La Sécurité dans les Réseaux Sans Fil Ad Hoc

Valérie Gayraud[1], Loutfi Nuaymi[2], Francis Dupont[2], Sylvain Gombault[2], and Bruno Tharon[2]

Thomson R&I, Security Lab,
1, Avenue de Belle-Fontaine,
35551 Cesson Sévigné
valerie.gayraud@thomson.net
ENST Bretagne,
2, Rue de la Châtaigneraie,
CS 17607, 35576 Cesson Sévigné
{loutfi.nuaymi, francis.dupont, sylvain.gombault,
bruno.tharon}@enst-bretagne.fr

Résumé Cet article présente une étude sur la sécurité des réseaux sans fil ad hoc. La première partie définit la notion de réseaux sans fil ad hoc et leurs contextes d'utilisation. Une synthèse d'analyse de risque de haut niveau menée sur ce type particulier de réseaux fait l'objet de la seconde partie. La troisième partie se focalise sur le routage, une fonction particulièrement sensible des réseaux sans fil ad hoc. Le fonctionnement général des protocoles de routage et les attaques correspondantes sont présentés. La partie quatre concerne l'état de l'art actuel des solutions proposées par les différentes équipes de recherche travaillant sur ce sujet à travers le monde. Nous concluons sur la sécurisation des réseaux sans fil ad hoc et indiquons les axes futurs de développement qui nous semblent intéressants.

1 Les Réseaux sans fil Ad Hoc

Les réseaux sans fil ad hoc sont composés de systèmes informatiques divers, plus ou moins complexes, appelés **nœuds** par la suite, ayant la possibilité de communiquer de manière autonome par ondes radio. Les nœuds interagissent et peuvent coopérer pour s'échanger des services. Un nœud peut à la fois communiquer directement avec d'autres nœuds ou servir de **relais**. Un relais permet à des nœuds se trouvant hors de portée radio les uns des autres de communiquer. Ces réseaux sont dits ad hoc dans la mesure où ils ne nécessitent pas d'infrastructure fixe. Ils peuvent exister temporairement pour répondre à un besoin ponctuel de communication. Le mode de fonctionnement **ad hoc** se distingue du mode **infrastructure** dans lequel les nœuds du réseau communiquent entre eux via un point d'accès, aussi appelé base, qui peut être relié à un réseau fixe. La figure 1 montre la différence d'utilisation des réseaux sans fil en mode infrastructure fixe et en mode ad hoc. Les applications de tels réseaux sont nombreuses et tendent à se multiplier avec la miniaturisation des processeurs et la diversité des terminaux. Les situations à caractère exceptionnel se prêtent bien à l'utilisation de

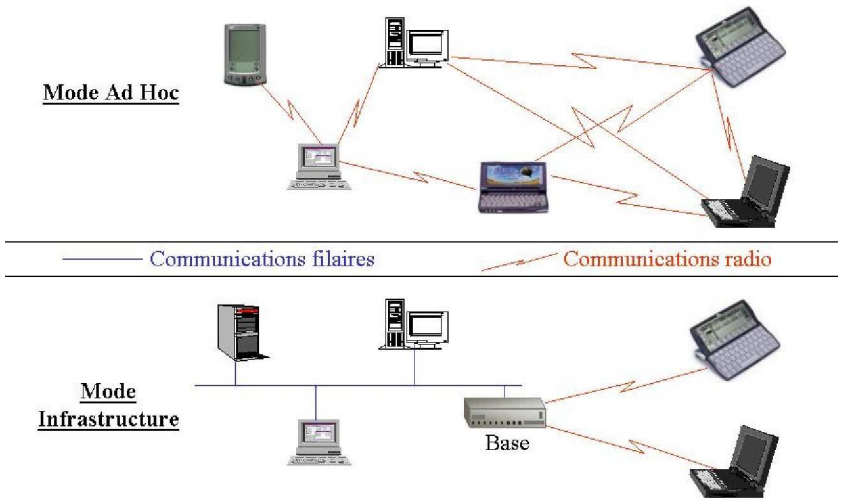

Fig. 1. Mode infrastructure versus mode ad hoc

réseaux sans fil ad hoc : opérations militaires, couvertures d'évènements sportifs, opérations de secours. Plus simplement, une réunion de travail peut demander la création ponctuelle d'un réseau informatique entre ses participants. Les réseaux domestiques représentent aussi un vaste champ d'application en plein devenir. L'organisation d'une soirée de jeux vidéo en réseaux, où chacun apporte son matériel, illustre une utilisation possible dans ce milieu.

L'**IETF** (*Internet Engineering Task Force*) a créé une entité spécifique pour les réseaux mobiles ad hoc, le groupe de travail **MANET** (*Mobile Ad hoc Networks*). Les membres de ce groupe soumettent régulièrement des propositions de protocoles de routage adaptés aux réseaux mobiles ad hoc.

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

- Les technologies IEEE 802.11a, 802.11b (*Wireless Fidelity*, WiFi), 802.11g, HiperLan/1 (remplacé par HiperLan/2), HomeRF (SWAP) sont propres aux réseaux WLAN (*Wireless Local Area Network*).
- La technologie Bluetooth, pour les réseaux **WPAN** (*Wireless Personal Area Network*). Bluetooth fonctionne en mode point à point ou point à multipoint.
- Les technologies infrarouges (IrDA, *Infrared Data Association*), utilisées dans les télécommandes par exemple, peuvent aussi être considérées comme support des réseaux ad hoc. Mais ces technologies se limitent à des communications point à point.

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

2 Les Risques Liés à la Sécurité Informatique

2.1 L'Analyse de Risque en Sécurité

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

1. Détermination des **fonctions** et **données** sensibles des réseaux sans fil ad hoc.
2. Recherche des **exigences de sécurité** par le biais des critères de sécurité que sont l'authentification, l'intégrité, la confidentialité, l'anonymat et la disponibilité.
3. Étude des **vulnérabilités**.
4. Étude des **menaces** et quantification de leur probabilité d'occurrence ou de leur faisabilité.
5. **Mesure du risque** encouru en fonction des vulnérabilités mises en lumière et des menaces associées.

À partir de ces différents points d'entrée, il est possible de déterminer quelles sont les parties critiques, en terme de sécurité, que les concepteurs, administrateurs, et utilisateurs de réseaux sans fil ad hoc doivent appréhender. La figure 2 retrace les différentes phases de ce processus.

