s'échangent leur liste de certificats et vont essayer de créer une *chaîne de confiance* entre eux (Figure 1).

Supposons qu'un élément ***x*** veuille communiquer avec un autre élément (nœud) ***z***, si ***x*** fait confiance en un troisième élément ***y***, et ***z*** fait aussi confiance en ***y***, alors une chaîne de confiance entre ***x*** et ***z*** pourra être établie via ***y*** (le principe de recommandation). Dans ce cas, ***x*** peut donner physiquement sa clé publique à ***y*** (main à main ou par téléphone, etc.) l'élément ***y*** connaît ***x*** et donc signe sa clé publique. Puis il redonne la clé signée et en garde une copie. Quand ***x*** veut communiquer avec ***z***, il lui envoie une copie de la clé que ***y*** a signée. Le nœud ***z***, qui a déjà la clé publique de ***y*** (il l'a eu à un autre moment) et qui fait confiance à ***y*** pour certifier les clefs d'autre nœuds, vérifie sa signature sur la clé de ***x*** et l'accepte. De ce fait ***y*** a recommandé ***x*** à ***z***.

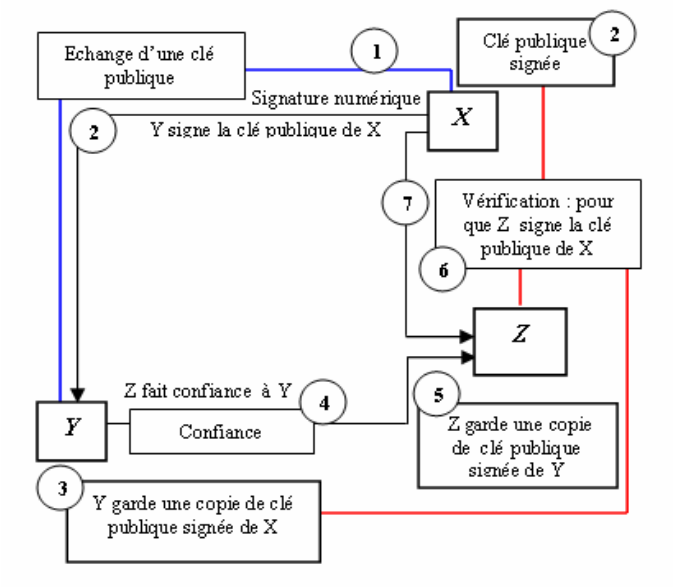


**Fig. 1.** Création d'une chaîne de confiance

Notre modèle de confiance commence par instaurer à la place d'une autorité centrale de certification un climat de confiance entre toutes les entités du groupe. Ensuite le modèle va donner à chaque nœud connecté les deux valeurs (Sc, Vr) selon son état dans le réseau (nœud de confiance, nœud de réputation, nœud visiteur, nœud inconnu, etc.), et qui à partir de ces valeurs, le nœud peut authentifier ou s'authentifier au sein de notre groupe.

### 3.3 Architecture distribuée Clusterisée

Le réseau dans notre architecture est divisé en plusieurs Clusters afin d'éviter le trafic à longue portée et d'augmenter la disponibilité en fournissant les services locaux, ainsi que d'assurer une tolérance aux pannes. Si une tentative d'intrusion est détectée suffisamment tôt, les réponses de notre système peuvent permettre de limiter localement les conséquences d'une attaque. La formation des Clusters est faite automatiquement. Tout Cluster se voit affecté un chef (Cluster-head "CH"). Le nœud CH émet périodiquement la liste des nœuds et des passerelles appartenant au Cluster.

Les caractéristiques principales de notre architecture sont énumérées comme suit :

- Le système n'a besoin d'aucun tiers de confiance central. Ce système est dynamiquement adapté à tout changement de topologie.
- La fonction d'authentification est distribuée à chaque groupe. Les nœuds ayant un degré de confiance élevé contrôleront le comportement de chaque nœud ayant un degré de confiance faible au sein du groupe.
- La stabilité de la gestion des clés publiques dépend de la stabilité du groupe.

