Etudes des vulnérabilités du protocole de routage OLSR

Céline Burgod

Etude des vulnérabilités du protocole de routage OLSR

Céline Burgod

26 septembre 2007

Résumé

Dans cette étude, nous considérons le problème de la sécurisation des informations de routage du protocole proactif OLSR dans les réseaux mobiles ad hoc. Premièrement, nous examinons les vulnérabilités et les attaques relatives à ce protocole, en mettant tout particulièrement l'accent sur celles visant à compromettre l'intégrité de l'infrastructure de routage. Ensuite, nous proposons une architecture de sécurité entièrement distribuée et basée sur l'intégration d'un environnement de confiance. Cette architecture nous permet de réduire les vecteurs d'attaques en dérivant d'une part des propriétés de sécurité explicites basées sur la cryptographie (telles que l'authenticité et l'intégrité des données échangées), et d'autre part des propriétés de sécurité implicites basées sur un protocole dédié de contrôle des échanges.

1 Vulnérabilités du protocole OLSR

Les protocoles de routage opèrent selon deux phases distinctes : une phase de découverte de la topologie du réseau durant laquelle des informations de contrôle relatives à la connaissance topologique du réseau sont échangées, puis une phase de retransmission des messages de données durant laquelle les données sont acheminées d'une source vers une destination. Contrairement aux réseaux filaires où les opérations de routage sont généralement réalisées par des équipements physiques d'interconnexion dédiés et gérés par une administration légitime, dans les réseaux mobiles ad hoc, ces opérations sont entièrement sous la responsabilité des nœuds qui les composent. Cette caractéristique de fonctionnement soulève de nombreux problèmes de sécurité. Au regard du protocole de routage OLSR, il est prévu que chaque nœud génère correctement des messages de contrôle HELLO et TC, puis maintienne une vue de la topologie du réseau dérivée à partir des messages qu'il reçoit. Or comme les nœuds sont autonomes, des comportements déviant des règles définies par le protocole peuvent apparître et causer des déformations sur la vue de la topologie du réseau construite.

Nous allons présenter dans un premier temps une liste des attaques possibles sur les opérations du protocole et sans altération des messages (telles que le rejeu ou la non-retransmission des messages de contrôle), puis une liste des attaques par construction ou altération des messages de contrôle.

1.1 Perturbation du protocole par rejeu et non retransmission des messages

Attaque simple par rejeu. Cette attaque consiste en la réémission d'informations de contrôle caducs (car ancienne). Elle est généralement empêchée par l'intégration d'une estampille temporelle dans les messages. Néanmoins, nous pouvons constater que dans le cadre de l'architecture de sécurité proposée par Raffo [6], le mécanisme de vérification distribué des estampilles temporelles requiert qu'il y ait une synchronisation d'horloge entre les nœuds.

Non retransmission des messages de contrôle. Si un nœud adversaire est désigné MPR par un de ses voisins et qu'il ne retransmet pas les messages de contrôle TC, alors des pertes de connectivité peuvent apparaître. Suite à cette attaque, tout nœud ciblé et voisin de l'adversaire devient non-atteignable par les autres nœuds du réseau situés à plus de deux sauts (car les informations d'état de liens ne sont pas disséminées à travers le réseau). Il est à noter que l'impact de l'attaque est d'autant plus important si l'adversaire parvient à se faire élire unique MPR par les nœuds ciblés.

Non retransmission des messages de données. Dans cette attaque, un nœud advesaire supprime une partie ou tous les messages de données qu'il reçoit des autres nœuds du réseau et qui ne lui sont pas destinés.

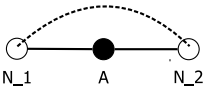

FIG. 1 – Attaque du trou de ver menée par un seul nœud adversaire

Attaque du trou de ver (dite attaque wormhole). De manière générale l'attaque par trou de ver (terme en référence aux trous de ver en astronomie qui sont des raccourcis entre deux points éloignés dans l'espace), le trafic d'une partie du réseau est enregistré puis relayé dans une autre partie du réseau. Une attaque par trou de ver peut être menée soit par un seul nœud adversaire, soit par une coalition d'adversaires.

La figure 1 illustre le principe de l'attaque selon la premier modèle d'adversaire. Nous considérons un nœud adversaire (dénoté A) situé à la fois dans le champ direct de communication de deux nœuds légitimes (dénotés N_1 et N_2), sachant que N_1 et N_2 ne sont pas à porté directe de communication. De par un simple relais des messages de contrôle de N_1 vers N_2 (et vis-versa), l'adversaire A parvient à créer un lien physiquement inexsitant entre N_1 et N_2et dont il a entièrement le contrôle. En effet, dans la suite des échanges entre N_1 et N_2, l'adversaire peut soit poursuivre le relais des messages par le tunnel soit briser le lien.

Une variante consiste en une coalition d'au minimum deux nœuds connectés entre eux soit par une liaison sans-fil soit par une liaison privée cablée. Le résultat est la création d'un trou de ver plus long (et peut être plus nocif car plus difficilement détectable de manière explicite).

Il est à noter que de sorte à paraître vituellement invisible, l'adversaire n'effectue aucune manipulation sur les messages de contrôle relayés, à savoir par exemple l'annonce de son adresse en tant que source dans l'en-tête du message. La sévérité de l'attaque vient du fait d'une part qu'elle est difficilement détectable et d'autre part qu'elle est effective même dans le cadre d'un réseau où l'authentifcation, l'intégrité et la confidentialité sont préservées.

1.2 Altération des messages de contrôle

Dans cette partie, nous décrivons quelques attaques unitaires sur les messages de contrôle (HELLO et TC) du protocole de routage OLSR, puis pour chacune des attaques décrites, nous étudions les impacts causés sur le réseau. L'ensemble des attaques décrites dans les paragraphes suivant impliquent un seul et unique adversaire.

Il est à noter qu'il s'agit des types d'attaques communément rencontrées dans la littérature traitant de la sécurité du protocole de routage OLSR. Dans la section suivante, nous étudierons d'autres types d'attaque où la puissance (ou les moyens) de l'adversaire est augmentée, à savoir que plusieurs nœuds pourront être en conivence. La classification proposée s'appuie sur les travaux menés par Raffo dans [6].

Normalement, chaque nœud dissémine des informations relatives à la topologie du réseau à travers les messages de contrôle de type HELLO et TC. L'injection de messages de contrôle truqués (qui peut être due soit à un disfonctionnement ou à un acte délibéré) conduit à une compromission de l'intégrité du réseau (annonces de routes conflictuelles, erreurs dans les tables de routage calculées, augmentation de la longueur des routes, redirection des trafics, perte de liens et de connectivité, création de partitionnement réseau). Il est important de signaler que les informations contenues dans les messages HELLO sont uniquement diffusées et utilisées localement (voisinage direct à un saut) tandis que les informations contenues dans les messages TC sont disséminées à travers tous les nœuds du réseau (pour le calcul des routes). Par conséquent, une attaque sur les messages HELLO conduit à des incohérences locales (à un ou deux sauts) sur la topologie du réseau tandis qu'une attaque sur les messages TC conduit à des incohérences sur la globalité du réseau.

