Contributions à la sécurité dans les réseaux mobiles ad Hoc

Abderrezak Rachedi

ACADÉMIE D'AIX-MARSEILLE
UNIVERSITÉ D'AVIGNON ET DES PAYS DE VAUCLUSE

THÈSE

présentée à l'Université d'Avignon et des Pays de Vaucluse
pour obtenir le diplôme de DOCTORAT

SPÉCIALITÉ : Informatique

École Doctorale « I2S »
Laboratoire d'Informatique (EA 4128)

Contributions à la sécurité dans les réseaux mobiles ad Hoc

par
Abderrezak RACHEDI

Soutenue publiquement le 26 novembre 2008 devant un jury composé de :

M.	Hossam AFIFI	Professeur, RS2M, Telecom Sud Paris	Rapporteur
M.	Bernard COUSIN	Professeur, IRISA, Université de Rennes	Rapporteur
M.	Joffroy BEAUQUIER	Professeur, LRI, Université de Paris-Sud	Président
M.	Jean-Claude KÖNIG	Professeur, LIRMM, Université de Montpellier	Examinateur
M.	Ahmed MEHAOUA	Professeur, CRIP5, Université de Paris-5	Examinateur
M.	Abderrahim BENSLIMANE	Professeur, LIA, Université d'Avignon	Directeur de thèse

Remerciements

Je tiens à remercier particulièrement et chaleureusement Monsieur Abderrahim BENSLIMANE, professeur à l'université d'Avignon, pour son encadrement, sa patience, sa présence, ses conseils très précieux, son dévouement et sa disponibilité à l'élaboration de cette thèse.

Je tiens à remercier chaleureusement tous les membres du jury qui ont accepté de juger ce travail, le président du jury le professeur Joffroy BEAUQUIER, les rapporteurs le professeur Bernard COUSIN et le professeur Hossam AFIFI et les examinateurs le professeur Jean-Claude KÖNIG et le professeur Ahmed MEHAOUA

Mes remerciements vont aussi à tous les membres du laboratoire d'informatique d'Avignon (LIA) pour le cadre de travail.

Je remercie également tous ceux qui ont contribué directement ou indirectement à l'aboutissement de cette thèse. Merci à tous les membres de ma famille, à mes soeurs et à mes frères, à mon père qui m'a beaucoup soutenu et encouragé et à ma mère à qui je dédie tout ce travail et qui m'a donné le courage de le mener à bien. Enfin, j'adresse aussi mes sincères remerciements à ma femme à qui je dois en grande partie l'accomplissement de ce travail, grâce à l'espoir et à la confiance qu'elle a toujours su me donner.

Résumé

La thèse se focalise sur la sécurité dans les réseaux mobiles ad hoc (MANET : Mobile Ad hoc NETwork) [RFC 2501]. 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 la thèse 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. De plus, les vulnérabilités au niveau des autorités de certification sont prises en compte dans le nouveau concept de DDMZ (zone dynamique démilitarisée) que nous proposons.

Dans le but de sécuriser les nœuds dont le rôle est crucial au sein du réseau, leur identité doit être cachée. C'est pourquoi le concept d'anonymat est introduit. Un protocole d'authentification anonyme est proposé. De plus, nous nous inspirons du modèle militaire pour mettre en place un mécanisme de camouflage qui cache le rôle des nœuds sensibles.

Pour entretenir le modèle de confiance, un mécanisme de surveillance est indispensable. Il est adapté aux contraintes de l'environnement sans fil dynamique et réduit le taux de fausses alarmes (faux positifs). Il est fondé sur une approche inter-couches et un modèle probabiliste pour améliorer l'observation du nœud surveillant.

Pour faire face aux attaques intelligentes de type inter-couches, une étude des vulnérabilités au niveau des couches inférieures comme la couche MAC est menée. Ensuite, des mécanismes de prévention et de détection sont analysés et évalués. La performance de ces mécanismes est évaluée avec la prise en compte des métriques primordiales pour les réseaux mobiles ad hoc, telles que la consommation d'énergie, la mobilité, la densité des nœuds et du trafic, etc . . .

Mots clés :
Réseaux mobiles Ad hoc, Sécurité, Algorithmes distribués, Mécanisme de surveillance, IEEE 802.11, Système de détection d'intrusions (IDS), Infrastructure à clé publique (PKI), Zone dynamique démilitarisée (DDMZ), Anonymat, Attaques inter-couches.

Abstract :

The thesis focuses on security in Mobile Ad hoc Networks (MANETs) [RFC 2501]. The lack of any central management of the network functions make MANETs more vulnerable to attacks than wireless (WLANs) and wired networks (LANs). Unfortunately, security protocols that currently exist are not designed to adapt MANETs characteristics. They do not take into account the resource limits, while the environment is dynamic and the resources are limited (memory storage, computation power and energy), and this complicates the problem, because, as we know, security solutions require a high amount of resources. However, we have to face the challenge, because the application fields of MANETs, such as military and emergency operations, are so numerous that it is necessary to design a robust security mechanism for Mobile Ad hoc Networks.

The main goal of my thesis consists in examining the solutions that are likely to insure security in MANETs, and in proposing a hierachical distributed architecture that enables to implement a dynamic public key infrastructure. This solution must be adapted to MANETs characteristics (no control central unit, dynamic network topology, etc.). With this aim in view, a trust model adapted to the dynamic environment to insure the nodes trust level updating must be designed. Moreover, the certification authority vulnerabilities must be taken into account in the new DDMZ concept (dynamic dmilitarized zone), that we propose. In order to increase the security level of the important nodes in the network, their identity must be hidden. That is why we introduced the anonymity concept.

We also proposed an anonymous authentication protocol. Moreover, we drew our inspiration from the military model in order to implement a camouflage mechanism that hides the important nodes' roles.

In order to maintain the trust model, a monitoring mechanism is necessary. It must be adapted to dynamic wireless environment constraints and must reduce the rate of false positives (false alarms). It is based on a cross-layer approach and a probabilistic model to improve the monitor node's observation.

In order to face smart attacks, such as cross-layer attacks, we must study the vulnerabilities located at the lower layers, such as the MAC layer. Then, prevention and detection mechanisms are analysed and assessed. In order to assess the performance of these mechanisms, we take into account the main metrics of Mobile Ad hoc Networks, such as energy consumption, mobility, nodes' density, traffic rate, etc.

Key words :
Mobile Ad hoc Networks, Security, Distributed algorithms, Monitoring mechanism, Intrusion Dectection system (IDS), IEEE 802.11, Public key infrastructure (PKI), Dynamic Demilitarized Zone (DDMZ), Anonymity, Cross-layer attacks.

Table des matières

Chapitre 1

Introduction Générale

Sommaire

1.1 Contexte

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

Les réseaux mobiles Ad hoc ont été initialement développés pour des applications militaires, mais leurs propriétés en font des solutions pratiques dans de nombreux domaines de la vie courante. Grâce à cette technologie mobile Ad hoc, les utilisateurs n'ont pas besoin d'une infrastructure préexistante pour communiquer et ils peuvent aussi se déplacer tout en restant connectés à leurs services. Parmi les solutions offertes par les réseaux mobiles Ad hoc, il existe par exemple l'extension de l'accès aux bornes d'une infrastructure fixe (téléphonie sans fil, Wifi etc.), en dépassant la portée radio de ces bornes grâce aux relais Ad hoc que les utilisateurs peuvent se fournir les uns aux autres pour accéder indirectement à l'infrastructure. Cependant, l'aspect le plus novateur des réseaux Ad hoc est leur capacité à fournir une couverture réseau mobile de manière automatique et autonome, et ce même sans accès à une infrastructure préexistante.

L'élargissement du domaine d'application des réseaux mobiles Ad hoc nécessite plus de sécurité pour assurer l'intégrité et la confidentialité des données qui circulent dans le réseau. En effet, les réseaux mobiles Ad hoc sont confrontés à de nombreux

problèmes liés à leurs caractéristiques qui rendent les solutions de sécurité développées pour les réseaux filaires ou sans fil avec infrastructure inapplicables dans le contexte des réseaux mobiles Ad hoc. Parmi les vulnérabilités qui touchent les réseaux mobiles Ad hoc nous pouvons citer :

- *L'absence d'infrastructure :* les réseaux mobiles Ad-hoc sont des réseaux sans infrastructure fixe. Ceci ne nous permet pas d'opter pour une architecture centralisée. En effet, l'absence d'une unité centralisée accentue le défi pour proposer une solution de sécurité comme c'est le cas dans les réseaux filaires ou sans fil avec infrastructure fixe. Cependant, une architecture centralisée est déconseillée dans les réseaux mobiles Ad hoc, car elle peut créer un point de vulnérabilité dans le réseau.
- *La topologie réseau dynamique :* parmi les caractéristiques des réseaux mobiles Ad-hoc, on trouve l'environnement dynamique, qui est dû à la mobilité des nœuds. Cette caractéristique nécessite le développement de protocoles de routage sophistiqués et de solutions de sécurité adaptées à un tel environnement, ce qui constitue un vrai défi.
- *La vulnérabilité des nœuds :* les nœuds ne sont pas physiquement protégés, ils peuvent être capturés par des attaquants (l'ennemi), ce qui pose problème au niveau des relations de confiance entre les nœuds. Ainsi, n'importe quel modèle de sécurité dédié au réseau mobile Ad hoc doit prendre en compte la compromission des nœuds, ainsi que la résistance à cette attaque.
- *La vulnérabilité du canal :* le support de transmission est l'air. Ce dernier est très vulnérable aux écoutes clandestines. N'importe quelle machine qui dispose d'une carte sans fil adaptée à la technologie utilisée, est capable de capturer le trafic, de l'analyser et même d'injecter du nouveau trafic, soit dans le but de surcharger le réseau soit dans celui de faire circuler des fausses informations pour changer la topologie du réseau. De plus, le canal sans fil est fortement vulnérable au risque de brouillage « jamming », ce qui a des conséquences néfastes sur le réseau.
- *Les ressources limitées :* les nœuds mobiles dans les réseaux mobiles Ad-hoc ont des ressources très limitées, comme la capacité de calcul, de stockage et surtout d'énergie. La batterie ne tient pas longtemps si le nœud travaille sans arrêt, ce qui complique davantage le problème de la sécurité. En effet, nous savons que la plupart des solutions de sécurité sont basées sur la cryptographie, mais malheureusement cette dernière est gourmande en terme de ressources : capacité de calcul, consommation d'énergie et mémoire de stockage.

Par conséquent, de nombreux thèmes de recherches ont surgi au cours des dernières années pour remédier à ces vulnérabilités et assurer les services de sécurité dans les réseaux mobiles Ad hoc.

1.2 Problématique et motivations

Les réseaux mobiles Ad hoc sont vulnérables à divers types d'attaques qui peuvent être lancées de façon relativement simple. En particulier, la communication sans fil facilite l'écoute clandestine dans le but d'analyser le trafic réseau et de lancer par la suite

des attaques de type actives. L'usurpation d'identité est une autre attaque qui est facilement exploitable dans l'environnement sans fil. Avec l'accès physique au réseau, n'importe quelle machine a l'opportunité de se mettre à la portée des autres machines du réseau et donc aussi de créer des attaques et de perturber l'activité du réseau, sans pour autant se faire détecter. De plus, un attaquant qui connaît bien les mécanismes des couches physique et MAC et qui possède une puissance de transmission suffisante peut alors empêcher ses voisins d'accéder au canal de communication. A cause de ces vulnérabilités qui caractérisent la communication sans fil, les nœuds malicieux peuvent modifier, usurper, injecter les données et générer de faux messages, et, de façon générale, ne respectent pas les protocoles utilisés. L'impact d'un tel comportement malicieux peut être grave en particulier parce que la coopération des nœuds de tout le réseau joue le rôle d'infrastructure. Un nœud malicieux peut potentiellement empêcher la communication entre les nœuds en refusant de les relier. Il agit ainsi dans le but soit de préserver sa propre énergie (égoïsme), soit juste pour interrompre la communication entre les nœuds. De plus, les nœuds dans le réseau mobile Ad-hoc peuvent rejoindre et quitter le réseau librement sans préavis. Ainsi il est difficile dans la plupart des cas d'avoir une image claire de la distribution des nœuds dans le réseau. La confiance entre les nœuds est un paramètre très important dans la fonctionnalité du réseau. Les relations de confiance se développent avec le temps et risquent de changer. Cette situation rend nécessaire le développement d'un modèle de confiance dynamique. En outre, l'absence d'infrastructure fait obstacle à l'établissement d'une ligne de défense qui sépare les nœuds de confiance des nœuds malicieux. L'inexistence d'une entité centrale rend la détection des attaques très difficile, car un réseau hautement dynamique ne peut être facilement surveillé. Etant donné que des erreurs bénignes, telles que la détérioration des transmissions, la rupture de l'acheminement des paquets, ou encore la suppression de paquets, se produisent souvent dans les réseaux mobiles Ad hoc, il est encore plus ardu de détecter les erreurs provoquées par des attaques. En conséquence, avoir un modèle du comportement de l'attaquant n'est pas une tâche facile. C'est pourquoi la détection des attaquants exige une longue phase d'observation. La plupart des protocoles développés pour les réseaux mobiles Ad hoc n'étaient pas conçus à la base pour faire face au comportement malicieux des nœuds et aux autres menaces pour la sécurité.

Pour remédier à ces vulnérabilités, plusieurs architectures de sécurité ont été proposées pour distribuer les clés de chiffrement ainsi que les certificats dans le but de sécuriser la communication entre les nœuds. Cependant, la plupart de ces architectures ne respectent pas les caractéristiques des réseaux mobiles Ad hoc : soit elles adoptent un schéma centralisé (Sanzgiri et al., 2005a), soit elles ne supportent pas la mobilité et la dynamique de la topologie des nœuds (Bechler et al., 2004), soit elles ne possèdent aucun modèle de confiance dynamique et se limitent à un réseau fermé. Après avoir étudié ces différentes approches et en avoir analysé les faiblesses, nous avons proposé dans la thèse une architecture hiérarchique de sécurité distribuée adaptée aux caractéristiques des réseaux mobiles Ad hoc pour distribuer les certificats et les clés de chiffrement de manière dynamique. Notre approche permet non seulement d'éviter les vulnérabilités citées ci-dessus, mais aussi d'améliorer le niveau de sécurité dans le réseau. Nous nous focalisons sur la gestion dynamique distribuée des clés de chiffrement pour assurer une communication sécurisée dans le réseau. De plus, nous nous concentrons

sur l'étude des modèles de confiance distribués pour assurer la distribution dynamique des services de sécurité. Nous prenons en compte la sécurité des nœuds qui possèdent un rôle sensible dans le réseau et cela via l'introduction du concept d'anonymat. Ce concept empêche tout nœud de connaître l'identité des nœuds dont le rôle est crucial pour le réseau (la sécurité de l'autorité de certification (CA), par exemple).

Nous savons que les modèles de confiance dans les réseaux mobiles Ad-hoc doivent être dynamique, ce qui malheureusement n'est pas souvent le cas dans les solutions proposées dans la littérature. Ces modèles de confiance nécessitent des mécanismes de surveillance avancés. C'est pourquoi, nous proposons un mécanisme de surveillance sophistiqué, fondé sur une approche inter-couches pour entretenir le modèle de confiance, renforcer la sécurité dans le réseau et détecter les intrusions ainsi que les attaques intelligentes. Avec notre mécanisme de surveillance, nous permettons non seulement d'entretenir correctement le modèle de confiance, mais aussi d'assurer la détection des attaques intelligentes tout en réduisant le taux de faux positifs.

Parmi les attaques les plus difficiles à détecter et à corriger, on trouve les attaques de type inter-couches. Plusieurs travaux ont été présentés pour éviter ce genre d'attaques mais seulement quelques-uns traitent des attaques basées sur les paquets de contrôle de la couche MAC, particulièrement la technologie IEEE 802.11 (IEEE802-11, 1999) . Nous avons analysé de nouvelles vulnérabilités de ces paquets de contrôle et montré leur exploitation et leur impact au niveau des couches supérieures (couche réseau, par exemple). Contrairement aux autres travaux qui ne se basent que sur les simulations pour montrer l'impact des attaques, nous avons opté pour une étude expérimentale pour analyser l'impact réel de ces attaques ainsi que leur faisabilité. Nous avons proposé un ensemble de solutions : certaines sont fondées sur les mécanismes cryptographiques, d'autres non. Puis, nous avons évalué ces solutions ainsi que le compromis entre le niveau et le coût de la sécurité.

1.3 Contributions

Notre première contribution de la thèse a été de proposer une architecture distribuée pour assurer la sécurité dans les réseaux mobiles Ad-hoc. Le but principal de cette architecture est d'établir un mécanisme de certification à clé publique distribuée, basé sur un modèle de confiance. L'idée consiste à distribuer le rôle de l'autorité de certification de manière dynamique, en fonction de l'évolution de la topologie du réseau, du niveau de confiance des nœuds, ainsi que de la stabilité du réseau. Pour atteindre ce but, nous avons opté pour la division du réseau sous forme de groupes (clusters), via un algorithme de groupage appelé « *algorithme de clustering sécurisé* ». Chaque groupe (cluster) possède sa propre autorité de certification appelée (CA), qui assure le rôle de leader du groupe. Pour protéger cette autorité contre les attaques de type Déni de Services, nous avons proposé un nouveau concept appelé « zone dynamique démilitarisée » ($DDMZ$). Ce concept n'est qu'un ensemble de nœuds qui possèdent un certain niveau de confiance et dont la tâche consiste à filtrer toutes les communications entre le CA et les autres mobiles, jugés non confidents ou inconnus. Nous avons présenté

une évaluation de cette architecture via des simulations et nous avons évalué la qualité d'authentification au niveau des groupes. Ensuite, nous avons proposé un modèle probabiliste pour évaluer la robustesse de l'architecture en général, et celle de la $DDMZ$ en particulier. L'idée consiste à estimer la possibilité de former des groupes de mobiles robustes à partir d'une configuration donnée du réseau. Cette information est importante pour évaluer les risques et la résistance aux attaques.

Comme extension de notre architecture, nous avons introduit un nouveau niveau de sécurité qui consiste à assurer l'anonymat des nœuds de confiances. Dans un environnement hostile, assurer l'anonymat des nœuds sensibles, en particulier l'identité des CA et RA (les mobiles qui assurent des tâches de sécurité sensibles) est devenu nécessaire pour échapper aux attaques qui se basent sur l'analyse du trafic réseau. Ainsi, la confidentialité du trafic réseau ainsi que les services réseau sont devenus des éléments clés, au même titre que la confidentialité des données, pour assurer la sécurité des réseaux.

Notre deuxième contribution consiste à assurer l'évolution du modèle de confiance dans notre architecture. A cet effet, nous avons proposé un mécanisme inter-couches (cross-layer) pour surveiller les actions des nœuds dans le réseau, et en particulier la coopération. La coopération est un facteur important dans les réseaux mobiles Ad-hoc. Ainsi, avoir des nœuds qui ne coopèrent pas dans le réseau, et en particulier dans l'établissement des routes et dans le routage peut avoir des impacts négatifs sur le réseau. La plupart des solutions existantes dans la littérature sont basées sur l'observation et la surveillance de chaque couche du modèle OSI sans prendre en compte l'interaction entre les couches. Cependant, dans le contexte des réseaux sans fil mobiles, ces solutions ne permettent pas d'éviter les fausses alarmes (faux positifs). Notre contribution consiste à réduire de manière considérable les faux positifs et à rendre l'opération de surveillance efficace. C'est pourquoi nous avons opté pour une approche inter-couches avec le mécanisme de surveillance. Nous avons introduit les paramètres de la couche physique et de la couche MAC au niveau de la couche de routage pour déterminer si le nœud surveillant est en mesure d'assurer la tâche de surveillance sans faux positif. La distance entre le nœud surveillant et le nœud surveillé est prise en compte, ainsi que la différence entre le rayon de transmission et le rayon d'interférence. Les paramètres de la couche physique, tels que le SNR (Signal to Noise Ratio) et la puissance de réception, ainsi que les paramètres de la couche MAC tels que les paquets de contrôle et les acquittements sont aussi pris en compte. Notre proposition permet d'améliorer l'observation du nœud surveillant et de réduire les fausses alarmes, ce qui implique une évolution correcte du modèle de confiance.

Notre troisième contribution est la proposition d'une analyse approfondie des nouvelles vulnérabilités de type inter-couches qui visent les réseaux mobiles Ad hoc, et en particulier le mécanisme de surveillance. Ces nouvelles vulnérabilités consistent à exploiter les faiblesses du protocole MAC IEEE 802.11, dans le but de créer une attaque au niveau de la couche de routage. Nous avons étudié l'impact de ces attaques via des simulations. De plus, nous avons démontré la faisabilité de ces attaques après les avoir implémentées via des expériences de laboratoire. En outre, nous avons montré comment une vulnérabilité au niveau de la couche MAC peut perturber le mécanisme

de surveillance et même fausser l'observation du nœud surveillant sans qu'il ne s'en rende compte. Comme solution à ces attaques particulièrement complexes, nous avons présenté un ensemble de solutions possibles. Ces solutions sont classées en deux catégories : solutions avec cryptographie et solutions sans cryptographie. Enfin, nous avons étudié avec analyse et simulations les différentes solutions qui permettent d'authentifier les paquets de contrôle au niveau de la couche MAC.

1.4 Plan du mémoire

La thèse est divisée en sept chapitres. Dans chaque chapitre, nous présentons une étude et une analyse des solutions déjà existantes, puis décrivons en détail notre contribution, suivie d'une validation et d'une analyse comparative avec d'autres approches similaires.

Le chapitre 2 est consacré principalement à l'état de l'art sur la sécurité dans les réseaux mobiles Ad hoc. Tout d'abord, nous présentons les réseaux mobiles Ad hoc, leurs caractéristiques, leurs domaines d'application, ainsi que la couche MAC 802.11 utilisée dans ces réseaux. Ensuite, nous présentons les besoins de la sécurité dans les réseaux. De plus, nous décrivons les différentes vulnérabilités et la classification des attaques dont les réseaux mobiles Ad hoc souffrent. Nous citons les principaux axes de sécurité dans les réseaux mobiles Ad hoc. Puis, nous étudions les différentes approches de sécurité dédiées à l'environnement des réseaux mobiles Ad hoc.

Le chapitre 3 aborde l'architecture distribuée pour assurer la distribution de l'autorité de certification (CA) via la division du réseau sous forme de groupes (clusters). Tout d'abord, nous définissons le modèle de confiance distribué adopté par notre architecture. Nous expliquons les relations de confiance entre les différents acteurs du réseau. Nous définissons le nouveau concept appelé « *zone dynamique démilitarisée* » ($DDMZ$) pour sécuriser les autorités de certification dans chaque groupe. Nous présentons également l'algorithme distribué d'élection de CA dans chaque groupe appelé $SDCA$. Ensuite, nous effectuons une analyse de la performance de notre architecture par des simulations et nous comparons notre architecture avec d'autres architectures déjà existantes. Enfin, nous analysons la sécurité de notre architecture.

Le chapitre 4 consiste à étendre l'architecture proposée dans le chapitre précèdent par l'introduction du concept d'anonymat. Nous proposons un protocole qui assure l'anonymat des nœuds qui ont des rôles importants dans le réseau tel que l'autorité de certification (CA) et l'autorité d'enregistrement (RA). Par conséquent, nous introduisons le concept d'anonymat dans le mécanisme de protection du nœud CA appelé la zone dynamique démilitarisée (DDMZ). Cette zone devient une zone anonyme, car elle sera formée par des nœuds dont l'identité est cachée (n'est pas connue par les autres nœuds). Elle sera notée (ADDMZ). De plus, nous nous inspirons des mécanismes de défense militaire tels que les techniques de camouflage et les mécanismes de changement d'identité. Nous proposons un protocole pour réaliser ces mécanismes avec l'utilisation de la cryptographie basée sur la fonction bilinéaire. L'analyse de sécurité du protocole

proposé est présentée avec les discussions et l'évaluation.

Le chapitre 5 traite du mécanisme de surveillance inter-couches. C'est un processus très important pour l'évolution du modèle de confiance de manière dynamique et pour la détection des intrusions. Le but de notre modèle de surveillance est de réduire les fausses alarmes et de rendre l'opération de surveillance plus efficace. Dans ce modèle, nous nous sommes focalisés sur les problèmes de collisions qui empêchent le bon déroulement de l'opération de surveillance. Ce modèle est un modèle de type inter-couches car il prend en considération les paramètres des couches inférieures MAC et physique au niveau de la couche réseau (routage) pour déterminer les conditions les plus favorables à l'opération de surveillance. Nous avons effectué une analyse de la performance de notre mécanisme de surveillance en prenant en compte les différentes caractéristiques des réseaux mobiles Ad hoc, telles que la densité des nœuds dans le réseau, le trafic réseau, ainsi que la mobilité des nœuds. Enfin, une étude comparative avec le mécanisme de surveillance connu sous le nom de Watchdog (S. Marti et Baker, 2000) a été effectuée.

Le chapitre 6 se focalise sur les différentes vulnérabilités cachées qui peuvent être exploitées par des attaques de type inter-couches. Nous définissons des algorithmes d'attaques qui exploitent les vulnérabilités cachées au niveau de la couche MAC, et en particulier les paquets de contrôle, tels que les paquets RTS, CTS et ACK. Pour valider ces algorithmes d'attaques, nous avons simulé ces algorithmes dans le simulateur *NS*2 (ns 2, 1999). Ensuite, nous avons expérimenté ces algorithmes au sein de scénarios réels avec l'utilisation des cartes wifi, munies des chipsets Atheros et du driver *MdWifi* (Leffler, 2007). Puis, nous avons proposé plusieurs solutions pour sécuriser les paquets de contrôle au niveau MAC. Enfin, une évaluation des performances des solutions proposées est effectuée, ainsi que l'analyse de la sécurité.

Enfin, le dernier chapitre constitue la conclusion de cette thèse. Nous proposons une synthèse de nos contributions, puis nous évoquons les perspectives possibles de nos travaux.

Chapitre 2

Etat de l'art

Sommaire

Ce chapitre est organisé comme suit : dans la section 2.1, nous présentons les réseaux mobiles Ad hoc, leurs caractéristiques et leurs domaines d'application, ainsi que les réseaux sans fil avec infrastructure ($WLAN$). La section 2.2 est dédiée aux besoins de la sécurité dans les réseaux mobiles Ad hoc. Ensuite, dans la section 2.3, nous classifions les différentes attaques dans les réseaux mobiles Ad hoc. Dans la section 2.4, nous montrons les domaines et les axes de sécurité dans les réseaux mobiles Ad hoc. Nous décrivons les différentes solutions de sécurité basées sur le concept inter-couches dans la section 2.5. Enfin, la section 2.6 conclut le chapitre.

2.1 Réseau mobile ad hoc : généralités

Les réseaux mobiles Ad hoc (MANETs) ne cessent d'évoluer grâce au développement de la technologie mobile. Les équipements mobiles deviennent de plus en plus petits et puissants en terme de capacité de traitement et de stockage des données. Ceci permet aux nœuds d'assurer des applications et des services plus avancés. Parmi les applications et services, nous pouvons citer les demandes de connexion, de routage, de sécurité, etc . . .

Les réseaux Ad hoc sont divers, nous pouvons en citer quelques uns :

- Les réseaux personnels : PAN (Personal Area Network) désigne un réseau restreint d'équipements informatiques habituellement utilisés dans le cadre d'une utilisation personnelle. Parmi les technologies sans fil utilisées par les réseaux PAN, nous pouvons citer le Bluetooth, l'infrarouge (IR), ou le zigbee (la technologie 802.15.4).
- Les réseaux poste-à-poste ou Peer-to-Peer sont des réseaux dont le fonctionnement est décentralisé entre les différents utilisateurs du réseau, dont les machines sont simultanément clients et serveurs des autres machines (et aussi routeur, en passant les messages de recherche voire les données vers leur(s) destinataire(s)).
- Les réseaux de capteurs sont des réseaux composés de nœuds intègrant une unité de mesure chargée de capter des grandeurs physiques (chaleur, humidité, vibrations) et de les transformer en grandeurs numériques, une unité de traitement informatique et de stockage de données et un module de transmission sans fil (wireless).
- Les réseaux de voitures : les voitures de nos jours embarquent de plus en plus de technologie et ont de plus en plus besoin de communiquer avec l'extérieur. Les voitures équipées par des capteurs dans les toits et/ou les pare-chocs sont capables de créer des plateformes de réseaux mobile Ad-hoc et de relier en réseau les automobiles passant à proximité les unes des autres. Des prototypes ont déjà été développés pour les véhicules d'urgence (les ambulances, les voitures des pompiers, etc).
- etc . . .

2.1.1 Caractéristiques des réseaux mobiles Ad hoc

Les réseaux mobiles Ad hoc possèdent non seulement les mêmes caractéristiques que les réseaux mobiles, mais aussi un certain nombre de caractéristiques qui leur sont propres et qui les différencient des autres. Nous pouvons citer quelques caractéristiques principales :

- *Absence d'infrastructure :* pas de station de base ou de point d'accès, tous les nœuds du réseau se déplace dans un environnement distribué sans point d'accès ou un point de rattachement à l'ensemble du réseau. Un nœud joue le rôle aussi bien d'un acteur actif dans le réseau émetteur et récepteur mais aussi de routeur pour relayer la communication des autres nœuds du réseau.

- *Topologie du réseau dynamique :* les nœuds du réseau sont autonomes et capables de se déplacent de manière arbitraire. Cette mobilité fait que la topologie réseau est dynamique car elle peut changer à tout instant de façon rapide et aléatoire. Ce changement de topologie a un impact sur les connexions ou les liens unidirectionnels et bidirectionnels des nœuds. Comme exemple, un nœud (routeur) peut à chaque moment quitter ou rejoindre le réseau.
- *Canal de communication sans fil :* nous savons que les liaisons sans fil auront toujours une capacité inférieure à des liaisons filaires. La bande passante est moins importante, et en plus le débit est confronté aux effets multiples d'interférences, du bruit ...
- *Ressources limitées :* les sources d'énergie telles que les batteries sont nécessaires pour la communication des nœuds mobiles. Malheureusement, ces sources d'énergie ont une durée de vie limitée et leur épuisement dépend des traitement effectués au niveau du nœud tels que les opérations de transmission, réception et les calculs complexes, etc ... Par conséquent, la consommation d'énergie consitue un véritable problème. Les mécanismes de gestion d'énergie sont nécessaires pour les nœuds dans le but de conserver l'énergie et d'augmenter leur durée de vie. Donc, n'importe quelle solution destinée aux réseaux mobiles Ad hoc doit prendre en compte la contrainte de l'énergie.
- *Taille du réseau :* Dans le réseau mobile Ad hoc, la portée de transmission des nœuds est petite ou moyenne (environ 250 mètres). Cela a un impact sur la couverture du réseau (la taille du réseau est de quelques centaines de nœuds). C'est pourquoi le réseau est utilisé dans certains cas pour étendre temporairement un réseau filaire dans un environnement où le déploiement du réseau filaire n'est pas possible.
- *Vulnérabilité aux différentes attaques :* les réseaux mobiles Ad hoc sont des réseaux qui héritent des mêmes vulnérabilités que les réseaux sans fil classiques et sont en plus sensibles à d'autres menaces liées à leurs propres caractéristiques.

2.1.2 Applications dans les réseaux mobiles Ad hoc

Les réseaux mobiles Ad hoc ont réussi à s'imposer en tant que technologie prometteuse. Leurs caractéristiques et en particulier la mobilité et l'absence d'infrastructure élargissent leurs domaines d'application. Nous pouvons citer les points forts des réseaux mobiles Ad hoc comme suit :

- *Réseau à coût réduit :* Les réseaux filaires sont des réseaux coûteux du point de vue économique, car ils nécessitent du câblage et le déploiement d'une infrastructure. Cependant, les réseaux mobiles Ad hoc peuvent être déployés partout, surtout dans des endroits où les réseaux filaires ne peuvent pas être déployés pour des raisons de difficultés géographiques. Ainsi, les réseaux Ad hoc deviennent une alternative pour réduire les coûts financiers.
- *Réseau en endroit hostile :* Dans les environnements à accès difficile tels que les régions montagneuses, les réseaux mobiles Ad hoc sont très pratiques. Un autre exemple d'endroits hostiles est le champ de bataille.

– *Réseau sans infrastructure :* Dans le cas d'une communication locale qui ne nécessite pas de ressources de réseaux filaires, nous pouvons par exemple citer le cas des conférences ou des réunions. Il n'est pas nécessaire de passer par le réseau filaire pour les communications inter-membres.

A- Applications militaires

Les réseaux mobiles Ad hoc sont conçus à la base pour des applications et des opérations à caractère militaire. Ces réseaux sont adaptés aux environnements hostiles, car ils sont dynamiques et rapidement déployables. Les nœuds du réseau ne sont que des équipements militaires communiquants : soldats, véhicules blindés, etc. . . Cependant, l'application de ces réseaux a dépassé le domaine militaire grâce au développement technologique des réseaux sans fil tel que le bluethooth.

B- Opérations de sauvetage

Les réseaux mobiles Ad hoc sont aussi utilisés lors des opérations de sauvetage, notamment lors de tremblements de terre ou autres catastrophes. Ces réseaux peuvent être rapidement déployés sur des terrains de sinistres pour assurer le relai et la liaison des communications entre sauveteurs.

C- Domaine commercial

Les réseaux mobiles Ad hoc peuvent étendre un réseau avec infrastructure pour offrir un service tel que l'accès à Internet à moindre coût. De plus, ils permettent de relier plusieurs ordinateurs entre eux pour partager des fichiers, des jeux, la tenue des réunions, la communication entre agents, etc. . .
Il existe d'autres applications des réseaux mobiles Ad hoc, comme la communication entre les véhicules. Cette application est prometteuse car elle permet de réduire le risque d'accidents sur les autoroutes, d'assurer la communication des véhicules dans les tunnels, etc . . .

D- Réseau d'entreprise

La facilité à déployer ces réseaux et leur coût réduit intéressent de plus en plus les entreprises. Cela permet d'assurer une grande mobilité des agents, le partage des données et les conférences. Par exemple, lors d'une réunion ou conférence, l'intervenant peut communiquer avec tous les participants et créer un débat interactif.

2.1.3 Réseaux sans fil avec infrastructure WLAN

Les réseaux sans fil (WLAN/WiFi) utilisent la technologie IEEE 802.11 (IEEE802-11, 1999) pour accéder au canal de communication. Cette technologie peut opérer selon deux modes de configuration du réseau sans fil local : réseau avec infrastructure et réseau sans infrastructure (autonome). Dans la configuration de réseau avec infrastructure, un point d'accès (AP) est nécessaire pour jouer le rôle de contrôleur centralisé. Le point d'accès est connecté au réseau filaire et peut fournir aux stations mobiles les mêmes services que ceux qui sont disponibles pour le réseau filaire, tels qu'Internet. C'est le mode par défaut des adaptateurs sans fil : chaque ordinateur se connecte à un point d'accès (AP) via son adaptateur sans fil. On identifie chaque point d'accès par un identifiant appelé SSID (Service Set IDentifier) qui représente le réseau sur lequel on veut se connecter. Pour que toutes les machines se connectent au réseau sans fil, elles doivent au préalable connaître le SSID du réseau, donné sur le point d'accès. Si la machine est à la portée d'un point d'accès, elle se connectera au réseau. Cependant, le deuxième mode de configuration du protocole MAC 802.11 appelé Ad hoc est un système pair à pair constitué de stations mobiles autonomes capables de communiquer et de s'auto-configurer pour former un réseau dynamique. Donc, aucun point d'accès n'est nécessaire, chaque machine joue en même temps un rôle de client et un rôle de point d'accès.

Description de la couche MAC IEEE 802.11

Le protocole MAC IEEE 802.11 est la technologie d'accès au canal que nous avons utilisée dans cette thèse. Il existe deux modes de fonctionnement de ce protocole : le mode PCF (Point Coordination Function) et le mode DCF (Distributed Coordination Function). Le mode PCF est utilisé pour supporter les trafics synchrones tels que les trafics en temps réel. Ce mode est utilisé dans le cas des réseaux avec infrastructure, car un point d'accès est nécessaire. Le mode DCF est utilisé par les réseaux mobiles Ad hoc. Nous ne nous focalisons que sur le mode DCF qui se base sur l'utilisation de CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) pour assurer la transmission asynchrone des données. Le principe de fonctionnement du DCF consiste à écouter le canal de communication pour détecter si le canal est libre ($IDLE$) ou bien si un autre nœud est en train d'émettre. Avant chaque transmission, le nœud doit vérifier que le canal est libre pour une certaine durée appelée DIFS (Distributed Inter Frame Space). Dans le cas où le canal est occupé, la transmission est différée d'un certain temps appelé Backoff qui est choisi de manière aléatoire dans une fenêtre de contention (Contention Window : CW). La valeur du Backoff n'est décrémentée que si le canal est libre. Cependant, une collision peut apparaître si au moins deux stations transmettent en même temps, mais la station émettrice n'a pas la possibilité de détecter cette collision. Ainsi, un mécanisme d'acquittement (ACK) est nécessaire pour informer la station émettrice de la bonne réception du paquet. De plus, pour éviter le problème des stations cachées et réduire le nombre de collisions, le mécanisme RTS/CTS (Request-To-Send/Clear-To-Send) est utilisé. Avec ce mécanisme, la station émettrice envoie un

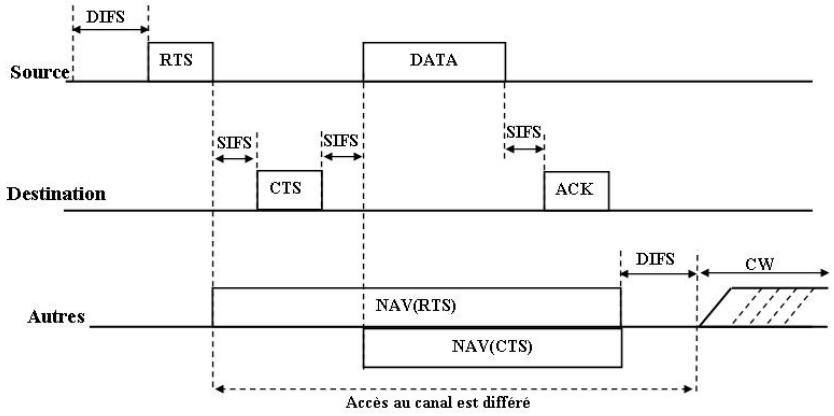


FIG. 2.1 – *Méthode d'accès au canal avec le mode DCF*

paquet de contrôle RTS dans le but d'informer les stations voisines de son souhait de transmettre ainsi que de la durée de transmission appelée $NAV(RTS)$. Une fois que la station réceptrice reçoit le paquet RTS correctement, elle va répondre avec un autre paquet de contrôle CTS dans le but d'informer ses voisins de son état de réception pendant une durée $NAV(CTS)$. Toutes les stations qui reçoivent soit le paquet de contrôle RTS, soit le CTS doivent bloquer leur transmission pendant $NAV(RTS)$ ou $NAV(CTS)$ respectivement. Lorsque la station émettrice reçoit le paquet CTS, elle en déduit que son paquet RTS a bien été reçu par la station réceptrice et donc qu'elle a bien réservé le canal pour transmettre. Elle va donc lancer la transmission du paquet DATA. Si la station réceptrice reçoit le paquet DATA avec succès, elle va répondre avec un acquittement pour informer la station émettrice de la bonne réception du paquet DATA. Ce mécanisme d'accès canal dans le mode DCF est décrit dans la figure 2.1.

2.2 Besoins en sécurité

Les besoins de base en sécurité pour les réseaux mobiles Ad-hoc sont plus ou moins les mêmes que pour les réseaux filaires ou sans fil avec infrastructure. Les services de sécurité sont basés sur quatre concepts fondamentaux : l'authentification des utilisateurs, la confidentialité, l'intégrité des données et du trafic du réseau, et enfin la non répudiation des utilisateurs.

2.2.1 Authentification

L'authentification permet de vérifier l'identité d'une entité ou d'un nœud dans le réseau. C'est une étape incontournable pour le contrôle de l'accès aux ressources réseau. Sans l'authentification, un nœud malicieux peut facilement usurper l'identité d'un autre nœud dans le but de bénéficier des privilèges attribués à ce nœud ou d'effectuer des attaques sous l'identité de ce nœud et de nuire à la réputation du nœud

victime. De manière générale, l'authentification est un processus basé sur trois principes qui peuvent être définis en une seule phrase : « c'est quelque chose qu'on est, quelque chose qu'on connaît et quelque chose qu'on a ». En d'autres termes, « c'est quelque chose qu'on est » : c'est la biométrie, comme la rétine des yeux, l'empreinte digitale, etc ..., « c'est quelque chose qu'on connaît » : c'est un mot de passe ou une clé, etc ..., « c'est quelque chose qu'on a » : c'est une carte d'accès ou un certificat, etc ... Dans le cadre des réseaux filaires ou des réseaux sans fil avec infrastructure, le processus d'authentification est basé sur un tiers de confiance en qui toutes les entités du réseau ont confiance. Le tiers de confiance n'est que l'autorité de certification qui distribue les certificats aux nœuds qui ont le droit d'accéder à un certain service du réseau. Ce schéma d'authentification est centralisé, et est connu sous le nom d'infrastructure à clé publique (PKI) (S. Chokhani, 2003). Appliquer le modèle PKI directement au réseau mobile Ad Hoc n'est pas possible pour des raisons de changement dynamique et fréquent de topologie réseau, car la disponibilité du service d'authentification est limitée en raison de la limite des capacités des nœuds (énergie, calcul, etc ...).

2.2.2 Confidentialité

La confidentialité est un service essentiel pour assurer une communication privée entre les nœuds. C'est une protection contre les menaces qui peuvent causer la divulgation non autorisée d'informations alors qu'il faut veiller au caractère privé de l'information. Elle est principalement basée sur la cryptographie, en particulier les algorithmes de chiffrement. Le chiffrement peut être appliqué à différents niveaux des couches de protocoles. Au niveau de la couche réseau, nous pouvons citer le protocole *ESP* (Encapsulating Security Payload (RFC2406, 1998)), qui assure la confidentialité aux datagrammes IP par le chiffrement. ESP est un protocole appartenant à *IPsec* (Internet Protocol Security) (RFC2401, 1998). Les algorithmes de chiffrement, qu'ils soient symétriques ou asymétriques, nécessitent une clé de chiffrement pour chiffrer le message avant de l'envoyer à la destination. Cependant, la destination doit avoir une clé de déchiffrement pour pouvoir déchiffrer le message. Par conséquent, un mécanisme de gestion de clés adapté au contexte du réseau mobile Ad hoc est primordial ; mais réaliser un tel mécanisme constitue un vrai défi.

2.2.3 Intégrité

Ce service assure que le trafic de la source à la destination n'a pas été altéré ou modifié sans autorisation préalable pendant sa transmission. C'est la protection contre les menaces qui peuvent causer la modification non autorisée de la configuration du système ou des données. Les services d'intégrité visent à assurer le bon fonctionnement des ressources et la transmission. Ces services assurent une protection contre la modification délibérée ou accidentelle et non autorisée des fonctions du système (intégrité du système) et de l'information (intégrité des données). Dans le réseau sans fil, le message peut être modifié pour des raisons non malicieuses, telles que la corruption du paquet au niveau de la propagation radio. Cependant, le risque qu'un nœud malicieux modifie

le paquet est toujours présent. En fait, ce service peut être appliqué de manière indirecte avec des protocoles de sécurité qui assurent la confidentialité ou l'authentification.

2.2.4 Non-répudiation

la non-répudiation est la possibilité de vérifier que l'émetteur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message. Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues. En d'autres termes, la non-répudiation permet de garantir qu'une transaction (émission/réception/action) ne puisse pas être niée. Cela est très pratique pour détecter et isoler les nœuds compromis. N'importe quel nœud qui reçoit un message (paquet) erroné peut accuser l'émetteur avec une preuve et cela permet de convaincre d'autres nœuds de la compromission du nœud émetteur. Généralement, la non-répudiation peut être atteinte seulement en utilisant la technologie du certificat numérique. En effet, cette technologie permet de prouver l'identité d'une personne qui possède sa propre clé privée.

2.2.5 Autres services de sécurité

Nous définissons d'autres paramètres de sécurité utilisée dans l'analyse des aspects de sécurité réseau mobiles Ad hoc qui sont les suivants :

Disponibilité : la disponibilité consiste à assurer la continuité du service fourni par un nœud même en présence d'une attaque. En d'autres termes, les nœuds doivent assurer la continuité des services réseau quelle que soit l'attaque de déni de service. Pour cela, la protection contre les menaces qui peuvent causer la perturbation des fonctions du réseau est nécessaire pour assurer à tous les nœuds l'accès aux ressources réseau comme le routage, l'accès aux données, etc . . .

Autorisation d'accès : un utilisateur ou un nœud autorisé à utiliser un service doit posséder un certificat ou une référence de l'autorité de certification (un tiers de confiance). Cette référence spécifie les privilèges et les autorisations associés avec l'utilisateur ou le nœud.

Contrôle d'accès : le contrôle d'accès détermine la méthode et la politique qui permettent à un utilisateur ou à un nœud d'accéder aux données ou services. Seuls les nœuds autorisés peuvent former, détruire, rejoindre ou quitter un groupe (cluster). Parmi les approches de contrôle d'accès, nous pouvons citer :

- Contrôle d'accès discrétionnaire (DAC) : cette approche permet aux utilisateurs (nœuds) de définir eux-mêmes la politique de contrôle d'accès.
- Contrôle d'accès mandataire (MAC) : cette approche introduit un mécanisme de contrôle d'accès centralisé avec une politique d'autorisation formelle bien définie.
- Contrôle d'accès basé sur des rôles : cette approche introduit le concept de rôles pour autoriser l'accès.

Gestion des clés : la gestion des clés est un élément très important pour assurer la sécurité des nœuds dans les réseaux mobiles Ad hoc contre les attaques passives comme l'écoute clandestine via des chiffrements. Pour que les nœuds puissent utiliser le mécanisme de chiffrement, il faut soit un partage des clés, soit un échange des clés publiques au préalable. Les mécanismes de gestion des clés existants pour les réseaux classiques filaires ou sans fil avec infrastructure ne peuvent pas être directement utilisés pour les réseaux mobiles Ad hoc car ils ne prennent pas en compte les caractéristiques de ces réseaux. Pour mettre en place un système de gestion des clés dans un réseau mobile Ad hoc, il faut répondre à trois principales fonctions :

- Comment établir une relation de confiance entre les différents éléments du réseau ? Pour répondre à cette question, il faut développer un modèle de confiance.
- Utiliser la cryptographie à clé publique, qui offre un niveau de sécurité avantageux, mais ce crypto-système est lourd et consomme des ressources non négligeables en comparaison avec la cryptographie symétrique ou à clé secrète. Quel est le compromis entre consommation des ressources et niveau de sécurité ?
- Quel est l'élément qui permet de générer des clés pour d'autres éléments du réseau et quel est le type de clé généré ?

Anonymat : L'anonymat permet d'assurer l'absence de lien entre l'identité réseau d'un nœud qui peut être : adresse MAC ou IP et l'identité de l'utilisateur ou le rôle d'un nœud dans le réseau. Cela consiste à assurer la sécurité des nœuds sensibles, dont le rôle est crucial pour le bon fonctionnement de réseau, ou l'identité de l'utilisateur qui peut être la cible d'une attaque.

Position/Emplacement privé(e) : La position d'un nœud dans le réseau peut être considéré comme une information sensible. Rendre cette information publique peut permettre à un attaquant de localiser la cible qu'il veut éliminer. Pour augmenter le niveau de sécurité du réseau, la position ou l'emplacement des nœuds, surtout ceux dont le rôle est sensible, doit être privé(e) ou confidentiel(le). Ainsi, les protocoles de routage, par exemple, doivent prendre en considération cette vulnérabilité et garder cette information confidentielle. Comme exemple de vulnérabilité lié à cette information de l'emplacement des nœuds c'est le domaine militaire particulièrement la communication dans un champ de bataille. La position des soldats ou de l'agent de commandement militaire doit être confidentielle et hautement sécurisée car la divulgation de cette information permet à l'ennemi de cibler les points sensibles de l'adversaire pour gagner la bataille.

Complexité de calcul faible : La plupart des terminaux dans les réseaux mobiles Ad-hoc sont équipés d'une batterie dont la capacité de calcul est limitée. Par conséquent, les protocoles de sécurité ainsi que les algorithmes de chiffrement doivent être adaptés à cette contrainte.

Auto-stabilisation : Un protocole de routage dans un réseau mobile Ad hoc doit être capable de détecter des anomalies et de reprendre le fonctionnement normal du protocole sans intervention humaine. N'importe quel protocole destiné aux réseaux mobiles Ad hoc doit être capable de s'auto-organiser et d'assurer la continuité du service quelle que soit la situation, sans lourde intervention.

Tolérance aux pannes : Le principe de tolérance aux pannes permet à un système de fonctionner avec la présence d'attaquants ou de possibles pannes. Si un attaquant veut affecter le bon fonctionnement du réseau dans le but de créer un déni de service, l'attaque sera détectée avec le protocole tolérant aux pannes et le service de reprise après pannes est enclenché pour réduire l'impact de l'attaque et assurer la continuité du service. Ce principe est très important pour la phase de réaction contre les attaques, dans le but de les isoler et de réduire leur impact.

Relations de confiance : Dans le cas où le niveau de sécurité physique est faible et où la relation de confiance entre les nœuds est dynamique, la probabilité d'avoir un problème de sécurité augmente rapidement. Si un certain nombre de nœuds de confiance est compromis, cela risque de compromettre tous les modèles de confiance. Construire des liens de confiance au début n'est pas une tâche difficile, mais maintenir ces liens de confiance et supporter les changements dynamiques des liens est un vrai défi.

2.3 Classification des attaques dans les réseaux mobiles Ad hoc

Nous avons classé les attaques dans les réseaux mobiles Ad-hoc selon plusieurs critères, tels que l'objectif de l'attaque, son intelligence, son impact, sa source, sa localisation, etc . . .

Objectif de l'attaque : Souvent, l'objectif de l'attaque a une relation avec le profil de l'attaquant. Nous distinguons deux types d'attaquants : l'attaquant rationnel et l'attaquant irrationnel. L'attaquant rationnel prépare son attaque dans le but de tirer un bénéfice direct ou indirect des résultats de cette attaque. Nous pouvons citer divers objectifs d'attaques :

- Augmentation des performances réseau (ex. bande passante) de l'attaquant et obtention de plus de ressources avec un coût (énergie) minimum. Ce profil d'attaque est connu sous le nom de comportement égoïste (Kyasanur et Vaidya, 2005; A.-A. Cardenas et Baras, 2004; S. Buchegger, 2002).
- Violation de l'intégrité des informations décisives pour déterminer le niveau de confiance des nœuds. Le changement de la métrique de réputation de l'attaquant a pour but d'augmenter le niveau de confiance de l'attaquant et de perturber le bon fonctionnement du modèle de confiance (Michiardi et Molva, 2002).
- Violation de la politique de sécurité dans le réseau dans le but de perturber le bon fonctionnement du service réseau (Guang et al., 2008; Buttyan et Hubaux, 2003; M. Cagalj et Hubaux, 2003).

Cependant, l'objectif d'un attaquant irrationnel est juste de perturber les différents services réseau sans tirer de profit ou de bénéfice de ses attaques. Ce type de profil d'attaquant est connu sous le nom de comportement malicieux. Parmi ces attaques, nous pouvons citer les attaques de type Déni de Services tel que le « jamming » (W. Xu, 2005).

Intelligence de l'attaque : l'attaque peut être basée sur une ou plusieurs couche(s) du modèle OSI. A titre d'exemple, nous pouvons citer l'attaque de type « jamming », qui est basée sur la couche physique (W. Xu, 2005). Parmi les attaques qui touchent la couche

MAC, nous pouvons citer la violation de l'algorithme BEB (Binary Exponential Backoff) (IEEE802-11, 1999), et en particulier la manipulation non autorisée de ses paramètres ainsi que d'autres paramètres d'IEEE 802.11 tels que SIFS, DIFS, EIFS, etc ... (Guang et al., 2008). D'autres attaques se focalisent sur les paquets de contrôle comme les paquets RTS (Request-To-Send) et CTS (Clear-To-Send) pour créer une situation de blocage et perturber la politique d'accès au canal (Ray et al., 2003; S. Ray, 2007). En outre, il existe des attaques basées sur les faux paquets ACK et qui consistent à créer une fausse validation d'un paquet DATA (Rachedi et Benslimane, 2008b). La couche réseau n'est pas épargnée par les attaques. La plupart des attaques basées sur cette couche exploitent la faiblesse des algorithmes de routage. Nous pouvons citer quelques attaques, comme l'attaque connue sous le nom du trou noir (Black Hole) et qui consiste à intercepter les paquets via la proposition d'un faux plus court chemin (M. Al-Shurman, 2004). Une autre attaque connue sous le nom de Worm Hole (tunneling) nécessite une coordination entre deux ou plusieurs attaquants dans le but de créer un tunnel et d'intercepter le trafic (Y.-C. Hu, 2003). De plus, plusieurs attaques s'inscrivent dans l'objectif d'empoisonner la table de routage et de perturber le routage dans le réseau (R. P. Sam et Reddy, 2007). Dans la couche transport du modèle OSI, nous trouvons d'autres catégories d'attaques qui consistent à créer un déni de service. Nous pouvons citer par exemple le vol de session TCP, connu sous le nom de « TCP hijacking » (B. Guha, 1997) : l'idée est de bénéficier d'un service sans passer par la phase d'authentification. Une autre attaque de type déni de service connue sous le nom de « SYN Flooding » (X. Bin, 2005) consiste à épuiser les ressources du serveur dans le but de créer un déni de service. Les autres couches supérieures sont aussi affectées par des attaques. Cependant, les attaques les plus redoutables et les plus difficiles à détecter sont les attaques de type inter-couches « cross-layers attacks » (Radosavac et al., 2004; Baras et Radosavac, 2004; L. Guang et Benslimane, 2006) : l'idée de cette attaque est de lancer une attaque basée sur une couche du modèle OSI, mais la répercussion de cette attaque se produit sur une autre couche.

Impact de l'attaque : Une attaque peut avoir un impact passif qui ne nécessite aucune transmission de paquet ou injection d'information dans le réseau. Un attaquant peut se limiter à la capture du trafic réseau pour l'analyser et extraire des informations sensibles. Cette attaque est connue sous le nom du « sniffing attaque » (Z. Trabelsi et Frikha, 2004). Un autre type d'impact, appelé actif, est un résultat des attaques dites actives. Souvent, des attaques actives sont précédées par des attaques passives. Contrairement aux attaques passives, les attaques actives nécessitent d'injecter de l'information dans le réseau et/ou d'interagir avec d'autres nœuds dans le réseau. Nous pouvons citer quelques attaques actives telles que « sleep deprivation » (M. Pirretti et Brooks, 2005), qui consiste à faire travailler inutilement la victime de manière permanente dans le but d'épuiser sa batterie. Une autre attaque active connue sous le nom de débordement de la taille de la table de routage « Routing table overflow » (L. Zhe et Ye, 2005), consiste à créer des routes pour des nœuds qui n'existent pas.