#### 3.3.1 Contrôle des nœuds et gestion des groupes

**A) Contrôle des nœuds :** Dans le module de contrôle, chaque nœud ayant un degré de confiance élevé contrôle ses nœuds voisins, c'est à dire ceux qui ont un degré de confiance faible. Dans le cas que nous étudions, le processus de contrôle agit sur deux couches différentes du réseau :

***A.*** **La couche MAC :** les nœuds responsables du contrôle surveillent l'occupation du canal de communication par leurs voisins. Cette opération consiste à mesurer la durée de l'occupation du canal par des nœuds. Le but de cette fonction est de détecter les nœuds qui exercent un certain type de comportement égoïste [8], les nœuds égoïstes trichent en choisissant leur backoff, dans le but d'obtenir une bande plus importante et de pénaliser les nœuds qui se comportent bien. Nous supposons que les nœuds chargés du contrôle à ce niveau génèrent un rapport noté $R_1$ ($R_1$ correspond l'estimation du confiance d'un nœud de confiance (Sc (i) = 1) sur ses voisins qui ont un degré de confiance faible). (Dans notre contribution, nous ne nous focalisons pas sur le contrôle de la couche MAC).

- **La couche réseau :** les nœuds chargés du contrôle surveillent les activités de transmission de paquets de leurs nœuds voisins, qui ont un degré de confiance faible. Cette idée est basée sur le paramètre de coopération des nœuds dans le réseau. La définition de ce paramètre consiste à calculer pour chaque nœud la proportion de paquets bien retransmis par rapport au nombre total de paquets devant être transmis sur une certaine période. Cette période est la période qui consiste à collecter les informations données par les nœuds pour calculer le niveau de réputation. Soient deux nœuds *X* et *Y* avec *Sc(X) > Sc(Y)*, dans ce cas, le nœud *X* peut contrôler le nœud *Y*. Le nœud *X* envoie un certain nombre de paquets de données au nœud *Y* avec un autre nœud comme destination, et après une période de temps limitée, le nœud *X* peut calculer le niveau de réputation :

$$R_2(X, Y) = \frac{\textit{Nombre des paquets acheminés}}{\textit{Nombre total des paquets}} \qquad (1)$$

Comme nous avons déjà expliqué précédemment, chaque nœud inconnu commence avec une valeur de réputation la plus faible (Vr = 0) et ce degré augmente au fur et à mesure que le nœud prouve sa coopération et son bon comportement. Les niveaux de réputation générés par les nœuds sont liés aux degrés de confiance correspondant à chaque nœud. Telle est la tâche du chef de groupe. Le rapport final *R*(X, Y) concernant la valeur de réputation Vr fourni au nœud *Y* généré par chaque nœud chargé du contrôle *X*, est :

$$R(X,Y) = \frac{R_1(X,Y) + R_2(X,Y)}{2} \qquad (2)$$

***B) Gestionnaire du groupe :*** est constitué de l'autorité de certification du groupe (le nœud CA) et d'un ensemble de nœuds ayant des degrés de confiance élevés (les nœuds qui constituer le climat de confiance). Le rôle de gestionnaire du groupe est d'assurer la sécurité du groupe là où le nœud CA génèrera un certificat pour les membres du groupe.

Le module gestionnaire du groupe collecte le rapport de réputation des membres du groupe. Les nœuds chargés du contrôle génèrent des rapports évaluant la réputation de leurs voisins sur demande. Le nœud CA exige que les nœuds chargés du contrôle génèrent le rapport de réputation des nœuds. Lorsque le CA reçoit le rapport d'évaluation de réputation envoyé par les nœuds chargés du contrôle, le calcule du rapport de réputation finale de chaque nœud est effectué comme indiquer dans l'équation ci-dessous. Si le CA reçoit k rapports de la part des nœuds chargés du contrôle, pour évaluer le nœud y, alors :

$$R_r(y) = \frac{1}{k} \sum_{i=1}^{k} Sc(\chi_i) * R(\chi_i, y) \quad (3)$$

Lorsque le nœud CA possède les rapports de réputation, la classification des comportements est effectuée pour classer les nœuds. Si le rapport de réputation dépasse un certain seuil, le degré de confiance augmente, sinon, le degré de confiance ne change pas. Cependant, si le rapport est en dessous d'un certain seuil, le degré de confiance diminue et les nœuds se comportant mal seront punis. Dans le cas où les nœuds ont un rapport négatif plusieurs fois (récidivistes), les nœuds se comportant mal seront rejetés du groupe et le CA informe les autres CA de groupes adjacentes de la récidive des nœuds se comportant mal.