1.2.1 Altération des messages de contrôle de type HELLO

Génération. Pour réduire ou augmenter ses changes d'être sélectionné MPR, un nœud adversaire peut exploiter le champ willingness défini dans les messages HELLO du protocole. Les valeurs admissibles pour le champ willingness sont 0 (jamais), 1 (basse), 3 (défaut), 6 (haute), 7 (toujours). Par exemple, par annonce d'une willingness à zéro, un nœud adversaire peut s'exclure naturellement du mécanisme de sélection des MPR excécuté par ses voisins. Il s'agit d'un comportement dit d'égoïsme où l'objectif d'un nœud n'est pas de dégrader intentionnelement le fonctionnement du réseau mais de profiter au maximum des services réseau offerts tout en y contribuant le moins possible. La rareté des ressources énergétique tend à justifier ce type de comportement.

Usurpation d'identité. A l'émission des messages HELLO, un nœud adversaire annonce (à travers le champ adresse d'origine) l'identité d'un autre nœud (la cible). Il en résulte que tous les nœuds voisins de l'adversaire

considéreront le nœud ciblé identifié dans le message HELLO comme étant un de leur voisin direct. De plus, tous les nœuds MPR de l'adversaire se présenteront eux-mêmes comme le dernier saut vers le nœud cible ce qui entrainera des conflits dans les annonces de routes.

Usurpation de liens. Une première altération consiste en l'annonce dans les messages de contôle HELLO d'un ensemble d'informations erroné sur l'état des liens avec des voisins, et plus précisément l'annonce de relations de voisinage non-existantes. Selon la manière dont est menée cette altération (à savoir augmentation des chances de l'adversaire de se faire élire MPR par ajout de tous les voisins à un saut des voisins du nœud ciblé), des répercutions peuvent apparaître sur l'opération de sélection des relais multi points pour les nœuds présents dans le voisinage de l'adversaire et par conséquent peut entraîner une redirection de tous les trafics des nœuds ciblés vers l'adversaire. En tant que nœud MPR, un adversaire pourra par la suite manipuler les trafics. Le second impact est l'établissement incorrect de l'ensemble du voisinage à deux sauts (puisque construit sur des informations d'état de liens incorrectes).

Une seconde altération consiste en la suppression dans les messages HELLO de liens existants entre l'adversaire et ses voisins directs. Selon la redondance des routes disponbiles dans le réseau, les nœuds voisins ignorés peuvent être soumis à des pertes en connectivité avec le reste du réseau. Cette altération a également pour impact de rendre les nœuds cibles voisins non atteignables directement par l'adversaire et vis-versa. Le trafic est redirigé et des routes plus longues doivent être établies!

Dans un message HELLO, l'état d'un lien est soit asymétrique (caractérise le fait que la relation est directionnelle), soit symétrique (caractérise le fait que la relation est bidirectionnelle), soit perdu (caractérise le fait que la relation n'est plus valide). L'altération de l'état des liens (LINK_TYPE) avec les nœuds présents dans le voisinage de l'adversaire conduit à des effets similaires à l'ajout ou la suppression de voisins.

Un nœud adversaire a également la possibilité d'annoncer dans ses messages HELLO l'ensemble de ses voisins comme étant nœuds MPR. Dans cette attaque, le mécanisme d'optimisation d'OLSR qui consiste à réduire au strict minimum le nombre de nœuds relais multi points afin de couvrir l'ensemble des nœuds situés à deux sauts n'est pas exploité. Ceci conduit à une augmentation locale du nombre de messages TC échangés. En effet, tous les nœuds situés à un saut de l'adversaire vont générer un message TC annonçant l'adversaire comme adresse de destination.

1.2.2 Altération des messages de contrôle de type TC

Génération. Dans les spécifications du protocole de routage OLSR, il est précisé que seuls les nœuds sélectionnés comme MPR génèrent des messages de contrôle TC. Aucun mécanisme n'est prévu pour vérifier si l'origine d'un message TC est un nœud MPR pour la liste des adresses déclarées. Par conséquent, un nœud adversaire peut actuellement envoyer des messages TC sans être sélectionné comme nœud MPR par son voisinage. L'impact de cette attaque est la définition de routes qui passeront potentiellement par l'adversaire (+ conflit dans les annonces de routes).

Usurpation d'identité. Une usurpation de l'adresse source (Originator Address) dans les messages TC a pour conséquence l'annonce incorrecte dans le réseau de relations de voisinage.

Usurpation de liens. Une attaque par usurpation de liens peut être menée soit dans la phase de génération soit dans la phase de retransmission des messages TC. Dans l'usurpation de lien, nous pouvons distinguer deux types d'altération : soit l'ajout de liens non-existants soit la suppression de liens existants. La suppression de liens existants conduit au même résultat que la suppression de messsages TC, à savoir une non dissémination des informations sur l'état des liens les concernant (+ une perte de connectivité pour les nœuds ignorés dans la signalisation des messages TC), et ce uniquement pour les nœuds dont les adresses ont été supprimées. Par l'ajout de liens non-existants, la distance entre le nœud adversaire et le(s) nœud(s) ciblé(s) va être réduite à un saut (+ conflits dans les annonces de routes).

1.3 Résumé des attaques sur le protocole OLSR

Le tableau 1 présente un résumé des attaques et de leurs impacts sur le protocoles de routage OLSR .

			Conflit de routes	Perte de connecti-vité	Perte de messages	Cible
Génération du trafic incorrecte	HELLO	Usurpation d'identité	X	X	X	Tous les nœuds
		Usurpation de lien	X	X		Nœuds dans le voisinage direct de l'adversaire
	TC	Usurpation d'identité	X	X	X	Tous les nœuds
		Usurpation de lien	X	X		Sous-ensemble de nœuds
	Attaque ANSN			X (partitionnement du réseau)	X	Sous-ensemble de nœuds
Relayage du trafic incorrecte	Modification de message		X	X		
	Trou noir			X	X	Nœuds spécifiques
	Rejeu		X	X	X	
	Trou de ver			X		Sous-ensemble de nœuds à proximité du trou
	MPR			X	X	Nœuds spécifiques

TAB. 1 – Résumé des attaques sur le protocoles OLSR

2 Mécanismes de contre-mesures pour la génération incorrecte des trafics de contrôle

Introduction Les récents efforts de recherche abordant la sécurisation des réseaux mobiles ad hoc se sont orientés vers la définition d'architecture de gestion de clés.

