Groupe de travail Réseau
Request for Comments : 4866
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

J. Arkko, Ericsson Research NomadicLab
C. Vogt, Universitaet Karlsruhe (TH)
W. Haddad, Ericsson Research
mai 2007

Optimisation de chemin améliorée pour IPv6 mobile

Statut du présent mémoire

Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

Le présent document spécifie une version améliorée de l'optimisation de chemin IPv6 mobile, fournisant de plus courts délais de transfert, une sécurité accrue, et des frais généraux de signalisation réduits.

Table des matières

1. Introduction....2
2. Objectifs....3
2.1 Latence de transfert....3
2.2 Sécurité....3
2.3 Frais généraux de signalisation....4
3. Conception du protocole....4
3.1 Adresses de rattachement générées cryptographiquement....5
3.2 Adresses d'entretien non cryptographiques....5
3.3 Associations de sécurité semi permanentes....5
3.4 Vérification d'adresse de rattachement initiale....5
3.5 Vérifications d'adresses d'entretien concurrentes....5
3.6 Autorisation fondée sur le crédit....6
3.7 Enregistrements parallèles de rattachement et de correspondant....6
4. Fonctionnement du protocole....6
4.1 Envoi de messages de mise à jour de lien....6
4.2 Réception des messages de mise à jour de lien....11
4.3 Envoi des messages d'accusé de réception de lien....13
4.4 Réception des messages d'accusé de réception de lien....14
4.5 Envoi des paramètres de CGA....15
4.6 Réception des paramètres de CGA....16
4.7 Envoi de jetons permanents de génération de clé de rattachement....16
4.8 Réception des jetons permanents de génération de clé de rattachement....16
4.9 Renouvellement des jetons permanents de génération de clé de rattachement....17
4.10 Traitement des paquets de charge utile....17
4.11 Vieillissement de crédit....19
4.12 Mouvements simultanés....19
5. Formats d'option et codes d'état....19
5.1 Option Paramètres de CGA....19
5.2 Option Signature....20
5.3 Option jeton permanent de générateur de clé de rattachement....20
5.4 Option Initiation de vérification d'adresse d'entretien....21
5.5 Option Essai d'adresse d'entretien....21
5.6 Option Demande de paramètres de CGA....21
5.7 Codes d'état....22
6. Considérations sur la sécurité....23
6.1 Propriété de l'adresse de rattachement....23
6.2 Propriété de l'adresse d'entretien....24

6.3. Autorisation fondée sur le crédit....25
6.4 Attaques de glissement de temps....27
6.5 Attaques en répétition....27
6.6 Épuisement des ressources....27
6.7 Possession d'adresse IP du nœud correspondant....28
7. Constantes et variables de configuration du protocole....28
8. Considérations relatives à l'IANA....29
9. Remerciements....29
10. Références....30
10.1 Références normatives....30
10.1 Références pour information....30
Adresse des auteurs....31
Déclaration complète de droits de reproduction....31

1. Introduction

L'optimisation de chemin IPv6 mobile [RFC3775] permet aux nœuds mobiles et correspondants de communiquer via un chemin d'acheminement direct en dépit des changements de connexité IP du côté du nœud mobile. Les deux nœuds d'extrémité utilisent une "adresse de rattachement" stable en identifiant le nœud mobile aux piles de protocoles au dessus de IP, tandis que les paquets de charge utile sont envoyés ou reçus via une "adresse d'entretien" qui achemine au rattachement réseau actuel du nœud mobile. IPv6 mobile échange les adresses de rattachement et d'entretien quand un paquet de charge utile traverse la couche IP. L'association entre l'adresse de rattachement et l'adresse d'entretien d'un nœud mobile est appelée un "lien" pour le nœud mobile. Il est de la responsabilité du nœud mobile de mettre à jour son lien au nœud correspondant par un "enregistrement de correspondant" quand il change sa connexité IP. Un enregistrement de correspondant implique de plus l'agent de rattachement du nœud mobile, qui sert de mandataire au nœud mobile à l'adresse de rattachement et sert principalement de relais pour les paquets de charge utile échangés avec les nœuds correspondants qui ne prennent pas en charge l'optimisation de chemin. Le nœud mobile garde l'agent de rattachement à jour sur son adresse d'entretien actuelle au moyen des "enregistrements de rattachement".

Du point de vie de la sécurité, l'établissement d'un lien durant un enregistrement de correspondant exige que le nœud correspondant vérifie que le nœud mobile possède les deux adresses de rattachement et d'entretien. Des menaces sans précédent d'usurpation d'identité et d'inondation [RFC4225] se feraient jour si les nœuds correspondants prenaient des libertés avec le respect de ces obligations. Un enregistrement de correspondant incorpore donc un "essai d'adresse de rattachement" et un "essai d'adresse d'entretien", appelés collectivement la "procédure d'acheminement de retour". Ces vérifications permettent au nœud correspondant de sonder l'accessibilité du nœud mobile aux adresses de rattachement et d'entretien d'une manière ad hoc, non cryptographique. La vérification réussie de l'accessibilité aux deux adresses IP indique (mais sans la garantir) la possession par le nœud mobile des adresses IP, et donc que le lien entre l'adresse de rattachement et l'adresse d'entretien est légitime.