### 3.3.2 Algorithme d'élection distribué (AED)

La formation des Cluster dans l'architecture proposée se fait par l'élection des Cluster-heads et par la ré-affiliation des nœuds à ces Cluster-heads. Contrairement à beaucoup d'algorithmes dans la littérature, le mécanisme d'élection des Cluster-heads n'est pas synchronisé entre tous les nœuds du réseau. Il n'implique pas que tous les nœuds exécutent en même temps la procédure d'élection. La décision d'être Cluster-head est effectuée par chaque nœud ne détectant pas dans le k-voisinage un Cluster-head à qui s'affilier. Il diffuse alors un message "MES" dans son k-voisinage tout en indiquant son seuil de confiance. Chaque nœud qui reçoit un message "MES" compare le seuil de confiance de son Cluster-head avec le seuil de confiance reçu dans ce message. Si le seuil reçu est supérieur, il peut se joindre à ce nouveau Cluster-head sous certaines conditions.

Notons qu'une ré-affiliation peut se produire lorsque :

- Un nœud membre se déplace d'un Cluster à un autre.
- Un nœud membre devient un Cluster-head.

Nous avons opté pour une élection du nœud CH "CA" selon un algorithme de Clustering distribué ***AED*** (**A**lgorithme d'**E**lection **D**istribué). Cet algorithme sera implémenté selon les critères suivants :

1. Pour chaque Cluster, il existe un seul CH.
2. Seulement les nœuds de confiance qui peuvent être candidats au statut CH "CA".
3. Chaque chef de groupe est le CA d'un seul groupe.
4. Les nœuds qui appartiennent au groupe doivent être à (k) sauts du nœud CA tels que (k) est la taille du groupe à définir.

**5.** Le nœud passerelle *Np*, sera sélectionné parmi les nœuds de confiance voisins au CA.
**6.** Les nœuds membres *Nm,* ce sont les nœuds qui appartiennent au groupe.

Notre algorithme est basé sur l'émission périodique des paquets balise par les nœuds de confiance vers leurs voisins à chaque période de temps prédéfinie. Chaque paquet balise contient les informations nécessaires pour l'élection d'un nœud CA. La sélection d'un nœud CA est basée sur deux critères principaux : la sécurité et la stabilité.

Le paramètre de la sécurité dépend de la valeur de confiance, uniquement les nœuds (i) avec (Sc (i) = 1) et au moins un nœud de confiance comme voisin direct qui peuvent se présenter comme candidats pour devenir un CA dans un groupe. Cette condition est nécessaire pour la formation des groupes. Pour renforcer la sécurité, l'algorithme sélectionne le candidat avec un nombre maximum de voisins de confiance, cela indique aussi le degré de confiance dans le groupe.

Le paramètre de la stabilité est très important pour la formation des groupes, ce paramètre est défini comme la durée de vie d'un groupe. Plusieurs stratégies sont utilisées par des algorithmes proposés dans la littérature, comme Lowest-ID [5] Mobic [9], l'idée consiste à sélectionner le nœud dont l'identité est la plus petite. Dans notre algorithme, nous avons adopté la métrique de mobilité comme paramètre de stabilité.

La métrique de mobilité est basée sur le niveau de puissance du signal à la réception sur chaque nœud, c'est un indicatif de distance relative entre les nœuds émetteurs et récepteurs.

Le ratio Rα entre les transmissions de deux paquets successifs, donne une connaissance sur la mobilité relative entre deux nœuds voisins X et Y [8].

$$Rm_{y}(x) = 10 \log_{10} \frac{R\alpha_{x \to y}^{new}}{R\alpha_{x \to y}^{old}} \quad (4)$$

Le calcul de la mobilité relative d'un nœud Y par rapport à ses *n* voisins, consiste à calculer la variance de l'ensemble de mobilité relative $Rm_y$ de ses voisins $X_i$ :

$$Rm_y = \mathrm{var}(Rm_y(X_1), Rm_y(X_2), \ldots Rm_y(X_n)) \quad (5)$$

Une faible valeur de $Rm_y$ indique que Y est moins mobile par rapport à ses voisins. Par contre, une grande valeur de $Rm_y$ montre que le nœud Y est très mobile par rapport à ses voisins.

## 4 Evaluation de performances

Nous avons mené une série de simulations afin d'évaluer les performances du mécanisme de Clustering proposé. Nous avons utilisé pour cela le simulateur NS-2 [12], dans lequel nous avons implémenté notre algorithme décrit précédemment. L'utilitaire « setdest » de NS-2 a été utilisé pour générer les scénarios de mobilité des nœuds selon le modèle de mobilité «Random Waypoint ». Nous avons fait varier la vitesse des nœuds en maintenant les temps de pause constants.