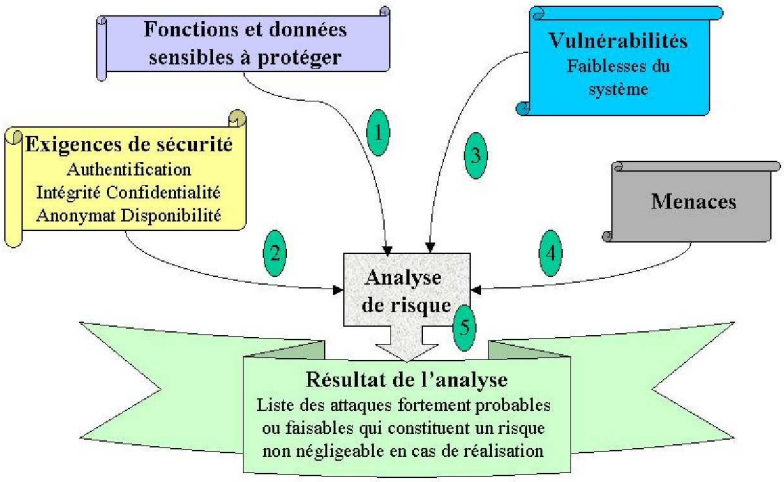

Fig. 2. Les étapes de l'analyse de risque

Il faut noter qu'une généralisation des besoins en sécurité faisant abstraction des contextes d'utilisation a été nécessaire pour mener à bien cette analyse de

risque. En effet, une application commerciale civile, par exemple, n'aura pas les même contraintes qu'une application militaire. Un contexte militaire mettra en avant le fort besoin d'authentification, de furtivité et d'intégrité physique des éléments alors qu'une utilisation commerciale critique nécessitera de se focaliser sur la confidentialité des services. Selon les cas, il peut donc être indispensable d'étudier des solutions appropriées au contexte d'utilisation à travers une analyse approfondie prenant en compte des contraintes spécifiques. L'analyse indiquée ici se veut générale et peut servir de base à une telle étude.

2.2 Fonctions et Données Sensibles

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

- Des données relatives au routage (tables de routage et données de configuration des mécanismes de routage)
- Des mesures et données de configuration pour la gestion de l'énergie.
- Des données relatives à la sécurité (clés cryptographiques, mots de passe, certificats...)
- D'une manière générale tout ce qui concerne les données de configuration.

Les informations personnelles des utilisateurs doivent aussi être considérées comme des données sensibles.

2.3 Exigences de Sécurité des Réseaux sans fil Ad Hoc

Contraintes :

Déterminer les exigences de sécurité d'un système nécessite d'appréhender l'ensemble des contraintes qui pèsent sur ce système. Cette étape permet par la suite de quantifier les critères de sécurité. Les spécificités des réseaux sans fil ad hoc sont multiples. On peut les répartir en six grands thèmes traitant des caractéristiques des nœuds, de la gestion de l'énergie, des caractéristiques du réseau, des technologies sans fil sous jacentes, de la mobilité et de la configuration.

Caractéristiques des Nœuds :

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

Gestion de l'Énergie :

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

Caractéristiques du réseau :

- La **charge** du réseau doit être **distribuée équitablement** entre les éléments en tenant compte de leur capacité respective.
- Chaque élément d'un réseau ad hoc est autonome et possède à la fois les fonctionnalités de **relais** et de **point de communication**. L'administration de ces éléments reste interne au réseau.
- L'**absence d'infrastructure centralisée** sera une contrainte très forte pour la gestion des accès aux ressources du réseau.

Technologie sans fil :

- Les perturbations dûes à l'environnement radio peuvent entraîner des **diminutions de débit et bande passante**.
- Les réseaux sans fil ad hoc héritent de l'architecture propre aux technologies WLAN et WPAN, et notamment des couches **physique** et **liaison de données** de ces technologies.

Mobilité :

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

Configuration :

- L'**auto configuration** permet aux nœuds de s'intégrer facilement dans un réseau. Elle facilite la gestion du réseau car l'interconnexion des éléments ne nécessite qu'un minimum d'intervention technique externe. Cette fonctionnalité est de plus en plus nécessaire pour un déploiement à grande échelle des réseaux sans fil ad hoc.

Authentification / Intégrité / Confidentialité / Disponibilité :

Coopérer au sein de tels réseaux présente un risque s'il n'y a aucun contrôle des participants. L'**authentification** des parties apparaît donc comme la pierre angulaire d'un réseau sans fil ad hoc sécurisé. En effet, comment assurer une quelconque confidentialité et intégrité des messages échangés si, dès le départ, on n'est pas sûr de communiquer avec la bonne entité ?

Contrairement au réseau filaire, il n'est pas nécessaire de pénétrer dans un local physique pour accéder au réseau. Si l'authentification est mal gérée, un attaquant peut s'attacher au réseau sans fil et injecter des messages erronés. L'**intégrité** des messages échangés est donc une exigence importante pour ces réseaux. L'intégrité des nœuds est, elle aussi, primordiale car les éléments d'un réseau ad hoc sont moins sujets à surveillance. En effet, ils ne sont pas confinés

dans un bureau mais transportés par leur propriétaire et peuvent donc être momentanément égarés. Un attaquant peut subtiliser un appareil, le corrompre avec un cheval de Troie par exemple, avant de le restituer discrètement à son propriétaire.

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

La **disponibilité** est une propriété difficile à gérer dans les réseaux sans fil ad hoc étant donné les contraintes qui pèsent sur ces réseaux :

- Topologie dynamique.
- Ressources limitées sur certains nœuds de transit.
- Communications sans fil pouvant être facilement brouillées ou perturbées.

Les applications sans fil en mode ad hoc ne devraient donc pas se focaliser sur ce critère.

Anonymat / Protection de la Vie Privée :

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

2.4 Vulnérabilités

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

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

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

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

Enfin, ces réseaux héritent de toutes les vulnérabilités propres aux technologies sans fil WLAN et WPAN.