2.1 Authentification

Certaines propositions de sécurisation des protocoles de routage sont fondées sur l'établissement et l'emploi de clés cryptographiques pour assurer des propriétés de sécurité telles que l'authentification, la confidentialité et l'intégrité des échanges dans la phase de découverte de la topologie du réseau ainsi que dans la phase de retransmission des messages de données. Des exemples de ces protocoles sont SEAD (extension de sécurité pour la protocole DSDV où il est proposé une protection contre des altérations des champs mutables, à savoir le champ *métrique* et le champ *numéro de séquence*), secure OLSR (extension de sécurité pour OLSR), ARIADNE, ARAN (Royer ?), etc.

Critique des extensions de sécurité fondées uniquement sur l'authenticité des nœuds dans un réseau. Dans la majorité des cas, ce type d'extension vise essentiellement à discriminer les nœuds qui font partie du réseau des nœuds qui n'en font pas partie. Seuls les nœuds en possession des outils cryptographiques valides (c'est à dire des autorisations nécessaires : credentials) peuvent participer aux opérations de routage.

Les inconvénients majeurs des méthodes proposées est qu'elles reposent sur une infrastructure de gestion des clés plus ou moins adaptée à l'environnement des réseaux mobiles ad hoc et qu'elles ne traitent pas les problèmes relatifs aux comportements (parfois non conformes au regard des spécifications) des nœuds internes au réseau.

2.2 Approches basées cryptographie : An Advanced Signature System for OLSR

Objectifs de sécurité. L'objectif en terme de sécurité du système proposé est d'empêcher la modification (par ajout de liens non-existants) des messages de contrôle de type HELLO et TC du protocole de routage OLSR par des adversaires internes au réseau. (Impact direct) Assurer l'intégrité du réseau et portentiellement éviter les nœuds malveillants dans la phase d'établissement des routes.

Principe général. L'approche est fondée sur l'injection d'une information de contrôle authentifiée dans le réseau, et la réutilisation de cette information par un nœud pour prouver son état de lien lors d'une prochaine étape. Modèle basé sur l'existence de relations atomiques dans la phase d'établissement de liens : l'état du lien entre deux nœuds au temps t_{i+1} dépend de l'état du lien au temps t_i. Ainsi, les certificats émis à un temps t_i servent de preuves afin de garantir, lors d'un échange au temps t_{i+1}, l'état d'une relation entre deux nœuds. (Reprendre la diagramme de transitions des états de liens d'OLSR.)

Un message additionnel nommé ADVSIG est couplé avec les messages de contrôle de type HELLO et TC. Chaque message ADVSIG contient des certificats et de preuves de certificats. Un certificat est inclus uniquement dans les messages de contrôle de type HELLO et est composé de l'adresse d'un voisin, de l'information sur l'état du lien avec ce voisin, de l'estampille de temps de création et d'une signature établie par l'initiateur. Une preuve, inclus dans les messages de contrôle HELLO et TC, contient l'adresse de l'initiateur du message, l'information de l'état de lien avec un voisin, l'estampille de temps de création et la signature produite par un voisin.

Chaque nœud, sur réception d'un message de contrôle (de type HELLO ou TC), extrait et stocke les informations atomiques du message ADVSIG le concernant et signées par le voisin initiateur du message. Ces informations collectées à un temps t_i vont constituer une preuve à un temps t_{i+1} de l'existence d'une relation d'état de lien entre deux nœuds. Lorsqu'un nœud émet un message HELLO à un temps t_{i+1}, il doit joindre les preuves fournies par chacun de ses voisins à un temps $t_i$afin d'apporter une preuve sur l'état de leur relation au temps t_i. .

Avantages. Les auteurs prétendent que leur solution ne demande pas de modification des messages standard du protocole OLSR. Les signatures et estampilles temporelles permettent de contrecarrer les attaques de type rejeu et altération des messages.

Inconvénients. Une infrastructure à clé publique (PKI) est requise de sorte que chaque nœud soit en possession d'une identité (clé publique) prouvable/vérifiable par tous les autres nœuds du réseau . Les identités sont un élément fondamental dans le modèle proposé car c'est sur elles que reposent la génération des signatures globales des messages ADVSIG, l'établissememnt des certificats ainsi que la vérification de la validité des certificats/preuves. A partir du moment où des attaques par usurpation, vol d'identité ou encore pis, par échange d'identité entre des nœuds en coalition sont possibles, alors les services de securité offerts par le modèle deviennent caducs. Un algorithme de synchronisation faible/forte est requis pour la phase de vérification des estampilles de temps entre les nœuds. Par ailleurs, le mécanisme ne présente pas de protection face à des attaques menées par des coalitions d'adversaires. Des surcoûts induits par les opérations de calculs et de vérifications des signatures numériques conduisent à des pertes notables de messages. Ces résultats sont présentés dans l'étude de Lin Chen et al [1].

Une autre faiblesse de cette approche soulevée par Chen vient du fait qu'aucun certificat et preuve de certificat n'est requis dans la phase de déclaration d'un lien asymétrique entre deux nœuds. Il en résulte qu'un nœud est en mesure, de par une fausse déclaration d'un lien asymétrique, de conduire un autre nœud à croire qu'il existe une relation symétrique (bidirectionnelle). La méthode proposée par le auteurs pour remédier à ce problème présente l'inconvénient majeur de n'être valide que sous l'hypothèse d'un modèle d'attaquant définit par une absence de coalition.

2.3 Approche basée système d'identification d'intrusion

Principe général des méthodes basées sur des IDS. Détection d'anomalie par l'observation (locale) du comportement des nœuds.

Dans [3], il est fait une proposition simple de sécurisation contre les attaques : (1) par fabrication/modification de messages TC avec des annonces de liens non-existants (l'objectif de l'adversaire est d'aquierir des privilèges en se faisant passer pour un nœud MPR alors qu'il ne l'est pas) ; (2) par modification des informations d'état de liens dans les messages HELLO (l'objectif de l'adversaire est d'augmenter ses changes d'élection en tant que MPR en ajoutant de liens symétriques non-existants).

Méthode de détection. (Basée sur la nature diffuse des messages TC à l'ensemble des nœuds du réseau). Dans la méthode proposée, lorsqu'un nœud reçoit un message TC avec une annonce de son adresse d'interface dans la liste des « Advertise Neighbor », il vérifie dans sa base locale de connaissance si l'origine du message est bien connue de lui en tant que MPR selector ou pas. Dans le cas négatif, une anomalie est détectée et un message d'alarme est diffusé sur le réseau pour informer les autres nœuds.