Dans cette simulation, notre modèle est établi selon les paramètres suivants :

**Tableau 1.** Paramètres de simulation

| *Paramètres* | *Valeurs* |
|---|---|
| Vitesse de mobilité minimale | 0 |
| Vitesse de mobilité maximale | variable (0.2 à 10 m/s) |
| Dimensions du terrain | 100*100 $m^2$ |
| Nombre de nœuds | 100 |
| Temps de simulation | 3000 s |
| Portée de transmission | 10 à 250 m |
| Le temps de pause | 20 m/s |
| Rayon maximum des Clusters | à savoir : K = 1, 2, 3. |

La (Figure 2) montre la comparaison entre notre algorithme d'élection (AED) et deux autres algorithmes : Mobic [9] et Lowest-ID [5].

Nous remarquons une grande différence au niveau de la portée de transmission à 50 m, cela est dû à notre condition de formation de groupes (Clusters), un nœud de confiance tout seul ne peut pas former son propre groupe, il doit avoir au moins un nœud voisin de confiance. Dans cette simulation, le nombre de groupes formés ne doit pas dépasser 25 groupes. Cependant, avec la portée de transmission entre 50 et 125 m, le nombre de groupes diminue et lorsque la porte de transmission dépasse les 150 m, le réseau devient plus stable et le nombre de groupes devient plus ou moins stable. Avec des groupes de taille égale à 2 sauts (k=2), nous obtenons moins de groupes que dans le cas de Mobic et Lowest-ID.

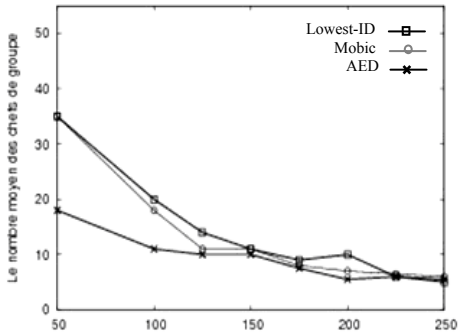


**Fig. 2.** Comparaison entre notre algorithme (AED), Mobic et Lowest-ID

### 4.1 Discussion et analyse

La sécurité de l'architecture qu'on propose dépend principalement du modèle de confiance proposé. La présence d'un grand nombre de nœuds de confiance augmente le niveau de sécurité du réseau. Les nœuds avec un faible seuil de confiance ne peuvent pas

participer à l'élection du nœud CA. Seuls les nœuds de confiance peuvent être candidats au rôle de CA.

Si un nœud malicieux tente de s'introduire dans le processus d'élection, cela soit par l'annonce de sa candidature, soit par la manipulation non autorisée de l'information des paquets balises d'élection, les nœuds de confiance le détectent au niveau de la phase d'authentification dans l'algorithme AED. Supposons que les nœuds malicieux ont réussi à former leurs groupes et qu'ils tentent de communiquer avec d'autres groupes, les nœuds CAs des groupes de destination authentifient le nœud CA du groupe source, enfin, selon le résultat de l'authentification et après l'évaluation du seuil de confiance de chaque nœud, les nœuds CAs décident d'accepter ou de rejeter la communication.

L'approche de notre modèle de gestion de la confiance oblige les nœuds à collaborer et à adopter un bon comportement pour l'obtention d'un niveau de confiance plus élevé.

Dans notre modèle de gestion de la confiance :

- Toutes les communications venant des nœuds ou des groupes malicieux sont ignorées.
- Les attaques de type déni de service (DoS) sont évitées par les nœuds de confiance qui filtrent toutes les requêtes venant des nœuds inconnus.
- Les nœuds malicieux peuvent utiliser l'identité des nœuds légitimes uniquement si leur clé privée est divulguée.
- Si un attaquant tente de compromettre tout le réseau, il doit compromettre tous les nœuds de confiance.
- La taille du groupe doit être adaptée au nombre de nœuds de confiance pour bien sécuriser le nœud CA (un compromis entre les nœuds de confiance et les nœuds inconnus doit être trouvé).
- La présence de deux nœuds de confiance est une configuration minimale pour former un groupe.

## 5 Conclusion

Dans cet article, nous avons proposé un modèle de connectivité de confiance pour étudier la robustesse de la sécurité au sein des groupes. Nous avons proposé une nouvelle architecture distribuée basée sur un modèle de confiance et un algorithme d'élection et de formation de groupes, dans le but de distribuer l'autorité de certification (CA). L'algorithme d'élection de formation des groupes et d'élection de CA est basé sur deux paramètres : la sécurité et la stabilité. La sécurité est un paramètre lié au modèle de confiance proposé, seuls les nœuds de confiance qui peuvent jouer le rôle de CAs. La stabilité est un facteur basé sur la métrique de mobilité pour assurer la stabilité des groupes. Nous avons aussi présenté les différents modules de l'architecture : le modèle de confiance, le processus d'élection, le gestionnaire de groupe et le module chargé du contrôle basé sur le principe de réputation.