2.5 Menaces

On distingue les menaces de type passif, où l'attaquant est limité à l'écoute et l'analyse du trafic échangé, des menaces de type actif. Dans ce dernier mode,

l'attaquant se donnera les moyens d'agir sur la gestion, la configuration et l'exploitation du réseau. Il peut injecter son propre trafic, modifier le fonctionnement d'un nœud, usurper l'identité d'un élément valide, rejouer des messages, modifier des messages transitant sur le réseau ou provoquer un déni de service. L'attaque passive prive le réseau de la confidentialité des messages échangés. Éventuellement, l'analyse du trafic représente un risque pour l'anonymat des participants et le respect de leur vie privée.

2.6 Résultat de l'Analyse de Risque

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

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

- Brouillage du canal radio pour empêcher toute communication.
- Tentative de débordement des tables de routages des nœuds servant de relais.
- Non-coopération d'un nœud au bon fonctionnement du réseau dans le but de préserver son énergie. L'égoïsme d'un nœud est une notion propre aux réseaux ad hoc. Un réseau ad hoc s'appuie sur la collaboration sans condition de ses éléments. Un nœud refusant de jouer le jeu peut mettre en péril l'ensemble.
- Tentative de gaspillage de l'énergie de nœuds ayant une autonomie de batterie faible ou cherchant à rester autonome (sans recharge) le plus longtemps possible. Ces nœuds se caractérisent par leur propension à passer en mode veille le plus souvent possible. L'attaque consiste à faire en sorte que le nœud soit obligé de rester en état d'activité et ainsi de lui faire consommer toute son énergie. Cette attaque est référencée par Ross Anderson et Franck Stajano ([8,9])) sous l'appellation ***sleep deprivation torture attack***, un scénario de torture par privation du sommeil.
- Dispersion et suppression du trafic en jouant sur les mécanismes de routage.

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

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

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

Enfin, il apparaît clairement que les attaques sur les **mécanismes de routage** sont particulièrement critiques. Ce papier accorde donc une large part à cette problématique dans la partie qui suit.

3 Le Routage dans les Réseaux sans fil Ad Hoc

Les protocoles de routage peuvent être classés en différentes familles selon le moment auquel ils initient la découverte de route, selon la manière dont les nœuds d'un réseau se partagent le travail de routage et selon la manière dont les informations de routage sont échangées.

3.1 Classification des Protocoles de Routage

Si un protocole initie la découverte de route lorsque le besoin s'en fait ressentir, c'est à dire lorsqu'un paquet doit être transmis vers une destination dont la route n'est pas connue dans la table de routage, il sera considéré comme faisant partie de la famille des protocoles **réactifs**. Si le protocole initie des découvertes de route régulièrement sans attendre qu'il y ait un paquet à transmettre, il sera dit **proactif**. Certains protocoles combinent ces deux manières d'initier des découvertes de routes, à la demande et en avance, et sont donc considérés comme **hybrides**. Certains protocoles de routage n'utilisent pas tous les nœuds d'un réseau pour faire transiter les messages, au contraire ils en sélectionnent certains, en fonction du voisinage ou pour former des cellules. Ces protocoles sont dits **non-uniformes**. Ceux qui utilisent tous les nœuds du réseau capables de router sont appelés **uniformes**. Les algorithmes permettant de maintenir la table de routage sont de deux types : les algorithmes basés sur le ***distance vector*** et ceux basés sur le ***link state***. Les protocoles de type *distance vector* n'ont qu'une vision partielle du réseau. Les protocoles de type *link state* maintiennent leur table de routage à jour grâce à des annonces faites régulièrement par les différents nœuds reflétant l'état de l'ensemble des liaisons du réseau. Ces protocoles ont une vision totale du réseau. On peut citer quelques protocoles de routage proposés au sein du groupe de travail MANET :

- **AODV** (*Ad hoc On demand Distance Vector*) est un protocole réactif, uniforme, de type *distance vector*.
- **DSR** (*Dynamic Source Routing*) est réactif, uniforme, de type *link state*.
- **OLSR** (*Optimized Link State Routing*) est un protocole non-uniforme, proactif, de type *link state*.
- **FSR** (*Fisheye State Routing*) est proactif, uniforme, de type *distance vector*.

3.2 Le Routage de Paquets

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

une route existe pour ce nœud. Si elle n'existe pas, il initie une découverte de route, ***route discovery***, en diffusant sur le réseau, dans les airs pour les accès sans fil, un message de type ***route request***. Le message de *route request* contient l'adresse du nœud émetteur, l'adresse du nœud destinataire, un marqueur permettant d'identifier la découverte de route et une liste initialement vide à remplir par les nœuds intermédiaires. Lorsqu'un nœud intermédiaire reçoit ce paquet, s'il n'en est pas le destinataire et si sa table de routage n'indique pas de chemin pour le nœud recherché, il diffuse à son tour le paquet de type *route request* en rajoutant son adresse à la liste de nœuds intermédiaires. Dans le cas où le nœud intermédiaire possède dans sa table de routage un chemin pour le nœud destinataire, la majorité des protocoles prévoit que le nœud intermédiaire renvoie directement un message de type ***route reply*** à l'émetteur en indiquant ce chemin. Lorsqu'un paquet de requête atteint son destinataire, ce dernier émet un paquet de réponse du type *route reply*. Ce paquet transite par les nœuds intermédiaires de la liste. La figure 3 schématise l'évolution des messages lors de la découverte de route.