Méthode pour limiter les attaques par diffamation. La solution proposée repose uniquement sur le nœud ciblé pour la phase de détection des anomalies. De nouveaux flux incohérents peuvent être introduits par des adversaires qui forgeraient des messages d'alertes contre les nœuds honnêtes du réseau. Pour faire face à ce problème, les auteurs proposent que la détection des anomalies soit réalisée de concert entre les nœuds à un saut du nœud ciblé, en plus du nœud ciblé lui-même.

Remarques. La méthode proposée ne permet pas de localiser une attaque (les messages peuvent être forgés par n'importe quel nœud du réseau). Ceci complexifie la phase de discrimination entre les nœuds conformes et les nœuds défaillants). De toute évidence, sans identité avec propriétés de sécurité fortes (liste), le mécanisme proposé ne présente qu'un faible intérêt.

La méthode de détection des anomalies dans les messages HELLO est identique. Un nœud voisin du nœud ciblé peut détecter l'attaque puisqu'il connaît l'état des liens du nœud ciblé à partir des messages HELLO qu'il reçoit périodiquement et directement de ce dernier. Un des inconvénients de cette approche est que des messages d'alerte doivent être disséminés à travers le réseau afin que chaque nœud puisse prendre des décisions de routage adaptées (évitement des nœuds considérés comme défaillants/suspicieux). Cependant, il n'est pas précisé comment les messages d'alerte doivent être gérés. Bien que les nœuds présentant un comportement défaillant peuvent être évités dans la phase de sélection des MPR (donc dans la construction des routes) ...

2.4 Approche basée sur la correlation des informations contenues dans les messages HELLO et TC

(Synthèse : système de contrôle de conflits basé sur les informations redondantes disséminées dans les messages de contrôle - il s'agit d'une généralisation de la méthode proposée précédemment) Dans cette catégorie de mécanisme de contre-mesure, aucune modification du protocole n'est requise. L'idée proposée intialement par Wang et al. dans [8] et puis reprise par Cuppens dans [2] est de dériver des propriétés de sécurité pour le protocole OLSR à partir de la corrélation des informations contenues dans les messages HELLO et TC. Les relations/règles qui doivent être vérifiées pour qu'une information soit considérée comme valide sont les suivantes : (1) la relation HELLO-TC définit que chaque nœud annoncé MPR selector dans un message TC doit également être annoncé comme étant un voisin symétrique de l'originateur dans un message HELLO antérieur ; (2) la relation MPR-MPR définit qu'un nœud annoncé MPR selector dans un message TC doit avoir annoncé l'originateur dans le MPR_set d'un message HELLO antérieur ; (3) la relation intégrité des messages définit que dans la phase de retransmission des messages TC, l'en-tête OLSR ne doit subir aucune modification ; (4) la relation voisinage-MPR définit qu'un nœud originateur d'un message TC doit être annoncé dans les messages HELLO de chaque nœud déclaré MPR comme étant un de leur voisin symétrique.

Avantages. Ne requiert pas de modification du format des messages du protocole. Tentive de formalisation des relations extraites/dérivé à partir de la corrélation des informations contenues dans les messages HELLO et dans les messages TC. Il s'agit d'un raisonnement sur le protocole OLSR.

Inconvénients. Néanmoins, la validation de l'approche n'est pas formelle (l'efficacité de l'approche est vérifiée par l'expérimentation). La relation (4) requiert que chaque nœud puisse observer les retransmissions de ses voisins. Les coalitions d'adversaire ne sont pas étudiées.

2.5 Environnement de confiance (processeur sécurisé)

Afin d'assurer la véracité des informations disséminées à travers le réseau au moyen des échanges de messages de contrôle, nous proposons de déléguer certaines des opérations de routage à un tiers de confiance sécurisé. Ce tiers de confiance, embarqué sur chacun des nœuds faisant partis du réseau, est responsable des opérations fondamentales du protocole de routage telles que la génération et le traitement des messages de contrôle ainsi que le stockage des données collectées. Dans cette architecture, un nœud hôte joue un rôle (minimaliste) d'intermédiaire. En effet, il se charge uniquement de relayer les messages, à savoir émettre les messages générés

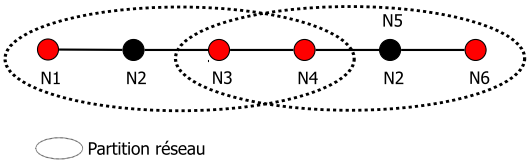

FIG. 2 – Attaque par duplication d'identité

par son tiers de confiance vers le réseau, puis transmettre les messages en provenance du réseau (reçus sur son médium de communication) à son tiers de confiance.

Avantages. Seules les informations de contrôle générées par les tiers de confiance sont considérées comme valides sur le réseau. En d'autres termes, un nœud adversaire n'est plus en mesure d'altérer directement (par modification des champs) l'état des liens avec ses voisins (soit par suppression ou par ajout).

Attaques possibles (à considérer dans la phase de retransmission). Bien que l'intégration d'un tiers de confiance offre des garanties fortes d'intégrité sur les contenus des messages de contrôle, des vulnérabilités résident dans les flux d'échange de messages entre le tiers de confiance et l'environnement hôte.

(Impact sur l'intégrité de la topologie) Un moyen de contourner l'architecture de sécurité proposée est pour un nœud hôte de ne pas jouer entièrement son rôle d'intermédiaire, soit en ne transmettant pas (ou en transmettant sélectivement) les messages fournis par son tiers de confiance vers le réseau (comportement de type 1) , soit en ne transmettant pas (ou en transmettant sélectivement) les messages de contrôle en provenance du réseau vers son tiers de confiance (comportement de type 2). Nous devons faire la distinction entre les messages HELLO qui sont des messages émis en diffusion locale (à un saut) et les messages TC qui sont inondés sur le réseau par l'intermédiaire des relais multi points.

Néanmoins, au regard des messsages HELLO, l'impact de l'attaque peut être considéré comme minimal puisqu'un nœud qui suivrait le comportement de type 1 ou 2 se retrouverait dans une position d'isolement (car non-découvert pas son voisinage). Du point de vue du réseau, ces deux types de comportement conduisent à une déformation de la vision locale du réseau pour les nœuds voisins de l'adversaire (bien que certaines rélations existent physiquement, elles ne sont pas détectées dans la phase de découverte qui repose sur des échanges de messages HELLO).