L'avantage de la procédure d'acheminement de retour est qu'elle est légère et ne dépend pas d'une infrastructure de clé publique ou d'une relation préexistante entre le nœud mobile et le nœud correspondant. Cela facilite un large déploiement. Par ailleurs, la procédure a un impact négatif sur les délais de transfet car les deux essais d'adresse de rattachement et d'adresse d'entretien consistent en un échange de messages de bout en bout entre le nœud mobile et le nœud correspondant. La latence de l'essai d'adresse de rattachement peut être particulièrement élevée parce que il s'achemine à travers l'agent de rattachement. La procédure d'acheminement de retour est aussi vulnérable aux attaquants qui sont dans une position où ils peuvent s'interposer dans l'essai d'adresse de rattachement ou d'entretien. La valeur de l'interposition est limitée en ce que la procédure d'acheminement de retour doit être répétée à des intervalles d'au plus 7 minutes, même en l'absence de changement de la connexité IP sur le côté du nœud mobile. Mais c'est au prix de frais généraux accrus de signalisation. Beaucoup d'efforts ont donc été consacrés aux améliorations de l'optimisation de chemin IPv6 mobile [RFC4651] qui atténuent ces inconvénients.

Le présent document spécifie l'optimisation de chemin améliorée, un amendement à l'optimisation de chemin dans IPv6 mobile de base. L'optimisation de chemin améliorée sécurise l'adresse de rattachement d'un nœud mobile contre l'usurpation d'identité par un identifiant d'interface qui est lié cryptographiquement et est vérifiable [RFC3972] pour le composant public de la paire clé publique/privée du nœud mobile. Le nœud mobile prouve sa possession de l'adresse de rattachement en fournissant des preuves qu'il connaît la clé privée correspondante. Un essai initial d'adresse de rattachement valide le préfixe de l'adresse de rattachement ; des essais suivants d'adresse de rattachement sont inutiles. L'optimisation de chemin améliorée permet de plus au nœud mobile et aux nœuds correspondants de reprendre des communications bidirectionnelles en parallèle avec la poursuite d'un essai d'adresse d'entretien. La latence des essais d'adresse de rattachement et d'entretien est donc éliminée dans la plupart des cas. L'utilisation d'adresses de rattachement

générées cryptographiquement atténue aussi la menace qu'un usurpateur s'interpose dans l'essai d'adresse de rattachement et facilite ainsi de plus longues durées de vie de lien. Cela conduit à une sécurité accrue et à une réduction des frais généraux de signalisation. Les adresses de rattachement générées cryptographiquement et les essais concurrents d'adresse d'entretien sont de préférence appliqués ensemble, mais un nœud mobile peut choisir d'utiliser seulement une de ces améliorations.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Objectifs

Le concept d'optimisation de chemin dans IPv6 mobile de base est de nombreuses façons prudent, laissant de la place pour l'optimisation du delai de tansfert, de la sécurité, et des frais généraux de signalisation. L'optimisation de chemin améliorée touche à ces questions et constitue donc une variante plus progressive de IPv6 mobile.

En dépit de toutes les optimisations de IPv6 mobile, il est important de prendre en compte que les activités relatives à la mobilité ailleurs dans la pile de protocoles peuvent avoir leur propre impact. Par exemple, les procédures de rattachement, le contrôle d'accès, et l'authentification à la couche de liaison contribuent à leurs propres délais de transfert. Ainsi font aussi des tâches de couche IP comme la découverte de route, la découverte de voisin, la détection de mouvement, et la configuration d'adresse IP. Les délais de transfert et les frais généraux de signalisation de IPv6 mobile sont normalement petits comparés au délai et aux frais généraux totaux. Les améliorations de l'optimisation de chemin améliorée devraient donc être vues sur l'ensemble de la pile de protocole.

2.1 Latence de transfert

Le délai normal de transfert dans l'optimisation de chemin IPv6 mobile de base est d'un délai d'aller-retour entre le nœud mobile et l'agent de rattachement pour l'enregistrement de rattachement, un délai d'aller-retour entre le nœud mobile et l'agent de rattachement plus un délai d'aller-retour entre l'agent de rattachement et le nœud correspondant pour la procédure d'acheminement de retour, et un délai de trajet simple du nœud mobile au nœud correspondant pour la propagation du message de mise à jour de lien. (L'hypothèse ici est que la latence de la procédure d'acheminement de retour est dominée par l'essai d'adresse de rattachement.) Le premier paquet de charge utile envoyé à la nouvelle adresse d'entretien exige un délai de trajet simple supplémentaire pour se propager du nœud correspondant au nœud mobile. Le nœud mobile peut reprendre les transmissions juste après qu'il a expédié le message de mise à jour de lien. Mais si il demande un message d'accusé de réception de lien de la part du nœud correspondant, les communications sont généralement retardées jusqu'à sa réception.

