Université de L'Hadj Lakhdar-Batna
Faculté des sciences de l'ingénieur
Département d'informatique

MÉMOIRE DE MAGISTÈRE EN INFORMATIQUE

Option : Informatique industrielle

Intitulé :

De la Sécurité à la E-Confiance basée sur la Cryptographie à Seuil dans les Réseaux sans fil Ad hoc

Présenté par : ***M^r^ Abdesselem BEGHRICHE***

Sous la direction de : ***Dr Azeddine Bilami***

Membre de Jury composé de :

Dr M.K. Kholladi :	M.C Université de Constantine	Président
Dr B. Belattar :	M.C Université de Batna	Examinateur
Dr R. Maamri :	M.C Université de Constantine	Examinateur
Dr A. Bilami :	M.C Université de Batna	Rapporteur

Promotion 2008/2009

A mes chers parents qui m'ont soutenu durant mon existence et ma scolarité. Je leur dédie ce mémoire.

Abdesselem

Remerciements

Au terme de ce travail, Je tiens à remercier :

Merci à Dr Azeddine Bilami, mon encadrant, tu m'as fait bénéficier de ton savoir, de tes compétences scientifiques et de ta passion pour la recherche. Je te remercie également de m'avoir appris à aller jusqu'au bout de mes idées.

Merci très vivement à Dr Mohammed Kheireddine Kholladi, Dr Brahim Belattar et Dr Ramdane Maamri de l'honneur qu'ils m'ont fait en acceptant de siéger à mon jury de magistère.

Mes remerciements vont à tous les membres de ma famille à qui je dois beaucoup, sans leurs aides, ce travail n'aurait pu voir le jour.

Merci à tous ceux qui m'ont aidé sans ménager ni leurs temps, ni leurs encouragements, ni leurs savoirs.

Je tiens tout particulièrement à remercier, mon cher ami Abderrahmane Boumezbeur pour ses conseils et ses aides.

Et enfin, merci à tous les chercheurs que j'ai pu rencontrer lors des conférences et qui sont intéressés à mes travaux.

Abdesselem BEGHRICHE

ملخص :

موضوع هذه المذكرة يركز على الأمن في شبكات المحمول اللاسلكية المخصصة (أد-هوك). نقوم بدراسة أمن هذه الشبكات نظرا لعدم وجود إدارة مركزية، الشيء الذي يجعل من هذه الأخيرة أكثر عرضة للهجوم مقارنة بالشبكات الأخرى (السلكية واللاسلكية). للأسف، بروتوكولات الأمن والحماية الموجودة حاليا ليست مصممة لمثل هذا النوع من الشبكات (محيط ديناميكي متحرك)، أضف إلى ذلك محدودية الطاقة والذاكرة وضعف القدرة على الحساب) وذلك مما يزيد من تعقيد مشكلة الأمن في هذه الشبكات، ونظرا لأهمية إستخدام هذه الشبكات في عدة مجالات مثل العمليات العسكرية، الاتصالات بين الطائرات والسيارات والأفراد وعمليات الإغاثة في حالات الطوارئ والكوارث، وما إلى ذلك)، فإنه من الضروري أن يكون الهدف الرئيسي من هذا العمل هو وضع آلية أمنية مضمونة وذلك من خلال اقتراح بنية هرمية توزيعية والتي تسمح باستخدام هيكل مبني على مفتاح عام. كما يجب دعم هذه البنية للخصائص المختلفة لهذه الشبكات (عدم وجود مركزية لإدارة الشبكة، محدودية الطاقة والذاكرة، الخ) وتحقيقا لهذه الغاية، نقوم بتكييف نموذج للثقة مع هذه البنية لتطوير مستويات الثقة في كل عقدة من الشبكة.

هذا النموذج يؤسّس على مبدأ عتبة الكتابة السرّيّة، ويجمع بين عناصر أمن الشبكات التقليدية والعناصر الجديدة التي نقترحها، بحيث يتغذى هذا النموذج على تفاعلات وسلوك العقدة مع بيئتها.

كلمات البحث الرئيسية : شبكات المحمول المخصصة (أد-هوك)، أمن الشبكات، خوارزميات توزيعية، أنظمة المراقبة، هياكل المفاتيح العمومية، تفصيص الشبكات، الثقة والسمعة، IEEE 802.11.

Abstract:

This research work is focused on security in Ad hoc mobile networks (MANET: Mobile Ad hoc NETwork). The absence of a central management of the functionalities of the network makes them much more vulnerable to attacks than wireless networks (WLAN) and ordinary wire networks (LAN). Unfortunately, the protocols of security which exist nowadays are not conceived for such environment (dynamics).

They do not take in consideration the shortage of means because not only the environment is dynamic, but means are also restricted (memory, capacity of calculation and especially energy), which make the problems more complicated, as it is known that the resolutions of security are very demanding in term of means. However, owing to the importance of the domains of application of Ad hoc mobile networks in the military (communication between planes, cars and personnel and operations of assistance, urgent situations in case of disaster, etc), therefore, to take up the challenge for the design of a mechanism of infallible security for mobile networks Ad hoc is necessary.

The main objective of this thesis is to study the resolutions that are likely to ensure security in Ad hoc mobile networks, by offering a distributed hierarchic architecture which allows the establishment of dynamic facilities with public key. This architecture must support the different characteristics of these networks (absence of a central processing unit of management of network, dynamic network topology, etc). To this end, a trust model adapted to a dynamic environment, to ensure the evolution of the trust levels of the nodes, is established. This model based on the principle of threshold cryptography and combines at the same time the classical elements of security and the new elements which we suggest, which are nourished by the correlations of entity (node) with its environment.

Key words: Mobile Ad hoc networks, Security, Distributed Algorithms, Public Key Infrastructure (PKI), Mechanism of surveillance, IEEE 802.11, Clustering, Trust and Reputation.

Résumé :

Le sujet de ce mémoire se focalise sur la sécurité dans les réseaux mobiles sans fil Ad hoc (MANET : Mobile Ad hoc NETwork). L'absence d'une gestion centrale des fonctionnalités du réseau rend ces réseaux beaucoup plus vulnérables aux attaques que les réseaux sans fil (WLAN) et filaires (LAN). Malheureusement, les protocoles de sécurité qui existent actuellement ne sont pas conçus pour un tel environnement (dynamique). Ils ne prennent pas la contrainte des ressources en considération car non seulement l'environnement est dynamique, mais les ressources sont aussi limitées (mémoire, capacité de calcul et surtout énergie), ce qui complique davantage la problématique, car on sait bien que les solutions de sécurité sont gourmandes en terme de ressources. Cependant, en raison de l'importance des domaines d'application des réseaux mobiles Ad hoc comme les opérations militaires (communication entre les avions, les voitures et le personnel et opérations de secours, situations d'urgence en cas de sinistre, etc.), il faut relever le défi, car concevoir un mécanisme de sécurité infaillible pour les réseaux mobiles Ad hoc est nécessaire.

L'objectif principal de ce mémoire consiste à étudier les solutions susceptibles d'assurer la sécurité dans les réseaux mobiles Ad hoc, en proposant une architecture hiérarchique distribuée qui permet d'établir une infrastructure dynamique à clé publique. Cette architecture doit supporter les différentes caractéristiques de ces réseaux (absence d'une unité centrale de gestion de réseau, topologie réseau dynamique, etc.). Dans ce but, un modèle de confiance adapté à l'environnement dynamique pour assurer l'évolution des niveaux de confiance des nœuds est établi. Ce modèle basé sur le principe de la cryptographie à seuil, et combine à la fois les éléments classiques de la sécurité et de nouveaux éléments que nous suggérons, et qui sont nourris par les interactions de l'entité (nœud) avec son environnement.

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

Liste des figures

Liste des tableaux

Table des matières

Introduction générale

Introduction générale :

Ces dernières années, nous assistons à une très forte accélération de l'impact des télécommunications dans la société. A l'heure où la convergence commence à prendre tout son sens autour de l'Internet Protocol (IP), les révolutions actuelles à l'œuvre ne reposent plus sur des innovations technologiques majeures, mais sur des usages dont on ne commence qu'à entrevoir les effets et sur lesquelles les acteurs classiques des technologies de l'information et de la communication n'ont que très peu de prise.

Actuellement, nous assistons à une urbanisation des technologies d'accès haut débit à l'Internet combinée à l'explosion des communications sans fil. Si l'UMTS (Universal Mobile Telecommunications System) mettra probablement plus de temps à s'imposer que ce à quoi on pouvait s'attendre, les technologies de radiocommunication à courte et moyenne portée viennent compléter cet arsenal : explosion des Wireless Local Area Network (WLAN) grâce au Wifi, et réalité des Personal Area Network (WPAN) grâce au Bluetooth. Cet ensemble de technologies de radiocommunications doit permettre, de voir un autre concept devenir réalité : l'Internet ambiant. Dans cette vision, l'accès à Internet sera disponible en tout lieu, aussi naturellement que l'on s'attend à trouver l'électricité dans toutes les pièces d'un bâtiment ou l'éclairage public dans toutes les zones habitées. L'Internet ambiant permettrait aux entités (objets) communicantes de puiser des ressources et des services dans le réseau des réseaux.

L'objet communicant n'en est encore qu'à ses débuts, se limitant actuellement à quelques niches, mais dont le nombre ne cesse de croître. Actuellement, ces objets communicants permettent des échanges de données avec d'autres objets, des ordinateurs personnels ou Internet, essentiellement dans les domaines de la gestion des agendas personnels, les documents multimédias (sons, images, vidéos). Mais on prendra très vite l'habitude d'échanger des horaires de transports, des informations sur le trafic automobile, etc. On dépassera rapidement le stade de l'échange d'informations pour aller vers l'échange de services entre objets. Mais au-delà de la révolution technologique, il faut souligner celle des comportements. L'appréhension face à un objet doté de capacités de communication s'est fortement réduite et des scénarios d'usage tels que celui où un usager combine les services d'un téléphone cellulaire et d'un portable PC pour spontanément créer une extension de l'Internet pour l'offrir à ses proches via une connexion Wifi ou Bluetooth, sans être courant, effraie de moins en moins.

Les réseaux de télécommunications de seconde génération ne sont pas les seuls à familiariser un nombre croissant d'usagers à un éventuel futur Internet mobile. Les acteurs classiques de l'Internet ont été débordés par le concept du pair-à-pair et ils ne mesurent pas encore parfaitement l'impact que cette révolution a eu sur l'usager. Ces réseaux ont permis à un très grand nombre de renforcer leur rôle d'acteur de l'Internet en créant ***un espace d'échange sans aucune administration centralisée***. Ceci a permis l'avènement d'un usage renforcé pour les objets communicants permettant le stockage et l'échange de données. Des concepts tels que les formats de stockage de données, le stockage sur des supports multiples, l'archivage de documents ne sont plus l'apanage d'informaticiens chevronnés, mais apparaissent de plus en plus dans les usages de monsieur " tout le monde ".

La prochaine étape sera de doter ces systèmes autonomes que sont les objets communicants de la capacité à s'organiser de façon plus ou moins spontanée en pico-réseaux : c'est le concept de Personal Area Network (PAN). Ces pico réseaux sont de moins en moins personnel puisqu'impliquant des équipements qui ne sont pas sous une autorité commune. Ces pico-réseaux établiront des relations, éventuellement spontanées, entre eux pour s'offrir mutuellement des ressources et des services : ils seront dotés d'une capacité de communication dite ***Ad hoc***, c'est à dire de la capacité à communiquer en mode pair-à-pair, éventuellement en se servant d'autres objets communicants comme intermédiaires et sans l'aide d'aucune infrastructure. En unifiant toutes ses visions, on peut imaginer un écosystème d'entités communicantes s'appuyant sur un support réseau hybride.

Bien évidemment, nos entités communicantes actuelles n'en sont pas encore rendues là et quiconque a bataillé un peu pour configurer deux équipements Bluetooth jugera aisément du chemin qu'il reste à parcourir. Toutefois, les réseaux mobiles, et leur support réseau hybride, c'est à dire combinant des capacités de communication multiples [1], constituent un champ d'investigation d'une extrême importance. Il est difficile de savoir si cette vision est réaliste ou non, optimiste ou pas, mais on peut être sûr d'une chose : elle ne verra le jour que si les problèmes liés à la ***sécurité*** sont traités efficacement.

Actuellement, les objets autonomes sont sous le contrôle total de leur propriétaire. Pour établir une communication entre deux objets, les techniques actuelles de sécurité nécessitent la participation active des utilisateurs des deux objets. Leur accord respectif est obtenu sous la forme d'une manipulation à réaliser sur chacun des objets. Ce concept ne permet pas l'explosion de l'usage des objets communicants. Les objections majeures que l'on peut opposer aux techniques actuelles sont doubles. En tout premier lieu, l'intervention

systématique de l'usager restreint fortement les scénarios dans lesquels on autorise l'accès à l'objet dont on est le contrôleur, on n'imagine pas arrêter son véhicule sur le bord d'une route pour taper les commandes permettant à son assistant de navigation d'échanger des informations avec celui d'un autre véhicule. On n'imagine toutefois pas non plus laisser complètement ouvert aux communications provenant de l'extérieur son système d'aide à la navigation, avec les risques de piratages, ou de virus qui pourraient apparaître !

L'opération permettant d'autoriser un accès s'effectue généralement sans aucune information permettant d'évaluer la ***confiance*** que l'on peut faire à une telle requête, elle repose donc généralement sur un contact physique avec le propriétaire de l'objet pour laquelle est faite la requête. A ce manque d'information vient s'ajouter un autre problème majeur : l'absence de graduation dans la nature de l'échange (on laisse l'accès ou non) et la non répudiation de l'accord que l'on octroie. Les mécanismes d'établissement de la confiance actuellement déployés dans les réseaux fixes s'appliquent mal au concept d'objets communicants parce qu'ils nécessitent l'usage d'un tiers de confiance au moment de l'établissement de celle-ci.

Les solutions existantes pour la sécurité dans les réseaux sans fil Ad hoc traitent les problèmes de la sécurité de manière isolée, la plupart des propositions présupposent une phase de distribution de clefs pour protéger le routage, et assurer l'authentification des participants. Cependant, ces travaux reposent implicitement sur une infrastructure de sécurité, ce qui est contradictoire avec la nature d'un réseau Ad hoc. De nombreux travaux focalisent sur les comportements malveillants débouchant sur des attaques actives en négligeant les comportements égoïstes qui peuvent avoir des conséquences dramatiques dans le cas d'un réseau Ad hoc, ou bien concentrent sur le second type de comportement en négligeant le premier. Il nous paraît nécessaire de traiter la sécurité dans les réseaux Ad hoc de manière plus globale et en tenant compte des spécificités de tels réseaux.

La question de la confiance s'est appliquée dans le monde des télécommunications notamment dans les réseaux Ad hoc 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 [2] [5]. C'est bien cette condition qui rend ces modèles contraignants et binaires, imposant que les entités communicantes soient d'abords connus 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 tels environnements, la question qui se pose est comment valider une identité ?

Pour cela, l'objet de notre travail dans ce mémoire consiste à définir et proposer une architecture de sécurité adaptée aux réseaux sans fil Ad hoc, et prenant en compte les points suivants : un protocole de sécurité sans fil Ad hoc, doit s'appuyer sur un modèle de confiance réaliste et viable, et doit intégrer des mécanismes contrant les attaques actives, en forçant la coopération entre les nœuds, et détectant les comportements défaillants.

L'architecture proposée n'a pas la prétention de correspondre à toutes les situations d'usage de tels environnements et pose encore plus de questions qu'il n'apporte de réponse. En effet, il aborde non pas un problème spécifique de la sécurisation de ces réseaux, mais propose une architecture globale de sécurité, dynamique et auto-adaptable, permettant de gérer la mise en relation d'objets communicants.

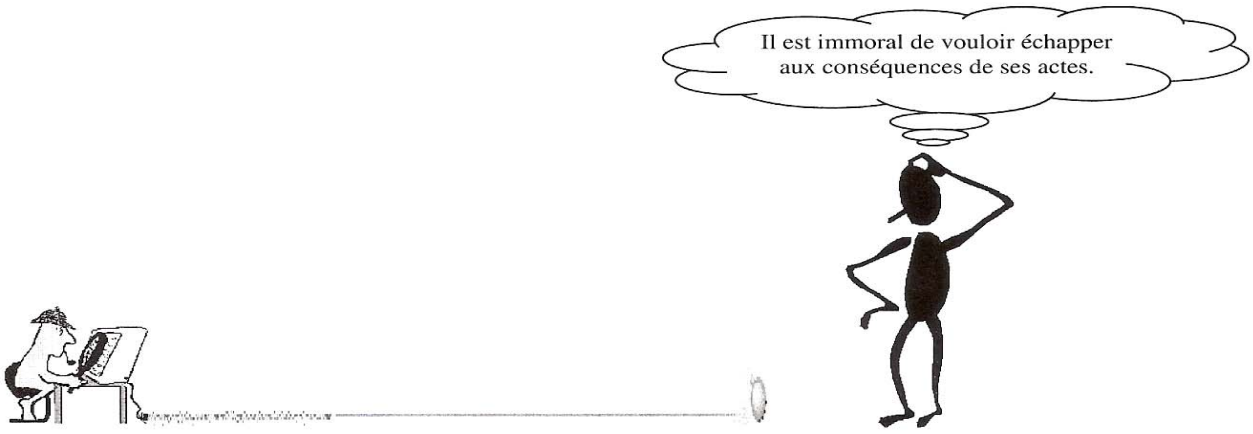
Donc, notre travail définira une architecture de sécurité repose sur la définition de la notion de confiance entre les objets désirant entrer en collaboration de façon spontanée, cette notion peut correspondre à des concepts très différents suivant le contexte dans lequel on l'emploi. L'ambiguïté de cette notion doit être levée pour permettre la définition d'une instance de l'architecture de sécurité proposée, et ouvre également de nouvelles voies pour compléter les modèles de sécurité initiaux.

En effet, dans un scénario d'usages, les mécanismes techniques doivent permettre de mettre en œuvre la politique de sécurité et d'établissement des interactions désirées par les communautés qui utilisent ces environnements. Une politique trop restrictive n'offrira que très peu de possibilités d'interaction et donc rendra le système inopérant, il en va de même d'une politique très permissive qui n'engendrera aucune confiance des utilisateurs dans le système, le rendant non pas inopérant, mais plutôt inopéré !

L'organisation générale du mémoire est décrite comme suit : Dans la première section, nous définirons précisément ce qu'est pour nous un réseau sans fil Ad hoc, nous en donnerons les principes fondamentaux, les propriétés et les protocoles que doivent suivre de telles structures, et aussi les challenges auxquels est confrontée la sécurité de ces réseaux. Dans la seconde section nous présenterons également un panorama des différentes solutions proposées auparavant pour sécuriser les réseaux Ad hoc, et nous expliquerons quelles en sont les carences. La troisième section présentera notre contribution en expliquant les objectifs de

notre modèle de confiance notamment la robustesse et la stabilité de l'architecture proposée. Enfin, et avant de conclure, nous discutons et commentons les résultats obtenus par simulations de la solution proposée.

Sécurité,
Risques et Attaques



1. Sécurité dans l'ère numérique :

"Chacun a le droit à la protection des intérêts moraux et matériels découlant de toute production scientifique, littéraire ou artistique dont il est l'auteur. » Art 27.2_Déclaration universelle des droits de l'homme (1948)." [7].

Le principe de la propriété privée est un des piliers sur lesquels se base la société moderne. La protection de cette propriété, sous forme de biens, de patrimoine, d'investissements, ainsi que le respect des domaines implicitement annexes comme la sphère privée, les droits de l'homme, etc., sont des obligations morales et légales pour l'Etat, les entreprises et les citoyens.

Les développements culturels et industriels de la fin du XIX^{ème} et du XX^{ème} siècle et la globalisation technologiques ont changé la perception de la concrétisation des biens et des valeurs, en le poussant progressivement de sa forme purement matérielle (immobiliers, produits de base, etc.) vers des formes plus abstraites, comme le soulignent par exemple l'introduction des lois internationales sur la propriété intellectuelle (droit d'auteur) [21], l'évolution du secteur tertiaire, etc. ce processus a atteint son apogée avec le début de l'ère numérique qui, en introduisant la notion du patrimoine numérique, efface les dernières frontières entre les biens réels et les biens virtuels. Apparaissent enfin les notions de produit logiciel (software mais aussi multimédia, jeux, etc.) et, par la suite l'apparition d'Internet, de ventes de numérique par le numérique au numérique (iTunes, etc.).

Pourtant, c'est cette information numérisée qui est particulièrement sensible et vulnérable à la volatilité, aux changements et à une duplication incontrôlable. En effet, le produit numérique ne connaissant point la notion d'original, toute instance doit être traitée comme un clone.

De plus la globalisation et le développement des technologies de télécommunications et des services informatiques résultent dans une normalisation et une ouverture de système d'informations (SI). La partie propriétaire dans les SIs diminue continuellement, et l'on observe ainsi la banalisation d'accès, l'interconnexion amplifiée des systèmes et une forte tendance vers une convergence des secteurs auparavant séparés, comme on le voit avec le secteur du multimédia, les communications classiques et informatiques. La facilité d'accès amplifie les échanges du bien avec son environnement, étant donné la vulnérabilité innée des biens numériques, le risque d'abus augmente avec l'exposition à l'utilisation diversifiée alors que la protection devient plus compliquée.

Dans l'ère numérique, les biens virtuels (produit en logiciel, savoir-faire, algorithmes, connaissances, renseignements, multimédia, données, etc.) deviennent partie intégrante des infrastructures de SI conçus pour rendre différents services. Confrontés à une telle répartition de la propriété numérique dans les infrastructures interconnectées de systèmes d'information, les opérateurs de ces systèmes, ses utilisateurs (les entreprises et les individus) et l'Etat doivent se poser des questions quant à la protection des informations contenues et échangées. Cette protection doit couvrir :

- L'intégralité des biens, c'est-à-dire aussi bien les contenus transportés que les parties utilisées ou stockées dans les infrastructures en question.
- L'intégralité des types des acteurs.
- L'intégralité du temps, respectant notamment les aspects de l'usage réel mais aussi les aspects légaux imposés (expiration *versus* audit).

Fournissant aujourd'hui des services critiques (contrôle aérien, défense, services d'urgence, transaction commerciales, etc.), les systèmes des télécommunications deviennent indispensables pour tous les acteurs de la société de l'information. Les indépendances entre ces infrastructures et les infrastructures critiques classiques (énergie, transport, l'eau) créent de nouveau systèmes dont la complexité et la vulnérabilité sont supérieures à celles des systèmes qui les composent. De nouvelles dispositions deviennent nécessaires pour prendre en compte les indépendances des infrastructures critiques modernes (robustesse, résiliences, innocuité, etc.).

A l'autre bout du spectre, la démocratisation de l'informatique, poussée par le progrès technologique bouleversant, crée des véritables infrastructures personnelles dans l'espace privé des individus. Dans la plupart des cas, il ne s'agit plus de systèmes isolés, mais au contraire des systèmes de plus en plus ouverts, se chevauchant dans plusieurs dimension, difficiles à délimiter en pratique. Aujourd'hui, les divers acteurs, les particuliers comme les Etats, doivent maitriser aussi bien les contenus et les opérations (transport, traitement et stockage) que sécuriser les *infosphères*, c'est-à-dire les infrastructures virtuelles crées en partie dans l'espace privé respectif par les interconnexions des SIs et le partage des biens numériques.

2. Qu'est ce que la sécurité :

Il devrait alors nécessaire de trouver une définition de la sécurité comme à un bien, un service, une infrastructure et une infosphère pour tout propriétaire concerné.

On trouve dans la littérature plusieurs définitions de la sécurité. Le dictionnaire de l'académie française [15] définit la sécurité comme suit « Sécurité. n.f. Confiance, tranquillité d'esprit qui résulte de l'opinion, bien ou mal fondée, qu'on n'a pas à craindre de danger. ».

Plusieurs aspects discutés ci-dessous sont visibles dans cette définition où la sécurité est vue comme une situation caractérisée par l'absence de tout risque pour les personnes concernées ("Je me sens en sécurité"). Bien que cette définition soit d'un niveau suffisamment haut et notamment applicable sur les SIs [7], elle définit la sécurité d'une manière faible ("bien ou mal fondée") et se positionne comme constatation, c'est-à-dire une vue a posteriori, omettant toute notion de réalisation de la situation souhaitée.

Selon une autre vision, la sécurité est souvent vue comme l'art de partager les secrets. Cette définition de sécurité est celle donnée par les cryptologues, de très bas niveau, nécessaire mais insuffisante dans beaucoup de contextes actuels. Elle se révèle difficile à appliquer sur des systèmes d'informations modernes dans une approche *top-down.*

On peut définir la sécurité de l'ère numérique [7] comme une ***quête*** pour la protection des biens numériques et la protection des systèmes de traitement des biens numériques contre tout acte non voulu ou perçu comme un abus par les propriétaires. Les actes non voulus sont typiquement possibles à cause des vulnérabilités présentes dans les SIs. L'exploitation des vulnérabilités crée des menaces et représente ainsi un risque du point de vue de propriétaire. Ainsi, les risques mènent à l'implémentation d'un ensemble de contre mesures.

Cette définition se trouve alors au croisement de la définition habituelle, visant à installer la tranquillité d'esprit et de la définition militaire [7], visant à parler des mesures. Cette définition prend comme point de départ l'existence d'un bien méritant d'être protégé dans un certain environnement de traitement. Le terme quête utilisé dans cette définition, souligne la continuité du processus et l'incertitude liée, typiques pour la sécurité, les contre-mesures doivent évoluer dans le temps, et généralement on ne sait pas si elles sont suffisantes, les contre-mesures elles mêmes pourraient avoir des vulnérabilités (leur présence se traduit par des nouveaux risques contre lesquels le propriétaire doit se protéger). De plus, par la notion de "non voulu" la définition implique la présence d'au moins deux acteurs distincts, nommés respectivement *propriétaire* et *attaquant*, dont le dernier est présumé malveillant. C'est l'attaquant qui crée des menaces en exploitant les vulnérabilités dans ou autour du bien. Le propriétaire veut minimiser ses risques et impose des contre-mesures qu'il considère comme nécessaires pour protéger le bien (voir figure 1) :

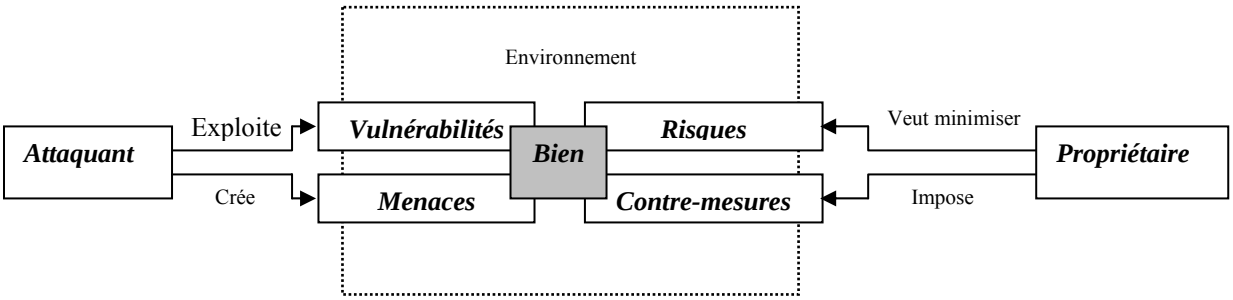


Figure 1 : <u>Les relations entre le bien, l'attaquant et le propriétaire</u>

La complexité de cette problématique est due à plusieurs facteurs. Etant donné la complexité architecturale et technologique et le dynamisme des biens dans le contexte du SI, il est ardu de cerner toutes les vulnérabilités possibles. Il est souvent difficile (c'est-à-dire couteux, trop contraignant) de réaliser l'ensemble de contre-mesures jugé nécessaire : le plus souvent, le propriétaire doit en pratique évaluer le compromis entre son estimation de la gravité d'un risque et le cout de la réalisation des contre-mesures. Il s'agit de l'analyse des risques. L'installation de l'ensemble jugé nécessaire augmente la complexité du SI initial. En effet, c'est ce nouveau système, résultant de l'ajout des contre-mesures au système initial, qui doit être évalué à nouveau. Les compromis acceptés par le propriétaire introduisent des risques résiduels, ce qui engendre souvent, à terme, de nouvelles vulnérabilités.

Ainsi, l'ensemble des contre-mesures est normalement insuffisant, d'une part à cause de l'ignorance de certaines vulnérabilités associée à la complexité des interactions entre le bien et son environnement, et d'autre part à cause de l'évaluation de risque pratiquée, typiquement liée à des modèles probabilistes (statistique de l'utilisation, confort de l'utilisation versus perception du risque, pertinence des services concernés, etc.). Evidement, il n'existe pas de modèle suffisant, car un attaquant en s'affranchissant de toute hypothèse utilise son intelligence pour trouver les vulnérabilités.

Donc la sécurité des SIs est avant tout un processus continu [14] et pas un produit final. Dans le cas idéal, la perception de l'environnement et des risques, l'estimation de la valeur de l'objet de sécurité, la recherche des vulnérabilités dans l'ensemble {système initial, contre-mesure} doivent être refaits systématiquement et périodiquement. Il n'existe pas aujourd'hui de système standard pour répondre aux exigences de chacune de ces phases pour différentes cibles, ni des spécifications pour les périodes exactes.

Classiquement le processus de sécurité est décomposé en trois aspects se référant à l'objet de sécurisation en spécifiant notamment ce qui doit être protégé. Cette vue de la sécurité est connue sous la trinité ***CIA*** (Confidentialité, intégrité et disponibilité). Cette décomposition est aujourd'hui normalement insuffisante, car elle ne couvre pas bien certaines nouvelles menaces comme les virus informatiques, les messages non sollicités, ou l'utilisation abusive.

Une autre approche se réfère à la question comment protéger le bien et décompose le processus de sécurité en phases de *Prévention, Détection* et *Réaction*, typiquement dénommées PDR. Il est évident que la réalisation de mécanismes pour ces phases sera également liée aux aspects de la *qualité de service.*

3. Confiance et subjectivité :

On note deux aspects importants inhérents à toute définition de la sécurité : le premier aspect est la notion de la ***confiance***, il est évident que la confiance absolue dans tout acteur de l'environnement étudié enlève le besoin pour la sécurité de la même façon que la méfiance totale interdit toute exposition d'un actif à son environnement et met en question la notion de la propriété privée. En effet, si tout acte possible sur l'actif est perçu comme un risque, le système converge inévitablement vers la clôture totale. Ceci souligne l'interdépendance entre la confiance et la sécurité [7] : le partage d'un secret présume aussi bien une confiance initiale que la notion du confort vis-à-vis des risques. De même, l'existence des parties du système. Pourtant dans le cas général, on ne connaît pas de transformation directe entre la confiance et la sécurité. Malgré leur influence mutuelle, il faut faire une distinction nette entre la sécurité et la confiance.

Le deuxième aspect important est la ***subjectivité***. En effet, pour le même bien dans le même environnement, l'évaluation des risques peut être radicalement différente. Elle ne dépend pas seulement de la confiance présumée (se basant par exemple sur des connaissances et des expériences du propriétaire) mais aussi de son investissement et principalement de son positionnement par rapport à l'objet (c'est-à-dire ses cibles, ses intérêts, l'utilisation prévue).