L'architecture proposée capable d'offrir un niveau de sécurité adapté à l'enjeu de la communication dans un environnement hostile, et dont le niveau pourra évoluer dans le temps en fonction du contexte. Cette architecture est adaptée au changement dynamique de topologie du réseau. Les résultats de la simulation montrent que l'algorithme que nous avons proposé pour la formation des groupes est mieux que les algorithmes proposés dans Mobic et Lowest-ID. Nous avons aussi remarqué que la disponibilité, la robustesse

et la stabilité des groupes permet de conserver l'énergie et d'augmenter la durée de vie du réseau.

Finalement, on peut dire que la conception d'une solution efficace pour sécuriser les réseaux MANETs doit être adaptée aux caractéristiques et spécificités d'un tel environnement, telles que la mobilité et la dynamicité des membres, les ressources limitées en termes d'énergie, de bande passante et de capacités de stockage et de calcul, ainsi que l'absence d'infrastructure fixe au sein du réseau. Les services de sécurité offerts par un protocole de sécurité de groupe dans un réseau Ad hoc, sont également étroitement liés à la nature de l'application à sécuriser et ainsi au niveau de sécurité requis pour les données envoyées par la source pour faire face aux attaques malicieuses qui peuvent le cibler.

## Références


[1]. G. Suryanarayana and R.N. Taylor, "A survey of trust management and resource discovery technologies", *in peer-to-peer applications*.

[2]. M. Blaze, J. Feigenbaurn, and J. Lacy, "Decentralized trust management". *In IEEE Symposium on Security and Prioacy*, pp. 164- 173, IEEE Computer Society, 1996.

[3]. T. Grandison and M. Sloman, "A survey of trust in internet applications", *IEEE Communications Surveys and Tutorials,* vol. 3, n. 4, 2000.

[4]. J.P. Hubaux, L. Buttyan and S. Capkun, "The Quest for security in mobile Ad hoc Networks", *Proceedings of ACM symposium on mobile Ad hoc Networking and Computing (Mobihoc)*, Long Beach, Canada, 2001.

[5]. M. Gerla, and J. Tsai. "Multicluster, mobile, multimedia radio network", *ACM-Baltzer Journal of Wireless Networks*, Vol.1, No.3, pp. 255-265, 1995.

[6]. V. Legrand, F. Abdesselam, and S. Ubéda, "Etablissement de la confiance et réseaux Ad hoc- un état de l'art", *In SAR'2003*, July 2003.

[7]. K. SANZGIRI, B. DAHILL, D. LAFLAMME, B. N. LEVINE, C. SHIELDS, and E. M. BELDING-ROYER, "An Authenticated Routing Protocol for Secure Ad Hoc Networks", *IEEE Journal on Selected Areas in Communication (JSAC)*, vol. 23, n. 3, pp. 598-610, 2005.

[8]. A. Rachedi et A. Benslimane, "Architecture Hiérarchique Distribuée pour sécuriser les Réseaux Ad hoc Mobiles", *8ème journées Doctorales en Informatique et Réseaux*, Marne la Vallée, Janvier 2007.

[9]. P. Basu, N. Khan, D Thomas and C. Little, "A Mobility Based Metric for Clustering in Mobile Ad Hoc Networks", *21st international Conference on Distributed Computing Systems Workshops (TCDCSW 01),* 2001.

[10]. J. Pujol, R. Sanguesa, and J. Delgado, "Extracting reputation in multiagent systems by means of social network topology", 2002.

[11]. J. Sabater and C. Sierra, "Regret: A reputation model for gregarious societies", 2000.

[12]. A. UC Berkeley and USC ISI, "The network simulator NS-2", *Part of the VINT project*, Available from www.isi.edu/nsnam/ns, 1998.

[13]. A. Beghriche, A. Bilami, "De la Sécurité à la E-Confiance dans les Réseaux sans fil Ad hoc", *1st Workshop on Next Generation Networks: Mobility (IEEE WNGN 2008)*, Fès Maroc, pp. 25-30, 18-19 Juillet 2008.

[14]. G. Zacharia, and P. Maes, "Trust management through reputation mechanisms", *Applied Artificial Intelligence*, 14(9), pp. 881-907, 2000.