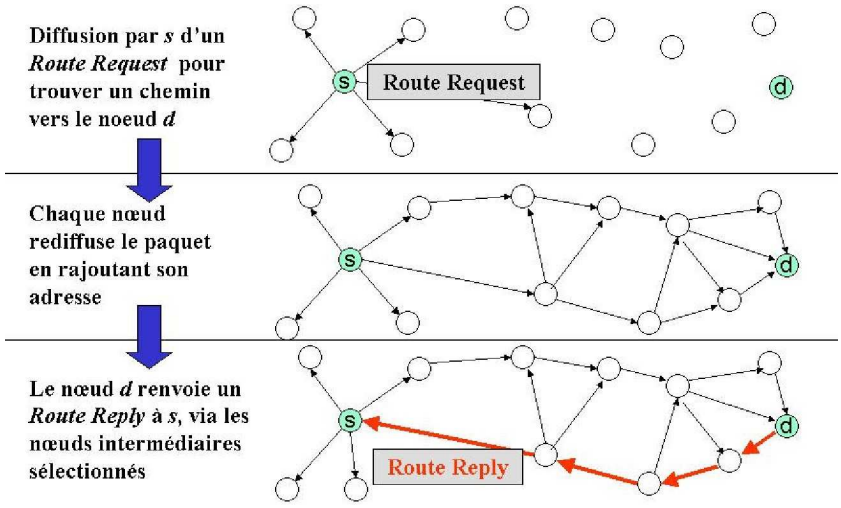

Fig. 3. Découverte de route initiée par le protocole de routage

Lorsque la réponse atteint l'initiateur de la découverte de route, ce dernier met à jour sa table de routage avec cette nouvelle route, qui consiste en la liste des nœuds intermédiaires avec un coût associé. Le coût sert aux nœuds à effectuer un choix entre deux routes menant à la même destination. Il peut être basé sur le nombre de nœuds intermédiaires traversés ou sur des critères plus complexes comme le débit, la fiabilité des liaisons ou la taille des paquets. Si l'initiateur reçoit ultérieurement une indication comme quoi cette destination

peut-être jointe avec un coût plus faible par un autre chemin, la table sera mise à jour avec la route ayant le coût le plus faible. Une fois une route établie, un protocole de routage doit aussi mettre en œuvre un mécanisme de maintenance des routes pour gérer les évènements comme la coupure d'un lien entre deux nœuds par lesquels transitent des messages. Lorsqu'un nœud reçoit un paquet de données pour une destination vers laquelle il ne peut plus émettre, il renvoie un message d'erreur de type ***route error*** vers la source du paquet de données. La route doit alors être supprimée de la table de routage. Des optimisations existent permettant à un nœud d'écouter les routes échangées par les autres nœuds et de mettre à jour sa table de routage en conséquence.

3.3 Les Attaques Liées aux Protocoles de Routage

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

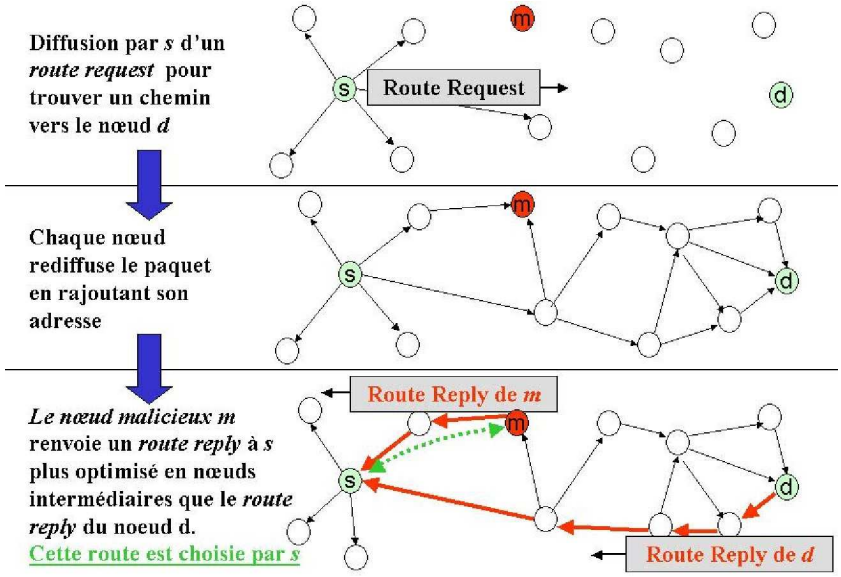

Fig. 4. Attaque *black hole* : Le nœud malicieux m capte le trafic dédié au nœud d

Si un nœud malicieux a la capacité d'usurper l'identité d'un nœud valide du réseau, il peut lors du mécanisme de découverte de route répondre au nœud initiateur avec un message de type *route reply* en annonçant un chemin, avec

un coût minimal, vers le nœud demandé. Le nœud émetteur mettra alors sa table de routage à jour avec cette fausse route. Les paquets de données du nœud émetteur vers le nœud destinataire transiteront par le nœud malicieux qui pourra tout simplement les ignorer. Cette attaque est appelée trou noir, ***black hole***[1]. Les paquets sont captés et absorbés par le nœud malicieux. La figure 4 illustre cette attaque.

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

4 État de l'Art des Solutions

4.1 Solutions pour l'Authentification

L'absence d'infrastructure centralisée dans les réseaux sans fil ad hoc compromet l'utilisation directe des systèmes d'authentification basés sur la cryptographie à clé publique. En effet, ces systèmes d'authentification supposent l'utilisation de **certificats** établis par une **autorité centrale**. Le certificat, signé par l'autorité centrale, permet de garantir qu'une clé publique appartient bien à son propriétaire et non à un usurpateur. L'opération de vérification de certificat ne se limite pas à contrôler la signature de l'autorité centrale. Il est aussi nécessaire de s'assurer que le certificat est toujours en cours de validité et qu'il n'a pas été révoqué. Une révocation de certificat est indispensable si la clé privée du propriétaire a été volée ou divulguée. Il existe trois grands courants dans le domaine de l'authentification pour les réseaux sans fil ad hoc. Deux de ces orientations se basent sur l'établissement d'une clé secrète permettant par la suite l'authentification des participants. Toute la complexité réside en la manière d'établir cette clé. Les deux modèles basés sur une clé secrète sont :

- ***The key agreement*** : Les participants s'entendent sur une clé secrète.
- ***The Duckling Security Policy Model*** : Le modèle d'authentification élaboré par Ross Anderson et Franck Stajano [9].

Le troisième axe de recherche pour l'authentification au sein de réseaux sans fil ad hoc, se base sur la cryptographie à clé publique et cherche à s'affranchir du besoin d'une entité centrale de certification :

- **L'infrastructure à clé publique auto-organisée** : Modèle proposée par Hubaux *et al.* [5].