La subjectivité et la confiance doivent être évaluées dans le contexte de l'environnement visé (militaire/hostile, civil/courtois). Par définition, la subjectivité de la sécurité ne pose pas de problèmes fondamentaux quant à l'évaluation de la sécurité, si le bien est isolé du monde extérieur, et si l'environnement du bien d'un propriétaire ne chevauche pas avec les environnements des autres propriétaires (systèmes fermés, systèmes propriétaires, etc.). Mais dans l'ère numérique, plus souvent le contraire est le cas, les biens numériques de différents

propriétaires, il est souvent normal que le bien traverse pendant son traitement plusieurs dizaines de systèmes rendant des services différents. La complexité des interactions, les natures très différentes des biens mêmes et les évaluations de dangers très différentes posent un énorme problème quant à l'évaluation de risques pour la globalité du système.

Dans le cas général, il est en effet impossible de comparer deux ensembles de contre-mesures. De plus, on observe l'interdépendance naturelle entre la subjectivité et la confiance. A cause de cette interdépendance, les ensembles de contre-mesures demandés par deux propriétaires dans le cas d'un échange peuvent contenir des exigences contradictoires ou sémantiquement non recouvrables, une mesure de protection exigée pour un bien X peut se révéler irréalisable en vue d'une composition d'une série de traitements séquentiels, etc.

4. La relation service-sécurité :

La définition de sécurité utilisée ci-dessus saisit explicitement le service comme une cible à protéger. En effet, tout service, étant économiquement parlant un équivalent immatériel d'un bien, possède dans le cas général une valeur pour son offreur. Cette valeur est justifiée par l'investissement initial dans l'infrastructure du service, par le cout du maintien quotidien et des évolutions possibles, et par les objectifs commerciaux ou autre de cette offre. De plus implicitement, chaque service présume une interaction de son offreur (dans le cadre du service, c'est-à-dire contractuelle) avec au moins un deuxième acteur, l'utilisateur. Chaque service sous-entend donc une ouverture vers l'extérieur représente par l'interface d'accès par les utilisateurs. De plus, généralement, l'ensemble des utilisateurs prévus d'un service est un vrai sous-ensemble de l'ensemble total des acteurs. Par conséquence, chaque service est naturellement exposé aux menaces : en absence de contre mesures (contrôle d'accès), l'utilisation de chaque service (indépendamment de sa sémantique) est étroitement liée à la notion d'abus. La sémantique ajoute d'autres risques et pour l'offreur et pour l'utilisateur : en effet, les données échangées dans le cadre du service doivent normalement être réservées à leur destinataire, le fait de participation à un service est également une information confidentielle (par exemple protection de la sphère privée). En conséquence, chaque service nécessite une analyse du système propre au service et prenant en compte tout acteur impliqué dans son exécution. Le contrat de service est utile, parmi d'autres, pour homogénéiser la politique de sécurité des acteurs et créer une base de confiance entre les partenaires.

Au contraire, dans le cas général, la sécurité ne peut pas être vue comme un service. Le problème est dans la définition de la sécurité, souligné par la liaison intrinsèque et intime des

mesures de la sécurité à leur cible. Tout d'abord, la notion de "*service de sécurité*" suggère une sécurisation d'un bien (par exemple d'un service) peu ou pas assez sécurisé. Or, il serait préférable de réfléchir à des besoins et des problèmes de sécurité avant l'exposition du bien à son environnement (par exemple avant le déploiement de service, notamment dans la phase de conception). Ensuite la subjectivité de l'appréciation de la sécurité d'un même bien est généralement impossible à résoudre, même en présumant une grande flexibilité du service (par exemple par personnalisation). La protection d'un bien par un service de protection ajoute au moins un partenaire "l'offreur du service de protection" ce qui peut contredire les exigences de certains propriétaires. L'exemple typique est le fournisseur de l'infrastructure du service, cette dernière exige des mesures de protection, mais elles sont à intégrer dans l'infrastructure même et ne peuvent donc pas appartenir à une tierce personne.

Généralement, la sécurité reste une propriété non fonctionnelle, souvent invisible mais intrinsèque à chaque service "on ne peut pas l'activer et la désactiver", on ne peut pas s'abonner à l'utilisation de sécurité. Autrement dit, chaque service, il faut prévoir un sous-système de sécurité, même si celui-ci reste invisible à l'utilisateur de service. Néanmoins, en pratique la sécurité peut être proposée comme un service dans certains cas de figures. Cela semble notamment applicable pour des services statiques, bien analysés, bien déployés et acceptés, c'est-à-dire pour les cas où les modèles de menaces sont approuvés, et les mesures de protection sont jugées largement suffisantes (par exemple par la pratique quotidienne : observation du risque réel sous la protection appliquée).

Ce sont surtout les *nouveaux services* qui entrainent le déroulement socio-technologique d'une spirale de développement mutuel des vulnérabilités et des mesures de protection. Les nouveaux services définissent de nouveaux usages et donc de nouveaux scénarios, ils subissent alors de nouveaux abus. De plus, la pression commerciale pour le déploiement des nouveaux services (effet de concurrence féroce sur le marché, etc.) étant importante, les nouveaux services sont souvent déployés avec une analyse insuffisante : les vulnérabilités sont naturellement méconnues et les modèles de menaces ne correspondent pas à la réalité. Dans cette situation, le service est souvent déployé avec un accent sur sa forme fonctionnelle. Toutefois, en fonction de progrès du déploiement, de nombreuses vulnérabilités sont découvertes. Celles-ci, exploitées par les attaquants, créent des menaces réelles, car ils débouchent sur un ensemble d'attaques. Perçues comme des risques par les offreurs et les utilisateurs, elles freinent le déploiement du service rendant l'investissement nécessaire dans les contre-mesures supérieur aux pertes liées à la gêne du déploiement.

Comme exemples de nouveaux services qui récemment ont engendré un changement radical dans la compréhension du besoin de protection, nous pouvons citer, la mobilité, les communications sans fil, et les nouvelles applications et formes de communications (communications égal-à-égal / pair-à-pair, etc.).

5. *Objectifs de la sécurité* :

On peut résumer les objectifs ou services de la sécurité dans les six (6) points suivants :

5.1. Confidentialité :

La confidentialité est de garder secret le contenu de l'information et empêcher (ou prévenir) sa divulgation à des entités (sites, organisation, personnes, etc.) non habilitées à le connaître. Seuls les destinataires prédéterminés doivent être capables de lire le contenu du message.

La confidentialité permet de rendre la lecture de l'information inintelligible à des tiers non autorisés lors de sa conservation ou surtout de son transfert. Dans le domaine des entreprises cette garantie concerne [9] [3] :

✓ Le droit de propriété des secrets de fabrication et des informations stratégiques de l'entreprise, et :

✓ Le droit des individus, défini par la loi informatique et liberté.

5.2. Intégrité :

L'intégrité est d'assurer que les données n'ont pas été modifiées et empêcher toute modification (intentionnelle ou accidentelle) non explicitement requise par une entité habilitée. Cela permet, par exemple, au récepteur d'un message d'être raisonnablement assuré que le message reçu est le même que le message envoyé. Donc, l'intégrité des données est la propriété qui assure qu'une information n'est modifiée que dans des conditions prédéfinies (selon des contraintes précises).

5.3. Authentification :

Le but de l'authentification est de garantir l'origine :

✓ d'une information : Prouver qu'une information provient de la source annoncée (auteur, émetteur).

✓ d'une personne (ou machine, groupe ou organisation) : Prouver que l'identité est bien celle annoncée.

5.4. Autorisation :

Interdire l'accès d'un service à toute entité non explicitement autorisée à y accéder (accès indu).

5.5. Disponibilité :

Assurer un accès effectif et fiable au service pour toute entité autorisée (empêcher le déni de service (DoS)).

5.6. Non-Répudiation :

Fournir des éléments de preuve (en temps réel ou a posteriori) sur :

- ✓ La réalité de certaines actions.
- ✓ Les tentatives d'actions non autorisées.

La Non - Répudiation est une propriété qui assure que l'auteur d'un acte ne peut ensuite nier l'avoir effectué (signature de l'acte) et que le récepteur ne peut ultérieurement dénier avoir reçu un message (exemple exécution d'un ordre boursier, d'une commande, etc.).

6. *Risques et menaces pour les systèmes de télécommunications* :

6.1. *Définitions* [4]:

a. Menace **:** Possibilité de faire une tentative, non autorisée, pour accéder ou manipuler une information ou de rendre un système inutile ou non fiable. Les menaces peuvent être :

- Des problèmes non spécifiques à l'informatique : tels que les accidents, le vol et le sabotage du matériel, départ de personnel stratégique, grèves, etc.
- Des erreurs non intentionnelles : Telles que les pannes (disfonctionnement du matériel ou des logiciels), les erreurs de manipulation ou les erreurs de conception ou d'implémentation des applications.
- Menaces intentionnelles passives : Ecouter ou accéder de manière non autorisée à l'information, et détourner des données en faisant par exemple des copies illicites. Dans ce cas on parle de violation de contrainte de confidentialité des données.
- Menaces intentionnelles actives : Soit par la modification des informations et des logiciels (exemple fraude financière informatique, sabotage des informations), il s'agit dans ce cas d'une atteinte à l'intégrité des données. Soit par détérioration de tout ou partie des données et ressources d'un système afin de le rendre inutilisable (bombe logique, virus,

ver, etc.), c'est le cas de la violation de la contrainte de disponibilité des données et des ressources d'un système.

b. Risque **:** Exposition accidentelle et imprévisible de l'information ou violation de l'intégrité des opérations due au mal fonctionnement du hardware ou à un software incorrect ou incomplet.

c. Vulnérabilité **:** Défaut, connu ou suspecté, dans la conception d'un software, un hardware ou dans les opérations d'un système qui l'expose aux pénétrations ou à ce qu'il révèle certaines informations.

d. Attaque **:** Mise en œuvre d'un plan pour exécuter une menace.

e. Pénétration **: A**ttaque avec succès.

f. Intrus interne **:** Est soit un :

- Utilisateur légitime qui accède à des informations non autorisées.
- Utilisateur légitime qui prend l'identité d'un autre.
- Intrus externe qui a réussi à avoir une identité interne.
- Clandestin, qui est un pénétrateur malin, qui efface ou déguise les traces de sa pénétration.

g. Intrus externe **:** Un étranger à l'organisation ou quelqu'un de l'organisation qui n'est pas autorisé à utiliser le système (femme de ménage). Avec le développement des systèmes réseaux, il peut être aussi quelqu'un qui est autorisé à utiliser le système mais pas la partie ciblée.

h. Pirate **:** Le pirate est généralement décrit comme un individu acharné passant ses jours et ses nuits dans d'obscures salles informatiques, entouré de pizzas et de tasses à café, pour espionner les réseaux informatiques de notre planète, à l'affût de quelques failles qui lui ouvriraient l'accès aux données secrètes ou aux serveurs protégés. Pour être pirate aujourd'hui, à cause de la démocratisation d'Internet, il n'est plus nécessaire d'être spécialisé dans les problèmes informatiques, ni de disposer de connaissances approfondies, encore moins d'avoir une longue expérience en informatique. Il suffit de connaître les bonnes adresses web ou de savoir manipuler habilement un moteur de recherche pour repérer les informations et les programmes voulus en quelques secondes [8].

i. Hacker **:** Le terme "hack" a été utilisé pour désigner un procédé de programmation élégant ou très astucieux, obligeant l'ordinateur à accomplir des taches pour lesquelles il n'était nullement prévu. Celui qui en a les aptitudes est appelé "hacker", c'est un maître en

informatique. Aujourd'hui la notion de hacker est étendue au domaine de la violation des données, dans ce contexte on parle de crackers. Il détruit les données d'autrui ou provoque volontairement des désastres. Un hacker est une personne plutôt constructive ayant hérité de l'âme de ses inventeurs, s'il découvre une faille, il met en garde le concerné sans causer de dégâts, c'est le cas de celui qui a trouvé des failles dans un système informatique d'une banque mais qui n'a retiré qu'un centime symbolique comme preuve de faits.

6.2. Le rôle des systèmes des télécommunications :

En tant que dénominateur commun de toute interconnexion de systèmes d'informations modernes, les systèmes des télécommunications sont au cœur de l'ère numérique. Ils forment ainsi l'interface cruciale et se retrouvent au point critique du point de vue de sécurité.

Historiquement formés par une infrastructure fermée sous le contrôle de l'état, ce sont les systèmes des télécommunications qui ont subi le changement le plus radical durant ces dernières décades.

Aujourd'hui, les systèmes des télécommunications sont considérés comme des infrastructures critiques. Leur protection devient même une préoccupation politique [7] plus que commerciale et personnelle. Tout acteur impliqué (Etat, entreprise, particuliers) doit assumer les responsabilités autour des systèmes des télécommunications qui se trouvent au centre de leurs usages quotidiens. Ces responsabilités peuvent être dues aux risques perçus (et dépendent dans ce cas du positionnement de l'acteur par rapport au système en question) mais aussi d'une nature légale.

Les réseaux (optique, filaires et sans fil) sont des composants principaux des systèmes des télécommunications. Ces réseaux et leurs utilisateurs sont exposés à plusieurs risques. Nous classifions ici ces risques selon un modèle qui distingue les rôles des propriétaires des données et des propriétaires des infrastructures les traitant.

7. Des vulnérabilités filaires aux vulnérabilités dans le sans-fil :

Le médium sans fil est très vulnérable par sa nature, beaucoup plus vulnérable que le medium filaire. Le médium sans fil permet un accès libre de tout acteur : la lecture, l'injection, la suppression et la modification des données sont possibles dans la plupart des configurations. De plus toute communication est de nature purement virtuelle : en général, on ne peut ni limiter le périmètre du réseau (à cause de propriété physiques : l'affaiblissement est fort, mais la propagation multi-chemin, les réflexions/réfraction, etc., produisent souvent des

résultats étonnants), ni distingues ses vis-à-vis. Autrement dit, le médium ne permet pas de limiter le cercle des acteurs impliqués dans le traitement des données envoyées. Il ne permet pas non plus de détecter si un accès au médium ou aux données a eu lieu pendant la transmission.

Pour un attaquant le medium sans fil est souvent plus attractif, car il ne nécessite pas de la présence physique de l'attaquant. Bien équipé, il est capable de monter des attaques contre les vulnérabilités naturelles du medium en restant en dehors du domaine attaqué (*parking lot attack*). De plus, les attaques peuvent être autorisées ou au moins semi-automatisées facilement. Les équipements peuvent enregistrer les trames reçues pour espionner l'infrastructure rencontrée (*wardriving*) ou même un traitement autonome a posteriori (attaque par dictionnaire, attaque par force brute), même sans exploiter les failles éventuelles dans les contre-mesures de sécurité normalement implémentée dans ce genre de réseaux (principalement contrôle d'accès, confidentialité et intégrité).

Pour pallier les problèmes de transmission, les systèmes de gestion, les machines à état et les piles protocolaires employés dans ces réseaux exposent souvent une complexité élevée au niveau d'implémentation de la carte réseau, des pilotes, des applications dédiées, etc. Ils représentantes ainsi des nouvelles vulnérabilités et donc cibles d'attaques.

Les terminaux utilisés dans les réseaux sans fil sont caractérisés par leur probabilité. Ils sont alors petits, possèdent souvent une interface homme-machine (IHM) restreinte, limités au niveau des capacités de calcul et de stockage et alimentés par une batterie.

Ces caractéristiques ont un impact important sur la sécurité du terminal, et, par extension du SI les employant. L'interface IHM limitée pose souvent des problèmes dans les phases d'appairage et de contrôle d'accès (comment faire entrer un mot de passe dans un pair d'écouteurs, comment établir une identité unique d'une clé USB, etc.). les capacités de calcul (CPU) et stockage (mémoire, disque) limitées introduisent des contraintes quant aux calculs possibles. Il est par exemple assez ardu de vouloir faire du calcul aux clés privées dans un équipement embarqué comme un capteur ou même un téléphone portable sans un module dédié.

L'alimentation par la batterie provoque aussi bien un changement de comportement (On/Off inattendu, techniquement proche de la mobilité) et nécessite de système de gestion supplémentaire (gestion de veille, des mécanismes de paging, etc.). De plus, le développement

des technologies de batterie est constant mais linéaire, il ne peut pas suivre la vitesse du développement exponentiel de la microélectronique (loi de Moore).

Au delà de ces aspects, les réseaux basés sur la transmission radio ajoutent un degré de liberté à toute une transmission : le contexte spatio-temporel. Il est alors raisonnable de parler de la mobilité, du nomadisme et de la localisation des utilisateurs connectés par ce medium. Ces nouvelles libertés justifient des services de la mobilité ou encore de la localisation (*location-based service*, etc.).

La mobilité représente en effet un problème connu pour la sécurité car elle introduit non seulement des nouveaux mécanismes et sous-systèmes et donc une nouvelle complexité mais surtout la présence potentielle de plusieurs domaines d'autorité. Donc la sécurité de la mobilité doit être traitée avec une prudence élevée. Le problème c'est que les mécanismes de sécurité interviennent souvent en même temps que les mécanismes typiques de mobilité comme le changement de cellule.

8. Conclusion :

La sécurité constitue un problème essentiel dans les systèmes des technologies de l'information modernes. Il se posera certainement de manière encore plus importante dans les technologies du futur (réseau des capteurs, Internet du futur, réseaux autonomes, 4G, etc.). La démocratisation des technologies de l'information et des communications, matérialisée par l'interconnexion de divers systèmes (filaires, sans fil, autonomes ou autres), rend la protection des données et des infrastructures considérablement plus complexe.

Malgré les problèmes de sécurité intrinsèque, les réseaux sans fil continueront à se développer dans plusieurs marchés verticaux comme les télécommunications, les applications industrielles et le M2M (machine-to-machine) et la domotique. Il est important de bien connaître les difficultés liées à la mise en place de ce type de réseaux, mais aussi les nouvelles opportunités qu'ils proposent et les particularités de provisionnement du service dans ce nouveau monde interconnecté et communicant.

Incapable de trouver un bon compromis entre la sécurité et son coût pour les services requis par leurs propres moyens, les entreprises et les particuliers deviennent plus exigeants sur les garanties de sécurité que leur apportent les fournisseurs des services. La sécurité apparaît donc comme l'un des enjeux majeurs pour la commercialisation des services et des produits dans le domaine des SIs et dépasse les dimensions purement techniques. Aujourd'hui, la sécurité concerne tous les acteurs impliqués (opérateurs des réseaux,

fournisseurs des services, intégrateurs des systèmes, utilisateurs, Etat, etc.). La législation, les industriels, les académiques et les utilisateurs sont appelés à collaborer pour développer des meilleurs méthodologies pour les processus de protection.

Une sensibilité accrue aux problématiques de sécurité se reflète aujourd'hui dans les débats politiques, le marketing des produits et les demandes des clients. En même temps, une panoplie de travaux est menée par les académiques, les industriels et dans le cadre de consortiums et d'organismes de normalisation afin d'apporter des améliorations et de définir des solutions plus robustes.

En revanche, il faut comprendre qu'il ne peut pas y voir de sécurité standardisée, suffisante pour tout le monde. Cela est dû à l'appréciation très différente des risques autour d'un même bien dans un environnement donné mais surtout à cause de la complexité croissante des SIs. De plus le développement constant des nouveaux services et de nouveaux produits amène des nouvelles vulnérabilités, dont la gravité ne peut être mesurée à l'avance, car elle dépend parmi d'autre de l'échelle du déploiement. La sécurité reste un processus qui doit accompagner le développement d'un système d'information. Le monde devenant plus connecté et plus communicant, les problèmes de sécurité vont probablement s'aggraver dans le futur.

Réseaux sans fil
Ad hoc

1. Introduction :

Les équipements mobiles deviennent de plus en plus petits et puissants en termes de capacité de traitement et de stockage de données. De plus, ils sont dotés d'une multitude de fonctionnalités qui permettent d'assurer différents types d'applications et de services.

Parmi les applications et services offerts via un équipement mobile, figurent les services de connexions et les services de données correspondants. Ces derniers représentent le service le plus demandé par les utilisateurs mobiles. Par exemple, les connexions entre deux téléphones mobiles cellulaires sont assurées par les BSC (Base Station Controller) et les MCS (Mobile services Switching Center), les ordinateurs portables sont connectés à Internet via des points d'accès fixes.

Il y a, en outre, des situations spécifiques où les besoins de connexions des utilisateurs ne sont pas assurés par le réseau dans une zone géographique donnée. Dans cette situation fournir la connectivité est un réel défi. Récemment, de nouvelles alternatives pour fournir les services ont été proposées. Elles sont basées sur le fait d'avoir des stations mobiles interconnectées les unes aux autres grâce à une configuration autonome, créant ainsi un réseau Ad hoc flexible et performant. Parallèlement, le réseau Ad hoc peut être utilisé pour l'extension d'un réseau filaire. Dans ce cas, les nœuds mobiles peuvent avoir accès à l'Internet à travers une passerelle, pour étendre les services de l'Internet au-delà de l'infrastructure filaire.

Historiquement, les réseaux mobiles Ad hoc ont été d'abord introduits pour l'amélioration des communications dans le domaine militaire. Dans ce contexte, il n'existe pas d'infrastructure existante pour relier les communications, vue la nature dynamique des opérations et des champs militaires.

Les premières applications dans les réseaux Ad hoc sont apparues avec le projet PRNet (Packet Radio Network) [12] en 1972. Ce projet a été inspiré par l'efficacité la technologie par commutation de paquet, le partage de la bande passante, le routage 'store-and-forward', et ses applications dans l'environnement mobile sans fil.

SURAN (Survivable Radio Networks) [20] a été développé par la DARPA en 1983 pour dresser les principaux problèmes du projet PRNet dans le domaine de la stabilité, la sécurité, la capacité de traitement et gestion d'énergie. Les objectifs étaient de proposer des algorithmes qui peuvent supporter jusqu'à une dizaine de milliers de nœuds, tout en utilisant des mécanismes radio simples, avec une faible consommation d'énergie, et un faible coût. Ce

travail a amené à la conception de la technologie LPR (Low-cost Packet Radio) [22] en 1987, dotée d'une couche radio DSSS (Direct Sequence Spread-Spectrum) avec un processeur pour la commutation de paquets intégré (Intel 8086). De plus, une famille de protocoles pour la gestion du réseau a été développée, et une topologie hiérarchique du réseau basée sur un clustering dynamique est utilisée pour remédier au problème de la stabilité. Des améliorations pour l'adaptabilité de la couche radio, la sécurité et l'augmentation de la capacité ont été proposées.

L'évolution des infrastructures du réseau Internet et la révolution de la micro informatique ont permis de rendre faisables et applicables les idées initiales des réseaux radio de paquets. Le programme GloMo (Global Mobile) [25] initié par la DARPA en 1994 avait comme objectif de supporter les communications multimédia n'importe quand et n'importe où à travers des équipements sans fil.

Tactical Internet (IT) [12] est l'une des implémentations des réseaux sans fil Ad hoc grandeur nature développée par l'armée américaine en 1997, utilisant des débits de plusieurs dizaines de kilobits par seconde.

Un autre déploiement a été réalisé en 1999, avec ELB ACTD (Extending the Littoral Battle-space Advanced Concept Technology Demonstration) [30] qui permet de démontrer la faisabilité de concepts militaires pour les communications des bateaux en mer aux soldats sur la terre par l'intermédiaire d'un relais aérien. 20 nœuds dans le réseau ont été considérés.

2. Les Réseaux sans fil Ad hoc :

2.1. Définition :

Les réseaux Ad hoc auxquels nous nous sommes intéressés sont ceux décrits et étudiés par le groupe de travail Mobile Ad-hoc NETworks (MANET) de "l'Internet Engineering Task Force (IETF)".

Une définition de ces réseaux est donnée formellement dans la RFC 2501 [24]. Il s'agit de réseaux sans fil qui composent de systèmes informatiques divers, plus ou moins complexes, appelés nœuds, par la suite, ayant la possibilité de communiquer de manière autonome par ondes radio, Les nœuds interagissent et peuvent coopérer pour s'échanger des services. Ces réseaux sont dits Ad hoc dans la mesure où ils ne nécessitent pas d'infrastructure fixe. Ils peuvent exister temporairement pour répondre à un besoin ponctuel de communication. Le mode de fonctionnement Ad hoc se distingue du mode infrastructure dans lequel les nœuds du

réseau communiquent entre eux via un point d'accès, aussi appelé base, qui peut être relié à un réseau fixe. La figure 2 montre la différence d'utilisation des réseaux sans fil en mode infrastructure fixe et en mode Ad hoc.

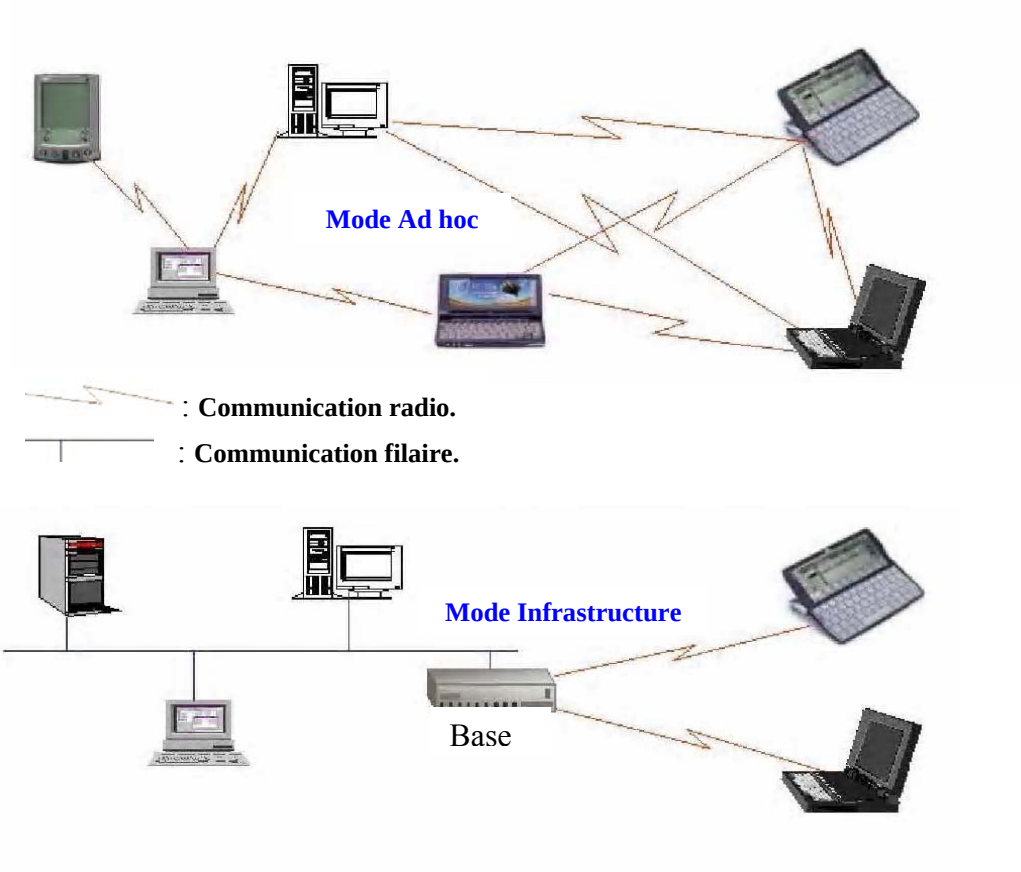


Figure 2 : Mode Ad hoc versus mode Infrastructure

Les réseaux sans fil Ad hoc s'appuient sur les technologies sans fil conçues à l'origine pour des réseaux locaux et domestiques :

✓ Les technologies IEEE 802.11a, 802.11b (*Wireless Fidelity, Wifi*), 802.11g, HiperLan/1 (remplacé par HiperLan/2). HomeRF (*SWAP*) : sont propres aux réseaux WLAN (*Wireless Local Area Network*).

✓ La technologie Bluetooth, pour les réseaux WPAN (*Wireless Personal Area Network*). Bluetooth fonctionne en mode point à point ou point à multipoint.

✓ Les technologies infrarouges (*IrDA. Infrared Data Association*), utilisées dans les télécommandes par exemple, peuvent aussi être considérées comme support des réseaux Ad-hoc. Mais ces technologies se limitent à des communications point à point.

✓ Les technologies Wifi. IEEE 802.11g. HiperLan. HomeRF et Bluetooth opèrent dans la bande ISM (*Industrial, Scientific and Medical*) à 2.4 GHz alors que 802.11a opère dans la région des 5 GHz.

Les réseaux Ad hoc peuvent également être connectés au monde filaire (figure 3) par l'intermédiaire d'une ou plusieurs passerelles, que nous appellerons, en référence au monde cellulaire IP, des points d'accès (AP). De tels réseaux sont communément appelés réseaux hybrides [26]. Chaque terminal du réseau Ad hoc, s'il possède une double interface filaire et sans fil peut donc agir en tant que passerelle pour les autres clients de la bulle Ad hoc. Les réseaux hybrides constituent les prémices de l'Internet ubiquitaire de demain.

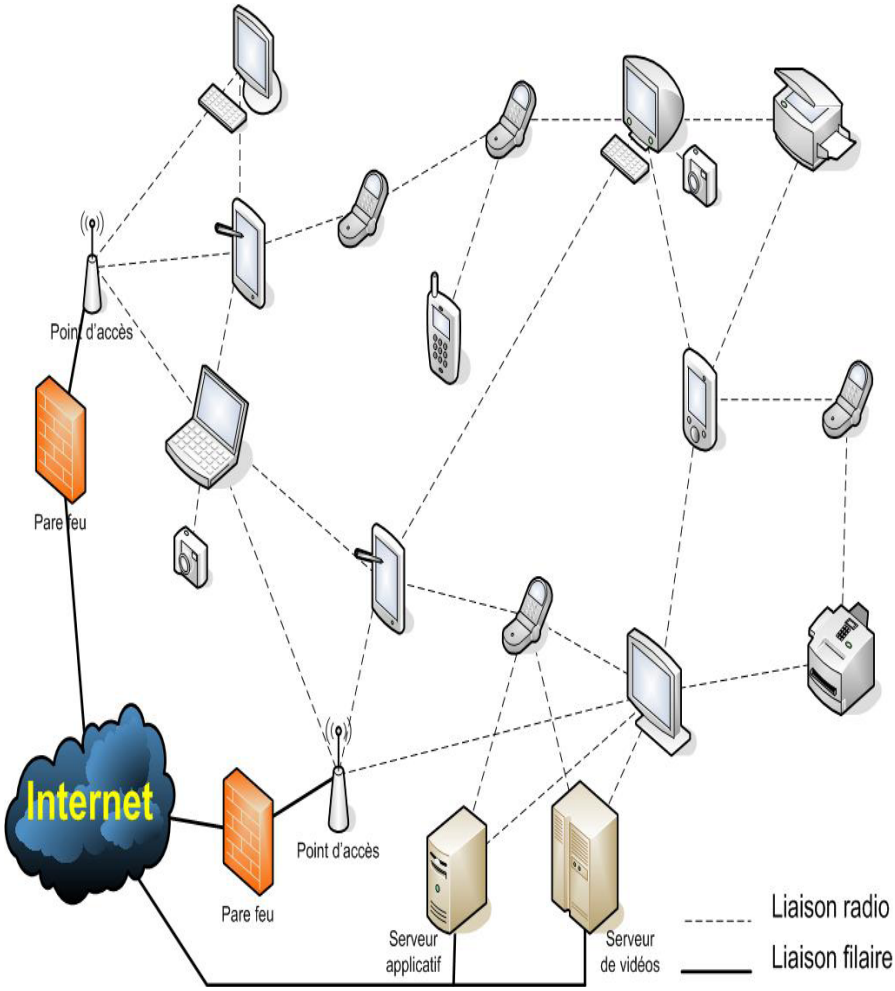


Figure 3 : <u>Un réseau Ad hoc</u>

2.2. Contextes d'utilisation des réseaux Ad hoc :

Les premières applications des réseaux Ad hoc concernaient les communications et les opérations dans le domaine militaire. Cependant, avec l'avancement des recherches dans le

domaine des réseaux et l'émergence des technologies sans fil (ex : Bluetooth, IEEE 802.11 et HiperLan), d'autres applications civiles sont apparues. On distingue :

✓ Les services d'urgence : Opération de recherche et de secours des personnes, tremblement de terre, feux, inondation, dans le but de remplacer l'infrastructure filaire.