Source de l'attaque : La source de l'attaque est un paramètre important pour les mécanismes de défense. Dans cette classe d'attaques, nous distinguons trois types d'attaques :

- One vs. one : Un seul attaquant cible de manière directe ou indirecte une seule victime.
- Many vs. one : Cette attaque nécessite une collaboration entre deux ou plusieurs attaquants dans le but de cibler une seule victime.
- One vs. many : Dans cette attaque, l'attaquant cible plusieurs victimes. Nous pouvons par exemple citer les attaques de diffusion de type multicast.
- Many vs. many : Plusieurs attaquants collaborent pour attaquer plusieurs victimes. C'est le cas des attaques de type « Worm hole » (Y.-C. Hu, 2003).
- One vs. all : Dans cette attaque, l'attaquant ne cible pas la victime mais lance l'attaque contre tous les nœuds (ses voisins ou d'autres). Cette attaque s'inscrit dans le type des attaques par diffusion aveugle.

Localisation de l'attaque : un nœud attaquant peut lancer son attaque en fonction de la position de la cible dans le réseau. Dans les réseaux mobiles Ad hoc, la position des nœuds dans le réseau a un rôle très important pour déterminer les rôles et les services offerts par chaque nœud. Ainsi, les nœuds n'ont pas le même degré d'importance dans le réseau, ce qui implique qu'un attaquant peut identifier ces nœuds et lancer des attaques dans le but de les mettre hors service. Par exemple, un nœud dont la position est primordiale pour assurer la connectivité du réseau peut être la cible de l'attaquant qui cherche à isoler un segment du réseau. Ce type d'attaques est connu sous le nom de « location disclosure ».

Attaques militaires : Un des domaines d'application des réseaux mobiles Ad hoc est l'application militaire, en particulier dans les champs de bataille. La plupart des attaques dans l'environnement militaire se focalisent sur les attaques de type routage. Nous distinguons deux types d'attaques de routage : attaques stratégiques et attaques tactiques.

- *Attaques de routage stratégiques :* ces attaques consistent à détruire le réseau de l'ennemi pour préparer la bataille. Pour cela, rassembler les informations du réseau et déterminer les relations entre les nœuds est nécessaire pour en déduire le rôle de chaque nœud dans le réseau et déterminer qui commande ou contrôle la prochaine opération. Cette attaque peut être réalisée via des attaques passives.
- *Attaques de routage tactiques :* Ces attaques sont actives et opérationnelles pendant la bataille. Elles utilisent les informations collectées auparavant pour en déduire la topologie du réseau et les différentes relations entre les nœuds. L'idée principale est de paralyser le coeur du réseau via des attaques de type déni de services.

2.4 Domaine de sécurité dans les réseaux mobiles Ad hoc

Il est clair que le problème de la sécurité dans les réseaux mobiles Ad hoc est large et qu'il n'existe pas de solution générale. Il est aussi clair que les différentes applications des réseaux mobiles Ad hoc n'ont pas les mêmes besoins en sécurité. Parmi les axes de recherche dans ce domaine nous pouvons en citer quelques-uns :

- *Gestion de la confiance et des clés :* De nombreux objectifs en terme de sécurité peuvent être atteints en utilisant les mécanismes cryptographiques. Les méca-

nismes cryptographiques, quant à eux, dépendent d'une bonne gestion des clés cryptographiques. Les travaux de Zhou et Haas (Zhou et Haas, 1999) et Capkun et Cie (Capkun et al., 2002) traitaient de ce sujet, et en particulier de la distribution de clés publiques basée sur les certificats dans les réseaux mobiles Ad-hoc.

- *Opération de routage sécurisée et détection d'intrusions :* Les protocoles de routage Ad-hoc existants, tels que le DSR (David B. Johnson et Broch, 2001) ou l'AODV (Charles E. Perkins et Chakeres, 2003), sont vulnérables à divers types d'attaques. Il est relativement simple d'injecter de faux messages de routage ou de modifier les messages légitimes, dans le but d'affecter lourdement l'activité du réseau (e.g. en créant des boucles ou en déconnectant le réseau). Les travaux de Haas et Zhou (Zhou et Haas, 1999), Hu et Cie (Hu et al., 2002) et Sanzgiri et Cie (Sanzgiri et al., 2005b) proposent de sécuriser les protocoles de routage Ad-hoc pour résister à divers types d'attaques. L'approche de Castelluccia et Yi (C. Castelluccia et Yi, 2007) suggére d'utiliser des identifiants basés sur la cryptographie pour sécuriser les protocoles de routage Ad-hoc. Enfin, le travail de Zhang et Lee (Zhang et Lee, 2000), se focalise sur la question de la détection des intrusions dans les réseaux Ad-hoc.
- *Disponibilité :* Cette axe traite le problème d'indisponibilité du service, dû soit à des attaques de type déni de service intentionnelles, soit à l'égoïsme des nœuds. L'égoïsme est un nouveau problème qui se produit en particulier dans le contexte des réseaux Ad-hoc, où les nœuds appartiennent à de multiples domaines administratifs. Dans ces réseaux, les nœuds risquent d'avoir tendance à refuser de fournir des services pour le bienfait des autres nœuds, dans le but de préserver leurs propres ressources (e.g., la puissance énergétique de la batterie). Le papier de Vaidya et Kyasanur (Kyasanur et Vaidya, 2005) traite du problème de l'avidité (une forme d'égoïsme) au niveau de la couche MAC, tandis que les travaux de Molva et Cie (Michiardi et Molva, 2002), Buchegger et Cie (S. Buchegger, 2002) et de Buttyán et Cie (Buttyan et Hubaux, 2003) traitaient de l'égoïsme dans le contexte de la transmission de paquets.
- *Protocoles cryptographiques :* Les solutions traditionnelles de gestion des clés ne sont pas toujours applicables pour les réseaux Ad-hoc ; de même, des solutions existant pour d'autres services de sécurité de niveau plus élevé doivent aussi être retravaillées. Comme exemple, on peut citer l'échange équitable, connu pour être impossible sans la présence d'une troisième partie confidente. Ainsi, son implémentation peut s'avérer problématique dans un réseau Ad-hoc sans infrastructure. Les travaux de Vaudenay et Cie (Avoine et Vaudenay, 2004) et Buttyán et Cie (Levente Buttyán, 2001) traitent de ce problème en proposant des concepts qui fournissent des garanties plus faibles que la véritable équité, mais peuvent être implémentés dans les réseaux Ad-hoc.

2.5 Sécurité inter-couches dans les réseaux mobiles Ad hoc

La sécurité de la communication au sein des réseaux mobiles Ad hoc (MANETs) dépend des relations de confiance entre les nœuds. L'idée de confiance signifie que les

nœuds doivent totalement coopérer entre eux pour assurer des mécanismes d'établissement de chemin corrects, la protection des informations de routage et sécuriser la transmission de paquets. Auparavant, les travaux de recherche étaient principalement centrés sur la sécurité des mécanismes de routage Ad hoc (M. Cagalj et Hubaux, 2003; B. Awerbuch et Rubens, 2002; Y.-C. Hu, 2003), en utilisant la cryptographie ; c'est par exemple le cas des protocoles Ariadne, SEAD et ARAN (Hu et al., 2002; Y.-C. Hu et Perrig, 2002; Sanzgiri et al., 2005b). Cependant, des travaux de recherche récents montraient un intérêt grandissant pour l'étude de la sécurité du contrôle d'accès au médium (MAC) et de ses impacts sur la performance du réseau.

2.5.1 Architecture de sécurité inter-couches

Les solutions inter-couches dans les réseaux mobiles Ad hoc sont essentiellement utilisées dans le but d'améliorer la qualité de service de ces réseaux (Toumpis et Goldsmith, 2003). D'après nos connaissances, il n'existe aucune étude majeure traitant de la sécurité et utilisant l'approche inter-couches pour éviter le déni de service (DoS) ou le comportement avide. Dans cette perspective, nous avons développé de nouveaux axes de recherche dans ce domaine, pour montrer le bénéfice qui peut être tiré de l'utilisation d'une approche inter-couches pour améliorer les détections d'attaques et développer un nouveau mécanisme de réaction (Rachedi et Benslimane, 2007)(Rachedi et Benslimane, 2008c)(Rachedi et Benslimane, 2008b).

Ce concept inter-couches utilise trois couches : les couches physiques, MAC et de routage. La couche physique est seulement utilisée pour détecter des anomalies dans la consommation d'énergie, tandis que la couche MAC est utilisée pour détecter les attaques de type déni de service (DoS) ou les comportements avides. Les mécanismes de détection classiques sont fondés sur une seule couche. Ainsi, il est plus facile pour un attaquant de déjouer le système de détection. Utiliser le système de détection sur plusieurs niveaux rend la tricherie plus difficile. C'est pourquoi nous avons étudié, dans la thèse, une approche inter-couches. Cette approche devrait aussi permettre de réagir lorsqu'une attaque est détectée. Pour réagir à la suite d'une attaque, la couche de routage est utilisée.

Les auteurs dans (L. Guang et Benslimane, 2006) ont montré une nouvelle vulnérabilité exploitable basée sur la technologie IEEE 802.11. Un nœud qui se comporte mal et met en place ce type d'attaques suit complètement les spécificités de la norme IEEE 802.11 et les protocoles de routage sur demande existants, e.g. AODV et DSR. Cependant, il peut causer des attaques de court-circuit au niveau de la couche de routage ou des attaques de détour. Ainsi, le PSD (mécanisme de prévention contre les attaques de détour et les courts-circuits) a été détaillé pour prévenir ce type d'attaques. Le PSD contient deux phases :

1. sélection aléatoire de paquets de routage avec un intervalle de temps défini par les informations de la couche MAC.
2. délai aléatoire des paquets de routage au niveau de la couche de routage.

Cependant, ce travail ne se focalise pas sur les vulnérabilités liées aux paquets de contrôle (RTS, CTS et ACK). Un autre travail proposé par Ray et Cie (S. Ray, 2007) (Ray et al., 2003) traite uniquement des vulnérabilités des paquets de contrôle RTS (Request to Send). Contrairement aux travaux existant déjà dans la littérature, dans notre thèse, nous présentons des nouvelles vulnérabilités basées sur les paquets de contrôle CTS et ACK (Rachedi et Benslimane, 2008b)(Rachedi et Benslimane, 2008a). Des solutions pour remédier à ces vulnérabilités sont analysées et évaluées via des simulations.

2.5.2 Mécanisme de détection

En l'absence de tout système de détection des nœuds se comportant mal, les effets du mauvais comportement ont montré qu'ils diminuaient radicalement la performance du réseau (Buchegger et Boudec, 2002b) et produisaient le déni de service (DoS). Dans le but de résoudre ce problème, divers travaux ont déjà tenté de définir une sorte de schémas de « détection d'intrusions locales » pour les réseaux MANETs (S. Marti et Baker, 2000; Buchegger et Boudec, 2002a; A. Patwardhan et Iorga, 2005; Michiardi et Molva, 2002). Ces schémas adoptent seulement une approche commune fondée sur l'utilisation conjointe d'un mécanisme de contrôle et d'un mécanisme de réputation qui sont mis en place dans chaque nœud du réseau. Dans (Afifi, 2007), une étude propose une façon d'adapter le fameux système de détection d'intrusions IDS (Snort) à un environnement de réseau personnel distribué. L'idée est que l'IDS doit être d'abord distribué puis être complètement en phase avec les paramètres de l'utilisateur tels que les profils, les clés, les droits d'accès, etc . . .

2.5.3 Mécanisme de surveillance

Le mécanisme de contrôle ou de surveillance est défini comme l'ensemble des actions qui sont utiles pour surveiller le comportement des nœuds. Ces actions dépendent des services que l'on veut surveiller (routage, authentification, intégrité, etc . . .). Un principe du mécanisme de surveillance pour les réseaux mobiles Ad hoc a été initialement proposé dans (S. Marti et Baker, 2000), avec sa technique propore au mécanisme Watchdog. Ce mécanisme repose sur le mode de fonctionnement en promiscuité des cartes 802.11, qui permet à un nœud A dans la portée de transmission du nœud B d'écouter les messages de B, même si ces communications ne concernent pas A directement. Ce mécanisme est le fondement de nombreux autres travaux (Marti et Garcia-Molina, 2005; Buchegger et Boudec, 2002a; X. Xue et BenOthman, 2004), qui ont généralement pour but de détecter le mauvais comportement d'un nœud en prenant en compte la fonction de transmission de la couche de routage : un nœud qui transmet un paquet garde toujours l'emprinte numérique de ce paquet, puis démarre un compte à rebours associé à ce paquet et observe si le nœud situé un saut plus loin transmet correctement le paquet ou pas. L'observation est positive dans le premier cas et négative dans tout autre cas. Un nœud peut soit « contrôler ou surveiller un chemin » (i.e. pour des messages qui passent par lui), soit « contrôler le voisinage » (i.e. pour des messages

qui sont transmis dans son voisinage). Comme la capacité des nœuds risque d'être limitée dans un réseau Ad hoc, le premier mode est préférable pour diminuer la quantité de données stockées, mais risque d'allonger le délai de détection d'un attaquant. Ce schéma de contrôle n'est pas toujours fiable : un nœud qui se comporte mal risque de ne pas être détecté si une collision ambiguë a lieu au niveau du nœud surveillant, ou encore si le nœud surveillé limite sa puissance de transmission afin que le message atteigne le nœud surveillant mais pas le nœud récepteur, etc ... Ces problèmes peuvent être atténués si la métrique de réputation est tolérante, dans une certaine mesure, aux fausses observations.

Un autre point problématique est que la plupart des travaux existants basent leurs observations sur un identifiant comme l'adresse MAC qui peut être modifiée (par un attaquant) : si un attaquant A surveillé par un nœud honnête B, prend la forme de C, B risque d'attribuer un niveau de réputation incorrect à C. Ainsi, les observations doivent être authentifiées. En outre, contrairement à la plupart des travaux existants qui ne réalisent des observations qu'au niveau de la couche réseau, dans cette thèse, nous proposons d'étendre les observations à d'autres couches.

Dans la thèse, contrairement au mécanisme Watchdog, j'ai proposé un modèle de surveillance inter-couches pour réduire le taux du faux positif et d'améliorer l'observation du nœuds surveillant. Un modèle probabiliste est proposé avec la prise en compte des paramètres de la couche physique et MAC au niveau de la couche routage (Rachedi et Benslimane, 2007)(Rachedi et Benslimane, 2008c).

2.5.4 Mécanismes de réputation

Au-delà des exemples cités précédemment, il existe de nombreuses autres métriques de réputation ; certaines sont définies pour jouer un rôle d'ordre général dans la sécurité (T. Beth et Klein, 1994), d'autres dans le contexte similaire du système point-à-point (P2P) (Marti et Garcia-Molina, 2005). Un cadre d'évaluation général doit être défini dans le but de tester ces métriques existantes dans le contexte des réseaux mobiles Ad hoc. Le mécanisme de détection proposé sera d'abord simulé pour vérifier qu'il ne dégrade pas trop les performances du réseau. Les observations qui en découlent seront ensuite données comme entrées pour un mécanisme de réputation qui fournit un rang aux nœuds, dans le but de distinguer un nœud malicieux ou se comportant mal d'un nœud ordinaire. Ces rangs représentent les niveaux de confiance estimés par le nœud surveillant lorsqu'il observe les nœuds en prenant en compte une certaine fonction. Lorsque ce rang est inférieur à un certain seuil, le nœud est considéré comme un nœud se comportant mal. Selon les travaux, différentes métriques de réputation sont prises en compte ; certaines se focalisent sur le comportement égoïste et ne considèrent que l'observation personnelle (Michiardi et Molva, 2002), d'autres autorisent les recommandations, i.e. les rangs effectués par d'autres nœuds (de confiance) (X. Xue et BenOthman, 2004). Dans le dernier cas, il faut assurer la validité de la recommandation avec un certain mécanisme d'intégrité.

Les paramètres du protocole MAC peuvent être utilisés comme un outil pour dé-

tecter les nœuds égoïstes. En effet, ces paramètres de configuration sont la taille de la fenêtre de Backoff, la durée des espaces entre les trames (Interframe), le nombre de retransmissions, le niveau de coopération (pourcentage de transmission). Les auteurs dans (Kyasanur et Vaidya, 2005) ont étudié le mauvais comportement au niveau de la couche MAC en utilisant les mécanismes de détection et de correction. Tout d'abord, le récepteur décide à la fin d'une transmission (qu'il reçoit de l'émetteur), si l'émetteur risque de s'être détourné du protocole propre à cette transmission. Ensuite, si le récepteur a identifié un détournement de l'émetteur pour une transmission, il ajoute au Backoff suivant une pénalité équivalente à la magnitude du détournement perçu pour cette transmission. Enfin, selon la magnitude du détournement perçu sur plusieurs transmissions de l'émetteur, le récepteur identifie les émetteurs qui se comportent effectivement mal. Les problèmes de cette solution sont la modification du protocole IEEE MAC et le contrôle qui est donné au récepteur.

Les approches de détection d'intrusions sont fondées sur la détection d'un profil correct qui correspond aux activités autorisées qui respectent la spécificité du protocole le plus longtemps possible. L'identification de l'intrusion est basée sur l'observation des déviations du profil calculé. D'autre part, les modifications ne sont pas dépendantes de la disponibilité d'un profil de comportement correct à long terme (lorsque la topologie, les conditions du canal et les modèles de trafic sont dynamiques, un tel profil risque de ne pas être exact).

Comme mentionné dans (Michiardi et Molva, 2002), la détection des manipulations du Backoff est un des plus grands défis. En raison du caractère aléatoire introduit dans le choix du Backoff, il est difficile de détecter si un nœud a choisi de petites valeurs de Backoff par hasard ou non. Le travail (Lazos et Poovendran, 2004) se focalise sur la prévention et la détection des manipulations du mécanisme de Backoff par les nœuds égoïstes dans 802.11. Les auteurs proposent d'abord un algorithme pour assurer des Backoffs honnêtes si au moins l'émetteur ou le récepteur est honnête. Ils étudient ensuite les algorithmes de détection pour traiter du problème de collision avec les nœuds égoïstes.

Dans le but de diminuer le nombre d'attaques intelligentes citées ci-dessus et qui manipulent le Backoff, les auteurs, dans (Guang et al., 2008), ont présenté une nouvelle méthode d'accès, le PRB (Backoff aléatoire prévisible). Le PRB est fondé sur des modifications mineures du BEB (Backoff exponentiel binaire) 802.11 et force chaque nœud à générer un intervalle de Backoff prévisible ; l'idée clé est d'ajuster, de façon prévisible, la borne inférieure de la fenêtre de contention (CW) dans le but d'améliorer l'équité par station dans les environnements égoïstes. Les hôtes qui ne suivent pas l'opération du PRB sont ainsi faciles à détecter et isoler.

L'objectif des systèmes de réputation de type inter-couches consiste à utiliser les paramètres de configuration du protocole MAC pour détecter les nœuds qui trichent. En effet, chaque nœud doit évaluer ses performances (nombre de collisions, débit, délai, etc ...) en temps réel et les comparer à celles d'une configuration testée au préalable. Les informations de la couche MAC sont nécessaires pour corriger l'observation au niveau de la couche réseau. Le mécanisme de détection doit être capable de différencier

le nœud qui ne peut pas bien se comporter de celui qui ne veut pas bien se comporter. Cette différenciation est l'un des objectifs de la thèse. Dans (Masmoudi, 2008), les auteurs ont étudiés un nouveau système P2P distribué et fondé sur la réputation, basé sur l'histoire. Il utilise quelques caractéristiques de confiance connues dans certains outils d'Internet tels qu'Ebay et Kazaa. La confiance se construit avec l'expérience de l'ancien comportement. Ce comportement est calculé et on lui accorde des points en fonction des règles de comportement.

2.5.5 Mécanismes de réaction en faveur de la sécurité

L'architecture de réseau en couches a été la clé de l'énorme succès et de l'utilisation étendue d'Internet, ainsi que du développement initial des systèmes sans fil. Cependant, il devient de plus en plus clair que l'optimisation au sein des couches est insuffisante pour obtenir les gains de performance nécessaires pour alimenter la croissance majeure des services sans fil de la prochaine génération. Pour atteindre ces gains de performance, il est impératif que les protocoles et les concepts de réseau soient implémentés par l'optimisation inter-couches. L'idée est qu'en optimisant jointement le contrôle d'au moins deux couches, des solutions inter-couches peuvent fortement améliorer la performance en exploitant l'étroite connexion entre les couches dans les systèmes sans fil. Par exemple, la couche physique (PHY) peut transmettre à la couche réseau des informations dont elle pourra conclure quels sont les meilleurs chemins à prendre. De même, la couche MAC peut envoyer des informations à la couche réseau pour assurer la préservation d'énergie ou d'autres aspects importants. Nous nous intéressons à l'utilisation de l'approche inter-couches pour assurer la sécurité. Il n'existe que peu d'études qui ont été menées pour assurer la sécurité dans les réseaux sans fil avec infrastructure (WLANs) avec un concept inter-couches. Nous citerons des travaux liés à quelques solutions inter-couches proposées pour améliorer l'efficacité de la sécurité dans les réseaux sans fil. Dans (Baras et Radosavac, 2004) et (A.-A. Cardenas, 2004), les auteurs présentent une approche inter-couche qui a pour objectif de détecter les intrusions, de minimiser le temps de détection et le nombre de fausses alarmes, tout en maximisant la probabilité de détection. Cette étude est fondée sur deux idées principales :

- Risque d'attaques de type déni de service (DoS) au niveau de la couche MAC
- Risque de causer une attaque en manipulant le trafic au niveau de la couche MAC et de propager l'attaque à la couche réseau.

Ainsi, ils en concluent que les couches MAC et réseau doivent davantage interagir. La couche MAC doit transmettre les informations à la couche réseau dans le cas de surcharge, de sorte que le routage décide de nouveaux chemins non affectés par la surcharge de trafic. Le système de détection d'intrusions (IDS) assure que les nouveaux chemins ne contiennent pas de nœuds malicieux. Les principales questions sont les suivantes : Combien de temps un nœud peut-il rester malicieux sans être détecté ? Quels sont les paramètres MAC et de routage nécessaires pour avoir un mécanisme de détection d'intrusions inter-couches efficace ? Les auteurs utilisent la classification des nœuds en trois catégories : nœuds normaux, nœuds se comportant mal et nœuds malicieux. L'interaction se fera entre les couches MAC et réseau et l'IDS dans un concept

inter-couches. La couche de routage envoie divers chemins possibles à la couche MAC. La couche MAC utilise les informations locales et d'autres de la couche PHY pour délivrer le résultat à la couche réseau (le résultat sera un sous-groupe des chemins envoyés par la couche de routage). Les couches MAC et réseau consultent l'IDS, si nécessaire, pour une détection globale avant de choisir les chemins à emprunter.

Dans (Lazos et Poovendran, 2004), les auteurs traitent du problème de diffusion multicast sécurisée dans un environnement sans fil limité en énergie. Ils se sont focalisés sur la gestion des clés et soulignent qu'elle est dépendante de la topologie du réseau et de la méthode de distribution adoptée. Ils ont introduit un concept inter-couches pour la gestion des clés dans la multi-distribution sans fil, qui distribue des clés cryptographiques pour valider les membres du groupe de façon efficace en terme d'énergie. En ce qui concerne les couches physique et réseau, ils ont formulé un problème d'optimisation pour minimiser l'énergie nécessaire à la retransmission des clés. Les auteurs trouvent que la solution optimale ne convient pas à la taille des groupes multi-distribution et proposent un algorithme moins optimal, inter-couches et peu complexe pour une distribution de clés efficace en terme d'énergie. Ils présentent les résultats de simulation qui montrent les gains en énergie avec leur concept et comparent ses performances lorsque divers algorithmes de routage sont utilisés.

2.6 Conclusion

Nous avons présenté dans ce chapitre les différentes caractéristiques des réseaux mobiles Ad hoc, ainsi que leur domaine d'application et la technologie de la couche MAC 802.11. De plus, nous avons détaillé les besoins en sécurité dans ces réseaux. Une classification des attaques est proposée. En outre, nous avons discuté des différents domaines de recherche liés à la sécurité dans les réseaux mobiles Ad hoc. Ensuite, nous avons présenté les différents travaux en relation avec la sécurité dans les réseaux mobiles Ad hoc, en particulier les architectures et les mécanismes de sécurité (surveillance, détection, réputation et réaction). Nous avons axé notre travail sur l'architecture hiérarchique distribuée pour établir une infrastructure à clé publique et sur les mécanismes de surveillance et de détection de type inter-couches. A partir des travaux dèjà effectués, nous proposons dans la thèse une architecture hiérarchique distribuée qui supporte la topologie dynamique du réseau et qui supprime le point de vulnérabilité au niveau de l'autorité de certification (CA), ce qui nous procure une avance sur les approches existantes. De plus, nous avons amélioré le mécanisme de surveillance de type inter-couches en réduisant le taux de faux positifs. Ce mécanisme permet également d'entretenir correctement le modèle de confiance. Enfin, de nouvelles vulnérabilités au niveau de la couche MAC ont été identifiées et résolues.

Chapitre 3

Architecture Hiérarchique Distribuée Sécurisée

Sommaire

Dans ce chapitre, nous présentons une nouvelle architecture distribuée pour sécuriser les réseaux mobiles Ad hoc. Cette architecture est basée sur un modèle de confiance, qui permet d'attribuer un niveau de confiance aux nœuds selon leur comportement dans le réseau. Cette architecture consiste à diviser le réseau sous forme de groupes interconnectés entre eux. Chaque groupe contient au moins deux nœuds de confiance dont un joue le rôle de chef de groupe. L'idée principale est d'établir une infrastructure distribuée à clé publique (PKI) dans chaque groupe. La certification des clés publiques des nœuds est assurée par le chef de groupe. Pour éviter des attaques de type déni de service (DoS) au niveau des chefs de groupe, nous avons introduit un nouveau concept : zone dynamique démilitarisée ($DDMZ$: Dynamic Dimilitarized Zone). La $DDMZ$ est formée par des nœuds sacrifiables qui possèdent un niveau de confiance

élevé. Ces nœuds jouent le rôle d'intermédiaires entre le chef de groupe et les nœuds ayant un faible niveau de confiance. En outre, nous proposons un modèle probabiliste pour définir la connectivité directe qui existe entre les nœuds de confiance, dans le but d'étudier le degré de résistance de la $DDMZ$ contre différents types d'attaques. De plus, nous évaluons la robustesse et la disponibilité de la $DDMZ$ et analysons les effets de la connectivité directe et de la portée de transmission sur la stabilité et la sécurité au sein du réseau.

3.1 Introduction

Les réseaux mobiles Ad hoc sont formés de deux ou plusieurs nœuds mobiles capables de communiquer entre eux via des liens sans fil, sans infrastructure pré-deployée et sans aucune unité de contrôle centralisée. Ainsi, elle constitue une topologie dynamique. Ces caractéristiques rendent ces réseaux sophistiqués et capables d'opérer dans des conditions difficiles, mais aussi vulnérables aux différents problèmes de sécurité, comme la gestion des clés de chiffrement, la distribution des certificats, la gestion de confiance entre les nœuds, la coopération, etc ...
Les solutions de sécurité doivent proposer certains services de base, tels que l'authentification, l'intégrité, la confidentialité, la disponibilité et la non-répudiation. La majorité des solutions de sécurité proposées dans la littérature sont basées sur la cryptographie symétrique (Hu et al., 2002)(Perrig et al., 2002) ou asymétrique (S. Yi, 2003; Capkun et al., 2002; C. Satizabal, 2007). Mais le problème majeur de ces solutions dans l'environnement des réseaux mobiles Ad hoc est la gestion et la distribution des clés de chiffrement. Proposer une seule autorité de certification (CA) pour tout le réseau n'est pas une solution souhaitable car cette conception est vulnérable aux attaques de type déni de service (DoS) sur le CA. Le protocole $ARAN$ (Authenticated Routing for Ad hoc Networks) (Sanzgiri et al., 2005b) utilise une seule CA pour tout le réseau ; si le nœud CA est compromis, tout le réseau sera compromis. Cette solution n'est pas souhaitable, et n'est pas non plus adaptée à la dynamique de la topologie du réseau.

Dans ce chapitre, nous proposons une nouvelle architecture hiérarchique distribuée (Rachedi et Benslimane, 2006) pour développer les systèmes dynamiques de gestion de clés adaptés aux caractéristiques des réseaux mobiles Ad hoc. En effet, les architectures de sécurité existantes destinées aux réseaux mobiles Ad hoc telles que les architectures proposées par Bechler et Cie (Bechler et al., 2004), Dong et Cie (Y. Dong, 2007), Yi et Cie (S. Yi, 2003) ne prennent pas en compte toutes les caractéristiques de ces réseaux. Souvent, la topologie dynamique n'est pas supportée et l'absence d'un modèle de confiance dynamique fragilise les liens de confiance entre les nœuds. De plus, contrairement aux réseaux avec infrastructure, une architecture de sécurité centralisée n'est pas souhaitée dans les réseaux mobiles Ad hoc. Ceci nous mène à une architecture distribuée. En outre, la distribution des rôles importants dans le réseau tels que l'autorité de certification (CA) est souvent basée sur les mécanismes de cryptographie lourds comme la cryptographie à seuil (Shamir, 1995). Tous les nœuds dans le réseau n'ont pas la même importance, ce qui nous oblige à mettre en place une hiérarchisation des rôles dans le

réseau. C'est pourquoi dans notre nouvelle architecture distribuée hiérarchique, nous apportons des améliorations pour rendre la solution mieux adaptée au contexte des réseaux mobiles Ad hoc.

Les nouvelles contributions que nous avons apportées avec notre proposition d'architecture sont les suivantes :

- Introduction d'un modèle de confiance distribué dynamique capable de fixer des niveaux de confiance propres à chaque rôle dans le réseau.
- Division du réseau sous forme de groupes et élection d'un nœud chef de groupe (qui joue le rôle de l'autorité de certification).
- Introduction d'un nouveau concept ($DDMZ$) pour sécuriser le chef de groupe.
- Proposition d'un modèle probabiliste pour étudier la connectivité entre les nœuds de confiance et évaluer la robustesse de notre architecture hiérarchique distribuée (Rachedi et al., 2007).
- Analyse de sécurité et étude comparative de notre architecture et des architectures proposées dans la littérature.

Le reste de ce chapitre est organisé comme suit : dans la section 3.2, nous présentons notre positionnement bibliographique en ce qui concerne la distribution de l'autorité de certification (CA) dans les réseaux mobiles Ad hoc. La section suivante 3.3 est dédiée à la description de notre architecture hiérarchique distribuée pour la sécurité des réseaux mobiles Ad hoc. Dans la section 3.4, nous présentons les différents résultats analytiques et de simulations. Ensuite, nous proposons dans la section 3.5 une discussion et une analyse approfondies de notre solution. La section 3.6 présente une étude comparative des différentes solutions qui permettent de distribuer le CA. Enfin, la section 3.7 conclut le chapitre.

3.2 Positionnement bibliographique

Plusieurs travaux dans la littérature proposent des solutions au problème de la sécurité dans les réseaux mobiles Ad hoc. Nous nous intéressons spécialement aux modèles de confiance distribués et à la distribution du rôle de CA (Autorité de Certification) dans un environnement mobile.

L'infrastructure à clé publique appelée PKI (ou ICP en français) (S. Chokhani, 2003) consiste à assurer la sécurité de la communication en générant les services suivants : l'intégrité des données, la confidentialité, l'authentification et la non répudiation. La PKI est basée sur la cryptographie asymétrique et sur le principe de tiers de confiance appelé Autorité de Certification (CA). Le rôle de CA est de signer les clés publiques des nœuds et de générer les certificats numériques pour l'authentification. De plus, le CA attribut un certain niveau de confiance à chaque nœud avant de lui délivrer son certificat. Les certificats numériques permettent l'établissement des relations de confiance entre les acteurs de l'infrastructure à clé publique (PKI). Malheureusement, l'infrastructure à clé publique classique ne peut pas être directement appliquée aux réseaux mobiles Ad hoc, car elle est développée pour des réseaux filaires dont les machines sont bien connectées. Sachant que parmi les caractéristiques des réseaux mobiles Ad hoc

nous pouvons citer le manque d'une entité centrale de contrôle, la topologie du réseau est dynamique et la disponibilité des ressources change fréquemment. Tout cela complique davantage l'introduction de l'infrastructure à clé publique. Les inconvénients d'une introduction directe de la PKI dans le réseau mobile Ad hoc sont les suivants : la sélection d'un seul nœud comme CA pour tout le réseau crée un point de vulnérabilité qui peut être exploité par des attaquants. Si le CA est compromis, tout le réseau devient compromis. De plus, la sécurité du réseau ne peut pas passer à l'échelle et le nœud CA ne peut pas toujours être atteint par tous les nœuds. Cela est dû à la mobilité des nœuds. Cependant, dupliquer la fonctionnalité de l'autorité de certification dans le réseau peut améliorer la disponibilité du service de sécurité mais ne permet pas d'éliminer la vulnérabilité. Si une seule CA est compromise, l'ensemble des CA seront compromises. Plusieurs travaux dans la littérature ont traité le problème d'introduction de la PKI dans les réseaux mobiles Ad hoc. La plupart de ces travaux tentent de surmonter les problèmes d'introduction de la PKI dans les réseaux mobiles Ad hoc via la décentralisation des fonctionnalités de CA et de proposer une approche qui permette une auto-organisation de la PKI. Nous distinguons deux principales classes de décentralisations de CA pour les réseaux mobiles Ad hoc. La première classe est appelée « non auto organisation de la PKI », elle permet de distribuer les fonctionnalités de CA sur plusieurs nœuds via l'utilisation de la cryptographie à seuil (Shamir, 1995). La seconde classe appelée « auto organisation de la PKI » est basée sur le modèle de confiance, comme le principe de PGP (Zimmermann, 1995).

3.2.1 Cryptographie à seuil pour distribuer le CA

L'idée de base consiste à distribuer les fonctionnalités de CA (mais pas la duplication de CA) parmi les différents nœuds du réseau en utilisant l'approche de la cryptographie à seuil. Dans cette approche la clé secrète de CA est divisée en n parties $(S_1, S_2, \ldots, S_n)$ et chaque partie de la clé secrète est attribuée à un certain nœud. Cependant, seuls les nœuds qui possèdent une partie de la clé secrète sont capables de générer un certificat partiel au nœud demandeur. Pour qu'un nœud réussisse à obtenir le certificat final du réseau, il a besoin de collecter au moins k différents certificats partiels ($k < n$). Ainsi, ce schéma est appelé la cryptographie à seuil (n, k). Pour distinguer diverses approches basées sur la cryptographie à seuil dans le but de distribuer le CA, nous nous sommes posé la question suivante : Quels sont les nœuds qui sont capables d'assumer la responsabilité de CA et de générer des certificats partiels ? En d'autres termes, quel nœud est susceptible d'avoir une partie de la clé secrète de CA ? Il existe deux possibilités pour distribuer CA. La première est appelée « distribution partielle de CA » : seuls certains nœuds spécifiques sont capables d'assumer le rôle de CA. La deuxième possibilité est appelée « distribution totale de CA » : tous les nœuds ont la possibilité de jouer le rôle de CA.

A- Distribution partielle de CA : Pour des raisons de sécurité, la distribution de la fonctionnalité de CA est limitée à certains nœuds. Nous citons certains travaux basés sur la distribution partielle de CA tels que : Budakolglu et Gulliver (Budakoglu et Gulliver, 2004). Ils ont proposé un système qui permet de distribuer le CA sur cer-

tains nœuds spécifiques avec plusieurs niveaux de cryptographie à seuil, dans le but de proposer une sélection flexible des nœuds avec le niveau de sécurité souhaité. Ce système assure la tolérance aux pannes et la gestion hiérarchique des clés. Dans un autre travail, Yi et Kravets (S. Yi, 2003) ont proposé un système appelé MOCA (Mobile Certification Authority). Ce système sélectionne les nœuds les plus sûrs pour assurer les fonctionnalités de CA. Ils sont appelés les nœuds MOCA. Les nœuds MOCA utilisent la cryptographie à seuil pour partager leurs fonctionnalités et augmenter la disponibilité des services de sécurité dans le réseau. Lorsqu'un nœud veut rejoindre le réseau, il commence par envoyer au moins k demandes de certification (CREQ) aux différents nœuds MOCA. Chaque nœud MOCA reçoit le CREQ, il va répondre par CREP (Certification Reply) qui contient le certificat partiel. Le nœud demandeur obtient son certificat final signé par le CA de tout le réseau une fois qu'il a reçu les k différents certificats partiels de la part des nœuds MOCA. Dong et Cie (Y. Dong, 2007) proposent la distribution des services de CA en utilisant la cryptographie à seuil ainsi que l'introduction du concept de groupage (clustering). Le service de CA est assuré par le concept de groupage et un protocole dynamique pour partager les clés est proposé. Cependant, le mécanisme de cryptographie à seuil est lourd et nécessite l'intervention d'un tiers pour fragmenter la clé secrète et la distribuer. Un autre travail basé sur le concept de groupage pour distribuer le CA est proposé par Bechler et Cie (Bechler et al., 2004). C'est une architecture qui utilise le schéma de la cryptographie à seuil (k, n) pour distribuer le CA. L'idée consiste à distribuer la clé privée de CA sur les chefs de groupe appelés (cluster-heads : CHs). Chaque CH possède un fragment de la clé privée de CA. Si un nœud visiteur veut certifier sa clé publique et obtenir son certificat, il doit avoir au moins un certain nombre (w) de certificats générés par les nœuds garants. Une fois que les certificats des garants sont rassemblés, le nœud visiteur doit demander au moins k autres certificats aux CHs pour avoir le certificat final du réseau. Le nombre k représente ce n'est que le paramètre de la cryptographie à seuil. Cependant, le nombre w est le seuil de garanti nécessaire pour la génération d'un certificat par le nœud chef de groupe (CA). Les inconvénients de cette architecture sont les suivants : premièrement, cette approche n'est pas réaliste, car les nœuds garants n'ont pas d'information sur les nœuds visiteurs qui sont généralement de nouveaux arrivants dans le réseau (pas d'historique sur ces nœuds). Deuxièmement, même si le nœud visiteur a réussi à rassembler les w certificats que lui apporte le garant, il ne peut pas avoir son certificat final car il lui faut k autres certificats partiels des CHs pour obtenir son certificat final. Troisièmement, le trafic réseau généré par chaque nœud qui veut obtenir son nouveau certificat est au moins égal à $2 * (w + k)$ paquets. Un autre inconvénient se présente dans le cas de la fusion de plusieurs réseaux pour déterminer la clé secrète de la nouvelle CA du réseau fusionné. Or, le mélange des clés secrètes n'est pas possible, donc une seule clé est considérée comme la clé secrète du nouveau réseau et est appelée « la clé dominante ». Cette clé est sélectionnée en fonction du nombre de groupes (clusters) dans le réseau. La clé de CA du réseau qui possède le plus grand nombre de groupes devient la nouvelle clé de CA de tous les réseaux fusionnés. Cette procédure présente une vulnérabilité, car dans cette architecture, n'importe quel nœud peut former son propre cluster. Par conséquent, un ensemble de nœuds malicieux peuvent former un réseau avec le nombre maximum de groupes (clusters) dans le but de prendre le contrôle de CA une fois qu'ils auront

fusionné avec le réseau victime.

B- Distribution totale de CA : Kong et Cie (Kong et al., 2001) proposent une approche basée sur la distribution de la clé privée de CA sur un ensemble de coalitions de nœuds. Chaque coalition a au moins k nœuds qui sont tous situés l'un à portée de l'autre. Lorsqu'un nouveau nœud veut obtenir son certificat, il va diffuser une requête à un seul saut pour obtenir les k certificats. Si le nœud n'a pas reçu les k certificats après un certain temps limite, il doit se déplacer à une autre position. Le problème avec cette approche est la supposition qu'au moins k nœuds voisins, l'un à la portée de l'autre, existent toujours : cela est jugé irréaliste.

Malheureusement, le schéma non auto-organisé de la PKI basé sur la cryptographie à seuil (k, n) a certains inconvénients : premièrement, les n nœuds doivent être initialisés par une autorité de confiance qui est responsable de l'introduction des clés secrètes partielles de CA. En d'autres termes, une administration externe est nécessaire pour configurer le système et établir l'architecture. Deuxièmement, le nombre k doit assurer le compromis entre la robustesse et la disponibilité du système. Troisièmement, ce mécanisme surcharge le réseau, car au lieu d'envoyer une seule requête pour obtenir le certificat, il faut envoyer au moins k demandes de certificats. Pour conclure cette partie, nous pouvons dire que toute proposition doit prendre en compte les caractéristiques des réseaux mobiles Ad hoc.

3.2.2 Auto-organisation pour distribuer le CA

Un réseau mobile Ad hoc est complètement auto-organisé du point de vue de la sécurité, si et seulement s'il n'a aucune infrastructure, aucun serveur centralisé et aucun secret partagé. L'approche PGP (Pretty Good Privacy) (Zimmermann, 1995) est la plus répandue dans la PKI auto-organisée sur Internet. Le principe de cette approche est que tout utilisateur puisse certifier (signer) la clé publique d'un autre utilisateur s'il lui fait confiance. L'ensemble des signatures générées par les uns et les autres forme des relations de confiance entre les entités du réseau. A la base, PGP est développé pour établir des relations de confiance dans le Web mais il n'est pas développé pour supporter les caractéristiques des réseaux mobiles Ad hoc. Cependant, la nature distribuée du modèle PGP le rend favorable et il pourrait être introduit dans les réseaux mobiles Ad hoc. Le modèle PGP est vulnérable aux intrusions des nœuds malicieux. Par exemple, supposons que le nœud A fasse confiance au nœud B ; si le nœud B est compromis, alors il peut introduire plusieurs nœuds malicieux en signant leurs clés publiques et en générant des certificats. Par conséquent, tous les nœuds qui font confiance au nœud B vont faire confiance aux nœuds malicieux introduits par le nœud B, car la relation de confiance est transitive dans le cas du modèle PGP. Parmi les approches auto-organisées qui existent pour distribuer le CA basé sur le modèle PGP et adaptées au réseaux mobiles Ad hoc, nous citons la proposition du Hubaux et Cie (Capkun et al., 2002). Dans cette proposition, le nœud sauvegarde et distribue les clés lui-même contrairement au cas du PGP où la distribution des clés nécessite un serveur en ligne. Dans cette approche, chaque utilisateur maintient un répertoire de certificats. Si deux nœuds veulent

vérifier la clé publique de l'autre, ils vont chercher dans leur répertoire de certificats dans le but de trouver une chaîne de confiance vers l'un ou l'autre. Si la chaîne de confiance est trouvée, alors le nœud peut faire confiance à l'autre nœud. La réussite de cette approche dépend de la construction du répertoire de certificats et des caractéristiques du graphe de certification. Ce système présente aussi deux algorithmes pour former un arbre de certification dans chaque nœud et construire les répertoires de certificat. Ces algorithmes ont pour but de faciliter la recherche des certificats dans le répertoire. L'inconvénient de cette approche est la supposition que la relation de confiance est transitive ; alors, le système devient vulnérable à l'intrusion des nœuds malicieux. Dans un autre travail, Satizabal et Cie (C. Satizabal, 2007) ont proposé une extension de l'approche de Hubaux et Cie (Capkun et al., 2002) pour simplifier la procédure de découverte du chemin de certification. Les auteurs ont présenté un protocole pour établir une hiérarchie virtuelle entre les nœuds dans le réseau. Cependant, l'inconvénient majeur avec le modèle hiérarchique est la création d'un point de vulnérabilité au niveau du nœud avec le niveau de confiance le plus élevé. Par conséquent, si la clé privée de ce nœud est compromise, toute la PKI devient compromise.

Pour remédier aux problèmes cités ci-dessus, nous avons proposé une architecture qui s'inscrit dans cette catégorie de distribution de CA (Rachedi et Benslimane, 2006). Notre architecture est basée sur un modèle de confiance et sur le concept de groupage (clustering) pour former des groupes. Dans chaque groupe, nous avons introduit la PKI dont le CA est le chef de groupe. Si les conditions de formation de groupes ne sont pas favorables, alors notre architecture fonctionne comme le modèle PGP. C'est pour cela que nous avons introduit la notion de communauté de confiance. Cette communauté est formée par des nœuds dits de confiance (car il existe entre eux une relation de confiance). Le rôle de la communauté de confiance est d'auto-organiser la sécurité dans le réseau via l'établissement de la PKI dans chaque groupe du réseau. Le second concept que nous avons proposé est appelé la zone dynamique démilitarisé ($DDMZ$: Dynamic Demilitarized Zone). Cette zone est formée par l'ensemble des nœuds de confiance situés à un seul saut de CA du groupe. Donc, le but principal de la $DDMZ$ est de protéger le nœud qui joue le rôle de CA et d'éviter le point de vulnérabilité au niveau de CA.

3.3 Architecture hiérarchique distribuée

Nous proposons une architecture hiérarchique distribuée qui divise le réseau en groupes pour sécuriser le réseau. Ainsi, nous définissons un modèle de confiance pour assigner différents rôles, tels que les rôles d'autorité de certification (CA) et d'autorité d'enregistrement (RA) au sein de chaque groupe. Nous proposons également l'algorithme sécurisé de groupage distribué (SDCA) pour diviser le réseau en un certain nombre de groupes. De plus, nous introduisons le nouveau concept de $DDMZ$ pour sécuriser le nœud CA dans chaque groupe. Une zone $DDMZ$ est une zone intermédiaire déployée entre des nœuds inconnus et le nœud CA dans chaque groupe. Elle est constituée d'un ensemble de nœuds de confiance. L'un d'entre eux assure le rôle de

nœud CA, et au moins un autre a le rôle de nœud RA. Le nœud CA peut communiquer directement (1 saut) avec les nœuds RA. La communication est chiffrée puisque les nœuds de confiance connaissent leurs clés publiques au préalable. Les caractéristiques de cette architecture sont les suivantes :

1. Le système n'a besoin d'aucun tiers de confiance central. Ce système est dynamiquement adapté à tout changement de topologie.
2. 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.
3. La stabilité de la gestion des clés publiques dépend de la stabilité du groupe.

3.3.1 Modèle de confiance

Nous supposons que les nœuds de confiance se connaissent entre eux. Aussi, chaque nœud possède une paire de clés privées/publiques. Initialement, les nœuds de confiance se connaissent entre eux (l'identité et la clé publique) et sont considérés comme des nœuds honnêtes qui ne doivent pas générer de faux certificats.
Dans notre modèle de confiance, nous introduisons une nouvelle métrique de confiance (Tm) dans l'intervalle $[0..1]$. Chaque nœud de confiance possède une métrique $Tm = 1$. Un nœud (i) peut avoir la métrique de confiance la plus élevée $(Tm(i) = 1)$, s'il est connu par d'autres nœuds de confiance et a échangé les clés via un canal sécurisé (par exemple, rencontre physique) (Capkun et al., 2002) avec un ou plusieurs nœuds de confiance. Une métrique de confiance très élevée existe aussi si le nœud a prouvé sa coopération et son bon comportement. 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 leur liste de nœuds de confiance. Chaque nouveau nœud visiteur (inconnu) doit commencer par une faible métrique de confiance $(Tm = 0.1)$. Cependant, le nœud sans certificat (sans statut) sa métrique de confiance est nulle $(Tm = 0)$.

Nous définissons cinq rôles différents dans chaque cluster. Chaque rôle nécessite une valeur de métrique de confiance particulière.

1. CA_k : autorité de certification du groupe k, qui certifie les clés publiques des nœuds appartenant au même groupe. Le CA_k a la métrique de confiance la plus élevée $(Tm(k) = 1)$.
2. $RA_{i,k}$: autorité d'enregistrement du groupe k, assurée par le nœud de confiance (i) avec $Tm(i) = 1$. Le but principal du RA est de protéger le CA contre les différents types d'attaques (tels que le déni de service).
3. $VN_{i,k}$: nœud visiteur (i) qui appartient au groupe (k) et qui possède la plus faible métrique de confiance $Tm(i) \in [0.1, B_{Vsup}]$. La borne B_{Vsup} dépend de résultat de la phase de surveillance du nouveau nœud et du niveau de sécurité souhaité. Le nœud (i) ne peut pas communiquer à l'extérieur du groupe (k).
4. $MN_{i,k}$: nœud membre (i), qui appartient au groupe (k). Il possède une métrique de confiance moyenne $Tm(i) \in [B_{Minf}, B_{Msup}]$ où $B_{Minf} > B_{Vsup}$. Le nœud (i)

peut communiquer dans le groupe (k) et à l'extérieur du groupe. Le choix des bornes inférieure (B_{Minf}) et surppérieure (B_{Msup}) dépend de la politique de sécurité adoptée dans le groupe.

5. $GW_{i,j}$: nœud passerelle (g), qui assure la connexion entre deux différents groupes (i) et (j). Les nœuds passerelles doivent être certifiés par au moins deux CA et leur $Tm(g) \in [B_{Ginf} - 1.0]$ où $B_{Ginf} \geq B_{Msup}$. Sachant que le choix de la valeur B_{Ginf} dépend du niveau de sécurité souhaité.

La figure 3.1 ci-dessous montre le diagramme de transition d'un rôle à un autre. La transition entres les différents statuts est basée sur le comportement des nœuds et sur leur coopération, sauf pour le statut CA, qui nécessite une élection par les nœuds de confiance.

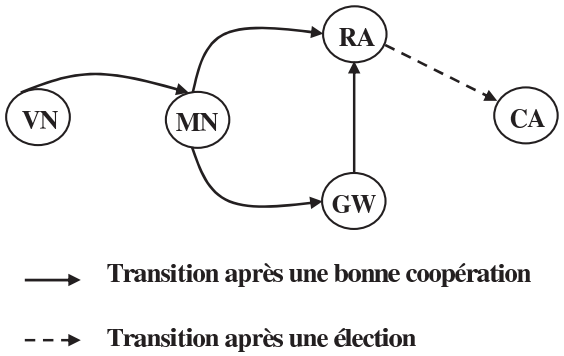


FIG. *3.1* – *Diagramme de transition d'état*

A- Monitoring

Pour assurer les transitions entre les statuts, un processus de monitoring est ajouté pour superviser le comportement des nœuds. Chaque nœud avec une certaine métrique de confiance peut surveiller ses voisins qui disposent de métriques de confiance inférieures à la sienne. La figure 3.2 montre la possibilité qu'ont les nœuds qui possèdent un certain statut de surveiller les nœuds ayant un statut inférieur. Le nœud avec le sta-

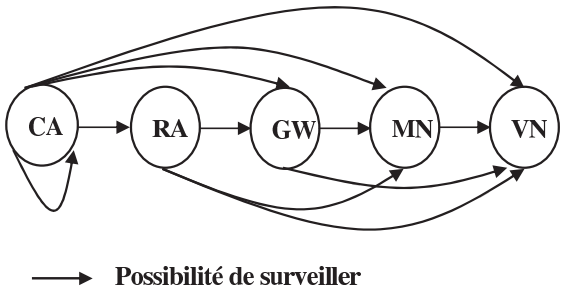


FIG. *3.2* – *Schéma de monitoring*

tut CA peut surveiller tous les autres nœuds, même les nœuds qui possèdent le même

statut que lui (CA). Les nœuds qui possèdent le statut RA peuvent surveiller les nœuds $\{GW, MN, VN\}$. De même, les nœuds avec le statut GW peuvent surveiller les statuts $\{MN, VN\}$. Enfin, les nœuds avec le statut MN ne peuvent surveiller que les nœuds de statut VN, mais les nœuds dont le statut est VN ne peuvent surveiller aucun statut.

Dans le modèle de confiance que nous proposons, la relation de confiance entre les clusters est assurée par les nœuds qui possèdent le statut CA. Un nœud CA peut recommander à un autre CA un noeud qui appartient à son cluster et qui possède un certain niveau de confiance. Les nœuds avec le statut RA peuvent recommander des nœuds au CA.

B- Chemin de confiance

La confiance d'un chemin dans le réseau dépend de la chaîne de confiance qui forme le chemin. Par exemple, la communication entre les clusters est basée sur l'évaluation du chemin de confiance entre les nœuds CA. La valeur du niveau de confiance entre deux nœuds est le plus faible niveau de confiance des deux. Par exemple, si les niveaux de confiance des nœuds A et B sont $Tm(a)$ et $Tm(b)$ respectivement, alors le niveau de confiance du lien A-B est $min(Tm(a), Tm(b))$. Le niveau de confiance d'une chaîne constituée de plusieurs liens est le produit des niveaux de confiance des liens. La figure 3.3 montre deux exemples (a) et (b) pour évaluer les chaînes de confiance (TC). Nous paramétrons le modéle de confiance comme suit : $B_{Ginf} = 0.7$, $B_{Minf} = 0.5$ et $B_{Msup} = 0.7$. Nous remarquons que $TC(a) \leq TC(b)$, car $\{V_1 \times V_2 \times V_2'\} \leq \{V_1' \times V_1''\}$ et la taille du chemin dans l'exemple (b) est plus petite que dans l'exemple (a). De plus, le fait d'avoir un nœud avec une faible métrique de confiance dans le chemin diminue le niveau de confiance du chemin.

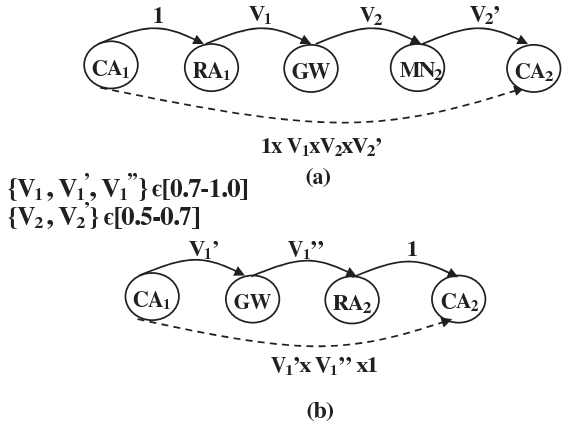


FIG. 3.3 – *Exemples des chaînes de confiance*

Pour sécuriser le nœud CA du groupe, nous proposons un nouveau concept que nous appelons $DDMZ$.

C- DDMZ (Dynamic Demilitarized Zone)

La $DDMZ$ est définie comme une zone située à un saut du nœud CA. Elle est formée par au moins un nœud de confiance, et plus précisément avec un statut RA. Le but de la $DDMZ$ est de filtrer les communications entre le nœud CA et les autres nœuds (dont la métrique de confiance est faible). Tous les nœuds visiteurs doivent passer par la $DDMZ$ pour demander leur certificat.
La figure 3.4 montre un exemple de DDMZ composée de deux nœuds RA {2,4}, dans un cluster de taille 2 (2 sauts). Le nœud (3), dont le statut est visiteur, ne peut pas communiquer directement avec le nœud CA (1). Il doit passer par la $DDMZ$, et plus exactement par le nœud (4).

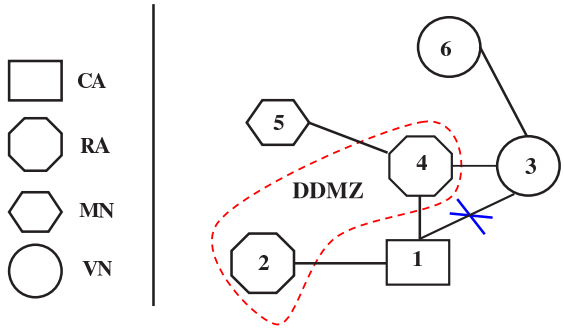


FIG. *3.4* – *Exemples d'un cluster avec la DDMZ*

3.3.2 Algorithme distribué d'élection sécurisée (ADES)

Pour élire les nœuds CA, nous proposons un algorithme sécurisé d'élection, dont les règles principales sont les suivantes :

1. Seuls les nœuds de confiance (Tm(i)=1) peuvent être candidats au statut CA.
2. Chaque chef de groupe est le CA d'un seul groupe.
3. Tous les nœuds de confiance voisins du nœud CA peuvent devenir RA dans le groupe.
4. Les nœuds qui appartiennent au groupe doivent être à (d) sauts du nœud CA, (d) étant la taille du groupe à définir.