2.6 Résumé des solutions existantes et analyse

Dans cette section, nous analysons les vulnérabilités des mécanismes de contre-mesure présentés. Un des majeurs problème d'AdvSig vient du fait que les identités distribuées ne présentent pas de propriétés de sécurité fortes. De par la présence d'une infrastructure à clé publique, les identités sont certes validées et vérifiables mais leur stockage et leur manipulation est entièrement sous la gouvernance de leur hôte. Une conséquence à ceci est que des identités valides dans le réseau peuvent être échangées entre des nœuds en coalition. (question : le problème des identités est-il bien une faiblesse de la méthode AdSig vu que leur but de sécurité n'est à priori pas de proposer une solution pour remédier au problème de la génération, révocation, distribution des identités dans les réseaux mobiles ad hoc ?). L'utilisation d'une même identité par deux nœuds physiquement différents dans le réseau peut conduire à un partitionnement du réseau (perte en connectivité) et à des conflits de routes. Que se passe-t-il exactement lorsque deux nœuds physiquement différent dans le réseau utilise la même identité pour générer leurs messages de contrôle (HELLO et TC). Dans les spécification d'OLSR, il est précisé que le traitement des messages TC est basé sur la valeur de l'ANSN. Le rôle du champ ANSN dans les messages TC est de permettre à un nœuds de s'assurer que les informations d'état de liens reçues sont "fraiches" et qu'elles peuvent par conséquent être utilisées pour le calcul de la topologie du réseau. Les informations de lien déclarées par chacun des deux nœuds sont correctes au regard des spécifications d'OLSR. Or comme le traitement des messages TC repose sur la valeur du champ ANSN, les informations de lien ne seront pas disséminées sur l'ensemble du réseau.

La figure 2 illustre une configuration réseau où N2 et N5 sont en coalition. N5 utilise l'identité de N2 pour l'émission de ses messages de contrôle (HELLO et TC). Au lieu de sélectinonner N2 et N4, N3 sélectionne uniquement N2 en tant que MPR. Il en est de même pour N4 qui, au lieu de sélectionner N5 et N3, sélectionne uniquement N5 (vu comme étant N2) en tant que MPR. Au respect des spécifications d'OLSR, puisque N4 a un ensemble de MPR selector vide, tous les messages TC émis par N5 et reçu par N4 ne seront pas disséminés plus

			AdvSig [6]	Environnement ou tiers de confiance	Propriétés sémantiques du protocole OLSR [8, 2]
Génération du trafic incorrecte	HELLO	Usurpation d'identité	Non, car les identités ne sont pas scellées	Oui	Oui
		Usurpation de lien	Oui	Oui	Oui
	TC	Usurpation d'identité	Non, car les identités ne sont pas scellées	Oui	Oui
		Usurpation de lien	Oui	Oui	Oui
	Attaque ANSN		Non	Oui	Non
Relayage du trafic incorrecte	Modification de message		Oui	Oui	En partie
	Trou noir		Non	? ? ? Possible	Non
	Rejeu		Oui	Oui	Non
	Trou de ver		Non	? ? ? Peut-être par une méthode d'emprunt couplée à une gestion des identités	Non
	MPR				
Besoins	Centralisation		Infrastructure à clé publique	Non	Non
	Synchronisation		Oui : doit elle être précise ou pas ?	Non	Non
	Matériel spécifique		Système de positionement : coordonnées géographique des nœuds obtenues par GPS	Processeur sécurisé embarqué sur chaque nœuds	
Remarques					Pas d'évaluation des propriétés des sécurité atteintes
Surcoûts introduits par le mécanisme			Importants en terme de calcul		Négligeables ? Seulement des traitements sur les messages

TAB. 2 – Résumé des solutions existantes

loin dans le réseau. Il en sera de même pour tous les messages TC émis par N2 et reçu par N3. Par conséquence, les nœuds N5 et N6 ne seront pas connus des nœuds N1 et N2, et vis-versa.

2.6.1 Introduction à la comprimission des clés cryptographiques et de l'attaque dite Sybil

Un adversaire en possession d'une clé compromise peut fabriquer et injecter des messages légitimes dans le réseau.

3 Mécanisme de contre-mesure pour la retransmission incorrecte des trafics de contrôle

3.1 Contre-mesure de l'attaque par isolation de nœud

Description. Le mode opératoire de cette attaque est décrit dans [?]. Le but de cette attaque est d'empêcher un nœud ciblé de recevoir des messages en provenance d'autres nœuds du réseau.

Le principe est le suivant : un adversaire empêche la diffusion sur le réseau complet des informations de lien d'un nœud spécifique ou d'un groupe de nœuds. Par conséquent, les autres nœuds du réseau : (1)

ne recevront aucune information de lien concernant les nœuds ciblés ; (2) ne seront pas capables de construire une route vers les nœuds ciblés ; (3) ne seront pas capables d'envoyer des données vers les nœuds ciblés.

A l'étape E0, l'adversaire doit découvrir les voisins à 2-sauts du nœud ciblé. Pour ce, il analyse des messages TC des voisins à 1-saut de sa cible. (remarques sur les hypothèses prises sur le réseau : l'adversaire communique avec l'ensemble des voisins du nœud cible ? par ailleurs, pourquoi ne pas utiliser les messages HELLO ?). A l'étape E1, l'adversaire crée un message HELLO en incluant la liste d'adresses des voisins à 2-sauts de la cible découverts précédemment. A l'étape E2, selon le protocole, la cible sélectionnera l'adversaire comme son seul MPR. Il est à noter que le seul nœud qui aura pour charge de générer et retransmettre les messages TC pour la cible sera l'adversaire. A l'étape E3, l'adversaire, par suppression des messages TC en provenance du nœud cible et par non génération des messages TC pour le nœud cible, peut empêcher la dissémination sur le réseau complet des informations de lien du nœud cible.

Résultat : les autres nœuds du réseau ne vont recevoir aucune information de lien relative au nœud cible et vont par conséquent en conclure que le nœud ciblé n'existe pas dans le réseau.

Dans OLSR, au moyen des messages HELLO, chaque nœud peut obtenir des informations de connectivité à 1 et 2 sauts : le nœud cible ne pourra plus recevoir de messages en provenance des nœuds situés à 3-sauts ou plus.

Besoin : l'adversaire ne peut mener cette attaque que lorsque le nœud ciblé est dans son champ de transmission.

Phase de détection. La méthode est basée sur une observation locale des messages TC émis par les nœds sélectionnés comme MPR.

Un nœud vérifie que ses nœuds voisins sélectionnés en tant que MPR génèrent correctement leurs messages TC. Si un nœud détecte qu'un de ses MPR ne signale pas correctement son adresse dans ses émissions de messages TC, il considère le nœud MPR comme suspect (sachant qu'avant de suspecter un nœud MPR, une vérification sur l'état du lien est réalisée au moyen des messages HELLO). Si l'observation de ce comportement suspect se répète, alors le nœud MPR est considéré comme malveillant.

Remarque de moindre importante : l'attaque ne peut plus être détectée par la cible en cas d'utilisation d'antenne directionnelle par l'adversaire.