Les délais de transfert dans l'optimisation de chemin IPv6 mobile de base sont à ajouter aux autres délais à la couche IP ou à la couche de liaison. Ils peuvent causer une dégradation de qualité perceptible pour les applications interactives et en temps réel. Les transferts de données TCP en vrac sont affectées de la même façon car les longues latences de tansfert peuvent conduire à des fins de temporisation de retransmission successives et un débit dégradé [IEEE]. Un objectif de l'optimisation de chemin améliorée est donc une réduction de la latence de transfert.

2.2 Sécurité

La procédure d'acheminement de retour a été conçue avec l'objectif de fournir un niveau de sécurité comparable à celui de l'Internet non mobile d'aujourd'hui [RFC4225]. À ce titre, elle protège contre les menaces d'usurpation d'identité, de déni de service, et d'inondation qui n'existent pas dans l'Internet non mobile, mais que l'introduction de la mobilité introduirait en l'absence de contre mesures appropriées. En particulier, la procédure d'acheminement de retour satisfait aux exigences suivantes :

- Un attaquant hors du chemin d'un nœud correspondant à une victime ne devrait pas être capable de faire qu'un nœud correspondant redirige des paquets qui devraient normalement être livrés à une victime, à lui-mêmse, ou à une adresse IP tierce. L'attaquant pourrait autrement se faire passer pour la victime auprès du nœud correspondant ou causer un déni de service à la victime. L'attaquant peut lancer ces attaques à partir d'une position arbitraire, qui ne serait pas nécessairement sur le chemin entre la victime et le nœud correspondant.

- Un attaquant hors du chemin d'un nœud correspondant à une victime ne devrait pas être capable de faire qu'un nœud correspondant redirige des paquets qui devraient normalement être livrés à l'attaquant lui-même, à la victime.

L'attaquant pourrait autrement inonder la victime avec des paquets non désirés. Une telle "inondation fondée sur la redirection" peut être intéressante pour l'attaquant parce que la charge de la génération de l'inondation de paquets et de leur envoi à la victime va être sur le nœud correspondant plutôt que sur l'attaquant. L'attaquant pourrait mystifier plusieurs nœuds correspondants pour les faire participer à l'inondation de la même victime. Cela permettrait à l'attaquant d'avoir un impact plus fort sur la victime qu'avec une attaque d'inondation directe, où l'attaquant devrait générer et envoyer lui-même les paquets d'inondation. Une amplification comparable n'est aujourd'hui possible qu'à travers une armée de nœuds compromis [DDoS]. Une façon de causer des inondations fondées sur la redirection est comme suit : l'attaquant pourrait accomplir la prise de contact initiale TCP pour un volumineus téléchargement de fichier à sa propre adresse IP, et ensuite lier l'adresse IP de la victime (comme adresse d'entretien) à la propre adresse IP de l'attaquant (ou son adresse de rattachement). Le nœud correspondant redirige ainsi le téléchargement sur la victime. L'attaquant pourrait falsifier les accusés de réception au nom de la victime sur la base des numéros de séquence qu'il apprend durant la prise de contact initiale afin de conserver ou accélérer le téléchargement. Les accusés de réception vont être plus petits et normalement de moins que la taille de segments complète que le nœud correspondant génère, facilitant donc l'amplification.

- Les attaquants ne devraient pas être capables de causer de déni de service aux nœuds mobiles ou nœuds correspondants par l'exploitation de calculs coûteux impliqués dans le protocole de mobilité.

La procédure d'acheminement de retour empêche l'usurpation d'identité, le déni de service, et l'inondation fondée sur la redirection par des attaquants qui ne sont pas sur le chemin entre un nœud correspondant et une victime, et elle est suffisemment légère pour ne pas exposer à des opérations coûteuses. Mais la procédure d'acheminement de retour ne peut pas protéger contre des attaquants qui sont situés sur le chemin entre le nœud correspondant et la victime. Il est génralement conseillé aux applications qui exigent un plus haut niveau de sécurité d'utiliser une protection de bout en bout comme la sécurité IP (IPsec) ou la sécurité de couche de transport (TLS, *Transport Layer Security*). Mais même elles sont vulnérables au déni de service ou à l'inondation. De plus, les mécanismes de sécurité de bout en bout exigent généralement que les nœuds mobiles et correspondants soient préconfigurés avec des accréditifs d'authentification, ou qu'ils dépendent d'une infrastructure de clé publique. Les deux entraveraient un large déploiement de l'optimisation de chemin IPv6 mobile si elles étaient un prérequis du protocole. Un objectif de l'optimisation de chemin améliorée est donc d'authentifier en toute sécurité les nœuds mobiles sans accréditifs préconfigurés ni infrastructure de clé publique, même en présence d'attaquants sur le chemin du nœud correspondant à la victime.