Notre algorithme est basé sur l'émission périodique des paquets balises par les nœuds de confiance vers leurs voisins à chaque période de temps pré-définie. Chaque paquet balise contient les informations nécessaires à 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 métrique de confiance. Seuls les nœuds (i) avec $Tm(i) = 1$ et au moins un nœud de confiance comme voisin direct 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 et augmenter

la disponibilité de la $DDMZ$ du groupe, l'algorithme sélectionne le candidat qui a le 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 (Gerla et Tsai, 1995) : l'idée consiste à sélectionner le nœud dont l'identité est la plus petite. Connectivité maximal (Max-connectivity) permet de sélectionner le nœud dont le degré de connectivité est le plus élevé (Chiang et al., 1997). Dans notre algorithme, nous avons adopté la métrique de mobilité comme paramètre de stabilité (Basu et al., 2001), car cette métrique donne de bons résultats comparée à $Lowest - ID$ et $Max - connectivity$ (jusqu'à 33% de réduction du nombre de changements de chefs de groupe, ce qui réduit le coût de l'énergie).

La métrique de mobilité est basée sur la variation du niveau de puissance du signal à la réception sur chaque nœud ($RxPr$), ce qui nous donne une indication sur la distance dans le cas d'un espace libre sans obstacle ($FRiiS$). C'est un indicatif de distance relative entre les nœuds émetteurs et récepteurs. Le ratio $RxPr$ entre les transmissions de deux paquets successifs donne une connaissance sur la mobilité relative entre deux nœuds voisins X et Y (Basu et al., 2001).

$$RM_Y^{\text{rel}}(X) = 10 \log_{10} \frac{RxPr_{X \to Y}^{\text{new}}}{RxPr_{X \to Y}^{\text{old}}} \tag{3.1}$$

Le calcul de la mobilité relative d'un nœud Y par rapport à ses (m) voisins, consiste à calculer la variance de l'ensemble de la mobilité relative RM_Y^{rel} de ses voisins X_i

$$RM_Y = \text{var}(RM_Y^{\text{rel}}(X_1), RM_Y^{\text{rel}}(X_2), \cdots, RM_Y^{\text{rel}}(X_m)) \tag{3.2}$$

Une faible valeur de RM_Y indique que Y est moins mobile que ses voisins. Par contre, une grand 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 d'élection qui contient les informations suivantes :

- ID du candidat : l'identité du nœud candidat au rôle de CA.
- Hop-Count : nombre de sauts vers le nœud CA.
- DTN : Degré de confiance, c'est le nombre de nœuds de confiance voisins du nœud candidat.
- RM : la mobilité relative, pour indiquer la stabilité du nœud candidat par rapport à ses voisins.
- ID-num : c'est le numéro de séquence du paquet qui est incrémenté par un à chaque nouveau paquet balise transmis par le candidat.
- MAC (Message Authenticated Code) : il sert à authentifier le paquet balise et à vérifier l'intégrité de ses informations. Le nœud candidat doit utiliser sa clé privée pour générer le MAC du paquet balise.

$$(MAC_{K-}[CA, Hopcount, DTN, RM, ID - num])$$

Initialement, chaque nœud de confiance envoie deux paquets "hello" successivement pour calculer la mobilité relative RM. Puis, il annonce sa candidature au rôle de CA, en générant son propre paquet balise d'élection. Quand les nœuds de confiance reçoivent des paquets balises de la part de leurs voisins, ils exécutent notre algorithme d'élection et de formation de groupe pour définir leur statut : CA (leader de groupe), RA ou juste membre du groupe. La décision dépend des paramètres de sécurité et de stabilité. Lorsqu'il y a compétition entre deux candidats, le nœud qui possède le nombre de nœuds de confiance voisins le plus petit et la mobilité relative la plus élevée perd la compétition et devient soit RA soit MN, en fonction du nombre de sauts qui le séparent du nœud qui a gagné l'élection. Si c'est un nœud situé entre deux groupes adjacents alors il peut devenir passerelle (GW) a condition qu'il possède une certaine métrique de confiance.
L'algorithme 1 ci-dessous est exécuté par chaque nœud de confiance (Tm=1) à la réception d'un paquet balise dont le nombre de sauts est inférieur à (d) (taille du cluster).

Algorithm 1: Algorithme d'élection

```
Quand le nœud (j) reçoit un paquet balise du nœud (i);
begin
    Authentication do if (Tm(i)! = 1) then
    RejectBeacon() ; Goto(end);
    else if (HopCount >= d) then
        No − Competition ; Goto(end);
    else if (RM_i < RM_j) OR ((RM_i == RM_j) AND (DTN_j < DTN_i)) then
        Accepter le nœud (i) comme CA;
        if (HopCount == 1) then
            Status(j) = RA;
            HopCount(i) = 1;
        else
            HopCount(i) = HopCount + 1;
            Status(j) = MN;
    else if (RM_j < RM_i) OR (DTN_j > DTN_i) then
        Le nœud (j) reste candidat au CA;
    else if (RM_i == RM_j) AND (DTN_j == DTN_i) then
        Exécuter Lowest-ID ;
end
```

L'algorithme 2 est exécuté lors de détection de changement de topologie. Le déplacement du nœud CA est détecté par ses voisins de confiance. Si les nœuds RA ne reçoivent pas les paquets balises pendant un temps pré-défini (calculé en fonction du timeout d'un paquet balise et la période de diffusion de ces paquets), cela implique que le nœud CA n'est plus disponible. Aussi, les nœuds du groupe peuvent détecter la mobilité des nœuds RA, lorsqu'ils ne reçoivent aucun paquet balise en provenance de ces

nœuds. La mobilité des nœuds CA et RA est très importante pour la durée de vie du groupe et sa stabilité. Chaque nœud appartenant au groupe avec un statut autre que

Algorithm 2: Algorithme exécuté par le nœud si ses RA ou CA ne sont plus disponibles

```
Si le nœud (i) ne reçoit pas de paquet balise de CA après un certain temps
pré-défini;
begin
    if , il peut atteindre le CA avec un autre RA then
    Garder le CA actuel;
    Mettre à jour le nœud RA et Hopcount;
    else if Il peut trouver un autre CA then
        Joindre le nouveau CA;
        if (Tm(i) == 1) then
            if (HopCount == 1) then
                Status(i) = RA_NODE;
                HopCount(newCA) = 1;
            else
                Status(i) = MN;
                HopCount(newCA) = HopCount + 1;
        else
            Demande de certification au nœud RA;
end
```

RA ou CA doit recevoir les paquets balises provenant du nœud CA à chaque période de temps pré-définie. Il doit vérifier l'authentification et l'intégrité de l'information du paquet balise en utilisant la clé publique du CA ($K_{CA}+$). Si la vérification est réussie, alors le nœud récepteur met à jour les changements à propos du nombre de sauts vers le CA (hop-count) ou un nouveau RA.

La figure 3.5 montre le résultat d'un exemple d'élection et de division d'un réseau sous forme de groupes dont la taille est de deux sauts. Les nœuds 2, 4, 5, 7, 8 et 3 sont des nœuds appartenant à un groupe dont le chef est le nœud 1 et joue le rôle de CA. Les nœuds 3, 6, 10 et 11 sont des nœuds appartenant à un groupe dont le CA est le nœud 9. Les nœuds 2 et 4 (resp. 6) sont des nœuds de confiance avec le statut RA, et sont à un seul saut du CA 1 (resp. 9). Le nœud 3 appartient aux deux clusters. Il peut devenir un nœud passerelle, s'il possède une certaine métrique de confiance et doit aussi être certifié par les deux CA. Les nœuds visiteurs comme 5, 8, 7, 10 et 11 ne peuvent pas communiquer directement avec le CA, bien que les nœuds 5 et 10 soient des voisins du CA, car ils doivent passer par la $DDMZ$.

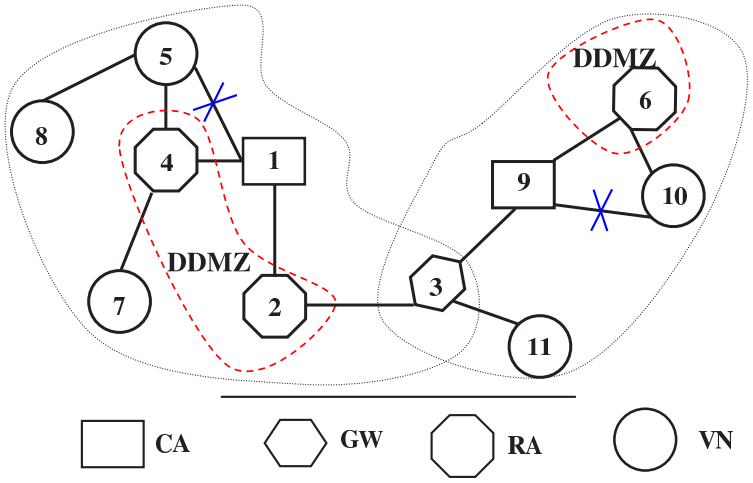


FIG. 3.5 – *Exemple de formation de clusters à deux sauts*

3.3.3 Contrôle des nœuds et gestion des groupes

A- Contrôle des nœuds (monitoring) : 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 faible degré de confiance. 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 (Kyasanur et Vaidya, 2005) : les nœuds égoïstes trichent en choisissant leur backoff, dans le but d'obtenir une bande passante 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 leurs voisins qui ont un degré de confiance faible. Nous ne nous focalisons pas sur le contrôle de la couche MAC.
- La couche réseau : les nœuds chargés du contrôle surveillent les activités de retransmission de paquets de leurs nœuds voisins, qui ont un degré de confiance inférieur. 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 d'observation qui consiste à collecter les informations données par les nœuds pour calculer le niveau de réputation. Soient deux nœuds x et y avec $Tm(x) > Tm(y)$. 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 à acheminer vers une autre destination, et après une période de temps limitée, le nœud x peut calculer le niveau de

réputation :

$$R_2(X,Y) = \frac{\text{Nombre de paquets acheminés}}{\text{Nombre total de paquets}} \tag{3.3}$$

Dans (Rebahi et al., 2005), Rebahi et Cie ont proposé une idée similaire pour calculer le niveau de réputation. La différence entre notre technique de contrôle et celui de Yacine est l'attribution d'un degré de confiance. Dans notre modèle, chaque nœud inconnu commence avec le degré de confiance le plus faible ($Tm = 0.1$) et ce degré augmente au fur et à mesure que le nœud prouve sa coopération et son bon comportement. Ainsi, dans notre approche, nous prenons en compte le degré de confiance des nœuds chargés du contrôle. Les niveaux de réputation générés par les nœuds sont liés au degré de confiance correspondant à chacun d'eux. Telle est la tâche du chef de groupe. Le rapport final du nœud y généré par chaque nœud chargé du contrôle x est le suivant :

$$R(x,y) = \frac{\alpha R_1(x,y) + \beta R_2(x,y)}{\alpha + \beta} \tag{3.4}$$

tel que, α et β représentent les coefficients des rapports au niveau des couches MAC et réseau respectivement. Ces coefficients peuvent être déterminés en fonction de l'importance des paramètres de chaque couche. Par example, le cas de même coefficient pour les deux couches MAC et réseau $\alpha = \beta = 1$.

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. Si un nœud de confiance est situé à un saut du nœud CA, il devient une autorité d'enregistrement (RA). Le rôle du gestionnaire de groupe est d'assurer la sécurité du nœud CA qui génère un certificat pour les membres du groupe. Un ensemble de nœuds RA forme la DDMZ dans le but de protéger le nœud CA contre les attaques, en filtrant les communications entre un nœud inconnu et le nœud CA. La $DDMZ$ utilise le niveau de réputation délivré par le processus de contrôle pour évaluer 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. Lorsque le CA reçoit le rapport d'évaluation de réputation envoyé par les nœuds chargés du contrôle, le calcul du rapport de réputation final de chaque nœud est effectué comme indiqué dans l'équation 3.5. Si le CA reçoit k rapports de la part des nœuds chargés du contrôle pour évaluer le nœud y, nous introduisons une nouvelle formule de calcul :

$$\text{Rapport de Réputation : } RR(y) = \frac{1}{k}\sum_{i=1}^{k} Tm(x_i) \times R(x_i,y) \tag{3.5}$$

Lorsque le nœud CA dispose des 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 (calculé en fonction du niveau de sécurité souhaité), 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 des groupes adjacents de la récidive des nœuds se comportant mal.

3.3.4 Modèle de connectivité de confiance

La connectivité directe entre les nœuds de confiance est un élément important non seulement pour la sécurité des liens, mais aussi pour la sécurité des groupes et de tout le réseau. En effet, l'existence d'un nombre important de liens de connectivité directe entre les nœuds de confiance augmente la probabilité d'avoir une $DDMZ$ robuste, car cette zone est formée par des nœuds de confiance situés à un saut les uns des autres. C'est pourquoi nous proposons un modèle de connectivité de confiance pour évaluer la robustesse de notre architecture et en particulier la $DDMZ$.

L'idée de base consiste à distribuer k nœuds de confiance parmi un nombre total de n nœuds dans le réseau. Ces nœuds de confiance doivent collaborer entre eux pour diviser le réseau en différents groupes et pour assigner les rôles de CA (autorité de certification) et de RA (autorité d'enregistrement) au sein de chaque groupe créé. Ainsi, les règles pour qu'un groupe soit établi sont les suivantes :

- un groupe ne peut pas accepter d'autres nœuds s'il est saturé.
- l'existence d'au moins deux nœuds de confiance qui doivent être directement connectés (reliés) l'un à l'autre.

Dans chaque groupe, le nœud CA et les nœuds de confiance directement reliés les uns aux autres forment la $DDMZ$.

Nous supposons qu'il n'existe aucun obstacle dans la surface de déploiement des nœuds, et que tous les nœuds possèdent le même rayon de transmission R. De plus, la distribution des nœuds est uniforme. Nous pouvons alors écrire la connectivité directe suivante : $\mid Xi - Xj \mid < R$, où X_i désigne la position du nœud (i). Chaque nœud de confiance connaît les clés publiques du chiffrement de tous les nœuds de confiance. Les nœuds inconnus peuvent devenir des nœuds de confiance, mais cela dépend du modèle de confiance ; dans notre architecture sécurisée, le module chargé du contrôle et de la surveillance est responsable de cette tâche. Les n nœuds sont distribués avec un taux d'arrivée qui suit une loi de Poisson afin d'estimer le nombre de nœuds dans un rayon donné. Nous définissons la probabilité qu'un nœud (i) puisse communiquer directement avec un nœud (j) ainsi : $P(R) = Pr\{\mid X_i - X_j \mid \leq R\} = 1 - e^{-\lambda.R}$ Dans notre cas, la probabilité d'avoir (d+1) nœuds de confiance directement connectés entre eux est la suivante :

$$P_d(R) = \prod_{i=1}^{d}(1 - e^{-\lambda.R}) = (1 - e^{-\lambda.R})^d \tag{3.6}$$

Le paramètre d ne peut prendre que des valeurs entières et représente le degré de connectivité directe entre les nœuds de confiance. La probabilité d'avoir un réseau muni d'une forte connectivité dépend du rayon de transmission des nœuds. Plus la portée de transmission est élevée, plus la probabilité d'une forte connectivité sur le réseau est grande.

La probabilité d'avoir deux nœuds (i) et (j) directement connectés entre eux, sachant qu'ils appartiennent à l'ensemble des nœuds de confiance K qui contient $\|K\| = k$ nœuds dans le réseau sur un nombre total de nœuds (de confiance ou non) n, est la suivante : $P = P(R).Pr\{noeud(i) \in K\}.Pr\{noeud(j) \in K \setminus noeud(i) \in K\}$

D'après l'équation 3.6, la probabilité d'avoir $(d+1)$ nœuds directement connectés entre eux, sachant qu'ils appartiennent à l'ensemble des nœuds de confiance $|K| = k$, est la suivante :

$$P_{n,k}(R) = (1 - e^{-\lambda.R})^d . \left\{ \frac{k}{n} . \frac{k-1}{n-1} \cdots \frac{k-d}{n-d} \right\} \tag{3.7}$$

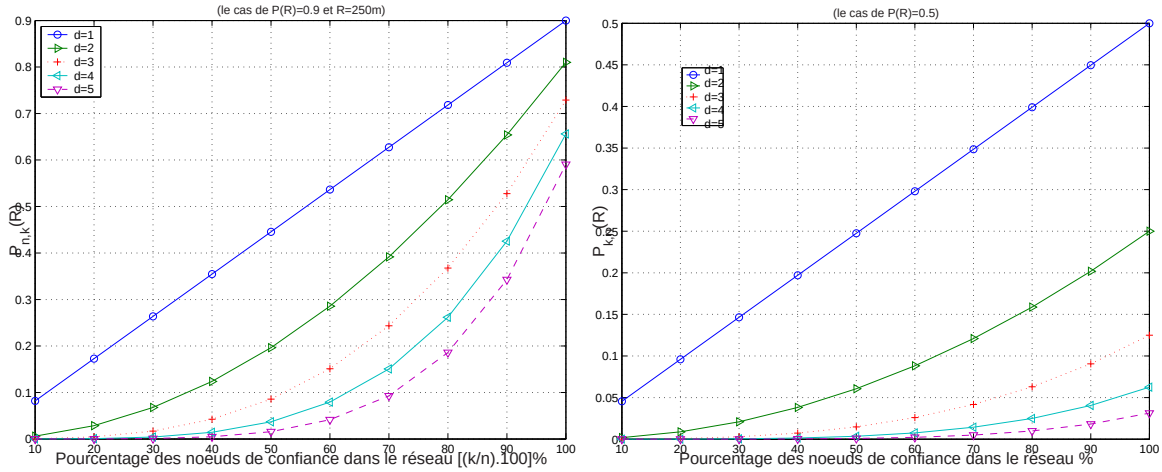
tel que $d < k \leq n$

Dans la $DDMZ$, d est un paramètre qui indique la robustesse et le degré de résistance de la $DDMZ$ contre des attaques telles que le DoS, mais également la disponibilité des services de sécurité, comme par exemple, le filtrage des demandes de certification avant leur transmission au nœud CA.

3.4 Simulation et évaluation de performance

3.4.1 Résultats numériques

Dans cette partie, nous présentons les principaux résultats de simulation du modèle de connectivité sécurisée. Les résultats présentés ci-dessous montrent la probabilité d'avoir des nœuds de confiance directement connectés entre eux, comme l'indique l'équation 6.4. La figure 3.6 montre la probabilité d'avoir des nœuds de confiance directement connectés les uns aux autres avec un degré d en fonction du pourcentage de nœuds de confiance dans le réseau. Les différents cas de probabilité d'avoir deux nœuds directement connectés entre eux $P(R)$ sont présentés. Dans le cas d'une forte probabilité $P(R) = 0.9$, c'est à dire dans le cas d'une grande portée de transmission, les résultats obtenus sont montrés dans la figure 3.6(a). Nous remarquons que plus le pourcentage de nœuds de confiance augmente, plus la probabilité de constituer une DDMZ robuste augmente avec le paramètre d. Les figures 3.6(b) et 3.7 montrent les



(a) Le cas de P(R)=0.9

(b) Le cas de P(R)=0.5

FIG. 3.6 – *Probabilité de former une DDMZ avec un degré d*

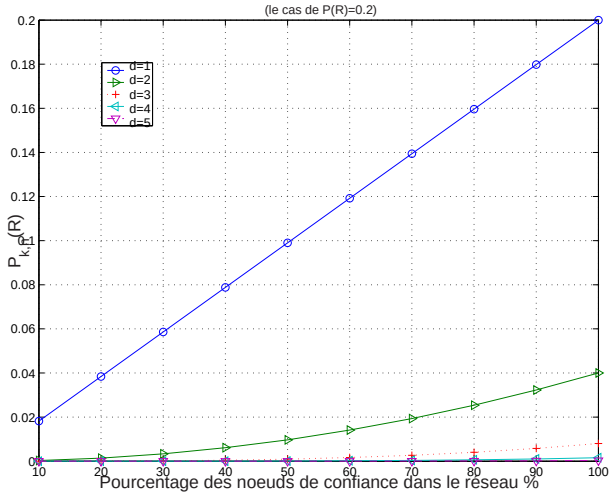


FIG. 3.7 – *Probabilité de former une DDMZ avec un degré d avec* $P(R) = 0.2$

effets de la portée de transmission (une faible connectivité $P(R) \leq 0.5$). Au niveau de la figure 3.6(b), nous étudions les résultats dans le cas où la probabilité d'avoir deux nœuds directement connectés entre eux est égale à 0.5 ($P(R) = 0.5$). Nous remarquons que la probabilité d'avoir des nœuds directement connectés entre eux avec un degré d en fonction du pourcentage de nœuds de confiance dans le réseau diminue par rapport au cas où la probabilité d'une connectivité directe était forte. Alors, la probabilité de constituer une DDMZ diminue. Enfin, la figure 3.7 illustre le cas d'une faible probabilité de connectivité directe ($P(R) = 0.2$). Nous remarquons que la probabilité d'avoir deux nœuds de confiance directement connectés entre eux dépend directement de la probabilité d'avoir deux nœuds directement connectés entre eux ($P(R)$). La probabilité $P(R)$ dépend de la portée de transmission.

3.4.2 Résultats des simulations

Nous avons implémenté nos algorithmes décrits précédemment dans le simulateur réseau ($NS - 2$) (ns 2, 1999). Pour générer le modèle de mobilité, nous avons utilisé CMU pour simuler nos algorithmes. Les scénarios de simulation sont générés avec les paramètres cités dans le tableau 5.3. Les résultats présentent dans cette partie sont des moyennes de 25 scénarios de simulation.

Le déplacement des nœuds est généré aléatoirement (Random waypoint) et de manière continue pendant les simulations.

Afin d'étudier la stabilité de notre algorithme ($ADES$), nous le comparons avec deux autres : $MOBIC$ (Basu et al., 2001) et $Lowest - ID$ (Gerla et Tsai, 1995). Cette comparaison est illustrée dans la figure 3.8. 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

TAB. *3.1* – *Paramètres de simulation*

Parameter	Valeurs
Nombre de nœuds (N)	50
Taille de la surface (mxn)	$670x670m^2$
Vitesse de mobilité	20 m/s
Portée de transmission	10 m - 250 m
Intervalle de diffusion (BI)	0.75-1.25 s
Intervalle de découverte	10*BI s
Période de contention	3.0 s
Temps de simulation	300 s

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 portée 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, nous obtenons moins de groupes que dans le cas de $MOBIC$ et $Lowest - ID$.

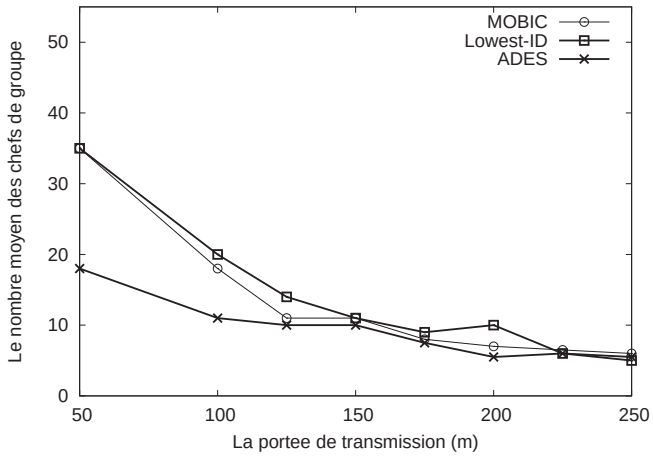


FIG. *3.8* – *Comparaison entre les algorithmes de formation de clusters*

La figure 3.9 montre le nombre moyen de différents statuts des nœuds dans le réseau. Les nœuds isolés sont des nœuds qui ne peuvent rejoindre aucun groupe. Nous remarquons que le nombre moyen de nœuds isolés diminue lorsque la portée de transmission diminue. Les autres statuts de nœuds augmentent quand nous augmentons la portée de transmission. Pour avoir une meilleure configuration afin de sécuriser le réseau, nous devons diminuer le nombre de nœuds isolés, car plus le nombre de nœuds isolés est grand, moins le réseau est sécurisé.

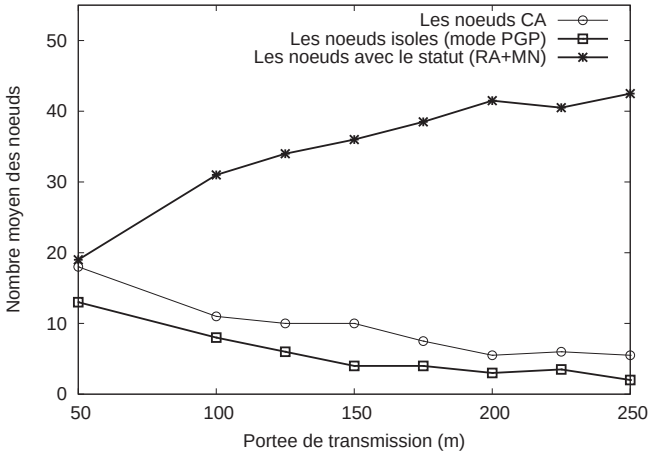


FIG. *3.9* – *Nombre moyen de différents statuts des nœuds*

3.5 Discussion et analyse

La sécurité de l'architecture que nous proposons dépend principalement du modèle de confiance. La présence d'un grand nombre de nœuds de confiance augmente le niveau de sécurité du réseau. Les nœuds avec une faible métrique 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 (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 cours de la phase d'authentification dans l'algorithme 1. Même si les nœuds malicieux réussissent à former leurs groupes et s'ils tentent de communiquer avec d'autres groupes, les nœuds CA des groupes de destination authentifient le nœud CA du groupe source. Enfin, selon le résultat de l'authentification et après l'évaluation de la métrique de confiance, les nœuds CA décident d'accepter ou de rejeter la communication.

L'attaque de type déni de service (DoS) sur le nœud CA est évitée par la DDMZ. Cette dernière consiste à filtrer toutes les requêtes venant des nœuds ayant un faible niveau de sécurité. La robustesse de la $DDMZ$ dépend du nombre de nœuds RA qui collaborent entre eux dans le but de protéger le nœud CA. Si un nœud malicieux tente d'usurper l'identité des nœuds CA ou RA, il sera détecté et isolé par le processus de monitoring. Un nœud malicieux peut usurper l'identité d'un nœud de confiance légitime, s'il réussit à avoir sa clé privée. Pour qu'un nœud malicieux réussisse à compromettre tout le réseau, il doit compromettre tous les nœuds CA.

Le nombre de groupes formés par notre approche est en relation avec le nombre de nœuds de confiance ainsi qu'avec leur mobilité. Si nous avons K nœuds de confiance, le nombre maximum de groupes sera $K/2$ si K est un nombre pair et $(K-1)/2$ si K est impair. La taille du groupe doit être adaptée au nombre de nœuds de confiance pour mieux sécuriser le nœud CA. La présence de deux nœuds de confiance est la configuration minimale pour la formation d'un groupe, mais cette configuration doit

suivre le nombre de nœuds de confiance et le nombre des autres nœuds.
Avec notre architecture, nous pouvons utiliser la cryptographie à seuil dans chaque groupe après l'élection du nœud CA. Ce dernier divise sa clé privée en (n) fragments de clé et l'association de (k) clés génère la clé privée du CA.

L'approche de notre architecture oblige les nœuds à collaborer et à adopter un bon comportement obtenir un niveau de confiance plus élevé. Chaque nœud inconnu doit commencer avec le statut de visiteur dont le niveau de confiance est le plus bas.

Paramètre de qualité d'authentification (QoA) : Dans le but de calculer le niveau de confiance de la procédure d'authentification entre les groupes, nous calculons la qualité d'authentification (QoA). Pour cela, nous appliquons un facteur d'atténuation à la chaîne de confiance (Yi et Kravets, 2004) (Rachedi et Benslimane, 2006). Ce facteur est $(1-p)^{s-1}$, (p) étant la probabilité d'existence d'un nœud compromis ou malicieux et (s) la longueur de la chaîne de confiance.

$$QoA(V_1 - V_2) = TC(V_1 - V_2) * (1-p)^{(s-1)} \tag{3.8}$$

où $TC(V_1 - V_2)$ représente la valeur de confiance de la chaîne entre les nœuds 1 et 2.

Plus la chaîne de confiance est longue, plus le risque d'être compromis est important. Donc, la taille du groupe doit être choisie avec prudence.
La QoA entre deux groupes dépend de la chaîne de confiance (TC) qui relie les deux CAs des groupes et aussi le pourcentage de nœuds malicieux dans le réseau. La communication entre les nœuds CAs doit passer par les chaînes de confiance dont le niveau de confiance est le plus élevé.

La figure 3.10 ci-dessous décrit la qualité d'authentification (QoA) en fonction de la probabilité des nœuds malicieux. Nous avons dessiné les courbes dans le cas d'un groupe de taille 1 ou 2 saut(s) avec un maximum et un minimum pour la valeur de chaîne de confiance de 1 et 0.49 (0.7*0.7) respectivement. Nous remarquons que dans le cas d'un groupe à 1 saut, la QoA décroît linéairement lorsque la probabilité que des nœuds malicieux soient présents est importante. Dans le cas d'un groupe à 2 sauts, nous remarquons que la QoA diminue rapidement comparée au cas d'un groupe à 1 saut.

La figure 3.11 montre le cas général de la QoA avec différentes valeurs de TC et de la probabilité que des nœuds malicieux soient présents. Nous comparons les trois cas de taille de groupe 1, 2 et 3 sauts. Nous remarquons que la meilleure valeur de la QoA est obtenue dans le cas d'un groupe avec un seul saut, avec une faible probabilité que des nœuds malicieux soient présents, et une chaîne de confiance (TC) plus élevée.

D'après les deux dernières figures 3.10 et 3.11, nous pouvons conclure que plus la taille du groupe est grande, plus le risque d'avoir une QoA est faible.

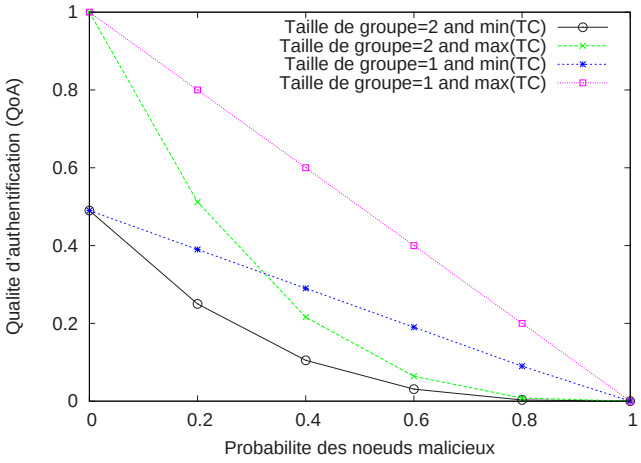


FIG. *3.10* – *QoA vs. probabilité que des nœuds malicieux soient présents*

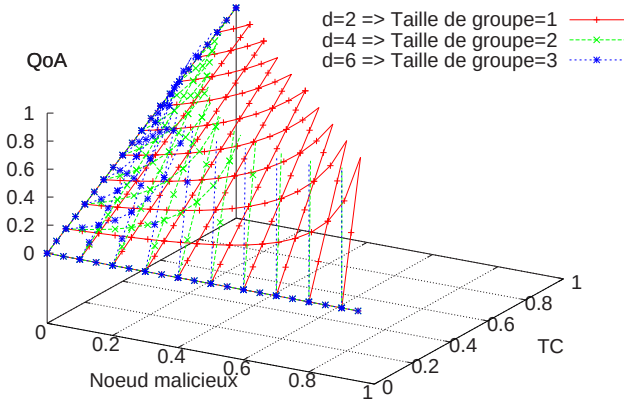


FIG. *3.11* – *QoA vs. probabilité que des nœuds malicieux soient présents et la chaîne TC*

3.6 Etude comparative

Dans cette partie, nous effectuons une étude comparative entre l'architecture que nous avons proposée et d'autres architectures et protocoles qui existent dans la littérature. Comme métriques de comparaison, nous citons :

A- Auto configuration : Dans cette métrique, nous distinguons deux catégories de métriques : auto configuration complète et auto configuration partielle. L'auto configuration complète ne nécessite ni la présence d'un serveur central, ni celle d'un secret partagé. Cependant, l'auto configuration partielle nécessite l'intervention d'une administration externe soit dans le phase initialisation, soit lorsqu'un changement de topologie ou un autre changement de configuration du réseau a lieu. Notre proposition

supporte l'auto configuration complète car aucune intervention externe n'est nécessaire pour assurer le fonctionnement de l'architecture. L'algorithme de groupage est proposé pour assurer la formation des groupes même en cas de changement de topologie. Aucun serveur central n'est nécessaire pour la distribution des clés. Un autre système qui supporte l'auto configuration complète est le système d'Hubaux et Cie (Capkun et al., 2002), qui a été amélioré par Satizabal et (C. Satizabal, 2007). Ce système est basé principalement sur le modèle PGP (Zimmermann, 1995), où chaque nœud joue le rôle d'autorité de certification (CA).

B- Mobilité : Cette métrique nous permet de distinguer parmi les différentes approches, celles qui sont les plus adaptées à la mobilité. En effet, la mobilité est l'une des caractéristiques les plus importantes des réseaux mobiles Ad hoc. Dans notre modèle, la mobilité est supportée grâce au protocole proposé, qui permet de déterminer la disponibilité du nœud CA et des nœuds RA. Ce protocole permet de déclencher l'élection d'un nouveau CA et la formation d'un nouveau groupe (cluster). Parmi les autres modèles qui supportent la mobilité, nous pouvons citer le modèle $MOCA$ proposé par Yi et Kravets (S. Yi, 2003), les systèmes proposés par Hubaux et Cie (Capkun et al., 2002) et Satizabal et Cie (C. Satizabal, 2007) et enfin le modèle proposé par Dong et Cie (Y. Dong, 2007).

C- Fiabilité : Cette métrique montre la capacité d'un système à accomplir les fonctions demandées sous certaines conditions, pendant une période de temps spécifique. Notre système est capable de mettre à jour le modèle de confiance de manière dynamique et de s'adapter aux changements de l'environnement. Il en va de même pour l'organisation du réseau en groupes (clusters). Parmi les autres modèles qui permettent d'assurer la fiabilité, nous pouvons citer les systèmes proposés par Hubaux et Cie (Capkun et al., 2002), Budakoglu et Cie (Budakoglu et Gulliver, 2004) et Satizabal et Cie (C. Satizabal, 2007) et enfin le modèle proposé par Dong et Cie (Y. Dong, 2007).

D- Passage à l'échelle : Le passage à l'échelle en terme de sécurité montre la capacité d'un système à garder un niveau de sécurité acceptable malgré l'augmentation de la densité des nœuds dans le réseau. En d'autres termes, le degré de robustesse doit être pris en compte quelle que soit l'augmentation de la taille du réseau. Dans le système que nous avons proposé, le passage à l'échelle est garanti, car avec le concept de groupage (clustering), la charge de l'autorité de certification (CA) est distribuée sur les groupes. Chaque groupe gère de manière indépendante les services de sécurité dans le groupe. D'autres systèmes permettent le passage à l'échelle, comme les systèmes proposés par Budakoglu et Cie (Budakoglu et Gulliver, 2004) et Dong et Cie (Y. Dong, 2007). Cf. le tableau 3.2 pour la comparaison avec d'autres systèmes qui permettent le passage à l'échelle.

E- Flexibilité : Cette métrique montre la capacité d'un système à s'adapter aux différentes situations possibles dans les réseaux mobiles Ad hoc, telles que le changement de topologie, le changement des ressources de sécurité, etc. La flexibilité est un paramètre très important dans les réseaux dynamiques comme les réseaux mobiles Ad hoc. Dans notre système, nous avons pris en compte ce paramètre. Par exemple, si les conditions de formation des groupes ne sont pas satisfaites, le système utilise l'approche PGP jus-

qu'à ce qu'au moins deux nœuds de confiance soient présents. D'autres systèmes proposés par Capkun et Cie (Capkun et al., 2002), Budakoglu et Cie assurent la souplesse et la flexibilité du système.

F- Disponibilité : Cette métrique montre le degré de disponibilité des services de sécurité assurés par le système. Notre système permet d'assurer la disponibilité des services de sécurité avec un certain degré en fonction des paramètres du réseau. Le degré de sécurité le plus sûr est présent dans le cas du groupage des nœuds et l'établissement d'une PKI dans chaque groupe. Cependant, le cas le moins souhaité est d'avoir des nœuds de confiance isolés incapables de former un groupe et d'établir une PKI, mais ce cas est pris en compte par le modèle PGP (Zimmermann, 1995).

G- Consommation d'énergie : C'est un paramètre important pour mesurer le coût de la solution de sécurité en terme de consommation d'énergie. Nous avons classé le coût de consommation d'énergie en trois catégories : élevé, moyen et faible. Les solutions qui utilisent la cryptographie à seuil (Shamir, 1995) sont classées comme solutions à coût de consommation d'énergie élevé, comme c'est le cas du système $MOCA$ (S. Yi, 2003), du modèle de Dong (Y. Dong, 2007) et de l'architecture de Bechler et Cie (Bechler et al., 2004). En effet, ces solutions nécessitent plus d'énergie pour générer un seul certificat. Contrairement aux solutions qui utilisent l'algorithme classique à clé publique adaptées aux contraintes des réseaux mobiles Ad hoc. Parmi ces solutions, nous citons notre modèle qui utilise la cryptographie asymétrique et l'algorithme de groupage. Notre solution, ainsi que le système proposé par Capkun et Cie (Capkun et al., 2002) sont classés à coût de consommation moyen. Toutes les solutions qui utilisent la cryptographie symétrique sont classées à faible coût de consommation d'énergie, comme c'est le cas du protocole $TESLA$ proposé par Perrig et Cie (Perrig et al., 2002). Cependant, le protocole $TESLA$ ne permet pas l'introduction d'une autorité de certification et est, de plus, contesté par la communauté scientifique à cause du problème de synchronisation et du problème de stockage des clés ou de la mémoire.

H- Point de vulnérabilité : Cette métrique permet de montrer si une vulnérabilité peut exister au niveau de l'autorité de certification (CA). Cela permet d'évaluer le risque au niveau du CA. Toutes les approches centralisées basées sur une seule entité comme CA sont vulnérables. Dans notre modèle, nous avons non seulement décentralisé le CA, mais nous avons aussi introduit un nouveau concept appelé la zone dynamique démilitarisée ($DDMZ$) pour protéger le CA dans chaque cluster (groupe). Les solutions basées sur la cryptographie à seuil (Shamir, 1995) empêchent l'existence d'un point de vulnérabilité au niveau du CA, comme c'est le cas de (S. Yi, 2003; Y. Dong, 2007; Bechler et al., 2004). Cependant, les solutions basées uniquement sur le modèle PGP comme celle de Capkun et Cie (Capkun et al., 2002) et celle de Satizabal et Cie (C. Satizabal, 2007) présentent des faiblesses au niveau de l'autorité de certification (CA), et donc l'existence d'un point de vulnérabilité.

I- Première ligne de défense : Cette métrique permet de déterminer si le modèle possède un mécanisme de première défense pour faire face aux attaques contre l'autorité de certification (CA). Notre modèle possède dans chaque groupe (cluster) un mécanisme de soutien au nœud CA. Ce mécanisme est appelé $DDMZ$. La plupart des attaques de

type déni de services peuvent être contrées via la $DDMZ$. Cette $DDMZ$ est formée de l'ensemble des nœuds de confiance situés à un saut du nœud CA et leur rôle est d'analyser et de filtrer le trafic vers le CA. La perte des nœuds de la $DDMZ$ n'implique pas la perte du nœud CA. A notre connaissance, nous sommes les premiers à introduire la notion de $DDMZ$ pour sécuriser le CA. Les autres solutions ne considèrent pas ce paramètre de première ligne de défense.

J- Modèle de confiance proactif : Ce paramètre nous permet de distinguer les solutions qui ont prévu un mécanisme de surveillance (monitoring) pour mettre à jour de manière dynamique le niveau de confiance des nœuds et assurer l'évolution du modèle de confiance. Dans notre solution, nous avons proposé un mécanisme de surveillance basé sur le modèle de confiance. Un nœud peut surveiller un autre nœud si son niveau de confiance est plus élevé ou égal à celui du nœud à surveiller. Les rapports de surveillance permettent d'augmenter ou de réduire le niveau de confiance du nœud en question. Parmi les solutions qui utilisent un mécanisme de surveillance pour entretenir le modèle de confiance, nous pouvons citer (Bechler et al., 2004; Capkun et al., 2002; C. Satizabal, 2007).

K- Tolérance aux pannes : Cette métrique est importante pour montrer que le système est capable de continuer sa tâche malgré la compromission d'un certain nombre de nœuds. En d'autres termes, elle permet de distinguer les systèmes qui ont la capacité de vivre avec la présence d'attaques ou qui tolèrent la présence de nœuds malicieux dans le réseau. La compromission d'un certain nombre de nœuds ne crée pas un déni de service. Dans notre solution, la compromission d'un certain nombre de nœuds de la $DDMZ$ n'entraîne pas la perturbation du cluster (groupe).

La table 3.2 résume la comparaison entre l'ensemble des solutions étudiées dans la section 3.2 avec toutes les métriques que nous venons de définir. Nous avons appelé notre architecture $DACA$ (Distributed Architecture for Certification Authority). Les autres architectures avec leurs références sont les suivants : $MOCA$ (S. Yi, 2003), $BEC.$ (Bechler et al., 2004), $HUB.$ (Capkun et al., 2002), $BUD.$(Budakoglu et Gulliver, 2004), $SAT.$(C. Satizabal, 2007) et $DON.$(Y. Dong, 2007). Le symbole «-» indique que le système ne supporte pas le paramètre en question.

Metrics	DACA	MOCA	BEC.	HUB.	BUD.	SAT.	DON.
Auto-configuration	✓	-	-	✓	-	✓	-
Mobilité	✓	✓	-	✓	-	✓	✓
Fiabilité	✓	-	-	✓	✓	✓	✓
Passage à l'échelle	✓	-	-	-	✓	-	✓
Flexibilité	✓	-	-	✓	✓	✓	-
Consommation d'énergie	Moyen	Elevé	Elevé	Moyen	Elevé	Moyen	Elevé
Première ligne de défense	✓	-	-	-	-	-	-
Modèle de confiance proactif	✓	-	✓	✓	-	✓	-
Tolérance aux pannes	✓	-	-	-	✓	-	-

TAB. 3.2 – *Tableau comparatif*

3.7 Conclusion

Dans ce chapitre, nous avons présenté 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 : seuls les nœuds de confiance peuvent jouer le rôle de CA. La stabilité est un facteur basé sur la métrique de la mobilité pour assurer la stabilité des groupes. Dans notre approche, le modèle de confiance est évalué par le processus de surveillance (monitoring), qui permet aux nœuds avec un niveau de confiance plus élevé de surveiller les nœuds dont le niveau de confiance est moins élevé. En outre, nous avons proposé un nouveau mécanisme, la $DDMZ$ (zone dynamique démilitarisée), pour protéger les nœuds CAs contre les attaques de type déni de service. Ce mécanisme augmente la robustesse de la sécurité dans les groupes.

De plus, nous avons proposé un modèle de connectivité de confiance pour étudier la robustesse de la sécurité au sein des groupes. Nous avons présenté les différents modules de l'architecture : le modèle de confiance, le processus d'élection, le gestionnaire de groupe et le module chargé du contrôle. Dans cette étude, nous nous sommes concentrés sur le gestionnaire de groupe, en particulier sur la $DDMZ$. Les résultats des simulations confirment ce qu'a montré notre modèle de connectivité sécurisé, à savoir que lorsque la probabilité d'avoir deux nœuds directement connectés entre eux augmente, la probabilité d'avoir une $DDMZ$ robuste augmente aussi parallèlement.

Les résultats de simulations montrent que l'algorithme que nous avons proposé pour la formation des groupes est meilleur que les algorithmes proposés dans $MOBIC$ (Basu et al., 2001) et $Lowest-ID$ (Gerla et Tsai, 1995). Nous avons aussi remarqué que la disponibilité et la robustesse de la DDMZ dépendent de la portée de transmission et du nombre de nœuds de confiance, ainsi que de leur mobilité. La stabilité des groupes permet de conserver l'énergie et d'augmenter la durée de vie du réseau.

Chapitre 4

Anonymat et sécurité dans une approche hiérarchique distribuée

Sommaire

La plupart des travaux qui traitent du concept d'anonymat se basent uniquement sur l'anonymat au niveau des protocoles de routage. Cependant, peu de travaux utilisent la combinaison entre les mécanismes de changement d'identité et de camouflage pour assurer l'anonymat de certains nœuds dans le réseau. Dans ce chapitre, nous proposons un protocole qui assure l'anonymat des nœuds ayant des rôles importants dans le réseau. Nous nous basons sur notre architecture hiérarchique distribuée pour sécuriser les réseaux mobiles Ad hoc (MANETs) (Rachedi et Benslimane, 2006). Cette architecture consiste à diviser le réseau sous forme de groupes de nœuds. Dans chaque groupe, un nœud de confiance est sélectionné pour assurer le rôle de l'autorité de certification (CA), sachant que la sécurité du groupe dépend de la sécurité du nœud CA. Par conséquent, nous introduisons le concept d'anonymat dans le mécanisme de protection du nœud CA. C'est le mécanisme que nous avons appelé zone dynamique démilitarisée

ou DDMZ (Cf. chap. 3) . Cette zone devient une zone anonyme, car elle sera formée par des nœuds dont l'identité est cachée (n'est pas connue par les autres nœuds). Elle sera notée (ADDMZ). Les nœuds qui forment l'ADDMZ sont des nœuds de confiance dont le niveau de confiance est le plus élevé et dont le but est de filtrer la communication entre les nœuds du groupe et le nœud CA. De plus, nous nous inspirons des mécanismes de défense militaire tels que les techniques de camouflage et les mécanismes de changement d'identité. Nous proposons un protocole pour réaliser ces mécanismes avec l'utilisation de la cryptographie basée sur la fonction bilinéaire. Ensuite, nous analysons le protocole présenté avec les discussions et l'évaluation.

4.1 Introduction

Au cours des dernières années, la communauté scientifique s'est de plus en plus intéressée au problème de la sécurité dans les réseaux mobiles Ad hoc (MANETs). Le concept d'anonymat dans les réseaux MANETs devient crucial et très important pour les nœuds, car l'environnement ouvert avec le partage du même canal radio pour tous les nœuds est l'une des caractéristiques des réseaux MANETs. Par conséquent, l'identité des nœuds est exposée à l'écoute passive du canal : n'importe quel nœud équipé de la même technologie sans fil est capable de déterminer l'identité des nœuds qui communiquent. Ainsi, ignorer la sécurité de l'identité des nœuds dont le rôle est très important dans le réseau peut créer des vulnérabilités exploitables par les nœuds malicieux dans le but de créer des attaques de type déni de services. C'est pourquoi nous introduisons dans cette partie le paramètre de l'anonymat dans notre architecture distribuée, dans le but de sécuriser l'identité des nœuds de confiance dont le rôle est important pour la sécurité. Parmi les rôles sensibles dont il faut protéger l'identité dans l'architecture, nous pouvons citer l'autorité de certification (CA) et l'autorité d'enregistrement (RA).

Nous utilisons le mécanisme SDVS (Simple Designed Verifier Signature) (X. Huang et Zhang, 2006) pour générer de manière dynamique une paire de clés publique et privée. Nous avons également recours à des pseudonymes pour les nœuds, au lieu d'utiliser leur identité réelle, pour les protéger contre les attaques potentielles. Nous améliorons le mécanisme $DDMZ$ en y introduisant le concept d'anonymat et en développant la $DDMZ$ anonyme (ADDMZ). L'idée consiste à garder l'identité réelle du nœud CA cachée pour les autres nœuds. Pour atteindre cet objectif, les mécanismes de changement d'identité et de camouflage doivent être développés. De plus, nous proposons un nouveau mécanisme pour établir l'$ADDMZ$. Un protocole de communication intra et extra $ADDMZ$ est également présenté. De même, la sécurité de la communication entre les groupes (clusters) est assurée.

Les nouvelles contributions que nous avons apportées avec notre proposition visant à sécuriser l'identité de certains nœuds dans le réseau sont les suivantes :

- Proposition d'un mécanisme qui permet d'assurer le changement d'identité des nœuds de confiance.
- Présentation d'un protocole d'authentification anonyme des nœuds de confiance.

– Introduction d'un mécanisme de camouflage pour sécuriser l'ADDMZ, en particulier les nœuds CA et RA.
– Proposition de protocoles de communication intra et inter-groupes, et d'authentification anonyme inter-groupes.
– Analyse de sécurité et étude de performance de notre solution.

Le reste de cette partie est organisé comme suit : la section 4.2 présente quelques travaux sur le concept d'anonymat. De plus, nous présentons un résumé sur le mécanisme SDVS. Dans la section 4.3, nous présentons notre protocole appelé ICCP (Identité Change and Camouflage Protocol), basé sur le changement d'identité et le mécanisme de camouflage. Dans la section 4.4, nous étudions et nous analysons la sécurité du protocole ICCP, puis nous montrons sa performance. Finalement, la section 4.5 conclut cette partie.

4.2 Positionnement bibliographique

4.2.1 Approches anonymes

Il existe plusieurs approches pour assurer la communication anonyme : Zhang et Cie (Y. Zhang et Lou, 2005) ont proposé un protocole de communication anonyme appelé MASK. Dans le protocole MASK, les auteurs assument que le système administrateur génère un nombre important de pseudo-identités pour chaque nœud dans le réseau. Cependant, chaque nœud doit avoir un grand nombre de pseudo identités. Ce nombre doit être assez grand pour que le nœud ne se fasse pas détecter par un nœud malicieux. Le problème avec ce mécanisme est que la pseudo identité fonctionne comme une identité réelle et que l'attaquant est capable d'identifier le nœud. De plus, la maintenance de ce mécanisme et sa gestion sont coûteuses. Rahman et Cie. (Sk. Md. M. Rahman et Okamoto, 2006) ont proposé le protocole RIOMO pour améliorer le protocole MASK et combler ses limites en réduisant le coût de la maintenance et en attribuant à chaque nœud une seule pseudo identité par le système administrateur. En fonction de cette pseudo identité, le nœud est capable de générer d'autres pseudo identités pour assurer l'anonymat de la communication. Cependant, ce protocole n'assure pas la fonction du camouflage. Reed et Cie (M.G. Reed, 1998) proposent un mécanisme de routage appelé « the onion routing protocol », repris par El-Khatib et Cie (K. El-Khatib et Yee, 2003) pour sécuriser le protocole dynamique de communication distribuée. Ce mécanisme assure l'anonymat de la route « chemin », mais pas le secret de localisation. Cela veut dire que la position des nœuds peut être détectée par l'attaquant. Kong et Cie (J. Kong et Gerla, 2007) ont proposé un protocole de routage à demande anonyme appelé ANODR. Ce protocole est basé sur la topologie et la diffusion pour améliorer l'anonymat du nœud récepteur. ANDOR est un protocole à demande basé sur une information chiffrée diffusée dans le réseau. Cette technique est appelée « trapdoor information ». Elle est largement utilisée dans les mécanismes de chiffrement et d'authentification.

4.2.2 Mécanisme SDVS (Simple designed verifier signature)

Le mécanisme SDVS est proposé par Hung et Cie (X. Huang et Zhang, 2006) et est divisé en trois algorithmes principaux : initiation, signature et vérification. Pour résumer, les principales étapes du SDVS sont présentées comme suit :

- ***Initiation :*** Soit G un groupe fini cyclique généré par le paramètre g et le nombre premier p, et soit H la fonction de hachage. Le nœud A choisit de manière aléatoire le nombre $K_A^- \in \mathbb{Z}_q$ ($\mathbb{Z}_q$ est l'ensemble des entiers modulo q) comme sa clé privée, puis il calcule la clé publique correspondante $K_A^+ = g^{K_A^-}$. De la même manière, le nœud B génère sa clé privée $K_B^- \in \mathbb{Z}_q$ et sa clé publique $K_B^+ = g^{K_B^-}$.
- ***Signature :*** Dans le but de signer le message $m \in \{0,1\}^*$ envoyé par le nœud A au nœud B, le nœud A calcule la clé $SK_A^B = (K_B^+)^{K_A^-} = g^{K_A^- \cdot K_B^-}$ et la signature $\theta = H(m, SK_A^B)$.
- ***Verification :*** Dans le but de vérifier la signature du message (m, θ), le nœud B calcule la clé $SK_A^B = (K_A^+)^{K_B^-}$ et effectue donc la vérification suivante : $H(m, SK_A^B) == \theta$. Si l'égalité est vérifiée, alors le message est accepté. Sinon, il est rejeté.

Le SDVS satisfait les tests formels de sécurité. Pour plus de détails, le lecteur peut se référer au travail dans (X. Huang et Zhang, 2006).

4.3 Protocole de changement d'identité avec le camouflage (ICCP)

4.3.1 Préliminaire

Les mécanismes de défense militaires, tels que les techniques de camouflage et de changement d'identité, sont généralement inspirés par les mécanismes de défense des animaux. Plusieurs animaux utilisent le mécanisme de camouflage pour se défendre contre les attaques des prédateurs. Nous pouvons citer par exemple l'iguane verte perchée sur un arbre (voir figure 4.1(a)). Le caméléon est un bon exemple pour les mécanismes de changement d'identité (voir figure 4.1(b)). Donc, dans notre proposition, nous adoptons le mécanisme de changement d'identité pour les nœuds de confiance et le mécanisme de camouflage pour les nœuds CA et RA dans le but de sécuriser la DDMZ. Le but est de protéger les nœuds de confiance, en particulier les nœuds CA et RA, pour préserver la sécurité des services assurés par ces nœuds contre l'écoute clandestine du canal et l'analyse illégale du trafic réseau. La figure 4.2 montre le coeur des groupes formés par les nœuds CA et RA à protèger dans l'architecture que nous avons proposée (Rachedi et Benslimane, 2006). Nous considérons que chaque nœud de confiance a deux identités, une réelle et un pseudonyme. Il possède également deux paires de clés : les clés réelles (privée/publique) et une paire de clés dynamiques générées avec le mécanisme SDVS à chaque changement de configuration ou de formation de groupe. L'ensemble des notations utilisées dans cette partie est représenté dans le tableau 4.1.