✓ Le travail collaboratif et les communications dans des entreprises ou bâtiments : Dans le cadre d'une réunion ou d'une conférence par exemple.

✓ Home network : Partage d'applications et communications des équipements mobiles.

✓ Applications commerciales : Pour un paiement électronique distant (taxi) ou pour l'accès mobile à l'Internet, où service de guide en fonction de la position de l'utilisateur.

✓ Réseaux de senseurs : Pour des applications environnementales (climat, activité de la terre, suivi des mouvements des animaux, etc.), ou domestiques (contrôle des équipements à distance).

✓ Réseaux en mouvement : Informatique embarquée et véhicules communicants.

✓ Réseaux Mesh : C'est une technologie émergente qui permet d'étendre la portée d'un réseau ou de le densifier.

En plus, dans un WLAN, un réseau Ad hoc fournit une solution pour étendre une couverture sans fil avec un moindre coût. Dans un WPAN (ex : UMTS), il permet d'accroître la capacité globale du réseau sans fil. En fait, plus de bande passante agrégée peut être obtenue en réduisant la taille des cellules et en créant des pico-cellules. Afin de supporter une telle architecture, les opérateurs disposent de deux options : déployer plus de stations de base (une station de base par cellule), ou utiliser un réseau Ad hoc pour atteindre la station de base. La deuxième solution est clairement plus flexible et moins coûteuse.

2.3. Propriétés et spécificités des réseaux Ad hoc :

En général, un réseau Ad hoc mobile est considéré comme un système autonome dynamique composé de nœuds mobiles interconnectés par des liens sans fil, sans l'utilisation d'une infrastructure fixe et sans administration centralisée [31]. Les nœuds sont libres de se déplacer aléatoirement et s'organisent arbitrairement. Par conséquent, la topologie du réseau peut varier de façon rapide et surtout imprévisible. La route entre un nœud source et un nœud destination peut impliquer plusieurs sauts sans fil, d'où l'appellation de "réseaux sans fil multi-sauts". Un nœud mobile peut communiquer directement avec un autre nœud s'il est dans sa portée de transmission. Au delà de cette portée, les nœuds intermédiaires jouent le rôle de routeurs (relayeurs) pour relayer les messages saut par saut.

Les réseaux Ad hoc héritent des mêmes propriétés et problèmes liés aux réseaux sans fil. Particulièrement, le fait que le canal radio soit limité en termes de capacité, plus exposé aux pertes (comparé au médium filaire), et sujet à des variations dans le temps. Le canal est confronté aux problèmes de "station cachée" et "station exposée". En outre, les liens sans fil sont asymétriques et pas sécurisés.

D'autres caractéristiques spécifiques aux réseaux Ad hoc conduisent à ajouter une complexité et des contraintes supplémentaires qui doivent être prises en compte lors de la conception des algorithmes et des protocoles réseaux, à savoir :

- ✓ ***L'absence d'une infrastructure centralisée*** : Chaque nœud travaille dans un environnement pair à pair distribué, et agit en tant que routeur pour relayer des communications, ou génère ses propres données. La gestion du réseau est ainsi distribuée sur l'ensemble des éléments du réseau.
- ✓ ***La mobilité des nœuds et maintenance des routes*** : La mobilité continue des nœuds, crée un changement dynamique de topologie. Par exemple, un nœud peut joindre un réseau, changer de position ou quitter le réseau. Ce déplacement a naturellement un impact sur la morphologie du réseau et peut modifier le comportement du canal de communication. Ajoutons à cela la nature des communications (longues et synchrones, courtes et asynchrones, etc.). Les algorithmes de routage doivent ainsi résoudre ces problèmes et supporter la maintenance et prendre en charge en un temps limité la reconstruction des routes tout en minimisant l'overhead généré par les messages de contrôle.
- ✓ ***L'hétérogénéité des nœuds*** **:** Un nœud mobile peut être équipé d'une ou plusieurs interfaces radio ayant des capacités de transmission variées et opérant dans des plages de fréquences différentes. Cette hétérogénéité de capacité peut engendrer des liens asymétriques dans le réseau. De plus, les nœuds peuvent avoir des différences en termes de capacité de traitement (CPU, mémoire), de logiciel, de taille (petit, grand) et de mobilité (lent, rapide). Dans ce cas, une adaptation dynamique des protocoles s'avère nécessaire pour supporter de telles situations.
- ✓ ***La contrainte d'énergie*** : Les équipements mobiles disposent de batteries limitées, et dans certains cas très limitées tels que les PDA, et par conséquent d'une durée de traitement réduite. Sachant qu'une partie de l'énergie est déjà consommée par la fonctionnalité du routage. Cela limite les services et les applications supportées par chaque nœud.

- ✓ ***La taille des réseaux Ad hoc*** : Elle est souvent de petite ou moyenne taille (une centaine de nœuds), le réseau est utilisé pour étendre temporairement un réseau filaire, comme pour une conférence ou des situations où le déploiement du réseau fixe n'est pas approprié (ex : catastrophes naturelles). Cependant, quelques applications des réseaux Ad hoc nécessitent une utilisation allant jusqu'à des dizaines de milliers de nœuds, comme dans les réseaux de senseurs [12]. Des problèmes liés au passage à l'échelle tels que : l'adressage, le routage, la gestion de la localisation des senseurs et la configuration du réseau, ***la sécurité***, etc., doivent être résolus pour une meilleure gestion du réseau.
- ✓ ***La faible sécurité :*** Il est facile 'd'espionner' un canal radio de manière passive. Les protections ne pouvant pas se faire de manière physique (il est en général difficile d'empêcher quelqu'un de placer discrètement une antenne réceptrice très sensible dans le voisinage), elles devront être mises en place de manière logique, avec de la cryptographie ou éventuellement des antennes très directionnelles. Mais le canal radio restera quoiqu'il en soit vulnérable à un brouillage massif (attaque de type denial of service). Dans les réseaux Ad hoc, non seulement les données sont vulnérables comme dans tout réseau radio, mais consécutivement au point précédent, il en est de même pour le trafic de contrôle et de gestion du routage [32], [33]. Les problématiques de la sécurité dans les réseaux Ad hoc sont donc très complexes, puisque l'on cherche à autoriser de nouveaux mobiles à participer au réseau, tout en évitant des nœuds "malins" qui détourneraient ou perturberaient le fonctionnement même du routage.
- ✓ ***La qualité de service :*** De nombreuses applications ont besoin de certaines garanties relatives par exemple au débit, au délai ou encore à la gigue. Dans ces réseaux Ad hoc, ces garanties sont très difficiles à obtenir. Ceci est du à la nature du canal radio d'une part (interférences et taux d'erreur élevés) et au fait que des "liens" entre des mobiles peuvent avoir à se partager les ressources (alors qu'en filaire, deux liens sont par définition indépendants). De ce fait, les protocoles de qualité de service habituels (par exemple IntServ / RSVP ou Diff-Serv) ne sont pas utilisables directement dans le monde Ad hoc et des solutions spécifiques doivent être proposées [34], [35].

3. Les risques liés à la sécurité des réseaux Ad hoc :

3.1. L'Analyse de risque en sécurité :

L'analyse de risque est nécessaire pour bien appréhender la problématique de la sécurité dans les réseaux sans fil Ad hoc. Elle suit les étapes suivantes :

1. Détermination des fonctions et données sensibles des réseaux Ad hoc à protéger.
2. 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.
3. Étude des vulnérabilités.
4. Étude des menaces et quantification de leur probabilité d'occurrence ou de leur faisabilité.
5. Mesure du risque encouru en fonction des vulnérabilités mise en lumière et des menaces associées.

A partir de ces différents points d'entrée, il est possible de déterminer quelles sont les parties critiques, en terme de sécurité, que les concepteurs, les administrateurs, et les utilisateurs de réseaux sans fil Ad hoc doivent appréhender. La figure 4 retrace les différentes phases de ce processus :

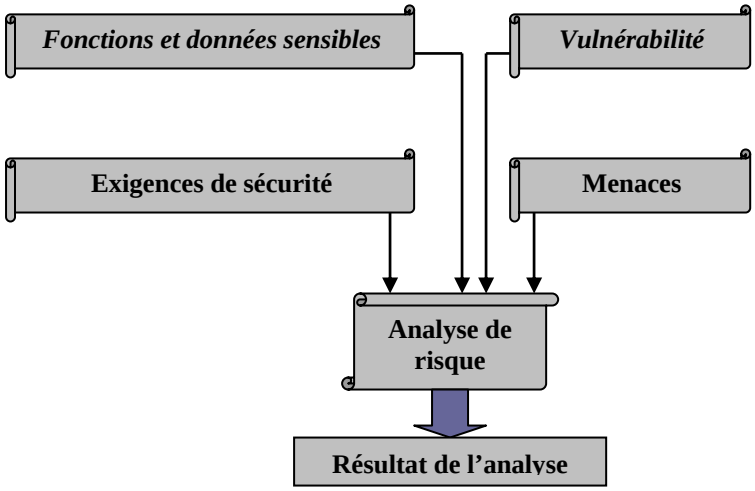


Figure 4 : Les étapes de l'analyse de risque

Il faut noter qu'une généralisation des besoins en sécurité faisant abstraction des contextes d'utilisation a été nécessaire pour mener à bien cette analyse de risque. En effet, une application commerciale civile, par exemple, n'aura pas les mêmes contraintes qu'une application militaire. Un contexte militaire mettra en avant le fort besoin d'authentification, de furtivité et d'intégrité physique des éléments alors qu'une utilisation commerciale critique nécessitera de se focaliser sur la confidentialité des services. Selon les cas, il peut donc être indispensable d'étudier des solutions appropriées au contexte d'utilisation à travers une analyse approfondie prenant en compte des contraintes spécifiques.

3.2. Fonctions et données sensibles :

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

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

3.3. Exigences de sécurité des réseaux sans fil Ad hoc :

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

3.3.1. 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 sécurisé. 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. L'intégrité des nœuds est, elle aussi, primordiale car les éléments d'un réseau Ad hoc sont moins sujets à surveillance. En effet, ils ne sont pas confinés dans un bureau mais transportés par leur propriétaire et peuvent donc être momentanément égarés. Un attaquant peut subtiliser

un appareil, le corrompre avec un cheval de Troie par exemple, avant de le restituer discrètement à son propriétaire.

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 Ad hoc étant donné les contraintes qui pèsent sur ces réseaux sont :

- Topologie dynamique.
- Ressources limitées sur certains nœuds de transit.
- Communication sans fil pouvant être facilement brouillées ou perturbées. Les applications sans fil en mode Ad hoc ne devraient donc pas se focaliser sur ce critère.

3.3.2. Anonymat / Protection de la vie privée :

Certaines applications peuvent nécessiter la discrétion sur l'identité des participants qui collaborent au réseau Ad hoc, par exemple un vote anonyme au cours d'une conférence. De plus, les différents gadgets électroniques qui formeront les nœuds des réseaux Ad hoc de demain, auront en toute probabilité, la possibilité de garder la trace de nos préférences afin de nous faciliter le quotidien et de nous offrir des services toujours plus appropriés. Cette tendance va pourtant à l'encontre de la protection de la vie privée de tout un chacun. Qui a envie de voir diffuser sur les ondes ses gouts et affinités ?

3.4. Vulnérabilités :

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

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

L'absence d'infrastructure fixe pénalise l'ensemble du réseau dans la mesure où il faut faire abstraction de toute entité centrale de gestion pour l'accès aux ressources.

Les mécanismes de routage sont d'autant plus critiques dans les réseaux Ad hoc que chaque entité participe à l'acheminement des paquets à travers le réseau. De plus, les messages de routage transitent sur les ondes radio.

3.5. Menaces :

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

3.6. Résultat de l'Analyse de Risque :

Après l'étude des besoins et exigences des réseaux sans fil Ad hoc en terme de sécurité, puis corrélation avec les risques issus des vulnérabilités et menaces s'appliquant à ces réseaux, nous avons pu dresser une liste des attaques fortement probables ou faisables et qui constituent un risque non négligeable en cas de réalisation.

Les dénis de services, *denial of services* (DoS), apparaissent comme les attaques les plus faciles à réaliser par un attaquant. La criticité de telles attaques dépend fortement du contexte d'utilisation mais n'est jamais complètement négligeable. Les modèles de dénis de services qui suivent se dégagent plus particulièrement dans le cas de réseau sans fil Ad hoc :

- Brouillage du canal radio pour empêcher toute communication.
- Tentative de débordement des tables de routages des nœuds servant de relais.
- Non-coopération d'un nœud au bon fonctionnement du réseau dans le but de préserver son énergie. "L'égoïsme d'un nœud est une notion propre aux réseaux Ad hoc". Un réseau Ad hoc s'appuie sur la collaboration sans condition de ses éléments. Un nœud refusant de jouer le jeu peut mettre en péril l'ensemble.
- Tentative de gaspillage de l'énergie de nœuds ayant une autonomie de batterie faible ou cherchant à rester autonome sans recharge le plus longtemps possible. Ces nœuds se caractérisent par leur propension à passer en mode veille le plus souvent possible. L'attaque consiste à faire en sorte que le nœud soit obligé de rester en état d'activité et ainsi de lui faire consommer toute son énergie. Cette attaque est référencée par Ross Anderson et Franck Stajano [36], [37] sous l'appellation *sleep deprivation torture attack*, un scénario de torture par privation du sommeil.
- Dispersion et suppression du trafic en jouant sur les mécanismes de routage.

Les attaques passives d'écoute et d'analyse du trafic constituent une menace certaine pour la confidentialité et l'anonymat.

L'usurpation de l'identité d'un nœud en leurrant les mécanismes de contrôle d'accès permet de nombreuses attaques actives rendant particulièrement critiques la protection des mécanismes de routage.

L'attaque physique d'un élément valide d'un réseau sans fil Ad hoc, entrainant la compromission du nœud, se révèle comme étant un point faible de ces réseaux.

Enfin, il apparait clairement que les attaques sur les mécanismes de routage sont particulièrement critiques.

4. Le routage dans les réseaux Ad hoc :

Les réseaux Ad hoc que nous considérons sont multi-sauts. Il peut donc arriver qu'un mobile veuille communiquer avec un autre qui n'est pas dans sa portée de communication directe. Les messages vont devoir être transmis de proche en proche jusqu'à la destination : c'est ce que l'on appelle le routage. La technique la plus basique est l'inondation, où chaque mobile réémet tous les paquets qu'il reçoit pour la première fois. Evidemment, l'inondation consomme beaucoup de ressources (bande passante et énergie) et n'est pas optimale. De nombreux protocoles de routage ont donc été proposés pour rendre les communications multi-sauts plus efficaces (moins de réémissions, chemins plus courts, etc.) que l'inondation basique.

Dans cette section, nous allons donc présenter certains des protocoles de routage développés dans le cadre du groupe de travail MANET de l'IETF. Ces protocoles travaillent au niveau IP et sont donc indépendants des couches physique et MAC. Le routage IP permet en particulier une inter-connectivité aisée avec toutes sortes d'autres réseaux ou matériels. Il est d'ailleurs possible d'utiliser ces protocoles pour fédérer en un seul réseau MANET des utilisateurs utilisant des matériels différents (cartes radios de technologies diverses, réseaux filaires, etc.). Les protocoles présentés sont parmi les plus représentatifs des diverses techniques utilisées pour le routage Ad hoc.

4.1. Routage hiérarchique ou plat :

Les protocoles de routage pour les réseaux Ad hoc peuvent être classés suivant plusieurs critères. Le premier d'entre eux concerne le type de vision qu'ils ont du réseau et les rôles qu'ils accordent aux différents mobiles.

- Les protocoles de routage "à plat" considèrent que tous les nœuds sont égaux (figure 5). La décision d'un nœud de router des paquets pour un autre dépendra de sa position et pourra être remise en cause au cours du temps.

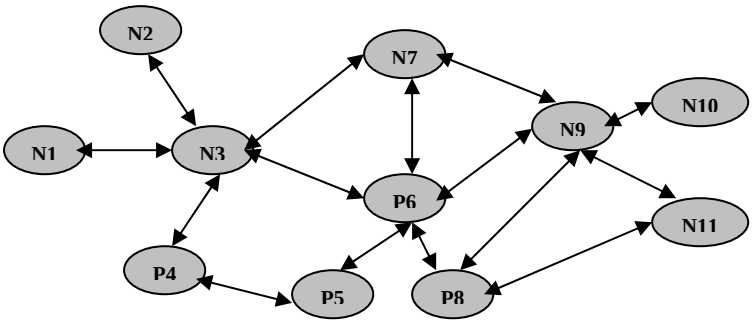


Figure 5 : Routage à plat

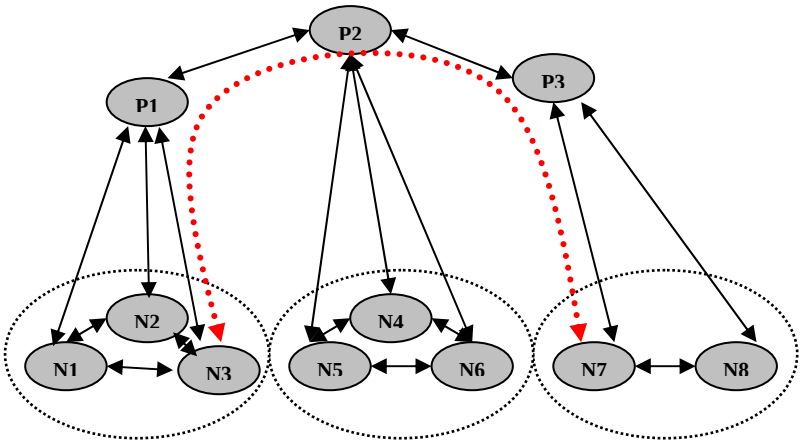


Figure 6 : Routage hiérarchique

- Les protocoles de routage hiérarchique fonctionnent en confiant aux mobiles des rôles qui varient de l'un à l'autre. Certains nœuds sont élus et assument des fonctions particulières qui conduisent à une vision en plusieurs niveaux de la topologie du réseau. Par exemple, un mobile pourra servir de passerelle pour un certain nombre de nœuds qui se seront attachés à lui. Le routage en sera simplifié, puisqu'il se fera de passerelle à passerelle, jusqu'à celle directement attachée au destinataire. Un exemple est donné sur la figure 6, où le nœud N3

passe par les passerelles P1, P2 et P3 pour atteindre N7. Dans ce type de protocole, les passerelles supportent la majeure partie de la charge du routage (les mobiles qui s'y rattachent savent que si le destinataire n'est pas dans leur voisinage direct, il suffit d'envoyer à la passerelle qui se débrouillera). Dans les réseaux où certains nœuds s'avèrent très sédentaires et disposent de suffisamment d'énergie (par exemple réseau d'ordinateurs portables mais où certains sont reliés au secteur, stations de base disposées là pour garantir la connectivité, etc.), ce type de routage présente certains avantages.

4.2. Etat de liens ou vecteur de distance :

Une autre classification, héritée du monde filaire, est possible pour les protocoles de routage :

- **Les protocoles à état de lien :** Ils cherchent à maintenir dans chaque nœud une carte plus ou moins complète du réseau où figurent les nœuds et les liens les reliant. A partir de cette carte il est possible de construire les tables de routage. Un des avantages de ce type de protocole est leur capacité à pouvoir facilement trouver des routes alternatives lorsqu'un lien est rompu. Il est même possible d'utiliser simultanément plusieurs routes vers une même destination, augmentant ainsi la répartition de la charge et la tolérance aux pannes dans le réseau. En contre partie, si le réseau est étendu, la quantité d'informations à stocker et diffuser peut devenir considérable.

- **Les protocoles à vecteur de distance :** Plutôt que de maintenir une carte complète du réseau (ce qui peut s'avérer extrêmement lourd), ces protocoles ne conservent que la liste des nœuds du réseau et l'identité du voisin par lequel passer pour atteindre la destination par le chemin le plus court.

4.3. Les différentes familles de protocoles de routage MANET :

Dans les travaux menés à l'IETF, plusieurs familles de protocoles se sont rapidement dégagées. Chaque protocole peut ainsi être classifié en tant que réactif, proactif, ou hybride.

4.3.1 Les protocoles réactifs :

Le principe des protocoles réactifs est de ne rien faire tant qu'une application ne demande pas explicitement d'envoyer un paquet vers un nœud distant. Cela permet d'économiser de la bande passante et de l'énergie. Lorsqu'un paquet doit être envoyé, le protocole de routage va rechercher un chemin jusqu'à la destination. Une fois ce chemin trouvé, il est inscrit dans la table de routage et peut être utilisé. En général, cette recherche se fait par inondation (un

paquet de recherche de route est transmis de proche en proche dans tout ou partie du réseau). L'avantage majeur de cette méthode est qu'elle ne génère du trafic de contrôle que lorsqu'il est nécessaire. Les principales contre parties sont que l'inondation est un mécanisme coûteux qui va faire intervenir tous les nœuds du réseau en très peu de temps et qu'il va y avoir un délai à l'établissement des routes.

4.3.2. Les protocoles proactifs :

Le principe de base des protocoles proactifs est de maintenir à jour les tables de routage, de sorte que lorsqu'une application désire envoyer un paquet à un autre mobile, une route soit immédiatement connue. Dans le contexte des réseaux Ad hoc les nœuds peuvent apparaître ou disparaître de manière aléatoire et la topologie même du réseau peut changer, cela signifie qu'il va falloir un échange continuel d'informations pour que chaque nœud ait une image à jour du réseau. Les tables sont donc maintenues grâce à des paquets de contrôle, et il est possible d'y trouver directement et à tout moment un chemin vers les destinations connues en fonctions de divers critères. On peut par exemple privilégier les routes comportant peu de sauts, celles qui offrent la meilleure bande passante, ou encore celles où le délai est le plus faible. L'avantage premier de ce type de protocole est d'avoir les routes immédiatement disponibles quand les applications en ont besoin, mais cela se fait au coût d'échanges réguliers de messages (consommation de bande passante) qui ne sont certainement pas tous nécessaires (seules certaines routes seront utilisées par les applications en général).

4.3.3. Les protocoles hybrides :

Les protocoles hybrides combinent les approches réactive et proactive. Le principe est de connaître notre voisinage de manière proactive jusqu'à une certaine distance (par exemple trois ou quatre sauts), et si jamais une application cherche à envoyer quelque chose à un nœud qui n'est pas dans cette zone, d'effectuer une recherche réactive à l'extérieur. Avec ce système, on dispose immédiatement des routes dans notre voisinage proche, et lorsque la recherche doit être étendue plus loin, elle en est optimisée (un nœud qui reçoit un paquet de recherche de route réactive va tout de suite savoir si la destination est dans son propre voisinage. Si c'est le cas, il va pouvoir répondre, et sinon il va propager de manière optimisée la demande hors de sa zone proactive). Selon le type de trafic et les routes demandées, ce type de protocole hybride peut cependant combiner les désavantages des deux méthodes échange de paquets de contrôle réguliers et inondation de l'ensemble de réseau pour chercher une route vers un nœud éloigné.

4.4. Description de quelques protocoles de routage représentatifs :

Les protocoles décrits par la suite sont issus du groupe de travail MANET de l'IETF. Ces protocoles sont représentatifs de diverses techniques et sont les plus avancés sur la voie d'une normalisation.

4.4.1. **AODV** *(Ad hoc On Demand Distance Vector) :*

AODV [67] est un algorithme de routage à la demande, c'est-à-dire qu'il ne construise de routes entre nœuds que lorsqu'elles sont demandées par les nœuds sources, et ce pour réduire le nombre de diffusions de messages. AODV utilise les principes des numéros de séquence afin de maintenir la consistance des informations de routage. Les numéros de séquence permettent d'utiliser les routes les plus récentes. Il utilise une requête de route dans le but de créer un chemin vers une destination. La route peut ne pas exister si la destination n'est pas connue au préalable, ou si le chemin existant vers la destination a expiré ou il est devenu défaillant. Cependant, AODV maintient les chemins d'une façon distribuée en gardant une table de routage, au niveau de chaque nœud de transit appartenant au chemin cherché. Afin de maintenir des routes cohérentes, une transmission périodique du message "*HELLO*" est effectuée. Si au bout d'un certain temps aucun message "*HELLO*" n'est reçu à partir d'un nœud voisin, le lien en question est considéré défaillant. Le protocole AODV ne présente pas de boucle de routage, et offre une convergence rapide quand la topologie du réseau Ad hoc change. Le protocole AODV est un protocole réactif, uniforme, de type distance vector.

4.4.2. **DSR** *(Dynamic Source Routing Protocol) :*

Le protocole DSR [57] est basé sur le principe de diffusion à la demande pour calculer une route vers une destination. Il utilise un routage par la source, et se base principalement sur deux mécanismes coopératifs : la découverte de route et la maintenance de route. Il permet aussi l'existence de plusieurs routes vers la destination. A partir des informations de routage qui sont incluses dans les paquets de données, les nœuds appartenant à la route, ainsi que leurs nœuds voisins, peuvent les collecter et les mettre dans leurs caches pour une utilisation ultérieure. Chaque nœud dans le réseau envoyant ou relayant un paquet est responsable de confirmer son acheminement vers le prochain nœud en recevant un acquittement. Si un nœud détecte une cassure de route, un message d'erreur de route est retourné à la source. Lors de la réception d'un message d'erreur de route, la source supprime la route défaillante de son cache. Si un chemin alternatif est disponible, il peut être employé pour des données restantes à la destination, autrement, une nouvelle découverte de route est lancée. Comme AODV, DSR

bufférise les paquets IP dans le nœud de source quand la découverte de route est effectuée. Ce protocole est un protocole réactif, uniforme, de type link state.

4.4.3. OLSR *(Optimized Link State Protocol) :*

OLSR [49] est un protocole de routage proactif. Il est considéré comme une optimisation du protocole à état des liens filaire pour les réseaux mobiles Ad hoc. Son innovation réside dans sa façon d'économiser les ressources radio lors des diffusions. Ceci est réalisé grâce à l'utilisation du concept des relais multi-points dans lequel chaque nœud choisit un sous-ensemble de ses voisins qu'il appellera "MPR" (multi-point relais) pour retransmettre ses paquets en cas de diffusion. En se basant sur la diffusion sur les MPRs, tous les nœuds du réseau sont atteints avec un nombre réduit de répétitions.

Comme dans le paradigme proactif, des messages de contrôle périodiques doivent être utilisés pour le maintien des tables de routage et de voisinage. Dans OLSR, principalement deux types de messages sont introduits : "*Hello*" et "*TC*" (Topology Control). Périodiquement, chaque nœud diffuse localement un message Hello contenant des informations sur son voisinage et l'état des liens. Ceci permet à chaque nœud de prendre connaissance de son voisinage à un et deux sauts. L'ensemble MPR est alors construit dans chaque nœud de façon à contenir un sous-ensemble de voisins à un saut qui couvre tous les voisins à deux sauts. Afin de construire les tables nécessaires au routage des paquets, chaque nœud génère périodiquement un paquet TC contenant la liste de ses voisins l'ayant choisi comme MPR. Le message TC est diffusé dans l'ensemble du réseau. Seuls les voisins MPR rediffusent un paquet TC reçu pour éviter l'inondation. Cette technique prometteuse réduit considérablement l'overhead généré par le trafic de contrôle. A la réception d'un message TC, la table de topologie peut être construite. Basé sur la table de topologie, chaque nœud peut calculer la table de routage qui permet d'acheminer les paquets vers n'importe quelle destination dans le réseau. OLSR est un protocole non uniforme, proactif de type link state.

4.4.4. TBRPF (*Topology Dissemination Based on Reverse-Path Forwarding) :*

TBRPF [55] est un protocole de routage proactif à état de lien. Chaque nœud exécutant TBRPF calcule un arbre de source fournissant des routes à tous les nœuds accessibles. Il se base sur l'information partielle de topologie stockée dans sa table de topologie, en utilisant une modification de l'algorithme de Dijkstra. Pour réduire l'overhead, chaque nœud rapporte seulement une partie de son arbre de source aux voisins. TBRPF emploie une combinaison de mises à jour périodiques et différentielles pour tenir tous les voisins au courant de la partie

rapportée de son arbre de source. Chaque nœud a également l'option pour rapporter l'information additionnelle de topologie (jusqu'à la topologie complète), pour fournir la robustesse améliorée dans les réseaux fortement mobiles. TBRPF effectue la découverte de voisins en utilisant des messages HELLO différentiels, qui rapportent seulement des changements sur l'état des voisins. Par conséquent, les messages HELLO sont beaucoup plus petits que ceux utilisés dans d'autres protocoles de routage à état de lien tels que OSPF (Open Shortest Path First).

4.4.5. ZRP (Zone-Based Hierarchical Link State Routing Protocol) :

ZRP [38] est un exemple de protocole hybride qui combine des approches proactives et réactives, essayant de ce fait de rassembler les avantages des deux approches. ZRP définit autour de chaque nœud une zone qui contient les nœuds voisins à un nombre donné de sauts du nœud. Des algorithmes proactifs et réactifs sont employés par le nœud pour acheminer les paquets, respectivement, dans et en dehors de la zone.

4.4.6. Autres protocoles :

De nombreux autres protocoles de routage ont été proposés pour les réseaux Ad hoc. [62] en décrit un certain nombre en sus de ceux déjà mentionnés. Dans la catégorie des protocoles construisant une topologie hiérarchique on peut citer *Cluster-head Gateway Switch Routing* (CGSR) présenté dans [53]. Certains autres protocoles nécessitent l'emploi de matériels externes. Par exemple Temporaly-Ordered Routing Algorithm (TORA) [40] a besoin que les mobiles soient synchronisés. D'autres ([46], [50]) utilisent le système GPS pour estimer la direction géographique de la destination et ne faire intervenir qu'une sous-partie du réseau dans la phase de construction des routes. Alors que beaucoup de protocoles cherchent à minimiser le nombre de sauts (minimum shortest path), certains protocoles enfin s'attachent à prendre d'autres critères en considération. ABR (*Associativity-Based Routing*) [65] par exemple privilégie les liens les plus stables (mobiles qui restent longtemps dans le voisinage les uns des autres). SSR (Signal Stability Routing) [43] travaille à partir des informations de niveau de signal et [47] cherche à maximiser la durée de vie du réseau en agissant sur la puissance d'émission de chaque mobile séparément.