2.3 Frais généraux de signalisation

Un enregistrement de correspondant complet implique six transmissions de messages au nœud mobile, totalisant environ 376 octets [AUTHO]. Ces frais généraux de signalisation peuvent être acceptables si les mouvements sont peu fréquents. Par exemple, un nœud mobile qui se déplace toutes les 30 minutes génère en moyenne 1,7 bits/s de trafic de signalisation. Une mobilité plus élevée cause cependant des frais généraux plus substantiels. Une taille de cellule de 100 mètres et une vitesse de 120 km/h donne un changement de connexité IP toutes les 3 s et environ 1 000 bits/s de trafic de signalisation. Ceci est significatif comparé à un flux vocal à haute compression avec un taux normal de données de 10 000 à 30 000 bits/s.

De plus, IPv6 mobile de base exige que les nœuds mobiles renouvellent un enregistrement de correspondant au moins toutes les 7 minutes. Les frais généraux de signalisation montent à 7,16 bits/s si le nœud mobile communique avec un nœud statique [AUTHO]. Cela double si les deux homologues sont mobiles. Ces frais généraux peuvent être négligés quand les nœuds communiquent, mais cela peut être un problème pour les nœuds mobiles qui sont inactifs et restent dans la même localisation pendant un certain temps. Ces nœuds préfèrent passer en mode inactif pour conserver des réserves de batterie. Aussi, les rafraîchissements périodiques consomment une fraction de la bande passante sans fil qui pourrait être utilisée de façon plus efficace. Ces observations conduisent à l'objectif de l'optimisation de chemin améliorée de réduire autant que possible les frais généraux de signalisation des enregistrements de correspondant de IPv6 mobile de base, en particulier quand le nœud mobile ne se déplace pas pendant un certain temps.

3. Conception du protocole

L'optimisation de chemin améliorée consiste en un ensemble d'optimisations qui réalisent collectivement les objectifs discutés à la Section 2. Ces optimisations sont résumées comme suit.

3.1 Adresses de rattachement générées cryptographiquement

Un lien IPv6 mobile est idéalement une redirection de paquet d'une adresse de rattachement à une adresse d'entretien. L'adresse de rattachement est la source de la redirection et l'adresse d'entretien est la destination. Les paquets à rediriger peuvent donc être identifiés sur la base de l'adresse de rattachement. Cela motive une preuve cryptographique de possession de l'adresse de rattachement. L'optimisation de chemin améliorée applique les adresses de rattachement générées cryptographiquement à cette fin [CAM], [DoS-AO]. En général, une adresse générée cryptographiquement (CGA, *Cryptographically Generated Address*) fournit un lien cryptographique fort entre son identifiant d'interface et la clé publique du possesseur de la CGA. Cela facilite la preuve de la possession d'une adresse de rattachement cryptographique sans infrastructure de clé publique, permettant que d'autres nœuds authentifient en toute sécurité et de façon autonome le possesseur de la CGA comme tel, modulo la correction du préfixe de sous réseau de la CGA. Les adresses de rattachement générées cryptographiquement peuvent se substituer aux essais d'adresse de rattachement à l'exception de l'essai initial pour valider le préfixe de l'adresse de rattachement. Cela facilite de plus faibles délais de transfert et de plus longues durées de vie de lien, ainsi que des frais généraux de signalisation réduits pour les nœuds mobiles qui sont temporairement immobiles. L'optimisation de chemin améliorée permet aussi facultativement au nœud correspondant de prouver la possession de son adresse IP.

3.2 Adresses d'entretien non cryptographiques

À la différence d'une adresse de rattachement, une adresse d'entretien n'a pas de fonction d'identification. Il y a donc peu d'avantages à la preuve de possession cryptographique d'une adresse d'entretien. Étant donné que l'adresse d'entretien est la destination d'une redirection de paquet, c'est plutôt l'accessibilité du nœud mobile à l'adresse d'entretien qui importe. L'optimisation de chemin améliorée utilise les essais d'adresse d'entretien à cette fin, mais permet aux nœuds correspondants d'envoyer des paquets à une nouvelle adresse d'entretien avant que le nœud mobile ait été trouvé y être accessible.