(a) L'iguane (b) Le caméléon

FIG. 4.1 – *Iguane et caméléon*

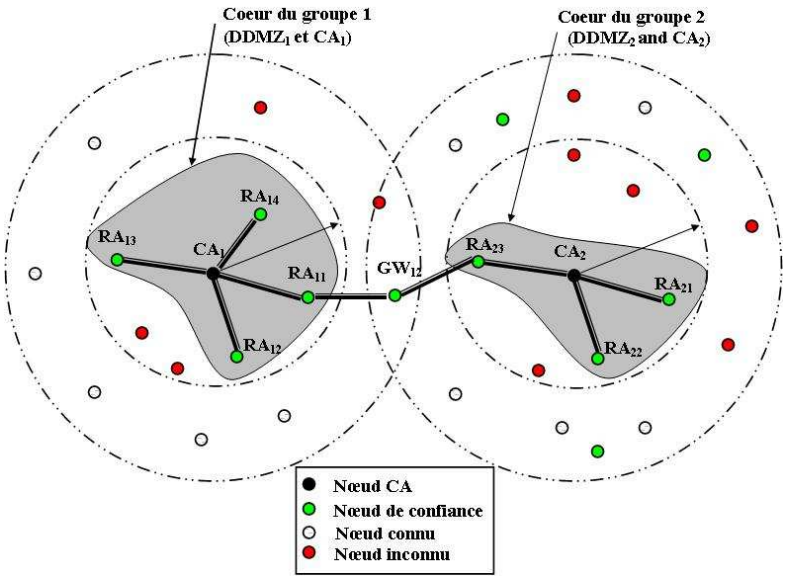


FIG. 4.2 – *Coeur des groupes*

4.3.2 Changement d'identité des nœuds de confiance

Dans le but de réaliser le masque d'identité des nœuds de confiance (les nœuds caméléons), nous utilisons une fonction bilinéaire et le mécanisme développé par Rahman et Cie (Sk. Md. M. Rahman et Okamoto, 2006). Nous supposons que chaque nœud de confiance possède un secret noté SP_i, qui dépend de l'identité réelle du nœud. Cependant, SP_i est généré comme suit : premièrement, le système détermine deux ensembles $\mathbb{G}_1$ (ensemble additif) et $\mathbb{G}_2$ (ensemble multiplicatif) avec le même nombre premier q. Deuxièmement, la fonction bilinéaire est choisie $f : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ ainsi que deux fonctions de hachage cryptographique résistantes aux collisions H_1 et H_2 définies comme suit : $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$ et $H_2 : \{0,1\}^* \rightarrow \{0,1\}^\ell$, où ℓ-bit est la taille de la sortie. Troisièmement, le secret $S_c \in \mathbb{Z}_q$ est généré pour l'ensemble des nœuds de la communauté

CA_i	Autorité de certification du cluster i
RA	Autorité d'enregistrement qui forme la DDMZ
ID_i	Identité réelle du nœud i
ID_{Pi}	Pseudonyme de l'identité du nœud i
$< K_i^+, K_i^- >$	Les clés publique et privé du nœud i
$< rK_j^+, rK_j^- >$	Les clés publique et privé réelles du nœud j
SK_i^j	Clé de session partagée entre les nœuds i et j
K_g^i	La clé du groupe i
$(\mathbb{G}_1, \mathbb{G}_2)$	$\mathbb{G}_1$ (Ensemble des nombres additifs) et $\mathbb{G}_2$ (Ensemble des nombres multiplicatifs) de même nombre premier q
H_1	Fonction de hachage particulière ($H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$)
H_2	Fonction de hachage à un seul sens (i.e. MD5, SHA-1)
H_{Z_p}	Fonction de hachage définie comme suit : $H_{Z_p} : \{0,1\}^* \longrightarrow G$
$HMAC(M, K)$	Code d'authentification du message M avec l'utilisation de la clé K.
$Ea_K(M)$	Cryptogramme du message M chiffré par l'algorithme à clé publique (RSA, ElGamal)
$SIN_{K_i^-}(M)$	Signature du message M générée par le nœud i
$Es_K(M)$	Cryptogramme du message M chiffré par l'algorithme symétrique (AES, 3DES) avec l'utilisation de la clé K

TAB. 4.1 – *Table des variables et des notations*

de confiance, mais aucun nœud de confiance ne possède ce secret S_c. Les nœuds de confiance reçoivent leur secret SP_i avant le déploiement des nœuds. De plus, les nœuds de confiance connaissent les paramètres du système $\{\mathbb{G}_1, \mathbb{G}_2, f, H_1, H_2\}$. Donc, chaque nœud de confiance possède son secret $SP_i = S_c.H_1(ID_i)$, où ID_i est son identité réelle. Lorsque le nœud de confiance (ID_i) veut changer son identité pour une quelconque raison de sécurité, le nœud génère un nouveau pseudonyme noté ID_{Pi} et son pseudo secret correspondant (SP_{Pi}) comme suit :

$$\begin{cases} ID_{Pi} = r_i.H_1(ID_i) \\ SP_{Pi} = r_i.SP_i = r_i.S_c.H_1(ID_i) = S_c.ID_{Pi} \end{cases}$$

où r_i est le nombre aléatoire généré par le nœud ID_i. La figure 4.3 présente le protocole d'authentification mutuelle entre deux nœuds de confiance A et B. Nous supposons que la nouvelle pseudo identité des nœuds A et B avec leur secret associé est notée comme suit : $\{ID_{PA}, SP_{PA}\}$ et $\{ID_{PB}, SP_{PB}\}$. Le nœud A envoie au nœud B sa nouvelle identité avec une valeur aléatoire : $\langle ID_{PA}, r_A, K_{PA}^+, s\rangle$, où $s = H_2(K_{PA}^+ || SK_{PA}^{PB})$ et $SK_{PA}^{PB} = (K_{PB}^+)^{K_{PA}^-}$. Lorsque le nœud B reçoit cette information et après le déchiffrement de cette information via l'utilisation de sa clé privée, il calcule la clé de session $SK_{PA}^{PB} = (K_{PA}^+)^{K_{PB}^-}$ pour l'utiliser au prochain chiffrement. Puis, il vérifie l'intégrité de la clé publique PA et de la clé de session en utilisant le paramètre « s ». Si la procédure de vérification se termine correctement, il calcule la clé K_{BA} en fonction des propriétés de la fonction bilinéaire, $K_{BA} = f(SP_{PB}, ID_{PA}) = f(ID_{PB}, ID_{PA})^{S_c}$ et il génère la valeur aléatoire r_B, puis il génère $Ver_B = H_2(K_{BA} || r_A || r_B)$. Ensuite, le nœud B envoie cette informa-

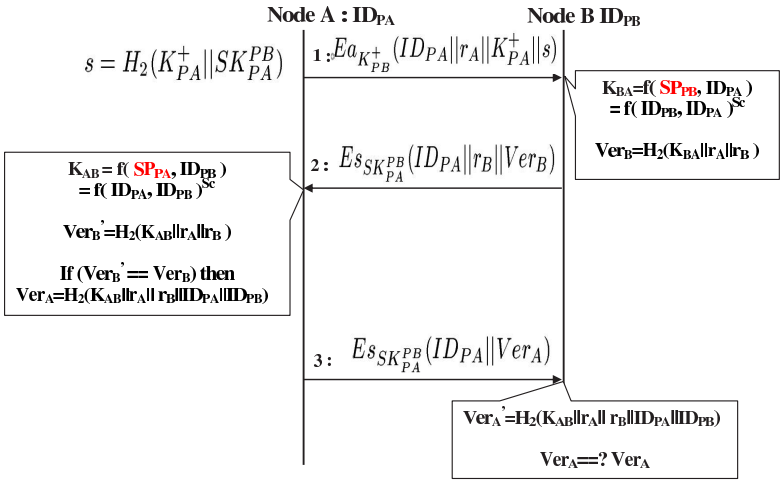


FIG. 4.3 – *Authentification anonyme des nœuds de confiance*

tion $\langle ID_{PA}, r_B, Ver_B \rangle$ au nœud A chiffré par la clé de session. Lorsque le nœud A reçoit cette information et après l'opération de déchiffrement par la clé de session, il calcule la clé K_{AB} de la même manière que le nœud B : $K_{AB} = f(SP_A, ID_{PB}) = f(ID_{PA}, ID_{PB})^{S_c} = K_{BA}$. Alors, le nœud A calcule $Ver'_B = H_2(K_{AB}||r_A||r_B)$. Si $Ver_B == Ver'_B$, alors il calcule $Ver_A = H_2(K_{AB}||r_A||r_B||ID_{PA}||ID_{PB})$ et envoie au nœud B l'information chiffrée $\langle ID_{PA}, Ver_A \rangle$ par la clé de session. Une fois que le nœud B reçoit cette information et une fois que l'opération de déchiffrement est correctement effectuée, il va calculer $Ver'_A = H_2(K_{AB}||r_A||r_B||ID_{PA}||ID_{PB})$, puis la comparer avec Ver_A. Si l'égalité est vérifiée, alors le nœud B en déduit que le nœud A est un nœud de confiance.

Selon le modèle de confiance que nous avons développé dans (Rachedi et Benslimane, 2006), chaque nœud a une métrique de confiance (Tm) qui définit le niveau de confiance du nœud. Seuls les nœuds de confiance ont le niveau de confiance le plus élevé ($Tm = 1$). Cependant, lorsqu'un nœud inconnu ID_k (qui n'appartient pas à l'ensemble des nœuds de confiance) rejoint le groupe (cluster), le nœud CA du groupe lui attribut le niveau le plus faible de confiance, puis il augmente ce niveau lorsque le mécanisme de surveillance donne un avis positif sur le nœud. Lorsque le nœud ID_k satisfait les conditions pour devenir un nœud de confiance, alors nous devons répondre à la question suivante : comment un nouveau nœud de confiance obtient-il son secret SP ? Dans notre modèle, seul le nœud CA peut attribuer le statut de confiance en changeant l'identité du nouveau nœud de ID_k à $ID_{Pk} = H_1(ID_k).ID_{Pi}$, où $CA_i = ID_{Pi}$ est la pseudo identité du nœud CA. En outre, le nœud CA génère le secret $SP_{ID_{Pk}}$ à ID_{Pk} comme suit :

$$SP_{ID_{Pk}} = r_i.SP_{ID_i}.H_1(ID_k) = r_i.S_c.H_1(ID_i).H_1(ID_k)$$
$$\Longrightarrow S_c.ID_{Pi}.H_1(ID_k) = S_c.ID_{Pk}$$

Lorsque le nœud ID_k reçoit sa nouvelle pseudo identité ID_{Pk} et le secret correspondant $SP_{ID_{Pk}}$, alors le nouveau nœud de confiance peut authentifier n'importe quel nœud de confiance et être authentifié par n'importe lequel d'entre eux.

4.3.3 Sécurité des nœuds CA et RA dans l'ADDMZ

Dans le but de sécuriser les nœuds CA et RA, nous adoptons le mécanisme de camouflage. Lorsque le nœud CA est sélectionné, il change son identité en générant une nouvelle pseudo identité notée ($CA_i = ID_{Pi}$), selon le mécanisme montré ci-dessus. $CA_i = r_i.H_1(ID_i)$, où r_i est un nombre aléatoire généré par ID_i. De plus, CA_i utilise le mécanisme SDVS pour générer de manière dynamique les clés privée et publique à chaque formation ou reconfiguration du groupe i. Ensuite, CA_i établit la clé de session ($SK_{CA_i}^{RA_j}$) avec chaque nœud RA_j via le SDVS. Le nœud CA_i établit la clé de session comme suit :

- Il calcule $K_{CA_i}^{-} = x_i.H_1(CA_i)$, où x_i est un nombre aléatoire dans $\mathbb{Z}_p$, puis il calcule la clé publique du groupe i (cluster) ($K_{CA_i}^{+}$) et la valeur « s » pour assurer l'intégrité de $K_{CA_i}^{+}$ et $SK_{CA_i}^{RA_j}$ comme suit :

$$\begin{cases} K_{CA_i}^{+} = g^{K_{CA_i}^{-}} \\ s = H_2(K_{CA}^{+} || SK_{CA_i}^{RA_j}) \end{cases}$$

  où $SK_{CA_i}^{RA_j} = (K_{RA_j}^{+})^{K_{CA_i}^{-}}$.
- Il forme le message $M = [\#Id_p || CA_i || RA_j || K_{CA_i}^{+} || s]$, où $\#Id_p$ est un identifiant unique pour chaque paquet dans tout le réseau et est généré de manière aléatoire. Ensuite, il chiffre le message M par l'utilisation de la clé publique du nœud RA_j comme suit : $C = Ea_{K_{RA_j}^{+}}(M)$.
- Le CA_i envoie le paquet P (P=$\langle C \rangle$) au nœud RA_j.

Lorsque le nœud est à un seul saut du nœud CA_i, il reçoit le paquet P, essaye de déchiffrer le cryptogramme « C » en utilisant sa clé privée $K_{N_j}^{-}$. Si l'opération de déchiffrement est réussie, alors le nœud récepteur en déduit que c'est lui la destination du paquet et donc, il vérifie l'intégrité du paquet P. Sinon il n'est pas la destination et le paquet sera rejeté.

Le nœud CA_i répète la même opération avec chaque nœud RA, puis partage une clé de session ($SK_{CA_i}^{RA_j}$) avec tous les nœuds RA (RA_j). De plus, le nœud CA_i utilise les clés de session partagées avec les nœuds RA pour générer la clé de groupe (K_g^i) de l'ADDMZ. Donc, si la taille de l'ADDMZ est k, alors K_g^i est générée comme suit :

$$K_g^i = H_2(SK_{CA_i}^{RA_1} || SK_{CA_i}^{RA_2} || ... || SK_{CA_i}^{RA_k})$$

où $K_g^i \in Z_p$

L'ensemble des nœuds RA qui forment la DDMZ du groupe i utilisent le pseudonyme « $DDMZ_i$ ». Nous utilisons le même principe de diffusion que celui qui est utilisé par le protocole ANODR (J. Kong et Gerla, 2007) pour assurer l'anonymat des nœuds CA et RA à la réception. Par exemple, pour chaque paquet transmis pour le CA_i ou n'importe quel nœud RA dans le groupe (i), l'adresse de destination doit être $DDMZ_i$. Aucun nœud, même situé à un seul saut de la $DDMZ_i$, n'est capable d'identifier le

pseudonyme du nœud RA et de connaître son identité réelle. Donc, dans le but de sécuriser l'identité des nœuds RA, les clés publique et privée $(K^{-}_{ddmz}, K^{+}_{ddmz})$ de la $DDMZ$ anonyme doivent être générées. Ces clés sont basées sur la clé secrète du groupe key K^{i}_{g} partagée entre les nœuds RA et CA_i. La clé privée de l'ADDMZ est uniquement connue par les nœuds RA et CA et est calculée comme suit : $K^{-}_{ddmz} = H_1(K^{i}_{g})$. Cependant, la clé publique de l'ADDMZ est calculée comme suit : $K^{+}_{ddmz} = g^{K^{-}_{ddmz}}$.

Nous distinguons deux sortes de communications principales : la communication intra-groupes et la communication inter-groupes.

4.3.4 Communication intra-groupe

Au niveau de la communication intra-groupe, nous distinguons deux types de communications : la communication intra-ADDMZ et la communication extra-ADDMZ.

A- Communication intra-ADDMZ

Cette communication ne doit pas s'établir à plus de un saut du nœud CA. Seuls les nœuds CA et l'ensemble des nœuds RA sont capables de déchiffrer l'information contenue dans le paquet diffusé dans cette zone. Cependant, le nœud CA peut communiquer en privé avec chaque nœud RA.

Pour chaque paquet généré par les nœuds dans le réseau, le nœud génère un identifiant unique pour chaque paquet $\#Id_p$ dans tout le réseau. Cet identifiant doit être choisi de manière aléatoire. Selon la condition de « birthday paradox » (Trappe et Wahington, 2006), la probabilité pour que les nœuds sources choisissent la même valeur est estimée à $2^{-|\#Id_p|/2}$, où $|\#Id_p|$ est la taille en bits de la valeur $\#Id_p$.

La communication entre les nœuds CA et RA est chiffrée par K^{i}_{g} dans le cas d'une diffusion de paquets dans la zone ADDMZ. Cependant, dans le cas d'une communication privée entre CA_i et RA_j qui partagent deux clés $(SK^{RA_j}_{CA_i})$ et la clé de groupe K^{i}_{g}. Lorsque RA_j veut envoyer un message privé m au nœud CA_i, il forme le paquet comme suit : $P = \langle Q \rangle$, où $Q = Es_{K^{i}_{g}}(\#Id_p, CA_i, RA_j, C)$ et où C est le cryptogramme chiffré par la clé de session $SK^{RA_j}_{CA_i}$ $(C = Es_{SK^{RA_j}_{CA_i}}(m))$. Seuls les nœuds CA et l'ensemble des nœuds RA sont capables de déchiffrer le paquet en utilisant la clé de groupe, puis ils vérifient les adresses destination et source.

B- Communication extra-ADDMZ

Dans le but de masquer l'identité des nœuds RA, la génération de la paire de clés $(K^{-}_{ddmz}, K^{+}_{ddmz})$ est nécessaire. Cette paire de clés est basée sur la clé de groupe K^{i}_{g}. La clé publique de l'ADDMZ (K^{+}_{ddmz}) et la clé publique de CA $(K^{+}_{CA_i})$ sont diffusées par

le nœud CA_i dans le paquet HELLO du groupe via les nœuds RA à tous les nœuds du groupe (i). Le paquet HELLO est généré périodiquement par le nœud CA dans le but de maintenir le groupe et d'assurer son bon fonctionnement via la distribution de l'identité du groupe et des clés publiques de l'ADDMZ et de rôle CA. Le paquet HELLO du groupe noté P_{Hello} est formé comme suit :

$P_{Hello} = [\#Id_p, hop, DDMZ_i, K^+_{CA_i}, K^+_{ddmz}, S]$, où $hop = hop_{max} - 1$ représente la taille du groupe et $S = SIN_{K^-_{CA}}(\#Id_p||K^+_{CA_i}||K^+_{ddmz})$.

Dans le but de réaliser le camouflage de la pseudo identité des nœuds CA et RA et d'après la section précédente, nous utilisons une adresse de diffusion anonyme. Dans le cas de la technologie IEEE 802.11, nous utilisons l'adresse de multicast comme une adresse MAC de source ou de destination (J. Kong et Gerla, 2007).

Lorsqu'un nœud N_i reçoit le paquet P_{Hello}, il doit vérifier la condition suivante : $hop - 1 \geq 0$. Si la condition est vérifiée, alors il continue l'opération de vérification, sinon le paquet est rejeté. Ensuite, il vérifie l'identifiant du paquet ($\#Id_p$) pour savoir si le paquet a déjà été reçu auparavant ou non. Si le paquet est nouveau (n'a jamais été reçu avant), alors il vérifie l'intégrité puis l'authentification de P_{Hello} en utilisant la clé publique de rôle CA. Si la vérification n'est pas réussie, le paquet est rejeté. Dans le cas où toute la procédure de vérification est bien terminée et où le nœud récepteur possède son certificat de la part du nœud CA_i, il fait suivre le paquet à ces voisins après avoir mis à jour le paramètre hop pour le nombre de sauts. De plus, il ajoute son certificat dans le paquet et il sauvegarde l'identifiant du paquet $\#Id_p$ et le temps de réception du paquet T_{recv}. Les paramètres $\#Id_p$, $DDMZ_i$ et T_{recv} sont importants pour acheminer le paquet à l'$ADDMZ_i$ et pour former la table de routage basée sur le concept du circuit virtuel identifié (VCI) (J. Kong et Gerla, 2007). Ce concept permet d'acheminer le paquet en fonction de l'identifiant du circuit ou du chemin.

Le format du paquet acheminé par le nœud N_i est le suivant :

$$N_i \rightarrow *(diffusion) :$$
$$\langle \#Id_p, hop - 1, N_i, Cert_{CA_i}(N_i), K^+_{CA_i}, K^+_{ddmz}, S \rangle$$

où le format de certificat est défini comme suit :

$$Cert_{CA_i}(N_i) = SIN_{K^-_{CA_i}}[N_i||statuts|K^+_{N_i}||validtime]$$

Le paramètre « status » détermine le niveau de sécurité attribué au nœud N_i : si N_i est inconnu, le nœud CA_i va lui attribuer le statut visiteur avec le niveau de confiance le plus bas. De plus, le paramètre « validtime » détermine la durée de validité du certificat. L'opération de retransmission est répétée comme décrit ci-dessus jusqu'à l'arrivée du paquet aux nœuds de bordure avec $hop = 0$.

C- Demande de certification

Si le nœud N_i veut rejoindre le groupe (i), il envoie sa demande au nœud CA_i via une requête de certification comme suit :

$$N_i \rightarrow DDMZ_i : \langle \#Id_p, Cert\_req, hop, DDMZ_i, N_i, S \rangle$$

où $S = SIN_{K^-_{ddmz}}(N_i||K^+_{N_i})$. Toutes les demandes de certificat doivent passer par la $DDMZ_i$ (les nœuds RA) avant d'arriver au nœud CA_i. Seuls les nœuds de groupes qui possèdent leur certificat peuvent retransmettre les paquets.

4.3.5 Communication inter-groupes

La communication inter-groupes est assurée par les nœuds de bordure. Pour des raisons de sécurité, tous les nœuds de bordures ne peuvent pas assurer le lien entre les groupes, car un certain niveau de sécurité est nécessaire pour obtenir le statut passerelle (GW). Pour plus de détails, le lecteur peut se référer au modèle de confiance que nous avons développé dans (Rachedi et Benslimane, 2006). La communication entre les nœuds GW et l'ADDMZ (Anonymous DDMZ) doit être chiffrée. Lorsque le nœud de bordure N_x avec un niveau de sécurité élevé reçoit des groupes (i) et (j) le paquet HELLO P_{Hello}, il va envoyer sa demande de certificat à l'$ADDMZ$ de chaque groupe pour obtenir le certificat avec le statut passerelle (GW). Ce certificat est généré par les nœuds CA_i et CA_j après une authentification mutuelle entre les deux nœuds. Le nœud N_x forme le paquet de demande de certificat comme suit :

$$\begin{aligned} &N_x/GW^j_i \rightarrow DDMZ_i : \\ &\langle \#Id_p, hop, DDMZ_i, N_x, Cert_{CA_i}(N_x), U, S \rangle \end{aligned}$$

où

$$\begin{cases} U = Ea_{K^+_{ddmz_i}}(N_x||Cert_{CA_j}(N_x)||CA_j||K^+_{CA_j}||K^+_{ddmz_j}) \\ S = SIN_{K^-_{N_x}}(\#Id_p||DDMZ_i||Cert_{CA_i}(N_x)||U) \end{cases}$$

Lorsque l'$ADDMZ_i$ reçoit la demande de certification pour le statut GW, elle vérifie la validité du certificat actuel du nœud N_x $Cert_{CA_i}(N_x)$, puis contrôle l'intégrité et la validité de $Cert_{CA_j}(N_x)$, et enfin le niveau de confiance du nœud N_x. Si la procédure de vérification se termine bien, alors l'$ADDMZ_i$ retransmet le paquet au nœud CA_i. Le nœud CA_i doit vérifier l'identité réelle du nœud CA_j s'il appartient à la communauté de confiance. Dans ce cas, l'authentification anonyme inter-groupes est nécessaire.

A- Authentification anonyme inter-groupes

Le nœud CA_i veut vérifier si le rôle de CA_j est assuré par un nœud de confiance et cela pour créer un réseau privé virtuel entre les deux groupes i et j. Le nœud CA_i

génère un paquet pour le CA_j avec une variable aléatoire « r_i = *challenge* » utilisée pour générer son pseudonyme CA_i ($CA_i = r_i.H_1(ID_i)$). Ensuite, il envoie le paquet au nœud RA_y, formé comme suit :

$$CA_i \rightarrow RA_y : \langle Es_{k_g^i}(\#Id_p||RA_y||CA_i||Q_1)\rangle$$

où Q_1 est défini comme suit :

$$\begin{cases} Q_1 = Es_{SK_{CA_i}^{RA_y}}(\#Id_p, hop, N_x, U_1) \\ U_1 = Ea_{K_{CA_j}^+}[K_{CA_i}^+||r_i||S] \\ S = SIN_{K_{CA_i}^-}(\#Id_p||N_x||K_{CA_i}^+||CA_i||r_i) \end{cases}$$

Lorsque l'$ADDMZ_i$ reçoit le paquet, seul RA_y prend en charge la demande de certification puis retransmet le paquet à ses voisins.

$$DDMZ_i(R_y) \rightarrow N_x : \\ \langle \#Id_p, hop, N_x, Cert_{CA_i}(DDMZ_i), U_1, S\rangle$$

où $S = SIN_{K_{addmz_i}^-}(\#Id_p||N_x||Cert_{CA_i}(DDMZ_i)||U_1)$

Lorsque le nœud N_x reçoit le paquet de l'$ADDMZ_i$, il vérifie l'intégrité et l'authentification du paquet via l'utilisation du paramètre S. Ensuite, il utilise son certificat $Cert_{CA_j}(N_x)$ pour communiquer avec le cluster j et envoie le paquet suivant :

$$N_x/GW_i^j \rightarrow DDMZ_j : \\ \langle \#Id_p, hop, DDMZ_j, Cert_{CA_j}(N_x), U_1, S\rangle$$

où $S = SIN_{K_{N_x}^-}(\#Id_p||DDMZ_j||Cert_{CA_j}(N_x)||U_1)$ et où U_1 est le même bloc que celui de la $DDMZ_i$.

Lorsque la $DDMZ_j$ reçoit le paquet de la part de N_x et après vérification du nombre de sauts « hop », $Cert_{CA_j}(N_x)$, de l'intégrité et de l'authentification du paquet, alors la $DDMZ_j$ retransmet le paquet au nœud CA_j comme suit :

$$DDMZ_j(RA_x) \rightarrow CA_j : \langle Es_{K_g^j}(\#Id_p||CA_j||RA_x||Q_2)\rangle$$

où $Q_2 = Es_{SK_{CA_j}^{RA_k}}(\#Id_p, hop, N_x, U_1)$ et où RA_x est membre de la $DDMZ_j$.
Après avoir déchiffré et vérifié les paramètres $\#Id_p$ et hop, le nœud CA_j déchiffre le bloc U_1 avec sa clé privée puis vérifie l'intégrité des informations telles que N_x et $K_{CA_i}^+$. Si toute l'opération de vérification se termine correctement, alors le nœud CA_j calcule la clé $K_{i,j}$ et le paramètre Ver_j comme suit :

$$\begin{cases} K_{i,j} = f(SP_j, CA_i) = f(CA_j, CA_i)^{Sc} \\ Ver_j = H_2(K_{i,j}||r_i||r_j) \end{cases}$$

où SP_j est le secret du nœud CA_j et r_j est un challenge aléatoire généré par le nœud CA_j dans le but de générer son pseudonyme $CA_j = r_j.H_1(ID_j)$. Ensuite, le nœud CA_j envoie les paramètres r_j et Ver_j au nœud CA_i de la même manière.

Lorsque le nœud CA_i reçoit le paquet, il va utiliser la clé de session partagée avec le nœud RA_y pour déchiffrer le paquet, et après il vérifie le paramètre du paquet S en utilisant la clé publique du nœud CA_j dans le but d'être sûr que le paquet est généré par le nœud CA_j. De plus, le nœud CA_j utilise sa clé privée $K^{-}_{CA_i}$ pour déchiffrer le paramètre U_2 (voir la figure 4.4). Si l'opération de déchiffrement est réussie, alors il calcule la clé $K_{i,j}$ et vérifie le paramètre Ver_j.

$$\begin{cases} K_{i,j} = f(SP_i, CA_j) = f(CA_i, CA_j)^{Sc} \\ Ver'_j = H_2(K_{i,j}||r_i||r_j) \end{cases}$$

Si Ver'_j est égal à Ver_j, alors le nœud CA_i en déduit que CA_j est un nœud de confiance. Puis, le nœud CA_i génère Ver_i et il vérifie si CA_i est un nœud de confiance.

$$Ver_i = H_2(K_{i,j}||r_i||r_j||CA_i||CA_j)$$

En utilisant le même mécanisme, le nœud CA_i envoie Ver_i au nœud CA_j. Lorsque CA_j reçoit ces paramètres et après avoir vérifié les métriques de sécurité (authentification et intégrité), le nœud CA_j calcule Ver'_i ($Ver'_i = H_2(K_{j,i}||r_i||r_j||CA_i||CA_j)$) et vérifie si $Ver'_i == Ver_j$. Si c'est le cas, alors CA_j est maintenant sûr que CA_i est un nœud de confiance. Donc, le certificat de passerelle pour le nœud N_x est généré par les deux nœuds CA_i et CA_j. La figure 4.4 montre le protocole d'authentification anonyme des nœuds CA. Ce protocole permet à n'importe quel nœud CA d'authentifier un autre nœud CA d'un groupe voisin de manière anonyme.

4.4 Analyse de sécurité et de performance

4.4.1 Analyse de la sécurité

A- Identité privée des nœuds confiance : avec ICCP, les identités des nœuds confiance sont protégées grâce à l'utilisation d'un pseudonyme ou d'une pseudo identité, de façon à ce qu'aucun nœud ne soit en mesure de deviner l'identité réelle des nœuds de confiance à partir de ces pseudonymes. Le mécanisme de fausse identité permet de modifier la fausse identité des nœuds de confiance que les nœuds CA et RA de façon dynamique lors de chaque formation ou nouvelle configuration de groupe. Sécurité des services de sécurité : dans le but de sécuriser les nœuds CA et RA de chaque groupe, nous ne nous somme pas limités à la protection de l'identité des nœuds confidents, mais nous avons aussi proposé un autre mécanisme pour protéger les rôles sensibles des nœuds de confiance qui appartiennent à la DDMZ. Nous avons appelé ce mécanisme le mécanisme de camouflage. Ce mécanisme assure l'anonymat des nœuds qui appartiennent à la DDMZ grâce à l'utilisation de l'adresse de diffusion allouée à ce groupe.

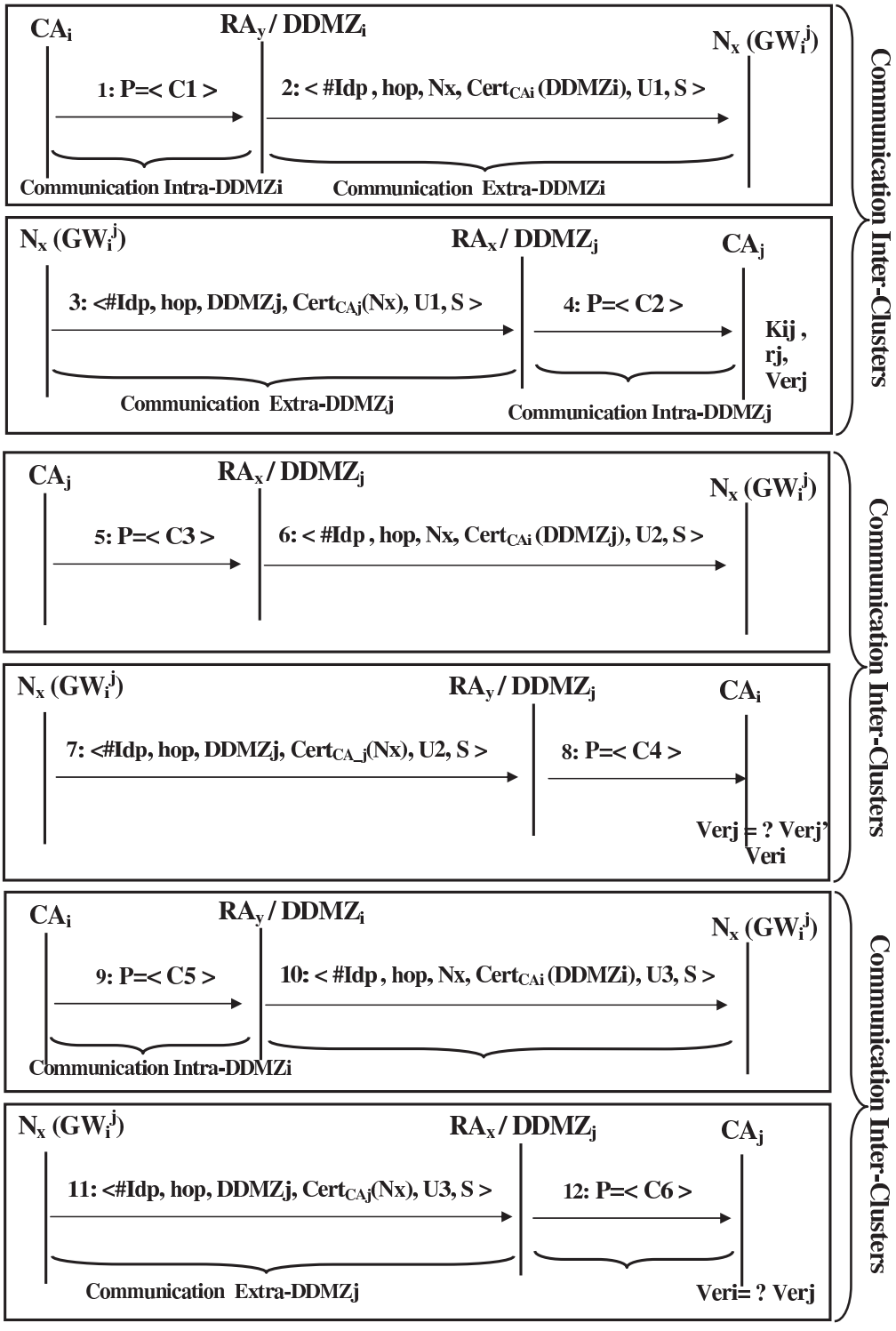


FIG. 4.4 – *Protocole d'authentification anonyme des nœuds CA*

B- Clé du groupe de la DDMZ : La clé du groupe de la DDMZ est le résultat d'une fonction de hachage à sens unique des clés de session (SK) partagées entre les nœuds CA et RA. Les nœuds RA se basent sur la clé de groupe de la DDMZ (K_g) pour constituer la paire de clés publique et privée de la DDMZ ($\{K^-_{ddmz}, K^+_{ddmz}\}$). A chaque fois que le groupe de nœuds RA change, soit parce qu'un ou plusieurs nœud(s) RA rejoint(gnent) ou quitte(nt) la DDMZ, la clé de groupe (K_g) est mise à jour par le nœud CA. Bien que les nœuds RA soient confidents, la clé du groupe DDMZ est mise à jour pour des raisons de sécurité. Cette mise à jour permet de préserver le secret de la DDMZ. Ainsi, la paire de clés publique et privée de la DDMZ change lorsque la clé de groupe de la DDMZ change. Cependant, même si l'attaquant a obtenu cette clé de groupe, il est incapable de connaître les clés de session ou de compromettre le groupe.
C- Attaques de type DoS : En général, l'attaquant doit écouter clandestinement le canal, dans le but de détecter les activités des nœuds et de planifier son attaque contre eux. Toutefois, avec le protocole ICCP, l'attaquant ne peut pas déterminer qui assure les rôles de CA ou RA. Si le nœud attaquant veut planifier une attaque contre le nœud CA ou le nœud RA, il doit avant tout les identifier. Même si l'attaquant utilise les attaques d'analyse du trafic pour identifier les nœuds RA ou CA, il peut seulement savoir s'ils sont situés dans le voisinage de la DDMZ, mais il ne peut en aucun cas identifier les nœuds RA ou le nœud CA, car les nœuds RA utilisent le pseudonyme DDMZ pour communiquer en tant que RA et leur pseudo identité pour communiquer normalement. Cependant, il est possible d'attaquer les nœuds RA en sélectionnant de façon aléatoire des nœuds situés dans le voisinage de l'attaquant, mais le risque de détecter l'attaquant est élevé. Supposons que l'attaquant réussisse à compromettre un nœud confident N_c, alors l'attaquant peut obtenir le point secret SP_c du noeud N_c, mais aussi son identité réelle ID_c. Toutefois, l'attaquant ne peut pas compromettre l'intégralité du modèle de confiance et démasquer les nœuds confidents, car avec cette information, l'attaquant ne peut que vérifier si le nœud appartient à l'ensemble des nœuds confidents ou non.

4.4.2 Etude de complexité

T_P	Temps de calcul de la fonction bilinéaire
T_X	Temps de calcul de l'exponentiel modulaire dans G_1
T_M	Temps de calcul de la multiplication modulaire dans G_1
T_H	Temps de calcul de la fonction de hashage
T_E	Temps de calcul pour le chiffrement asymétrique
T_D	Temps de calcul pour le déchiffrement asymétrique
T_S	Temps de calcul pour le chiffrement et le déchiffrement symétriques

TAB. 4.2 – *Table de définition et de notation pour évaluer la performance*

Dans le but d'analyser la performance du protocole ICCP en terme de complexité en temps (TC) au cours de différentes phases, nous définissons l'ensemble des notations illustrées dans la table 4.2.
Phase de changement d'identité : la complexité en temps du changement d'identité pour chaque N_x est évalué comme suit : $TC(N_x) = T_H + 2.T_M$, ce qui est acceptable

pour chaque formation ou configuration de groupe.
Phase d'authentification anonyme pour les nœuds de confiance : la complexité en temps de l'authentification anonyme entre deux nœuds confidents N_x et N_y est évaluée comme suit :

$$\begin{cases} TC(N_x) = T_E + T_X + T_P + 2.(T_H + T_S) \\ TC(N_y) = T_D + T_X + T_P + 2.(T_H + T_S) \end{cases}$$

Cette phase est exécutée avant la formation du groupe et durant la première communication entre deux groupes.
Etablissement de l'anonymat dans le groupe : la complexité en temps pour établir l'anonymat dans le groupe est évaluée pour les nœuds CA et RA comme suit :

$$\begin{cases} TC(CA) = 2.T_M + (3+k).T_H + (2+k).T_X + k.T_S + T_E \\ TC(RA) = k.T_D + 2.(T_X + T_H) + T_S \end{cases}$$

où k désigne le nombre de nœuds RA dans le groupe.

4.5 Conclusion

Dans ce chapitre, nous avons étudié les protocoles d'anonymat existants et nous avons proposé les protocoles de changement et de camouflage d'identité (ICCP), basés sur certains mécanismes de défense militaire. Le protocole proposé, appelé ICCP, est basé sur l'approche de groupes, et en particulier sur notre architecture hiérarchique (Rachedi et Benslimane, 2006). Nous concevons un mécanisme qui permet à tout nœud d'authentifier d'autres nœuds de façon anonyme. De plus, nous illustrons comment nous pouvons établir une DDMZ (Dynamic Demilitarized Zone) anonyme. En outre, deux sortes de communication intra-groupe sont présentées : la comunication intra-ADDMZ et la communication extra-ADDMZ. De plus, nous avons étudié la communication inter-groupe et nous avons présenté le protocole d'authentification des nœuds CA. L'ICCP est conçu pour résister contre diverses attaques telles que le DoS ou l'attaque par capture. Dans le but d'évaluer l'ICCP, nous avons étudié sa complexité en temps. Aussi, nous avons présenté une analyse de sécurité.

Chapitre 5

Vers une approche inter-couches pour les mécanismes de surveillance

Sommaire

Le système de détection d'intrusions (IDS) pour les réseaux mobiles Ad hoc (MANETs) consiste à contrôler le comportement des nœuds, dans le but de détecter toute activité frauduleuse des nœuds. Certaines solutions existantes traitent ce problème sur chaque couche du modèle OSI séparément. Cependant, de nouveaux types d'attaques apparaissent. Ils sont dus à un comportement malicieux intelligent et constituent des attaques inter-couches. De tels comportements jugés intelligents ne peuvent être détectés au niveau d'une seule couche du modèle OSI. Dans ce chapitre, nous présentons une nouvelle approche inter-couches fondée sur les paramètres des couches physique,

MAC et de routage pour la mise en place d'un mécanisme de contrôle et de surveillance efficace. Nous proposons un nouveau modèle analytique pour illustrer l'effet des différents paramètres sur ces différentes couches. L'impact du taux de signal bruit (SNR) et de la distance entre les nœuds surveillant et surveillé sont clairement introduits (Rachedi et Benslimane, 2008c). De plus, la différence entre la portée du signal, la portée d'interférence et la portée de transmission est prise en compte dans notre modèle. Ce modèle améliore l'évaluation de la coopération des nœuds et réduit le taux de faux positifs dit aussi taux de fausses alarmes (détection d'un comportement malicieux, qui en fait ne l'est pas). L'étude analytique et les résultats de simulations valident notre modèle. De plus, nous montrons, grâce aux résultats des simulations, l'impact de la distance entre les nœuds surveillant et surveillé sur le mécanisme de contrôle. Enfin, nous montrons que notre mécanisme inter-couches a un taux de faux positifs plus faible que le mécanisme classique appelé Watchdog (S. Marti et Baker, 2000) et nous prenons aussi en compte différents paramètres du réseau, tels que la densité des nœuds, la vitesse de déplacement des nœuds et les différentes charges du trafic.

5.1 Introduction

La détection d'un certain type de nœuds ayant un mauvais comportement dans les réseaux mobiles Ad hoc (MANETs) est un des problèmes les plus épineux, car les réseaux MANETs possèdent diverses caractéristiques comme leur propre configuration, une architecture pair à pair ouverte, un réseau sans fil partagé, des contraintes en terme de ressources et une topologie de réseau très dynamique. Ces caractéristiques les rendent vulnérables aux attaques. L'absence de tout système de détection d'intrusions (IDS) de nœuds malicieux pourrait incroyablement réduire la performance du réseau. Les solutions IDS existantes pour les réseaux filaires et les réseaux sans fil avec infrastructure (WLAN) ne peuvent pas être directement appliquées aux réseaux mobiles Ad hoc. De plus, les solutions qui ont déjà été proposées pour les réseaux mobiles Ad hoc ne pouvaient pas prendre en compte toutes les contraintes propres aux réseaux mobiles Ad hoc. En effet, au sein de l'IDS, réseau basé sur la couche routage, toutes les informations peuvent être capturées et analysées par des mécanismes d'audit qui fonctionnent sur des entrées fixes du réseau comme les routeurs par exemple. Ainsi, le trafic du réseau est contrôlé sur les réseaux filaires. Cependant, au sein des réseaux mobiles Ad hoc, les nœuds peuvent seulement surveiller le trafic du réseau à leur portée de transmission radio. Hormis quelques cas rares, un nœud mobile peut ne pas avoir la même observation que ses voisins : lorsqu'une collision a lieu au niveau du nœud moniteur (surveillant) et empêche l'observation du nœud surveillé durant une certaine période. Le nœud surveillé peut agir de façon normale (honnête) ou malicieuse. Cette situation peut être due au problème des nœuds cachés. Ainsi, l'IDS pour les réseaux mobiles Ad hoc doit aussi prendre en compte un autre problème lié au manque d'interaction entre les couches MAC et de routage. Cette vulnérabilité est exploitée par les nœuds malicieux, dans le but de lancer une nouvelle catégorie d'attaques appelées « attaques inter-couches ». En général, ces attaques viennent de la couche MAC mais leur objectif est de créer un déni de service (DoS) au niveau des couches de routage et supérieures.

C'est pourquoi une nouvelle approche est nécessaire pour améliorer le processus de surveillance et de contrôle au sein des réseaux mobiles Ad hoc. D'après nos connaissances, il n'existe aucun travail traitant des paramètres de la couche MAC, dans le but d'améliorer le mécanisme de surveillance et de contrôle.

Dans ce chapitre, nous étudions le mécanisme de contrôle et de surveillance utilisé par l'IDS pour contrôler les activités des nœuds et pour évaluer leur coopération au sein du réseau. Nous nous intéressons au pourcentage de participation des nœuds à l'opération de routage. Le mécanisme de contrôle joue un rôle majeur dans l'évaluation de la réputation des nœuds et dans la mise à jour de leur niveau de confiance. Nous étudions divers problèmes qui ont un impact négatif, en particulier sur le mécanisme de surveillance, comme lorsqu'une collision se produit au niveau du nœud surveillant (avec un IDS) pendant l'opération de surveillance. Cette situation augmente de façon significative le taux de fausses alarmes. Dans le but de réduire le taux de faux positifs et d'améliorer le mécanisme de surveillance, la solution inter-couches est expérimentée. De plus, nous proposons un nouveau modèle analytique qui prend en compte les paramètres des couches MAC, physique et routage, tel que le processus d'acheminement. Le modèle proposé améliore l'évaluation de la coopération des nœuds et réduit le risque d'avoir un taux élevé de faux positifs. Les résultats des simulations illustrent l'impact de ces problèmes sur l'IDS des réseaux mobiles Ad hoc.

Ce chapitre est organisé comme suit : dans la section 5.2, nous présenterons les mécanismes de sécurité existants, leurs avantages et inconvénients. Dans la section 5.3, nous exposons la motivation et la problématique du mécanisme de surveillance au sein des réseaux mobiles Ad hoc. Les régions vulnérables cachées sont étudiées dans le mécanisme de surveillance. Dans la section 5.4, nous décrivons et détaillons notre modèle analytique. Dans la section 5.5, nous présentons les résultats analytiques et les analysons. La section 5.6 est dédiée aux résultats des simulations et à la validation du modèle. Enfin, nous concluons notre étude et présentons nos perspectives.

5.2 Positionnements bibliographiques

Le mécanisme de surveillance fait partie du système de détection des intrusions (IDS), qui est nécessaire à l'évaluation du comportement des nœuds. Ce mécanisme est l'ensemble des actions qui sont utiles pour contrôler le comportement des nœuds. Ces actions dépendent des services que nous voulons contrôler (routage, authentification, etc). La plupart des travaux récents sur l'IDS pour les réseaux mobiles Ad hoc utilisent une architecture distribuée et coopérative. L'aspect coopératif des réseaux mobiles Ad hoc est essentiel pour que les opérations de réseau soient efficaces et pour agir et détecter les intrusions à l'échelle du réseau. En effet, la présence de nœuds non-coopératifs peut affecter le fonctionnement du réseau.

Hang et Cie (Huang et Lee, 2003) ont proposé l'IDS coopératif pour chercher à améliorer l'approche de détection des anomalies et pour fournir davantage de détails sur les divers types d'attaques. Ils ont présenté un ensemble de règles qui peuvent iden-

tifier le type de diverses attaques très connues. D'autres travaux ont étudié le modèle d'IDS fondé sur le groupe pour préserver la batterie et réduire la consommation d'énergie. Dans ce modèle, un groupe de nœuds voisins peut élire un nœud contrôleur qui va jouer le rôle de chef de groupe de façon aléatoire. Ce chef de groupe procède alors aux opérations de l'IDS pour tous les nœuds qui appartiennent au groupe. Toutes les solutions IDS proposées pour les réseaux mobiles Ad hoc nécessitent un modèle de confiance dynamique pour évaluer le comportement des nœuds. Le modèle de confiance dynamique doit être mis à jour régulièrement. C'est pourquoi le système de réputation est exigé pour la mise en place d'un modèle de confiance efficace. Des travaux de recherche ont pris en compte le système de réputation fondé sur l'observation des réactions des nœuds contrôlés. Dans le but d'établir un système de réputation, un mécanisme appelé Watchdog a été proposé (S. Marti et Baker, 2000). Il est basé sur l'acheminement des paquets, qui permet de détecter les nœuds qui ne transmettent pas les paquets pour conserver leur énergie. Watchdog est basé sur la couche de routage, il ne prend pas en compte les paramètres des couches physique ou MAC. L'idée est que le nœud contrôleur ou surveillant peut écouter le trafic entre ses voisins et détecter si les nœuds surveillés transmettent et acheminent les paquets lors des opérations de routage. Le problème majeur des modèles proposés récemment pour surveiller le réseau, tels que Watchdog, est le taux élevé de fausses alarmes. Les concepteurs de l'IDS doivent prendre en compte cette mesure pour déterminer le taux de faux positifs généré au cours de l'opération de surveillance. De plus, les caractéristiques propres aux réseaux mobiles Ad hoc doivent être bien prises en compte.

Malheureusement, les solutions existantes sont affectées par les fausses alarmes. C'est pourquoi, dans ce travail, nous étudions le mécanisme de surveillance et de contrôle dans diverses situations (collision au niveau du nœud surveillant ou du nœud surveillé), dans le but d'améliorer l'observation du nœud surveillant et de réduire le taux de faux positifs du processus de contrôle et de surveillance. Ces améliorations ont un impact positif sur les modèles de confiance. En effet, ces modèles sont, en général, fondés sur les paramètres de réputation utilisés pour évaluer le comportement des nœuds.

5.3 Problèmes cachés au sein du mécanisme de surveillance

5.3.1 Préliminaires

Dans cette partie, nous donnons quelques définitions de base, telles que celles des portées de transmission, de signal et d'interférence. De plus, nous présentons la relation qu'elles entretiennent.

La portée de transmission notée R_t est centrée sur l'émetteur et est définie comme la zone dans laquelle la puissance du signal reçu est suffisante pour décoder correctement le paquet.
La portée de détection de porteuse (portée du signal) notée R_s (carrier sensing range) est la portée au sein de laquelle les nœuds sont capables de détecter le signal, bien qu'une réception correcte du paquet ne soit pas possible (le nœud récepteur peut être

incapable de décoder correctement le paquet qu'il a reçu).
De nombreux chercheurs semblent ignorer la portée d'interférence notée R_i. La région d'interférence désigne la zone ou tout nœud peut transmettre et la collision se produit au niveau du nœud récepteur. Lorsque le nœud récepteur reçoit le paquet du nœud émetteur, toute nouvelle transmission au sein de la zone d'interférence du nœud récepteur crée une collision au niveau de ce nœud. R_i dépend de la distance entre les nœuds transmetteur et récepteur notée d et du rapport signal sur bruit noté SNR, qui doit dépasser un certain seuil T_{SNR} pour savoir si le signal est valide lorsqu'il atteint le nœud récepteur. Ainsi, R_i est définie par l'équation suivante : $R_i = \sqrt[l]{T_{SNR}} * d$ où l dépend du modèle de propagation utilisé (K. Xu et Bae, 2003). La relation entre la portée du signal, la portée d'interférence et la portée de transmission est $R_t < R_i < R_s$, avec $R_s = \beta R_t$ dans un simulateur réseau tel que $NS2$, $\beta = 2.2$ (ns 2, 1999). Le tableau 5.1 reprend nos abréviations et les notations.

R_t	Portée de transmission (Transmission range)
R_s	Portée de détection de porteuse (Carrier sensing range)
R_i	Portée d'interférence (Interference range)
T_{SNR}	Seuil du signal sur bruit (Threshold Signal to Noise Ratio)
TR_A	Région de transmission du nœud A
IR_A	Région d'interférence du nœud A
CS_A	Région à détection de porteuse du nœud A
d_{AB}	Distance entre les nœuds A et B
$TR_{BA}(d_{AB})$	$TR_B - TR_A$
$A_{S1S2}(d_{AB})$	Zone cachée vulnérable au niveau du nœud surveillé ($IR_B - CS_A$)
$A_{S3S4}(d_{AB})$	Zone cachée vulnérable au niveau du nœud surveillant ($IR_A - CS_B$)

TAB. 5.1 – *Tableau d'abréviations et de notations*

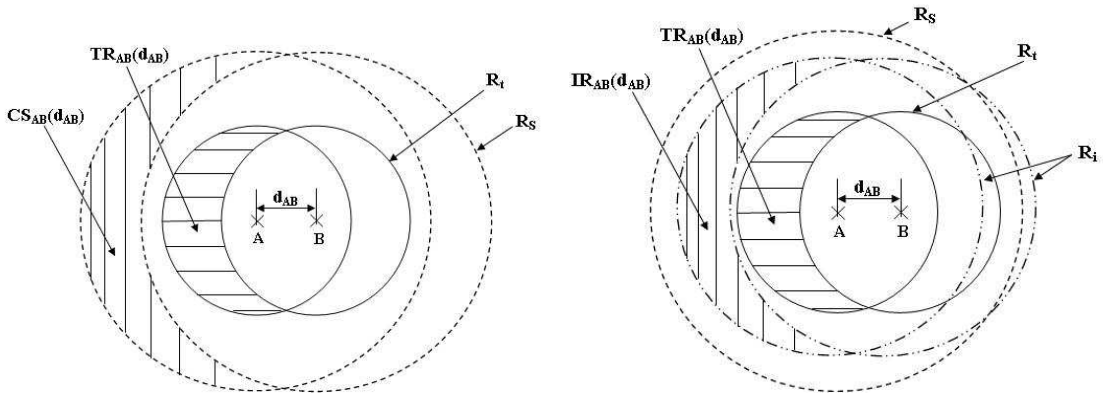
Pour estimer la distance d entre deux nœuds, nous utilisons l'index de force du signal reçu (RSSI). En fonction de la puissance du signal de réception au niveau du nœud récepteur, on peut évaluer la distance de la source émettrice du signal (nœud émetteur) avec une certaine exactitude (M. Maroti, 2005).

Nous proposons dans notre modèle le concept inter-couches pour utiliser les paramètres de la couche physique tels que le SNR, la puissance du signal de réception et les paramètres de la couche MAC au niveau de la couche routage. C'est pourquoi il est nécessaire que les couches du modèle OSI, en particulier les couches : physique, MAC et routage communiquent. Pour mettre en place la conception inter-couches, nous devrons utiliser l'architecture qui permet à chaque couche du modèle OSI d'échanger les informations inter-couches. Plusieurs architectures ont été proposées dans divers articles, comme $ConEx$ par exemple (R. E. Kodikara et Ahlund, 2006). $ConEx$ est fondé sur le module de communication verticale, qui est le processus d'échange de communication inter-couches. Le module de communication verticale est composé des agents de notification d'événements locaux (LENA) au niveau de chaque couche du modèle OSI, qui gère les échanges d'informations au niveau de chaque couche et facilite l'échange d'informations inter-couches. Chaque LENA est connecté à l'agent de no-

tification d'évenements globaux (GENA). Pour plus de détails sur l'architecture $ConEx$, le lecteur peut se reporter au papier original (R. E. Kodikara et Ahlund, 2006).

5.3.2 Diverses régions cachées

Dans cette sous-section, nous décrivons les diverses régions cachées qui ont des impacts importants sur le processus de surveillance et de contrôle.



(a) CS_{AB} et TR_{AB}regions (b) IR_{AB} et TR_{AB} regions

FIG. 5.1 – *Différentes régions cachées, CS_{AB}, IR_{AB} et TR_{AB}*

Les schémas 5.1(a) et 5.1(b) illustrent la région cachée de la portée de détection de porteuse et la région de transmission cachée de deux nœuds voisins A et B. Nous définissons $CS_{AB}(d_{AB})$ en fonction de la distance d_{AB} (entre les nœuds A et B) ; la région de portée de détection de porteuse du nœud A n'inclut pas la région à détection de porteuse du nœud B. De plus, $IR_{AB}(d_{AB})$ est la zone d'interférence du nœud A et n'inclut pas la zone d'interférence du nœud B. Si un nœud dans la zone $CS_{AB}(d_{AB})$ transmet, le signal peut être senti par le nœud A mais pas par le nœud B. La différence entre $CS_{AB}(d_{AB})$ et $IR_{AB}(d_{AB})$ est visible lorsqu'un nœud dans la zone $IR_{AB}(d_{AB})$ transmet : celui-ci peut créer une collision au niveau du nœud récepteur A mais ce n'est pas le cas pour les nœuds situés dans la zone $CS_{AB}(d_{AB})$.