Phase d'évitement. Les auteurs exposent le problème de l'attribution d'une identité pour un nœud dans un réseau mobile ad hoc (sans mécanisme d'authentification, un nœud peut soit usurper l'identité d'un autre nœud ce qui a pour conséquence la fausse accusation d'un nœud légitime dans le réseau, soit changer d'identité pour se défaire d'une mauvaise réputation ce qui a pour conséquence l'inopérance du mécanisme d'expulsion de nœuds) et propose, pour faire face à ce problème, une méthode simple d'évitement de nœuds malveillants. Les objectifs de sécurité sont d'atténuer les pertes dues à l'attaque présentée précédemment et par conséquent améliorer les performances du réseau. Pour ce, dans la méthode proposée, il est question de modifier légèrement les messages de contrôle de OLSR.

Afin d'éviter l'attaque décrite précédemment, lorsqu'un nœud détecte une anomalie, il demande à l'ensemble de ses voisins directs de retransmettre ses informations de liens. Par ce biais, un œud s'assure que ses informations

de lien sont propagées sur le réseau (remarque : les auteurs partent de l'hypothèse qu'il y a au moins un nœud bienveillant dans le voisinage du nœud ciblé par l'attaque). La méthode requiert l'ajout d'un champ « Request_value » dans les messages HELLO. Les valeurs admises pour le champ « Request_value » sont 0 (valeur par défaut) ou 1, la valeur 0 indiquant aux nœuds qui reçoivent le message HELLO qu'ils doivent suivre normalement le protocole OLSR, et 1 indiquant aux nœuds qu'une anomalie a été détectée et que par conséquent, ils doivent ajouter l'adresse de l'interface de l'origine du message HELLO dans le champ « Advertised Neighbours » de leur messages TC.

Vulnérabilités de l'approche proposées. Premièrement, un adversaire peut exploiter ce mécanisme en initialisant à « 1 » le champ « Request_value » dans chacun de ses messages HELLO. Par conséquent, tous les voisins de l'adversaire seront pas MPR pour ce dernier. Deuxièmement, il est fait l'hypothèse de communications omnidirectionnelles. Un adversaire doté d'une antenne directionnelle peut détourner le mécanisme de contrôle en faisant en sorte de paraître en conformité avec les opérations du protocole : en effet il a l'opportunité d'émettre ses messages TC uniquement en direction du nœud voisin intéressé (le contrôleur).

3.2 Environnement de confiance

Au regard de l'opération de retransmission des messages de contrôle, nous proposons l'ajout d'informations additionnelles vérifiables uniquement par les tiers de confiance. Nous partons du principe que nous ne pouvons pas évaluer de manière fine l'origine (à savoir la source ou la destination) d'un défaillance (caractérisée par une perte de messages) sur un lien de communication. (Expliquer d'où viennent ces incertitudes - l'intégration d'un tiers de confiance ne permet ni le contrôle des flux d'informations sortant ni le contrôle des flux d'information entrant - nous ne pouvons pas faire la distinction entre une perte due à une non-émission par l'environnement hôte sur le réseau des messages générés par le tiers confiance et une perte due à une non-retransmission par l'environnement hôte des messages en provenance du réseau vers le tiers de confiance distant). Ainsi, plutôt que de viser l'évaluation locale du comportement d'un nœud, nous optons pour une évaluation locale de l'état des liens entre les nœuds à partir des échanges de messages.

Applications possible. Nous abordons dans cette section comment, à partir des informations de contrôle additionnelles, nous pouvons vérifier l'état d'un lien entre deux nœuds[1]. Le déroulement du protocole est le suivant : lorsqu'un tiers de confiance d'un nœud génère un message à destination d'un ou plusieurs autres nœuds voisins, des informations identifiant d'une part le message et d'autre part les nœuds visés, sont maintenues par le tiers de confiance. Le tiers de confiance initiateur du message passe alors dans un état d'attente des réponses en provenance de l'ensemble des tiers de confiance des nœuds visés. Sur réception du message, un accusé de réception est généré par le tiers confiance de chaque nœud visé et présent dans le voisinage de l'originateur. La réception d'un accusé de réception par le tiers de confiance permet de valider l'échange ainsi que le lien (passage d'un état d'attente à un état de lien valide pour le message et le nœud considéré).

---

1. $T_{N_1} \rightarrow \{X_1, ..., X_n\} : M(id_i) \Rightarrow U_{N_1} \rightarrow \{X_1, ..., X_n\} : M(id_i)$; pour chaque nœud visé, T_{N_1} passe dans un état d'attente de réponse ACK pour le message émis ; (vulnérabilité à l'émission) dans le cas où le message ne serait pas émis sur le réseau suite à une rupture dans le flux de communication déclanchée par l'environnement hôte du nœud N_1(non-émission sur le réseau du messages M généré par T_{N_1}, alors les liens avec l'ensemble des voisins visés seront considérés comme dégradés (et déclarés comme tel dans la phase de génération des messages d'annonce HELLO) ; la conséquence directe est qu'un nœud optant pour un tel comportement se retrouve isolé du réseau.
2. $U_{X_1} \leftarrow U_{N_A} : M(id_i) \Rightarrow T_{X_1} \leftarrow U_{N_1} : M(id_i) \Rightarrow T_{X_1} \rightarrow N_1 : ACK(M(id_i) \Rightarrow U_{X_1} \rightarrow N_1 : ACK(M(id_i))$; lorsque l'environnement hôte du nœud X reçoit le message M, il peut soit le retransmettre à son tiers de confiance T_X, soit le supprimer. S'il prend la décision de le supprimer, alors le nœud N_1(ne recevant pas d'accusé de réception de la part de X) considérera le lien avec ce dernier comme dégradé (ceci conduit à une perte de connectivité à la fois pour les nœuds N_1 et X ; En revanche, s'il prend la décision de retransmettre le message à son tiers de confiance, alors un accusé de réception pour le message M et à destination de N_1sera généré. La non-émission de l'accusé de réception par le nœud X sur le réseau conduit au même résultat que la non-transmission du message à son tiers de confiance.
3. $U_{N_1} \leftarrow U_{X_1} : ACK(M(id_i)) \Rightarrow T_{N_1} \leftarrow U_{X_1} : ACK(M(id_i))$; la réception d'un accusé de réception pour un message donné et un nœud donné signifie que le lien est valide et qu'il peut continué à être exploité

[1] Il est à noter que nous faisons la distinction entre l'état d'un lien obtenu à partir des échanges de messages HELLO dans la phase de découverte et l'état d'un lien tel qu'il est évalué à partir soit des échanges de messages TC ou des messages de données.

pour les échanges futurs ; dans le cas où un accusé de répcetion n'est pas retransmis au tiers de confiance du nœud N_1, alors le lien avec l'originateur de l'accusé de réception est considéré comme dégradé.