[1] Cette attaque n'est pas spécifique aux réseaux sans fil, on la retrouve aussi dans les réseaux filaires

Clé Secrète Commune (*Key Agreement*) :

Les recherches en matière de *key agreement* dans les réseaux ad hoc se focalisent sur la manière d'établir une clé commune entre plusieurs participants qui ne se connaissent pas à priori. La mise en place de protocoles assurant l'authentification mutuelle n'est pas abordée dans le cadre de ce papier car ces problématiques ne sont pas typiques au réseau ad hoc. Les participants établissent entre eux une clé secrète leur permettant de s'authentifier afin de communiquer de manière sécurisée. La mise en place de cette clé peut se faire de manière **distribuée**. Dans ce cas, la clé secrète est fournie aux participants du réseau ad hoc via un canal supposé sûr. C'est le cas lorsque des collègues souhaitant établir une communication sûre entre eux à l'occasion d'une réunion dans une salle de conférence close, distribuent un mot de passe inscrit sur un morceau de papier qui fait le tour de la salle. Seules les personnes présentes dans la salle en ont connaissance. Une clé forte peut être dérivée du mot de passe à l'aide d'une fonction de hachage. La difficulté de ce mode de fonctionnement est de trouver un canal sécurisé pour distribuer la clé. Une autre manière d'établir une clé secrète commune est de faire en sorte que chaque participant apporte sa **contribution** à la clé finale. Lorsqu'il n'y a que deux nœuds, le protocole de **Diffie-Hellman** [2] peut être utilisé.

Méthode de Diffie-Hellman

Alice et Bob se mettent d'accord sur un entier N et un générateur α du groupe cyclique fini d'ordre N (ce groupe est constitué de tous les entiers positifs ou nul strictement inférieur à N, les calculs dans le groupe cyclique se font modulo N). Alice et Bob choisissent chacun un nombre **secret** utilisé comme exposant. Le secret d'Alice est a, et celui de Bob est b. Alice envoie alors $\alpha^a modulo(N)$ à Bob et Bob envoie $\alpha^b moduloN$ à Alice :

$$Alice \longrightarrow Bob : \alpha^a modulo(N)$$

$$Bob \longrightarrow Alice : \alpha^b modulo(N)$$

Une fois que Bob a reçu $\alpha^a modulo(N)$ de la part d'Alice, il peut utiliser son nombre secret b pour calculer :

$$(\alpha^a modulo(N))^b modulo(N) \Longrightarrow (\alpha^a)^b modulo(N) \Longrightarrow (\alpha^{a.b}) modulo(N)$$

De son côté, Alice peut calculer :

$$(\alpha^b modulo(N))^a modulo(N) \Longrightarrow (\alpha^b)^a modulo(N) \Longrightarrow (\alpha^{b.a}) modulo(N)$$

La **clé résultante**, secret partagé par Alice et Bob, sera $\alpha^{a.b} modulo(N)$. Un attaquant qui a la possibilité d'écouter les échanges entre Alice et Bob, ne pourra pas deviner la clé car il est très difficile (en terme de puissance de calcul), lorsque N, a et l'exposant sont suffisamment grands, de calculer le nombre secret a connaissant N et α. L'opération revient à calculer un logarithme discret dans le groupe cyclique fini d'ordre N.

Il faut noter que le protocole de Diffie-Hellman tel que présenté ici ne résiste pas aux attaques du type *man in the middle*, il faut donc rajouter des éléments

dans les échanges permettant une authentification mutuelle des participants. Lorsqu'il y a plus de deux nœuds, le protocole de **Diffie-Hellman doit être généralisé à de multiples participants**. Chaque nœud i possède son exposant secret e_i, la clé résultante sera $\alpha^{e_1 \cdot e_2 \cdot \ldots \cdot e_n}$ pour n participants. La mise en pratique du protocole de Diffie-Hellman à de multiples participants n'est pas si simple et fait l'objet de nombreuses recherches. En effet, il ne suffit pas que chacun envoie la valeur α^{e_i} aux autres pour que tous les nœuds aient la possibilité de déterminer la clé. Le protocole de Diffie-Hellman s'appuie sur le fait que les participants calculent la clé à l'aide de la valeur reçue des autres participants et leur exposant secret. Il faudrait donc que le nœud i reçoive la valeur $\alpha^{e_1 \cdot e_2 \ldots \cdot e_{i-1} \cdot e_{i+1} \ldots \cdot e_n}$ pour être capable de calculer la clé. La mise en pratique peut se faire comme indiqué dans la figure 5.

1 Le premier nœud envoie α^{e_1} au second nœud

2 Le deuxième nœud envoie $\alpha^{e_1 \cdot e_2}$ au troisième nœud

3 Le (n -2)-ième nœud envoie $\alpha^{e_1 \cdot e_2 \cdot \ldots \cdot e_{n-2}}$ au (n -1)-ième

4 Le (n -1)-ième nœud envoie la valeur $\eta = \alpha^{e_1 \cdot e_2 \cdot \ldots \cdot e_{n-1}}$ à tous les autres nœuds

5 Le dernier nœud n peut alors déterminer la clé secrète partagée,

$$k = \alpha^{e_1 \cdot e_2 \cdot \ldots \cdot e_n} = \eta^{en}$$

6 Chaque nœud i envoie la valeur $\eta^{\frac{E_i}{e_i}}$ au nœud n, (E_i est un facteur de brouillage choisi par i)

7 Le nœud n renvoie à chacun des nœuds la valeur $(\eta^{\frac{E_i}{e_i}})^{e_n} = \eta^{e_n \cdot \frac{E_i}{e_i}}$

8 Les nœuds i enlèvent le facteur de brouillage $\frac{E_i}{e_i}$ pour retrouver la clé $k = \eta^{en}$

$$(\eta^{en \cdot \frac{E_i}{e_i}})^{\frac{e_i}{E_i}} = \eta^{en}$$

Fig. 5. Exemple d'application du protocole de Diffie-Hellman à de multiples participants

Cette application de Diffie-Hellman à de multiples participants a pour inconvénient de nécessiter d'établir au préalable une relation d'ordre entre les nœuds du réseau. De plus, il faut que le pénultième et l'antépénultième éléments aient la possibilité de communiquer avec tous les autres nœuds, ce qui est une contrainte beaucoup trop forte pour les réseaux sans fil ad hoc. D'autres possibilités ont été étudiées. Elles se basent sur le principe d'établir deux clés secrètes indépendamment entre deux groupes parallèles de deux entités à l'aide du protocole de Diffie-Hellman. Les deux clés secrètes sont ensuite utilisées comme exposant secret pour établir une troisième clé secrète entre les deux groupes de deux entités. La figure 6 illustre ces échanges.