4.5. Le routage de paquets :

Afin de comprendre les attaques sur les protocoles de routage, il est nécessaire de comprendre leur fonctionnement global. Lorsqu'un nœud dans un réseau veut émettre un message vers un autre nœud, il regarde dans sa table de routage si une route existe pour ce

nœud. Si elle n'existe pas, il initie une découverte de route, ***route discovery***, en diffusant sur le réseau, dans les airs pour les accès sans fil, un message de type ***route request***. Le message de route request contient l'adresse du nœud émetteur, l'adresse du nœud destinataire, un marqueur permettant d'identifier la découverte de route et une liste initialement vide à remplir par les nœuds intermédiaires. Lorsqu'un nœud intermédiaire reçoit ce paquet, s'il n'en est pas le destinataire et si sa table de routage n'indique pas de chemin pour le nœud recherché, il diffuse à son tour le paquet de type route request en rajoutant son adresse à la liste de nœuds intermédiaires. Dans le cas où le nœud intermédiaire possède dans sa table de routage un chemin pour le nœud destinataire, la majorité des protocoles prévoit que le nœud intermédiaire renvoie directement un message de type **route reply** à l'émetteur en indiquant ce chemin. Lorsqu'un paquet de requête atteint son destinataire, ce dernier émet un paquet de réponse du type route reply. Ce paquet transite par les nœuds intermédiaires de la liste. La figure 7 schématise l'évolution des messages lors de la découverte de route.

Lorsque la réponse atteint l'initiateur de la découverte de route, ce dernier met à jour sa table de routage avec cette nouvelle route, qui consiste en la liste des nœuds intermédiaires avec un cout associé. Le cout sert aux nœuds à effectuer un choix entre deux routes menant à la même destination. Il peut être basé sur le nombre de nœuds intermédiaires traversés ou sur des critères plus complexes comme le débit, la fiabilité des liaisons ou la taille des paquets. Si l'initiateur reçoit ultérieurement une indication comme quoi cette destination peut être jointe avec un cout plus faible par un autre chemin, la table de routage sera mise à jour avec la route ayant le cout le plus faible. Une fois une route établie, un protocole de routage doit aussi mettre en œuvre un mécanisme de maintenance des routes pour gérer les évènements comme la coupure d'un lien entre deux nœuds par lesquels transitent des messages.

Lorsqu'un nœud reçoit un paquet de données pour une destination vers laquelle il ne peut plus émettre, il renvoie un message d'erreur de type **route error** vers la source du paquet de données. La route doit alors être supprimée de la table de routage. Des optimisations existent permettant à un nœud d'écouter les routes changées par les autres nœuds et de mettre à jour sa table de routage en conséquence.

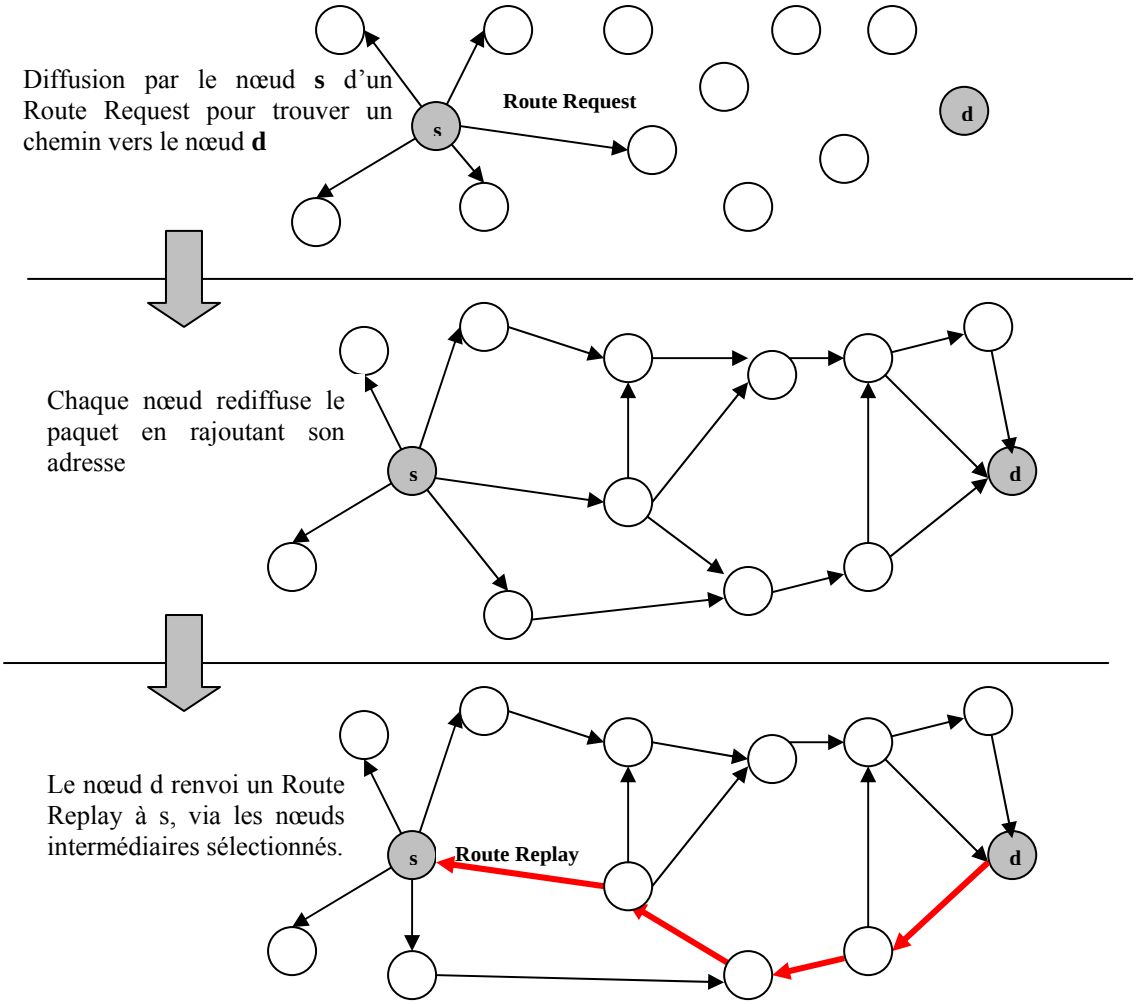


Figure 7 : Découverte de route initiée par le protocole de routage

4.6. Les Attaques Liées aux Protocoles de Routage :

Si aucun contrôle n'est fait sur la provenance et l'intégrité des messages de routage du réseau Ad hoc, un nœud malicieux pourra facilement causer des perturbations au réseau. Cela lui sera d'autant plus facile que les réseaux sans fil Ad hoc n'ont pas de barrière physique pour se protéger et que tous les éléments peuvent potentiellement participer au mécanisme de routage.

Si un nœud malicieux a la capacité d'usurper l'identité d'un nœud valide du réseau, il peut lors du mécanisme de découverte de route répondre au nœud initiateur avec un message de type route replay en annonçant un chemin avec un cout minimal, vers le nœud demandé. Le nœud émetteur mettra alors sa table de routage à jour avec cette fausse route. Les paquets de données du nœud émetteur vers le nœud destinataire transiteront par le nœud malicieux qui

pourra tout simplement les ignorer. Cette attaque est appelée ***trou noir***, ***(black hole)*** Les paquets sont captés et absorbés par le nœud malicieux. La figure 8 illustre cette attaque.

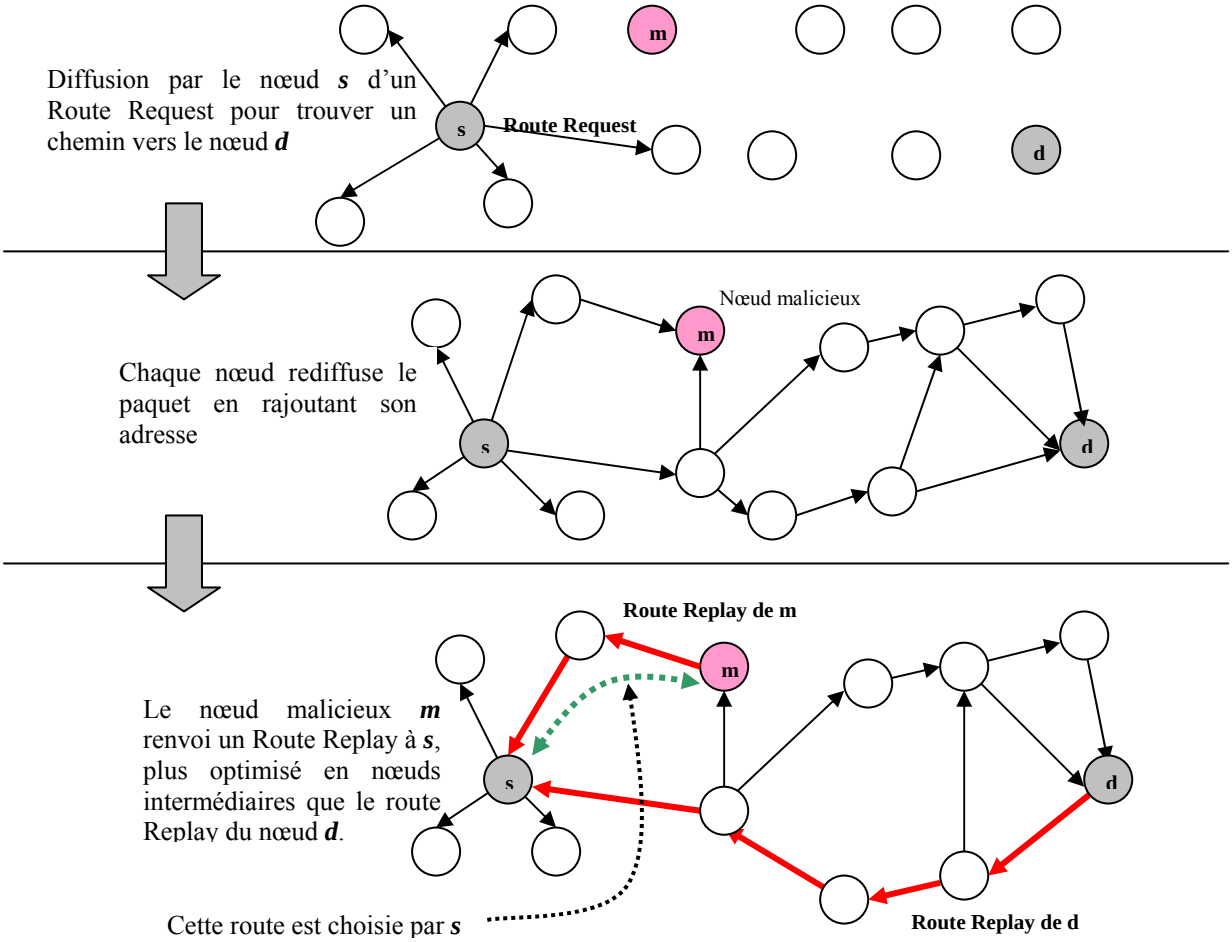


Figure 8 : Attaque black hole

Une variante est appelée ***grey hole***, seuls certains types de paquets sont ignorés par le nœud malicieux. Par exemple, les paquets de données ne sont pas retransmis alors que les paquets de routage le sont. Un attaquant peut aussi créer des boucles infinies dans le réseau ou imposer aux paquets de faire des détours consommant la ressource radio inutilement. Un nœud malicieux ayant usurpé l'identité d'un nœud valide peut aussi générer des messages d'erreurs de type route error, de manière aléatoire, pour perturber le fonctionnement du mécanisme de maintenance des routes.

5. Conclusion :

Les réseaux Ad hoc font partie d'un domaine de recherche qui n'a pris son essor que très récemment. Le facteur qui a déclenché cet intérêt fut l'arrivée de technologies relativement bon marché qui ont favorisé la **conception et le déploiement** de tels réseaux notamment dans

la matière de sécurité. Avant cela, ce domaine était réservé aux militaires qui disposent de moyens tout autres.

Sécurité dans les Réseaux Ad hoc

1. Introduction :

Pendant de nombreuses années, la problématique de la sécurité a été totalement ignorée dans le domaine des réseaux Ad hoc, la plupart des recherches s'appliquent à améliorer les performances (rendement des protocoles, limitation de l'overhead, etc.). Par la suite, plusieurs mécanismes ont été envisagés pour accroitre la robustesse des protocoles de routage sans pour autant trop affecter les performances. Certains d'entre eux consistent simplement en des optimisations basiques des protocoles, en vue de prolonger leur utilisation en milieu hostile. D'autres, en tel revanche s'inspirent de techniques plus avancées mais également plus coûteuses telles que la cryptographie pour garantir des fonctionnalités essentielles comme la confidentialité et l'authentification.

2. Notions de base de la sécurité :

2.1. Cryptographies symétrique et asymétrique :

Deux familles de cryptographie coexistent depuis les années 1970 [39]. Elles se distinguent en fonction du type de clés utilisées. La cryptographie symétrique nécessite que les systèmes de chiffrement et de déchiffrement disposent de la même clé cryptographique tandis que la cryptographie asymétrique ou à clés publiques considère deux clés complémentaires " les clés publique et privée " réalisant indifféremment l'une le chiffrement et l'autre le déchiffrement. Ces deux familles sont ci-après décrites avec quelques exemples d'algorithmes couramment utilisés de nos jours, leurs avantages et inconvénients ainsi que leurs complémentarités.

Notons que les algorithmes cryptographiques antérieurs à ces deux familles reposaient sur le secret de l'algorithme lui-même. Ainsi dès l'algorithme craqué, les cryptographes devaient inventer de nouveaux algorithmes. L'originalité des algorithmes symétriques et asymétriques a donc été de rendre publique le processus de chiffrement et d'externaliser le secret dans un paramètre secret appelé ici «clé cryptographique ».

2.1.1. Cryptographie symétrique :

La Cryptographie symétrique se base sur l'usage d'une même clé pour chiffrer et déchiffrer des données. Ces clés sont appelées des clés symétriques (par fois secrètes). Dans le cadre d'échanges sur un réseau, une entité émettrice chiffre les données avec une clé et l'entité destinatrice déchiffre les données avec la même clé. Si les algorithmes symétriques sont performants et permettent d'atteindre des débits importants dans le chiffrement et

déchiffrement, ils posent cependant le problème de la mise en place d'une même clé entre émetteur et récepteur. Partager une clé avec chaque entité communicante potentielle, même dans un groupe fermé d'entités est extrêmement contraignant et conduit rapidement à un très grand nombre de clés à gérer. Il est donc préférable d'automatiser la mise en place de ces clés.

Les algorithmes symétriques les plus connus sont dans l'ordre chronologique de définition, le DES (*Data Encryption Standard*), le 3DES (prononcé « Triple DES »), et l'AES *(Advanced Encryption Standard).*

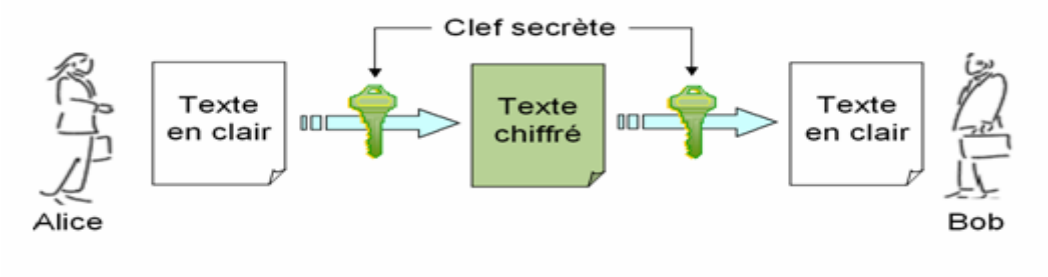


Figure 9 : Chiffrement symétrique "Clef secrète"

2.1.2. Cryptographie asymétrique ou à clés publiques :

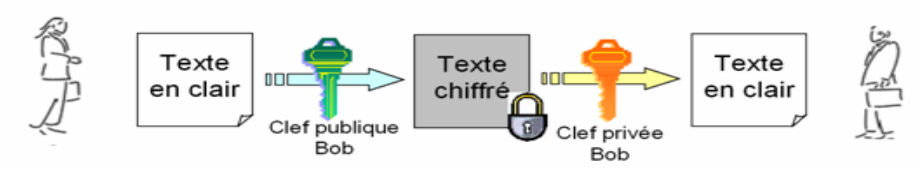
La cryptographie asymétrique ou à clé publique considère deux clés de chiffrement, dites “clés asymétriques”. Ces deux clés sont générées simultanément et sont complémentaires car le chiffrement avec l'une de ces clés nécessite le déchiffrement avec l'autre clé. Chaque clé a un rôle bien défini. La clé privée est une clé qui ne doit être connue que d'une seule entité, c'est elle qui permettra à cette entité de s'authentifier par exemple. La clé publique peut être largement diffusée et il est même préférable qu'elle soit largement diffusée si on souhaite que l'entité concernée puisse être authentifiée par un grand nombre d'entités. Bien entendu, la connaissance de la clé publique ne doit pas permettre de déduire la clé privée complémentaire.

Pour authentifier l'origine d'un message dans une communication sur un réseau, l'émetteur doit utiliser sa propre clé privée, par exemple pour générer une signature électronique (voir paragraphe 2.3) qu'il apposera au message avant émission. La clé publique étant connue de tous, le destinataire sera à même de vérifier la validité de la signature et aura une garantie sur la provenance du message.

Pour garantir la confidentialité d'un message, il est nécessaire de chiffrer le message émis avec la clé publique du destinataire. Cette clé publique est connue de tout le monde et peut donc servir à n'importe quelle entité pour chiffrer un message. Par contre, la clé privée

complémentaire n'est connue que du destinataire du message; le destinataire sera donc le seul à pouvoir déchiffrer le message. La propriété de confidentialité est ainsi obtenue.

Chiffrement **:**



Signature **:**

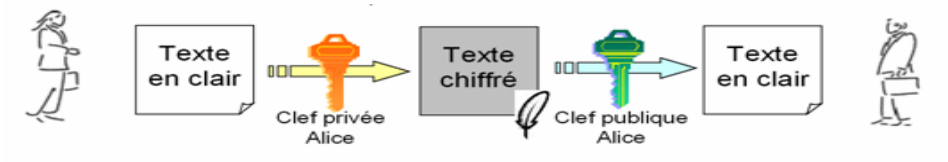


Figure 10 : Chiffrement asymétrique "Clef publique"

2.1.3. Complémentarité des deux systèmes cryptographiques :

Face aux avantages offerts par les deux familles cryptographiques précédemment décrites, les protocoles de sécurité font un usage ciblé de chacun de ces systèmes :

- ✓ La cryptographie symétrique (ou à clés secrètes) permet de protéger de façon intensive les données échangées sur le réseau, la rapidité de traitement des algorithmes symétriques est ici exploitée.
- ✓ La cryptographie asymétrique (ou à clés publiques) sert à initialiser une connexion sécurisée entre deux entités de réseau en permettant aux entités communicantes de s'authentifier mutuellement et de mettre en place une clé symétrique partagée de façon confidentielle.

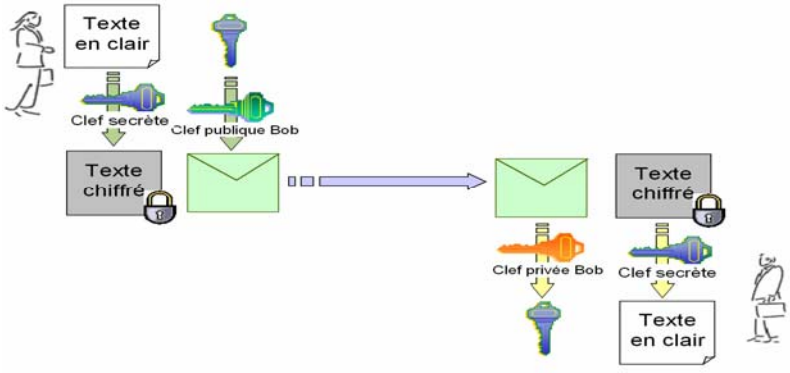


Figure 11 : Combinaison clefs publiques / clefs secrètes

2.2. Fonctions de hachage :

Les fonctions de hachage ont pour objectif de fournir un résultat représentatif du contenu d'un message, et ce, sur un nombre d'octets restreints. Elles s'apparentent en quelque sorte à un CRC *(cyclic redundancy check),* mais en plus sophistiqué.

Les propriétés attendues de ces fonctions de hachage sont les suivantes :

- Un résultat sur un nombre limité d'octets (en général 16 ou 20 octets).
- L'impossibilité de retrouver le message original à pm1ir du résultat de la fonction.
- Deux messages différant de 1 bit seulement produisent deux résultats qui diffèrent d'au moins la moitié des bits.

Plusieurs termes désignent ces mêmes fonctions de hachage, à savoir : fonctions irréversibles, ou fonctions à sens unique. De même, plusieurs termes désignent le résultat de cette fonction appliquée à un message : hash, haché, empreinte, condensat ou encore condensé. Par la suite, on emploiera le terme : « empreinte ».

2.3. Signatures électroniques et MAC :

L'objectif d'une signature électronique ou d'un MAC *(Message Authentication Code)* apposé à un message a pour double objectif de permettre au destinataire d'authentifier l'origine de ce message et de lui prouver son intégrité. Leur implémentation fait appel aux fonctions de hachage et aux clés symétriques ou asymétriques. Dans le cas de l'usage de la cryptographie symétrique, on emploie exclusivement le terme de MAC, tandis que dans l'usage de la cryptographie asymétrique, on peut parler de MAC, mais on préférera le terme de signature électronique.

Dans ce paragraphe, on décrit les deux manières de générer un MAC, puis de vérifier la validité d'un MAC en fonction du type de cryptographie utilisée. Dans le cas de la cryptographie symétrique, comme le montre la figure 12, la génération du MAC suppose les opérations 1 à 4 de la part de l'émetteur (A), tandis que la vérification par le récepteur (B) de sa validité nécessite les étapes 5 à 9.

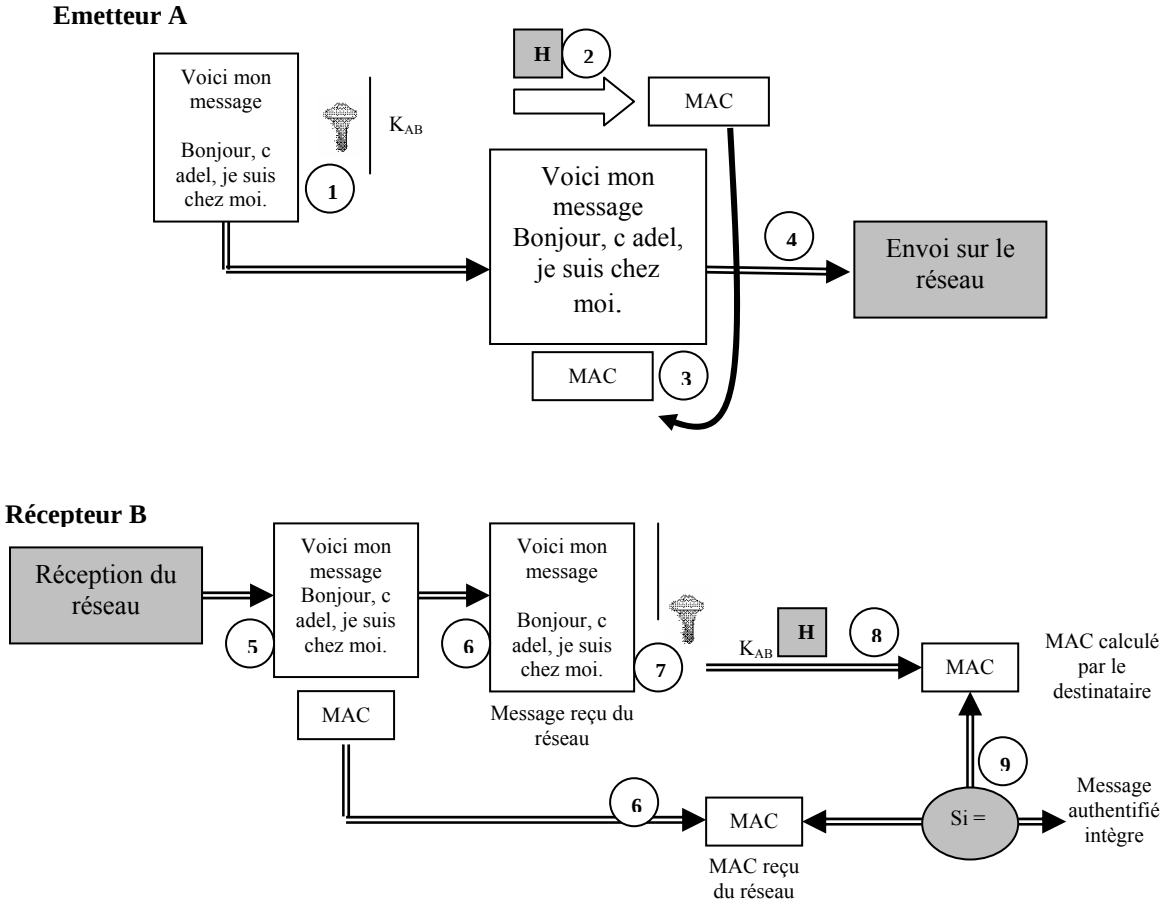


Figure 12 : <u>Génération et vérification d'un MAC (cryptographie symétrique)</u>

L'émetteur tout d'abord combine le message et la clé K_{AB}. Le résultat de cette première étape se trouve alors haché par la fonction de hachage H et le MAC est alors obtenu (étape 2) et apposé au message émis sur le réseau (étape 3) avant émission sur le réseau (étape 4). A la réception du message (étape 5), le récepteur sépare le message du MAC (étape 6). Sur le message reçu, un MAC est alors calculé localement en suivant les mêmes étapes que l'émetteur (étapes 7 et 8). Le MAC calculé en local est ensuite comparé au MAC reçu du réseau (donc logiquement celui calculé par l'émetteur s'il est intègre). En cas d'égalité (étape 9), le message reçu peut être considéré comme authentique et intègre. En effet, d'une part, le calcul du MAC faisant intervenir la clé partagée K_{AB}, nécessairement l'émetteur d'un tel MAC ne peut être que l'émetteur déclaré, sinon l'entité ne connaîtrait pas la bonne clé. D'autre part, en cas de modification du message ou du MAC lors du transfert sur le réseau, il est clair que le MAC calculé par le récepteur serait différent du MAC reçu et il n'y aurait pas d'égalité.

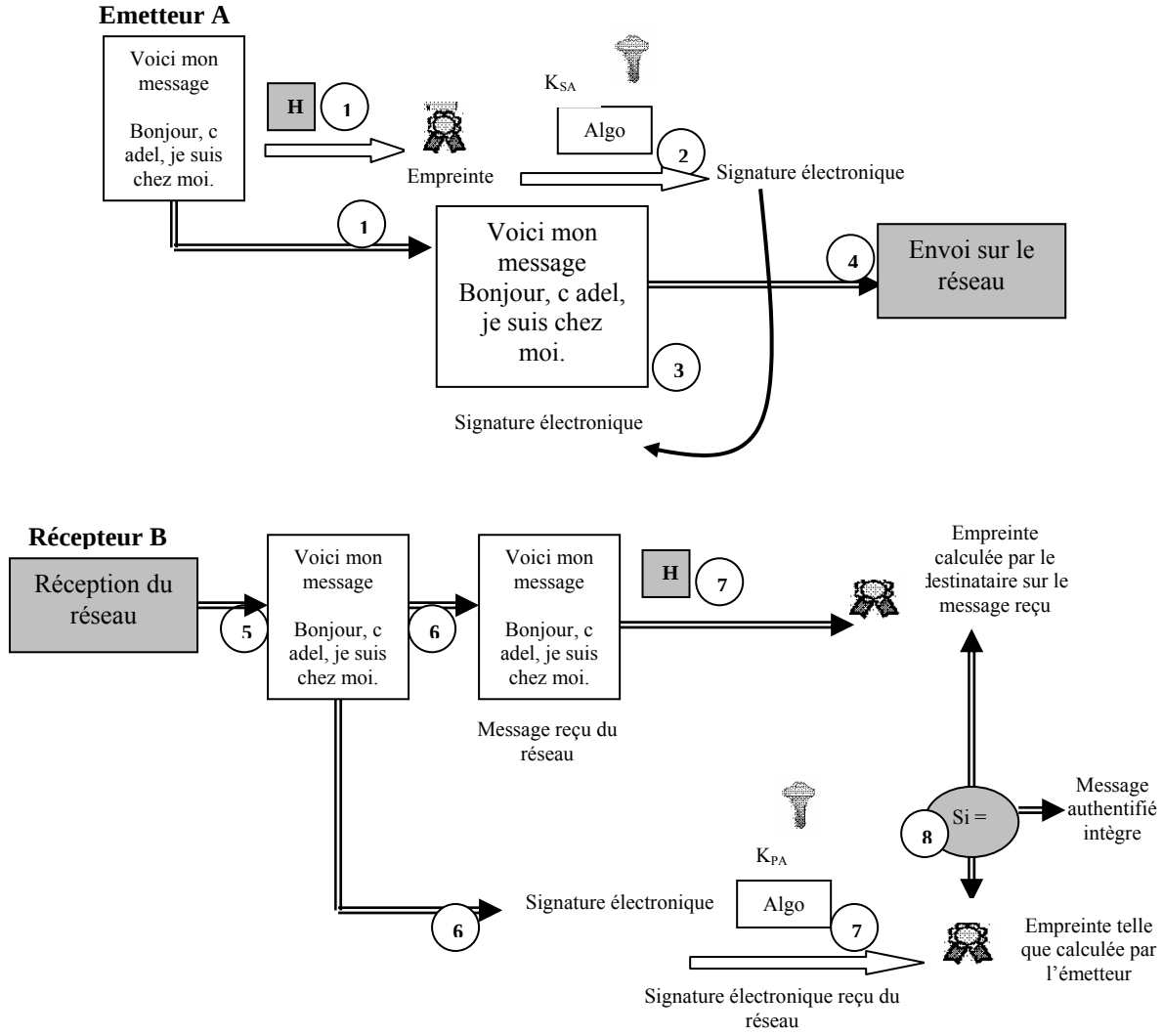


Figure 13 : <u>Génération et vérification d'une signature électronique (cryptographie asymétrique)</u>

Dans le cas de la cryptographie asymétrique, comme t'illustre la figure 13, l'émetteur A commence par générer une empreinte à l'aide de la fonction de hachage H (étape 1), puis chiffre cette empreinte avec un algorithme asymétrique à raide de sa clé privée (étape 2). Il obtient alors une signature électronique qu'il appose au message original (étape 3) avant d'émettre l'ensemble : message et signature sur le réseau (étape 4). A la réception (étape 5), le récepteur B sépare le message de la signature (étape 6). Dans l'étape 7, d'une part, il calcule l'empreinte du message reçu localement et d'autre part, il déchiffre la signature reçue à l'aide du même algorithme de déchiffrement et de la clé publique de A pour obtenir l'empreinte telle que l'avait calculée l'émetteur. En cas d'égalité (étape 8), le message est prouvé authentique et intègre. Pour preuve, l'entité génératrice de la signature reçue doit nécessairement posséder la bonne clé privée K_{SA}. Donc il ne peut s'agir que de A. De plus, en cas de modification du

message transmis sur le réseau, il est clair que l'empreinte calculée localement par le destinataire aurait abouti à un résultat très différent de celle calculée par l'émetteur (obtenue après déchiffrement de la signature par le récepteur).

2.4. Infrastructure de gestion de clés (PKI) et certificats électroniques :

Une infrastructure de gestion de clés (IGC) ou PKI *(public key infrastructure)* [63] prend en charge les aspects tant organisationnels que techniques afin d'assurer les fonctions suivantes : la génération de clés publiques/privées et leur distribution à leurs propriétaires à l'initialisation d'une nouvelle entité dans la PKI, ainsi que la publication, révocation et validation de clés publiques. Généralement, les PKIs se basent sur des certificats électroniques et des listes de certificats révoqués, mais parfois, la simple publication de clés publiques de façon sécurisée dans un annuaire peut suffire. Parfois aussi, le jeu de clés est généré par son propriétaire qui ne requiert alors de la PKI que la certification de sa clé publique.