Avantages. L'idée de base consiste à évaluer localement la fiabilité des liens entre les nœuds à partir des échanges de messages. Un avantage est qu'il n'est pas nécessaire de disséminer des rapports d'anomalies à travers le réseau : les décisions sont prises localement.

Inconvénients. Une modification du protocole par ajout de messages ACK. L'approche introduit des surcoûts importants en terme de paquets émis. A évaluer plus finement car cela dépend de la manière dont nous générons les accusés de réception. Nous pouvons par exemple envisager d'ajouter les accusés de réception dans les messages HELLO qui sont diffusés en broadcast.

4 Mécanismes de contre-mesure pour l'attaque du trou de ver

La particularité de l'attaque du trou de ver est qu'elle ne nécessite aucune modification des messages de la part de l'adversaire. La conséquence directe est qu'aussi bien les nœuds légitimes (c'est à dire les nœuds en possession des autorisations nécessaires pour participer aux opérations réseau) que les nœuds illégitimes peuvent la mettre en œuvre. Par conséquent, bien que l'ensemble des mécanismes de sécurisation des protocoles de routage basés sur des méthodes cryptographiques offrent des garanties de sécurité en terme de confidentialité, d'authenticité, et d'intégrité des messages, ils ne sont pas résistants à ce type d'attaque. Cette attaque affecte tout particulièrement les protocoles s'appuyant sur une phase de découverte de voisinage direct par échange de messages de contrôle pour les rôles et les chemins entre les nœuds. Elle peut mener à des conflits dans les relations de voisinage établies. Les moyens actuellement proposés dans la littérature sont les suivants :

- Contre-mesure au niveau de la couche physique ;
- Module matériel spécifique et fenêtre de temps ;
- Synchronisation d'horloge lâche et positionnement géographique des nœuds ;
- Synchronisation d'horloge fine et fenêtre de temps ;
- Antennes directionnelles ;

4.1 Contre-mesure au niveau de la couche physique

Les premiers travaux traitant l'attaque du trou de ver reposent sur un matériel et des techniques de traitement du signal. Il est suggéré une méthode secrète de modulation de bits du signal radio. Le signal peut uniquement être démodulé par des nœuds autorisés. Une vulnérabilité de cette méthode vient du fait que la méthode n'est pas conservée dans un espace de confiance, ce qui peut conduire des adversaires non-autorisés à compromettre des nœuds légitimes dans le réseau pour obtenir les accès nécessaires, ou bien des adversaires autorisés à divulguer leur connaissance de la méthode. (Il pourrait être envisagé des mécanismes complémentaire de sécurisation du code de modulation/démodulation telle que l'obfuscation, ou bien l'emploi d'un environnement resistant à l'altération). En termes de sécurité, cette méthode permet seulement une défense contre l'attaque du trou de ver menée par des nœuds adversaires extérieurs (non-autorisés) au réseau, c'est à dire des nœuds qui ne possèdent pas les clés cryptographiques. Se pose également la question de l'établissement/de la négociation de la méthode secrète entre les nœuds légitimes dans le réseau.

4.2 Synchronisation d'horloge et fenêtre de temps : Packet leashes

Packet leashes est une solution de détection de l'attaque du trou de ver proposée par Hu et al. [5]. Un leash est une information (de temps ou de positionnement géographique) qui est incluse dans chacun des paquets émis sur le réseau et qui sert à restreindre leur distance maximale autorisée de transmission. Deux méthodes d'utilisation des leashes sont présentées : une première basée sur le support d'un service de positionnement géorgraphique et une seconde basée sur une synchronisation d'horloge précise (fine) entre les nœuds.

Leashes géographiques. Les leashes géographiques permettent d'assurer la distance entre le récepteur et l'émetteur d'un message. Le mécanisme requiert d'une part que chaque nœud connaisse sa propre position géographique, et d'autre part que les horloges de tous les nœuds soient lâchement synchronisées (de l'ordre de la milliseconde). A l'émission d'un message, le nœud émetteur inclut dans le message une version authentique de

sa propre position géographique et l'heure d'émission. Un nœud récepteur utilise les informations de leashes encapsulées dans le message reçu ainsi que sa propre position géographique et l'heure de réception du message enregistré pour estimer une borne supérieure de la distance avec l'émetteur. En prenant en considération certaines variables telles que la vélocité maximale des nœuds, l'erreur maximale dans le système de synchronisation d'horloge, et l'erreur maximale possible dans le système de positionnement géographique, la borne supérieure de la distance entre l'émetteur et le récepteur peut alors être déterminée. Dans le cas où la distance calculée est supérieure à la portée maximale de transmission, alors le lien est probablement faux.

Une des limitations de cette méthode vient du fait qu'elle repose sur un système de positionnement géographique. En effet, la technologie GPS est actuellment inopérante dans les environnements clos (tels que les immeubles), les environnement sous-marins, les environnements soumis à un fort rayonnement magnétique, etc. Se pose également la question de la précision des informations de positionnement fournies par la technologie GPS. Les auteurs précisent que selon l'état de l'art dans la technologie GPS, il est possible d'atteindre une précision d'environ 3 m.

Leashes temporelles. Les leashes (laisses) temporels(les) assurent que chaque message transmis à travers le réseau encapsule une borne supérieure sur sa durée de vie. Un paquet reste valide sur le réseau tant que le temps d'expiration n'est pas dépassé, après quoi le paquet est rejeté. Un des prérequis non-négligeable de la méthode est une synchronisation d'horloge précise entre tous les nœuds du réseau. Selon cette méthode, un émetteur inclut dans chaque message une version authentique de l'heure d'émission. Dans la phase de vérification, un récepteur compare cette valeur à l'heure de réception du message. Dans une variante des leashes temporelles, un émetteur détermine le temps d'expiration à partir duquel un message ne doit plus être accepté, puis inclu cette information dans le leash. En résumé, la méthode s'appuie sur le temps de parcours d'un message puis sur la vitesse de la lumière pour déterminer sa distance approximative de parcours. Une hypothèse implicite est que les délais de traitement des messages, d'émission et de réception sont négligeables.

Discussion. Aussi bien l'approche basée sur les leashes temporels que celle basée sur les leashes géographiques requierent l'ajout de données d'authentification pour chaque message afin de protéger les leashes (contre l'usurpation d'identité et la modification). L'authentification indroduit un surcoût en terme de traitement et de temps (du fait des opérations de haché, de vérification et de signature des messages entrants et sortants). Tandis que les auteurs discutent de mécanismes pour amélioration de l'efficacité des opérations de signature, il n'est précisé que les délais leur sont associés peuvent potentiellement rendre la borne imprécise et non-fiable. Un surcoût en terme de communication est essentiellement du à l'ajout d'un protocole d'authentification avec distribution/échange de clé. Enfin, une capacité de stockage importante pour le schéma d'authentification basé sur un arbre de haché est requise (à quantifier !).