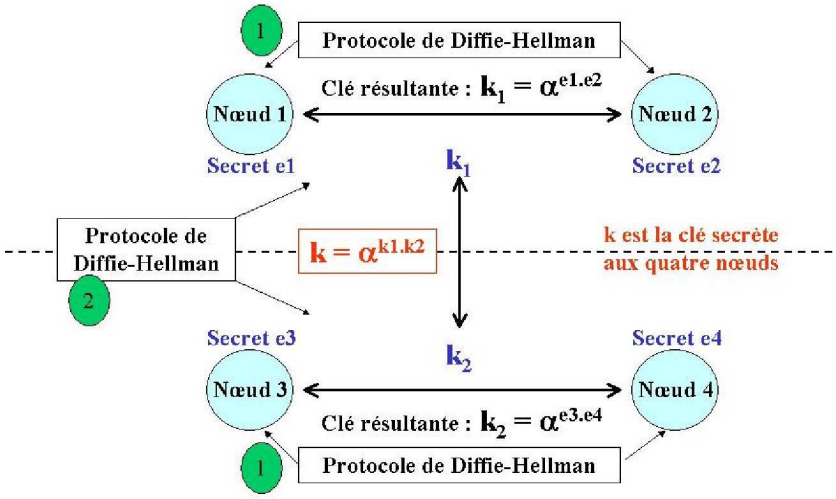

Fig. 6. Diffie-Hellman à quatre participants, configuration en cube

Le problème est que ces méthodes exploitent des organisations particulières de réseau, en cube par exemple. Un travail supplémentaire est donc nécessaire pour trouver le moyen d'appliquer le protocole de Diffie-Hellman aux réseaux à topologie dynamique et arbitraire que sont les réseaux ad hoc. Maarit Hietalahti [3] a, au cours de sa thèse à l'université d'Helsinki, travaillé sur un protocole mettant en œuvre une généralisation du protocole de Diffie-Hellman à de multiples participants par le biais du protocole **AT-GDH**, pour *Arbitrary Topology Generalisation of Diffie-Hellman*, dont le but est de résoudre ces problèmes. La solution proposée est basée sur la construction au préalable d'une topologie de type *spanning tree* et ensuite d'appliquer le protocole de Diffie-Hellman de la même manière que précédemment en balayant l'arbre des feuilles à la racine.

Relation de Type Maître-Esclave (*Duckling Security Policy Model*) :

Le travail de Ross Anderson et Franck Stajano s'inscrit dans la notion d'informatique omniprésente, ***ubiquitous computing***. Dans ce modèle, la plupart des objets nous entourant sont voués à recevoir un processeur leur permettant d'effectuer des comptes rendus de mesure (ce serait le cas pour un thermomètre dans le milieu médical par exemple) ou de rendre des services à d'autres objets de type maître comme le PDA (*Personal Digital Assistant*) d'un médecin. Les communications entre objets s'établissent via le canal radio. Le modèle d'authentification élaboré par Ross Anderson et Franck Stajano, *The Duckling Security Policy Model*, est basé sur une relation de type **maître-esclave**. Lors de sa première utilisation, un objet doit être marqué, ***imprinting***, par son propriétaire. Lors de cette opération une clé secrète est échangée entre les deux

entités via un canal supposé sûr. Il peut s'agir d'un contact physique entre le maître et l'esclave. Un point important à soulever dans cette politique est la **gestion de clés**. Doit-elle se faire par une entité centralisée, qui liste les objets sous son contrôle associés à leur propriétaire et à la clé correspondante ou bien par l'utilisateur lui-même. L'option centralisée semble tentante pour éviter aux utilisateurs la charge de gestion de clés, néanmoins elle implique un fort risque de violation de la vie privée en cas de divulgation par l'entité centrale de la liste objet-propriétaire-clé.

L'Infrastructure à Clé Publique Auto-Organisée :

Le troisième courant pour l'authentification, développé par Hubaux *et al.* [5], se base sur des infrastructures à clé publique, *public key infrastructure* (PKI), autogérées au sein du réseau ad hoc. Chaque nœud établit des certificats pour les nœuds en qui il a confiance. Lorsque deux éléments d'un réseau veulent communiquer sans connaissance au préalable l'un de l'autre, ils s'échangent leur liste de certificats et vont essayer de créer une **chaîne de confiance** entre eux. Supposons qu'un élément a veuille communiquer avec un nœud c, si a fait confiance en un troisième élément b et c fait aussi confiance en b, alors une chaîne de confiance entre a et c pourra être établie via b.

4.2 Solutions pour l'Intégrité Physique des Nœuds

L'intégrité des nœuds du réseau dépend fortement des capacités physiques de ce nœud à résister à des attaques qui permettraient à un attaquant de modifier le fonctionnement du nœud afin de le corrompre. Avoir la possibilité de booter sur la disquette ou le CD-ROM d'un PC en libre service dans un réseau ouvert corrompt fortement l'intégrité de ce nœud. En effet, l'OS (*Operating System*) du nœud peut alors être échangé par un OS corrompu. L'intégrité physique d'un système informatique, ***tamper resistance***, est une propriété très difficile à mettre en œuvre par les fabricants. Un moyen de contourner ce problème peut se faire en mettant en place des fonctions permettant de mettre en évidence une attaque physique sur un élément. Une telle fonction peut être comparée à un sceau assurant l'inviolabilité d'un courrier. Elle met en œuvre des notions de traçabilité de l'attaque.

4.3 Solutions pour l'Intégrité et l'Authentification des Messages

Les moyens classiques pour assurer l'intégrité et l'authentification des messages échangés par les nœuds d'un réseau sont l'utilisation de **signatures numériques** ou de **MACs** (*Message Authentication Code*). Les signatures numériques s'appuient sur la cryptographie à clé publique. Un nœud possède une clé publique qui sert à ses correspondants pour chiffrer des messages lui étant destinés et le nœud déchiffre les messages qu'il reçoit avec sa clé privée. Dans le cas de la signature, le nœud utilise une clé privée (dédiée à la signature) pour signer un message. Le destinataire du message déchiffre la signature avec la clé publique

de l'émetteur et est convaincu que ce dernier est bien l'auteur du message car lui seul connaît sa clé privée. De plus, le message est bien intègre car ne connaissant pas la clé privée de l'émetteur un attaquant ne pourra pas modifier le message original. L'utilisation de la cryptographie asymétrique n'est pas une solution préférée dans les réseaux ad hoc car certains nœuds peuvent avoir des capacités de calcul réduites. Or, la cryptographie asymétrique demande plus de temps de calcul que la cryptographie symétrique.