La différence entre $IR_{AB}(d_{AB})$ et $TR(d_{AB})$ n'est autre que le problème des nœuds cachés, qui peut être résolu par exemple avec le mécanisme RTS/CTS du protocole d'accès au canal dans IEEE 802.11 (IEEE802-11, 1999). Ce mécanisme est conçu pour ne prendre en compte que la portée de transmission mais pas la zone d'interférence. Cependant, les nœuds au sein de la zone d'interférence ne peuvent pas décoder les paquets correctement lorsque le nœud A transmet. L'idée fondamentale du mécanisme RTS/CTS est que lorsqu'un nœud veut transmettre un paquet DATA, il envoie le paquet RTS au récepteur. Une fois que le nœud récepteur a reçu le paquet RTS, il répond en envoyant le paquet CTS. Tous les nœuds reçoivent le paquet de contrôle RTS ou CTS, et différent leur transmission pendant un temps défini dans le NAV (Network Allocation Vector) sauf les nœuds destinataires de ces paquets de contrôle. La valeur du NAV

se trouve dans les paquets de contrôle RTS et CTS et est calculée par le nœud émetteur et réactualisée par le nœud récepteur en fonction de la taille du paquet DATA à envoyer. La difficulté se présente lorsqu'un nœud détecte un signal mais ne peut pas le décoder, cela signifie qu'il ne peut pas obtenir le NAV. C'est pourquoi tout nœud utilise un temps d'attente générique appelé EIFS (Extented Interference Frame-Space). IEEE 802.11 n'empêche pas complètement le risque de collisions dues à un nœud caché dans la zone à détection de porteuse.

5.3.3 Difficulté due aux zones cachées

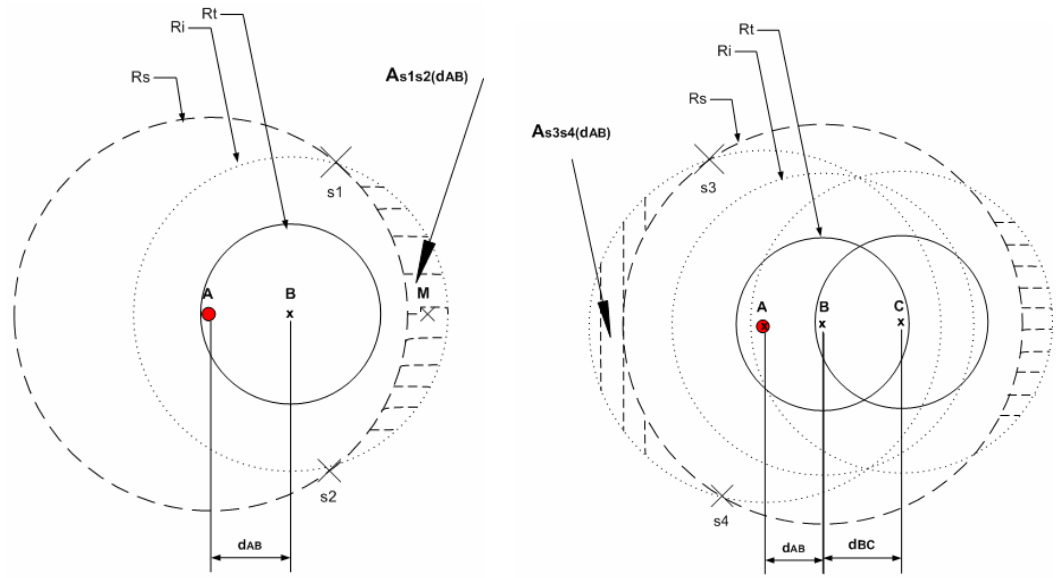
Dans le cadre du processus de surveillance et de contrôle, nous distinguons deux zones cachées essentielles :

A- Zone cachée vulnérable au niveau du nœud surveillé : Un nœud surveillant A veut surveiller un nœud B, qui est son voisin, mais n'a aucune connaissance de l'environnement du nœud B. Soit IR_B la zone d'interférence du nœud surveillé. Si elle n'est pas couverte par la zone à détection de porteuse du nœud surveillant (CS_A), on l'appelle « zone cachée vulnérable au niveau du nœud surveillé » (Cf. figure 5.2(a)). Elle est notée $As_1s_2(d_{AB})$. Si un nœud M est situé dans cette zone vulnérable, il peut réduire le taux de transmission du nœud surveillé B, en générant un important trafic vers un autre nœud. L'objectif de l'attaquant consiste à empêcher le nœud surveillé B de communiquer et à réduire sa capacité à transmettre les paquets. Or, le taux de transmission ou d'acheminement des paquets est utilisé comme métrique pour déterminer la coopération des nœuds au sein du réseau et est aussi appelé taux de réputation. Pour plus de détails, le lecteur peut se reporter à la section 5.2(a).

B- Zone cachée vulnérable au niveau du nœud surveillant : Une autre zone vulnérable peut affecter le mécanisme de surveillance ; cette région n'existe que si la zone d'interférence d'un nœud A n'est pas couverte par la région de portée du signal d'un nœud surveillé B ; nous l'avons appelée « zone cachée vulnérable au niveau du nœud surveillant ». Cette région est illustrée sur la figure 5.2(b) et notée $As_3s_4(d_{AB})$. Si un nœud dans cette zone commence à transmettre, il perturbe l'observation du nœud surveillant. Cela signifie que si un nœud dans la zone $As_3s_4(d_{AB})$ transmet lorsque le nœud A surveille le nœud B, l'observation du nœud surveillant A n'est pas exacte.

5.3.4 Impact de la distance sur les zones cachées

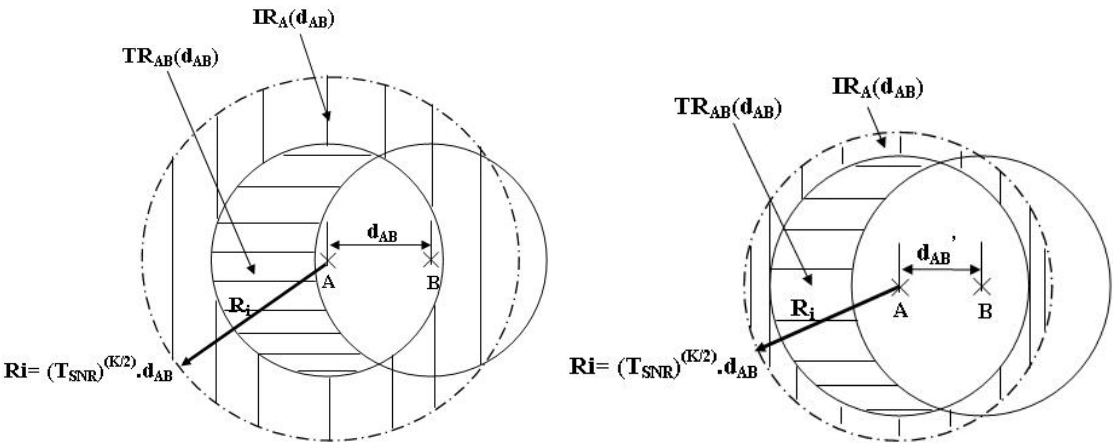
La distance entre le nœud surveillant et le nœud surveillé a un impact important sur le mécanisme de surveillance. Dans le but d'expliquer cet impact, nous prenons l'exemple de deux nœuds voisins A et B. Le nœud B transmet au nœud A. Soit d_{AB} la distance entre A et B. Les figures 5.3(a) et 5.3(b) illustrent cet exemple : sur la figure 5.3(a), la distance entre le nœud A et le nœud B est plus grande que sur la figure 5.3(b). Cela signifie que la zone d'interférence du nœud A et la région $TR_{BA}(d_{AB})$ sont plus grandes dans le cas 5.3(a) que dans le cas 5.3(b). Lorsqu'un nœud A se rapproche d'un nœud B, la région $TR_{BA}(d_{AB})$ devient plus petite et la zone d'interférence peut être



(a) Zone cachée vulnérable au niveau du nœud surveillé

(b) Zone cachée vulnérable au niveau du nœud surveillant

FIG. 5.2 – *Zones cachées vulnérables dans le mécanisme de surveillance*



(a) d_{AB} est grand

(b) d_{AB} est petit

FIG. 5.3 – *Impact de la distance sur les zones cachées et la région d'interférence*

couverte par la zone de transmission lorsque $d_{AB} \leq \frac{R_t}{\sqrt[4]{T_{SNR}}}$. Le nombre moyen de nœuds dans la région $TR_{BA}(d_{AB})$ dépend de la distribution des nœuds et du modèle de mobilité. Plus la région $TR_{BA}(d_{AB})$ est grande, plus la probabilité d'obtenir un grand nombre (k) de nœuds dans cette région est grande.

5.4 Modèle proposé

Dans cette partie, nous présentons notre modèle analytique qui a pour but d'améliorer le processus de surveillance. L'idée consiste à déterminer les conditions favorables à une surveillance qui permet d'éliminer les fausses alarmes. En effet, les fausses alarmes nuisent non seulement au système de réputation des nœuds, mais aussi à l'évolution du modèle de confiance.

5.4.1 Modèle de réseau

Dans notre modèle, nous supposons que les nœuds sont distribués au sein d'une topologie qui suit un processus Poisson bidimensionnel avec le paramètre λ. Nous utilisons le modèle de propagation TWO-RAY GROUND avec un seuil pour le SNR (T_{SNR}) fixé à $10db$. La portée d'interférence est $R_i = \sqrt[l]{10} * d = 1.78 * d$, où $l = 4$ (K. Xu et Bae, 2003). Tous les nœuds ont la même portée de transmission (R_t) et la même portée de détection de porteuse (R_s). Cela signifie que les nœuds au sein d'un cercle de rayon R_t centré au niveau du transmetteur peut être capable de recevoir les paquets correctement. De plus, le nombre moyen de nœuds au sein des portées de signal, d'interférence et de transmission d'un rayon de R_s, R_i et R_t respectivement est $N_j \approx \lambda \pi R_j^2$ où $j = \{s, i, t\}$ (Takagi et Kleinrock, 1984).

Avec les paramètres de Poisson, la probabilité d'obtenir k nœuds dans la zone $TR_{BA}(d_{AB})$ est notée $p(k, TR_{BA}(d_{AB}))$ et calculée ainsi :

$$p(k, TR_{BA}(d_{AB})) = e^{-\lambda TR_{BA}(d_{AB})} \frac{(\lambda TR_{BA}(d_{AB}))^k}{k!} \tag{5.1}$$

Le calcul est le même pour $CS_{BA}(d_{AB})$ et $IR_{BA}(d_{AB})$, car elle est proportionnelle à la distance d_{AB}.

5.4.2 Modèle de surveillance et de contrôle

Un événement perturbateur dans le processus de surveillance se produit lorsqu'un nœud surveillé transmet correctement pendant qu'au moins un nœud dans la zone d'interférence du nœud surveillant et hors de la portée de détection de porteuse du nœud surveillé (As_3s_4) transmet. En d'autres termes, le nœud surveillant peut surveiller correctement ses voisins si les deux conditions suivantes sont vérifiées :

– *Première condition :* le nœud surveillé transmet un paquet à un autre nœud parmi ses voisins avec succès.
– *Deuxième condition :* le nœud surveillant peut entendre correctement la transmission du nœud surveillé. Aucun nœud dans la zone d'interférence du nœud surveillant et hors de la zone à détection de porteuse du nœud surveillé ($As_3s_4(d_{AB})$) ne transmet.

Le nœud surveillant doit évaluer la probabilité que les deux conditions soient remplies pour calculer la probabilité d'observer correctement le nœud surveillé lorsqu'il transmet. Cette probabilité est notée P_w :

$$P_w = P\{\text{condition 1}\}.P\{\text{condition 2}\} \tag{5.2}$$

5.4.3 Probabilité que la condition 1 soit vérifiée

La probabilité que la condition 1 soit remplie est définie comme une transmission de paquets réussie par le nœud surveillé. Elle est notée P_{succ} dans notre modèle. Elle montre la probabilité qu'un nœud surveillé parvienne à accéder au canal pour transmettre un paquet émis par le nœud surveillant. Cette probabilité peut nous donner des informations sur la capacité des nœuds surveillés à transmettre les paquets. Dans le but de calculer P_{succ}, nous devons calculer la probabilité τ qu'un nœud transmet dans un intervalle de temps aléatoire. τ doit prendre en compte deux scénarios possibles en terme de trafic : les cas saturé et non saturé. Pour le cas saturé, le trafic est intensif ; cela signifie que les nœuds ont toujours un paquet à transmettre. De nombreuses recherches ont été menées pour calculer τ, avec la supposition que $R_t = R_i = R_s$ (Bianchi, 2000)(Takagi et Kleinrock, 1984). Cependant, d'après nos connaissances, aucune étude ne prenait en compte la différence entre les portées de transmission, d'interférence et de détection de porteuse. Pour le cas non-saturé, la transmission des nœuds dépend de la probabilité q qu'un nœud ait un paquet à transmettre. Dans le but de calculer τ en fonction de la probabilité q et de la probabilité de collision p, nous utilisons le même résultat que celui obtenu en (Hung et Marsic, 2007)(D. Malone, 2006). Ces recherches sont fondées sur le modèle proposé par Bianchi (Bianchi, 2000), étendu et amélioré pour le cas non-saturé. Dans notre cas, P_{succ} se calcule comme suit :

$$P_{succ} = \frac{N_s\tau(1-\tau)^{N_s-1}}{P_{tr}} \tag{5.3}$$

où N_s est le nombre de nœuds qui sont capables d'écouter le signal du nœud émetteur. D'autre part, N_s est aussi le nombre de nœuds présents dans la zone à détection de porteuse du nœud émetteur. P_{tr} désigne la probabilité qu'au moins une transmission se produise dans l'intervalle de temps étudié. Dans le cas où N_s rivalisent pour l'accès au canal, P_{tr} se calcule comme suit :

$$P_{tr} = 1 - (1-\tau)^{N_s} \tag{5.4}$$

La probabilité τ est calculée en fonction des paramètres de l'algorithme de backoff exponentiel (IEEE802-11, 1999), de la probabilité de collision p et de la probabilité q. Le

cas saturé est en fait un cas spécifique du cas non-saturé, qui existe lorsque $q = 1$. La probabilité τ est définie par l'équation suivante :

$$\tau = \frac{2(1-2p)q}{q[(W_0+1)(1-2p) + W_0 p(1-(2p)^m)] + \psi} \tag{5.5}$$

où $\psi = 2(1-q)(1-p)(1-2p)$. La fenêtre minimum de contention du backoff est $W_0 = CW_{min} + 1$ et la fenêtre maximum de contention du backoff est appelée $CW_{max} = 2^m W_0$. Ainsi, $m = log_2 \frac{CW_{max}}{CW_0}$. Pour plus de détails, le lecteur peut se référer à l'étude menée en (F. Daneshgaran, 2008)(Hung et Marsic, 2007)(D. Malone, 2006).

La probabilité de collision p, nécessaire pour calculer τ, désigne la probabilité qu'au moins un nœud dans la zone d'interférence (R_i) transmette en même temps que le nœud émetteur. Ainsi, p peut être calculée comme suit :

$$p = 1 - (1-\tau)^{N_i - 1} \tag{5.6}$$

où N_i est le nombre de nœuds dans la zone d'interférence. Les hypothèses prises en compte pour N_i, peuvent être calculées comme suit : $N_i \simeq \lambda \pi R_i^2 = \lambda \pi \sqrt{T_{SNR}}(d_{AB})^2$.

La modélisation de la probabilité q est fondée sur la charge de trafic qui a pour caractéristique le paramètre $\lambda^\star$. Celui-ci présente le taux d'arrivée des paquets au nœud et est mesuré en paquets par seconde (pkt/s). Comme pour (F. Daneshgaran, 2008) (D. Malone, 2006), nous supposons que le processus d'arrivée du paquet est un mécanisme qui suit une loi de Poisson. Ainsi, la probabilité q peut être correctement évaluée comme suit :

$$q = 1 - \exp^{\lambda^\star . T_{av}} \tag{5.7}$$

où T_{av} est le temps moyen prévu par intervalle, calculé en fonction de P_{tr}, P_{succ}, du temps d'une transmission réussie (T_s) et du temps prévu en cas de collision (T_c) :

$$T_{av} \quad = (1-P_{tr}).\sigma + P_{tr}(1-P_{succ}).T_c + P_{tr}P_{succ}.T_s$$

où T_c et T_s sont les durées moyennes au cours desquelles un canal est occupé en raison d'une collision et d'une transmission de données réussies. T_c et T_s peuvent être calculées ainsi :

$$\begin{cases} T_c = H + PL + ACK_{timeout} \\ T_s = H + T_{PL} + SIFS + 2.\delta + T_{ACK} + DIFS \end{cases}$$

où H désigne la durée de transmission des en-têtes des couches physique et MAC. T_{ACK} désigne la durée de transmission d'un ACK ; T_{PL} est la durée de transmission de données et MPD est le délai de propagation maximum (Maximum Propagation Delay). De plus, $ACK_{timeout} = SIFS + T_{ACK} + DIFS$, où SIFS et DIFS sont les acronymes pour Short Inter-Frame Space et Distributed Inter-Frame Space.

5.4.4 Probabilité que la condition 2 soit vérifiée

La probabilité que la condition 2 soit remplie nous donne quelques informations sur la qualité d'observation d'un nœud surveillant. Cette probabilité est égale à 1 lorsqu'aucun nœud dans la zone $As_3s_4(d_{AB})$ ne transmet au cours d'une période vulnérable. Cette période dépend de la durée de transmission T_{av} d'un paquet : lorsqu'un nœud B commence à transmettre en t_s, l'intervalle de temps vulnérable est [$t_s - T_{av} - 1$, $t_s + T_{av} - 1$]. Les nœuds dans la région $As_3s_4(d_{AB})$ doivent rester silencieux pendant une durée μ avec $\mu = (T_{av}/\sigma)$, car un nœud dans les zones à détection de porteuse et d'interférence attend pendant un EIFS lorsqu'il ne peut pas calculer un vecteur NAV. Si l'EIFS est plus grand qu'un T_{av}, le paquet peut être reçu correctement par le nœud C. Dans le cas contraire, le paquet ne peut pas être reçu correctement. La région $As_3s_4(d_{AB})$ peut être nulle si elle est couverte par la zone à détection de porteuse d'un nœud B. Dans le cas contraire, nous définissons P{cond.2}(d_{AB}), avec $d_{AB} > \frac{R_s}{1+\sqrt[k]{T_{SNR}}}$ ainsi :

$$\begin{aligned} P\{cond.2\}(d_{AB}) &= \Big(\sum_{k=0}^{\infty}(1-\tau)^k \frac{(N_h)^k}{k!} e^{-N_h.\mu}\Big) \\ &= e^{-\tau N_h.\mu} \end{aligned}$$

où $N_h = \lambda A_{S3S4}(d_{AB})$.

L'équation finale définissant P{cond.2}(d_{AB}) est la suivante :

$$P\{cond.2\}(d_{AB}) = \begin{cases} 1 & \text{si } d_{AB} \leq \varphi \\ e^{-\tau N_h.\mu} & \text{sinon} \end{cases} \tag{5.8}$$

où $\varphi = \frac{R_s}{1+\sqrt[k]{T_{SNR}}}$.

Dans le but de calculer $As_3s_4(d_{AB})$, nous calculons la zone d'intersection entre la zone de détection de porteuse et la zone d'interférence de deux nœuds X et Y, en supposant que la distance entre ces deux nœuds est d.

$$Ar_{\{X\cap Y\}}(d) = R_s(arccos(\alpha) - \alpha\sqrt{1-\alpha^2}) + R_i(arccos(\beta) - \beta\sqrt{1-\beta^2})$$

Où $\alpha = \frac{R_s^2 - R_i^2 + d^2}{2dR_s}$ et $\beta = \frac{R_i^2 - R_s^2 + d^2}{2dR_i}$

Ainsi, $As_3s_4(d_{AB})$ se calcule comme suit :

$$A_{S3S4}(d_{AB}) = \begin{cases} 0 & \text{si } d_{AB} \leq \varphi \\ \pi R_s^2 - Ar_{\{A\cap B\}}(d_{AB}) & \text{sinon} \end{cases}$$

A partir des équations 5.2 et 5.8, nous pouvons alors calculer $P_w(d_{AB})$ comme suit :

$$P_w(d_{AB}) = \begin{cases} P_{succ} & \text{si } d_{AB} \leq \varphi \\ P_{succ}.e^{-\tau N_h.\mu} & \text{sinon} \end{cases} \tag{5.9}$$

Le rapport de réputation du nœud surveillé B, généré par le nœud surveillant A, est défini comme suit :

$$R_{A,B}(d_{AB}) = \eta.P_w(d_{AB}) \tag{5.10}$$

où η est le taux de transmission évalué par le nœud surveillant.

$$\eta = \left(\frac{\text{\#nombre de paquets retransmis observés}}{\text{\#nombre total de paquets bien reçus par le nœud surveillé}}\right) \tag{5.11}$$

Contrairement au mécanisme Watchdog, le taux de transmission ou d'acheminement des paquets dans notre modèle est le rapport du nombre de paquets observés sur le nombre total de paquets envoyés par le nœud surveillant et reçus correctement par le nœud surveillé (cf. équation 5.11). Cependant, dans Watchdog, le dénominateur est le nombre total de paquets envoyés au nœud surveillé sans prendre en considération la bonne réception ou non des paquets. Cette différence a un important impact sur le processus de surveillance, car tous les paquets envoyés au nœud surveillé ne sont pas automatiquement reçus avec succès si le nœud surveillant ne considère que la couche de routage, sans prendre en compte l'état du canal. Dans le but d'éviter la vulnérabilité de l'équation 5.11, et d'évaluer correctement le nombre total de paquets (sujets de surveillance) bien reçus par le nœud surveillé, nous prenons en compte l'approche inter-couches, ce qui confère son originalité à notre contribution. Cette approche permet d'évaluer correctement le taux de transmission η au niveau de la couche de routage en prenant en compte le paquet ACK au niveau de la couche MAC. Le nœud surveillant a besoin de cette information inter-couches pour être sûr que le nœud surveillé a reçu correctement le paquet au niveau de la couche de routage. Même si le trafic réseau varie, la probabilité qu'un nœud surveillé reçoive correctement le paquet de la part du nœud surveillant permet au nœud surveillant d'évaluer le trafic dans la zone d'interférence du nœud surveillé.

Une fois que le nœud surveillant a calculé le rapport de réputation R_{AB} du nœud B, il peut prévoir le nombre de paquets qui peuvent être retransmis par le nœud B. Si la différence entre le nombre prévisible et le nombre observé est grande, le nœud surveillant peut en déduire que le nœud surveillé a changé son comportement ou bien que son environnement a changé par rapport au calcul d'évaluation de départ. Dans cette situation, le nœud surveillant a besoin de mettre à jour l'évaluation du nœud surveillé. Le nombre prédictible de retransmissions du nœud surveillé doit prendre en compte les trois paramètres importants pour les mécanismes de surveillance qui sont les suivants : la densité des nœuds, la mobilité des nœuds et le trafic réseau. Ce nombre prédictible de paquets peut être calculé comme suit :

$$\text{\#paquets retransmis} = \frac{(\text{\#total des paquets envoyés}).R^*_{(AB)}}{P_w} \tag{5.12}$$

où $R^*_{(AB)}$ est le rapport d'évaluation déjà effectué.

Le but de l'équation 5.12 est d'analyser le comportement du nœud surveillé dans les mêmes conditions d'évaluation que P_W. P_W dépend des probabilités P{condition 1} et P{condition 2}. P{condition 1} prend en compte la variation du trafic réseau par la probabilité q définie dans l'équation 5.7. Cependant, P{condition 2} prend en considération

la densité des nœuds dans la région cachée vulnérable au niveau du nœud surveillant notée $As3s4(d)$ (Cf. figure 5.2(b)). Ainsi, cette probabilité dépend de la distance entre les nœuds surveillant et surveillé (d). Lorsque nous parlons des mêmes conditions de calcul pour l'évaluation P_W, cela veut dire que l'évaluation est effectuée avec les mêmes valeurs de probabilité q (trafic réseau) et la même distance entre les nœuds surveillant et surveillé (d). De plus, dans notre modèle, l'évaluation de P_W est dynamique pour chaque paquet transmis au nœud surveillé (sujet de surveillance). D'où l'équation 5.12, qui permet de discuter le comportement du nœud surveillé dans les mêmes conditions de calcul que P_W.

Avec ce modèle, nous pouvons répondre à la question de départ : Est-ce que le nœud surveillé refuse de coopérer ou bien est-il incapable de coopérer ? Nous avons apporté une amélioration dans le mécanisme de surveillance en réduisant le taux de fausses alarmes. Cette améloration a un impact positif sur le modèle de confiance, car la majorité des modèles de confiance utilisent l'évaluation du comportement des nœuds, et en particulier le paramètre de réputation.

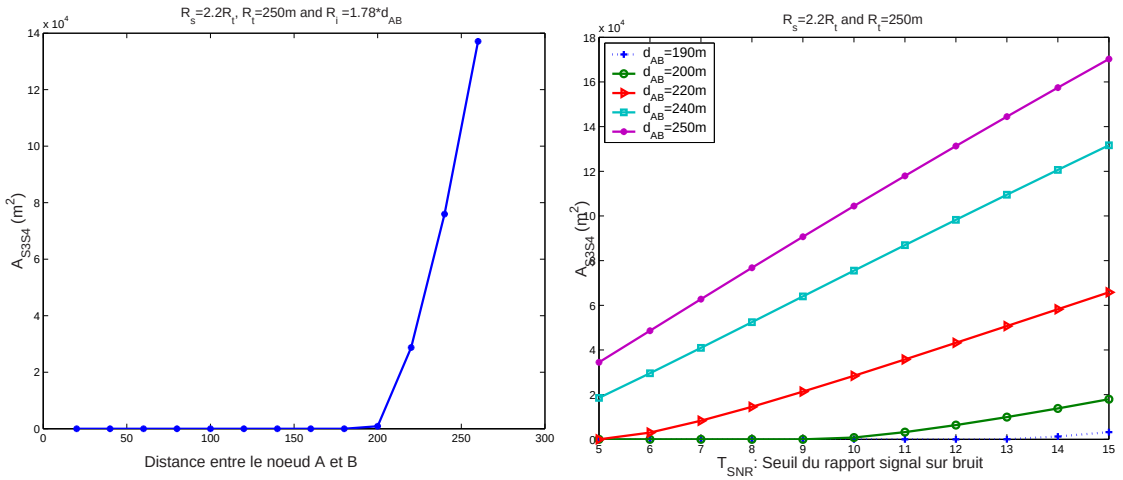
5.5 Résultats numériques et analyses

Dans cette section, nous présentons les résultats numériques du modèle proposé avec différentes situations (variation de la distance entre les nœuds surveillant et surveillé), et avec la prise en compte de l'impact de la probabilité de transmission τ. Les paramètres du réseau dans le cas de IEEE 802.11 sont présentés dans la table 5.2.

Débit de transmission	$1Mbit/s$
Taille des paquets	1024 Bytes
Taille de l'en-tête MAC (MAC header)	24 Bytes
Taille de l'en-tête physique (Physical header)	16 Bytes
Taille du paquet ACK	14 Bytes
Taille du paquet CTS	14 Bytes
Taille du paquet RTS	20 Bytes
Temps slot (Slot time) σ	$20\mu s$
δ	$1\mu s$

TAB. 5.2 – *Paramétres du réseau*

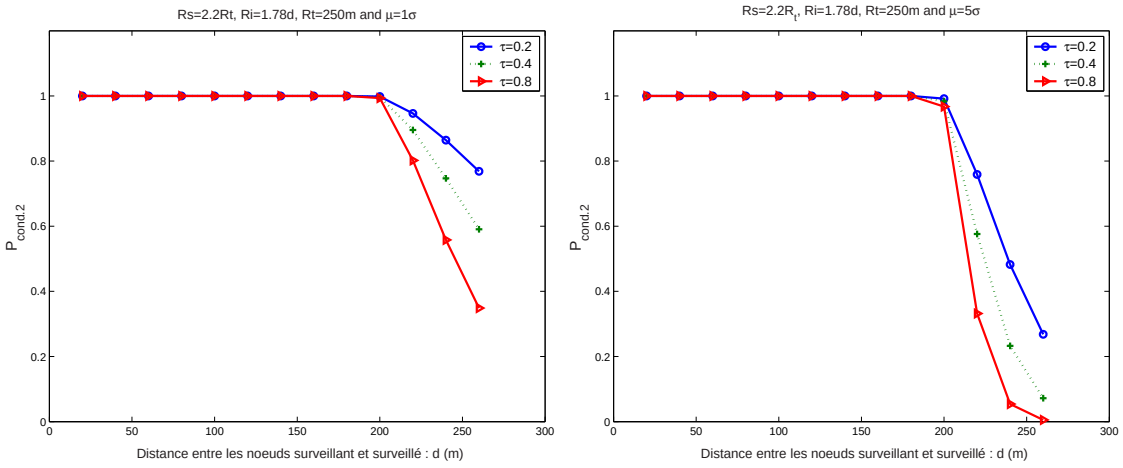
Dans le but de montrer l'impact de la distance entre le nœud surveillant et le nœud surveillé sur la région vulnérable A_{S3S4}, nous traçons dans la figure 5.4(a) la région cachée A_{S3S4}, en fonction de la distance entre les nœuds A et B avec $550m$ de porteuse de transmission (R_s) et $R_i = \sqrt[4]{10}.d_{AB}$ de rayon d'interférence. Quand la distance entre les deux nœuds est inférieure à $200m$ et $A_{S3S4} = 0$, alors cela veut dire que la région A_{S3S4} est couverte par la région de la porteuse de signal du nœud B. Dans la figure 5.4(b), nous présentons la région vulnérable cachée du surveillant (moniteur) en fonction du seuil de rapport signal sur bruit, dans le but d'étudier l'impact de la sensibilité du



(a) A_{S3S4} en fonction de la distance d_{AB} (b) A_{S3S4} en fonction du T_{SNR}

FIG. 5.4 – *Région cachée A_{S3S4} en fonction de T_{SNR} et de la distance d_{AB}*

signal sur le processus de surveillance, et en particulier sur la région vulnérable A_{S3S4}. Nous remarquons que quand $d_{AB} \leq 200m$ et $T_{SNR} = 10$, la région vulnérable est nulle ($A_{S3S4} = 0$). Cependant, $A_{S3S4} \neq 0$ lorsque $T_{SNR} > 10$. Donc, le rayon d'interférence R_i augmente avec l'augmentation de la sensibilité du signal et la région A_{S3S4} devient moins couverte par la porteuse de transmission (R_s) du nœud B ($A_{S3S4} \neq 0$). Nous pouvons en déduire que la sensibilité du signal a un impact important sur le mécanisme de surveillance. Le compromis entre T_{SNR} et la distance entre les nœuds surveillant et surveillé peut améliorer de manière significative le processus de surveillance.



(a) cas de $\mu = \sigma$ (b) cas de $\mu = 5\sigma$

FIG. 5.5 – *$P\{cond.2\}$ en fonction de la distance entre les nœuds A et B*

$P\{cond.2\}$ est un paramètre important dans le modèle proposé. Par conséquent,

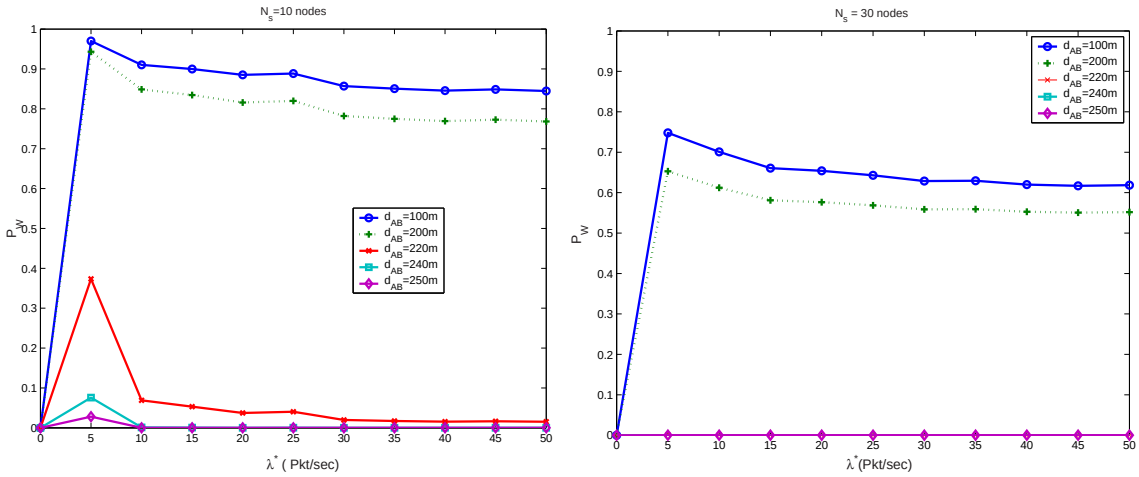
nous étudions $P\{cond.2\}$ avec différentes distances entre les nœuds surveillant et surveillé. De plus, nous introduisons la probabilité et la durée de transmission dans le but de montrer leur impact sur le mécanisme de surveillance. Dans la figure 5.5(a), nous illustrons la probabilité qu'aucun nœud dans la région $A_{s3s4}(d)$ ne transmette pendant la durée $\mu = \sigma$. Nous remarquons que la probabilité $P\{cond.2\}$ est égale à un quand la distance entre A et B est inférieure à 200 mètres. Cela est dû à la région $A_{s3s4}(d)$ qui est couverte par la région à détection de porteuse du nœud B. Cependant, quand la distance entre le nœud A et le nœud B devient grande, $P\{cond.2\}(d)$ diminue et elle décroît rapidement quand la probabilité de transmission τ est grande. Par exemple, quand $d_{AB} = 250m$ et $\tau = 0.2$ alors $P\{cond.2\} = 0.75$, par contre, quand $\tau = 0.8$ avec la même distance d_{AB}, $P\{cond.2\}$ décroît de manière significative jusqu'à $0,35$. La figure 5.5(b) montre $P\{cond.2\}(d)$ avec une durée de transmission plus grande ($\mu = 5\sigma$). Nous constatons que $P\{cond.2\}(d)$ est petite dans le cas où la durée de transmission est $\mu = \sigma$. Quand la durée de transmission est grande, cela implique que la durée de surveillance est grande aussi, et que le risque d'avoir une collision au niveau du nœud surveillant est important. Donc, plus la durée de transmission est petite, plus l'opération de surveillance est efficace. Nous pouvons en conclure que le seuil T_{SNR}, la distance entre les nœuds surveillant et surveillé et le temps de transmission μ ont un impact important sur le mécanisme de surveillance.

5.5.1 Cas saturé et cas non-saturé

Nous discutons dans le cas général de la probabilité appelée P_w que le nœud surveillant surveille correctement le nœud surveillé. Le cas général englobe deux types de trafic : le cas saturé et le cas non saturé. Cependant, le cas saturé est un cas particulier du cas non saturé avec une probabilité $q = 1$ (le nœud a toujours un paquet à transmettre). Nous étudions le cas général via la variation des paramètres suivants : le nombre de paquets arrivés dans la file ($\lambda^\star$) pour étudier la probabilité q, la distance entre les nœuds surveillant et surveillé (d_{AB}) et la densité des nœuds dans la région de portée du signal N_S.

Les figures 5.6(a) et 5.6(b) montrent la probabilité que le nœud surveillant A ait une observation correcte du nœud surveillé B (cette probabilité est appelée P_w) en fonction du trafic d'arrivée des paquets dans la file ($\lambda^\star$) avec deux densités de nœuds différentes : $N_s = 10$ et $N_s = 30$. Dans la figure 5.6(a), nous remarquons que la valeur maximum de P_w est égale à 0.95 quand le nombre d'arrivées des paquets dans la file est d'environ $5Paquet/s$ avec une distance entre les nœuds A et B égale à $100m$. Cependant, P_w diminue quand $\lambda^\star$ augmente, même si $\lambda^\star = 50Paquet/s$. P_w ne diminue pas au-delà de 0.85. P_w diminue de manière significative quand la distance entre les nœuds A et B est de plus de $200m$. Nous constatons que quand $d_{AB} = 220m$ et $\lambda^\star \geq 10Paquet/s$, P_w diminue de 75%. Quand nous augmentons la densité des nœuds dans la région de portée du signal $N_s = 30$ (figure 5.6(b)), nous observons que P_w diminue d'environ 20% en comparaison avec le cas d'une faible densité de nœuds. De plus, P_w est nulle quand la distance d_{AB} est supérieure à $200m$. Nous pouvons dire que malgré le fait que la charge de trafic des paquets et la densité des nœuds ont un impact sur le mécanisme

de surveillance, la distance entre les nœuds surveillant et surveillé a un impact plus négatif sur le mécanisme de surveillance et particulièrement sur l'observation du nœud surveillant.

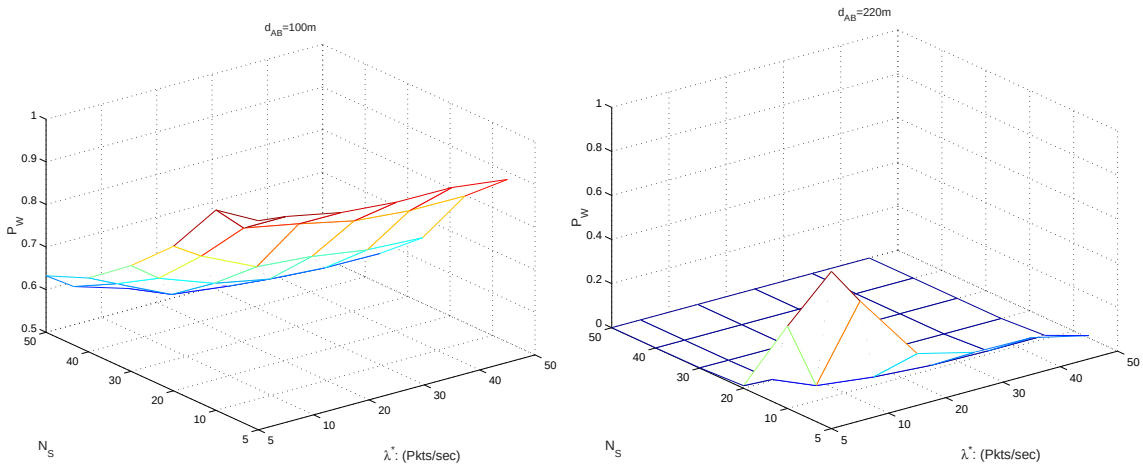


(a) cas de $N_s = 10$ (b) cas de $N_s = 30$

FIG. 5.6 – *P_w en fonction de la densité du trafic $\lambda^\star$*

Dans les figures 5.7(a) et 5.7(b), nous traçons deux cas de probabilité P_w quand $d_{AB} = 100m$ et $d_{AB} = 220m$ en fonction de la densité des nœuds (N_s) et du taux d'arrivée des paquets dans la file ($\lambda^\star$). Nous observons que dans le cas de $d_{AB} = 100m$ (figure 5.7(b)), P_w diminue rapidement quand la densité des nœuds augmente et P_w diminue moins rapidement quand $\lambda^\star$ augmente. Cependant, quand les deux paramètres N_s et $\lambda^\star$ augmentent, P_w diminue de manière significative, cela implique que l'observation du nœud surveillant n'est pas correcte dans cette situation. Dans la figure 5.7(b), nous remarquons que P_w est très faible et que P_w est nulle avec $N_S = 20$ nœuds et $\lambda^\star = 20Pkt/sec$. La mauvaise situation du mécanisme de surveillance est obtenue quand la distance d_{AB} est supérieure à $200m$.

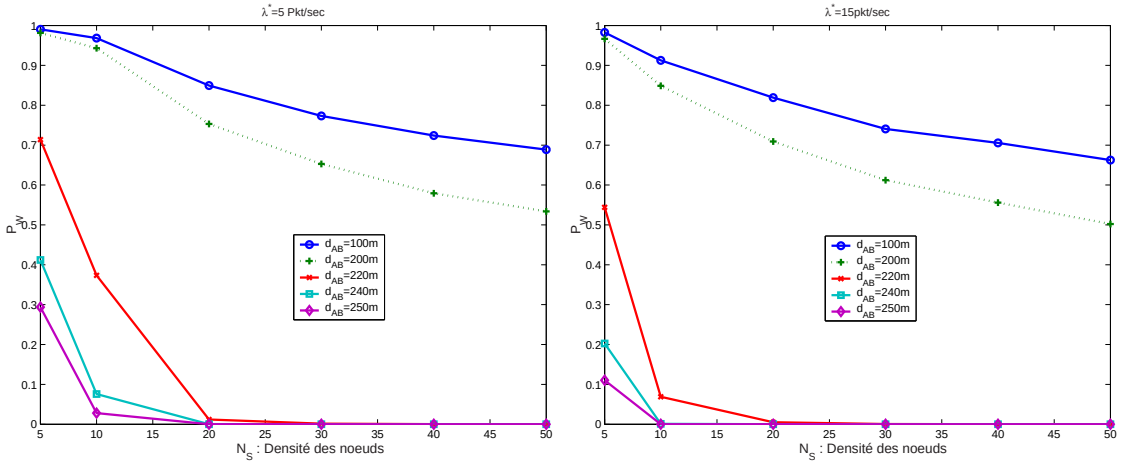
Dans les réseaux sans fil, la densité des nœuds a non seulement un impact important sur la performance du réseau, mais aussi sur le mécanisme de surveillance. Dans le but d'étudier cet impact sur le mécanisme de surveillance, nous traçons dans les figures 5.8(a) et 5.8(b), P_w en fonction de la densité des nœuds avec deux cas de charges de trafic : $\lambda^\star = 5pkt/s$ et $\lambda^\star = 15Paquet/s$. Nous remarquons que P_w est comparable dans les deux cas, mais elle se dégrade un peu plus quand la densité des nœuds augmente (avec $d_{AB} \leq 200m$). Nous constatons que P_w atteint sa meilleure valeur (0.98) avec une faible densité de nœuds $N_s = 5$ et avec une distance $d_{AB} = 100m$. Cependant, P_w diminue quand la densité des nœuds augmente et atteint 0.7 avec $N_s = 50$ nodes. De plus, nous remarquons que P_w diminue de manière significative quand la distance entre les nœuds A et B est supérieure à $200m$. P_w diminue de 30% à 60% dans les cas où la distance $d_{AB} = 240m$ et $d_{AB} = 250m$ avec une faible densité de nœuds ($N_s = 5$). P_w est égale à zéro quand la distance d_{AB} est supérieure à $200m$ et quand la densité



(a) cas de $d_{AB} = 100m$ (b) cas de $d_{AB} = 220m$

FIG. 5.7 – *P_w en fonction de la densité du trafic $\lambda^\star$ et la densité des nœuds (N_s)*

du trafic est supérieure à $20Paquet/s$ ($\lambda^\star \geq 20pkt/s$). Cette situation représente de mauvaises conditions pour le mécanisme de surveillance. Quand la densité du trafic $\lambda^\star$ augmente (dans la figure 5.8(b)), nous remarquons que P_w diminue de 15% dans le cas où $d_{AB} > 200m$.



(a) cas de $\lambda^\star = 5Pkt/sec$ (b) cas de $\lambda^\star = 15Pkt/sec$

FIG. 5.8 – *P_w en fonction de la densité des nœuds N_s*

Dans le but de montrer l'impact des deux paramètres (la densité du trafic et la distance entre les nœuds surveillant et surveillé) sur le mécanisme de surveillance, et particulièrement sur P_w, nous traçons dans la figure 5.9, P_w en fonction de $\lambda^\star$ et d_{AB} avec la densité des nœuds dans la région d'une portée de transmission $N_s = 10$. Nous constatons clairement que même si la densité du trafic a un impact sur P_w, la distance d_{AB} a

un impact plus négatif quand elle est supérieure ou égale à $200m$ ($d_{AB} \geq 200m$). Cependant, lorsque la distance est inférieure à $200m$, nous remarquons qu'aucun impact n'est observé sur le mécanisme de surveillance en comparaison avec la densité du trafic $\lambda^{\star}$.

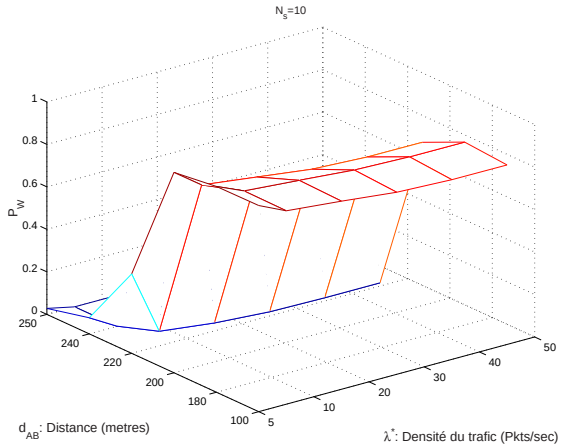


FIG. 5.9 – *P_w en fonction de la densité du trafic $\lambda^{\star}$ et de la distance d_{AB} ($N_s = 10$)*

Dans la figure 5.10, nous montrons l'impact des deux paramètres (la densité des nœuds et la distance d_{AB}) sur l'observation du nœud surveillant P_w dans le cas où $\lambda^{\star} = 15Pkt/s$. Nous observons que la densité des nœuds n'a pas d'impact significatif sur l'observation du surveillant quand la distance d_{AB} est inférieure à un certain seuil ($200m$). Cependant, quand la distance est plus grande que le seuil, P_w diminue de manière significative par rapport à l'augmentation de la densité des nœuds.

Pour conclure, nous pouvons dire que les paramètres suivants : la distance entre les nœuds surveillant et surveillé (d_{AB}), la densité des nœuds dans la région de la portée du signal (N_s) et la densité du trafic ou le taux d'arrivée des paquets dans le buffer ($\lambda^{\star}$) ont des impacts relatifs sur le mécanisme de surveillance, mais le paramètre le plus important est la distance entre les nœuds A et B (d_{AB}), car elle peut réduire de manière significative P_w (plus de 70% de dégradation de la qualité d'observation du nœud surveillant). Par conséquent, la distance d_{AB} est un facteur clé pour la région vulnérable A_{S3S4}, car cette région devient non couverte quand la distance est grande. De plus, réduire P_w permet d'augmenter la probabilité des fausses alarmes.

5.6 Résultats des simulations et discussions

Cette section est divisée en deux parties. Dans la première partie, nous étudions la question suivante : comment la zone d'interférence affecte-t-elle le mécanisme de surveillance via la distance entre les nœuds surveillant et surveillé et la densité du trafic réseau ? Dans la deuxième partie, nous présentons une étude comparative entre notre mécanisme de surveillance inter-couches et le mécanisme existant appelé Watchdog (S. Marti et Baker, 2000). En outre, nous étudions le cas général de la densité des nœuds

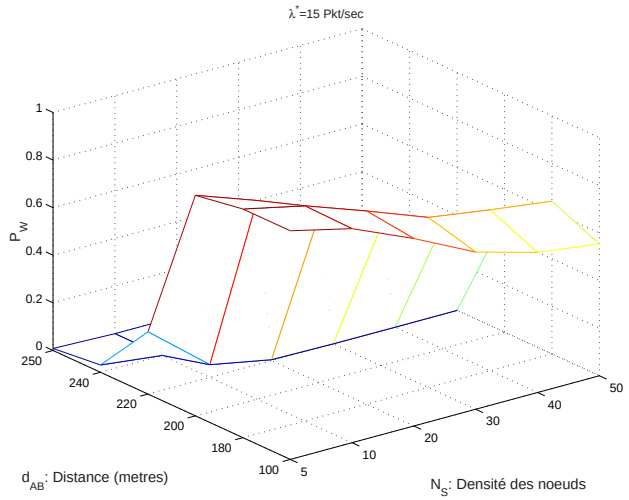


FIG. 5.10 – *P_w en fonction de la densité des nœuds N_s et de la distance d_{AB} ($\lambda^\star = 15ptk/s$)*

avec différentes vitesses de mobilité des nœuds. Dans le but de simuler tous ces cas de figure, nous avons implémenté les deux mécanismes (Watchdog et notre proposition inter-couches) sur le simulateur NS2 (ns 2, 1999). Les paramètres de simulation de NS2 sont montrés dans le tableau 5.3.

Paramètre	Valeur dans notre simulation
Nombre de nœuds (N)	[5 - 50]
Technologie MAC	IEEE 802.11
Protocole de routage	DSR
Taille de la surface (mxn)	$670 \times 670m^2$
Mobilité	[5 - 40 m/s]
Portée de transmission (R_t)	250 m
Portée de détection de porteuse (R_s)	550 m
Taille des paquets	512, 1000 bytes
Densité du trafic	[20 - 60 Kbit/s]
Temps de simulation	150 sec

TAB. 5.3 – *Paramètres de simulation*

Nous définissons une nouvelle métrique pour évaluer le mécanisme de surveillance est le faux positif appelé FP. Cette métrique nous permet de savoir quand le nœud surveillé réussit à acheminer le paquet mais le nœud surveillant n'a pas pu observer cette opération. Cette métrique est calculée comme suit :

$$Fp = 1 - \eta \tag{5.13}$$

où η représente le taux moyen d'acheminement des paquets défini par l'équation 5.11.

5.6.1 Etude de l'impact de la distance et de la densité du trafic

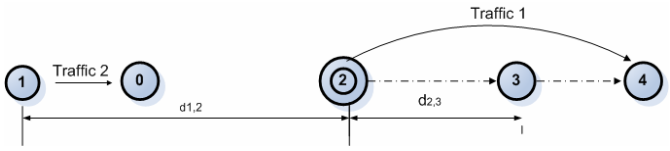
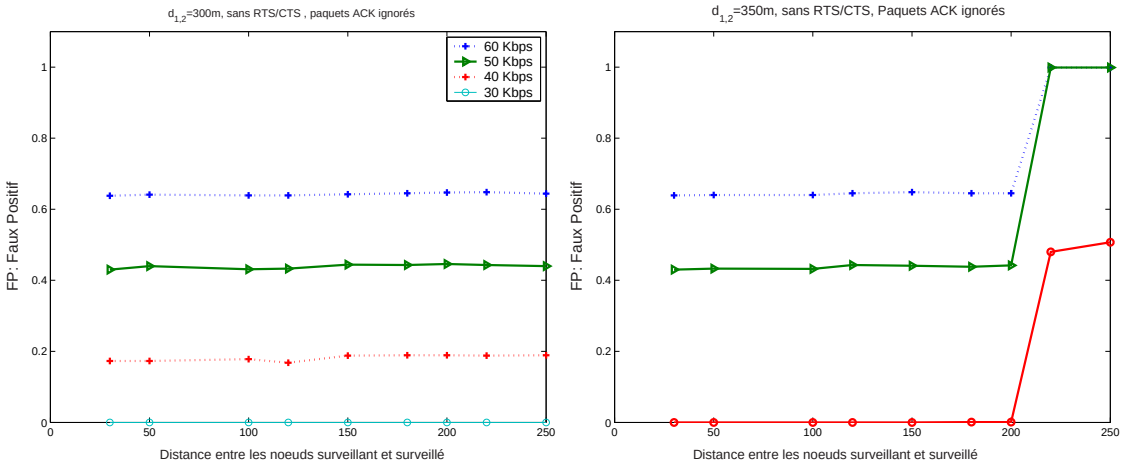


FIG. 5.11 – *Topologie réseau pour le modèle de simulation*

Dans cet exemple, nous considérons 5 nœuds disposés de façon linéaire. La topologie réseau montrée dans la figure 5.11 est simulée avec différentes distances entre le nœud surveillant 2 et le nœud surveillé 3. Le nœud 1 génère un trafic CBR (Constant Bit Rate) appelé *traffic2* au nœud 0, la distance entre eux est minime ($d_{1,0} = 10m$), mais la distance entre le nœud 1 et le nœud surveillant 2 est variable pendant la simulation. Un autre trafic CBR appelé *traffic1* est généré entre les nœuds 2 et 4, la distance entre eux est plutôt grande, supérieure à $250m$; le nœud surveillé 3 doit acheminer les paquets au nœud 4. La taille des paquets est fixée à 1000 bytes. Nous avons simulé le réseau avec différents taux de trafic variables entre 20 et 60 Kbps.

A- Cas du mécanisme Watchdog

Dans ce cas, nous étudions le mécanisme de surveillance sans prendre en compte les paquets d'acquittement ACK au niveau de la couche MAC. En d'autres termes, c'est le mécanisme classique Watchdog. Cela signifie que le nœud surveillant ne vérifie pas si le nœud surveillé a bien reçu le paquet à acheminer. Le mécanisme d'acquittement se passe au niveau MAC, or le Watchdog se situe au niveau routage.



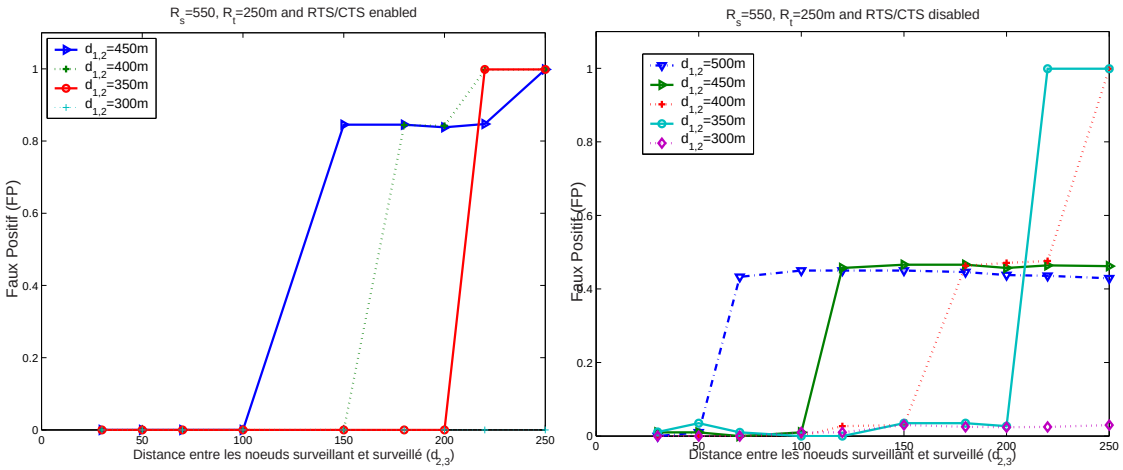
(a) $d_{1,2} = 300m$ (b) $d_{1,2} = 350m$

FIG. 5.12 – *Taux de faux positifs en fonction de $d_{2,3}$ dans le cas du Watchdog*

Dans les figures 5.12(a) et 5.12(b), nous montrons la relation entre les paramètres suivants : le faux positif, la distance entre les nœuds surveillant et surveillé et la densité du trafic. La figure 5.12(a) illustre le cas d'une distance entre les nœuds 1 et 2 égale à $d_{1,2} = 300m$. Nous remarquons que l'impact de la distance entre les nœuds surveillant et surveillé n'est pas significatif dans le cas où la densité du trafic est faible. Cependant, le taux de faux positifs FP augmente parallèlement à la densité du trafic, malgré le fait que la région vulnérable est couverte. Cela est principalement dû à la suppression des paquets, car le nœud surveillant génère des paquets au niveau de la couche de routage et ne vérifie pas si le paquet n'a pas été supprimé au niveau des couches inférieures et aussi si le paquet a bien été reçu par le nœud surveillé. Les résultats obtenus dans le cas d'une distance entre les nœuds 1 et 2 égale à $350m$ sont représentés dans la figure 5.12(b). Nous relevons quelques différences comparé au premier cas. Quand la distance entre les nœuds surveillant et surveillé est supérieure à $200m$, le FP augmente rapidement. Cela veut dire que l'observation du nœud surveillant est perturbée en permanence. Cette dégradation du mécanisme de surveillance est due principalement aux collisions au niveau du nœud surveillant, car la région d'interférence de ce nœud n'est pas couverte par la portée de détection de porteuse du nœud surveillé. En d'autres termes, quand le nœud surveillé transmet, le nœud surveillant subit des collisions et il ne sera pas capable de surveiller le nœud en question. Pour conclure ces résultats, la densité du trafic a un impact négatif sur le mécanisme Watchdog.