3.3 Associations de sécurité semi permanentes

L'authentification fondée sur la CGA implique le chiffrement à clé publique et est donc beaucoup moins efficace du point de vue du calcul que l'authentification par une clé secrète partagée. La technique exige de plus qu'une quantité substantielle de paramètres de CGA supplémentaires soit portée sur des messages protégés. L'optimisation de chemin améliorée atténue ces inconvénients en ce qu'elle utilise une authentification initiale fondée sur la CGA pour échanger en toute sécurité un jeton secret permanent de génération de clé de rattachement entre un nœud mobile et un nœud correspondant. Le jeton permanent de génération de clé de rattachement est utilisé pour authentifier plus efficacement le nœud mobile dans les enregistrements de correspondant suivants. Les nœuds mobiles et correspondants renouvellent le jeton permanent de génération de clé de rattachement de façon peu fréquente. Le jeton n'est donc ni constant ni de courte durée de vie, c'est pourquoi l'association de sécurité entre le nœud mobile et le nœud correspondant est appelée "semi permanente".

3.4 Vérification d'adresse de rattachement initiale

Une vérification initiale d'adresse de rattachement est nécessaire en dépit d'une preuve cryptographique de possession de l'adresse de rattachement pour protéger contre les préfixes de sous réseau usurpés dans les adresses de rattachement. En l'absence complète d'essais d'adresse de rattachement, un nœud malveillant pourrait générer cryptographiquement une adresse de rattachement avec le préfixe de sous réseau d'un réseau victime, et demander à un nœud correspondant d'enregistrer un lien entre cette adresse de rattachement usurpée et la propre adresse d'entretien de l'attaquant. L'attaquant trompe alors le nœud correspondant en lui envoyant un flux de paquets à l'adresse d'entretien et ensuite désenregistre le lien ou le laisse expirer. La conséquence est que le nœud correspondant redirige le flux de paquets "en retour" à l'adresse de rattachement, causant au réseau victime une inondation de paquets non demandés. Pour empêcher ces pratiques, une vérification initiale d'adresse de rattachement est exigée pour le nœud mobile et pour le nœud correspondant pour établir une association de sécurité semi permanente. La vérification d'adresse de rattachement est, si possible, exécutée de façon proactive afin d'épargner un échange potentiellement coûteux de messages via l'agent de rattachement durant la période critique de transfert. La vérification d'adresse de rattachement n'a pas besoin d'être répétée lors des mouvements suivants.

3.5 Vérifications d'adresses d'entretien concurrentes

L'optimisation de chemin améliorée permet à un nœud correspondant d'envoyer des paquets de charge utile à la nouvelle adresse d'entretien du nœud mobile avant que le nœud mobile ait été trouvé être accessible à l'adresse d'entretien. Quand le nœud mobile change sa connexité IP, il met d'abord à jour son lien au nœud correspondant à la nouvelle adresse d'entretien sans fournir de preuve s'accessibilité. Le nœud correspondant enregistre la nouvelle adresse d'entretien de façon provisoire

et la règle à l'état NON VÉRIFIÉ. Des paquets de charge utile peuvent alors être échangés de façon bidirectionnelle via la nouvelle adresse d'entretien, tandis que l'accessibilité du nœud mobile à la nouvelle adresse d'entretien est vérifiée pendant ce temps. Le nœud correspondant passe l'adresse d'entretien à l'état VÉRIFIÉ quand la vérification d'accessibilité est achevée.

3.6 Autorisation fondée sur le crédit

Des essais concurrents d'adresse d'entretien sans protection supplémentaire permettraient à un attaquant de tromper un nœud correspondant pour lui faire temporairement rediriger des paquets de charge utile, qui auraient autrement été adressés à l'attaquant lui-même, à l'adresse IP d'une victime. De telles"inondations fondées sur la redirection" [RFC4225] peuvent être attractives pour l'attaquant parce que le nœud correspondant (pas l'attaquant) génère les paquets de l'inondation et les envoie à la victime. Cela permet à l'attaquant d'amplifier la force de l'attaque à un degré significatif par rapport à une attaque directe où l'attaquant génèrerait lui-même les paquets de l'inondation.

L'optimisation de chemin améliorée protège contre les attaques d'inondation fondée sur la redirection par l'utilisation de l'autorisation fondée sur le crédit. L'autorisation fondée sur le crédit gère l'effort qu'un nœud correspondant dépense dans l'envoi de paquets de charge utile à une adresse d'entretien dans l'état NON VÉRIFIÉ afin de s'assurer qu'une attaque d'inondation fondée sur la redirection ne puisse pas être plus efficace qu'une inondation directe. La capacité d'envoyer des paquets non demandés est une propriété inhérente des réseaux en mode paquet, et l'inondation directe est une menace qui en résulte. Comme l'inondation directe existe avec et sans prise en charge de la mobilité, et que les attaques d'inondation fondées sur la redirection ne peuvent pas être plus efficaces qu'elle, l'autorisation fondée sur le crédit augmente le niveau de sécurité fourni par l'optimisation de chemin améliorée à l'égard de l'inondation par rapport à celui de l'Internet non mobile. L'optimisation de chemin améliorée satisfait donc à l'objectif de fournir un niveau de sécurité comparable à celui de l'Internet non mobile.