Une autre solution consiste à utiliser des MACs. Il s'agit de fonctions mathématiques à sens uniques dépendant d'une clé secrète qui, à partir du message original, produisent un condensé de ce message. Ces fonctions mathématiques sont telles qu'il est difficile de retrouver un message à partir de son condensé ou de produire deux messages ayant le même condensé. De plus, la moindre modification du message original entraîne un changement dans le condensé. L'inconvénient de cette solution est qu'il est nécessaire au préalable d'établir autant de clés secrètes que de paires de nœuds susceptibles de vouloir communiquer ensemble. D'autres solutions doivent donc être envisagées pour les réseaux ad hoc.

TESLA (*Time Efficient Stream Loss-tolerant Authentication*) a été proposé par Perrig *et al.* [7]. Il s'agit d'une extension au protocole décrit en [1], dit *Guy Fawkes' protocol*. TESLA permet d'authentifier les messages avec un MAC dépendant d'une clé secrète qui n'est divulguée par l'émetteur du message qu'après un délai d'attente δ. La valeur δ est calculée de manière à ce qu'on soit sûr que le destinataire a reçu le message avant la divulgation de la clé, cette condition garantie l'intégrité du message. Le temps δ ne doit pas être trop important pour limiter les latences dans le réseau, en effet un destinataire doit attendre la divulgation de la clé secrète avant de pouvoir effectivement traiter un message. La figure 7 décrit le fonctionnement de TESLA.

La clé secrète utilisée pour le MAC est issue d'une chaîne de clés. Un élément de la chaîne k_i est calculé de la manière suivante : $k_i = \hbar(k_{i+1})$ où $\hbar$ est une fonction de hachage. L'élément initial k_n est choisi par l'émetteur. Celui-ci va utiliser ces clés par ordre croissant c'est à dire en commençant par k_1. En réception, le destinataire pourra vérifier la relation suivante : $k_{i-1} = \hbar(k_i)$ où k_i est la clé dernièrement reçue et k_{i-1} correspond à la clé précédente. Cette condition assure que la clé k_i fasse bien partie de la chaîne de clé de l'émetteur, ce qui assure, en plus de l'intégrité, la propriété d'authentification du paquet. Il est à noter que ce processus doit être initialisé par l'authentification du premier paquet émis à l'aide d'une signature numérique.

Un exemple de protocole de routage sécurisé utilisant TESLA :

Une manière de contrer les attaques sur les mécanismes de routage consiste en l'authentification des messages de découverte et de maintenance de route. Hu, Perrig et Johnson ont développé un protocole de routage, **Ariadne** [4], basé sur le protocole DSR et qui implémente des mécanismes d'authentification des messages de routage en utilisant au choix un schéma de signature numérique, l'utilisation de MAC avec autant de clés secrètes établies que de paires de nœud ou bien en mettant en œuvre TESLA. Leur article se focalise sur cette dernière

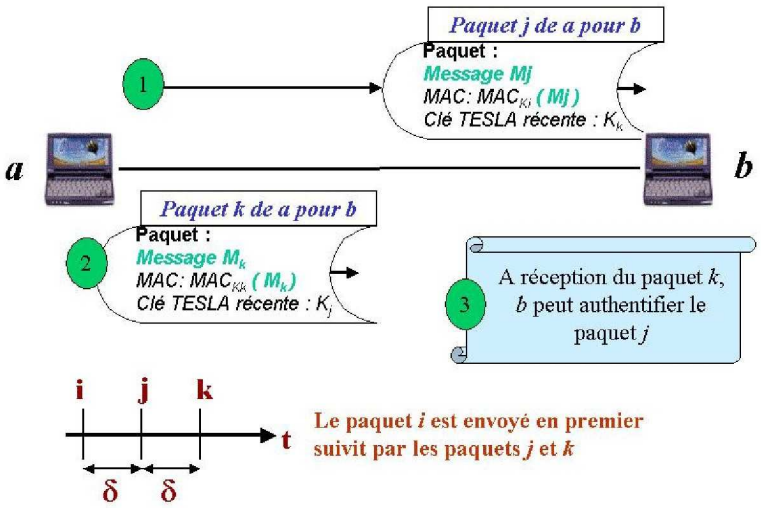

Fig. 7. Authentification de messages avec TESLA. Les messages M_i sont authentifiés à l'aide d'un MAC dont la clé k_i est divulguée dans un paquet subséquent

solution. Une conclusion intéressante de leur travail montre que l'introduction de mécanismes de sécurité dans un protocole de routage passe nécessairement par une diminution des performances de ce protocole. En effet, les entêtes des paquets de routage voient leur taille augmenter avec l'authentification des messages. De plus, une baisse de réactivité dûe au temps d'attente pour authentifier un message apparaît. Un compromis entre niveau de sécurité et performance est donc clairement nécessaire. Il faut rester prudent avec les mécanismes d'authentification de messages. En effet, un attaquant peut générer une multitude de paquets sur le réseau avec une fausse authentification. Les nœuds sont alors submergés par un nombre trop important de paquets non-valides à authentifier, ce qui ralentit le fonctionnement du réseau jusqu'à provoquer un déni de service. Il est aussi important de prévoir des mécanismes permettant de se prémunir contre un attaquant cherchant à rejouer des messages authentifiés.

4.4 Solutions pour la Confidentialité

La confidentialité dans les réseaux sans fil ad hoc est d'abord traitée par l'utilisation de transmission par saut de fréquences, *frequency hoping*. Les données sont transmises sur une séquence de fréquences définies pseudo-aléatoirement. L'attaquant doit connaître cette séquence pour pouvoir se synchroniser en réception. Une fois l'authentification des participants clairement établie, les outils cryptographiques permettent de rendre les communications confidentielles. Toutefois, étant donné qu'une des contraintes des réseaux ad hoc est de devoir être adaptables à des nœuds ayant de faibles capacités de calcul, la cryptographie

symétrique sera préférée à la cryptographie à clé publique, cette dernière nécessitant beaucoup plus de puissance de calcul.