Sur Internet, aujourd'hui, de nombreuses PKI existent, elles se présentent sous la forme d'autorités de certification organisées hiérarchiquement entre elles, avec l'autorité supérieure déléguant la gestion d'une partie des certificats à des autorités de certification inférieures. Plus exactement, les PKI distinguent les deux rôles d'autorités suivants :

- ✓ Autorité de certification (AC) : l'autorité de certification est la seule autorité à détenir la clé privée de l'autorité de certification et donc habilitée à émettre des certificats électroniques et des listes de certificats révoqués.
- ✓ Autorité d'enregistrement : une (ou plusieurs) autorité d'enregistrement est associée à une autorité de certification et réalise l'interface avec les utilisateurs. Elle se charge de filtrer les demandes de certificat en effectuant un contrôle plus ou moins strict sur l'identité du demandeur, elle se charge aussi de publier et valider les certificats électroniques générés par l'autorité de certification, enfin clic vérifie l'authenticité d'une demande de révocation de certificat et publie les listes de certificats révoqués.

Au sein d'une même PKI, plusieurs niveaux de certificats sont également possibles suivant l'usage que l'on souhaite faire du certificat, suivant le niveau de sécurité attendu, etc. Il est clair qu'un certificat émis pour un utilisateur pour protéger ses messages électroniques n'a pas besoin du même niveau de sécurité qu'un certificat émis pour une entreprise désireuse de signer électroniquement des contrats.

2.4.1. Certificats électroniques :

Les certificats électroniques ont pour objectif de lier de façon sûre une clé publique à une entité (utilisateur, serveur, etc.). Ces certificats correspondent concrètement à une structure de données dont le format le plus courant est fourni par le standard X.509v3 [63] et comprend entre autres : un numéro de série, une clé publique, l'identifiant du propriétaire de la clé publique, la date de validité (date de début et date de fin de validité), l'identifiant de l'autorité de certification (AC) émettrice du certificat, la signature du certificat à l'aide de la clé privée de l'autorité de certification. C'est la signature apposée par l'AC qui garantit l'authenticité du certificat. En effet, il suffit qu'une entité ait confiance dans l'AC et dispose de sa clé publique pour qu'elle puisse en confiance utiliser des clés publiques gérées par l'AC. S'il existe plusieurs niveaux d'AC, alors chaque AC doit posséder un certificat de clé publique signé par l'AC de niveau supérieur et incluant son rôle d'AC, ce certificat prouve alors que l'AC est habilitée par l'AC supérieure hiérarchique à gérer des certificats. Seule l'AC racine signe elle-même son propre certificat, ce type de certificat est appelé " certificat auto-signé ". Dans une hiérarchie d'AC, une chaîne de certification d'un certificat est formée par l'ensemble des AC depuis l'AC racine jusqu'à l'AC émettrice. Cette notion de chaîne de certification sert lors de la vérification d'une clé publique car la vérification consiste à vérifier tous les certificats composant la chaîne.

En pratique, avant d'employer une clé publique d'un dispositif distant pour sécuriser des échanges, il est nécessaire de procéder aux vérifications suivantes pour prouver la validité du certificat, à savoir :

- ✓ La date de validité du certificat : lors de la vérification, le certificat doit être dans sa fenêtre de validité. Cela suppose en particulier que le système vérificateur soit à l'heure et à la bonne date. Très souvent, dans la pratique, les problèmes de rejet de certificats sont dus à des horloges non mises à l'heure dans un système, ou à des certificats générés à la va-vite avec une durée· de validité nulle.
- ✓ La confiance dans l'AC émettrice : il est nécessaire que l'AC ayant signé le certificat soit reconnue comme de confiance. Plusieurs cas peuvent se produire :
  - L'AC émettrice est préenregistrée dans le dispositif de vérification, auquel cas cette opération de vérification est immédiate.
  - L'AC émettrice appartient à une hiérarchie d'AC : il est théoriquement nécessaire de vérifier toute la chaîne de certification. Cela suppose de récupérer un à un tous les certificats des AC de la chaîne, d'avoir confiance dans l'AC racine, puis de vérifier

un à un la validité de tous les certificats, depuis celui de l'AC racine jusqu'à celui de l'AC émettrice, en suivant exactement les mêmes étapes décrites ici. En général, les dispositifs de vérification ne procèdent pas à la vérification de la chaîne de certification, ils se contentent de la seule vérification de la présence du certificat de l'AC émettrice dans leur magasin de certificats.

- L'AC émettrice n'est pas de confiance car son certificat n'est pas connu du dispositif de vérification comme de confiance, ou bien l'AC racine de la hiérarchie d'AC à laquelle elle appartient n'est pas reconnue de confiance.

✓ L'état non révoqué du certificat : la preuve doit être acquise que le cel1ifieat n'a pas été révoqué préalablement.

La validité de la signature de l'AC : la signature électronique présente dans le certificat doit être valide.

3. La sécurité dans les réseaux Ad hoc :

Plusieurs approches et solutions ont été proposées pour sécuriser les réseaux Ad hoc. Chacune d'elles se base sur un raisonnement différent suivant le type d'application, l'extension du réseau, la moyenne du nombre de nœuds ainsi que les aspects de sécurité pris en priorité (authenticité, confidentialité, Intégrité, disponibilité, anonymat et protection de la vie privée, etc.).

3.1. Protections basiques :

Si les caractéristiques spécifiques des réseaux Ad hoc constituent souvent un obstacle à la sécurisation du routage, elles peuvent également être exploitées a contrario comme un atout, pour renforcer l'acheminement des données. C'est le cas par exemple de la redondance de routes. Chaque nœud dans un réseau Ad hoc est susceptible à tout moment de servir de routeurs. Dès lors, pour peu que le nombre de nœuds soit suffisant, il est souvent possible de trouver plusieurs chemins différents entre deux nœuds. Or, la plupart des protocoles classiques (AODV, OLSR, ZRP, etc.) ont justement la faculté d'établir plusieurs routes entre deux nœuds s'échangeant des informations. Une solution simple consiste alors à profiter de cette multiplicité de routes pour sécuriser le transfert [7]. D'une part, lorsqu'un nœud malveillant est identifié, le protocole peut presque toujours trouver une route qui permette de le contourner. D'autre part, il devient possible de transmettre de l'information redondante à travers des routes additionnelles afin de permettre au destinataire de vérifier l'intégrité de

l'information envoyée. On peut ainsi adjoindre des codes détecteurs d'erreur, correcteurs d'erreur, ou des hachages des données transmises.

Bien qu'offrant un bon niveau de sécurité, cette technique a pour inconvénient de réduire sensiblement la bande passante disponible en augmentant le trafic de contrôle d'autre part, elle ne répond pas â un certain nombre de problèmes évoqués en premier partie comme l'usurpation d'identité, l'injection de faux paquets de signalisation ou la redirection de route.

Une autre approche consiste à utiliser la nature du médium, à savoir l'onde radio que l'information est réellement transmise. En effet une autre des caractéristique des réseaux Ad hoc étant un médium totalement ouvert avec un accès partagé, tous les nœuds peuvent écouter les informations transmises par leurs voisins â un saut. Ainsi, une solution [7], mise au point par une équipe de l'université du Maryland consiste à modifier le protocole de base (DSR) de manière a ce chaque réponse à un Route_Request fasse l'objet d'une confirmation par un voisin de l'émetteur. Lorsqu'un nœud reçoit un paquet de type Route_Request auquel correspond une route valide dans son cache de route, il répond bien sûr par un paquet de type Route_ Reply, mais envoie également un paquet de demande de confirmation (CREP) auprès du premier voisin en aval. Celui-ci examine son cache de roule à la recherche d'une route vers la destination. S'il en trouve une, il répond à la source par un paquet (CREP) contenant cette information, dans le cas contraire, il ne répond rien. De son côté, le nœud source compare les informations envoyées par le premier nœud intermédiaire avec la confirmation reçue par le voisin. Si elles s'avèrent différentes ou plus simplement, si le voisin en aval n'a rien envoyé, le nœud source ne prend pas en compte la réponse du nœud intermédiaire et recherche une autre route.

On constate que ce procédé a pour objectif de sécuriser la découverte des routes en s'assurant que le chemin annoncé existe réellement. Cependant il est beaucoup trop simple et limitatif pour sa sécurité soit jugée suffisante. Tout d'abord, il ne prend en compte que la sécurisation des Route_Reply des nœuds intermédiaires, ce qui ne représente, somme toute, qu'une amélioration de la technique *de source caching* du protocole DSR. Ensuite, il nécessite obligatoirement l'emploi d'outils supplémentaires, capables de fournir l'authentification des paquets car sinon, rien n'empêcherait le nœud intermédiaire de falsifier une confirmation et de l'envoyer au nœud source en usurpant l'adresse de son voisin. D'autre part, supposons qu'un autre nœud intermédiaire décide de supprimer la confirmation des paquets Route_ Reply qu'il relaie, la route ne sera jamais établie et le soupçon pèsera immédiatement sur le nœud à l'origine du Route_Reply. La confirmation de route doit donc obligatoirement être

transmise à travers un autre chemin. Enfin, si deux nœuds malveillants s'associent pour mener une attaque, le procédé de protection peut très bien être contourné. Le premier nœud envoie un Route_Reply qui est confirmé par le second nœud â l'aide d'une *route confirmation reply* et une fausse route sera établie.

Ces mécanismes permettent d'offrir un niveau de sécurité supérieur aux protocoles classiques en permettant de renforcer le processus d'acheminement des paquets. En revanche, il ne s'avère pas suffisants dès lors qu'il s'agit de satisfaire les exigences de sécurité de bases que sont la confidentialité et l'authentification. C'est pourquoi les protocoles les plus efficaces utilisent des mécanismes plus conventionnels hérités des réseaux filaires tels que le contrôle d'accès, la cryptographie à clés publiques, les signatures digitales, etc. Ces mécanismes sont dits préventifs car ils visent à empêcher à l'avance, les attaques de nœuds compromis sur le réseau. Parallèlement, certaines approches visent à détecter en temps réel les attaque au sein du réseau ainsi qu'à favoriser la coopération entre les nœuds afin de restreindre l'impact des nœuds malicieux. Ces approches sont dites réactives et peuvent être utilisées en supplément des approches préventives.

3.2. Les architectures de gestion de clés :

3.2.1. Le resurrecting duckling :

Dans une volonté de permettre une distribution facilitée des clés dans un réseau Ad hoc, Franck Stajano et Ross Anderson ont proposé dans [37] un mécanisme pour échanger une clé secrète entre deux nœuds. Ce modèle, appelé "*The resurrecting duckling*", repose sur la relation de maître/esclave et sur le concept d'imprégnation. Ainsi, pendant une phase d'initialisation (avant son introduction au sein du réseau), un nœud esclave doit être 'imprégné' par son nœud maître (éventuellement, le propriétaire) par le biais d'un contact physique (par exemple électrique). Lors de ce contact, une clé secrète est échangée en toute confidentialité. Par la suite, cette clé peut être utilisée pour chiffrer et authentifier des informations, comme une liste d'autres clés partagées par exemple. Bien qu'innovante, cette approche laisse plusieurs questions en suspens. La première concerne la phase d'imprégnation. Si un contact physique est possible dans le cadre d'un petit réseau (un piconet [66] par exemple) avec un leader désigné, il devient moins envisageable dans le cadre d'un grand réseau ouvert. Le deuxième problème porte sur la gestion de clés. En effet, l'approche ne propose pas comment faire pour échanger une clé secrète entre chaque paire de nœuds du réseau. Par ailleurs, si l'un des nœuds est corrompu, toutes les autres clés liées à ce nœud

peuvent se trouver menacées et rien n'est mentionné quant à la répudiation d'une clé. Une réinitialisation systématique paraît difficile à mettre en place.

3.2.2. SUCV :

Dans [41], G. Montenegro et C. Castellucia ont mis au point une autre approche appelée SUCV (Statistically Unique Cryptographically Verifiable identifiers and addresses) dans laquelle chaque nœud construit une adresse basée sur sa clé publique. Chaque nœud génère une paire clé publique/clé privée et choisit ensuite son adresse calculée à partir de la clé publique, à l'aide d'une fonction de hachage cryptographique. Les auteurs proposent deux mécanismes. Dans le premier, l'adresse IPv6 d'un nœud correspond au résultat complet de la fonction de hachage sur la clé publique. Dans l'autre approche, seuls les 64 bits les moins significatifs correspondent au résultat de la fonction de hachage. Ainsi, si un attaquant désire compromettre une adresse SUCV donnée, il devra effectuer 2^{63} (approximativement 4,8 x 10^{18}) essais pour trouver une clé publique dont l'empreinte est identique à celle de cette adresse SUCV. Si cet attaquant a la possibilité de calculer un milliard d'empreintes par seconde, il lui faudra approximativement 142 années pour trouver cette collision. L'inconvénient de cette approche est qu'elle ne résout pas entièrement le problème de mise en place des clés. Ainsi, si dans un réseau normal, le problème consiste à obtenir une liste de couples (nœuds, clés publiques) de confiance, ici on doit malgré tout déterminer une liste de nœuds de confiance.

Une approche alternative consiste à définir une ou plusieurs autorités de certification. En effet, la seule présence d'une clé publique ne suffit pas, encore faut-il que les nœuds puissent vérifier la légitimité de la clé publique utilisée par chaque nœud, c'est là le rôle de l'autorité. Chaque nœud du réseau possède un certificat qui contient son adresse IP, sa clé publique et bien sûr, une signature de l'autorité de certification. Lorsqu'un nœud désire envoyer un message, il le signe et y joint son certificat. Par la suite, le nœud récepteur vérifie dans un premier temps le certificat puis utilise la clé publique contenue dans ce certificat pour vérifier la signature du message. Plusieurs problèmes se posent cependant. Le premier concerne la disponibilité de l'autorité, En effet, dans un réseau exempt de toute infrastructure fixe, la question de l'accès à l'autorité se pose pour vérifier le certificat. Certains liens se rompent, les nœuds sont amenés à bouger et ainsi, il n'est pas sûr que chaque nœud ait à tout instant un accès à l'autorité et donc au service de certification. Le deuxième problème concerne la dépendance mutuelle entre sécurité et routage. En effet, pour valider un certificat auprès d'une autorité de certification, il faut au préalable établir une route, mais pour que cette route puisse

être établie de manière sûre, il faut d'abord vérifier les clés publiques de chacun des nœuds qui la composent.

3.2.3. L'architecture de certification distribuée :

Pour remédier aux contraintes induites par l'absence d'infrastructure centralisée, Zhou et Haas ont imaginé profiter des caractéristiques intrinsèques des réseaux Ad hoc pour concevoir une nouvelle approche de gestion des certificats. Ils ont ainsi imaginé un système de certification de clés [61] dont L'autorité est non plus confiée à une seule entité fixe mais qui est au contraire distribuée entre plusieurs nœuds du réseau. Ainsi, le service de certification obtenu revient à définir une autorité de certification distribuée disposant d'une paire de clés publique/privée. La clé publique est connue de chaque nœud du réseau, ce qui leur permet de vérifier en confiance tout certificat signé avec cette clé privée. La clé privée n'est connue d'aucun nœud particulier, mais se trouve en fait partiellement distribuée sur des nœuds appelés contributeurs. Ainsi, un nœud client qui souhaite obtenir les clés publiques des autres clients ou lancer des mises à jour pour changer sa propre clé publique, émet une requête vers le service de certification. Pour garantir un niveau suffisant de sécurité même dans un contexte distribué, le service de certification repose sur **la cryptographie à seuil**. Un schéma de cryptographie à seuil *(n, t+1)* est conçu de telle manière que parmi les *n* nœuds qui se partagent la gestion des clés, *t+1* auront la possibilité de procéder aux opérations de chiffrement, tandis que *t* nœuds seuls en seront incapables, même en coalition, Ainsi, lorsque le service doit signer un certificat, chaque nœud serveur génère une signature partielle en utilisant sa clé privée, et transmet le résultat à un autre serveur appelé assembleur qui sera chargé d'assembler les portions de signature des *t* nœuds. Lorsque ce serveur a reçu *t+1* signatures partielles correctes, il est capable de calculer la signature finale du certificat. On notera que ce rôle d'assembleur peut être rempli par n'importe lequel des *n* nœuds. Pour renforcer la robustesse du dispositif et déjouer la compromission éventuelle de ce serveur, les auteurs préconisent d'affecter éventuellement ce rôle à *t+1* nœuds simultanément (bien sûr, la phase de vérification des signatures en est alors considérablement alourdie). L'avantage de ce modèle [61] réside dans le fait que *t* nœuds malveillants complices ne peuvent créer de certificat valide puisque *t+1* signatures partielles valides sont nécessaires, Bien entendu, nous ne sommes pas à l'abri d'un attaquant qui génère systématiquement de fausses signatures, en vue de conduire à la création d'un certificat invalide. Toutefois, Le nœud assembleur a toujours la possibilité de vérifier la validité d'une signature en utilisant la clé publique du service. Dans le cas où la vérification échoue, l'assembleur se doit de désigner un autre

ensemble de *t+1* signatures partielles. Cette procédure continue jusqu'à cc qu'il parvienne à générer une signature correcte.

Le point négatif de l'architecture proposée par Zhou et Haas est sa complexité de mise en œuvre. En effet, la sécurité repose pour une grande partie sur le choix des nœuds assembleurs, si le nombre de nœuds malicieux ou corrompus dépasse un certain seuil, le service devient inopérable. En outre, il est probable que le fait de requérir des certificats de plusieurs nœuds pour chaque message chiffré engendre un overhead conséquent au niveau de la charge réseau, dans la mesure où l'on doit envoyer et recevoir de l'information de tous les nœuds assembleurs.

3.2.4. L'approche de type PGP :

Une autre solution [64] propose de s'affranchir du modèle de certification en ligne classique en s'inspirant du concept de graphes de certificats (les sommets du graphe représentent les clés publiques des utilisateurs tandis que les arêtes représentent les certificats) du protocole PGP (*pretty good privacy*). Dans ce modèle, chaque nœud signe des certificats pour les participants en qui il a confiance, en fonction de ses propres critères. Les certificats reposent sur une confiance transitive, c'est-à-dire que si *A* fait confiance à *B* et que *B* fait confiance à *C*, alors *A* fait confiance à *C*. Mais à la différence de PGP, les certificats sont stockés puis distribués par les nœuds eux-mêmes et non pas par un serveur en ligne. Ainsi, chaque nœud possède un "dépôt de certificats local". Par la suite, lorsque deux nœuds désirent mutuellement vérifier leurs identités, ils fusionnent leurs dépôts respectifs dans le but de trouver une chaîne de certificats qui les lie dans une relation de confiance.

Le succès de cette approche dépend en grande partie des caractéristiques des graphes de certificats mais également de la construction des dépôts de certificat locaux. D'autre part, avant d'être à même de générer des certificats, chaque nœud doit d'abord construire son dépôt de certificat, ce qui constitue une opération complexe, En outre, si le nombre de certificat révoqués devient trop important, les dépôts de certificats deviennent obsolètes dans la mesure où les chaînes de certificats ne sont plus valides.

3.2.5. TESLA :

Le protocole TESLA (*Time Efficient Stream Loss-tolerant Authentication*), a été proposé par [60], comme solution contre les comportements malveillants dont l'objectif est la découverte des informations de topologie ou l'injection de fausses informations de routage.

TESLA permet d'authentifier les messages avec un MAC (*Message Authentification Code*) dépendant d'une clé secrète qui n'est divulguée par l'émetteur du message qu'après un délai d'attente δ. La valeur δ est calculée de manière à ce qu'on soit sûr que le destinataire a reçu le message avant la divulgation de la clé, cette condition garantie l'intégrité du message. Le temps δ ne doit pas être trop important pour limiter les latences dans le réseau, en effet un destinataire doit attendre la divulgation de la clé secrète avant de pouvoir effectivement traiter un message.

Une manière de contrer les attaques sur les mécanismes de routage consiste en l'authentification des messages de découverte et de maintenance de route. *Hu, Perrig et Johnson* ont développé un protocole de routage, *Ariadne* [69], basé sur le protocole DSR (Dynamic Source Routing) et qui implémente des mécanismes d'authentification des messages de routage en utilisant au choix un schéma de signature numérique, l'utilisation de MAC avec autant de clés secrètes établies que de paires de nœud ou bien en mettant en œuvre TESLA. Leur travail se focalise sur cette dernière solution. Une conclusion intéressante de leur travail montre que l'introduction de mécanisme de sécurité dans un protocole de routage passe nécessairement par une diminution des performances de ce protocole.

3.3. Protections utilisant la cryptographie asymétrique :

3.3.1. SAODV :

M.G. Zapata et N. Asokan ont mis au point un Protocole dédié à la sécurisation du protocole AODV, appelé SAODV (*Secure Ad hoc On demand Distance Vector*) [48]. L'idée principale de SAODV consiste à utiliser des signatures afin d'authentifier la plupart des champs des paquets Route_Request et Route Reply et d'utiliser des chaines de hachage pour protéger l'intégrité du compteur de sauts. Ainsi, SAODV constitue-t-il une extension d'AODV avec des signatures, afin de contrer les attaques de type "usurpation d'identité". SAODV nécessite la présence d'une autorité de certification afin de vérifier les paquets signés, assurant ainsi leur authenticité. Dans SAODV, chaque paquet RREQ inclut une extension de signature simple. L'initiateur du paquet choisit un nombre de sauts maximal en se basant sur une estimation du diamètre du réseau et il génère ensuite une chaîne de hachage à sens unique d'une longueur égale au nombre de sauts, plus un.

Ce protocole assure une bonne authentification des messages de contrôle ainsi qu'une bonne intégrité. Cependant, l'utilisation de chaînes de hachage ne permet pas d'empêcher à 100% les attaques sur le nombre de sauts. Ainsi, bien que le hachage du nombre de sauts

empêche un éventuel nœud malicieux d'annoncer des routes plus courtes qu'en réalité, rien n'empêche un attaquant d'augmenter arbitrairement la longueur des routes, En effet, un tel nœud peut appliquer la fonction de hachage plusieurs fois consécutives avant de relayer un paquet, la route apparait ensuite plus longue qu'elle n'est en réalité.

D'autre part, dans l'éventualité où il y aurait plusieurs attaquants complices, une attaque de type tunnel peut toujours être lancée et le nombre de sauts peut même être décrémenté à l'arrivée, de manière transparente pour les autres nœuds.

3.3.2. ARAN :

Les concepteurs du protocole ARAN (A secure Routing protocol for Ad hoc Network) [70] ont également choisi d'utiliser la cryptographie à clés publiques pour sécuriser les routes. ARAN est un protocole à la demande, qui fournit un service d'authentification de saut en saut par le biais d'une infrastructure à clés publiques. Il suppose donc l'existence d'un serveur d'authentification T, dont le rôle est de gérer les certificats et dont la clé publique est connue de tous les participants. Ainsi, avant d'entrer dans le réseau, chaque nœud doit s'identifier auprès du serveur et solliciter auprès de lui un certificat qui lui servira à signer les messages qu'il enverra. Ce certificat contient l'adresse IP du nœud, sa clé publique, une première estampille qui rend compte de la date de création du certificat, et une seconde qui indique sa date d'expiration. De manière classique, ce certificat est ensuite signé par T et doit être mis à jour régulièrement.

Le principe d'ARAN est sécuriser le mécanisme de découverte de routes de nœuds en nœud. Ainsi lorsqu'un nœud désire envoyer un message, il génère, signe puis diffuse un paquet de type RDP (Route Discover Packet). Par la suite, chaque nœud intermédiaire recevant ce paquet vérifie le certificat du nœud précédent, appose son propre certificat et rediffuse le paquet. Une fois ce paquet arrivé au nœud destination, celui-ci vérifie à son tour le certificat et répond en unicast, par un message de type REP (reply packet) qui est à son tour vérifié de nœuds en nœuds.

En effet, dans ce protocole, pour chaque paquet de découverte do route, il faut vérifier le certificat fourni, déchiffrer le paquet, le rechiffrer avec sa propre clé et apposer son certificat. Lorsque le nombre de paquets devient important, cela peut se révéler extrêmement coûteux. Aussi une attaque par déni de service consistera à inonder le réseau de faux paquets de contrôle, dont la vérification va monopoliser exagérément les ressources des nœuds. D'autre

part, si un nœud ne peut effectuer cette vérification en temps réel, il peut dire amené par un attaquant à supprimer certains paquets aléatoirement, y compris des paquets valides.

3.4. Protection utilisant la cryptographie symétrique :

3.4.1. SRP :

Panagiotis Papadimitratos et Zygmunt Haas ont proposé un protocole de routage sécurisé, SRP (Secure Routing Protocol) [45] spécialement adapté aux caractéristiques du protocole DSR et du protocole de routage interzone ZRP. Ainsi, ils ont conçu SRP comme une extension de l'en-tête des paquets Route_Request et Route_Reply. SRP utilise des numéros de séquence à l'intérieur des requêtes, de manière à garantir leur fraîcheur, cependant, ce numéro de séquence ne peut être vérifié qu'au niveau de la destination. Il établit en outre des associations de sécurité, entre les nœuds communicants uniquement. Cette association est ensuite utilisée pour authentifier les paquets Route_Request et Route_Reply par le biais de MAC. Au niveau de la destination, SRP permet de détecter des modifications de paquets de type Route_Request tandis qu'au niveau de la source, c'est l'intégrité des Route_Reply qui sera analysée.

Puisque SRP ne nécessite des associations de sécurité qu'entre les nœuds communiquant entre eux, il est relativement léger. En contrepartie, certains défauts ont assez pénalisants et limitent son intérêt, Tout d'abord, SRP ne sécurise pas le mécanisme de maintenance des routes et délègue cette tâche à un autre protocole. De plus, SRP ne permet pas de détecter les modifications portant sur les informations de routage habituellement soumises à modification lors du routage. Par exemple, un nœud peut aisément corrompre voire supprimer le contenu de la liste de nœuds comprise à l'intérieur d'un paquet de type Route_Request. Enfin, l'intégrité des messages n'étant vérifiée qu'au niveau des nœuds source et destination, un attaquant eut toujours corrompre des paquets de manière à gaspiller les ressources du réseau en retransmissions inutiles.

3.4.2. SAR :

Le protocole SAR (*Security-aware Ad hoc Routing protocol)* [52] se base lui aussi sur des procédés de chiffrement symétrique. Il a été élaboré à l'origine pour prévenir les attaques de type "*trou noir* " qui consiste à supprimer l'intégralité des paquets au niveau d'un nœud malicieux. A l'instar des protocoles précédents, SAR est conçu pour être employé conjointement avec des protocoles réactifs tels qu'AODV ou DSR. Il utilise la notion de "niveaux de confiance" pour établir la sécurité d'un chemin. Ainsi, lorsqu'un nœud désire

établir une route avec un certain niveau de sécurité, il génère un nouveau paquet RREQ indiquant le niveau requis. Par la suite, le mécanisme de découverte de routes diffère légèrement du schéma classique des protocoles réactifs en ce sens que seuls les nœuds satisfaisant le niveau de sécurité requis peuvent rediffuser la requête à ses voisins. Dans le cas contraire, la requête est rejetée par le nœud. Une fois la route établie jusqu'à la destination, celle-ci génère en retour un paquet PREP avec le même niveau de sécurité. Dans l'éventualité où aucune route en retour ne garantit le niveau de sécurité requis, celui-ci peut être ajusté par le nœud source.

Bien sûr, cette approche implique de lier l'identité d'un nœud à un certain niveau de sécurité. Pour ce faire, il existe une clé secrète pour chaque niveau de sécurité défini et celle-ci doit être distribuée à tous les nœuds du réseau satisfaisant ce niveau de sécurité. Le contenu ainsi que l'en-tête des paquets sont ensuite chiffrés par la clé de sorte que les nœuds de niveau inferieur ne puissent pas le lire, Par conséquent, même l'information sur la topologie peut être cachée aux nœuds non sûrs.

Cette capacité à partitionner le réseau en fonction de différents niveaux de sécurité fait de SAR un protocole original. En contrepartie, il souffre de plusieurs défauts importants, le principal réside dans la distribution des clés [7]. Celle-ci doit être effectuée préalablement à la mise en place du réseau, par le biais d'un canal sûr. Ensuite, on peut imaginer que les nœuds de plus hauts niveaux de confiance sont utilisés pour distribuer les clés correspondant à des niveaux inférieurs. Mais ceci ouvre la voie à des attaques sévères de type usurpation d'identité si un nœud vient à être corrompu. En effet, dans ce cas, ce sont les clés de tous les niveaux de sécurité inferieurs qui deviennent obsolètes, menaçant de fait, la sécurité globale du réseau. D'autre part, le fait de chiffrer et déchiffrer tous les paquets (y compris les en-têtes) risque d'avoir un impact important sur les ressources du réseau. Et ceci peut être utilisé par un nœud malicieux pour lancer une attaque de type déni de service. Enfin, un effet de bord inhérent à cette approche est que Les routes ne sont plus optimales en termes de sauts.

3.4.3. Ariadne :

C'est en prenant en compte les inconvénients des procédés de chiffrement asymétrique que Hu, Perrig et Johnson ont mis au point un protocole de routage sécurisé : Ariadne [69], inspiré du protocole classique DSR et s'appuyant uniquement sur des mécanismes de chiffrement symétriques. L'enjeu était de proposer un protocole qui puisse être implémenté aussi bien sur des portables puissants que sur des assistants personnels, c'est pourquoi les

auteurs ont choisi de l'associer à trois méthodes d'authentification, afin de s'adapter aux capacités de calcul des nœuds :

- ✓ Utilisation d'une clé partagée entre chaque paire de nœuds.
- ✓ Utilisation d'une clé partagée entre chaque paire de nœuds communicants combinée à une authentification par diffusion.
- ✓ Utilisation de signatures digitales.

3.5. Protections contre la modification des données :

Les chaines de hachage sont un outil très efficace et permettent d'offrir une protection très suffisante à bien moindre coût par rapport aux approches cryptographiques détaillées précédemment. Ainsi le protocole SEAD *(Secure Efficient distance vector Routing for mobile Ad hoc networks)* propose de renforcer la sécurité du protocole DSDV en utilisant les chaînes de hachage à sens unique. Celles-ci permettent de prévenir d'éventuels attaquants d'incrémenter artificiellement le nombre de sauts dans l'en-tête des paquets de signalisation. Un nœud génère une chaîne de hachage et la décompose en plusieurs segments de *m* éléments (h_0, h_1, ..., h_{m-1}**),**..., (h_{km}, h_{km+1},…, h_{km+m-1}) avec $k = m/n-i$, m correspondant au diamètre maximal du réseau et *i* étant le numéro de séquence (voir figure 14).

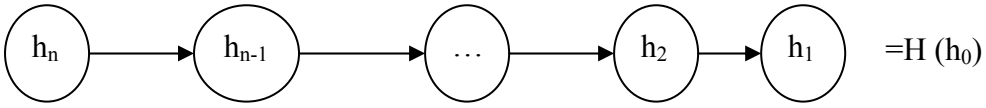


Figure 14 : <u>Les chaines de hachage dans SEAD</u>

Puisque $h_i = H(h_{i-1})$, connaissant h_i, il est facile de vérifier l'authenticité de h_j, tant que *j* reste inferieur à *i*. De plus, comme des fonctions de hachage différentes sont utilisées pour des diamètres et des métriques différentes, un attaquant ne peut jamais forger une valeur de métrique inférieure ou un plus grand numéro de séquence. Enfin, le protocole DSDV spécifie que lorsqu'un nœud reçoit un message de signalisation, il met à jour sa table de routage si le numéro de séquence est plus grand ou identique avec une métrique inférieure. Donc, SEAD permet d'empêcher un attaquant potentiel de décrémenter artificiellement le nombre de sauts ou d'incrémenter le numéro de séquence des paquets.