4.3 Positionnement géographique

Antennes directionnelles. Les nœuds équipés d'antennes direcitonnelles utilisent des secteurs (au nombre de 8, à savoir N, S, E, W, NE, NW, SE, SW) pour communiquer entre eux. Un nœud qui reçoit un message de l'un de ses voisins obtient une information aproximative (N, S, E, W) concernant sa position : il connait l'orientation relative de son voisin par rapport à lui-même. Ce sont ces bits d'information additionnels (angle d'arrivée du signal) qui sont exploités dans certaines méthodes pour faciliter la détection/découverte des trou de ver.

Dans [4], Hu et Evans proposent une méthode de vérification du voisinage au moyen d'antennes directionnelles. Les nœuds voisins examinent la direction du signal reçu pour chacun des autres nœuds et partage un témoin. La relation de voisinage est confirmée uniquement lorsque les directions de l'ensemble des paires concordent.

4.4 Module matériel spécifique et fenêtre de temps

Dans [7], il est supposé que chaque nœud est équipé d'un matériel spécifique capable de répondre sans délai à un défi sur 1-bit. Le challenger mesure le temps de parcours du signal avec une horloge précise pour calculer la distance entre les nœuds. (Il est précisé que la probabilité qu'un adversaire puisse deviner tous les bits correctement diminue exponentiellement lorsque le nombre de défis augmente.)

Hypothèses : (0) les nœuds communiquent entre eux via des transmissions radio ; deux nœuds sont considérés comme étant voisins s'ils sont à porté de transmission ; (1) chaque nœud a une horloge local et les horloges entre les nœuds sont faiblement (lâchement) synchronisées (la différence d'horloge entre deux nœuds du réseau est

inférieure à 1 seconde). Pour obtenir une synchronisation d'horloge faible, les auteurs reportent les lecteurs sur "Time synchronization in ad hoc networks, K. Romer" ; (2) chaque nœud est équipé d'un module matériel spécifique qui permet de temporairement d'assurer le contrôle de l'unité d'émission/réception (transceiver) radio à partir du CPU. Gâce à ce module matériel, un nœud peut recevoir un unique bit, exécuter une opération XOR sur deux bits, et ensuite retransmettre un unique bit sans impliquer le CPU d'un nœud (l'intérêt de ce module matériel spécifique est de passer outre le délais imposé la méthode habituelle de traitement des messages) ; (4) il n'est pas requis que les nœuds soient équipés d'un module de positionnement géographique ; (5) les nœuds sont capables de générer des clés cryptographiques, de vérifier des signatures, d'exécuter des fonctions de haché (c'est à dire accomplir toute tâche requise pour sécuriser ses communications) ; (6) le réseau opère avec une autorité centrale dont le rôle est de contrôler les associations au réseau et d'assigner une identité unique à chaque nœud ; cette autorité est soit en ligne (accessible au moyen de communications à 1 voire plusieurs sauts), soit hors ligne (non accessible par le réseau) ; (7) tous les nœuds du réseau possèdent soit les clés secrètes partagées par paires (par configuration à priori ou par l'utilisation d'un schéma probabiliste de distribution de clés, ou par un centre en ligne de distribution de clés couplé à l'authentification TELSA des messages de diffusion ou par un shéma d'établissement de clés basé sur la mobilité des nœuds et la rencontre mutuelle des nœuds) , soit les clés publiques authentiques de chacun des autres nœuds (par configuration à priori de tous les nœuds).

La technique proposée permet à une entité (le vérifiant) de déterminer une borne supérieure sur sa distance physique avec une autre entité (le prouvant). Elle est fondée sur deux éléments : sur le fait que la lumière se propage à une vitesse finie (environ 30cm par nanoseconde), puis sur le fait que les technologies actuelles permettent de mesurer localement les synchronisations (timings) avec une précision allant à la nanoseconde. Grâce à ces deux éléments, il est possible à partir du temps de voyage du signal sur un tour de dériver une borne supérieure de la distance physique entre un vérifiant et un provant. Elle requiert plusieurs échanges rapides de séries de bits entre le vérifiant et le prouvant (plusieurs tours d'échange de bits). Chaque bit émis par une première entité est considéré comme étant un défi pour lequel chaque autre entité doit émettre une réponse sur 1 bit immédiatement. Par une mesure locale du temps écoulé entre l'heure d'émission du défi et l'heure de réceptions des réponses, la première entité peut calculer une borne supérieure de la distance avec les autres entités. Les auteurs proposent une variante au protocole de Brands-Chaum nommée MAD (Mutual Authenticated Distance-bounding). Il s'agit d'un protocole à plusieurs tours qui permet d'estimer de manière sécurisée une borne de la distance entre une paire de nœuds.

Références

[1] Chen, L., Xue, X., and Leneutre, J. A lightweight mechanism to secure olsr. In *IMECS* (2006), pp. 887–895.

[2] Cuppens, F., Cuppens-Boulahia, N., Nuon, S., and Ramard, T. Property based intrusion detection to secure olsr. In *ICWMC '07 : Proceedings of the Third International Conference on Wireless and Mobile Communications* (Washington, DC, USA, 2007), IEEE Computer Society, p. 52.

[3] Fourati, A., and Khaldoun, A. A. An ids first line of defense for ad hoc networks. In *Wireless Communications and Networking Conference, WCNC 2007* (March 11–15 2007), IEEE, pp. 2619–2624.

[4] Hu, L., and Evans, D. Using directional antennas to prevent wormhole attacks. In *Proceedings of Network and Distributed System Security Symposium, NDSS' 2004, San Diego, California, USA* (San Diego, California, USA, 2004), The Internet Society.

[5] Hu, Y.-C., Perrig, A., and Johnson, D. B. Packet leashes : A defense against wormhole attacks in wireless networks. In *Proceedings of INFOCOM, Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies* (April 2003), vol. 3, pp. 1976–1986.

[6] Raffo, D., Adjih, C., Clausen, T., and Mühlethaler, P. An advanced signature system for OLSR. In *Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04)* (Washington, DC, USA, October 25 2004), ACM Press, pp. 10–16.

[7] Čapkun, S., Buttyán, L., and Hubaux, J.-P. Sector : secure tracking of node encounters in multi-hop wireless networks. In *SASN '03 : Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks* (New York, NY, USA, 2003), ACM Press, pp. 21–32.

[8] Wang, M., Lamont, L., Mason, P., and Gorlatova, M. An effective intrusion detection approach for olsr manet protocol. pp. 55–60.