La mesure et la limitation de l'effort sont techniquement réalisés par le concept de "crédit", que tient un nœud correspondant pour mettre son propre effort en relation avec l'effort déployé par un nœud mobile durant les communications régulières avec le nœud correspondant. Le nœud correspondant augmente le crédit pour les paquets de charge utile qu'il reçoit d'une adresse d'entretien du nœud mobile dans l'état VÉRIFIÉ, et il réduit le crédit en proportion de son propre effort d'envoi des paquets de charge utile à une adresse d'entretien au nœud mobile dans l'état NON VÉRIFIÉ.

3.7 Enregistrements parallèles de rattachement et de correspondant

L'optimisation de chemin améliorée permet aux nœuds mobiles de poursuivre un enregistrement de correspondant en parallèle avec l'enregistrement de rattachement correspondant. Cela réduit les délais de transfert comparés à l'IPv6 mobile de base, qui exige des nœuds mobiles qu'ils attendent un message d'accusé de réception de lien indiquant la réussite d'un enregistrement de rattachement avant d'initier un enregistrement de correspondant.

4. Fonctionnement du protocole

L'optimisation de chemin améliorée permet à un nœud mobile de s'authentifier en toute sécurité à un nœud correspondant sur la base de la propriété de CGA de son adresse de rattachement, et de demander une vérification concurrente d'adresse d'entretien pour une efficacité de transfert accrue. Selon que le nœud mobile souhaite tirer parti de l'une ou l'autre de ces améliorations, ou des deux, les messages échangés durant un enregistrement de correspondant sont différents. C'est ce qui est décrit dans les paragraphes qui suivent.

4.1 Envoi de messages de mise à jour de lien

Un nœud mobile peut initier un enregistrement de correspondant pour toutes les raisons suivantes :

- Établir un nouveau lien avec un nœud correspondant lorsque il est éloigné de sa liaison de rattachement afin que l'acheminement des paquets soit optimisé et ne soit plus à travers l'agent de rattachement du nœud mobile.
- Pour mettre à jour un lien existant au nœud correspondant tout en se déplaçant d'un point de rattachement IP à un autre.
- Pour suivre un message de mise à jour de lien précoce avec un message de mise à jour de lien complète après la réception d'un message d'accusé de réception de lien avec une option Essai d'entretien *(Care-of Test)*.
- Pour rafraîchir un lien existant au nœud correspondant sans changer le point de rattachement IP actuel.
- Pour demander au nœud correspondant de renouveler un jeton permanent de génération de clé de rattachement existant partagé entre le nœud mobile et le nœud correspondant (paragraphe 4.5).

o Pour demander au nœud correspondant de désenregistrer un lien existant.

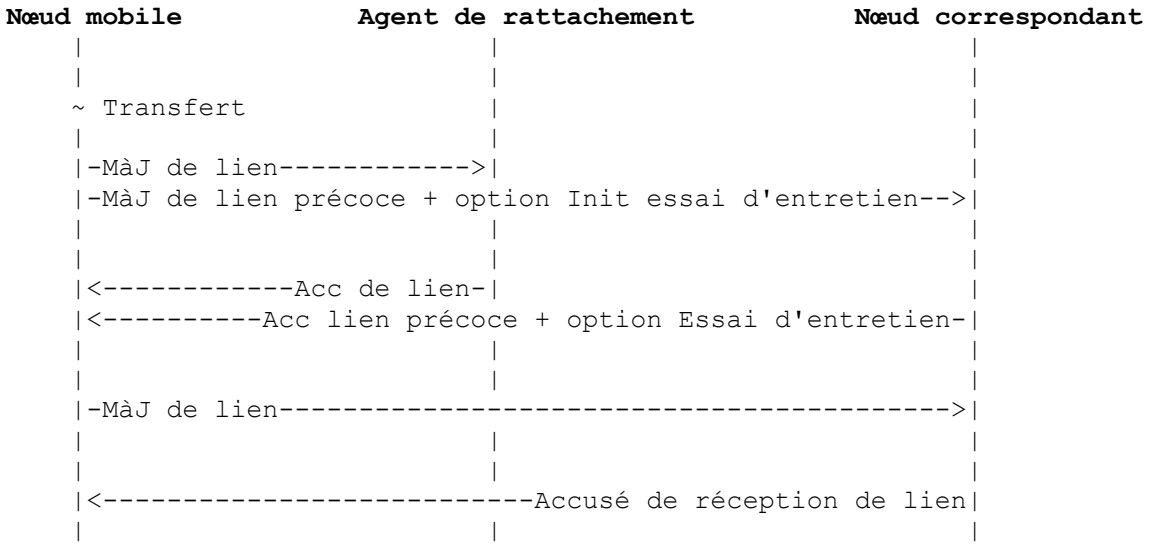


Figure 1 : Enregistrement de correspondant avec authentification par preuve de la connaissance du nœud mobile du jeton permanent de génération de clé de rattachement ; essai concurrent d'adresse d'entretien