4.5 Solutions pour l'Anonymat

L'anonymat est très difficile à obtenir dans des réseaux coopératifs. Il est préfèrable de parler de pseudo-anonymat. L'identité d'un participant est associée à un code à la manière d'un pseudonyme. Une autorité centrale de confiance est nécessaire pour stocker de manière sécurisée la correspondance identité / code.

4.6 Solutions pour la Disponibilité

Il n'existe aucun moyen de contrer un déni de service sur le canal radio provoqué par un attaquant puissant ayant les moyens de brouiller efficacement la totalité du spectre radio. Néanmoins, des techniques comme le saut de fréquence permettent de se prémunir contre des attaquants ayant des capacités plus réduites. En effet, ces techniques permettent une transmission des données sur un large spectre de fréquence. Pour être efficace un attaquant doit donc être capable de brouiller l'étendue des fréquences utilisées.

4.7 Solutions Complémentaires

Pour contrer les attaques sur les mécanismes de routage de type *black hole*, où un nœud malicieux prétend être un relais pour un autre nœud mais ne transmet pas les messages de données, Marti *et al.* [6] ont développé deux méthodes appelées ***watchdog*** et ***pathrater***. Le *watchdog* permet d'identifier les nœuds malicieux. Le *pathrater* est une technique permettant au protocole de routage d'éviter les nœuds corrompus inscrits dans une liste noire, *blacklist*. Il faut rester prudent quant à l'utilisation de ces mécanismes car ils peuvent être détournés par un attaquant. En effet, un nœud malicieux peut aussi faire en sorte qu'un nœud valide soit ajouté à la liste noire, l'isolant ainsi du réseau. L'utilisation de détecteurs d'intrusion dans les réseaux ad hoc est une solution complémentaire faisant l'objet de recherches intensives. L'**IDS** (***Intrusion Detection System***) collecte et analyse les données du trafic afin de déterminer si des utilisateurs non autorisés sont connectés ou si certains nœuds ont des comportements anormaux. Un axe de recherche consiste à étudier la manière dont les protocoles de routage pourraient utiliser ces informations pour prévenir certaines attaques.

5 Conclusion

Cet article montre à quel point les réseaux sans fil ad hoc constituent, de par leur nature, un formidable challenge pour la sécurité informatique. Les spécificités de ces réseaux sont principalement :

- La transmission en milieu ouvert.
- Les topologies dynamiques.

- L'absence d'autorité centrale.
- La nécessité de bonne coopération des nœuds.
- L'hétérogénéité des participants avec pour certains des capacités restreintes.

Toutes ces contraintes concourent à rendre la sécurité des réseaux sans fil ad hoc difficile et complexe à appréhender. Ce sujet va devenir d'autant plus critique que le développement de tels réseaux va rapidement s'amplifier. En effet, les réseaux sans fil ad hoc sont stimulés par l'évolution rapide des technologies informatiques vers la miniaturisation et l'intégration. L'authentification des nœuds et des messages échangés, constitue le point de départ incontournable pour la sécurité des réseaux ad hoc. Il existe de nombreuses études théoriques mais finalement peu d'applications pratiques qui puissent satisfaire l'ensemble des contraintes inhérentes aux infrastructures sans fil ad hoc. Enfin, il apparaît clairement que les mécanismes de routage constituent un point sensible pour la sécurité des réseaux sans fil ad hoc. La profusion de propositions diffusées au sein du groupe de travail MANET de l'IETF montre clairement le manque de maturité sur ce sujet. Un risque est que l'accent soit mis sur la résolution des problèmes fonctionnels au détriment de la sécurité. Les deux axes de recherche que sont l'authentification des nœuds et messages d'un côté, les mécanismes de routage sécurisés de l'autre, apparaissent comme des directions de travail primordiales. La prise en compte de ces deux problématiques doit se faire rapidement afin d'assurer un déploiement des réseaux sans fil ad hoc fiables et sécurisés.

Remerciements :

Les auteurs tiennent à remercier Jean-Marie Bonnin et Bruno Stevant de l'ENST Bretagne pour leur participation à la mise en place des manipulations. Merci à Eric Diehl, Olivier Heen et Nicolas Prigent du Security Lab de Thomson pour leurs conseils avisés et leur précieuse contribution à la préparation de ce papier et de la présentation. Nous souhaitons aussi remercier Thierry Martineau et Franck Veysset pour leur relecture du document et les remarques constructives qui ont suivi.

Références

1. Ross Anderson, Francesco Bergadano, Bruno Crispo, Jong-Hyeon Lee, Charalampos Manifavas and Roger Needham, A new family of authentication protocols, *ACM SIGOPS Operating Systems Review*, Vol. 32, no. 4, pp. 9–20, 1998.
2. Whitfield Diffie and Martin E. Hellman, New Directions in Cryptography, *IEEE Transactions on Information Theory*, IT-22, no. 6, pp. 644–654, 1976.
3. Maarit Hietalahti, Efficient Key Agreement for Ad Hoc Networks, Ph. D, Helsinki University of Technology, May 2001.
4. Yih Chun Hu, Adrian Perrig and David B. Johnson, Ariadne : A secure on-demand routing protocol for ad hoc networks, *Proceedings of The 8th ACM International Conference on Mobile Computing and Networking*, 2002, *citeseer.nj.nec.com/hu02ariadne.html*

5. Hubaux, J. P., Buttyan, L. and Capkun, S., The Quest for Security in Mobile Ad Hoc Networks, *Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Long Beach, CA, 2001.
6. , Sergio Marti, T.J Giuli, Kevin Lai and Mary Baker, Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks,
7. Adrian Perrig, Ran Canetti, J.D. Tygar and Dawn Song, Efficient Authentication and Signing Multicasts Streams over Lossy Channels, *IEEE Symposium on Security and Privacy*, September 2002.
8. Frank Stajano, *Security for Ubiquitous Computing*, John Wiley and Sons, 2002, *ISBN 0-470-84493-0*, *http ://www-lce.eng.cam.ac.uk/ fms27/secubicomp/*
9. Frank Stajano and Ross Anderson, The Resurrecting Duckling : Security Issues for Ad-hoc Wireless Networks, *7th International Workshop on Security Protocols*, pp. 172–194, 1999.