En plus de leurs travaux sur SRP, P. Papadimitratos et Z. Haas ont également mis au point un mécanisme destiné à sécuriser les protocoles de routage à état de lien, appelé SLSP (*Secure Link State Protocol*) [45]. A l'instar de SEAD, ce protocole utilise les signatures

digitales ainsi que les chaînes de hachage à sens unique pour garantir l'intégrité des mises à jour de l'état des liens. SLSP peut être utilisé seul, de manière indépendante ou bien comme le protocole de routage interzone (IARP) qui est une composante du protocole ZRP. Le protocole SRP comporte quatre mécanismes principaux, à savoir un protocole de surveillance des voisins (NLP), un protocole de distribution de clés (PKD), un protocole de mises à jour des états des liens (LSU) et enfin un mécanisme de prévention des attaques de type déni de service.

Grace à NLP, chaque nœud s'authentifie auprès de ses voisins en diffusant à travers le réseau un couplet (adresse IP/adresse MAC) signé. Un nœud peut également avertir SLSP lorsque pour une même adresse physique, correspondent deux adresses IP, lorsque deux adresses physiques différentes revendiquent la même adresse IP ou bien encore lorsqu'un nœud utilise la même adresse physique. Ensuite, chaque nœud diffuse périodiquement â l'intérieur d'une zone, un paquet PKD qui contient sa clé publique certifiée. Les mises à jour de l'état de liens (LSU) quant â elles, sont également signées et périodiquement diffusées à l'intérieur d'une même zone. Pour s'assurer que les paquets PKD et LSU ne traversent pas trop de nœuds, chacun d'entre eux inclut un compteur de sauts. A l'instar de SEAD et SAODV, des chaînes de hachage sont utilisées pour protéger ces compteurs. Enfin, afin de limiter les attaques de type déni de service, chaque nœud surveille ses voisins et affecte une priorité basse aux nœuds qui génèrent trop de mises à jour. La technique est ici exactement la même que peur le protocole SRP. En contrepartie, l'inconvénient est le même à savoir qu'un attaquant â la possibilité d'usurper l'identité d'une victime et inonder son voisinage avec des mises à jour qui vont sembler avoir été émises par la victime. De plus, bien que la victime ait toujours la possibilité de détecter l'attaque, en raison des détections d'adresses physiques multiples du mécanisme NLP, il est fortement probable qu'elle ne puisse réagir. Enfin, SLSP ne permet pas de prendre en compte d'éventuels attaquants complices qui pourraient forger des métriques erronées ou même de créer des tunnels.

3.6. Protection contre les attaques de type "tunnel" :

Les procédés cryptographiques employés dans les schémas précédents permettent de contrer efficacement un nombre important d'attaques. Pourtant, aucun d'entre eux, qu'il soit asymétrique ou à clés secrètes, ne permet de remédier au problème du tunnel ou (*Wormhole*). En effet, même si toutes les entrées d'un chemin semblent parfaitement identifiées, rien n'empêche un nœud chargé de transférer un paquet, de requérir parallèlement une route jusqu'à un nœud complice et de transférer le paquet encapsulé vers ce complice, lequel sera

ensuite chargé d'acheminer le tout vers la destination. Plusieurs solutions peuvent être envisagées pour résoudre ce problème. Tout d'abord, lors du processus de découverte de route, le paquet RREQ est inondé à travers le réseau et puisque le tunnel passe forcément par un nombre de nœuds plus important, si la destination établit le temps comme critère de choix d'un chemin, il y a fort à parier que la route passant par le tunnel ne sera pas choisie car elle sera moins rapide. D'autre part, on peut imaginer que les nœuds situés autour du premier nœud malveillant relaient le paquet jusqu'à la destination avant même que les nœuds complices aient eu le temps de l'encapsuler dans un tunnel. Toutefois, ces solutions ne sont pas viables en toutes circonstances et notamment dans le cas où le nœud complice est un nœud indispensable sur le chemin. C'est pourquoi une équipe de l'université de Carnegie Mellon a mis au point une parade basée sur la localisation des nœuds d'une part et sur leur synchronisation temporelle d'autre part : *packet leashes* [54]. Dans la version de base, l'émetteur d'un paquet y inclut sa localisation et un horodateur correspondant à son horloge lors de l'émission. Lorsque la destination reçoit le paquet, elle compare ces valeurs avec sa propre localisation et son horloge au moment de la réception du paquet. Si les deux nœuds sont synchronisés à un coefficient près, le destinataire peut estimer, à partir des marqueurs temporels, une approximation de la distance qui les sépare et ainsi vérifier si cela correspond bien à la distance réelle. Néanmoins, il existe certaines circonstances pour lesquelles cette technique est inefficace. C'est le cas par exemple lorsque des obstacles s'immiscent entre deux nœuds voisins. Dans de telles circonstances, un schéma de protection basé sur la corrélation entre distances et temps de transfert ne pourrait empêcher une attaque de type tunnel, C'est pourquoi les chercheurs ont développé un deuxième schéma dans lequel seule la métrique temporelle est prise en compte. Pour ce faire, les nœuds doivent être synchronisés entre eux à quelques microsecondes, voire nanosecondes près, cette différence doit être connue de tous les nœuds. Le procédé est alors identique lorsqu'un paquet est envoyé, on y inclut un horodateur (horloge d'émission). Ensuite, le nœud destination compare cette valeur avec son horloge au moment de la réception du paquet. Il est ainsi capable de déterminer si la distance parcourue est raisonnable en comparant le temps de transfert avec la vitesse de propagation de l'onde, Une variante consiste à inclure dans le paquet une date d'expiration au-delà de laquelle le paquet doit être purement et simplement ignoré.

3.7. Mécanismes basés sur la réputation :

Les mécanismes détaillés précédemment se révèlent efficace pour assurer les fonctionnalités de sécurité classiques que sont la confidentialité, l'intégrité et surtout

l'authentification. Ils permettent ainsi d'empêcher de nombreuses attaques qui perturbent considérablement le processus de routage. En revanche, ils ne se révèlent pas du tout adaptés pour résoudre le problème de non-participation des nœuds. En effet, les mécanismes cryptographiques, aussi efficaces soient-ils ne permettent pas de s'assurer qu'un nœud participe au processus de routage en relayant tous les paquets. Or, dans le contexte des réseaux Ad hoc, c'est là une fonctionnalité primordiale dans la mesure où ce type de réseaux est basé sur la coopération entre les nœuds. C'est pourquoi en sus des mécanismes de sécurité, certains protocoles visent plus spécifiquement l'incitation à la coopération. Parmi ceux-ci, on distingue généralement deux catégories ceux qui se basent sur une réputation des nœuds élaborée au cours du temps en fonction des observations, et d'autre part ceux qui instaurent un système de paiement virtuel.

3.7.1. Mécanismes de micro-paiement :

Le concept consiste à monnayer les services auxquels les nœuds souhaitent accéder en échange de crédits virtuels. Pour obtenir ces crédits, chaque nœud doit fournir des services aux autres nœuds. Les crédits sont ultérieurement dépensés pour pouvoir acheter des services. Si un nœud n'a plus assez de crédits pour acheter le moindre service, cela signifie alors qu'il n'a pas suffisamment participé au bon déroulement du processus de routage.

Le protocole Nuglets [54], s'inscrit dans cette optique. Son objectif est à la fois d'inciter les nœuds à participer et de limiter les inondations du réseau, dès lors qu'elles deviennent payantes. Afin, de sécuriser les crédits virtuels, le protocole suppose l'existence de matériels inviolables. L'hypothèse principale est donc qu'aucune attaque ne peut être lancée contre la monnaie virtuelle. Deux modèles sont spécifiés par le protocole. Dans le premier, un nœud désirant envoyer un paquet doit au préalable y incorporer suffisamment de crédits. Par la suite, chaque nœud intermédiaire sur la route prélève une quantité de crédits. Si le nombre de crédits est insuffisant, le paquet est rejeté. L'intérêt de cette approche est qu'elle limite les attaques de type déni de service dans la mesure où aucun nœud ne peut se permettre de financer une inondation. En revanche, elle implique que chaque nœud connaisse par avance le nombre de nœuds sur la route. Si le nombre de crédits est trop grand, ils sont gaspillés. Dans le cas contraire, le paquet est perdu et davantage de crédits doivent être dépensés pour sa réémission. Dans le second modèle, le routage fait l'objet de transactions puisque ce sont ici les nœuds destinataires qui doivent payer pour recevoir les paquets qui leur sont destinés. En effet, chaque nœud achète les paquets reçus de son voisin amont et le destinataire d'un paquet l'achète donc au dernier nœud intermédiaire. Cette approche souffre d'un inconvénient encore

plus conséquent que la précédente puisqu'elle ne permet pas d'empêcher un attaquant d'inonder le réseau [7]. Au contraire, un nœud peut être tenté de relayer beaucoup de paquets vers de nombreux nœuds afin de maximiser ses profits lors des transactions.

D'une manière générale, ces protocoles ne collent pas suffisamment au modèle Ad hoc pour être efficaces. Tout d'abord, ils ne prennent pas assez en compte la mobilité des nœuds. En effet, si un nœud intermédiaire quitte la route, le paquet est perdu ainsi que l'investissement en termes de crédits, soit pour l'émetteur (cas du premier modèle) soit pour le dernier nœud intermédiaire (deuxième modèle). Enfin, cette approche pose de gros problèmes concernant le fonctionnement même du protocole de routage [7]. Ainsi dans le cas d'un protocole réactif les nœuds peuvent être tentés de ne pas envoyer de messages d'erreur RRER lors de la détection de la rupture d'un lien puisqu'ils auraient alors à payer pour cela. Dans le cas d'un protocole proactif, cela concernerait les messages de contrôle qui deviendraient alors trop coûteux. Enfin, le protocole devrait aussi s'assurer que les nœuds ne puissent pas voler des crédits simplement en espionnant les conversations de ses voisins.

3.7.2. Mécanismes basés sur la confiance :

Ces protocoles ont pour but de fournir des classements des nœuds afin de différencier les "bons" nœuds, qui ont une bonne réputation car ils coopèrent régulièrement, des "mauvais" qui adoptent un comportement égoïste.

Le protocole Confidant [71] "*cooperation of nodes-fairness in dynamic Ad hoc networks*", utilise une infrastructure à clés publiques auto-organisée inspirée du protocole PGP. L'objectif de *Confidant* est de traiter à la fois les nœuds malicieux et égoïstes à travers la supervision et l'analyse de deux processus du routage à savoir le transfert de données et la découverte de voisins. Il est ainsi conçu pour être utilisé conjointement avec un protocole réactif, typiquement DSR. Confidant se compose de quatre éléments complémentaires : le moniteur, le moniteur de confiance, le système de réputation et le mécanisme de gestion de chemins. Le rôle du moniteur consiste à s'assurer que les voisins du nœud auquel il est rattaché relaient correctement le paquet. Lorsque le moniteur détecte une anomalie ou une incohérence, il avertit le système de réputation, qui de son côté maintient à jour des listes de notes pour chaque nœud observé. Les listes peuvent être éventuellement échangées entre les nœuds. Ainsi, si une liste est reçue d'un nœud de grande confiance, le récepteur peut directement enregistrer les informations à l'intérieur de sa propre liste. Dans le cas contraire, si la liste est envoyée par un nœud suspect, le récepteur peut l'ignorer totalement ou bien encore l'accepter tout en lui donner significativement moins d'importance qu'une liste reçue

d'un nœud sûr. Finalement, le mécanisme de gestion de chemin détermine les routes les plus sûres à partir des listes de nœuds exclus et des nœuds de confiance. En outre, il peut décider de refuser de relayer les requêtes en provenance de nœuds mal notés.

Concernant la gestion de la confiance, l'approche s'inspire de celle utilisée dans PGP. Ainsi, les nœuds disposent de quatre niveaux de confiance: ami, marginai, inconnu ou ennemi. Chaque nœud enregistre ses amis dans une liste dédiée. Par la suite, si un nœud *A* parvient à détecter un comportement malicieux de la part d'un nœud *B*, le nœud *A* va avertir tous les amis contenus dans la liste à l'aide d'un message d'alarme signé. De tels messages peuvent être diffusés à travers le réseau, Il appartient ensuite à chaque nœud de décider si le message doit être pris en considération, suivant que l'émetteur est de confiance ou non. Une version améliorée de Confidant utilise une approche bayésienne afin de différencier plus efficacement les vraies alarmes de mensonges destinés à faire baisser la réputation d'un nœud.

Une des motivations principales qui peuvent pousser un nœud à ne pas participer au routage est l'économie d'énergie. Celle-ci étant parfois une ressource critique, certains nœuds peuvent être tentés de l'épargner en adoptant un comportement égoïste. Pour lutter contre ce phénomène, *Michiardi* et *Molva* ont mis au point le protocole CORE (*a collaborative reputation mechanism to enforce node cooperation in mobile Ad hoc networks*) [56]. L'objectif est ici non plus d'exclure définitivement les nœuds mais au contraire de les encourager à participer en rejetant leurs paquets jusqu'à ce qu'ils coopèrent au processus de routage. CORE prend entre autres comme hypothèses que : les identités des nœuds sont uniques et non modifiables, qu'un mécanisme de routage adapté est à même de sécuriser la phase de découverte de voisins et enfin, que le trafic à l'intérieur du réseau est suffisamment dense. Le fonctionnement est très similaire à celui de Confidant à savoir des moniteurs qui analysent le trafic et qui transmettent les résultats à un système de gestion des réputations. L'échange des réputations entre les nœuds est ici optionnel. Les auteurs ont en outre validé leur approche à la fois par la simulation et la théorie des jeux.

CORE souffre malheureusement de défauts importants [7]. Tout d'abord, il ne résout pas réellement le problème de non-participation. Certes, les nœuds égoïstes voient leurs paquets systématiquement rejetés et en ceci, le protocole est efficace. Mais en contrepartie de grandes quantités de données demeurent perdues, diminuant significativement le rendement du réseau.

Le tableau suivant récapitule les possibilités de défense qu'offrent les différents protocoles de sécurité décrits dans ce chapitre. On constate que les protocoles ont tendance à cibler certaines attaques en particulier, de sorte qu'aucun n'offre une protection efficace face

à toutes les attaques décrites ici. La conclusion que l'on peut en tirer est que la solution la plus prometteuse est probablement dans l'utilisation d'un protocole combinant ces approches un protocole basé sur la cryptographie pour assurer l'authentification des nœuds et l'intégrité des messages de contrôle et un protocole basé sur les modèles de confiance pour déceler puis ignorer les nœuds présentant un comportement malicieux.

	Ecoute indiscrète	**Usurpation**	**Grey hole**	**Black hole**	**Tunnel**	**Non-coopération**
ARAN	Oui	Non	Oui	Oui	Oui	Oui
Ariadne	Oui	Non	Oui	Oui	Oui	Oui
SRP	Non	Oui	Non	Non	Oui	Non
CORE						
SAODV	Non	Non	Oui	Oui	Oui	Oui
Confidant	Oui	Non	Non	Non	Oui	Non
Packet leashes	Oui	Oui	Oui	Oui	Non	Oui

Tableau 1 : Protocoles sécurisés, prévention des attaques

3.9. Systèmes de détection d'intrusion :

Pour contrer les attaques sur les mécanismes de routage de type *black hole*, où un nœud malicieux prétend être un relais pour un autre nœud mais ne transmet pas les messages de données. Maarit et al. [68] Ont développé deux méthodes appelées *watchdog* et *pathrater*. Le *watchdog* permet d'identifier les nœuds malicieux. Le *pathrater* est une technique permettant au protocole de routage d'éviter les nœuds corrompus inscrits dans une liste noire, *blacklist*. Il faut rester prudent quant à l'utilisation de ces mécanismes car ils peuvent être détournés par un attaquant [68].

En effet, un nœud malicieux peut aussi faire en sorte qu'un nœud valide soit ajouté à la liste noire, l'isolat ainsi du réseau. L'utilisation de détecteurs d'intrusion dans les réseaux Ad hoc est une solution complémentaire faisant l'objet de recherches intensives. L'IDS (*Intrusion Detection System*) collecte et analyse les données du trafic afin de déterminer si des utilisateurs non autorisés sont connectés ou si certains nœuds ont des comportements anormaux. La fonction de l'IDS est de détecter les attaques menées contre les services implicites fournis par un nœud, comme le protocole de routage, mais aussi de surveiller le

respect des règles définies explicitement par la politique de sécurité. Plus généralement, la fonction de l'IDS est de détecter et de réagir à l'apparition de certains scénarios prédéfinis.

4. Conclusion :

Nous avons vu dans ce chapitre que tous les protocoles de routage classiques dans les réseaux Ad hoc (AODV, DSDV, OLSR) sont particulièrement vulnérables à un grand nombre d'attaques qui peuvent aller de la capture d'informations sensibles à la paralysie complète du réseau. Or, à l'époque actuelle, où l'utilisation des réseaux sans fil connaît un essor sans précédent (notamment grâce au Wi-fi, au Wi-max et aux téléphones mobiles) et où parallèlement, le nombre d'attaques contre les systèmes informatiques n'a jamais été aussi élevé, l'enjeu de la sécurité des réseaux est devenu considérable. Ainsi, même si les réseaux Ad hoc constituent une solution tout à fait prometteuse aux problèmes actuels liés à la mobilité des utilisateurs et des réseaux eux-mêmes, leur développement est freiné aujourd'hui par l'absence de mécanismes de sécurité suffisamment efficaces pour subvenir aux besoins actuels en protection des données tels que ceux des applications commerciales.

Partant de ce constat, les recherches qui autrefois étaient concentrées sur l'amélioration des performances, se réorientent aujourd'hui sur la sécurisation des protocoles de routage. Cependant les procédés employés sont souvent très différents d'un algorithme à l'autre et les caractéristiques inhérentes au modèle Ad hoc telles que la mobilité, l'absence d'infrastructure et la limitation des ressources imposent de repenser complètement les dispositifs de protection classiques utilisés dans le domaine filaire et obligent les concepteurs à frire des compromis entre la sécurité des protocoles et les contraintes de performances. En effet, dans un contexte totalement distribué, ces mécanismes doivent être adaptés en conséquence, au risque d'engendrer une surcharge conséquente du réseau. C'est la raison pour laquelle aucun des protocoles sécurisés élaborés dernièrement ne s'est avéré suffisamment satisfaisant pour s'imposer comme standard. Tous se révèlent soit trop coûteux en termes de ressources (délai, débit, mémoire, etc.), soit trop complexes pour être implantés. Les problèmes posés par l'échange de clés secrètes ou la mise en place de clés de groupe sont souvent éludés par les concepteurs des protocoles qui considèrent ces étapes comme indépendantes.

L'expérience dans le domaine de la cryptographie a déjà montré que la conception de protocoles sécurisés est souvent sujette à des faille difficilement détectables même en admettant que le chiffrement est parfait. Ainsi, même si les protocoles détaillés dans ce chapitre permettent d'améliorer sensiblement la sécurité du processus de routage, ils offrent

en contrepartie une vulnérabilité accrue aux attaques de type déni de service. Or l'analyse des protocoles cryptographiques est complexe car l'ensemble des configurations à envisager est immense voire infini. C'est pourquoi bon nombre de travaux portent actuellement sur l'automatisation de la vérification des protocoles Ad hoc à partir de leurs spécifications.

Quoi qu'il en soit, aucun protocole ne peut en l'état contrer toutes les attaques détaillées ici, la plupart se contentant de cibler une menace (non-participation, usurpation d'identité, détournement de trafic) et de fournir une solution relativement adaptée. C'est pourquoi la tendance la plus probable est à une utilisation combinée de différentes approches (cryptographie symétrique/asymétrique, modèles de confiance) au sein d'un même protocole, pour sécuriser le réseau. Une autre tendance possible est l'apparition d'un clivage qui verrait apparaître deux types de réseau distincts, les réseaux fermés et les réseaux ouverts. Les premiers seraient restreints à un groupe d'individus définis au sein d'une même entité (unité militaire, réseau d'un fournisseur d'accès, d'une entreprise, etc.). Le contrôle d'accès sur les composants du réseau garantirait une sécurité élevée mais au détriment de la souplesse (les nœuds devraient être configurés préalablement à leur entrée sur le réseau, pour permettre la mise en place de clés et l'attribution d'une adresse par exemple). Les seconds se caractériseraient par un accès totalement ouvert au réseau (comme pour les réseaux citoyens par exemple ou les réseaux véhiculaires). En revanche, la sécurité ne pourrait alors plus être totalement garantie.

Architecture Ad hoc Sécurisée

1. Introduction :

Pour sécuriser les réseaux Ad hoc, nous envisageons une architecture qui devra être capable de proposer un niveau de sécurité adapté à l'enjeu de la communication et dont le niveau pourra évoluer dans le temps en fonction du contexte. Bien entendu, une solution complètement opérationnelle respectant l'ensemble de toutes les spécificités exigées par un tel réseau n'existe pas encore. Mais, il nous a apparu que la notion de confiance constitue le levier incontournable à l'émergence d'une solution globale au problème de la sécurité dans des réseaux d'objets autonomes. En effet, il est admis que la construction d'une relation de confiance entre deux entités autonomes, en l'absence de tiers, est un enjeu très complexe.

2. La confiance :

2.1. Définition de la confiance :

La confiance est un mécanisme de coordination des échanges en situation d'ignorance ou d'incertitude : c'est elle qui permet de prendre une décision malgré l'existence d'un risque [2]. Il faut remarquer que l'on ne parle de confiance que par rapport à une personne (éventuellement morale) : cette notion se distingue ainsi de celles qui s'appliquent aux techniques ou aux technologies, comme la sécurité, la fiabilité, la sûreté. Bien sûr, ces notions sont liées en pratique : le fait qu'une entreprise utilise des technologies sûres et fiables peut influencer la confiance que l'on fait à l'entreprise.
On distingue en général deux types de confiance :

- ✓ La confiance assurée (on parle parfois de confiance aveugle), c'est-à-dire que la confiance est acquise a priori, sans réelle évaluation du risque, ceci peut être le cas parce que l'on estime que la réalisation du risque est très improbable, que les inconvénients possibles sont minimes par rapport aux avantages attendus, ou encore que l'on n'a pas vraiment d'alternative.
- ✓ La confiance décidée, résultat d'un réel processus d'appréciation du risque (évaluation des avantages attendus de la décision et des inconvénients qui peuvent en découler) et décision parfaitement consciente. Celle-ci sous-entend que la décision prise peut conduire à une déception, et un regret de l'avoir prise. Elle ne peut donc être requise que dans le cas où les dommages possibles sont supérieurs aux avantages reçus.

Sauf à vivre dans un état d'incertitude et d'indécision permanente "ce qui conduirait à ne jamais décider" un certain niveau de confiance assurée est indispensable : dans l'histoire, cette

confiance a pu être placée en la famille, la tribu, Dieu, le roi, l'Etat, la Science, etc. La frontière entre confiance assurée et confiance décidée n'est d'ailleurs pas fixe : en fonction de l'expérience notamment, on peut être amené à revoir notre confiance assurée.

2.2. Les fondements de la confiance :

La confiance étant une espérance, sur quels éléments tangibles peut-on se fonder pour accorder sa confiance ? Trois fondements peuvent être identifiés :

- ✓ L'historique des relations : "*cela s'est bien passé avant, donc cela se passera bien la prochaine fois* ".
- ✓ Les recommandations des tiers : "*cela s'est bien passé avec d'autres, donc cela se passera bien avec moi*".
- ✓ La capacité à exercer des représailles : "*cela va bien se passer car il a plus à perdre que moi, si cela se passe mal*".

3. Architecture distribuée pour sécuriser les réseaux Ad hoc :

Pour sécuriser les réseaux Ad hoc, nous envisageons une architecture hiérarchique 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) 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 (le nœud) avec son environnement (principes de : *réputation* et *recommandation*).

- ❖ Dans chaque groupe, élire un nœud chef (Cluster Head), parmi les nœuds qui disposent d'un niveau de confiance (réputation) et/ou de stabilité 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) [72] [58] 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 [59].
- 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 (voir figure 15). 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***.

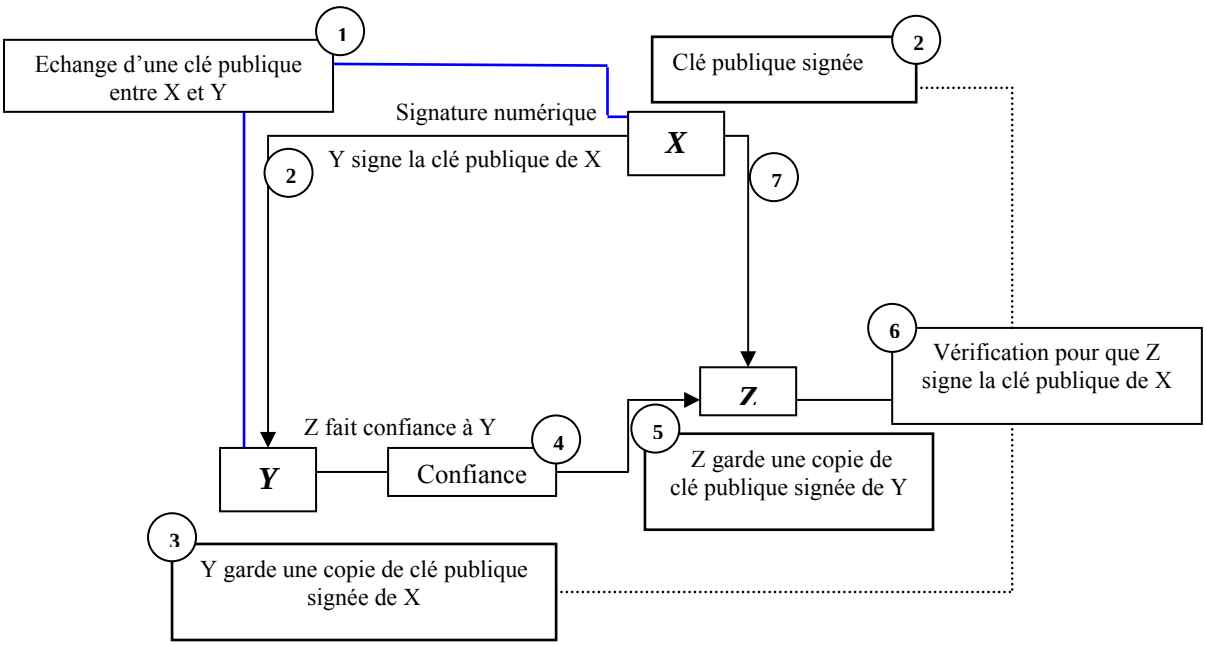
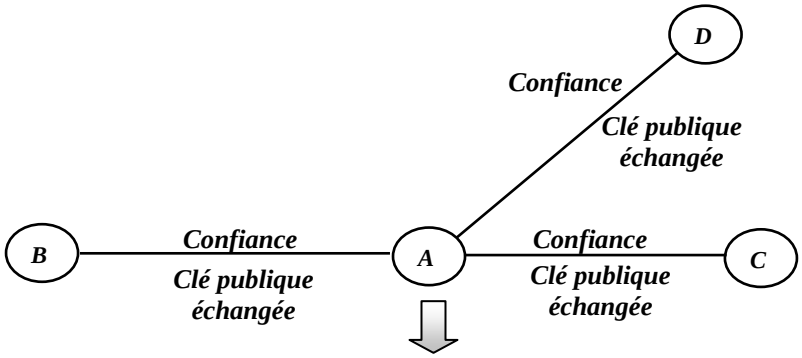


Figure 15 : Création d'une chaîne de confiance

Les figures ci-dessous, montre à ce quoi un tel modèle pourrait ressembler notre idée :

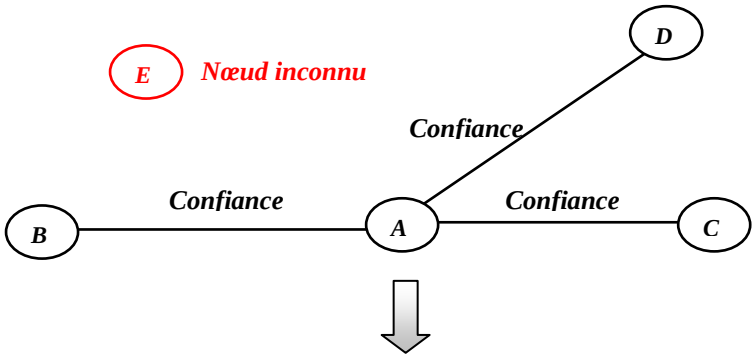
- Chaque utilisateur engendre et distribue sa propre clé publique. Cela mène à ce que tous les utilisateurs signent mutuellement leurs clés publiques. Créant ainsi une communauté d'utilisateurs interconnectés (Climat de confiance) (Figure 16).



Nœuds	Sc	Vr
A	1	1
B	1	1
C	1	1
D	1	1

Figure 16 : Climat de confiance

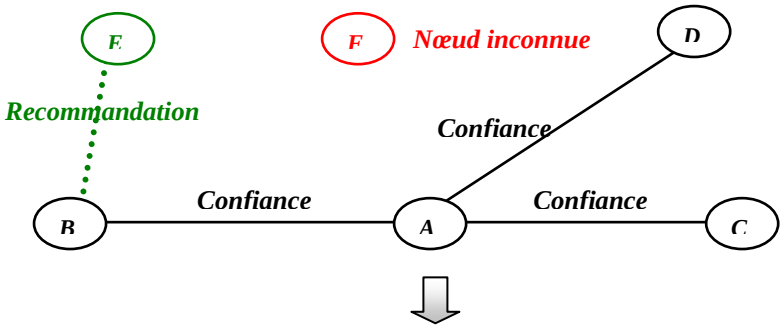
- Le nœud E (Figure 17) est un nouveau nœud qui rejoint le groupe



Nœuds	Sc	Vr
A	1	1
B	1	1
C	1	1
D	1	1
E	0.1	0

Figure 17 : Le nœud E rejoint le groupe

- Dans le groupe, seul le nœud *B* qui connaît le nœud *E*, et par conséquent lui recommande, par contre le nœud *F* est inconnu (aucun nœud ne le connaît dans cette étape) (Figure 18).

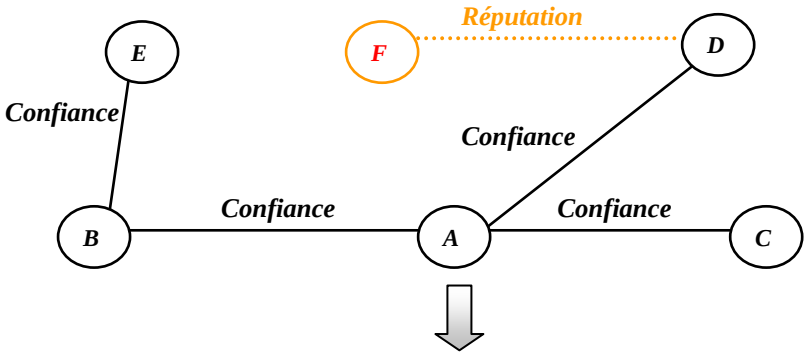


Nœuds	Sc	Vr
A	1	1
B	1	1
C	1	1
D	1	1
E	1	1
F	0.1	0

Figure 18 : Le nœud E ayant une recommandation

- Si le nœud *F* communique avec un nœud de confiance et a prouvé sa totale coopération (ré-acheminement des paquets), alors à chaque fois qu'il échange des paquets de données,

sa valeur de réputation augmente progressivement, jusqu'à ce que le nœud devienne un nœud de confiance (voir paragraphe 3.3.1). (Figure 19).