Dans ces deux cas, le nœud mobile envoie un message de mise à jour de lien au nœud correspondant. Le message de mise à jour de lien est authentifié par une des trois méthodes d'authentification suivantes :

o Si l'adresse de rattachement du nœud mobile est une CGA, mais si le nœud mobile n'a pas un jeton permanent de génération de clé de rattachement dans son entrée de liste de mise à jour de lien pour le nœud correspondant, le nœud mobile DEVRAIT authentifier le message de mise à jour de lien sur la base de la propriété de CGA de son adresse de rattachement. Cela exige du nœud mobile qu'il envoie ses paramètres de CGA et sa signature au nœud correspondant et qu'il passe une vérification d'accessibilité à l'adresse de rattachement.

o Si l'adresse de rattachement du nœud mobile est une CGA, et si le nœud mobile a un jeton permanent de génération de clé de rattachement dans son entrée de liste de mise à jour de lien pour le nœud correspondant, le nœud mobile DOIT authentifier le message de mise à jour de lien par la preuve de sa connaissance du jeton permanent de génération de clé de rattachement.

o Si l'adresse de rattachement du nœud mobile n'est pas une CGA, le nœud mobile DOIT authentifier le message de mise à jour de lien par une preuve d'accessibilité à son adresse de rattachement.

La durée de vie demandée par le nœud mobile dans le champ Durée de vie du message de mise à jour de lien NE DOIT PAS excéder MAX_CGA_BINDING_LIFETIME (Section 7) si le message de mise à jour de lien est à authentifier sur la base de la propriété de CGA de l'adresse de rattachement du nœud mobile ou par la preuve de la connaissance par le nœud mobile du jeton permanent de génération de clé de rattachement. Si la méthode d'authentification choisie est une preuve de l'accessibilité du nœud mobile à l'adresse de rattachement, la durée de vie NE DOIT PAS excéder MAX_RR_BINDING_LIFETIME [RFC3775]. Il est RECOMMANDÉ dans tous les cas que le nœud mobile demande la durée de vie maximum permise afin d'éviter d'inutiles rafraîchissements de lien et donc de réduire les frais généraux de signalisation. Le champ Durée de vie d'un message de mise à jour de lien qui demande la suppression d'un lien existant au nœud correspondant DOIT être réglé à zéro.

Si la méthode d'authentification choisie est au moyen de la propriété de CGA de l'adresse de rattachement du nœud mobile, le nœud mobile inclut ses paramètres de CGA et sa signature dans le message de mise à jour de lien en ajoutant une ou plusieurs options Paramètres de CGA (paragraphe 5.1) directement suivies par une option Signature (paragraphe 5.2). Ceci est décrit au paragraphe 4.5. Une fois qu'un jeton permanent de génération de clé de rattachement a été obtenu du nœud correspondant, le nœud mobile DOIT authentifier tous les messages de mise à jour de lien suivants par une preuve de sa connaissance de ce jeton permanent de génération de clé de rattachement jusqu'à ce que soit la durée de vie de lien expire, soit que le jeton permanent de génération de clé de rattachement soit renouvelé, soit que le nœud mobile désenregistre explicitement le lien au nœud correspondant. Cela assure qu'un attaquant sur le chemin du nœud correspondant à l'adresse de rattachement du nœud mobile ne peut pas dégrader la méthode d'authentification choisie par le nœud mobile pour une preuve d'accessibilité à l'adresse de rattachement. Le nœud mobile PEUT choisir d'ignorer la propriété de CGA de son

adresse de rattachement et authentifier les messages de mise à jour de lien par une preuve d'accessibilité à l'adresse de rattachement. Cependant, ce comportement augmente la vulnérabilité à des attaquants sur le chemin et N'est donc PAS RECOMMANDÉ.