B- Cas du mécanisme inter-couches

Dans cette partie, nous illustrons et analysons les résultats de simulation dans le cas où les paquets d'aquittement ACK au niveau MAC sont pris en compte par le nœud surveillant au niveau de la couche de routage.



(a) Avec RTS-CTS (b) Sans RTS-CTS

FIG. 5.13 – *Taux de faux positifs en fonction de la distance $d_{2,3}$*

Nous avons activé le mécanisme RTS/CTS, puis nous avons tracé les résultats ob-

tenus dans la figure 5.13(a). Cette figure représente le FP en fonction de différentes distances entre les nœuds surveillant et surveillé avec différentes positions des nœuds 0 et 1. Quand la distance entre les nœuds surveillant et surveillé est inférieure à $100m$, le taux de faux positifs est nul ; si la distance entre le nœud 1 et le nœud 2 est de $450m$, cela veut dire que la région d'interférence du nœud surveillant 2 est couverte par la portée de détection de porteuse du nœud surveillé 3 ($d_{2,3} + d_{1,2} <= 550m$). Nous remarquons que quand $d_{2,3}$ devient supérieure à $100m$, FP augmente de 84%, car la région d'interférence du nœud 2 n'est pas couverte par la portée de détection de porteuse du nœud 3. Nous observons aussi que quand la région d'interférence du nœud surveillant est couverte par la portée de détection de porteuse du nœud surveillé, l'observation est correcte et le taux de faux positifs est nul, autrement le FP augmente et l'observation est fausse.

Quand le mécanisme RTS/CTS est désactivé, les résultats obtenus sont montrés dans la figure 5.13(b). Nous constatons quelques différences en comparaison avec le cas précédent. L'observation du nœud surveillant est perturbée même si la région d'interférence de ce nœud est couverte. Ce phénomène est dû aux collisions au niveau du nœud surveillant. De plus, nous observons que la valeur de FP est très petite mais pas nulle comme dans le premier cas (5.13(a)).

Une autre remarque importante concerne la densité du trafic : ce paramètre n'a pas d'impact significatif dans le cas de l'approche inter-couches ; les résultats présentés dans les figures 5.13(a) et 5.13(b) sont similaires.

Comme conclusion de ces résultats, le mécanisme RTS/CTS améliore le processus de surveillance. Les résultats illustrés dans les figures 5.13(a) et 5.13(b) prouvent cette conclusion. En outre, le nœud surveillant doit prendre en compte la distance entre lui et le nœud qu'il surveille, dans le but d'évaluer le risque que la région vulnérable ne soit pas couverte par la portée de détection de porteuse du nœud surveillé. Comme nous l'avons montré dans les deux résultats obtenus avec et sans le mécanisme RTS/CTS, la distance entre les nœuds surveillant et surveillé affecte les deux régions vulnérables des nœuds surveillant et surveillé. De plus, l'approche inter-couches que nous avons proposée permet de prendre en compte au niveau de la couche routage les paquets d'acquittement ACK de la couche MAC. Cette approche améliore l'exactitude de l'observation du nœud surveillant et réduit le taux de faux positifs. Nous pouvons résumer comme suit : l'approche inter-couches avec le mécanisme RTS/CTS réduit de manière significative le taux de faux positifs et améliore l'observation du nœud surveillant.

5.6.2 Scénarios de simulation dans le cas général

Dans cette partie, nous étudions le scénario général avec différentes charges de trafic, différentes densités de nœuds dans le réseau et différentes vitesses de mobilité des nœuds. De plus, le nombre de sauts de la source à la destination ou la longueur de la connexion sont pris en compte.

A- Impact de la densité du trafic

La figure 5.14 montre le taux moyen de faux positifs (FP) en fonction de différents trafics réseau. Nous avons distribué 50 nœuds de manière aléatoire et un trafic de type CBR (Constant Bit Rate) est généré par l'outil «cbrgen» de $NS2$ avec différents nombres de paquets par seconde. Nous remarquons que le taux de faux positifs (FP) augmente avec l'augmentation du débit de trafic. En outre, nous constatons que notre approche inter-couches obtient de meilleurs résultats que le mécanisme Watchdog. Cette approche réduit le FP de plus de 20% en comparaison avec le mécanisme Watchdog. Cette amélioration est principalement due à l'approche inter-couches, car avec cette approche le nœud surveillant arrive à estimer correctement le taux de réacheminement des paquets η au niveau de la couche de routage après avoir pris en compte la bonne réception des paquets par le nœud surveillé. Nous observons que la plus mauvaise valeur de FP est obtenue quand le trafic est intense. Dans la pire situation, FP ne peut pas dépasser 0.45 dans notre approche. Cependant, FP atteint 0.72 avec le mécanisme Watchdog.

Les résultats obtenus s'expliquent ainsi : dans le cas de notre proposition (l'approche inter-couches), la réduction de FP malgré le trafic intense est due à la prise en compte uniquement des paquets bien reçus par le nœud surveillé pour calculer le taux de coopération. Nous savons que le taux de réacheminement des paquets est calculé au niveau de la couche de routage et qu'un trafic intense génère plus de collisions et de pertes de paquets. C'est pourquoi, nous prenons en compte les paquets ACK au niveau de la couche MAC pour être sûrs que le paquet destiné au nœud surveillé est bien reçu. Ceci explique que dans le cas d'un faible trafic, la différence de FP dans les approches inter-couches et classique (Watchdog) ne soit pas significative, c'est-à-dire que la probabilité pour qu'un paquet soit bien reçu par le nœud surveillé soit grande.

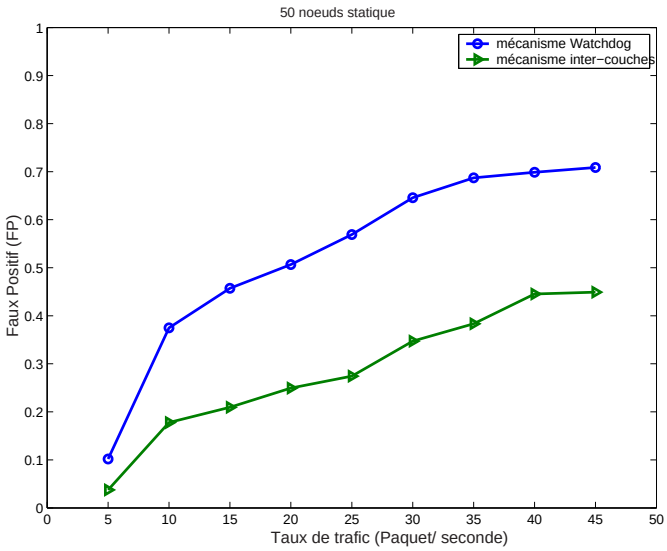


FIG. 5.14 – *Faux positifs (FP) en fonction de la densité du trafic (cas de 50 nœuds statiques)*

B- Impact de la densité des nœuds

Nous avons tracé dans la figure 5.15 le taux de faux positifs FP en fonction de la densité des nœuds dans le réseau avec une densité de trafic fixée à $10 Paquet/s$. Nous remarquons que dans les deux approches, FP augmente avec l'augmentation de la densité des nœuds dans le réseau. Cependant, FP dans le cas de Watchdog est plus proche que celui de l'approche inter-couches quand la densité des nœuds est faible (moins de 10 nœuds). Dans les pires situations, nous avons obtenu 45% de FP avec l'approche inter-couches, mais 68% avec le mécanisme Watchdog. Nous observons qu'avec l'approche inter-couches, nous avons réduit le faux positif (FP) de 20% comparé à l'approche classique Watchdog. La densité des nœuds dans le réseau a un impact direct sur la probabilité de collision, ce qui affecte négativement le mécanisme de surveillance. Selon la modélisation effectuée par Bianchi (Bianchi, 2000), nous pouvons dire que lorsque la densité des nœuds augmente, la probabilité de collisions augmente aussi. En outre, dans notre contexte, l'augmentation de la densité des nœuds implique l'augmentation de la probabilité d'avoir un nœud dans la région vulnérable As_3s_4. Dans cette région, n'importe quelle transmission d'un nœud pendant la durée de surveillance crée des collisions au niveau du nœud surveillant et perturbe son observation. C'est pour cela que la densité des nœuds a un impact négatif sur le mécanisme de surveillance.

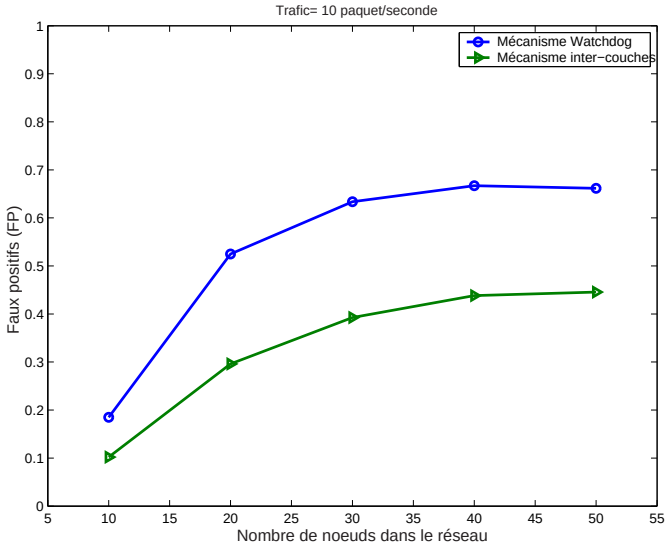


FIG. 5.15 – *Faux positifs (FP) en fonction de la densité des nœuds dans le réseau (taux de trafic 10 pkt/sec)*

C- Impact de la mobilité des nœuds

Dans cette partie, nous étudions l'impact de la mobilité sur le mécanisme de surveillance. Les problèmes avec le mécanisme de surveillance dans le cas de la mobilité apparaissent quand le nœud surveillant envoie un paquet au nœud surveillé pour que

ce dernier l'achemine à un autre nœud, mais le nœud surveillé se déplace en dehors de la région de transmission du nœud surveillant. Dans ce cas, deux situations se présentent :

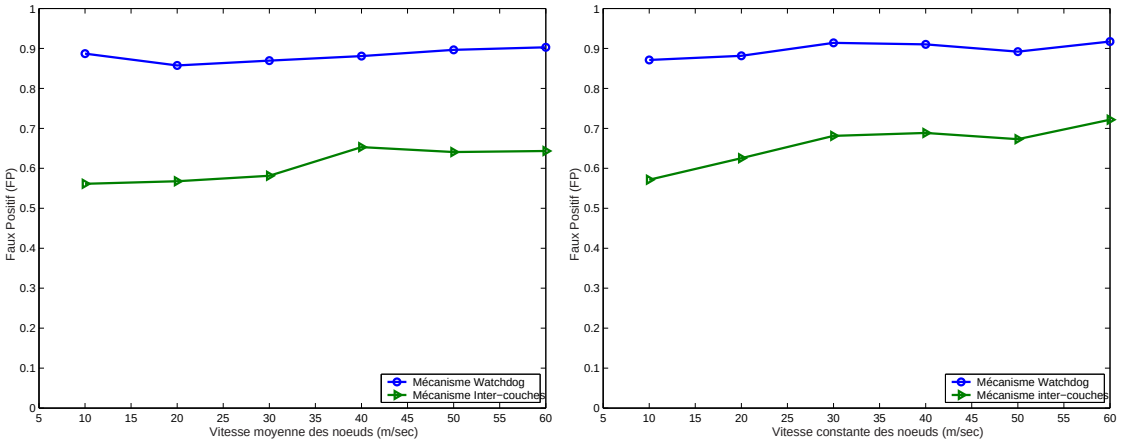
- Premièrement, le nœud surveillé se déplace en dehors de la portée du nœud surveillant après avoir envoyé le paquet d'acquittement (ACK). Dans ce cas, les deux mécanismes Watchdog classique et l'approche inter-couches produisent des faux positifs (FP) si le nœud surveillé réachemine le paquet après.
- Deuxièmement, le nœud surveillé se déplace en dehors de la portée du nœud surveillant avant de transmettre le paquet ACK. Dans ce cas, notre approche permet d'éviter le faux positif (FP), contrairement au mécanisme Watchdog classique qui ne permet pas d'éviter le FP, car il ne prend pas en compte les paquets ACK.

Dans le but d'étudier l'impact de la mobilité sur les deux mécanismes, nous avons utilisé le modèle de mobilité proposé par Le Boudec et Cie (Boudec et Vojnovic, 2005) appelé « Random Trip Model » et en particulier « Random Way Point model » (RWP). Les figures 5.16(a) et 5.16(b) montrent le taux de faux positifs (FP) en fonction de la vitesse moyenne des nœuds et de la vitesse constante des nœuds, avec respectivement 30 nœuds et 15 connexions de type CBR ($30 Paquet/s$). Nous remarquons que dans les deux cas, le FP augmente quand la vitesse des nœuds augmente aussi. Cependant, même l'approche proposée est affectée par la mobilité des nœuds, mais elle donne de meilleurs résultats comparée au Watchdog classique puisqu'elle permet de réduire FP de plus de 30% les résultats de Watchdog dans le cas d'une vitesse moyenne des nœuds. Dans le cas de la mobilité constante des nœuds, le FP augmente un peu plus que dans le cas précédent, mais avec notre approche FP est réduit de 20% comparé au cas de Watchdog. Pour conclure sur l'impact de la mobilité sur le mécanisme de surveillance, nous pouvons dire que la mobilité a un impact négatif sur les deux approches Watchdog classique et inter-couches. Cependant, l'impact n'est pas significatif dans notre modèle comparé au mécanisme Watchdog.

L'avantage de notre modèle inter-couches dans le cas d'un scénario de mobilité se présente lorsque le nœud surveillé se déplace en dehors de la portée du nœud surveillant avant de transmettre le paquet d'acquittement (ACK). Dans ce cas, le nœud surveillant ne prend pas en compte les paquets non acquittés dans le calcul du taux de réacheminement η. Cependant, le mécanisme Watchdog classique génère des faux positifs dans cette situation.

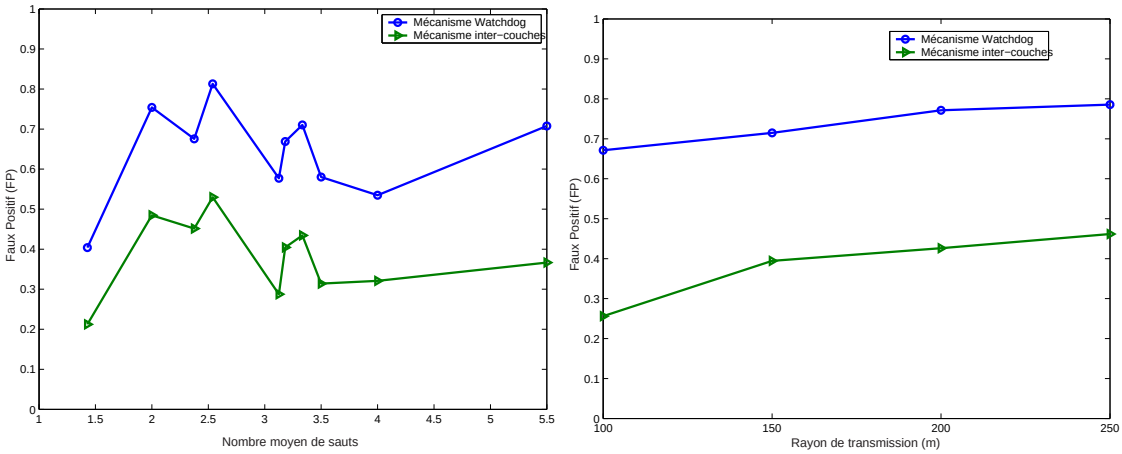
D- Impact de la longueur du chemin et du rayon de la portée de transmission

Dans cette sous section, nous étudions l'impact du nombre de sauts (la longueur du chemin ou de la connexion) et du rayon de la portée de transmission sur le mécanisme de surveillance. La figure 5.17(a) montre le FP en fonction de la longueur du chemin (PL) dans le cas de 50 nœuds statiques avec 20 connexions de type CBR ($30 Pkt/sec$). Différentes superficies de domaine de simulation et différents rayons de transmission sont pris en compte pour obtenir différents nombres de sauts (différentes tailles de connexion). Nous remarquons que le nombre moyen de sauts n'a pas d'impact direct ou clair sur le mécanisme de surveillance. Le FP augmente avec l'augmentation de la



(a) Mobilité moyenne (b) Mobilité constante

FIG. 5.16 – *FP en fonction de la vitesse des nœuds utilisant le modèle RWP*



(a) Longueur moyenne du chemin (b) Portée de transmission

FIG. 5.17 – *FP en fonction de la longueur moyenne du chemin et du rayon R_t*

longueur des connexions dans certains cas comme lorsque $PL = 2$ ou $PL = 2.5$, mais il diminue dans certains cas, lorsque $PL = 3$ et $PL = 3.5$. Ces résultats s'expliquent ainsi : la longueur du chemin de la connexion n'a pas d'impact direct sur le mécanisme de surveillance. Cependant, lorsque la longueur moyenne du chemin augmente, le nombre de nœuds surveillants augmente aussi. Donc, la probabilité que le nœud surveillant ait un nombre important de voisins est grande. Cela implique que la probabilité qu'un nœud dans la région vulnérable (voir la figure 5.2(b)) transmette pendant le processus de surveillance est grande. Nous observons que quelle que soit la longueur moyenne de connexion (chemin), le modèle de surveillance inter-couches que nous avons proposé donne de meilleurs résultats que Watchdog et réduit le FP de plus de 20%.

Ainsi, nous concluons que la longueur moyenne des connexions (chemins) n'a pas d'impact direct sur le mécanisme de surveillance mais il a une relation avec la densité des nœuds au niveau du nœud surveillant et la distance entre les nœuds surveillant et surveillé. C'est pourquoi nous avons étudié l'impact du rayon de la portée de transmission sur le mécanisme de surveillance. La figure 5.17(b) montre le taux de faux positifs (FP) en fonction du rayon de la portée de transmission dans le cas de 50 nœuds statiques avec 20 connexions de type CBR ($30 Pkt/sec$). Nous remarquons que le FP augmente lorsque la portée de transmission augmente. L'augmentation du rayon de la portée de transmission implique que la densité des nœuds autour des nœuds surveillants augmente. De plus, l'augmentation de la densité des nœuds augmente le nombre de nœuds qui veulent accéder au canal de communication. Lorsque le rayon de la transmission est égal à $100m$, le FP dans le cas de Watchdog est d'environ 0.66, mais dans notre mécanisme FP, il ne dépasse pas 0.28. Dans le cas classique de la portée de transmission ($250m$), FP atteint avec Watchdog 0.8 mais dans le cas de notre mécanisme inter-couches, FP est limité à 0.47. Ces résultats de simulation montrent que le mécanisme de surveillance avec l'approche inter-couches donne des résultats nettement meilleurs que celui de Watchdog avec différentes densités de nœuds et de longueurs de connexion.

Selon les résultats présentés ci-dessus, nous concluons qu'avec notre approche inter-couches, nous obtenons de meilleurs résultats : le taux de faux positifs est réduit significativement avec différents taux de charge de trafic, différentes densités de nœuds et différentes mobilités des nœuds. Finalement, ces résultats confirment la validité du modèle analytique proposé.

5.7 Conclusion

Dans ce chapitre, nous avons montré l'avantage d'opter pour une approche inter-couches destinée au mécanisme de surveillance. Nous avons proposé un nouveau modèle analytique dans le but d'évaluer correctement la réputation et la coopération du nœud surveillé. Nous avons clairement pris en compte l'impact du rapport signal sur bruit (SNR) et la distance entre les deux nœuds surveillant et surveillé. Dans notre modèle, la meilleure observation du nœud surveillant est obtenue lorsque le nœud surveillant est proche du nœud surveillé. La différence entre les portées de transmission,

d'interférence et de signal est prise en compte, contrairement à certaines modélisations qui prétendent que la portée de transmission est égale à la portée de détection de porteuse. De plus, l'approche inter-couches (les couches physique, MAC et routage) adoptée pour notre modèle permet de prendre en compte le SNR de la couche physique et les paquets ACK de la couche MAC au niveau de la couche de routage. L'objectif de l'approche inter-couches pour le mécanisme de surveillance est d'obtenir une évaluation plus précise du nœud surveillé via l'amélioration de l'observation du nœud surveillant. Les résultats de simulations obtenus confirment l'impact de la distance entre les nœuds surveillant et surveillé. En outre, ces résultats montrent que notre modèle inter-couches a de plus faibles taux de faux positifs que le mécanisme Watchdog avec différents paramètres réseau comme : la densité des nœuds, la mobilité des nœuds et la densité du trafic réseau.

Chapitre 6

Nouvelles vulnérabilités cachées : impact et solutions

Sommaire

Dans ce chapitre, nous nous focalisons sur la couche MAC (Medium Access Control) en particulier sur la technologie IEEE 802.11 et nous montrons les vulnérabilités cachées basées sur les paquets de contrôle *CTS* (Clear to Send) et *ACK*. A travers ces vulnérabilités, nous montrons de nouvelles attaques intelligentes qui n'ont jamais été traitées auparavant, sauf les attaques basées sur la vulnérabilité des paquets *RTS* (Request to

Send). Un nœud malveillant peut exploiter ces vulnérabilités au niveau du protocole de la couche MAC dans le but de perturber les mécanismes de surveillance et de routage. De plus, nous décrivons comment ces vulnérabilités peuvent être exploitées et comment des attaques peuvent être implémentées par un attaquant. Nous étudions l'impact de ces attaques sur le réseau avec une étude analytique, des simulations ainsi qu'une étude expérimentale. Les résultats de simulations et leur analyse illustrent l'impact négatif de ces attaques sur le réseau. En outre, les résultats d'expérimentation démontrent la possibilité d'implémenter et d'exploiter ces attaques. Ces expérimentations nous permettent de confirmer les résultats de simulations. Dans le but de prévenir ces attaques, des solutions basées sur l'authentification des paquets de contrôle sont présentées. Nous proposons deux classes de solutions pour contrer ces attaques. La première classe n'utilise pas le concept de cryptographie. Cependant, la deuxième solution est basée sur la cryptographie, et en particulier sur la fonction de hashage améliorée, appelée Enhanced *HMAC*. L'évaluation et l'analyse des solutions proposées sont présentées et soutenues par une étude analytique et par les résultats de simulations. Les résultats de simulations des solutions proposées montrent que l'impact négatif des attaques est significativement réduit. Ainsi, les attaques sont bien contrées. De plus, le coût des solutions proposées est étudié. En comparaison avec l'impact négatif des attaques, le coût de sécurité n'est pas significatif.

6.1 Introduction

Plusieurs solutions de sécurité proposées pour sécuriser les réseaux mobiles Ad hoc (MANETs) se focalisent sur la sécurité des protocoles de routage comme les protocoles Ariadne ou SRP (Secure Routing Protocol) (Buttyan et Hubaux, 2002) et le protocole ARAN (Authenticated Routing for Ad Hoc Networks) (Sanzgiri et al., 2005a). Cependant, dans les réseaux MANETs, les mécanismes de sécurité ont besoin d'un modèle de confiance dans le but d'évaluer de manière dynamique le niveau de confiance des nœuds et d'assurer la sécurité du réseau. C'est pourquoi le mécanisme de surveillance est nécessaire pour évaluer le comportement des nœuds. Nous pouvons citer le mécanisme Watchdog (S. Marti et Baker, 2000), le mécanisme basé sur l'approche inter-couches que nous avons proposé (Rachedi et Benslimane, 2007) et d'autres (Zhang et Lee, 2000). Le mécanisme de surveillance est une partie intégrante du système de détection d'intrusions (IDS). L'étude effectuée par Buchegger et Cie (Buchegger et Boudec, 2002b) a montré que sans un système de détection d'intrusions, les performances du réseau se dégradent avec les attaques de type déni de services (DoS). Malheureusement, les solutions proposées ne prennent pas en compte les vulnérabilités au niveau de la couche MAC. Ces vulnérabilités peuvent être exploitées pour perturber les couches supérieures telles que la couche réseau ou la couche de routage. Les exploitations de ces vulnérabilités sont appelées les attaques inter-couches. Nous adoptons la définition suivante d'une attaque inter-couches : c'est une attaque qui se focalise sur la couche MAC et dont l'impact se propage jusqu'aux autres couches supérieures. Certains chercheurs ont traité des vulnérabilités au niveau de la couche MAC et même de certaines attaques de type inter-couches (Radosavac et al., 2004)(Guang et al., 2008), mais ils se sont focali-

sés uniquement sur la manipulation des paramètres d'accès au canal de communication tels que le backoff, le DIFS (Distributed Inter Frame Space) et le SIFS (Short Inter Frame Space). Un autre travail proposé par Ray et Cie (S. Ray, 2007) (Ray et al., 2003) traite uniquement des vulnérabilités des paquets de contrôle RTS (Request to Send). Contrairement aux travaux existant déjà dans la littérature, nous ne nous focalisons pas sur la vulnérabilité du backoff ni sur les attaques fondées sur les faux paquets RTS, mais nous montrons de nouvelles vulnérabilités basées sur le format des paquets de contrôle, en particulier les paquets *CTS* (Clear to Send) et *ACK*. De plus, nous introduisons un nouveau défi pour les systèmes de détection d'intrusions (IDS), dans le but de détecter ces attaques intelligentes.

Dans ce chapitre, nous nous focalisons sur les vulnérabilités cachées au niveau de la couche MAC avec leurs impacts négatifs sur les performances du réseau et le mécanisme de surveillance. Nous classons ces attaques comme attaques inter-couches, car elles sont basées sur les vulnérabilités au niveau de la couche MAC mais leur impact touche les couches supérieures, particulièrement la couche de routage. Généralement, l'un des objectifs d'un attaquant consiste à réduire la performance du réseau, à perturber le bon fonctionnement du mécanisme de surveillance et à pénaliser les nœuds qui se comportent bien en réduisant leur réputation (niveau de confiance). En outre, nous étudions les implémentations potentielles de ces attaques. Ainsi, l'implémentation et la simulation de ces attaques sont effectuées et leurs résultats sont analysés. De plus, nous avons proposé de nouvelles solutions de sécurité basées sur le principe d'authentification des paquets de contrôle avec et sans concept de cryptographie. La fonction de hashage, en particulier « Hashed Message Authentication Code » (*HMAC*) (PUB, 2001) et la version améliorée de cette fonction appelée « Enhanced HMAC » (*EHMAC*) (Patel, 2002) sont utilisées pour assurer l'authentification et l'intégrité des paquets de contrôle au niveau de la couche MAC. L'évaluation des solutions proposées est effectuée via les simulations et leur analyse. Le coût de la sécurité est pris en compte avec la perte de la bande passante, la charge de trafic des paquets de contrôle et l'énergie additionnelle due aux fonctions de sécurité ajoutées. Le coût des solutions proposées dépend du niveau de sécurité qu'on veut assurer. C'est pourquoi, un compromis entre le coût de la sécurité et la qualité de service du réseau doit être trouvé.

Nous résumons l'ensemble des contributions principales de ce chapitre comme suit :

- De nouvelles vulnérabilités basées sur le format des paquets de contrôle, en particulier les paquets *CTS* and *ACK*, sont présentées et étudiées. La difficulté à détecter les attaques basées sur ces vulnérabilités et à identifier l'attaquant est étudiée et analysée.
- Deux nouveaux algorithmes d'attaque sont présentés avec leur implémentation. Deux organigrammes d'attaques avec leur modèle analytique sont présentés et discutés.
- Une étude de l'impact de ces attaques sur le réseau est effectuée via des simulations sous *NS2* (ns 2, 1999) et aussi via une implémentation réelle sous le pilote MadWiFi (Leffler, 2007).
- Deux types de solutions (avec et sans cryptographie) sont proposés pour contrer ces attaques. Les avantages et les inconvénients de chaque solution sont étudiés

et présentés.
- Les simulations des solutions proposées sont effectuées et leurs résultats sont analysés et présentés. Le coût additionnel des solutions proposées en terme de perte de bande passante, de surcharge de réseau et de consommation d'énergie est bien étudié. Enfin, la comparaison entre le coût des solutions et l'impact de ces attaques sur le réseau est présentée.

Le reste de ce chapitre est organisé comme suit : dans la section 6.2, nous présentons le positionnement bibliographique de ce travail. Dans la section 6.3, nous présentons les vulnérabilités cachées avec le mécanisme *RTS/CTS* telles que : la vulnérabilité de format des paquets de contrôle, le faux paquet *CTS* et la fausse validation du paquet *DATA* basés sur le faux *ACK*. De plus, l'impact de ces attaques sur le mécanisme de surveillance est analysé. Dans la section 6.4, nous montrons l'impact de ces attaques sur le réseau via des simulations et une implémentation réelle de ces attaques. Les résultats de simulations et d'expérimentations sont présentés et analysés. La section 6.5 est consacrée aux différentes solutions proposées pour contrer ces attaques avec et sans le concept de cryptographie. Dans la section 6.6, nous évaluons les solutions proposées via des simulations et l'analyse de leurs résultats. Dans la section 6.7, nous proposons une analyse de sécurité de l'ensemble des solutions proposées. Enfin, la dernière section est réservée à la conclusion de ce chapitre.

6.2 Positionnement bibliographique

Dans cette section, nous présentons le mécanisme *RTS/CTS* de la technologie IEEE 802.11 et le problème du faux blocage.

6.2.1 Mécanisme RTS/CTS

Le mécanisme *RTS/CTS* est utilisé par le protocole MAC IEEE 802.11 dans le but d'éviter le problème bien connu des nœuds cachés (A. Rahman, 2006). L'idée de base du mécanisme *RTS/CTS* consiste en la transmission du paquet *RTS* par le nœud émetteur vers le nœud récepteur. Lorsque le nœud récepteur reçoit le paquet *RTS*, il va répondre en émettant un paquet *CTS*, dans le but d'informer tous les nœuds voisins qui vont recevoir ce paquet de la durée de transmission et d'éviter le problème des nœuds cachés. Comme illustré dans la figure 6.1(a), le nœud C reçoit le paquet *RTS* et bloque sa transmission par un certain *NAV(RTS)*[1].

$$NAV(RTS) = 3.SIFS + T_{CTS} + T_{DATA} + T_{ACK} \tag{6.1}$$

où T_{CTS}, T_{DATA} et T_{ACK} sont les temps de propagation des paquets *CTS*, *DATA* et *ACK* respectivement. Le temps $SIFS$ est l'abréviation de « Short InterFrame Spacing » [2].

[1] *NAV* (Network Allocator Vector), qui est la durée de transmission calculée par le nœud émetteur A
[2] Dans IEEE 802.11, $SIFS = 10us$

Il en est de même pour le nœud D, qui bloque sa transmission pendant un certain *NAV(CTS)*, une fois qu'il a reçu le paquet *CTS*. Le *NAV(CTS)* est calculé par le nœud B, fondé sur le *NAV(RTS)* contenu dans le paquet RTS.

$$NAV(CTS) = NAV(RTS) - (SIFS + T_{CTS}) \tag{6.2}$$

L'émetteur A envoie le paquet DATA une fois qu'il a reçu le paquet *CTS* du nœud B. Le nœud B répond par un paquet d'aquittement (*ACK*) lorsqu'il reçoit correctement le paquet *DATA*, comme indiqué dans la figure 6.1(b).

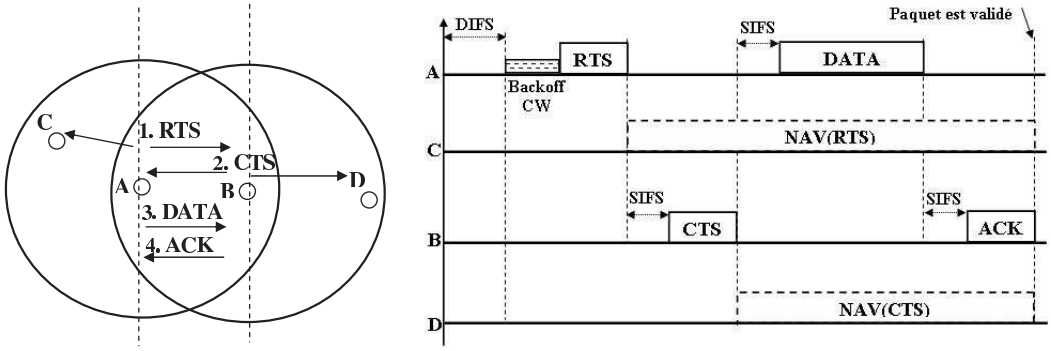


FIG. 6.1 – *Le mécanisme RTS/CTS dans le protocole MAC IEEE802.11*

Le mécanisme RTS/CTS n'est pas utilisé uniquement par le protocole MAC IEEE 802.11, mais aussi par d'autres protocoles MAC tels que : MACA (Multiple Access with Collision Avoidance) (Karn, 1990) et MACAW (Multiple Access with Collision Avoidance for Wireless) (V. Bharghavan et Zhang, 1994). Contrairement au protocole MAC IEEE 802.11, MACA n'utilise pas le paquet d'acquittement ACK pour assurer la bonne réception du paquet DATA. Cependant, MACAW utilise le mécanisme RTS/CTS, mais contrairement à MACA, MACAW utilise le paquet d'acquittement ACK et ajoute un autre paquet appelé «DATA-Send» (*DS*) dans le but d'indiquer le début de la transmission du paquet DATA.

6.2.2 Problème du faux blocage avec le mécanisme RTS/CTS

Le problème du faux blocage est introduit par Ray et Starobinski (S. Ray, 2007)(Ray et al., 2003). Le faux blocage se produit lorsque le nœud récepteur du paquet RTS bloque sa transmission inutilement. La figure 6.2 illustre le problème du faux blocage avec le mécanisme RTS/CTS. Lorsque le nœud A veut communiquer avec le nœud B, il lui envoie le paquet RTS pour l'informer de la durée de transmission et réserver le canal de communication. N'importe quel nœud dans le voisinage du nœud A qui reçoit le paquet RTS va se bloquer pendant la durée NAV indiquée dans le paquet RTS, sauf le nœud B qui va répondre par un paquet CTS. Si le nœud D veut communiquer avec le

nœud C ou si le nœud C veut assurer la bonne réception du paquet RTS, ce dernier ne peut pas répondre par un CTS car il est bloqué. Le problème avec ce scénario est que la situation de faux blocage risque de se propager et de s'étendre à d'autres nœuds, comme les nœuds E et H de la figure 6.2.

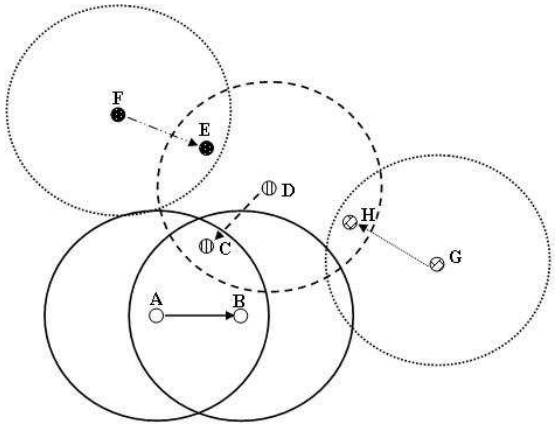


FIG. 6.2 – *Problème du faux blocage*

6.2.3 Brouillage virtuel

Le problème du faux blocage peut être exploité par un attaquant dans le but de créer une attaque de type déni de service dans le réseau. Rahman et Gburynski (A. Rahman, 2006) ont traité du problème du faux blocage basé sur l'émission volontaire d'un faux paquet RTS dont le but est de gêner et de retarder la transmission dans une partie du réseau. Cette attaque est appelée brouillage virtuel (*virtual jamming*). La plupart des solutions proposées dans la littérature consistent à réduire l'impact de cette attaque (Ray et al., 2003)(S. Ray, 2007) et non pas à l'éliminer définitivement. Parmi ces solutions, nous citons la solution fondée sur l'addition d'un paquet de contrôle comme le paquet DATA-Send (*DS*) dans MACAW (V. Bharghavan et Zhang, 1994). Ce paquet (*DS*) permet aux voisins de l'émetteur du paquet RTS de savoir que le paquet CTS a bien été reçu par l'émetteur du paquet RTS. Une autre solution a été proposée par Ray et Cie (S. Ray, 2007) pour réduire l'impact de cette attaque, et est appelée *RTS validation*. Cette solution a été améliorée dans (A. Rahman, 2006). L'idée principale de cette solution est basée sur la décision du nœud récepteur du paquet RTS : avant que ce nœud ne bloque sa transmission, il doit écouter le canal et vérifier son statut, puis enfin décider de son blocage après un certain temps (RTS_Defer_Time). Une fois que le nœud reçoit le paquet RTS, il doit bloquer sa transmission pour un certain temps défini RTS_Defer_Time et ne pas se bloquer pour NAV(RTS) comme c'est le cas dans le protocole classique. Après RTS_Defer_Time, le nœud vérifie le statut du canal, puis il bloque sa transmission si le canal est occupé. Dans le cas où le canal est libre, il ignore le paquet RTS. Dans (A. Rahman, 2006), les auteurs ont proposé une extension de la solution « RTS validation » et l'ont appelée « validation aléatoire de RTS » (*the random RTS validation*). Le

principe de cette solution est le même que celui de la précédente solution (simple RTS validation) : la différence entre les deux solutions se résume au niveau de la variable aléatoire RTS_Defer_Time sélectionnée dans un certain intervalle. Nous remarquons que même avec ces solutions, le problème du faux blocage ou du brouillage virtuel n'est pas résolu. De plus, toutes ces solutions ne se concentrent que sur le blocage dû au faux paquet RTS. Cependant, dans ce chapitre, nous introduisons de nouvelles vulnérabilités et de nouveaux algorithmes d'attaque basés sur les paquets CTS et ACK. En outre, nous proposons plusieurs solutions possibles avec et sans les mécanismes de cryptographie dans le but d'éliminer ces vulnérabilités et de contrer les attaques qui se basent dessus.

6.3 Vulnérabilités cachées

Dans cette section, nous illustrons les vulnérabilités cachées dans le mécanisme RTS/CTS dont l'impact sur les performances du réseau est négatif. Nous montrons comment ces vulnérabilités peuvent être exploitées et implémentées par des nœuds malicieux.

6.3.1 Vulnérabilités de format des paquets de contrôle

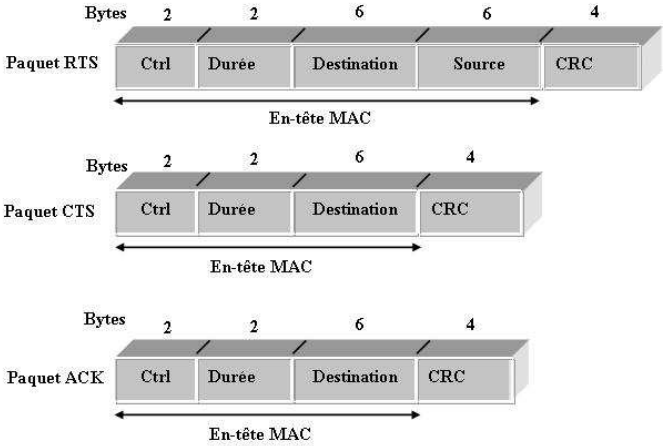


FIG. 6.3 – *Format des paquets RTS, CTS et ACK*

La figure 6.3 montre le format des paquets *RTS*, *CTS* et *ACK* défini par IEEE802.11 (IEEE802-11, 1999). Nous remarquons que pour des raisons d'optimisation de la taille des paquets de contrôle *CTS* et *ACK*, ces derniers ne contiennent pas l'adresse source de l'émetteur de ces paquets ; en effet, avec le mécanisme RTS/CTS, lorsqu'un nœud envoie le paquet *RTS* à la destination, tous les nœuds dans le rayon de transmission de l'émetteur bloquent leur transmission sauf le nœud destinataire qui répond par le

paquet *CTS* sans mettre son adresse dans le paquet. Ainsi, lorsque le nœud reçoit le paquet *CTS*, il en déduit que ce paquet est envoyé par le nœud destinataire du paquet *RTS*. C'est pourquoi aucune vérification n'est effectuée sur l'adresse source de l'émetteur du paquet *CTS*. Dans le protocole IEEE 802.11, le nœud ne communique pas avec plus d'un seul nœud à la fois (IEEE802-11, 1999). En outre, le paquet *ACK* ne peut être authentifié par le nœud qui le reçoit. Les nœuds malicieux peuvent exploiter ces vulnérabilités en introduisant de nouvelles attaques qui ne peuvent pas être identifiées par les systèmes de détection d'intrusions actuels. L'attaquant peut générer de faux *RTS* dans le but de bloquer ses voisins. Selon le format du paquet *RTS*, plusieurs solutions peuvent être proposées pour détecter cette attaque, comme c'est le cas pour la solution de validation aléatoire de *RTS* proposée dans (S. Ray, 2007). Cependant, cette solution est seulement limitée aux paquets *RTS* et ne peut pas éliminer les problèmes des faux paquets *CTS* et *ACK*. Par exemple, un attaquant peut générer uniquement de faux *CTS* ou de faux *ACK* dans le but de perturber le réseau. Les scénarios d'attaque sont expliqués en détail dans les sections suivantes.

6.3.2 Brouillage virtuel basé sur de faux CTS

Le faux paquet *CTS* peut être généré par un attaquant dans le but de créer une situation de blocage (brouillage virtuel).

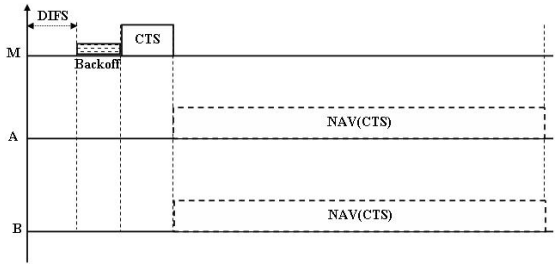


FIG. 6.4 – *Attaque de type faux CTS*

La figure 6.4 montre le cas classique d'une attaque via le faux *CTS*. Lorsque les nœuds dans le rayon de transmission de l'attaquant reçoivent le faux paquet *CTS*, ils sont inutilement bloqués pendant la durée de transmission présumée *NAV(CTS)*, même sans la réception du paquet *RTS* (ces nœuds se considèrent comme des nœuds cachés). L'attaque de type faux *CTS* peut bloquer les nœuds qui se trouvent dans la portée de transmission de l'attaquant, mais aussi les nœuds qui se trouvent en dehors du rayon de transmission de l'attaquant. Les nœuds qui se trouvent dans le rayon d'interférence seront bloqués pendant EIFS (Extended Inter-Frame Space)[3](IEEE802-11, 1999). En effet, les nœuds qui sont en dehors du rayon de transmission ne sont pas capables de décoder ou de recevoir correctement les paquets. Nous pouvons dire que l'impact de cette attaque ne se limite pas seulement au rayon de transmission de l'attaquant mais aussi au rayon d'interférence (pour plus de détails sur les rayons d'interférence et de

[3]The EIFS est estimé à 364μs dans le cas d'une vitesse de transmission de 1 Mbps

transmission, le lecteur peut se référer au chapitre précédent). Un autre problème important avec cette attaque est la détection de l'attaquant : même avec l'utilisation d'un mécanisme de surveillance ou d'un IDS, il est impossible de détecter le nœud attaquant, en raison des vulnérabilités au niveau du format du paquet *CTS*. Cela veut dire qu'un attaquant peut facilement échapper aux procédures de punition (par exemple, la baisse du niveau de confiance du nœud malicieux). C'est pourquoi, un attaquant peut facilement exploiter cette vulnérabilité et attaquer ses voisins en permanence sans se faire détecter. Dans la figure 6.5, nous présentons sous la forme d'un organigramme l'al-

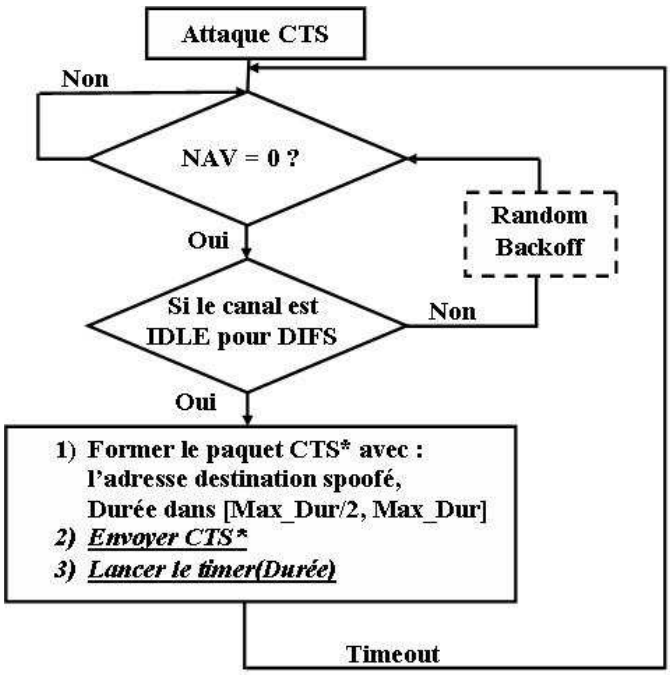


FIG. 6.5 – *Organigramme d'une attaque de type faux CTS*

gorithme de l'attaque de type faux *CTS*. Nous remarquons que l'attaquant vérifie si le NAV est égal à zéro. Ensuite, il passe à la vérification du statut du canal de communication. Si le canal est occupé, il va attendre pour certain temps ($DIFS + Backoff$), sinon il va former un faux paquet *CTS* avec une fausse adresse de destination, puis il lance l'attaque.

Cette attaque est difficile à détecter pour un IDS, car selon les caractéristiques des réseaux mobiles Ad hoc, même si le nœud surveillant ne reçoit pas le paquet DATA qui succède au faux paquet *CTS*, il ne sera pas en mesure d'en conclure si le paquet *CTS* est vrai ou faux. Le nœud surveillant peut être un voisin du récepteur du paquet *CTS* mais pas forcément de l'émetteur du paquet *RTS*. De plus, le nœud surveillant ne peut pas se focaliser sur le paquet *ACK*, car si le paquet *ACK* n'est pas reçu après un certain temps $TOut_1$, le *CTS* est classé comme faux paquet. Cependant, la solution n'est pas intéressante car le problème de blocage existe toujours : dans tous les cas, les nœuds victimes bloquent leur transmission pendant le $TOut_1$ qui est plus grand que NAV(CTS), donc la solution est écartée. De plus, le problème de collision peut

compromettre cette solution : le nœud émetteur du paquet *CTS* peut subir une collision lors de la réception du paquet DATA. Dans ce cas, le paquet *ACK* ne sera pas envoyé, même après $TOut_1$. En conclusion, cette solution peut générer beaucoup de fausses alarmes.

6.3.3 Fausse validation de paquet basée sur de faux ACK

Le faux paquet *ACK* peut être exploité par un attaquant dans le but de perturber les services réseau tels que le processus de routage ou le mécanisme de surveillance, etc ... Le problème avec cette attaque est que le faux paquet *ACK* ne peut pas être détecté et son impact sur le réseau est très négatif. L'idée consiste à faire croire au nœud émetteur du paquet DATA que ce paquet a bien été reçu par le nœud récepteur, ce qui n'est pas vrai. Un des impacts de cette attaque est que le nœud émetteur ne va pas retransmettre le paquet DATA car il a déjà reçu le faux paquet *ACK*.

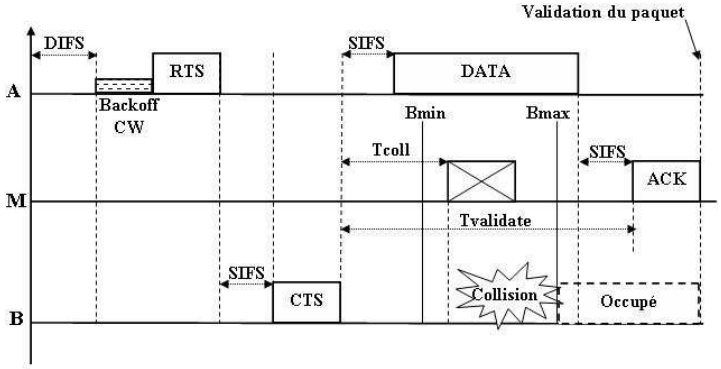


FIG. 6.6 – *Fausse validation de paquet basée sur le faux ACK.*

La figure 6.6 montre le scénario d'une fausse validation d'un paquet DATA basée sur le faux paquet *ACK*. Le nœud A veut envoyer un paquet au nœud B, le nœud M est un nœud malicieux situé dans la portée de transmission des nœuds A et B. Pour mettre en place son attaque, le nœud M a besoin de connaître les adresses des nœuds A et B ainsi que le $NAV(RTS)$ ou le $NAV(CTS)$. Lorsque le nœud M reçoit le paquet *RTS*, il obtient les deux adresses des nœuds A et B, ainsi que le $NAV(RTS)$. Selon le $NAV(RTS)$ ou le $NAV(CTS)$, le nœud M peut déterminer le temps T_{coll} pour lancer son attaque. Le scénario d'attaque est divisé en deux parties. Dans la première partie, l'attaquant envoie un paquet au nœud B à T_{coll}, dans le but de créer une collision au niveau du nœud B. Le temps T_{coll} est une valeur aléatoire dans l'intervalle $[B_{min}, B_{max}]$ avec

$$\begin{cases} B_{min} = \dfrac{NAV(CTS) - (T_{ACK} + SIFS)}{2} \\ B_{max} = NAV(CTS) - (T_{ACK} + SIFS + T_{JAM}) \end{cases}$$

où T_{JAM} est le temps de propagation du paquet qui va créer la collision au niveau du nœud B. Généralement, ce paquet de collision est d'une taille comparable à celle des paquets de contrôle *ACK* ou *CTS*.

La raison pour laquelle nous utilisons une valeur aléatoire T_{coll} est que nous voulons échapper à la détection par le nœud surveillant (l'IDS). En effet, une collision qui se produit à chaque fois à la même période peut être détectée et classée comme anomalie par l'IDS. Dans la deuxième partie du scénario, l'attaquant envoie le faux paquet *ACK* au nœud A à T_{valide}. La durée T_{valide} est calculée ainsi :

$$T_{valide} = NAV(CTS) - T_{ACK} - SIFS \tag{6.3}$$

Lorsque le nœud A reçoit le paquet *ACK* avant une certaine période $TOut_2$, il ne se rend pas compte de la présence d'une anomalie ou d'un faux paquet *ACK*. En effet, $TOut_2$ est le temps maximum entre le temps du début de transmission du paquet DATA et le temps de réception du paquet *ACK*. Le $TOut_2$ est calculé ainsi :

$$TOut_2 = T_{DATA} + \delta + SIFS + T_{ACK} + \delta \tag{6.4}$$

où δ est le délai de propagation maximum [4]. Ainsi, T_{valide} doit être inférieur à $TOut_2$, sinon le nœud émetteur peut détecter le problème et retransmettre à nouveau le paquet.

La figure 6.7 montre l'organigramme d'une attaque de type fausse validation de paquet, qui utilise le faux paquet *ACK*. Lorsqu'un attaquant reçoit un paquet *RTS* qui ne lui est pas destiné, il détermine l'adresse des deux nœuds émetteur et récepteur, puis il attend la réception du paquet *CTS* pendant maximum T_1. T_1 est défini par le temps $SIFS$, le temps de propagation du paquet *CTS* (T_{CTS}) et le délai maximum de propagation (δ). Ainsi, T_1 est calculé comme suit : $T_1 = SIFS + T_{CTS} + \delta$. Lorsque le nœud attaquant reçoit le paquet *CTS* avant que le timer T_1 soit écoulé, alors le timer T_1 est annulé, puis le nœud lance les deux timers T_{coll} et $T_{validate}$, comme illustré dans la figure. Autrement, l'attaquant relance à nouveau l'algorithme d'attaque. Une fois que le timer T_{coll} est terminé, l'attaquant envoie un paquet au nœud D dans le but de créer une collision. Lorsque le timer $T_{validate}$ est terminé, l'attaquant envoie le faux paquet *ACK* à l'émetteur dans le but de valider la transmission du paquet DATA.

L'attaque de fausse validation est limitée au rayon de transmission du nœud attaquant, car ce dernier a besoin de recevoir correctement le paquet *RTS* et/ou le paquet *CTS*, dans le but de lancer l'attaque décrite ci-dessus. De plus, le nœud attaquant a besoin d'atteindre les deux nœuds émetteur et récepteur, dans le but de créer une collision chez le récepteur et la validation via le faux *ACK* chez l'émetteur. Malgré le fait que cette attaque est limitée au rayon de transmission de l'attaquant, son impact sur le réseau est très important. Prenons le protocole de routage, par exemple : le nœud ne peut pas établir la table de routage et tout le processus de routage sera compromis. Un autre impact négatif de cette attaque est la perturbation du mécanisme de surveillance qui permet l'évaluation de la coopération des nœuds dans le réseau.

6.3.4 Impact des attaques sur le mécanisme de surveillance

Le mécanisme de surveillance est développé pour contrôler l'activité des nœuds surveillés. L'attaquant avec le faux *CTS* peut facilement perturber le mécanisme de sur-

[4] Dans IEEE 802.11 avec la technologie DSSS (Direct Sequence Spread Spectrum), $\delta = 2us$

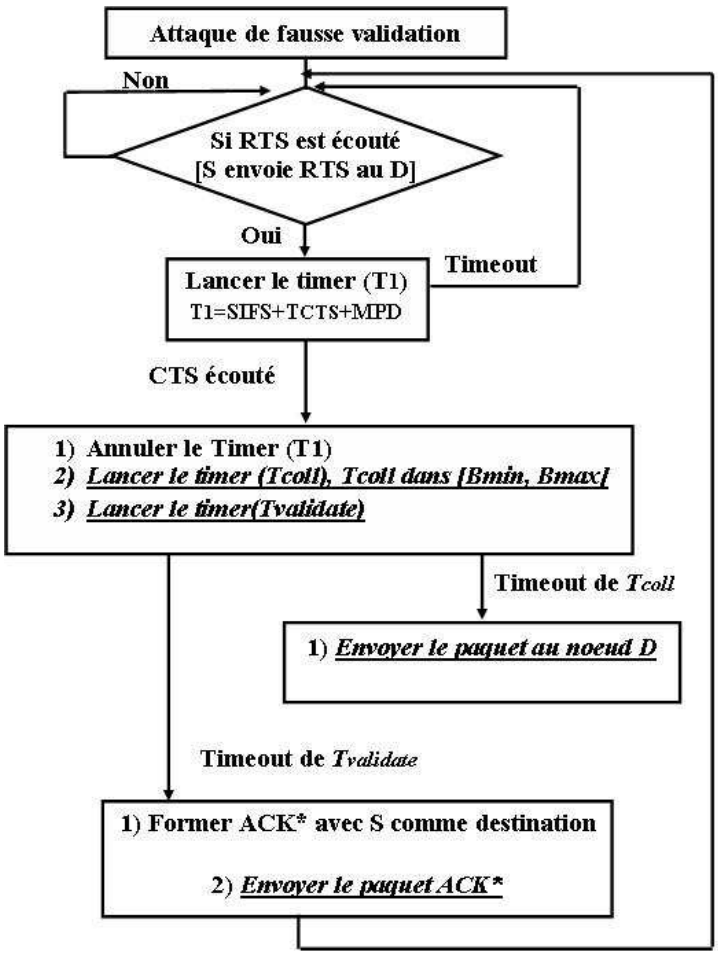


FIG. 6.7 – *Organigramme d'une attaque de type fausse validation de paquet*

veillance en se focalisant sur le nœud surveillé. Il peut ensuite le bloquer pendant une longue période pour l'empêcher de transmettre les paquets. Les paquets qui font l'objet du contrôle, et qui coopèrent dans le réseau, doivent participer à l'opération de routage des paquets, mais avec l'attaque répétitive de type faux *CTS*, le nœud sera bloqué et ne pourra pas transférer les paquets qu'il reçoit. Lorsque le nœud surveillant n'observe aucune transmission de paquet de la part du nœud surveillé, il va le classer comme un nœud égoïste qui ne veut pas coopérer dans le réseau. Ainsi, il va réduire le niveau de confiance du nœud surveillé et, bien sûr, sa réputation va diminuer aussi. Le nœud surveillant peut détecter que le nœud surveillé est bloqué si le nœud attaquant est un voisin des deux nœuds surveillé et surveillant. Autrement, le nœud surveillant ne se rend pas compte du faux *CTS* bloquant.