Nœuds	Sc	Vr
A	1	1
B	1	1
C	1	1
D	1	1
E	1	1
F	0.1	0.65

Nœuds	Sc	Vr
A	1	1
B	1	1
C	1	1
D	1	1
E	1	1
F	0.5	1

Figure 19 : Le nœud E devient un nœud 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. Avec ce procédé, aucun adversaire ne pourra se procurer de statut d'un partenaire légitime.

3.3. Architecture distribuée Clusterisée :

Le Clustering, ou regroupement a été utilisé pour différents objectifs comme la mise à l'échelle des réseaux Ad hoc [51], l'abstraction de la topologie pour le contrôle de l'inondation dans les réseaux [42], la collecte d'informations dans les réseaux de capteurs [44] et le partage de la bande passante [29].

Les premiers algorithmes de Clustering Lowest-ID [29] et Mobic [27] ont des mécanismes assez proches. Ils se sont basés sur un critère particulier pour le choix des Cluster-heads ou chefs de groupe, respectivement les identificateurs des nœuds. Le nombre de

voisins et le degré de mobilité. Ces algorithmes permettent de former des Clusters à un seul saut, où chaque membre est voisin direct de son Cluster-head. Ils considèrent une phase de formation des Clusters ou “Clustering set up”. Pendant cette phase, les nœuds procèdent à la connaissance de leurs voisins et déroulent entre eux l’algorithme de formation des domaines. Toutefois, les nœuds sont supposés fixes au cours de cette étape et une synchronisation entre eux est nécessaire pour le bon déroulement de l’algorithme. De plus, cette phase de formation des Clusters est répétée périodiquement suite aux changements de topologie qui peuvent survenir. La ré exécution périodique de ce processus du Clustering dégrade la stabilité des Clusters.

Dans [51], les auteurs présentent un mécanisme de Clustering qui permet de réduire l’over-head de Clustering. Chaque nœud ne diffuse qu’un seul message pendant la phase de formation des domaines, toutefois, là aussi, l’hypothèse d’absence de mobilité pendant la formation des Clusters doit être vérifiée. En outre, le mécanisme de clustering proposé s’affranchit de la notion des Cluster-heads et ne traite pas le cas où ces derniers quittent le Cluster.

L’algorithme “Distributed and Mobility Adaptive Clustering”, présenté dans [28] et [23] a introduit la notion de poids générique pour la sélection des Cluster-heads. C’est un mécanisme de Clustering qui permet de réagir aux changements de topologie. L’algorithme ne nécessite aucune synchronisation entre les nœuds. Pour améliorer la stabilité des Clusters formés, deux nouveaux facteurs de performances ont été définis. Le premier, *K*, autorise au maximum *K* Cluster-heads à être voisins directs. Le deuxième, *H*, permet de limiter les ré-affiliations entre les Clusters. Les nœuds ne se ré-affilient à un nouveau Cluster-head que lorsque le poids de ce dernier est supérieur d’un certain facteur *H* au poids de leur Cluster-head courant. Toutefois, cette solution ne permet la formation que de Clusters à un saut et le facteur de performance *H* est difficile à spécifier de façon judicieuse.

Dans [19], les auteurs ont présenté une formule multicritères pour les choix des Cluster-heads. Elle prend en considération la mobilité, la connectivité et l’énergie disponible. Ce mécanisme de Clustering “Weighted Clustering Algorithm” nécessite, toutefois, une synchronisation globale et un échange de voisinage entre tous les nœuds du réseau.

Dans d’autres travaux [18] et [17], les auteurs ont essayé de présenter des algorithmes adéquats à la formation de Clusters à *K* sauts.

Toutefois, [17] gère la mobilité par ré-exécution périodique de tout l'algorithme. [18] nécessite d'une part des informations sur le *k*-voisinage et d'autre part que les nœuds vérifient l'hypothèse de non mobilité pendant la phase de Clustering.

[11] présente un mécanisme de Clustering basé d'une part sur la connaissance préalable de l'aire de déploiement du réseau et sur la capacité de se positionner et d'autre part sur la prédiction des mouvements des nœuds en considérant leur historique.

Un sous ensemble de nœuds est élu, d'une manière complètement distribuée, pour jouer le rôle d'un coordinateur local. Les Cluster-heads peuvent être utilisés pour :

- Contrôler l'ordonnancement du canal.
- Contrôler la consommation d'énergie.
- Maintenir la synchronisation des trames.
- Améliorer la réutilisation des codes et du temps.
- Ainsi que pour servir de diffuseur régional.

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. Par exemple, 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 (Figure 20).

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.

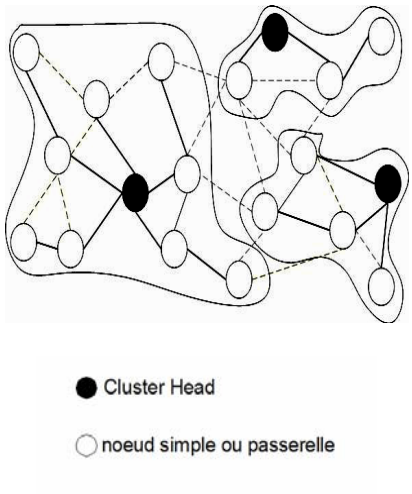


Figure 20 : Cluster-heads et passerelles

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. Le module de contrôle intervient sur différentes couches protocolaires :

- **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 [59], 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) 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 :

$$R_2\,(X, Y) = \text{Nombre des paquets acheminé} / \text{Nombre total des paquets}$$

Comme nous avons déjà expliqué précédemment (paragraphe 3.2.2), 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 concernant le nœud *Y* généré par chaque nœud chargé du contrôle *X*, est :

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

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 :

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

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 (Sc (i)=1) 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 l'ensemble des 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 [29], 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 $R\alpha$ entre les transmissions de deux paquets successifs, donne une connaissance sur la mobilité relative entre deux nœuds voisins X et Y [59].

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

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

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

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.

Chaque nœud de confiance candidat à l'élection pour le rôle de CA, transmet son paquet balise d'élection qui contient les informations suivantes :

- ID du candidat : l'identité du nœud candidat au rôle de CA.
- D : nombre de sauts vers le nœud CA.

- DDc : Degré de confiance, c'est le nombre de nœuds de confiance voisins au nœud candidat.
- Rm : la mobilité relative, pour indiquer la stabilité du nœud candidat par rapport à ses voisins.
- MAC : (Message Authenticated Code) : pour authentifier le paquet balise et aussi pour vérifier l'intégrité de ses informations. Le nœud candidat doit utiliser sa clé privée pour générer le MAC du paquet balise.

Initialement, chaque nœud de confiance (Sc=1) envoie deux paquets "hello" successivement pour calculer la mobilité relative Rm. Puis, il annonce sa candidature au rôle de CA, cela par la génération de son propre paquet balise d'élection. Quand les nœuds de confiance reçoivent des paquets balise de la part de leurs voisins, ils effectuent notre algorithme d'élection (AED) (Figure 21) et de formation de groupe pour définir leur statut : CA (chef de groupe), Np ou juste membre du groupe Nm. La décision dépend des paramètres de sécurité et de stabilité. Lorsqu'il y a compétition entre deux candidats, le nœud avec le nombre de nœuds de confiance voisins le plus petit et avec la mobilité relative la plus élevée perd la compétition et devient soit Np soit un Nm, cela dépend du nombre de sauts par rapport au nœud qui a gagné l'élection. L'algorithme ci-dessous est exécuté par chaque nœud de confiance (Sc=1) à la réception d'un paquet balise dont le nombre de sauts est inférieur à (d) (taille du cluster).

Dans le but de détecter le changement de topologie, nous proposons l'algorithme 2 (Figure 22). Le déplacement du nœud CA est détecté par ses voisins de confiance, si les nœuds de confiance ne reçoivent pas les paquets balise pendant un temps prédéfini, cela implique que le nœud CA n'est plus disponible. Aussi, les nœuds du groupe peuvent détecter la mobilité des nœuds de confiance, cela par la non réception des paquets balise en provenance de ces nœuds. La mobilité des nœuds CAs et les autres nœuds de confiance est très importante pour la durée de vie du groupe et sa stabilité.

Chaque nœud appartenant au groupe avec un statut autre que CA ou nœud de confiance doit recevoir les paquets balise venant du nœud CA à chaque période de temps prédéfinie. Il doit vérifier l'authentification et l'intégrité de l'information du paquet balise par l'utilisation de la clé publique du CA. Si la vérification est réussie alors le nœud récepteur met à jour les changements à propos du nombre de saut vers le CA "D".

Donc notre algorithme d'élection doit augmenter la durée de vie des Clusters formés afin de réduire la durée moyenne d'élection, c'est-à-dire le temps nécessaire d'élection d'un CH.

```
Quand le nœud (j) reçoit un paquet balise de nœud (i)
BEGIN
  Authentication do
  If (Sc <> 1) or (Vr <> 1) then
      Reject ( ); Goto (end);
  Else   ** Sc = 1 or Vr = 1**
     If (D > k) then
       Not valid election; Goto (end);
     Else ** D ≤ 3 **
       If (Rm (i) ≤ Rm (j)) and (DDc (i) > DDc (j)) then
           Node (i) is CA;
         If D =1 then
           node (j) is Np;
          D (i) =1;
         End if.
       Else
         If (Rm (i) > Rm (j)) then
           node (j) remains candidate for CA;
         Else
           If (Rm (i) = Rm (j)) or (DDc (i) < DDc (j)) then
             Run Mobic;
           End if.
         End if.
       End if.
     End if.
  End if.
END.
```

Figure 21 : Algorithme d'élection distribué (AED)

Algorithme distribué exécuté par le nœud si ses CAs ne sont plus disponible :

```
Si le nœud (i) ne reçoit pas de paquet balise de CA après certain temps prédéfini;
BEGIN
  If It can reach CA with another node of confidence then
        To keep CA current;
        To update the node Np and D;
  Else
     If It can find another CA then
          To join new CA;
          If (Sc = = 1) then
             If (D = = 1) then
                Status (i) = Np_Node;
                D (new CA) = 1;
             Else
                Status (i) = Nm;
                D (new CA) = D+1;
             End if.
          Else
             Ask certification a node of confidence;
          End If.
     End If.
  End If.
End.
```

Figure 22 : Algorithme distribué exécuté par le nœud si ses CAs ne sont plus disponible

3.4. La technique de cryptographie à seuil dans notre architecture :

Un réseau Ad hoc mobile peut être représenté par un ensemble de groupe des nœuds. Chaque groupe est représenté par un chef de groupe (leader) et des nœuds passerelles (Np) qui gèrent la communication avec les groupes voisins. Parmi plusieurs solutions de sécurité qui se base sur ce principe, notre architecture doit baser sur le principe de la cryptographie à seuil (thershold cryptography).

L'approche proposée utilise la cryptographie à seuil pour distribuer le rôle de l'autorité de certification. L'idée est de distribuer la clé privée de l'autorité de certification sur les chefs de groupe. Chaque chef de groupe doit posséder un fragment de la clé privée de l'AC. L'association de (k) fragments de clé permet de générer la clé privée de l'AC.

Le nouveau service de gestion de clés ayant la configuration (n, k) consiste à avoir *n* nœuds spéciaux qu'on appelle serveurs, présents dans le réseau Ad hoc et qui partagent la capacité de générer des certificats pour les autres membres du réseau. Chaque serveur a sa propre paire de clés, (publique et privée) et enregistre les clés publiques de tous les nœuds du réseau, en particulier, celles des autres serveurs. Ceci permet aux nœuds serveurs d'établir des liens sécurisés entre eux.

Dans le cas de notre schéma (n, k), les *n* serveurs partagent la capacité de signer les certificats pour les autres nœuds du réseau. La clé privée *k* de tout le service est divisée en *n* secrets partagés $(s_1, s_2,..., s_n)$, un secret étant connu d'un seul serveur. La (Figure 23) illustre cette configuration.

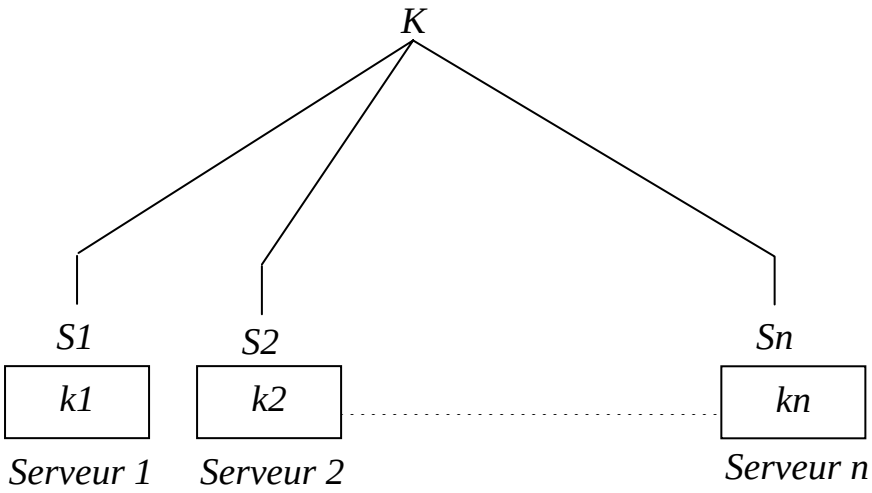


Figure 23 : Configuration du service de gestion de clés

Alors pour certifier un nœud visiteur, ce dernier doit avoir un certain nombre de certificats (W) délivrés par des nœuds qui ont le statut de garant (climat de confiance). Une fois les (W) certificats de garantie rassemblés, le nœud visiteur peut faire sa demande auprès d'au moins (k) chefs de groupe qui possèdent les fragments de la clé privée de l'autorité de certification. Si les (k) certificats sont réunis, alors le certificat du réseau peut être généré.

3.5. 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 [39], dans lequel nous avons implémenté nos algorithmes décrits 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.

Pendant les simulations, nous nous sommes intéressés aux métriques suivantes :

- Le taux d'élections : déclaration d'un nœud comme Cluster-head.
- Le taux de ré-affiliations : changement d'un nœud d'un Cluster à un autre.
- La durée de vie moyenne des Cluster-heads.
- Le nombre moyen de Clusters.

Dans cette simulation, notre modèle d'expérimentation est établi sur 100 nœuds répartis aléatoirement sur une surface carrée de 100 * 100 m² avec une portée de transmission de 250m, présentée par la (Figure 24). Nous avons varié les vitesses des nœuds (de 0.2 à 10 m/s).

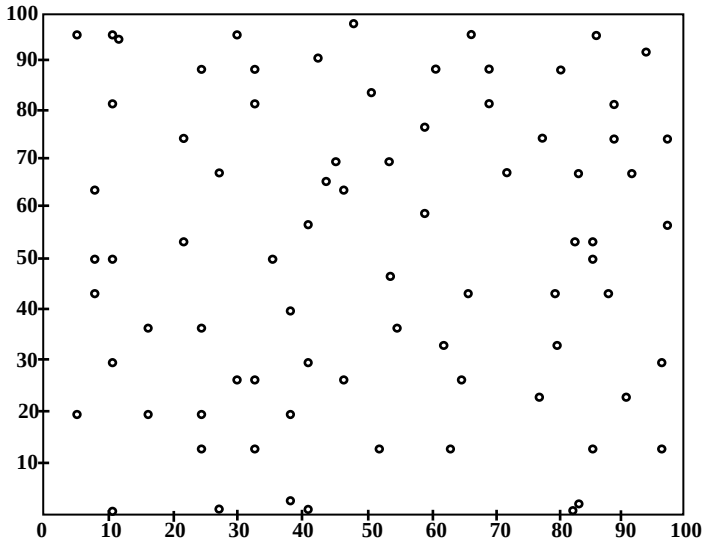


Figure 24 : Modèle d'expérimentation

Nous avons considéré trois valeurs de k (Rayon maximum des Clusters) à savoir 1, 2 et 3. Le temps de pause est de 20s. Les simulations ont une durée de 3000s et des valeurs moyennes sont calculées sur des blocs de 300s (voir Tableau 1).

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.

Tableau 2 : Paramètres de simulation

La (Figure 25) montre la comparaison entre notre algorithme d'élection (AED) et deux autres algorithmes : MOBIC [27] et Lowest-ID [29].

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.

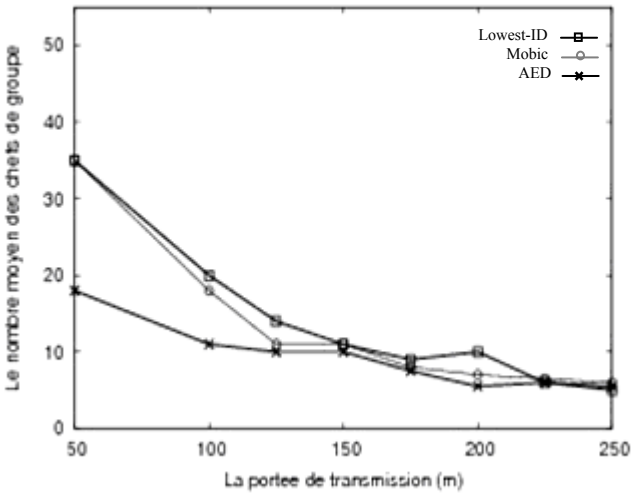


Figure 25 : Comparaison entre notre algorithme (AED), Mobic et Lowest-ID

Les (Figures 26 et 27) représentent respectivement les taux d'élections et des ré-affiliations en fonction de la vitesse. Ces deux taux augmentent en fonction de la vitesse des nœuds. En effet, plus la vitesse est grande, plus la probabilité qu'un nœud se trouve hors de son Cluster suite à un mouvement est grande. En revanche, nous remarquons que pour cette configuration, les ré-affiliations deviennent presque constantes à partir de la vitesse 8 m/s. On remarque aussi que les valeurs de k (1, 2 et 3) influent peu sur les ré-affiliations et les élections ce qui laisse plus de flexibilité à l'utilisateur pour le choix du rayon des Clusters.

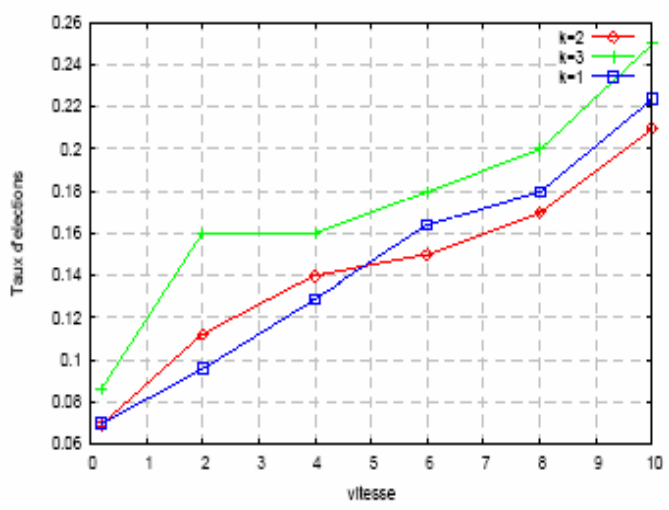


Figure 26 : Taux d'élection des CHs en fonction de la vitesse

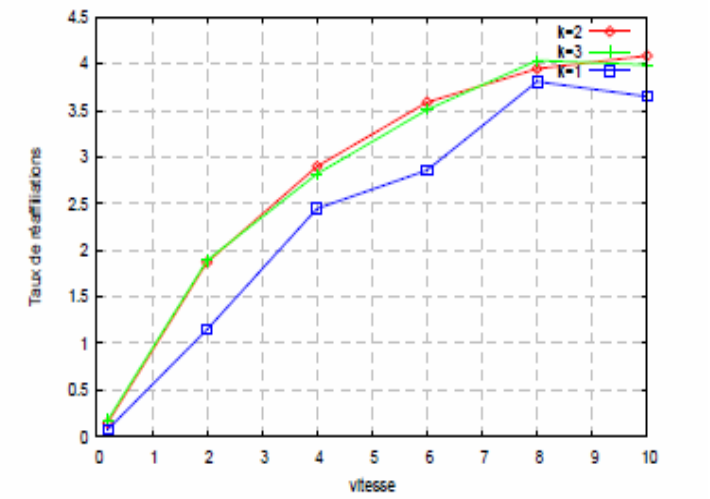


Figure 27 : Taux de ré-affiliations en fonction de la vitesse

Les durées de vie représentées dans la (Figure 28) diminuent en fonction de la mobilité puisque la mobilité des nœuds introduit plus d'instabilité dans le réseau. Toutefois, on remarque que cette diminution n'est pas trop importante surtout pour les valeurs de *k =1* et *k=2*.

La (Figure 29) représente le nombre moyen de Clusters générés. On remarque que ce nombre diminue faiblement en fonction de la vitesse. Ce résultat montre qu'en cas de mobilité, les nœuds sont capables de se réorganiser et de joindre des Clusters déjà existants.

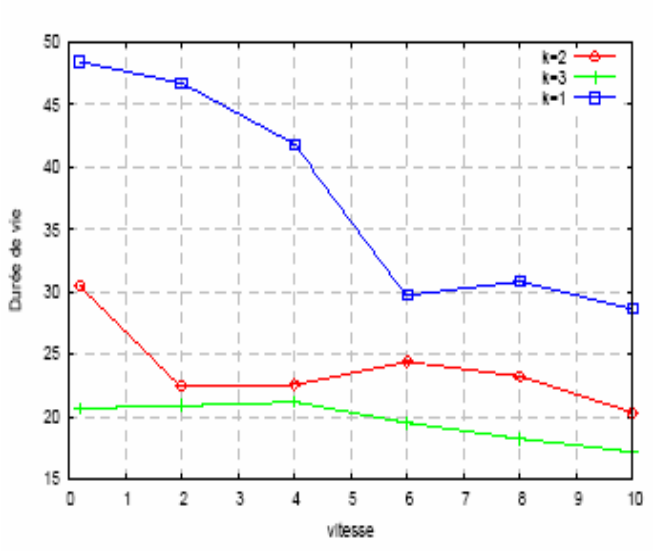


Figure 28 : Durée de vie des CHs en fonction de la vitesse

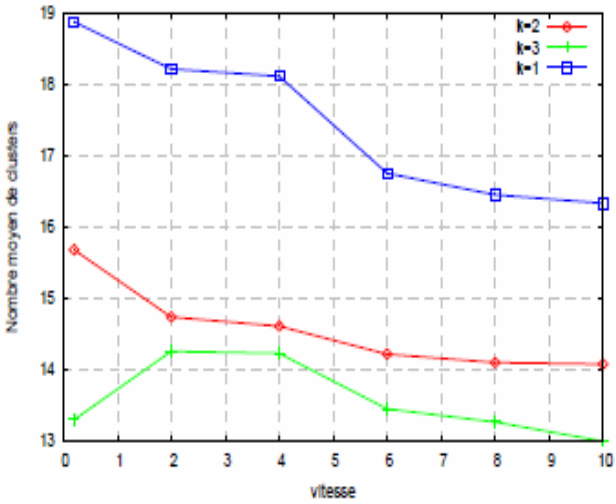


Figure 29 : Nombre moyen de Clusters en fonction de la vitesse

3.6. 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 architecture oblige les nœuds à collaborer et à adopter un bon comportement pour l'obtention d'un niveau de confiance plus élevé. Chaque nœud inconnu doit commencer avec le statut visiteur dont le niveau de confiance est le plus bas. Avec ce procédé on est sûr qu'aucun attaquant ne pourra se procurer le statut d'un partenaire légitime, et si un attaquant tente de compromettre tout le réseau, il doit compromettre avant tout les CAs de chaque Cluster.

- 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.

4. Conclusion :

La confiance avant d'être un problème technique, est avant tout un problème social. En effet, les mécanismes techniques doivent être au service de la politique de sécurité imposé par l'usage et non le contraire. Une politique trop restrictive n'offrira que très peu de possibilités d'interaction et donc rendra le système inopérant. Il en est de même pour une politique très permissive qui n'engendra aucune confiance entre les utilisateurs.

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.

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.

Conclusion générale :

Les réseaux sans fil et la sécurité sont vus comme un oxymoron par beaucoup d'utilisateurs. En effet il est difficile de croire à une sécurité lorsqu'on a une accessibilité aussi évidente à un support sans fil. Cependant, la communauté de recherche académique et industrielle développe des mécanismes et des protocoles de sécurité pour pérenniser ce mariage entre les réseaux sans fil/mobiles et la sécurité.

Les réseaux sans fil Ad hoc sont annoncent les réseaux de communication du futur où la mobilité en est l'idée maîtresse. Leur succès dépendra sans aucun doute de leur capacité à 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 l'intrusion par rapport à autres types de réseau et nécessitent de chiffrer les communications pour parer aux écoutes et de vérifier en permanence l'identité du mobile. Les mécanismes de sécurité traditionnels ne répondent pas aux exigences de tels réseaux. Il s'agit donc de concevoir de nouveaux mécanismes afin de garantir la sécurité de ces réseaux.

Dans ce mémoire, notre contribution consiste à définir et proposer une architecture de sécurité adaptée aux réseaux sans fil Ad hoc, les mécanismes de sécurité sont renforcés par un modèle de confiance hybride, distribué et coopératif basé sur le principe de la cryptographie à seuil. Ce modèle combine à la fois les éléments classiques de la sécurité et de nouveaux éléments que nous suggérons, et qui sont nourris par les interactions de l'entité (nœud) avec son environnement.

Au cours de ce travail, nous avons présenté les bases de la sécurité et de passer en revue les différentes technologies actuelles pour les réseaux Ad hoc en mettant l'accent sur les vulnérabilités, et les solutions de sécurité correspondantes, à savoir :

- Les architectures de gestion de clés.
- Protections utilisant la cryptographie asymétrique.
- Protections utilisant la cryptographie symétrique.
- Protections contre la modification des données.
- Protection contre les attaques de type "tunnel".
- Mécanismes basés sur la réputation.
- Systèmes de détection d'intrusion.

A travers de ces investigations, nous avons vu que chaque technologie pose ses propres challenges à la conception des solutions de sécurité, mais aucune de ces méthodes ne prétend toute exhaustivité, résoudre complètement le problème de sécurité dans les réseaux Ad hoc, chacune possède ses avantages, et ses inconvénients et chacune s'adapte mieux à un type particulier.

Dans les réseaux Ad hoc, assurer un routage fiable et sécurisé et maintenir un niveau de confiance entre les nœuds, sont essentiels, il s'agit de protéger ses ressources (batterie, disque, etc.) contre leur utilisation frauduleuse et d'assurer la confidentialité de ces données.

Toute la difficulté réside dans la conception des solutions de sécurité qui pourraient répondre à ces challenges est non seulement d'assurer la robustesse face à des attaques potentielles, de veiller à ne pas ralentir les communications, mais aussi d'optimiser l'utilisation des ressources en termes de bande passante, de mémoire, de batterie. Plus important dans ce contexte ouvert, est de garantir l'anonymat et le secret de la vie privée, tout en permettant la traçabilité pour des raisons légales. En effet, le besoin croissant de traçabilité est aujourd'hui nécessaire pour la lutte contre les organisations de malfaiteurs et de terroristes, mais aussi pour minimiser le pillage des droits d'auteurs. On se retrouve donc face à un dilemme, celui de fournir un cadre de liberté d'expression tout en contrôlant le contenu des échanges. Tous ces éléments influent dans le choix et la mise en place des outils de sécurité qui sont guidés par une évaluation du risque préalable et la politique de sécurité.

Pour cela, et à l'issus de ce travail nous avons définir et proposer une architecture de sécurité adaptée au ce type de tels réseaux, l'architecture proposée n'a pas la prétention de correspondre à toutes les situations d'usage de tels environnements et pose encore plus de questions qu'il n'apporte de réponse. En effet, il aborde non pas un problème spécifique de la sécurisation de ces réseaux, mais propose une architecture globale de sécurité, dynamique et auto adaptable, permettant de gérer la mise en relation d'objets communicants.

Enfin, pour les perspectives de ce travail, nous envisageons d'analyser notre architecture dans différents modèles de mobilité et aussi évaluer la résistance de notre modèle de confiance face aux différents types d'attaques.

Politique de sécurité

«....Un de mes amis vient de changer de travail. Sa nouvelle entreprise est plutôt en avance en matière de sécurité. On lui a remis une carte à puce multifonctions qui intègre son empreinte digitale. Ici, authentification forte et PKI sont à l'ordre du jour. Mais surtout, on lui a donné un fascicule expliquant la politique de sécurité. Le RSSI (Responsable de la Sécurité des Systèmes d'Information) n'a pas pour autant brider l'usage de l'ordinateur et de la messagerie. Il semble qu'un dialogue existe entre le service informatique et le salarié. Le premier ne voit pas le second comme un «abruti qui ne comprend rien » et, a posteriori, l'utilisateur n'a pas le sentiment d'entendre des propos abscons... La sécurité est une chaîne où tous les acteurs, à des degrés divers, sont impliqués. Comme toutes chaîne, sont point de rupture est lié au maillon le plus faible. Récemment, mon ami a appelé un collègue de son ancienne société qui, elle, a mis en place une politique de sécurité très rigide, et mal acceptée. Une partie des salariés ont apporté leur propre modem pour se connecter à Internet sur un compte personnel. Une semaine plus tard, plusieurs d'entre eux était piratés…..

Extrait de la revue 01-Réseau (Avril 2002)

Annexe 1 : Glossaire

Glossaire

- ***Administrateur*** **:** L'administrateur est la personne qui contrôle un système. Il est responsable d'un fonctionnement permanent et sans incident. Il installe des utilisateurs, attribue des autorisations, s'occupe de l'installation de nouveaux logiciels et effectue la maintenance de l'ensemble du système.

- ***Adresse IP*** **:** Numéro d'identification d'une machine sur Internet et sur les réseaux locaux. Elle se compose de quatre nombres, par exemple 156.125.55.22. Les adresses IP ne sont généralement utilisées que par les ordinateurs et les programmes. Pour les humains, il est plus facile de retenir les noms de hôte (ou nom de machine dans un domaine) qui peuvent être convertis en adresses IP par les DNS (*Domain Name Service*).

- ***Audit*** **:** L'audit est un contrôle de la sécurité d'un système, c'est-à-dire du bon fonctionnement des mesures de sécurité. Il permet d'analyser l'état du système en ce qui concerne sa sécurité et de découvrir d'éventuels points faibles. Sur des systèmes sensibles exposés aux attaques et intrusions, les audits devraient être effectués régulièrement, indépendamment des autres mesures de sécurité.

- ***Authentification*** **:** Au début de chaque communication confidentielle, les correspondants doivent identifier leur interlocuteur et vérifier qu'il s'agit bien de la personne supposée. Lorsqu'un utilisateur se connecte à un service, l'authentification se fait généralement au moyen d'un nom utilisateur et d'un mot de passe. Lorsque des machines communiquent entre elles, elles échangent et vérifient des signatures.

- ***Biométrie*** **:** Utilisation du corps humain pour protéger un système, à l'aide des empreintes digitales, la rétine, etc.

- ***Certificat*** **:** Attestation électronique grâce à laquelle un utilisateur ou un ordinateur peut prouver son identité.

- ***Clé*** **:** Séquence de symboles permettant de crypter ou décrypter des messages.