Le mécanisme de surveillance peut aussi être perturbé par l'attaque de type fausse validation, basée sur le faux *ACK*. L'idée consiste à réduire la réputation du nœud surveillé (victime). Dans ce cas, le nœud surveillé ne peut pas transférer les paquets car il ne les reçoit pas correctement à cause de la fausse validation, mais le nœud surveillant

ou émetteur reçoit bien le paquet *ACK*, ce qui lui permet de valider la transmission. Par exemple, lorsque le nœud surveillant A transmet le paquet au nœud surveillé B dans le but de le transférer à un autre nœud, le nœud A doit être sûr que le nœud B a bien reçu le paquet (objet de surveillance). En effet, les paquets d'acquittement au niveau MAC ne sont pas pris en compte dans la couche de routage. Nous avons développé un modèle inter-couches qui permet de prendre en compte les paquets *ACK* au niveau de la couche de routage (cf. le chapitre précédent). Malheureusement, même si le modèle inter-couches est adopté, avec l'attaque de type fausse validation, le mécanisme de surveillance est perturbé. Par conséquent, l'attaquant peut facilement réduire la réputation de n'importe quel nœud sans que le nœud surveillant ne le détecte.

Le problème avec le faux *CTS* et le faux *ACK* est que l'attaquant n'a pas besoin d'usurper ("spoofer") l'adresse source, car ces paquets n'en ont pas besoin d'adresse source. De plus, l'attaquant peut facilement échapper à la procédure de réaction et de punition et continuer à attaquer en permanence. Dans le but d'implémenter les deux attaques (le faux *CTS* et la fausse validation de paquet basée sur le faux *ACK*), l'attaquant peut tricher dans le choix du backoff pour accéder plus rapidement au canal de communication.

6.4 Evaluation de l'impact des attaques

Dans cette section, nous étudions l'impact du faux *CTS* et de la fausse validation des paquets sur le réseau. L'évaluation de l'impact de ces attaques est démontré par des résultats de simulations et des résultats de réelles expérimentations.

6.4.1 Résultats de simulations

Nous avons implémenté ces attaques avec le simulateur réseau *NS2* (ns 2, 1999) et nous avons simulé plusieurs scénarios dans différentes situations.

Tout d'abord, nous simulons une simple topologie réseau illustrée dans la figure 6.8. Dans ce scénario, nous avons deux ensembles de nœuds, $S_1 = \{0, 1, 2, 3\}$ et $S_2 = \{4, 5, 6, 7, 8\}$. Dans chaque ensemble, les nœuds peuvent communiquer directement avec les nœuds du même ensemble, mais les nœuds de l'ensemble S_2 ne peuvent pas atteindre les nœuds de l'ensemble S_1. Dans les deux ensembles, nous avons deux connexions de type CBR (la taille des paquets est de 1000 bytes et le débit est de 50 paquets/seconde). Dans l'ensemble S_1, il n'y a aucun nœud malicieux, mais dans l'ensemble S_2 le nœud 8 est un nœud malicieux capable d'attaquer par de faux *CTS* et de fausses validations de paquets via les faux *ACK*.

Nous choisissons le débit comme métrique pour montrer l'impact de ces attaques sur le réseau. Dans la figure 6.9, nous traçons le débit moyen du réseau en fonction du temps de simulation. Dans le cas de l'attaque de type faux *ACK*, nous remarquons une différence significative entre le débit obtenu sans et avec un attaquant dans le réseau. De même, dans le cas de l'attaque de type faux *CTS*, nous remarquons une dégradation

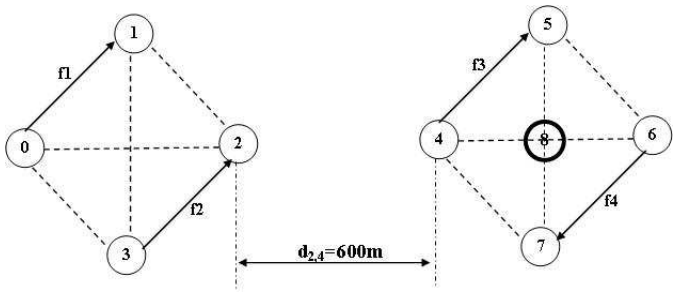


FIG. 6.8 – *Simple topologie réseau*

du débit avec la présence de l'attaquant dans le réseau. En revanche, l'attaque basée sur le faux *ACK* a un impact plus négatif sur le débit que celle qui se base sur le faux *CTS*, car le faux *CTS* génère une situation de blocage pour un certain temps, tandis que le faux *ACK* crée des collisions chez le nœud récepteur puis transmet le faux paquet *ACK* dans le but d'obtenir une fausse validation chez l'émetteur et d'empêcher une retransmission (par l'émetteur). Pour comparer les deux attaques, nous pouvons dire que la fausse validation est plus complexe à implémenter que celle du faux *CTS*, mais aussi que l'attaque de type fausse validation a un impact plus négatif sur le réseau que celle de type faux *CTS*.

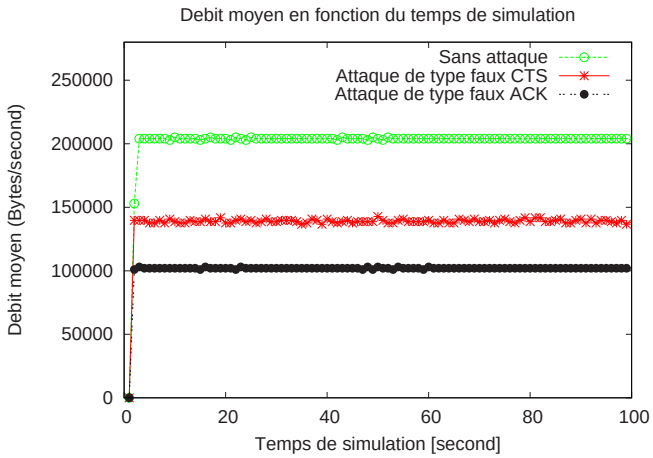
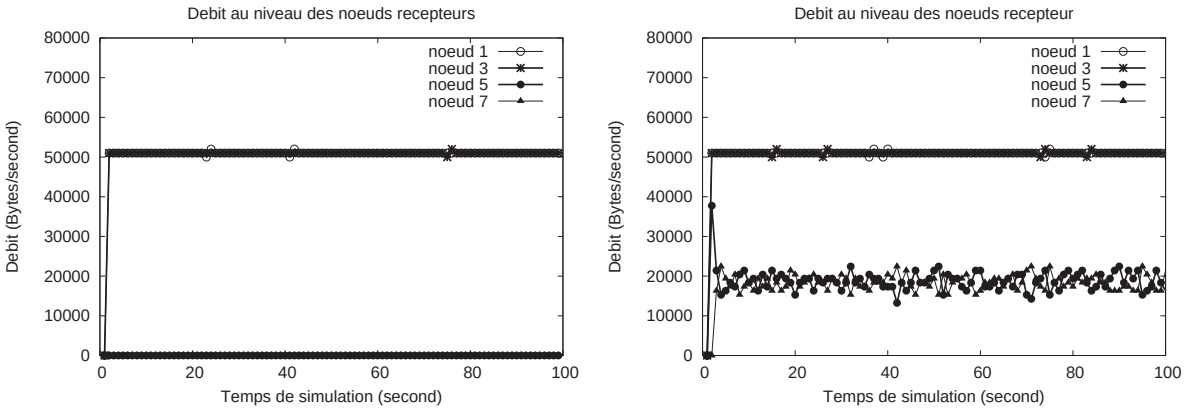


FIG. 6.9 – *Débit moyen en fonction du temps de simulation*

Dans le but de montrer l'impact de la fausse validation (faux *ACK*) au niveau de chaque récepteur et de prouver les résultats d'analyses précédents, nous traçons les résultats obtenus dans la figure 6.10(a). Nous remarquons que les nœuds récepteurs 1 et 3 de l'ensemble S_1 ont un débit plus ou moins stable, contrairement aux nœuds 5 et 7 de l'ensemble S_2 : leur débit est faible et instable dans le cas d'une attaque avec le faux *CTS*, comme illustré dans la figure 6.10(b), car les nœuds 5 et 7 sont situés dans la portée de transmission du nœud malicieux 8, ce qui n'est pas le cas des nœuds 1 et 3. Dans le cas d'une fausse validation (faux *ACK*), nous observons que le débit des

nœuds récepteurs 5 et 7 est nul. L'explication de ces résultats est la suivante : les nœuds 4 et 6 n'ont aucune information concernant les collisions chez les nœuds récepteurs 5 et 7, car les nœuds émetteurs ont déjà validé les paquets transmis via la réception des faux paquets d'acquittement *ACK* de la part du nœud malicieux 8. Ainsi, les nœuds émetteurs continuent à transmettre les paquets et ne retransmettent jamais les paquets DATA déjà acquittés.

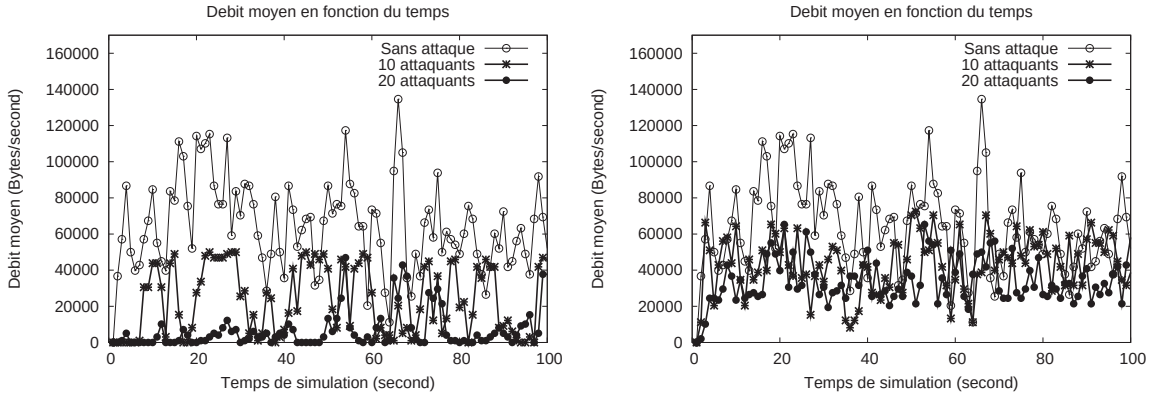


(a) Cas du faux ACK (b) Cas du faux CTS

FIG. *6.10* – *Débit moyen chez les nœuds récepteurs en fonction du temps*

Dans le but d'étudier l'impact de ces attaques dans le cas général, nous avons simulé un réseau de 50 nœuds distribués aléatoirement et de manière uniforme dans une surface de $800 \times 800m^2$ avec 25 connexions de type CBR et différents nombres de nœuds malicieux dans le réseau. Les figures 6.11(a) et 6.11(b) montrent le débit dans le cas normal et dans le cas où 10 à 20 nœuds malicieux capables de monter des attaques de type faux *CTS* et faux *ACK* sont présents dans le réseau. Nous remarquons que lorsque le nombre de nœuds malicieux augmente, le débit du réseau diminue rapidement. La figure 6.11(b) montre les résultats obtenus dans le cas du faux *CTS*. Nous observons quelques différences avec le cas de la fausse validation (faux *ACK*) : le débit diminue un peu avec l'introduction de 10 et 20 nœuds malicieux. La différence dans le cas de 10 et 20 attaquants n'est pas significative, comparée au cas du faux *ACK*.

Dans la figure 6.12, nous montrons l'impact de l'introduction de différents nombres de nœuds attaquants dans le réseau (de 0 à 25, soit 0 à 50%) avec 150 secondes comme durée de simulation. Dans le cas où 5 attaquants sont présents dans le réseau, nous remarquons que le débit diminue de la même manière dans les deux cas d'attaques (le faux *ACK* et le faux *CTS*). Cependant, lorsque le nombre d'attaquants est de 10, nous constatons que le débit du réseau décroît plus dans le cas du faux *ACK* que dans le cas du faux *CTS*. Le même constat est établi lorsque le nombre d'attaquants varie de 15 à 25. En revanche, le nombre d'attaquants a un impact plus négatif avec la fausse validation qu'avec le faux *CTS*.



(a) Cas du faux ACK (b) Cas du faux CTS

FIG. *6.11* – *Débit moyen du réseau en fonction du temps de simulation*

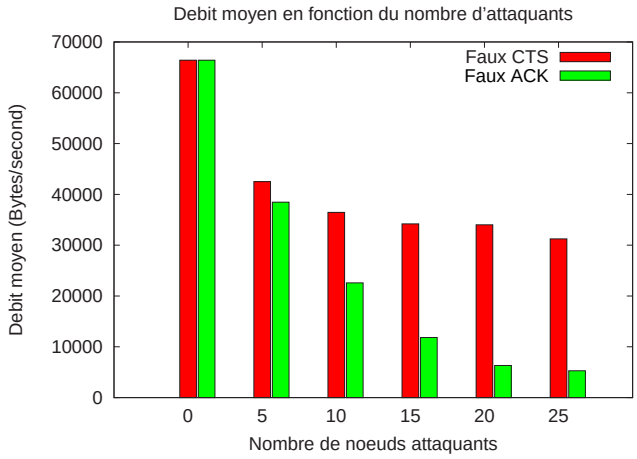


FIG. *6.12* – *Impact du nombre d'attaquants sur le débit du réseau*

6.4.2 Résultats d'expérimentations

Plusieurs simulations ont été effectuées par des chercheurs mais ne sont pas réalisables ou expérimentables via des « testbed ». Dans cette sous section, nous montrons que les attaques présentées ci-dessus peuvent être expérimentées par des tests réels. Dans le but de montrer la possibilité d'exploiter les vulnérabilités décrites dans la section précédente, nous avons décidé de réaliser ces attaques et de les expérimenter. Pour atteindre cet objectif, nous expérimentons un simple scénario d'attaque par l'utilisation du driver *MadWiFi* (Multiband Atheros Driver for Wireless Fidelity) Leffler (2007), disponible sous la plate-forme Linux. Pour des raisons de compatibilité avec divers *MadWiFi*, nous avons utilisé des cartes sans fil basées sur la chipset Atheros Communications (2007). Pour les équipements expérimentaux, nous avons utilisé les cartes WiFi Atheros *AR*5005*G* 802.11abg NIC Chipset de TP-Link et des ordinateurs (PC) avec

un processeur Intel Pentium 4 2.4GHz, 512KB cache L2 et 512MB de mémoire RAM. La figure 6.13 représente le simple scénario que nous avons mis en place. Les machines A et B veulent communiquer et la machine M joue le rôle de l'attaquant.

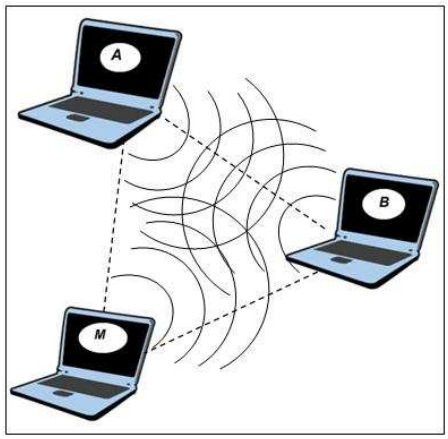


FIG. *6.13* – *Scénario de l'expérimentation*

A- Cas de l'attaque de type faux *CTS*

Le nœud A lance des pings de manière continue pour le nœud B. Le processus de ping se résume en deux types de paquets ICMP : requête (request) et réponse (reply). Après le premier échange (request/reply) réussi entre les nœuds A et B, le nœud M écoute la communication et obtient la durée de communication (NAV). Ensuite, il commence à planifier son attaque. Une fois le canal de communication libre (IDLE), le nœud M envoie le faux paquet *CTS* avec $NAV(CTS)$ comme durée de communication présumée (voir l'algorithme d'attaque). Le $NAV(CTS)$ peut être soit une valeur constante, soit une valeur aléatoire, mais elle ne doit pas dépasser $32767\mu Sec$ IEEE802-11 (1999). Nous avons utilisé l'analyseur Wireshark License (2008) pour écouter le trafic et superviser le réseau. Nous avons obtenu les résultats tracés dans la figure 6.14. Nous remarquons qu'après une première communication réussie entre les nœuds A et B, le nœud M lance son attaque vers environ 30 secondes et réussit à émettre le faux *CTS*. Ensuite, ni le nœud A ni le nœud B ne peuvent communiquer pendant la durée présumée de transmission $NAV(CTS)$. L'attaquant M continue à transmettre le faux paquet *CTS* de manière continue et domine le canal de communication en créant une situation de faux blocage. Nous nous focalisons sur la période comprise entre 30 et 35 secondes et nous traçons dans la figure 6.14 le nombre de paquets en fonction du temps de l'expérience. Nous remarquons que le premier faux *CTS* est transmis, puis après la durée de NAV, un autre faux *CTS* est transmis par l'attaquant dans le but de faire durer la situation de blocage le plus longtemps possible. Lorsque le nœud attaquant M arrête d'envoyer des faux *CTS*, soit vers 320 secondes, le nœud A peut envoyer son paquet au nœud B et la situation du canal revient à l'état normal.

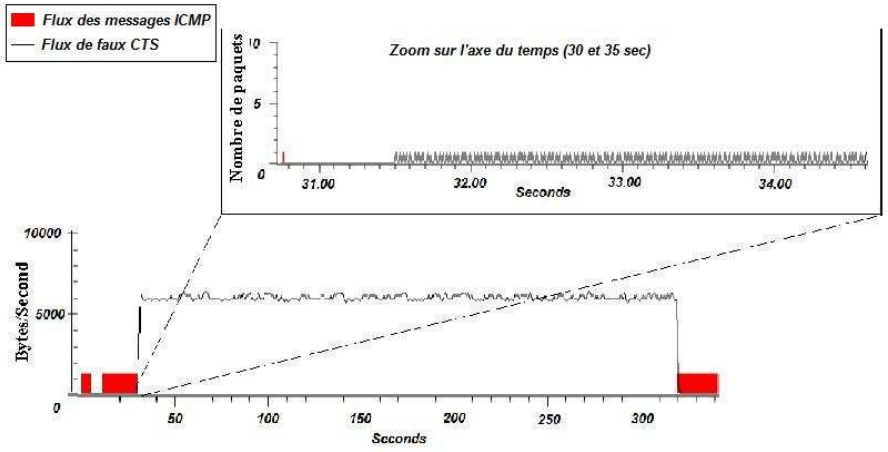


FIG. 6.14 – *L'impact de l'attaque de type faux CTS sur la communication ICMP entre A et B*

Dans le but d'étudier l'attaque de type faux *CTS* avec une communication TCP, nous avons lancé une connexion SSH entre les deux nœuds A et B. La figure 6.15 montre le résultat obtenu en utilisant l'analyseur Wireshark. La connexion SSH est représentée par le flux TCP dans la figure 6.15. Nous remarquons que lorsque l'attaquant a réussi à accéder au canal après avoir envoyé un faux *CTS*, soit vers 39 secondes de temps d'expérience, alors la communication entre les deux nœuds A et B est interrompue pendant la durée NAV introduite par l'attaquant. Ensuite, l'attaquant peut transmettre le faux *CTS* de manière continue, ce qui perturbe la communication entre les nœuds. Avec ces résultats, nous montrons l'efficacité et la faisabilité de l'attaque de type faux *CTS*, ainsi que son impact réel sur le réseau.

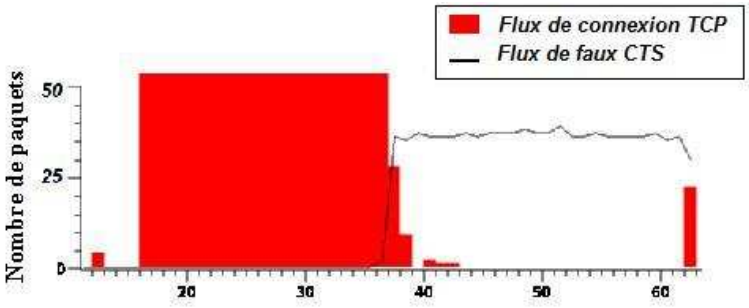


FIG. 6.15 – *Impact de l'attaque de type faux CTS sur la connexion SSH entre A et B*

B- Cas de l'attaque de type faux *RTS*

Dans le but de montrer l'impact de l'attaque de type faux *RTS* par l'étude expérimentale, nous avons implémenté cette attaque avec MadWiFi et les résultats obtenus sont montrés dans la figure 6.16. Nous observons que lorsque l'attaquant a réussi à

transmettre le faux *RTS*, il bloque les nœuds A et B pour une durée aléatoire $NAV(RTS)$ choisie par l'attaquant. Vers environ 68.5 secondes, le nœud A réussit à accéder au canal, mais peu après, le nœud M prend le contrôle du canal via la transmission d'un faux *RTS*. Le nœud attaquant M est en compétition avec les nœuds A et B pour accéder au canal et transmettre le paquet *RTS*. Si on compare les attaques de type faux *RTS* et faux *CTS*, nous remarquons que le faux *CTS* a un impact plus négatif que le faux *RTS*, car le nombre de collision des paquets *CTS* est moins que le nombre de collision des paquets *RTS*. Cela est dû à la taille du paquet *CTS* qui est égale à 38 bytes. Il est donc plus petit que le paquet *RTS* dont la taille est égale à 44 bytes. Pour conclure, nous pouvons dire que le faux *CTS* est plus efficace en terme d'attaque et plus difficile à détecter que le faux *RTS*.

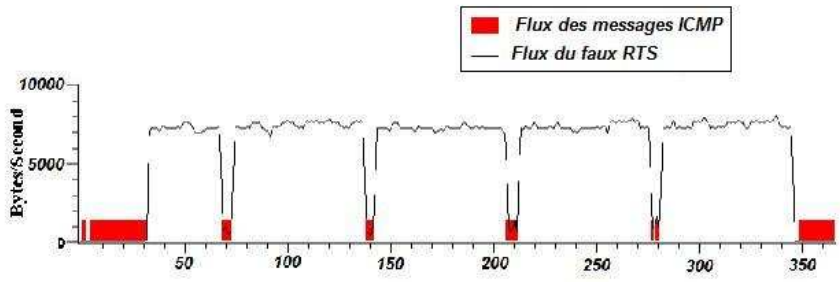


FIG. 6.16 – *Impact de l'attaque de type faux RTS sur la communication ICMP entre A et B*

Nos résultats d'expérimentation montrent la possibilité d'implémenter ces attaques et d'étudier leur impact réel sur le réseau.

6.5 Solutions de sécurité et leur analyse

Dans le but de contrer les attaques basées sur les faux paquets *RTS*, *CTS* et *ACK*, nous sommes amenés à répondre à la question suivante : Comment assurer l'authentification et l'intégrité des paquets de contrôle ? Plusieurs réponses peuvent être proposées pour traiter de ce problème. Nous avons classé les réponses en fonction des solutions qui utilisent ou non les mécanismes de cryptographie.

6.5.1 Solution simple sans utilisation de la cryptographie

Cette solution consiste à ajouter l'adresse du nœud émetteur dans les paquets *CTS* et *ACK* pour éliminer la vulnérabilité au niveau du format de ces paquets. Lorsqu'un nœud récepteur reçoit les paquets *CTS* et *ACK*, il peut vérifier l'adresse source avant de bloquer sa transmission ou de valider le paquet DATA. Cependant, la taille de ces paquets (*CTS* et *ACK*) augmente de 6 bytes, donc la taille finale de ces paquets après avoir pris en compte l'en-tête physique est de 44 bytes.

L'avantage principal de cette solution est qu'elle est simple à implémenter, car la modification du mécanisme classique *RTS/CTS* n'est pas significative et la charge additionnelle au niveau des paquets *CTS/ACK* ne dépasse pas 6 bytes. En outre, cette solution complique davantage la procédure d'attaque, mais ne la supprime pas définitivement. Un attaquant peut compromettre cette solution, mais à condition de rendre sa procédure d'attaque plus sophistiquée. Dans ce cas, l'attaquant a besoin de changer l'identité du nœud émetteur ("usurper l'adresse source") au niveau des paquets *CTS* et *ACK* avant de lancer son attaque et cela lui permet aussi d'échapper au système de détection d'intrusions (IDS). Malheureusement, cette solution ne permet pas d'éliminer définitivement la vulnérabilité et donc l'attaque, mais elle complique davantage la procédure d'attaque pour les nœuds malicieux. Le manque de fonctions de contrôle d'intégrité et d'authentification des paquets de contrôle rend cette solution compromise.

Dans le but d'améliorer cette solution, nous introduisons les mécanismes de cryptographie pour les paquets de contrôle. Cependant, nous devrons faire face au problème du coût des solutions de sécurité pour la qualité de service en terme de débit, de surcharge de réseau et enfin de consommation d'énergie. Nous avons classé les solutions basées sur la cryptographie en deux catégories : solution assurant la fonction d'authentification et solution sans fonction d'authentification.

6.5.2 Solution sans fonction d'authentification contre les faux ACK

D'après nos connaissances, il n'existe aucune solution dans la littérature qui permette de contrer l'attaque basée sur le faux ACK. Une solution possible pour remédier à cette attaque est d'utiliser la fonction de hachage telle que : *MD5*, *SHA-1*, etc. L'idée consiste à ce que le nœud émetteur calcule l'empreinte numérique du paquet DATA ($H(P_{DATA})$), comme cela est illustré dans la figure 6.17. Le résultat de la fonction de hachage $H(P_{DATA})$ est conservé par le nœud émetteur et il ne transmet pas le paquet DATA. Une fois que le récepteur reçoit le paquet DATA, il calcule l'empreinte numérique de ce paquet $H(P'_{DATA})$, puis cette empreinte est transmise dans le paquet *ACK*. Ainsi, lorsque le nœud émetteur du paquet DATA reçoit le paquet ACK, il va vérifier la validité de ce paquet (*ACK*) en comparant les deux empreintes numériques (celle qui se trouve dans le paquet ACK ($H(P'_{DATA})$) et celle qu'il a déjà calculée avant de transmettre le paquet DATA ($H(P_{DATA})$)). Si $H(P_{DATA})$ est égale à $H(P'_{DATA})$, alors le test est positif et le nœud émetteur peut valider le paquet DATA transmis. Dans le cas contraire, le nœud émetteur va en déduire que le paquet *ACK* est généré par un nœud malicieux qui cherche à créer une fausse validation. La figure 6.17 résume cette solution pour contrer les fausses validations basées sur les faux *ACK*.

L'avantage majeur de cette solution est le fait qu'elle n'a besoin d'aucun algorithme de chiffrement ni d'aucun système de gestion de clés. De plus, cette solution peut être facilement implémentée, car il suffit de changer le paquet *ACK* en augmentant la taille de ce paquet de maximum 20 bytes avec l'utilisation de la fonction de hashage *SHA1-160*. Cette solution permet de réduire significativement le risque d'une attaque basée

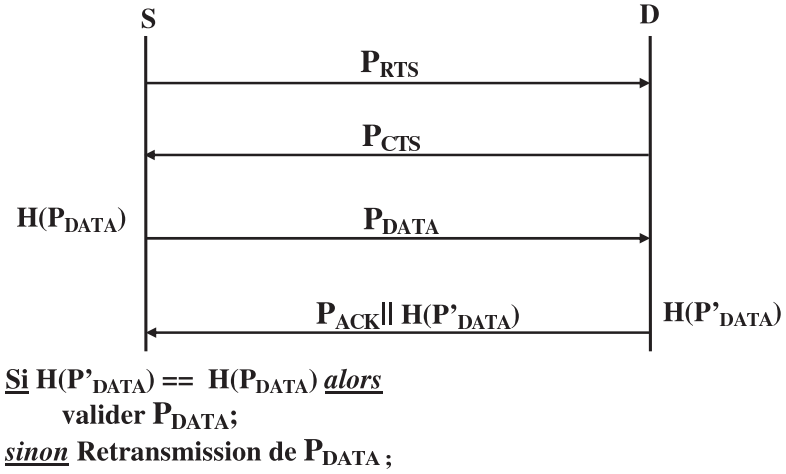


FIG. *6.17* – *Solution contre les fausses validations des paquets (faux ACK)*

sur le faux *ACK* (la fausse validation de paquet). Cependant, compromettre cette solution est possible mais très difficile. En effet, la procédure d'attaque contre cette solution nécessite au moins la collaboration de deux nœuds malicieux. La figure 6.18 décrit le scénario d'attaque comme suit : deux nœuds malicieux doivent être situés dans la portée de transmission du nœud S, dans le but de recevoir correctement les paquets de contrôle *RTS/CTS* et de mettre en place leur attaque. La position des nœuds attaquants M_1 et M_2 doit être choisie en fonction de la position des nœuds S et D, (sachant que le nœud S veut envoyer un paquet DATA au nœud D). Le premier attaquant M_1 doit être situé dans la zone d'interférence du nœud D (R_i), car son rôle est de créer une collision au niveau du nœud récepteur D. De plus, l'attaquant M_1 doit être en dehors de la zone d'interférence du nœud M_2 pour laisser la possibilité au nœud M_2 de recevoir correctement le paquet DATA transmis par le nœud S. Lorsqu'une collision se produit au niveau du nœud D, l'attaquant M_2 peut recevoir correctement le paquet DATA puis répondre au nœud S avec un faux *ACK* contenant la bonne empreinte numérique du paquet DATA. Le nœud S ne se rend pas compte que le paquet ACK est généré par un nœud malicieux, car $H(P_{DATA}) = H(P'_{DATA})$. La condition pour que cette attaque se réalise est la suivante : aucun nœud dans la région notée $AV(d_{M_2,S})$ (voir la figure 6.18) ne doit transmettre pendant la transmission du paquet DATA. Si un nœud dans cette région $AV(d_{M_2,S})$ transmet, l'attaquant M_2 ne reçoit pas correctement le paquet DATA. Par conséquent, l'attaquant $M2$ essaye d'être plus proche du nœud S dans le but de réduire la région AV. Néanmoins, il doit être en dehors de la région d'interférence du nœud M_1 pour pouvoir recevoir correctement le paquet DATA. Pour formuler ce problème, l'attaquant doit choisir la distance entre l'autre attaquant et lui même comme suit :

– L'attaquant M_1 doit être en dehors de la région d'interférence de l'attaquant M_2, cela veut dire que $d_{M_1M_2} > d_{M_2S}\sqrt[k]{T_{SNR}}$, où T_{SNR} est le seuil du rapport signal sur bruit (SNR) et k est un paramètre qui dépend de la propagation radio (ex. : dans le cas de l'environnement libre sans obstacle : le modèle TWO-RAY GROUND ;

k est égal à 4). Le rayon d'interférence entre les deux nœuds A et B est calculé comme suit : $R_i = d_{AB}\sqrt[k]{T_{SNR}}$ (K. Xu et Bae, 2003).

– Donc, l'attaquant M_2 reçoit le paquet DATA (P_{DATA}) correctement, si aucun nœud dans la région $AV(d_{M2,S})$ ne transmet pendant la phase de réception. La meilleure situation existe lorsque cette région est couverte par la portée de détection de porteuse (CS : Carrier Sense) du nœud S, c'est-à-dire lorsque $d_{M2,S} \leq \frac{R_S}{1+\sqrt[k]{T_{SNR}}}$

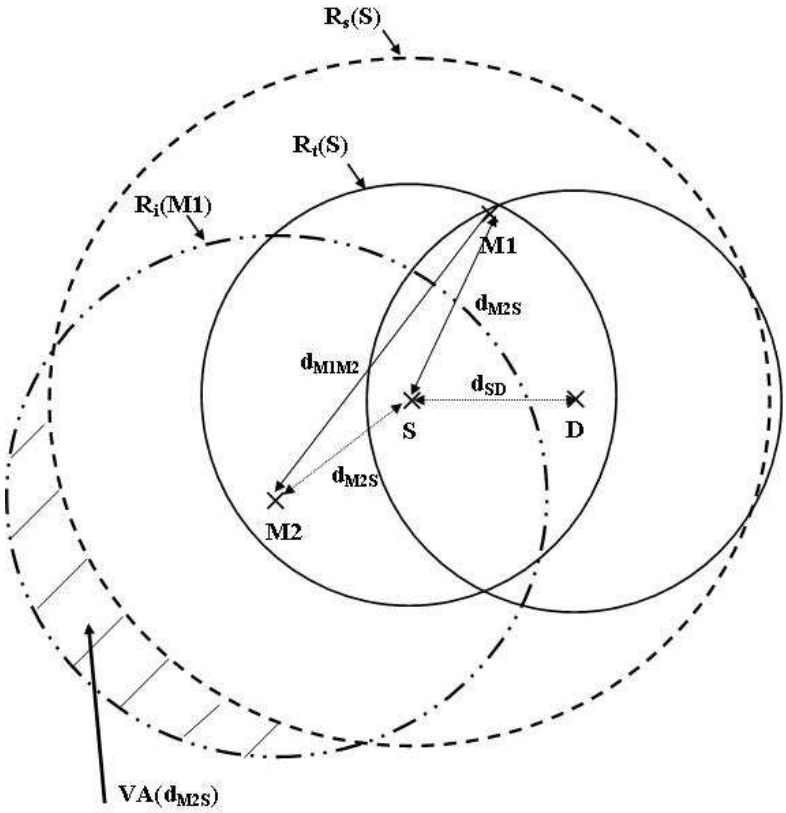


FIG. 6.18 – *Scénario d'attaque possible contre la solution 2*

En outre, avec cette solution, les paquets de contrôle ne peuvent pas être authentifiés par les nœuds récepteurs. Donc, les attaques basées sur le faux *RTS* et le faux *CTS* ne peuvent être contrées. Dans le but d'éliminer définitivement ces attaques, les deux fonctions de contrôle d'intégrité et d'authentification doivent être assurées. C'est pourquoi la prochaine sous-section est réservée aux solutions avec les deux fonctions primordiales pour éviter ces attaques.

6.5.3 Solution avec les fonctions d'authentification et d'intégrité

L'idée de cette solution est la suivante : lorsqu'un nœud reçoit un paquet de contrôle tel que : *RTS*, *CTS* ou *ACK*, il doit avant tout vérifier l'authentification de l'émetteur de

ce paquet puis vérifier l'intégrité des informations dans ces paquets. Si toute la procédure est exécutée correctement, le nœud récepteur peut bloquer sa transmission ou répondre par le paquet *CTS* si il est la destination du paquet *RTS*. Puis il envoie le paquet DATA s'il reçoit un paquet *CTS*. En outre, lorsque l'émetteur du paquet DATA reçoit le paquet *ACK*, il doit vérifier que le récepteur du paquet DATA a bien reçu ce paquet et que le paquet *ACK* est généré par le même nœud. Dans le but d'assurer l'authentification et le contrôle d'intégrité des données, plusieurs approches peuvent être discutées mais lorsque nous introduisons les contraintes de l'environnement, comme la restriction des ressources, la plupart de ces approches sont éliminées. Par exemple, il est préférable d'utiliser la cryptographie symétrique au niveau de la couche MAC du modèle OSI que la cryptographie à clé publique (asymétrique), car la cryptographie symétrique est plus rapide et moins coûteuse en terme de calcul et de complexité que la cryptographie asymétrique. Cependant, même avec la cryptographie asymétrique, le coût de la sécurité n'est pas négligeable au niveau de la couche MAC. C'est pourquoi nous avons choisi le code d'authentification de message (Message Authenticated Code : MAC), et en particulier le MAC hashé (hashed MAC (HMAC) (PUB, 2001)). Ce dernier compte parmi les mécanismes de cryptographie les moins coûteux aptes à résoudre ce problème. Le HMAC utilise les fonctions de hashage bien connues telles que MD5 et SHA1 pour assurer l'intégrité du message. De plus, HMAC permet d'utiliser une clé partagée (K) pour assurer l'authentification du message. Formellement, HMAC est défini comme suit :

$$HMAC(M,K) = H(K \oplus opad||H(K \oplus ipad)||M))$$

où $H(x)$ est la fonction de hashage et M le message à envoyer. Le *ipad* est une chaîne en hexadécimale (36) répétée B fois et *opad* est une chaîne hexadécimale (5C) répétée B fois. HMAC est développé pour les messages dont la taille est relativement longue. Cependant, pour les messages de petite taille, comme c'est le cas des paquets de contrôle, HMAC n'est pas la meilleure solution (Patel, 2002). Dans le cas des paquets de contrôle, la taille des paquets varie entre 44 bytes et 38 bytes. Cela signifie que la taille des paquets est inférieure à la taille nécessaire du bloc qui va servir aux itérations par la suite. D'une autre manière, lorsque le message est plus petit que la taille du bloc itératif B (ex. $B = 64bytes$), HMAC nécessite au moins deux appels de la fonction de hashage au lieu d'un seul. C'est pourquoi nous avons choisi la version modifiée de HMAC, appelée HMAC améliorée (Enhanced HMAC : EHMAC)(Patel, 2002) pour les paquets de contrôle *RTS*, *CTS* et *ACK*, dans le but de réduire le coût de calcul de la fonction de hashage. EHMAC(M, K) est formellement défini comme suit :

$$\begin{cases} H(K \oplus opad||M||pad||1) & \textbf{si } |M| \leq 445bits \\ H(K \oplus opad||H(K \oplus ipad||M_{pref})||M_{suff}||0) \end{cases}$$

où M_{pref} et M_{suff} dépendent de la fonction de hashage utilisée. Par exemple, dans le cas de SHA :

$$\begin{cases} M_{pref} = M_1 \dots M_{|M|-286} \\ M_{suff} = M_{|M|-285} \dots M_{|M|} \end{cases}$$

Cette solution, comme n'importe quelle autre solution basée sur les mécanismes de cryptographie, nécessite un système de distribution de clés ou d'échange de clés. Dans

cette solution, nous ne nous focalisons pas sur ces problèmes car plusieurs solutions existent déjà dans la littérature. Par exemple, nous avons déjà proposé une solution basée sur le modèle de confiance et la division du réseau en groupes pour distribuer les clés de certification. Il est possible d'utiliser cette solution dans cette situation (Rachedi et Benslimane, 2006). Lorsqu'un nœud veut rejoindre le réseau, il a besoin de demander un certificat numérique avec une clé de groupe (K_G) qui peut être mise à jour périodiquement par l'autorité de certification (CA).

Les nouveaux formats des paquets de contrôle sont illustrés dans la figure 6.19. Dans tous les paquets de contrôle *RTS*, *CTS* et *ACK*, nous introduisons le EHMAC avec différentes tailles d'empreinte numérique (entre 10 et 20 bytes, cela dépend de la fonction de hashage et du niveau de sécurité souhaités). De plus, dans le paquet *CTS*, nous avons ajouté 6 bytes pour le champ de l'adresse de l'émetteur, afin que les nœuds voisins de l'émetteur du paquet *CTS* puissent vérifier l'adresse source et l'intégrité des informations du paquet. Cependant, dans le paquet *ACK*, nous n'avons pas ajouté l'adresse du nœud émetteur car le nœud qui attend l'acquittement connaît l'identité du nœud qui va transmettre le paquet *ACK*. En revanche, nous avons ajouté l'adresse du nœud émetteur du paquet *ACK* dans le message M, tel que $M = \{Ctrl||Dure||Destination||Source\}$. Le message M subit une transformation via EHMAC avec le nœud qui émet le paquet *ACK*, puis ajoute le résultat obtenu de EHMAC(M, K_{SD}) dans le paquet *ACK*. Une fois que le nœud émetteur du paquet DATA reçoit le paquet *ACK*, il sera en mesure de vérifier l'intégrité des informations dans le paquet et ainsi, l'authentification de l'émetteur du paquet.

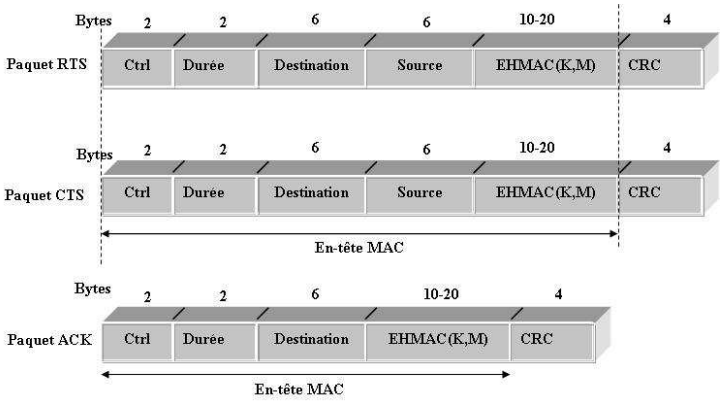


FIG. 6.19 – *Format des paquets RTS, CTS et ACK sécurisés*

Le nouveau mécanisme *RTS/CTS* avec les deux fonctions d'authentification et de contrôle d'intégrité est présenté dans la figure 6.20.

Nous appelons les voisins du nœud émetteur S NS_i, les voisins du nœud récepteur D ND_j et l'ensemble des nœuds voisins communs avec S et D NSD_k. Le nouveau mécanisme *RTS/CTS* fonctionne en quatre étapes. Première étape : le nœud S transmet un paquet *RTS* au nœud D avec $EHMAC(K_G, RTS)$. Ce paquet peut être reçu par les nœuds D, NS_i et NSD_j. Tous ces nœuds sont capables d'authentifier et de vérifier

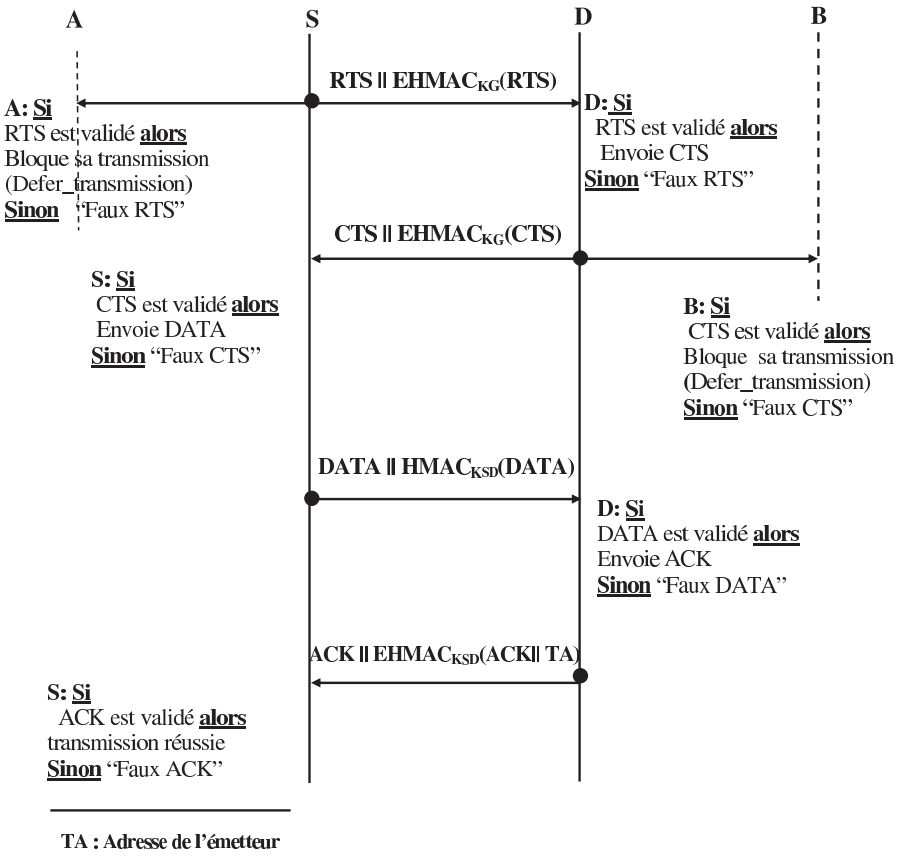


FIG. *6.20* – *Mécanisme RTS/CTS sécurisé.*

l'intégrité du paquet *RTS*. Deuxième étape : lorsque le nœud D reçoit le paquet *RTS* et après l'authentification et la vérification de l'intégrité des données, il répond par le paquet *CTS* avec son adresse et l'empreinte numérique suivante : $EHMAC(K_G, CTS)$. Cependant, l'ensemble des nœuds S, ND_k et NSD_k sont capables d'authentifier le paquet *CTS* s'ils possèdent la clé de groupe K_G. Troisième étape : le nœud S commence la transmission du paquet *DATA* avec $HMAC(K_{SD}, DATA)$, après avoir vérifié le paquet *CTS*, sachant que la clé K_{SD} est une clé partagée entre les deux nœuds S et D. Au cours de cette étape, seul le nœud D est capable d'authentifier le paquet *DATA*. Finalement, après une réception correcte et une vérification du paquet *DATA*, le nœud D répond par le paquet *ACK* avec $EHMAC(K_{SD}, ACK||Transmitter@)$ comme information. La quatrième et dernière étape concerne le S et uniquement le nœud S, qui est capable de vérifier l'authentification et l'intégrité du paquet *ACK*.

La complexité de ce problème consiste à assurer l'authentification des paquets *RTS* et *CTS*, et pas uniquement par les nœuds D et S respectivement, mais par l'ensemble des nœuds NS_i, ND_j et NSD_k. De plus, le mécanisme *RTS/CTS* est proposé à la base pour remédier au problème des nœuds cachés et des collisions. C'est pour cela que les paquets de contrôle sont de petite taille (44 bytes pour le *RTS* et 38 bytes pour le *CTS*). Donc, n'importe quelle solution proposée pour sécuriser le mécanisme *RTS/CTS* doit

prendre en considération la charge additionnelle au niveau des paquets de contrôle, car c'est un paramètre important en ce qui concerne les collisions de paquets. En outre, pour assurer l'authentification et le contrôle d'intégrité, nous sommes amenés à utiliser les mécanismes de cryptographie. Cependant, certaines approches basées sur les mécanismes de cryptographie ont un coût de sécurité non négligeable. C'est pourquoi nous étudions les performances des solutions que nous avons proposées dans la section suivante.

6.6 Evaluation de la performance des solutions proposées

Dans le but d'évaluer l'impact et le coût des solutions proposées sur le réseau, nous avons implémenté ces solutions dans le simulateur réseau *NS2* (ns 2, 1999) et dans différentes situations. Nous utilisons le mécanisme classique RTS/CTS comme référence pour le comparer avec les solutions proposées. La première solution ne prend pas en compte les mécanismes de cryptographie, mais uniquement l'ajout de l'adresse de l'émetteur dans les deux paquets *CTS* et *ACK*. La deuxième solution prend en compte les deux fonctions principales : l'authentification et le contrôle d'intégrité. Nous avons implémenté cette dernière avec différents types de HMAC et différentes tailles d'empreinte numérique (HMAC-MD5-80, HMAC-MD5-128, HMAC-SHA1-160). Nous étudions deux types de topologie réseau : la topologie du réseau de type Grid et la topologie réseau aléatoire, dans le but de montrer la faisabilité des solutions que nous avons proposées, et de les comparer avec le cas classique. Pour évaluer les performances de nos solutions, nous utilisons les métriques suivantes :

- Le débit, défini comme le nombre de bytes reçus avec succès chaque seconde.
- Le nombre de collisions des paquets de contrôle (*RTS/CTS/ACK*).
- La densité du trafic au niveau des paquets de contrôle : *RTS*, *CTS* et *ACK*

La figure 6.21 montre la topologie Grid de type 3×3 et la distance entre les nœuds est fixée à 225 mètres. Le rayon de la portée de transmission est fixé à 250 mètres. Pour le trafic réseau, nous utilisons des connexions de type CBR avec des paquets dont la taille est égale à 512 octets pendant une durée de simulation de 100 secondes.

La figure 6.22 montre le nombre de collisions des paquets de contrôle avec le protocole RTS/CTS classique, la solution simple avec l'adresse source (*TA*) dans les paquets *CTS* et *ACK* et la solution avec l'empreinte numérique HMAC-SHA1-160 (qui assure l'authentification et le contrôle d'intégrité). Nous remarquons que le nombre de collisions des paquets de contrôle augmente proportionnellement au débit de transmission. Cependant, il augmente un peu plus lorsqu'on utilise la solution simple avec *TA* dans tous les paquets de contrôle que lorsqu'on utilise le protocole classique. Dans le cas de la solution avancée (avec l'authentification et le contrôle d'intégrité), nous observons que le nombre de collisions des paquets de contrôle augmente, mais il est comparable à celui que l'on observe avec la solution simple sans mécanisme de cryptographie. D'après les résultats obtenus, nous pouvons dire que l'augmentation du nombre de collisions des paquets de contrôle dans les deux solutions reste raisonnable et même

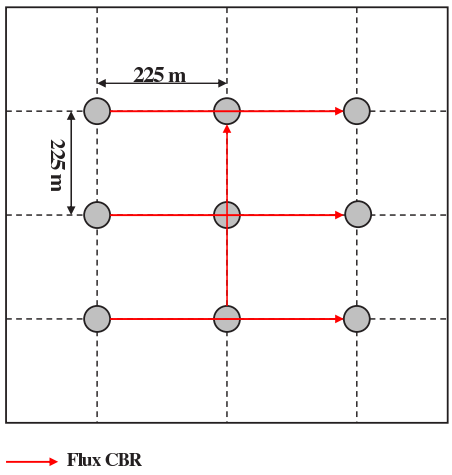


FIG. 6.21 – *Simple topologie de type Grid* (3×3)

comparable au cas du protocole classique *RTS/CTS*.

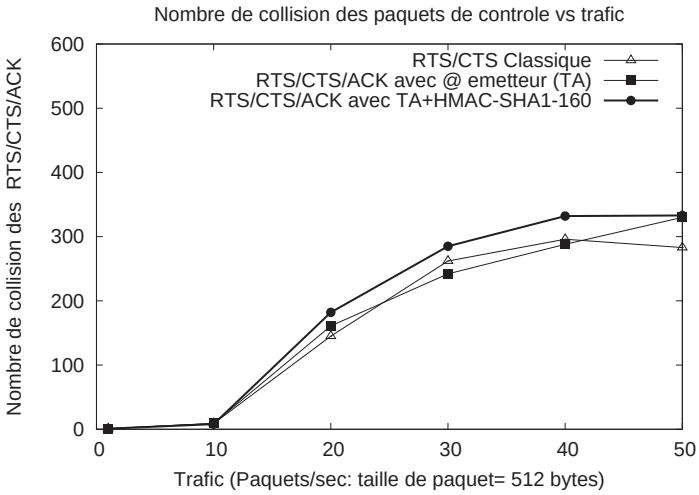


FIG. 6.22 – *Nombre de collisions des paquets de contrôle*

Dans le but de montrer l'impact des solutions proposées sur la métrique du débit, nous traçons dans la figure 6.23 le débit moyen dans le réseau en fonction de différentes densités de trafic, qui varient entre 10 et 40 paquets par seconde. Nous remarquons qu'avec une densité de trafic de $10 paquet/s$, le débit moyen dans le réseau est similaire dans les différentes solutions proposées et dans le mécanisme RTS/CTS classique. Lorsque la densité du trafic augmente, le débit du réseau diminue un peu plus avec la solution dont le niveau de sécurité est élevé (RTS/CTS/ACK avec TA+HMAC-SHA1-160) comparé à l'augmentation observée lorsqu'on utilise la solution de niveau moins élevé ou avec le mécanisme classique. Cela s'explique par l'augmentation de la taille des paquets de contrôle. Cependant, de ces résultats, nous pouvons déduire que le coût

des solutions proposées en terme de débit est négligeable avec une densité de trafic peu élevée.

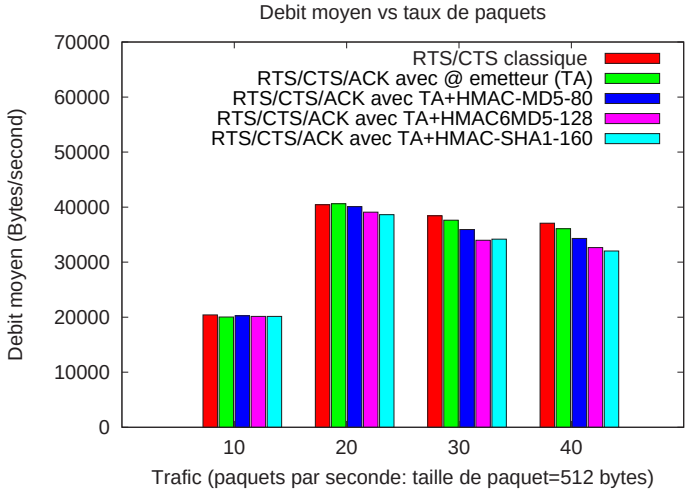


FIG. 6.23 – *Débit moyen du réseau en fonction de la densité du trafic*

Dans le but de comparer la surcharge du réseau liée aux paquets de contrôle *RTS*, *CTS* et *ACK* avec différentes solutions, nous traçons la surcharge du réseau liée aux paquets de contrôle en fonction de la densité du trafic dans la figure 6.24. Nous constatons que la surcharge augmente lorsque la densité du trafic augmente jusqu'à 20 paquets par seconde ($80Kbit/s$). Ensuite, la surcharge du réseau se stabilise à environ 2 Méga bytes pour le mécanisme RTS/CTS classique, $2.15MB$ pour la solution simple avec *TA* dans *CTS/ACK*, $2.6MB$ pour la solution avancée avec HMAC-MD5-80, $2.88MB$ avec HMAC-MD5-128 et enfin $3MB$ avec HMAC-SHA1-160. La table 6.1 montre la taille des paquets de contrôle *RTS*, *CTS* et *ACK* avec le mécanisme RTS/CTS classique et les différentes solutions proposées.

Protocole	RTS	CTS	ACK
RTS/CTS classique	44 bytes	38 bytes	38 bytes
CTS/ACK avec TA	44 bytes	44 bytes	44 bytes
HMAC-MD5-80	54 bytes	54 bytes	48 bytes
HMAC-MD5-128	60 bytes	60 bytes	54 bytes
HMAC-SHA1-160	64 bytes	64 bytes	58 bytes

TAB. 6.1 – *Taille des paquets de contrôle RTS, CTS et ACK avec les différentes solutions proposées*

Dans le but d'étudier les solutions proposées dans le cas général, nous avons simulé un réseau de 50 nœuds distribués de manière aléatoire dans une surface de $800 \times 800m^2$ avec 25 connexions de type CBR (Constant Bit Rate).