- ***Cookies*** **:** Sont de petits paquets de données que les serveurs web déposent sur les ordinateurs de leurs visiteurs pour l'identifier la prochaine fois lorsqu'il revient sur le site. Leur inconvénient est qu'ils permettent de reconstituer et d'espionner le parcours d'un

utilisateur sur Internet. La plupart des navigateurs web permettent de limiter ou d'interdire complètement la réception des cookies.

- ***Crack*** **:** Une technique permettant de déjouer des mesures de sécurité, par exemple en contournant une demande de mot de passe, en devinant des mots de passe ou en forçant des cryptages.

- ***DoS (Denial of Service)*** **:** Technique d'attaque qui consiste à rendre inopérant un système. Il peut être réalisé à l'aide d'une multitude de requêtes, par saturation de la bande passante, destruction de programmes, etc.

- ***Failles de sécurité*** **:** Point faible dans la sécurité d'un système, qui permet soit à des personnes non autorisées d'accéder au système soit à autoriser des fonctions qui devraient être normalement interdites. Elles sont dues à des erreurs de programmes ou de construction, ou encore à des défauts de configuration.

- ***Fonction de hachage*** **:** Fonction qui permet de créer, à partir d'un message de longueur quelconque, une valeur de longueur réduite (quelques octets) que l'on appelle le condensât. Ce type de fonction cryptographique est conçu pour avoir un certain nombre de propriétés qui autorisent l'utilisation du condensât comme une image infalsifiable du message initial.

- ***Hôte (ou serveur ou en anglais Host)*** **:** C'est un ordinateur distant qui reçoit les appels d'autres machines (connexion sur un site web par exemple) et qui met des informations (Informations, images, logiciels...) à la disposition des autres ordinateurs au sein d'un réseau. Sur Internet on trouve : serveur web, serveur FTP, serveur de messagerie, serveur IRC, etc. (voir serveur d'e-mail ou de messagerie plus loin).

- ***IDS (Intrusion Detection System)*** **:** Système de détection en temps réel des tentatives d'intrusion sur un réseau ou un poste.

- ***Internet*** **:** Réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés, qui sont reliés par le protocole de communication TCP/IP et qui coopèrent dans le but d'offrir une interface unique. Internet est divisé par ailleurs en plusieurs sous ensembles, utilisant des protocoles de communication différents : le World Wide Web (ou Web) qui regroupe les sites à consulter, la messagerie électronique (ou e- mail) et les forums de discussion (news-groups).

- ***Intranet*** **:** Réseau local et privé qui utilise les technologies d'Internet (web, e-mail, etc.) mais qui ne s'ouvre pas aux connexions publiques.

- ***Navigateur (ou logiciel de navigation Browser)*** **:** Logiciel permettant d'avoir accès aux sites Internet et de visualiser les pages HTML et de se promener de site Web en site Web au moyen des liens hypertextes. Parmi les navigateurs les plus répandus on trouve NCSA Mosaic, Netscape Navigator ou Microsoft Internet Explorer. Ils permettent aussi d'écrire des messages électroniques et d'accéder à des forums de discussion.

- ***PKI (Public Key Infrastructure)*** **:** Système de certificats numériques utilisés pour vérifier et authentifier les parties impliquées dans une transaction électronique.

- ***Port*** **:** Lors d'une connexion à un ordinateur hôte, il est nécessaire de spécifier son adresse mais aussi son numéro de port qui indique le type de communication utilisé. Celui d'une communication en HTTP est 80. Les ports sur une machine sont des entrées qui permettent d'échanger des informations dans un sens ou dans un autre avec une autre machine. Chaque port a ses caractéristiques, l'un permet de lire le courrier, l'autre permet de communiquer par ICQ, un autre permet de télécharger des fichiers... Il existe plusieurs centaines de ports différents sur une machine. C'est donc par eux qu'un hacker va pouvoir s'introduire sur un PC. A titre d'exemple, le port 21 est celui du FTP, le port 23 est aussi assez connu puisque c'est celui du telnet et l'entrée favorite de la majorité des troyens (d'où le nom socket 23), le port 25 appelé SMTP permet d'envoyer le courrier et le port 110 (POP) permet de relever celui-ci.

- ***Protocole*** **:** Convention précisant un ensemble de règles et de spécifications techniques à respecter dans le domaine des télécommunications. Un protocole est le langage utilisé par les ordinateurs pour communiquer entre eux. Le mot protocole désigne en général les messages échangés entre deux machines. L'intérêt d'un protocole est de définir des méthodes d'échange d'information, indépendantes des matériels. Ainsi une fois le protocole défini, chaque terminal, ou client ou serveur implémente ce protocole sans se soucier des autres ordinateurs.

- ***Routeur*** **:** Outil logiciel ou matériel pour diriger les données à travers un réseau. C'est une unité qui permet de connecter deux réseaux au niveau 3 (réseau).

- ***Serveur de mail*** : Serveur spécialisé dans la gestion du courrier électronique. Il abrite les "boîtes aux lettres" des internautes contenant leurs messages. Le serveur de mail d'un internaute est souvent géré par son fournisseur d'accès.

- ***Serveur de news*** **:** Ordinateur qui héberge et distribue les newsgroups (forums). Reliés entre eux au moyen du protocole NNTP (Net News Transfer Protocol), les serveurs de news

expédient entre eux les nouvelles contributions qui leur parviennent, afin que celles- ci soient visibles de tous, sur tous les serveurs.

- ***Serveur proxy*** **:** Assure le stockage des pages Web les plus consultées.

TCP/IP : ensemble de protocoles dont IP et TCP. JP est chargé de faire en sorte que les paquets de données arrivent à la destination prévue. En collaboration avec TCP, il assure la décomposition, le transfert et la recomposition des données. Fl utilise pour cela des noms IP ou numéros 1F qui identifient clairement l'expéditeur et le destinataire.

- ***www (World Wide Web ou tout simplement le web)*** **:** C'est la partie la plus connue d'Internet. Elle désigne tous les serveurs web et les informations qu'ils proposent. Ces serveurs d'informations sont consultables au moyen de pages reliées entre elles par des liens hypertextes. Ces pages, appelées pages Web, se composent de textes d'images, de sons, de séquences vidéos, etc. On les consulte par le biais d'un logiciel de navigation.

- ***Passerelle (ou gateway)*** **:** C'est un point de passage entre deux protocoles. Il existe ainsi des passerelles entre Internet et les services en ligne comme AOL pour permettre aux membres d'AOL d'utiliser des services Internet et d'être joignable par e-mail.

Annexe 2 : Nos simulations sur NS-2

1. Introduction :

La simulation permet de tester à moindre coût les nouveaux protocoles et d'anticiper les problèmes qui pourront se poser dans le futur afin d'implémenter la technologie la mieux adaptée aux besoins. NS [39] est un simulateur à événements discrets disponible gratuitement sur le site http://www.isi.edu/nsnam/. Il permet à l'utilisateur de définir un réseau et de simuler des communications entre les nœuds de ce réseau. NS utilise le langage OTCL (Object Tools Command Language), dérivé objet de TCL. À travers ce langage, l'utilisateur décrit les conditions de la simulation : topologie du réseau, caractéristiques des liens physiques, protocoles utilisés, communications, etc. La simulation doit d'abord être saisie sous forme de fichier texte que NS utilise pour produire un fichier trace contenant les résultats. NS est fourni avec différents utilitaires dont des générateurs aléatoires et un programme de visualisation (NAM).

Dans ce présent annexe, nous allons présenter le simulateur NS-2, que nous allons utiliser pour évaluer les performances de l'algorithme qu'on à présenter dans le chapitre 4. Nous allons, tout d'abord, éclaircir certaines fonctionnalités du simulateur NS-2. Tel que la prise en charge des réseaux (sans fil et câblés), et son adaptation aux réseaux mobiles Ad hoc, ainsi que la simulation proprement dite. Celle-ci comprend plusieurs phases : implémentation, scénario de simulation, et autres mesures tel que la connectivité, la charge et la mobilité.

2. Choix du langage et de l'environnement d'implémentation :

Nous avons choisi comme langage d'implémentation pour notre algorithme AED le langage TCL. Ce dernier est connu comme étant un langage de commandes interprété et extensif. En effet, les programmes écrits en TCL sont des fichiers texte constitués de commandes TCL qui sont traités via un interpréteur TCL au moment de l'exécution. L'avantage d'implémenter notre algorithme en TCL est de pouvoir facilement l'interpréter avec l'interpréteur TCL intégré dans le simulateur NS2, ce qui nous permet de simuler son fonctionnement afin d'évaluer ses performances.

Nous avons choisi comme plate-forme d'implémentation, le simulateur NS-2 [39] version NS-2.30, sous le système d'exploitation LUNIX MANDRIVA 2007. Ce choix est basé sur le fait que NS-2 est le leader en terme d'extensibilité puisque on peut facilement ajouter nos propres protocoles, que ce soit au niveau de la couche Réseau, Mac, application, etc. De plus, NS-2 est bâti selon les idées de conception par objets, de réutilisation du code et de modularité. Du point de vue utilisateur, la mise en oeuvre de ce simulateur se fait via une

étape de programmation qui décrit la topologie du réseau et le comportement de ses composant.

Ensuite, vient l'étape de simulation proprement dite et enfin l'interprétation des résultats. La description de la topologie du réseau peut être facilement effectuée en utilisant des primitives de base comme par exemple Nodes, Links, Agents, et Applications, où la primitive Nodes représente un nœud dans le réseau, la primitive Links représente le support de communication, la primitive Agents est utilisée pour implémenter différents protocoles réseaux, et la primitive Applications est chargée de la génération des données ainsi que la réalisation de plusieurs tâches spécifiques.

La méthode de simulation à suivre est montrée dans la Figure suivante :

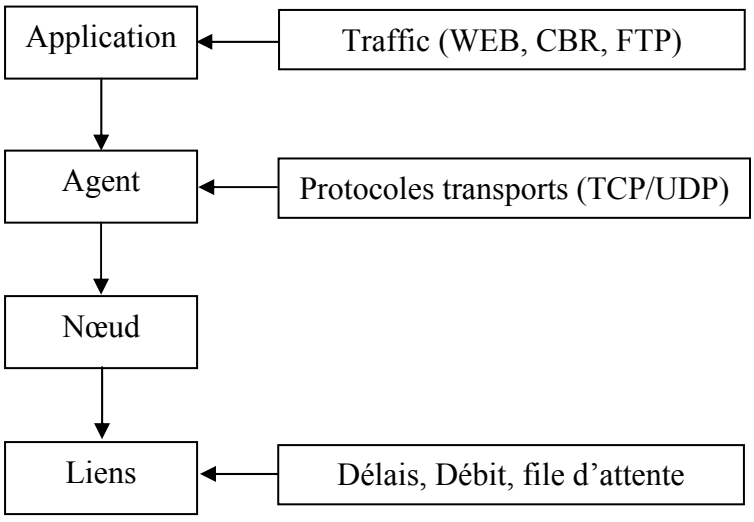


Figure 30 : La méthode de simulation NS-2

3. Etapes d'implémentation de l'AED :

L'implémentation de notre Algorithme passe par plusieurs étapes à savoir :

3.1. Préparation de l'environnement d'implémentation :

La préparation de l'environnement d'implémentation consiste à installer le simulateur de réseau NS-2 sous le système d'exploitation LUNIX MANDRIVA 2007. On a choisi la version NS-2.30 puisqu'elle prend en considération la topologie des réseaux sans fil Ad hoc. L'installation de NS-2.30 sous LUNIX MANDRIVA 2007 s'effectue suivant 4 étapes qui se résument en :

- Copier le package d'installation NS-2.30 dans le répertoire USER du système.

- Taper la commande d'installation "./Install " dans le terminal de commandes, dans le répertoire NS-2.30 précédemment copié.
- Modifier les variables d'environnement et cela consiste à ajouter les lignes de code à suivre dans le fichier ".bashrc".

```
export
PATH=${PATH}:/home/user/ns-allinone-2.30/bin:/home/user/
ns-allinone-2.30/tcl8.4.13/unix:/home/user/ns-allinone-
2.30/tk8.4.13/unix:/home/user/ns-allinone-2.30/nam-1.12
export
LD_LIBRARY_PATH=/home/user/ns-allinone-2.30/otcl-1.12,
/user/ns-allinone-2.30/lib
export
TCL_LIBRARY=/user/ns-allinone-2.30/tcl8.4.13/library
```

- Enfin taper la commande "./make" dans le terminal de commandes afin de compiler NS-2 et de générer tous les fichiers NS-2 nécessaires à son fonctionnement.

3.2. Implémentation de notre algorithme :

Après avoir préparé notre environnement d'implémentation, on entame l'étape d'intégrer le code de notre algorithme d'élection distribué (AED) sous NS-2, afin qu'il corresponde à l'architecture proposée. Pour cela, on va insérer notre programme d'élection dans la procédure de formation des groupes (Clusters) (Figure 31).

```
ELECTION/Clusters instproc chaine {tdma chid} {

#declaration des variables
Nodes ns_ opt tabdist tabchaine nodech nodechaine
$self instvar nbr_node farnode nearnode r cord dn dch
$self instvar i j r cord
$self instvar CA Np r cord
set tdma [sup $tdma $chid] #définir les nœuds appartenant au cluster
```

```
set nbr_node [llength $tdma]#définir le nombre de nœuds appartenant au cluster
set nodechaine ""
set cord $tabdist($chid)
set Sc [lindex $cord 1]
set Vr [lindex $cord 1]
set K= {1, 2, 3}#entamer la boucle de construction de chaîne
#quand le nœud (j) reçoit un paquet balise de nœud (i)
if {$nbr_node > 0} {
set farnode [$self far_node $chid $tdma ]#recherche du nœud le plus loin du i
set tdma [sup $tdma $farnode]
set nodechaine "$farnode" # initialiser la chaîne avec le nœud le plus loin
set nearnode [$self near_node $farnode $tdma $chid ]
#obtenir les cordonnées x,y du i
Set D [lindex $cord 1]
Set DDc [lindex $cord 1]
Set Rm [lindex $cord 1]
if {Sc<>1}  {
   puts "reject ()"
     } else {
if {D>k} {
   puts " Not valid election"   #recherche du nœud le plus proche de la tête de chaîne de nœuds
     } else {
if {Rm(i)<= (Rm(j)} and {DDc(i)>DDc(j)} {
       Node (i) is CA#obtenir les cordonnées x,y du nœud le plus loin du CA (la taille de cluster)
if {D = 1} {
       Node (i) is Np
       D(i) = 1 #obtenir les cordonnées x,y du nœud avec un seuil de confiance élevé
     } else {
if {Rm(i)>Rm(j)} {
       Node(j) remains candidate for CA
   } else {  #calculer la distance entre K et le CA
if {Rm(i)= Rm(j)} or {DDc(i)< DDc(j)} {
    Run Mobic
       }
set cord $tabdist($chid)
set XCA [lindex $cord 0]
set YCA [lindex $cord 1]
set cord $tabdist($farnode)
set X1 [lindex $cord 0]
set Y1 [lindex $cord 1]
set cord $tabdist($nearnode)
set X2 [lindex $cord 0]
set Y2 [lindex $cord 1]
set dch [dist $X1 $Y1 $XCA $YCA]
set dn [dist $X1 $Y1 $X2 $Y2]
set info "$nearnode 0 $dch $dn"
set tabchaine($farnode) $info
set r [$self remptab $info $farnode]
set nodech $nearnode
set tdma [sup $tdma $nearnode]
set nodechaine [linsert $nodechaine end $nearnode]
set i = 1
while {[llength $tdma] != 0} {
set nearnode [$self near_node $nodech $tdma $chid ]
#obtenir les cordonnées x,y du CA
set cord $tabdist($chid)
set XCA [lindex $cord 0]
set YCA [lindex $cord 1]
#obtenir les cordonnées x.v de la tête de la chaîne
```

```
set cord $tabdist($nodech)
set X1 [lindex $cord 0]
set Y1 [lindex $cord 1]
#obtenir les cordonnées x,y du nœud le plus proche de la tête de la chaîne CA
set cord $tabdist($nearnode)
set X2 [lindex $cord 0]
set Y2 [lindex $cord 1]

set tabchaine($nodech) $info
set r [$self remptab $info $nodech]
set tdma [sup $tdma $nearnode]
set nodechaine [linsert $nodechaine end $nearnode]
set nodech $nearnode
incr i 1
}
set cord $tabdist($chid)
set XCH [lindex $cord 0]
set YCH [lindex $cord 1]
set cord $tabdist($nodech)
set X1 [lindex $cord 0]
set Y1 [lindex $cord 1]
set dch [dist $X1 $Y1 $XCH $YCH]
set info "$chid $i $dch $dch"
set tabchaine($nodech) $info
set r [$self remptab $info $nodech]
set indice [lsearch $nodechaine $chid]
if {$indice == -1} {
set nodechaine [linsert $nodechaine end $chid]
} else {
set nodechaine [sup $nodechaine $chid]
}
} else {
puts "tdma vide."
}
set nodechaine [sup $nodechaine $chid]
}
```

Figure 31 : Code d'implémentation du programme de formation des Clusters

4. Conclusion :

L'implémentation de notre algorithme sous le simulateur de réseau NS-2 nous permettra d'évaluer les performances de notre algorithme d'élection en terme de formation de Clusters pour tester la mise en place d'une nouvelle architecture.

Cette mise en place nous permettra aussi de pouvoir apporter notre empreinte au niveau d'une meilleure gestion de sécurité dans les réseaux sans fil Ad hoc.

Bibliographie :

[Numéro de référence]. Auteur, "Titre", *Maison d'édition*, Ville d'édition, Nombre de pages, Année

[1]. G. Chelius and E. Fleury, "Ananas : A new Ad hoc network architectural scheme", *INRIA Research,* Report 4354, 2002.

[2]. V. Legrand et S. Ubéda "Vers un modèle de confiance pour les objets communicants : une approche sociale", *Centre d'Innovations en Télécommunications & Intégration de services CITI INRIA ARES*, INSA de Lyon, mars 2004.

[3]. A. Larab, "De la sécurité dans les réseaux"**,** *Thèse DEA informatique Université de François Rabelais*, Tours-France, 84. 2001.

[4]. C. Liorens et L. Levier, "Tableaux de bord de la sécurité réseau"**,** *Eyrolles*, Paris-France, 340. 2003.

[5]. V. Legrand, D. Hooshmand, and S. Ubéda, "Trusted ambient community for self-securing hybrid networks", *INRIA*, Research Report 5027, 2003.

[6]. V. Legrand, F. Nait-Abdesselem, et S. Ubéda, "Etablissement de la confiance et réseaux Ad hoc : un état de l'art", *dans 2ème rencontre francophone sur Sécurité et Architecture Réseaux*, Nancy France, 2003.

[7]. H. Chaouchi, M. Laurent-Maknavicius, "La sécurité dans les réseaux sans fil et mobiles, volume 1, 2, 3", *Lavoisier*, Paris-France, 239, 2007.

[8]. W. Gieseke, "Le guide Anti-Hacker", *Micro Application*, 245, 2001.

[9]. J. Stang et S. Moon, "Sécurité réseaux", *Dunod*, Paris-France, 652, 1996.

[10]. V. Legrand, "Etablissement de la Confiance et Réseaux Ad Hoc, Le Germe de Confiance", *Rapport de DEA*, EDIIS, Laboratoire CITI, INRIA ARES, Juillet 2003.

[11]. S. Sivavakeesar, G. Pavlou, C. Bohoris and A. Liotta, "Effective Management through Prediction-Based-Clustering Approach in the Next-Generation Ad hoc Networks", *in the Proceeding of the IEEE international Conference on Communications (ICC'04)*, France, Juin 2004.

[12]. J.A. Freebersyser, B. Leiner, "A DoD perspective on mobile Ad hoc networks", *Ad Hoc Networking,* Addison Wesley, pp. 29-51, 2001.

[13]. P. Barthélemy, R. Rolland et P. Véron, "Cryptographie principes et mises en ouvre"**,** *Lavoisier*, paris-France, 414, 2005.

[14]. J. Hallberg, A. Hunstad and M. Peterson, "A framework for system security Assessment", *Proceeding of the 2005 IEEE Workshop on information Assurance*, West Point, New-York, 15-17 Juin 2005.

[15]. Académie Française, "Dictionnaire de la langue française", 8ème édition, 1932-1935.

[16]. Bruce.Schneier, "Cryptographie Appliquée", *Vuibert Informatique*, Paris-France, 846. 1997

[17]. A. Amis, R. Prakash, T.Vuong, D. Huong, "Max-Min D-cluster formation in wireless Ad hoc networks", *in Proceeding of IEEE Infocom,* Tel Aviv, Mars 2000.

[18]. G. Chen, F. Nocetti, J.S. Gonzalez, and T. Stojmenovic, "Connectivity-based K_hop clustering in wireless networks", *in Proceeding of the 35th Hawaii international Conference on System Sciences (HTCSS-35)*, Janvier 2002.

[19]. M. Chatterjee, K. Das and D. Turgut, "WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks", Journal of Cluster Computing, No.5, 2002.

[20]. J. Westcott and G. Lauer, "Hierarchical routing for very large networks", *Proceeding of the IEEE MILCOM 1984*, pp. 214-218, 21-24 Octobre 1984.

[21]. Organisation Mondiale De La propriété Intellectuelle (OMPI), Convention de Berne pour la protection des ouvres littéraires et artistiques, 9 septembre 1886. http://www.wipo.int/treaties/fr/ip/berne/trtdocs_wo001.html (consulté avril 2007).

[22]. W. Fifer, F. Bruno, "The low-cost packet radio", *Proceeding of the IEEE 75 (1)*, pp. 33-42, 1987.

[23]. A. Siddiqui, R. Prakash, "Effect of availability factor threshold and clustering gap on performance of clustering mechanisms for multi-cluster mobile Ad hoc networks", *IEEE international Conference on Communications*, ICC 2002.

[24]. S. Corson, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", *RFC 2501*.

[25]. B. Leiner, R. Ruth and A.R. Sastry, "Goals and challenges of the DARPA GloMo program", *IEEE Personal Communications*, pp. 34-43, 1996.

[26]. F. Theoleyre, "Une auto-organisation et ses applications pour les réseaux Ad hoc et hybrides", *Thèse de doctorat, Institut national des sciences appliquées de Lyon-France*, Septembre 2006.

[27]. 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.

[28]. S. Basagni, “Distributed and mobility-adaptive clustering for multimedia support in multi-hop wireless networks”, *Proceeding of IEEE VTS 50th Vehicular Technology Conference.* 1999.

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

[30]. E. Althouse, “Extending the Littoral Battlespace (ELB), Advanced Concept Technology Demonstration (ACTD)”, *NATO Information Systems Technology Panel Symposium on Tactical Mobile Communications*, Juin 1999.

[31]. S. Corson and J. Macker, “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”, *Request for Comments 2501*, IETF, Janvier 1999.

[32]. V. Karpijoki. “Security in Ad Hoc Networks”, *Seminar on network security, In Proceedings of the Helsinki University of Technology*, 2000.

[33] J. Lundberg, “Routing Security in Ad Hoc Networks”,
http: //www.citeseer.nj.nec.com/400961.html.

[34]. S. Chen and K. Nahrstedt, “A distributed quality-of-service routing in ad-hoc networks”, *IEEE Journal on Selected Areas in Communications*, 17(8), August 1999.

[35]. C. Chaudet and I. Guérin Lassous, “Bruit: Bandwidth reservation under interferences influence”. *In European Wireless 2002 (EW 2002)*, pages pp. 466–472, Florence, Italy, Février 2002.

[36]. F. Stajano, “Security for Ubiquitous Computing”, http: //www.lce.eng.cam.ac.uk, 2002.

[37]. F. Stajano and R. Anderson, “The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks”, *7th International Workshop on Security Protocols*, pp. 172-194, 1999.

[38]. Z. Haas, M. Pearlman and P. Samar, “The Zone Routing Protocol (ZRP) for Ad Hoc Networks”, http: //www.draft-ietf-manet-zone-zrp-02.txt, Juillet 2002.

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

[40]. V. D. Park and M. Scott Corson, “A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks”, *In INFOCOM (3)*, pages 1405–1413, 1997.

[41]. G. Montenegro, C. Castelluccia, “Statistically unique and cryptographically verifiable identifiers and addresses”, *Proceedings ISOC Symposium on network and Distributed System Security (NDSS 2002)*, San Diego, Février 2002.

[42]. T.J Kwon and M. Gerla, “Efficient flooding with passive clustering in Ad hoc networks”, *ACM SIGCOMM computer Communication Review*, Janvier 2002.

[43]. R. Dube, C. Rais, K. Wang, and S. Tripathi, “Signal stability based adaptive routing (SSA) for Ad hoc mobile networks. In Signal stability based adaptive routing (SSA) for Ad hoc mobile networks”, *IEEE Personal Communication*, Février 1997.

[44]. S. Ghiasi, A. Srivastava, X. Yang and M. Sarrafzadeh, “Optimal Energy Aware Clustering in Sensor Networks”, *Sensors Magazine*, 2002.

[45]. P. Papadimitratos, Z.J. Haas, “Secure Routing For Mobile Ad Hoc Networks”, *SCS Communication Networks and Distributed Systems Modelling and Simulation Conference (CNDS 2002)*, San Antonio, Etats-Unis, 27-31 Janvier 2002.

[46] S. Giordano, I. Stojmenovic and L. Blazevie, “Position based routing algorithms for Ad hoc networks: a taxonomy”, Juillet 2001. http://www.site.uottawa.ca/-ivan/routing-survey.pdf.

[47] I. Kang and R. Poovendran, “On Lifetime Extension and Route Stabilization of Energy-Efficient Broadcast Routing over MANET”, *In Proceedings of INC 2002*, Plymouth, 2002.

[48]. M. Guerrero Zapata, N. Asokan, “Securing Ad hoc Routing Protocols”, *Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002)*, pp. 1-10, September 2002.

[49]. T. Clausen and P. Jacquet, “Optimized Link State Routing Protocol (OLSR): Request for Comments”, 3626, Octobre 2003.

[50] D. Camara and A.F. Loureiro, “A novel Routing Algorithm for Ad hoc networks”, *In Proc. HICSS*, Hawaii, 2000.

[51]. C. Lin and M. Gerla, “Adaptive Clustering for Mobile Wireless Networks”, *IEEE Journal on Selected Areas in Communications*, Vol.15, No.7, Septembre 1997.

[52]. S. Yi, P. Naldurg, R. Kravets, “A Securing-Aware Ad hoc Routing Protocol for Wireless Networks”, *6th World Multi-Conference on Systemics, Cybernetics and Informatics (SCI 2002)*, 2002.

[53]. C. Chiang, H. Wu, W. Liu, and M. Gerla. “Routing in Clustered Multihop, Mobile Wireless Networks”, *In Mobile Wireless Networks, the IEEE Singapore International Conference on Networks*, 1997.

[54]. Y.C. HU, A. Perrig, D.B. Johnson, “Packet Leashes: A Defence against Wormhole Attacks in Wireless Networks”, *INFOCOM 2003*, 2003.

[55]. R. Ogier, F. Templin and M. Lewis, “Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)”, *IETF RFC 3684*.

[56]. P. Michiardi, R. Molva, “Core: A Collaborative Reputation Mechanism to Enforce node Cooperation in Mobile Ad hoc networks”, *in Communication and Multimedia Security 2002 Conference*, 2002.

[57]. D. Johnson, D.A. Maltz, Y. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", Internet Draft: http: //www.draft-ietf-manetdsr-10.txt, 19 Juillet 2004.

[58]. 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.

[59]. 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.

[60]. A. Perrig, R. Canetti, J.D. Tygar and D. Song, "Efficient Authentication and Signing Multicasts Streams over Lossy Channels", *In IEEE Symposium on Security and Privacy*, pp. 56-73, 2000.

[61]. L. Zhou, Z. Haas, "Securing Ad hoc networks", *IEEE Network Magazine*, 13 Novembre 1999.

[62]. E. Royer and C. Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", *In IEEE Personal Communications*, Avril 1999.

[63]. R. Housley, W. Ford, W. Polk and D. Solo, "Internet X.509 Public Key Infrastructure: Certificate and CRL, Profile", *RFC 2459*, 1999.

[64]. J-B. Hubaux, L. Buttyan, V. Capkun, "The quest for securing in mobile Ad hoc networks", *in 2nd ACM Symposium on mobile Ad hoc Networking and Computing*, Octobre 2001.

[65] C-K Toh, "A Novel Distributed Routing Protocol to Support Ad-Hoc Mobile Computing". *In IEEE 15th Annual Int'l, Phoenix Conf. Comp. and Commun*, 1996.

[66]. F. Bennett, D.clarke, J. Evans, A. Hopper and D. Leask, "Piconet Embedded Mobile Networking", *IEEE Personnel Communications*, vol. 4, N° 5, Octobre 1997.

[67]. C.E. Perkins, E.M. Belding-Royer, and S. Das, "Ad Hoc On Demand Distance Vector (AODV) Routing", *IETF RFC 3561*.

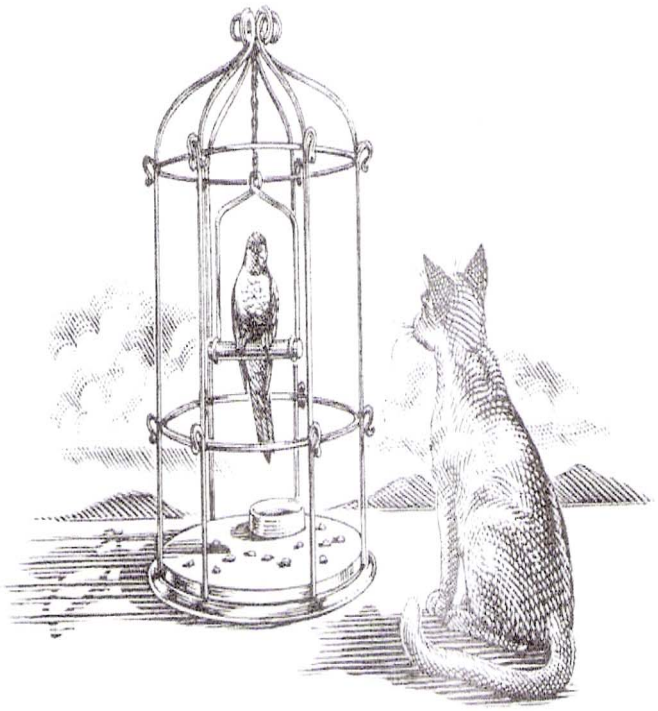
[68]. H. Maarit, "Efficient Key Agreement for Ad Hoc Networks", *Ph. D, Helsinki University of Technology*, Mai 2001.

[69] Y. Chun Hu, A. Perrig and D.B. Johnson, Ariadne, "A secure on-demand routing protocol for Ad hoc networks", *Proceedings of the 8th ACM International Conference on Mobile Computing and Networking*, 2002.

[70]. B. Dahill, B. Levine, E. Royer, C. Shields, "A Secure Routing Protocol for Ad hoc Networks", *Proceedings of the 10th Conference on Network Protocols (ICNP)*, Novembre 2002.

[71]. S. Buchegger, J.Y Le Boudec, "Performance analysis of the confidant protocol", *Proceeding ACM 3rd International Symposium on Mobile Ad hoc Networking and Computing (MobiHoc'02)*, pp. 226-236, 2002.

[72]. A. Beghriche, A. Bilami "Un Modèle de Confiance pour L'Authentification dans un Réseau sans fil Ad hoc", *Journées Ecole Doctorale & Réseaux de Recherche en Sciences et Technologies de l'Information JED'08,* Annaba Algérie, pp. 28-32, les 9-10 Juin 2008.



Oiseau se croyant en sécurité.