Dans la figure 6.25, nous traçons le nombre de collisions des paquets de contrôle *RTS*, *CTS* et *ACK* en fonction de la densité du trafic. Nous remarquons que lorsque la

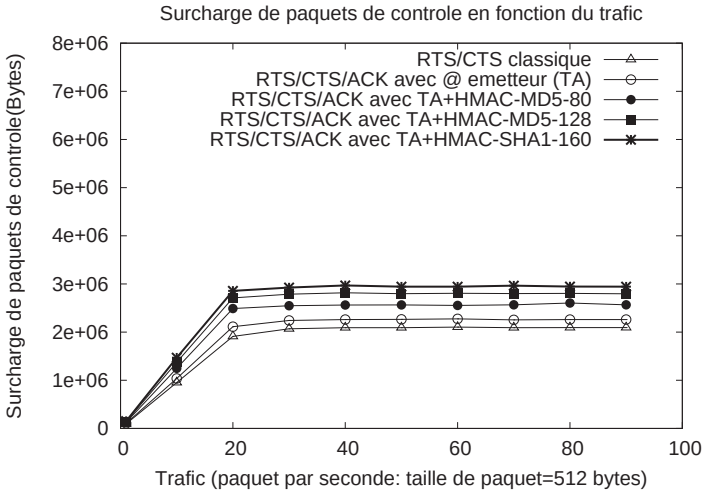


FIG. 6.24 – *Surcharge du réseau liée aux paquets de contrôle en fonction de la densité du trafic*

densité du trafic augmente, le nombre de collisions des paquets de contrôle augmente aussi, mais qu'il se stabilise vers 6500 pour le cas du mécanisme *RTS/CTS* classique. En revanche, le nombre de collisions augmente uniquement avec CTS et ACK dans le cas de la solution simple (sans mécanisme de cryptographie) et seulement avec les RTS et CTS dans le cas de la solution avancée HMAC-SHA1-160. Ces résultats sont comparables au cas de la topologie Grid. Selon ces résultats, le nombre de collisions des paquets de contrôle pour les solutions proposées augmente avec la densité du trafic, ce qui est aussi le cas pour le mécanisme RTS/CTS classique.

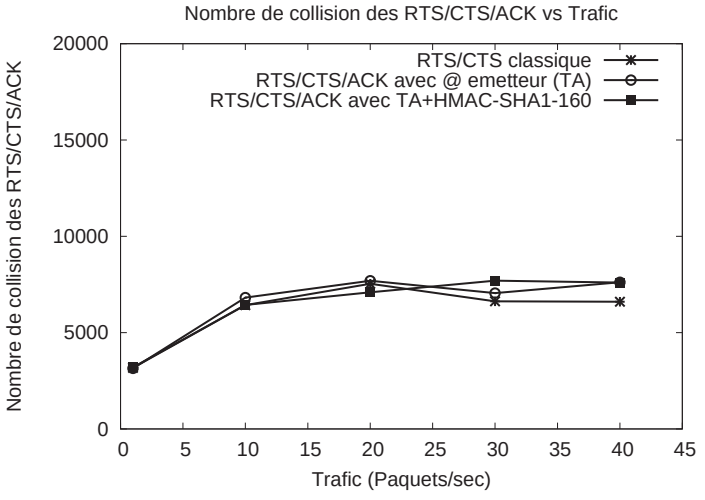


FIG. 6.25 – *Nombre de collisions des paquets de contrôle en fonction de la densité du trafic*

La figure 6.26 montre le débit moyen avec les différentes solutions en fonction de différentes densités de trafic. Nous remarquons une claire différence de niveau du dé-

bit moyen avec les différentes densités de trafic lorsque la taille des paquets de contrôle augmente. Cela est principalement du au nombre de collisions. Par conséquent, la différence entre les solutions proposées et le mécanisme RTS/CTS classique apparaît plus clairement que si on les compare au scénario de la topologie Grid. Nous pouvons en déduire que la densité des nœuds dans le réseau et la densité du trafic ont un impact important sur le débit moyen et sur les paquets de contrôle. Bien que le débit diminue un peu lorsque la taille des paquets de contrôle augmente, il diminue de manière très raisonnable. Avec ces résultats, nous pouvons estimer le coût des solutions proposées.

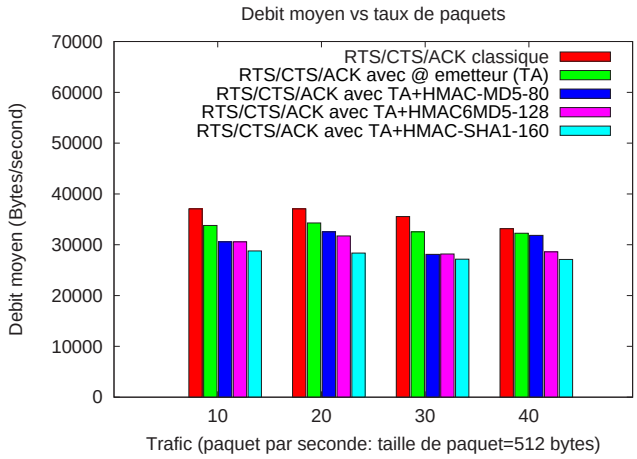


FIG. 6.26 – *Débit moyen du réseau en fonction de la densité du trafic (scénario général)*

6.6.1 Analyse des solutions

A- Perte de débit due au coût de la sécurité

Nous comparons les résultats obtenus dans les figures 6.9 et 6.12 pour montrer l'impact des attaques de type faux *CTS* et de type faux *ACK* sur le réseau. Nous remarquons que la perte de débit dans le cas où 5 nœuds attaquants sont présents dans un réseau de 50 nœuds est d'environ 38,46% pour les deux types d'attaques (le faux *CTS* et le faux *ACK*). De plus, la perte de débit peut atteindre 92,30% avec 25 nœuds attaquants. Cependant, le coût de la sécurité des solutions proposées avec le niveau de sécurité le plus élevé (HMAC-SHA1-160) en terme de débit est de 27,63%, et 10,52% pour le coût de sécurité le plus faible. La figure 6.27 résume les différents coûts de sécurité en terme de pourcentage de perte de débit. Selon ces résultats, nous concluons que le coût des différentes solutions proposées est négligeable par rapport à la dégradation et à la perte de débit dues aux deux types d'attaques.

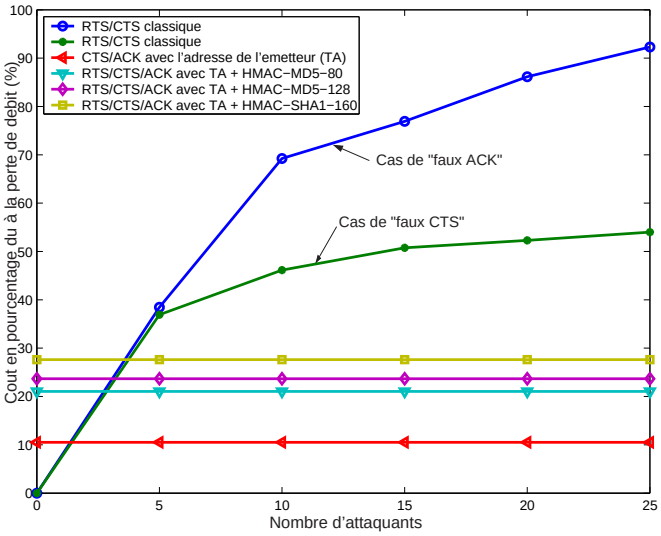


FIG. 6.27 – *Coût des solutions en terme de perte de débit en fonction de différents nombres d'attaquants)*

B- Consommation additionelle d'énergie

Le coût de sécurité des solutions proposées en terme de consommation d'énergie supplémentaire causée par l'interface réseau sans fil (NIC) est évalué dans cette partie. Nous savons que l'autonomie des équipements mobiles dépend de la puissance des batteries et de leur durée d'autonomie. Ainsi, l'énergie est un paramètre très important, ce qui nous amène à évaluer le coût des solutions proposées en terme de consommation d'énergie. Selon l'étude expérimentale sur la consommation d'énergie présentée dans (Feeney et Nilsson, 2001), la consommation d'énergie au niveau des interfaces réseau (NIC) est proportionnelle à la taille des paquets. D'où la formulation de consommation d'énergie suivante :

$$E = m.size + b \tag{6.5}$$

où les paramètres m et b dépendent de l'état de la carte réseau. Nous distinguons 5 états : transmission, réception, écoute, sleep et off. De plus, ils dépendent du mode de transmission/réception, tels que point-à-point ou diffusion. Soient ρ_{Tx}, ρ_{Rx}, ρ_{Ov} les paramètres qui représentent les puissances consommées pendant la transmission en Watts, la réception et l'écoute respectivement. L'énergie consommée pour transmettre le paquet *RTS* est calculée comme suit :

$$E_{Tx}(RTS) = \rho_{Tx}.T_{RTS}$$

où T_{RTS} est le temps nécessaire pour envoyer le paquet *RTS*. Donc, l'énergie supplémentaire consommée pour les solutions proposées peut être calculée comme suit :

$$AE_{Tx}(RTS*) = \rho_{Tx}.(T^*_{RTS} - T_{RTS}) \tag{6.6}$$

où T^*_{RTS} est le temps nécessaire pour envoyer le nouveau paquet *RTS* avec la prise en compte des fonctions de sécurité (l'authentification et le contrôle d'intégrité).

La consommation d'énergie pour chaque solution proposée en comparaison avec l'énergie consommée par le mécanisme RTS/CTS classique est montrée dans la figure 6.28. Nous remarquons que lorsque seule l'adresse source est ajoutée dans les paquets *CTS* et *ACK* (sans mécanisme de cryptographie), la consommation d'énergie est de $0.105mJ$. Cette consommation est similaire à celle de la transmission d'un paquet *RTS*. Cependant, lorsque nous utilisons la solution avec un mécanisme de cryptographie et en particulier HMAC-SHA1-160 (20 bytes) comme fonction de hashage avec l'ajout de 6 bytes dans le paquet *CTS* pour l'adresse source, alors l'énergie consommée est d'environ $0,153mJ$ au lieu de $0,0912mJ$ dans le cas du mécanisme RTS/CTS classique. L'énergie consommée pour transmettre un paquet DATA de 512 bytes est d'environ $1.2mJ$. Nous pouvons donc dire que l'énergie supplémentaire consommée par les nouveaux paquets de contrôle est raisonnable.

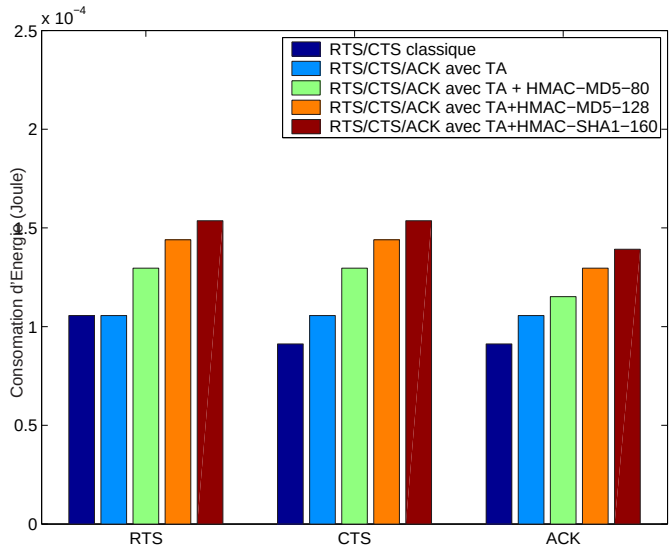


FIG. 6.28 – *Energie consommée par les paquets de contrôle en cas de transmission)*

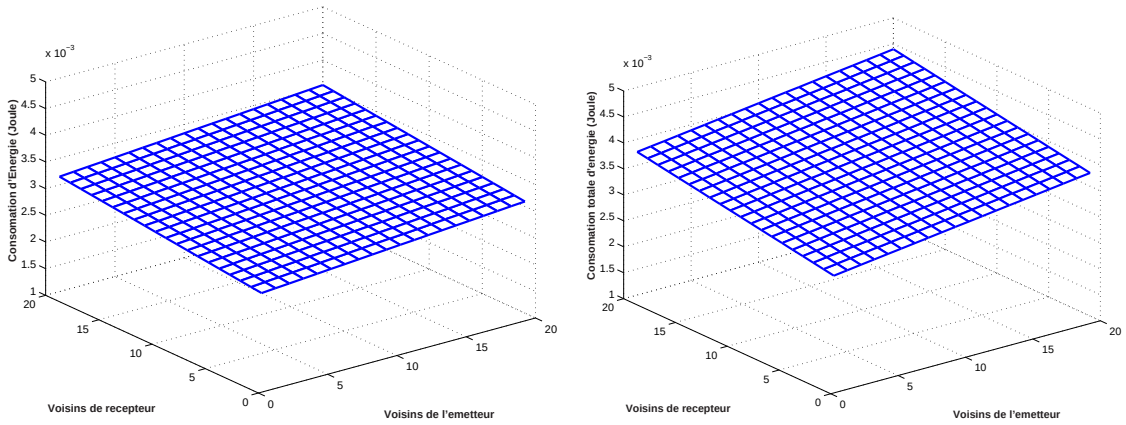
Dans le but d'évaluer le coût de l'énergie totale consommée dans le cas d'une transmission réussie sans retransmission ou collision, nous prenons en compte toutes les transmissions du mécanisme. Nous notons le coût de l'énergie supplémentaire AE, calculé comme suit :

$$\begin{aligned} AE_{Total} = {} & AE_{Tx}(RTS, CTS, DATA, ACK) + \\ & AE_{Rx}(RTS, DATA, CTS, ACK) + \\ & \sum_{l=1}^{c}[AE_{Ov}(RTS) + AE_{Ov}(CTS)] + \\ & \sum_{i=1}^{k}(AE_{Ov}(RTS)) + \sum_{j=1}^{r}(AE_{Ov}(CTS)) \end{aligned}$$

, où AE_{Ov} est l'énergie supplémentaire consommée dans le cas de l'écoute (overhearing). L'écoute est le nombre de voisins communs aux deux nœuds émetteur et ré-

cepteur, et k est le nombre de nœuds voisins de l'émetteur sans les voisins du nœud récepteur. Le paramètre r représente le nombre de voisins du nœud récepteur sans les voisins du nœud émetteur. La prise en compte de l'environnement des deux nœuds émetteur et récepteur nous permet d'évaluer le coût total de l'énergie consommée par les solutions proposées. Par exemple, avec la solution sans mécanisme de cryptographie, le coût est d'environ 8.66%. Cependant, pour la solution avec les mécanismes de cryptographie et avec un haut niveau de sécurité, l'énergie supplémentaire ne dépasse pas 54, 33% de l'énergie nécessaire pour transmettre un paquet avec succès.

Dans les figures 6.29(a) et 6.29(b), nous traçons l'énergie totale consommée pour la transmission d'un seul paquet d'une taille de 512 bytes en fonction des différents voisins des nœuds récepteur et émetteur. Le nombre de nœuds voisins communs entre le récepteur et l'émetteur est fixé à 5. La figure 6.29(a) montre le cas du mécanisme RTS/CTS classique. Nous notons que l'augmentation du nombre de nœuds voisins des nœuds émetteur et récepteur est proportionnelle à l'augmentation de la consommation d'énergie. La valeur maximum de l'énergie totale consommée est d'environ $3.5mJ$ avec 20 nœuds voisins chez l'émetteur et 20 nœuds voisins chez le récepteur. Cependant, dans les mêmes conditions avec la solution proposée utilisant le RTS/CTS/ACK avec $HMAC - SHA1$, la consommation d'énergie totale ne dépasse pas $4.5mJ$.



(a) RTS/CTS classique

(b) RTS/CTS/ACK avec TA+HMAC-SHA1

FIG. 6.29 – *Energie totale consommée en fonction de différents nombres de voisins*

Un autre type de consommation d'énergie est l'énergie consommée avec les algorithmes de cryptographie tels que MD5, SHA1, HMAC et EHMAC. L'énergie nécessaire pour générer et vérifier l'empreinte numérique avec HMAC est estimée à environ $1\mu J/byte$ par (N. R. Potlapally, 2003). Cependant, la consommation d'énergie nécessaire pour générer une empreinte numérique avec la fonction HMAC améliorée (Enhanced HMAC (EHMAC)), comme par exemple, l'énergie nécessaire pour générer EHMAC-MD5, est estimée à environ $0.60\mu J/Bytes$. Ainsi, lorsque nous comparons la consommation d'énergie par l'interface réseau (carte réseau) et l'énergie consommée par les algorithmes de cryptographie utilisés, nous pouvons dire que la consommation d'éner-

gie pour générer l'empreinte numérique avec EHMAC n'est pas significative.

6.7 Analyse de sécurité

Actuellement, aucun système de détection d'intrusions (IDS) n'est capable de détecter les attaques avec les faux *CTS* et la fausse validation basée sur les faux *ACK*, à cause de la vulnérabilité des formats de ces paquets. L'attaquant n'a pas besoin de "spoofer" (changer d'identité) l'adresse du nœud source, dans le but d'échapper à la détection et l'identification. Non seulement le nœud attaquant peut échapper à l'identification, mais il peut aussi créer une situation de suspicion : chaque nœud dans le rayon de transmission de l'attaquant suspecte les autres nœuds dans son rayon de transmission. Nous pouvons comparer cette situation au jeu « cache-cache » : l'attaquant utilise le faux *CTS* et défit n'importe quel IDS de le détecter.

Dans les solutions proposées sans l'utilisation des mécanismes de cryptographie (uniquement l'ajout de l'adresse de l'émetteur dans les paquets *CTS* et *ACK*), l'authentification et le contrôle d'intégrité ne sont pas assurés. Cela veut dire que la solution peut être compromise. Cependant, avec le niveau de sécurité le plus faible, cette solution est bien adaptée. La solution avec les mécanismes de cryptographie dont le niveau de sécurité est le plus élevé assure l'authentification et le contrôle d'intégrité des informations incluses dans les paquets de contrôle. Toutefois, cette solution dépend des clés de cryptographie pré-partagées entre les nœuds, ainsi que de la clé de groupe. Cette dernière dépend du modèle de confiance adopté pour la sécurité. Par exemple, lorsqu'un nœud inconnu veut rejoindre le réseau, la clé de groupe est attribuée avec le niveau de sécurité le plus faible. Alors, tous les nœuds avec le niveau de sécurité le plus élevé peuvent obtenir la clé de groupe avec le niveau de sécurité le plus faible. Cependant, pour des besoins de sécurité, la mise à jour de la clé de groupe nécessite le niveau de sécurité le plus élevé. Deux solutions sont possibles et peuvent être coûteuses : la première constitue l'utilisation de la cryptographie à clé publique avec la fonction MAC (Messsage Authentication Code). Ainsi, l'application des algorithmes de chiffrement et de déchiffrement est nécessaire. L'utilisation de EHMAC(M, K_G) est donc substituée par $E_{K^-}(H(M))$, où K^- est la clé privée du nœud émetteur, E l'algorithme de chiffrement à clé publique (ex. RSA) et H la fonction de hashage (ex. MD5, SHA1). Le nœud récepteur du paquet de contrôle *RTS* ou *CTS*, doit utiliser la clé publique du nœud émetteur pour vérifier la validité de ce paquet. La deuxième solution possible est de générer pour chaque nœud voisin du nœud émetteur une empreinte numérique de type EHMAC avec une clé déjà pré-partagée. Le problème de cette proposition concerne la taille des paquets *RTS* et *CTS* qui va augmenter proportionnellement au nombre de voisins du nœud émetteur. De plus, l'approche inter-couches doit être adoptée dans le but d'implémenter cette solution. Cependant, les deux solutions peuvent être plus résistantes en terme de sécurité que la solution basée sur la clé de groupe, mais elles ne sont pas recommandées si nous prenons en compte les contraintes de la qualité de service.

6.8 Conclusion

Dans ce chapitre, nous avons montré de nouvelles vulnérabilités cachées dans la technologie IEEE 802.11 et les attaques susceptibles d'exploiter ces faiblesses. Nous avons présenté l'analyse des vulnérabilités liées au format des paquets de contrôle CTS et ACK, et leurs attaques respectives sont appelées le faux CTS et la fausse validation du paquet DATA basée sur le faux ACK. Nous avons illustré l'impact négatif de ces attaques via des simulations et des expérimentations « testbed », après avoir réellement implémenté ces attaques. Un autre impact négatif sur les mécanismes de surveillance est étudié. Un attaquant peut facilement réduire la réputation ou le niveau de confiance d'un nœud qui se comporte bien. Ainsi, il perturbe tout le modèle de confiance. De plus, l'opération de routage peut être affectée par ces attaques, et en particulier par l'attaque de type fausse validation basée sur le faux ACK. Ces attaques peuvent créer des situations de suspicion : chaque nœud situé dans le rayon de transmission de l'attaquant va suspecter ses nœuds voisins pour déterminer l'origine de l'attaque. Pour prévenir ces attaques, nous avons proposé des solutions avec et sans mécanisme de cryptographie. Les solutions qui offrent la possibilité d'authentifier et de contrôler l'intégrité des données des paquets de contrôle doivent utiliser les mécanismes de cryptographie, tels que HMAC et particulièrement le HMAC amélioré (Enhanced HMAC). Après avoir implémenté les solutions proposées, les résultats de simulation ont montré les performances de ces solutions ainsi que leur coût de sécurité du point de vue de la qualité de service. Pour conclure ces résultats, l'impact négatif des attaques est plus significatif que le coût de sécurité de ces solutions et le compromis entre le coût de la sécurité et le niveau de sécurité doit être pris en compte. Enfin, nous avons présenté l'analyse de sécurité de ces solutions.

Chapitre 7

Conclusion et perspectives

Notre thèse a pour objectif d'apporter des solutions aux problèmes liés à la sécurité dans les réseaux mobiles Ad hoc. Les caractéristiques de ces réseaux empêchent l'utilisation des solutions de sécurité déjà existantes. Pour cela, nous avons étudié les solutions existantes et avons montré les limites de certaines solutions et bien sûr nous avons proposé des solutions plus adaptées à l'environnement des réseaux mobiles Ad hoc.

Dans un premier temps, nous nous sommes intéressés au problème de distribution des clés publiques dans les réseaux mobiles Ad hoc. 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). Dans cette approche, le modèle de confiance est évalué par le processus de surveillance (monitoring). En outre, nous avons proposé un nouveau mécanisme, la $DDMZ$, pour protéger les nœuds CA contre les attaques de type déni de service. Ce mécanisme augmente la robustesse de la sécurité dans les groupes. De plus, nous avons proposé un modèle de connectivité de confiance pour étudier la robustesse de la sécurité au sein des groupes. Une étude comparative est présentée pour montrer la valeur ajoutée de notre architecture.

Ensuite, nous avons étendu notre architecture en introduisant le concept d'anonymat dans le mécanisme de protection du nœud CA appelé zone dynamique démilitarisée ($DDMZ$). Cette zone devient une zone anonyme, car elle sera formée par des nœuds dont l'identité est cachée aux autres nœuds. De plus, nous nous sommes inspirés des mécanismes de défense militaire tels que les techniques de camouflage et les mécanismes de changement d'identité. Nous avons proposé un protocole appelé (ICCP) pour réaliser ces mécanismes avec l'utilisation de la cryptographie basée sur la fonction bilinéaire. Ce protocole permet à tout nœud d'authentifier d'autres nœuds de façon anonyme. L'ICCP est conçu pour résister à diverses attaques telles que le DoS ou l'attaque par capture.

Un autre point de cette thèse concerne l'étude du mécanisme de surveillance pour entretenir le modèle de confiance. Le modèle de confiance est le coeur de toutes les so-

lutions de sécurité. Nous avons montré la limite des modèles de surveillance existants tels que Watchdog (S. Marti et Baker, 2000). Pour remédier à ces limites, nous avons proposé une nouvelle approche inter-couches fondée sur les paramètres des couches physique, MAC et de routage pour la mise en place d'un mécanisme de contrôle et de surveillance efficace. De plus, nous avons présenté un nouveau modèle analytique pour illustrer l'effet des différents paramètres sur ces différentes couches. Cette approche améliore l'évaluation de la coopération des nœuds et réduit le taux de fausses alarmes (faux positifs). En outre, avec les résultats de simulations, nous avons montré que notre mécanisme inter-couches a un taux de fausses alarmes plus faible que le mécanisme classique appelé Watchdog avec différents paramètres du réseau, tels que la densité des nœuds, la vitesse de déplacement des nœuds et les différentes charges du trafic réseau.

Un autre volet de la thèse traite les attaques de type inter-couches. Nous nous sommes focalisés sur la couche MAC (Medium Access Control), en particulier sur la technologie IEEE 802.11. Nous avons montré les vulnérabilités cachées basées sur les paquets de contrôle *CTS* (Clear to Send) et *ACK*. A travers ces vulnérabilités, nous avons découvert de nouvelles attaques intelligentes qui n'ont jamais été traitées auparavant. Un nœud malveillant peut exploiter ces vulnérabilités au niveau du protocole de la couche MAC dans le but de perturber les mécanismes de surveillance et de routage. De plus, nous avons décrit comment ces vulnérabilités peuvent être exploitées et comment des attaques peuvent être implémentées par un attaquant. Nous avons étudié l'impact de ces attaques sur le réseau avec une étude analytique, des simulations ainsi qu'une étude expérimentale (testbed). Pour prévenir ces attaques, des solutions basées sur l'authentification des paquets de contrôle sont présentées. L'évaluation et l'analyse des solutions proposées sont présentées et soutenues par une étude analytique et par les résultats de simulations. De plus, le coût des solutions proposées est étudié. En comparaison avec l'impact négatif des attaques, le coût de sécurité n'est pas significatif.

Toutefois, dans la continuité du travail présenté, nous pouvons étendre l'analyse de notre architecture à différents modèles de mobilité et évaluer la résistance de la $DDMZ$ face aux différents types d'attaques comme le déni de service (DoS) tel que le brouillage. De plus, nous allons étendre le mécanisme $DDMZ$ pour assurer une couverture de toute la région du nœud CA, dans le but de détecter l'origine de l'attaque et de localiser l'attaquant. Pour cela, nous pouvons équiper des nœuds de confiance d'antennes directionnelles. En outre, pour optimiser la consommation d'énergie, nous pouvons sélectionner les nœuds RA dont le rôle consiste à protéger le CA de manière progressive en fonction de la menace dans le groupe. Par conséquent, un algorithme d'élection des nœuds RA est nécessaire. Nous envisageons d'étudier et de formuler l'analyse de risque dans les groupes.

Par ailleurs, nous avons l'intention de mettre en place et de simuler le mécanisme d'authentification anonyme et le protocole de camouflage et de changement d'identité (ICCP).

Enfin, pour les solutions basées sur la cryptographie pour contrer les attaques fondées sur les paquets de contrôle, une étude de compromis entre le coût de la sécurité

et le niveau de sécurité doit être menée. Pour cela, une plate-forme des attaques avec l'implémentation des solutions proposées peut être développée. Toutes les solutions proposées durant cette thèse peuvent être étendues et adaptées aux réseaux de capteurs.

Liste des Acronymes

ANODR - Anonymous On-Demand Routing
ANR - Agence Nationale de la Recherche
AODV - Ad hoc On Demand Distance Vector routing protocol
ARAN - Authenticated Routing protocol for Ad hoc Networks
BEB - Binary Exponential Backoff
CBR - Constant Bit Rate
CA - Certification Authority
CBRP - Cluster Based Routing Protocol
CDMA - Code Division Multiple Access
CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance
CTS - Clear To Send
CW - Contention Window
DCF - Distributed Coordination Function
DDMZ - Dynamic Demilitarized Zone
DIFS - Distributed Inter Frame Space
DSDV - Distance Source Distance Vector routing protocol
DSR - Distance Source Routing
GW - Gateway Node
HMAC - Hashed Message Authentication Code
ICCP - Identity Change and Camouflage Protocol
ICMP - Internet Control Message Protocol
IDS - Intrusion Detection System
IEEE - Institute of Electrical and Electronics Engineers
IETF - Internet Engineering Task Force
IP - Internet Protocol
LAN - Local Area Network
MAC - Medium Access Control
MANET - Mobile Ad hoc Network
MN - Member Node
MOCA - MObile Certificate Authority
OLSR - Optimized Link State Routing
OSI - Open Systems Interconnection
PAN - Personal Area Network
PCF - Point Coordination Function

PKI - Public Key Infrastructure
PRB - Predictable Random Backoff
QoS - Quality of Service
RA - Registration Authority
RFC - Request For Comments
RTS - Request To Send
SDVS - Simple Designed Verifier Signature
SNR - Signal-to-Noise Ratio
TCP - Transmission Control Protocol
TTL - Time To Live
UDP - User Datagram Protocol
VCI - Virtual Circuit Identifier
VN - Visitor Node
VPN - Virtual Private Network
ZRP - Zone Routing Protocol

Liste des illustrations

Liste des tableaux

Publications personnelles

Revues internationales avec comité de lecture

1. **Abderrezak Rachedi** and Abderrahim Benslimane, *"Impacts and Solutions of Control Packets Vulnerabilities with IEEE 802.11 MAC"*, Journal of Wireless Communications and Mobile Computing, John Wiley InterScience, 2008.
2. **Abderrezak Rachedi** and Abderrahim Benslimane, *"Toward a Cross-layer Monitoring Process for Mobile Ad Hoc Networks"*, Journal of Security and Communication Network, John Wiley InterScience, 2008.

Conférences internationales avec comité de lecture

1. **Abderrezak Rachedi** and Abderrahim Benslimane, *"Security and Pseudo-Anonymity with a Cluster-based approach for MANET"*, In proceedings of the 51th annual IEEE Global Telecommunications Conference (IEEE GLOBECOM'2008), New Orleans, LA, USA, 30 Nov.-3 Dec. 2008. (Accepté)
2. **Abderrezak Rachedi**, Abderrahim Benslimane, Hadi Otrok, Noaaman Mohammed and Mourad Debbabi, *"A Mechanism Design-Based Secure Architecture for Mobile Ad Hoc Networks"*, In proceedings of the 4th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (IEEE WiMob'2008), Avignon, France, 12-14 Oct. 2008.
3. **Abderrezak Rachedi** and Abderrahim Benslimane, *"Smart Attacks based on Control Packets Vulnerabilities with IEEE 802.11 MAC"*, In proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC'2008), pp. 588-593, Crete Island, Greece, August 6-8, 2008. (IEEE Press)
4. Abderrahim Benslimane and **Abderrezak Rachedi**, *"Relative Fairness and Optimized Throughput for Mobile Ad hoc Networks"*, The IEEE International Conference on Communications (ICC'2008), pp. 2233-2237, Beijing, China, 19-23 May, 2008. (IEEE Press)
5. **Abderrezak Rachedi** and Abderrahim Benslimane, *"Cross-Layer approach to improve the monitoring process for Mobile Ad Hoc Networks based on IEEE 802.11"*, 50th Anniversary of the annual IEEE Global Telecommunications Conference (IEEE

GLOBECOM'2007), pp. 1086-1091, Washington, DC, USA, 26-30 November 2007. (IEEE Press)

6. **Abderrezak Rachedi**, Abderrahim Benslimane, Lei Guang and Chadi Assi, *"A Confident Community to Secure Mobile Ad-Hoc Networks"*, In proceeding of the IEEE International Conference on Communications (ICC'2007), pp. 1254-1259, Glasgow, Scotland, UK, 24-28 June 2007. (IEEE Press)
7. **Abderrezak Rachedi** and Abderrahim Benslimane, *"A Secure Architecture for Mobile Ad Hoc Networks"*, In proceeding of the 2nd International Conference on Mobile Ad-Hoc and Sensor Networks (MSN2006),Lecture Notes in Computer Science 4325, pp. 424-435, Hong Kong, China, December, 2006. (IEEE Press)
8. **Abderrezak Rachedi** and Abderrahim Benslimane, *"Trust and Mobility-based Clustering Algorithm for Secure Mobile Ad Hoc Networks"*, In proceeding of the International Conference on Systems and Networks Communications, pp. 72, Tahiti, Frunch Polynesia, October 2006. (IEEE Press)

Conférences nationales avec comité de lecture

1. **Abderrezak Rachedi** et Abderrahim Benslimane, *"Gestion de confiance et résistance aux attaques dans les réseaux Ad hoc mobiles"*, 8ème Colloque Francophone de Gestion de Réseaux et de Services, "L'adaptation dynamique des réseaux et des services" (GRES2007). Hammamet, Tunisie du 6 au 9 Novembre 2007.
2. **Abderrezak Rachedi** et Abderrahim Benslimane, *"Architecture Hiérarchique Distribuée pour sécuriser les réseaux Ad hoc Mobiles"*, 8ème Journées Doctorales en Informatique et Réseaux (JDIR'2007), 17-19 Janvier, Marne la Vallée (Paris-Est), 2007.
3. Abdelkader Belkhir, Med Djamel Naci, **Abderrezak Rachedi**, *"Contribution à la sécurité du PDA : IDS Embarqué EIDS"*, SAR'04 (rencontre francophone sur Sécurité et Architecture Réseaux), 3ème Conférence sur la Sécurité et Architectures Réseaux La Londe, France, 2004.

Bibliographie

(A.-A. Cardenas, 2004) G. P. J.-S. B. A.-A. Cardenas, N. Benammar, 2004. Cross-layered security analysis of wireless ad-hoc networks. Dans les actes de *Army Science Conference*.

(A.-A. Cardenas et Baras, 2004) S. R. A.-A. Cardenas et J. S. Baras, 2004. Detection and prevention of mac layer misbehavior in ad hoc networks. Dans les actes de *ACM workshop on Security of ad hoc and sensor networks*, 17–22.

(A. Patwardhan et Iorga, 2005) A. J. A. K. A. Patwardhan, J. Parker et M. Iorga, 2005. Secure routing and intrusion detection in ad hoc networks. Dans les actes de *IEEE International Conference on Pervasive Computing and Communications*.

(A. Rahman, 2006) P. G. A. Rahman, 2006. Hidden Problems with the Hidden Node Problem. Dans les actes de *23rd Biennial Symposium on Communications*, 270–273.

(Afifi, 2007) K. M. H. Afifi, 2007. An identity-based key management framework for personal networks. Dans les actes de *IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS'07)*, 537–543.

(Avoine et Vaudenay, 2004) G. Avoine et S. Vaudenay, 2004. Optimal Fair Exchange with Guardian Angels. Dans les actes de *Lecture Notes in Computer Science, Information Security Applications*, 261–283.

(B. Awerbuch et Rubens, 2002) C. N.-R. B. Awerbuch, D. Holmer et H. Rubens, 2002. An on-demand secure protocol resilient to byzantine failures. Dans les actes de *ACM Workshop on Wireless Security*.

(B. Guha, 1997) B. M. B. Guha, 1997. Network security via reverse engineering of TCP code : vulnerabilityanalysis and proposed solutions. *IEEE Network 11-4*, 40–48.

(Baras et Radosavac, 2004) J. S. Baras et S. Radosavac, 2004. Attacks and defenses utilizing cross-layer interactions in cross-layer interactions in manet. Dans les actes de *Workshop on Cross-Layer Issues in the Design of Tactical Mobile Ad Hoc Wireless Networks : Integration of Communication and Networking Functions to Support Optimal Information Management*.

(Basu et al., 2001) P. Basu, N. Khan, et T. Little, 2001. A mobility based metric for clustering in mobile ad hoc networks. Dans les actes de *Distributed Computing Systems Workshop*, 43–51.

(Bechler et al., 2004) M. Bechler, H.-J. Hof, D. Kraft, F. Pahlke, et L. Wolf, 2004. A Cluster-Based Security Architecture for Ad Hoc Networks. Dans les actes de *IEEE INFOCOM'2004*, 2393–2403.

(Bianchi, 2000) G. Bianchi, 2000. Performance Analysis of the IEEE 802.11 Distributed Coordination Function. *IEEE Journal of Selected Area in Telecommunication Wireless series 18-3*, 535–547.

(Boudec et Vojnovic, 2005) J.-Y. L. Boudec et M. Vojnovic, 2005. Perfect Simulation and Stationarity of a Class of Mobility Models. Dans les actes de *IEEE Infocom 2005, Miami, FL (Infocom 2005 Best Paper Award)*.

(Buchegger et Boudec, 2002a) S. Buchegger et J. L. Boudec, 2002a. Nodes bearing grudges : Towards routing security, fairness, and robustness in mobile ad hoc networks. Dans les actes de *Euromicro Workshop on Parallel, Distributed and Network-based*, 2234–2240.

(Buchegger et Boudec, 2002b) S. Buchegger et J.-Y. L. Boudec, 2002b. Performance Analysis of the CONFIDANT Protocol : Cooperation Of Nodes- Fairness In Dynamic Ad-hoc NeTworks. Dans les actes de *IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH*.

(Budakoglu et Gulliver, 2004) C. Budakoglu et T. A. Gulliver, 2004. Hierarchical Key Management for Mobile Ad-hoc Networks. Dans les actes de *IEEE Vehicular Technology Conference (VTC'2004)*, Volume 4, 2735–2738.

(Buttyan et Hubaux, 2002) L. Buttyan et J.-P. Hubaux, 2002. Report on a working session on security in wireless ad hoc networks. Dans les actes de *ACM Mobile Computing and Communications Review (MC2R)*.

(Buttyan et Hubaux, 2003) L. Buttyan et J.-P. Hubaux, 2003. Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Networks and Applications 8-5*, 579–592.

(C. Castelluccia et Yi, 2007) N. S. C. Castelluccia et J. H. Yi, 2007. Robust self-keying mobile ad hoc networks. *International Journal of Computer and Telecommunications Networking 51*, 1169–1182.

(C. Satizabal, 2007) J. F. J. P. C. Satizabal, J. Hernandez-Serrano, 2007. Building a Virtual Hierarchy to Simplify Certification Path Discovery in Mobile Ad-hoc Networks. *Computer Communication 30*, 1498–1512.

(Capkun et al., 2002) S. Capkun, L. Buttyan, et J. Hubaux, 2002. Self-Organized Public-Key Management for Mobile Ad Hoc Networks. Dans les actes de *ACM International Workshop on Wireless Security, WiSe*, 52–64.

(Charles E. Perkins et Chakeres, 2003) E. M. B.-R. Charles E. Perkins et I. Chakeres, 2003. Ad Hoc On Demand Distance Vector (AODV) Routing. Dans les actes de *IETF Internet draft, draft-perkins-manet-aodvbis-00.txt (Work in Progress)*.

(Chiang et al., 1997) C. Chiang, H. Wu, W. Liu, et M. Gerla, 1997. Routing in Clustered Multihop Mobile Wireless Networks with Fading Channel. Dans les actes de *IEEE SICON'97*, 197–211.

(Communications, 2007) A. Communications, 2007. Atheros Chipset. *http ://www.atheros.com/*.

(D. Malone, 2006) D. L. D. Malone, K. Duffy, 2006. Modeling the 802.11 Distributed Coordination Function in Non-saturated Heterogeneous Conditions. Dans les actes de *IEEE/ACM Transactions on Networking*.

(David B. Johnson et Broch, 2001) D. A. M. David B. Johnson et J. Broch, 2001. The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks. Dans les actes de *Ad Hoc Networking, edited by Charles E. Perkins, Chapter 5, Addison-Wesley*, 139–172.

(F. Daneshgaran, 2008) F. M.-M. M. F. Daneshgaran, M. Laddomada, 2008. Unsaturated Throughput Analysis of IEEE 802.11 in Presence of Non Ideal Transmission Channel and Capture Effects Authors. Dans les actes de *IEEE Transactions on Wireless Communication*.

(Feeney et Nilsson, 2001) L. M. Feeney et M. Nilsson, 2001. Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment. Dans les actes de *IEEE INFOCOM'01*, 1548–1557.

(Gerla et Tsai, 1995) M. Gerla et J. T.-C. Tsai, 1995. SMulticluster, Mobile Multimedia Radio Networks. *Wireless Networks 1*(3), 255–265.

(Guang et al., 2008) L. Guang, C. Assi, et A. Benslimane, 2008. On MAC Layer Misbehavior in Wireless Networks : Challenges and Solutions. Dans les actes de *IEEE Wireless Communication Magazine*.

(Hu et al., 2002) Y. Hu, A. Perrig, et D. B. Johnson, 2002. A Secure On-Demand Routing Protocol for Ad Hoc Network. Dans les actes de *Eighth Annual International Conference on Mobile Computing and Networking (MobiCom'02)*.

(Huang et Lee, 2003) Y. Huang et W. Lee, 2003. A Cooperative Intrusion Detection System for Ad Hoc Networks. Dans les actes de *ACM workshop on Security of ah hoc and sensor networks*, 135–147.

(Hung et Marsic, 2007) F. Y. Hung et I. Marsic, 2007. Analysis of Non-Saturation and Saturation Performance of IEEE 802.11 DCF in the Presence of Hidden Stations. Dans les actes de *IEEE 66th Vehicular Technology Conference (VTC-Fall-2007)*.

(IEEE802-11, 1999) IEEE802-11, 1999. Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) specification. Dans les actes de *ANSI/IEEE std. 802.11*.

(J. Kong et Gerla, 2007) X. H. J. Kong et M. Gerla, 2007. An Identity-Free and On-Demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing 6*, 888–902.

(K. El-Khatib et Yee, 2003) R. S. K. El-Khatib, L. Korba et G. Yee, 2003. Secure Dynamic Distributed Routing Algorithm for Ad hoc wireless Networks. Dans les actes de *International Conference on Parallel Workshops (ICPPW'03)*, 359–366.

(K. Xu et Bae, 2003) M. G. K. Xu et S. Bae, 2003. Effectiveness of RTS/CTS Handshake in IEEE 802.11 based Ad Hoc Networks. *Ad Hoc Network Journal 1-1*, 107–123.

(Karn, 1990) P. Karn, 1990. MACA- A new Channel Access Method for Packet Radio. Dans les actes de *ARRL/CRRL Amature Radio 9th Computer Networking Conference*, 134–140.

(Kong et al., 2001) J. Kong, P. Zerfos, H. Luo, et L. Z. S. Lu, 2001. Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks. Dans les actes de *International Conference in Network Protocols (ICNP'01)*.

(Kyasanur et Vaidya, 2005) P. Kyasanur et N. Vaidya, 2005. Selfish MAC layer misbehavior in wireless networks. *IEEE Transactions on Mobile Computing 4-5*, 502–516.

(L. Guang et Benslimane, 2006) C. A. L. Guang et A. Benslimane, 2006. Interlayer attacks in mobile ad hoc networks. Dans les actes de *International Conference on Mobile Ad-hoc and Sensor Networks (MSN 2006)*, 436–448.

(L. Zhe et Ye, 2005) L. D. L. Zhe, L. Jun et L. Ye, 2005. A security enhanced aodv routing protocol. Dans les actes de *Mobile Ad-hoc and Sensor Networks (MSN2005)*, 298–307.

(Lazos et Poovendran, 2004) L. Lazos et R. Poovendran, 2004. Cross-layer design for energy-efficient secure multicast in ad hoc networks. Dans les actes de *IEEE ICC'2004 Communications in Ad Hoc Networks*, 3633–3639.

(Leffler, 2007) S. Leffler, 2007. MADWiFi project. *http ://madwifi.org/*.

(Levente Buttyán, 2001) J.-P. H. Levente Buttyán, 2001. Rational Exchange - A Formal Model Based on Game Theory. Dans les actes de *2nd International Workshop on Electronic Commerce (WELCOM)*, 16– 17.

(License, 2008) G. G. P. License, 2008. Wireshark : Capture packet analyser. *http ://www.wireshark.org/*.

(M. Al-Shurman, 2004) S. P. M. Al-Shurman, S. M. Yoo, 2004. Black hole attack in mobile Ad Hoc networks. Dans les actes de *42nd annual Southeast regional conference*, 96–97.

(M. Cagalj et Hubaux, 2003) I. A. M. Cagalj, S. Ganeriwal et J.-P. Hubaux, 2003. On cheating in csma/ca ad hoc networks. Dans les actes de *EPFL, Tech. Rep.*

(M. Maroti, 2005) S. D. B. K. A. N. A. L. G. B. K. M. M. Maroti, P. Volgyesi, 2005. Radio interferometric geolocation. Dans les actes de *International conference on Embedded net-worked sensor systems*, 1–12.

(M. Pirretti et Brooks, 2005) V. N. P. M. M. K. M. Pirretti, S. Zhu et R. Brooks, 2005. The Sleep Deprivation Attack in Sensor Networks : Analysis and Methods of Defense. *International Journal of Distributed Sensor Networks 2-3*, 267–287.

(Marti et Garcia-Molina, 2005) S. Marti et H. Garcia-Molina, 2005. Taxonomy of trust : Categorizing p2p reputation system. Dans les actes de *COMNET Special Issue on Trust and Reputation in Peer-to-Peer Systems*.

(Masmoudi, 2008) K. Masmoudi, 2008. Trust management in personal networks. Dans les actes de *Ph.D. Dissertation. Joint Diploma Telecom Sud Paris & University of Paris 6*.

(M.G. Reed, 1998) D. G. M.G. Reed, P.F. Syverson, 1998. Anonymous connections and onion routing. *IEEE Journal on Selected Areas in Communications 16*, 482–494.

(Michiardi et Molva, 2002) P. Michiardi et R. Molva, 2002. Core : A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. 107–121.

(N. R. Potlapally, 2003) A. R. N. K. J. N. R. Potlapally, S. Ravi, 2003. Analyzing the energy consumption of security protocols. Dans les actes de *International symposium on Low power electronics and design (ISLPED03) :ACM Press*, 30–35.

(ns 2, 1999) ns 2, 1999. UC Berkeley and USC ISI : The network simulator ns-2. Part of the VINT project. *Available from http ://www.isi.edu/nsnam/ns*.

(Patel, 2002) S. Patel, 2002. An Efficient MAC for short Messages. Dans les actes de *Selected Areas in Cryptography (SAC2002)*, 353–368.

(Perrig et al., 2002) A. Perrig, R. Canetti, J. Tygar, et D. Song, 2002. The TESLA Broadcast Authentication Protocol. *Cryptobytes journal 5*, 2–13.

(PUB, 2001) F. PUB, 2001. HMAC : The Keyed Hash Message Authentication Code. Dans les actes de *Federal Information Processing Standard (FIPS) Publication, National Institute of Standards and Technology, US Departement of Commerce*.

(R. E. Kodikara et Ahlund, 2006) A. Z. R. E. Kodikara et C. Ahlund, 2006. ConEx : Context Exchange in MANETs for Real time multimedia. Dans les actes de *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICN/ICONS/MCL'06)*, 70.

(R. P. Sam et Reddy, 2007) B. S. C. R. P. Sam et P. C. Reddy, 2007. Denial of Service attack through compromised nodes in Mobile Ad-Hoc Networks. *Academic Open Internet Journal 21*.

(Rachedi et Benslimane, 2006) A. Rachedi et A. Benslimane, 2006. A secure Architecture for Mobile Ad Hoc Networks. Dans les actes de *International Conference on Mobile Ad-Hoc and Sensor Networks (MSN'06), Lecture Notes in Computer Science, Hong Kong, China*, Volume 4325, 424–435.

(Rachedi et Benslimane, 2007) A. Rachedi et A. Benslimane, 2007. Cross-Layer approach to improve the monitoring process for Mobile Ad Hoc Networks based on IEEE 802.11. Dans les actes de *IEEE Global Telecommunications Conference (IEEE GLOBECOM 2007)*, 1086–1091.

(Rachedi et Benslimane, 2008a) A. Rachedi et A. Benslimane, 2008a. Impacts and Solutions of Control Packets Vulnerabilities with IEEE 802.11 MAC. *Journal of Wireless Communications and Mobile Computing, John Wiley InterScience.*.

(Rachedi et Benslimane, 2008b) A. Rachedi et A. Benslimane, 2008b. Smart Attacks based on Control Packets Vulnerabilities with IEEE 802.11 MAC. Dans les actes de *IEEE International Wireless Communications and Mobile Computing Conference (IWCMC 2008)*.

(Rachedi et Benslimane, 2008c) A. Rachedi et A. Benslimane, 2008c. Toward a Cross-layer Monitoring Process for Mobile Ad Hoc Networks. *Journal of Security and Communication Network, John Wiley InterScience*.

(Rachedi et al., 2007) A. Rachedi, A. Benslimane, L. Guang, et C. Assi, 2007. A Confident Community to Secure Mobile Ad-Hoc Networks. Dans les actes de *IEEE International Conference on Communications (ICC 2007), Glasgow, Scotland, UK*, Volume 24-28, 1254 – 1259.

(Radosavac et al., 2004) S. Radosavac, N. Benammar, et J. S. Baras, 2004. Cross-layer attacks in wireless ad hoc networks. Dans les actes de *Conference on Information Sciences and Systems*.

(Ray et al., 2003) S. Ray, J. Carruthers, et D. Starobinski, 2003. RTS/CTS-induced congestion in ad hoc wireless LANs. Dans les actes de *IEEE WCNC 2003*.

(Rebahi et al., 2005) Y. Rebahi, V. E. Mujica-V, et D. Sisalem, 2005. A Reputation-Based Trust Mechanism for Ad hoc Networks. Dans les actes de *Symposium on Communications (ISCC'05)*, 37–42.

(RFC2401, 1998) RFC2401, 1998. Security Architecture for the Internet Protocol. Dans les actes de *Request For Comment, RFC2401*.

(RFC2406, 1998) RFC2406, 1998. IP Encapsulating Security Payload (ESP). Dans les actes de *Request For Comment, RFC2406*.

(S. Buchegger, 2002) J. Y. L. B. S. Buchegger, 2002. Cooperative Routing in Mobile Adhoc Networks : Current Efforts Against Malice and Selfishness.

(S. Chokhani, 2003) R. S. C. M. S. Chokhani, W. Ford, 2003. Internet X.509 public key infrastructure certificate policy and certification practices framework. Dans les actes de *Internet Request for Comments (RFC3647)*.

(S. Marti et Baker, 2000) K. L. S. Marti, T.J. Giuli et M. Baker, 2000. Mitigating Routing Misebehavior in Mobile Ad Hoc Networks. Dans les actes de *ACM/IEEE International Conference on Mobile Computing and Networking*, 255–265.

(S. Ray, 2007) D. S. S. Ray, 2007. On False Blocking in RTS/CTS-Based Multihop Wireless Networks. *IEEE Transactions Vehicular Technology journal 56*, 849–862.

(S. Yi, 2003) R. K. S. Yi, 2003. MOCA : Mobile Certificate Authority for Wireless Ad-hoc Networks. Dans les actes de 2^{nd} *Annual PKI Research Workshop (PKI'03)*.

(Sanzgiri et al., 2005a) K. Sanzgiri, B. Dahill, D. LaFlamme, B. N. Levine, C. Shields, et E. Belding-Royer, 2005a. An Authenticated Routing Protocol for Secure Ad Hoc Networks. Dans les actes de *Selected Areas in Communication (JSAC)*, 598–610.

(Sanzgiri et al., 2005b) K. Sanzgiri, B. Dahill, D. LaFlamme, B. N. Levine, C. Shields, et E. M. Belding-Royer, 2005b. An Authenticated Routing Protocol for Secure Ad Hoc Networks. *Journal of Selected Areas in Communication (JSAC) 23*, 598–610.

(Shamir, 1995) A. Shamir, 1995. How to Share a Secret. Dans les actes de *Communications of the ACM*, Volume 22, 612–613.

(Sk. Md. M. Rahman et Okamoto, 2006) T. O. M. M. Sk. Md. M. Rahman, A. Inomata et E. Okamoto, 2006. Anonymous Secure Communication in Wireless Mobile Ad-hoc Networks. Dans les actes de *Cryptology ePrint Archive, Report 2006/328, http ://eprint.iacr.org/*.

(T. Beth et Klein, 1994) M. B. T. Beth et B. Klein, 1994. Valuation of trust in open networks. Dans les actes de *European Symposium on Research in Computer Security (ESORICS'94)*.

(Takagi et Kleinrock, 1984) H. Takagi et L. Kleinrock, 1984. Optimal Transmission Ranges for Randomly Distributed Packet Radio Terminals. *32-2*.

(Toumpis et Goldsmith, 2003) S. Toumpis et A.-J. Goldsmith, 2003. Performance, optimization, and cross-layer design of media access protocols for wireless ad hoc networks. Dans les actes de *IEEE ICC'2003 Communications in Ad Hoc Networks*, 2234–2240.

(Trappe et Wahington, 2006) W. Trappe et L. Wahington, 2006. Introduction to cryptography with coding theory. Dans les actes de *Pearson Education*.

(V. Bharghavan et Zhang, 1994) S. S. V. Bharghavan, A. Demers et L. Zhang, 1994. MACAW : A Media Access Protocol for Wireless LANs. Dans les actes de *ACM SIGCOMM'94*, 212–225.

(W. Xu, 2005) Y. Z. T. W. W. Xu, W. Trappe, 2005. The feasibility of launching and detecting jamming attacks in wireless networks. Dans les actes de *ACM international symposium on Mobile ad hoc Networking and Computing*, 46–57.

(X. Bin, 2005) H. Y. E.-M. S. X. Bin, C. Wei, 2005. An active detecting method against syn flooding attack. Dans les actes de *International Conference on Parallel and Distributed Systems*, 709–715.

(X. Huang et Zhang, 2006) Y. M. X. Huang, W. Susilo et F. Zhang, 2006. Short (identity-based) strong designated verifier signature schemes. Dans les actes de *International Conference Information Security Practice and Exprience (ISPEC'06) LNCS 3903*, 214–225.

(X. Xue et BenOthman, 2004) J. L. X. Xue et J. BenOthman, 2004. A trust-based routing protocol for ad hoc networks. Dans les actes de *Mobile and Wireless Communications Networks*.

(Y.-C. Hu et Perrig, 2002) D. J. Y.-C. Hu et A. Perrig, 2002. Sead : Secure efficient distance vector routing for mobile wireless ad hoc networks. Dans les actes de *IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002)*.

(Y.-C. Hu, 2003) D. J. Y.-C. Hu, A. Perrig, 2003. Packet leashes : A defense against wormhole attacks in wireless ad hoc networks. Dans les actes de *IEEE INFOCOM2003*.

(Y. Dong, 2007) A. F. S. V. L. L. H. S. Y. Y. Dong, H. W. Go, 2007. Providing Distributed Certificate Authority Service in Mobile Ad Hoc Networks. *Computer Communication 30*, 2442–2452.

(Y. Zhang et Lou, 2005) W. L. Y. Zhang et W. Lou, 2005. Anonymous Communication in Mobile Ad Hoc Networks. Dans les actes de *IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'05)*, 1940– 1951.

(Yi et Kravets, 2004) S. Yi et R. Kravets, 2004. Quality of Authentication in Ad Hoc Networks. Dans les actes de *ACM (MobiCom2004)*.

(Z. Trabelsi et Frikha, 2004) K. K. Z. Trabelsi, H. Rahmani et M. Frikha, 2004. Malicious sniffing systems detection platform. Dans les actes de *International Symposium on Applications and the Internet*, 201–207.

(Zhang et Lee, 2000) Y. Zhang et W. Lee, 2000. Intrusion detection in wireless ad-hoc networks. Dans les actes de *ACM MobiCom'2000*, 275–283.

(Zhou et Haas, 1999) L. Zhou et Z. J. Haas, 1999. Securing ad hoc networks. *IEEE Network 13*, 24–30.

(Zimmermann, 1995) P. R. Zimmermann, 1995. *The official PGP user's guide*.