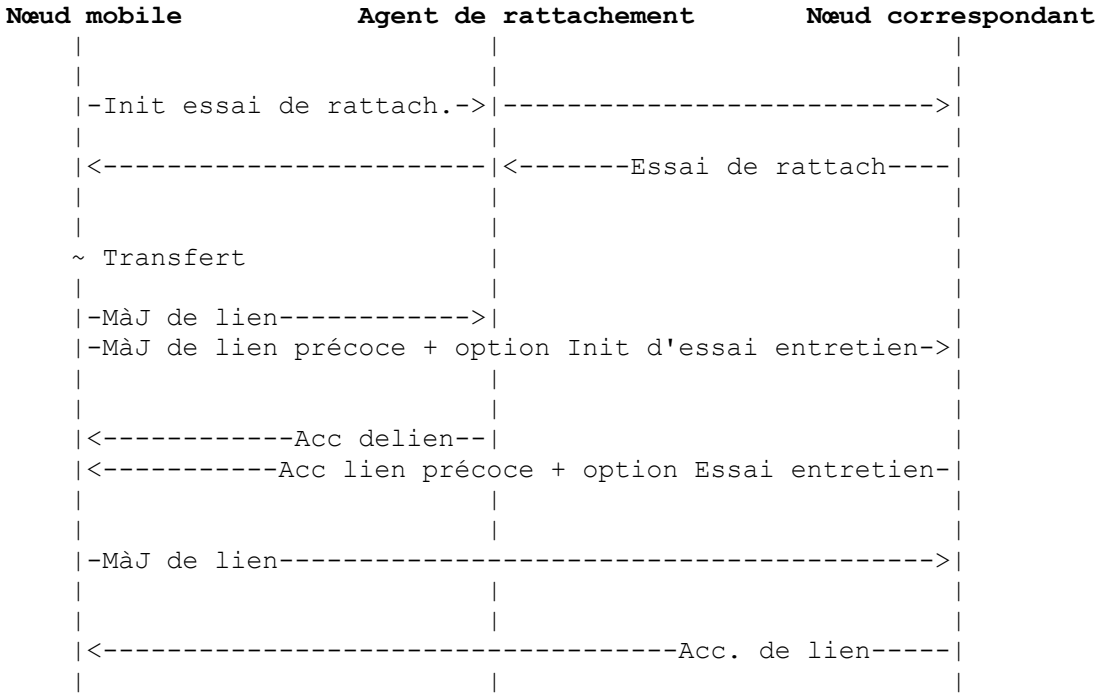


Figure 2 : Enregistrement de correspondant avec authentification fondée sur la vérification d'accessibilité à l'adresse de rattachement ; essai concurrent d'adresse d'entretien

Le nœud mobile inclut aussi ses paramètres de CGA dans le message de mise à jour de lien quand il a l'intention de renouveler un jeton permanent de génération de clé de rattachement existant partagé avec le nœud correspondant. Ceci est accompli, comme auparavant, en ajoutant au message une ou plusieurs options Paramètres de CGA et une option Signature.

L'authentifiant pour le message de mise à jour de lien est calculé sur la base d'un jeton permanent ou temporaire de génération de clé de rattachement. Le type de jeton de génération de clé de rattachemement que le nœud mobile utilise pour calculer l'authentifiant dépend de la méthode d'authentification :

- Si le message de mise à jour de lien est à authentifier sur la base de la propriété de CGA de l'adresse de rattachement du nœud mobile, le nœud mobile DOIT utiliser un jeton temporaire de génération de clé de rattachement provenant du nœud correspondant. Le nœud mobile peut avoir déjà un jeton temporaire de génération de clé de rattachement valide dans son entrée de liste de mise à jour de lien pour le nœud correspondant, ou il peut en récupérer un par l'échange d'un message Initiation d'essai de rattachement et d'un message Essai de rattachement.

- Si le message de mise à jour de lien est à authentifier par une preuve de la connaissance par le nœud mobile d'un jeton permanent de génération de clé de rattachement, le nœud mobile DOIT utiliser le jeton permanent de génération de clé de rattachement qu'il a dans son entrée de liste de mise à jour de lien pour le nœud correspondant.

- Si le message de mise à jour de lien est à authentifier par une preuve d'accessibilité à l'adresse de rattachement, le nœud mobile DOIT utiliser un jeton temporaire de génération de clé de rattachement provenant du nœud correspondant. Comme précédemment, le nœud mobile peut déjà avoir un jeton temporaire de génération de clé de rattachement valide dans son entrée de liste de mise à jour de lien pour le nœud correspondant, ou il peut en récupérer un par l'échange d'un message Initiation d'essai de rattachement et d'un message Essai de rattachement.

Sauf si l'objet du message de mise à jour de lien est de supprimer un lien existant au nœud correspondant, l'authentifiant est aussi calculé sur la base d'un jeton de génération de clé d'entretien. Le nœud mobile le choisit comme suit :

- Si le nœud mobile a un jeton de génération de clé d'entretien valide pour l'adresse d'entretien à enregistrer dans son entrée de liste de mise à jour de lien pour le nœud correspondant, le nœud mobile DOIT l'utiliser pour calculer l'authentifiant pour le message de mise à jour de lien. Le message de mise à jour de lien est dans ce cas "complet".

- Si le nœud mobile n'a pas un jeton de génération de clé d'entretien valide dans son entrée de liste de mise à jour de lien pour le nœud correspondant, le nœud mobile DEVRAIT définir le jeton de génération de clé d'entretien comme zéro et utiliser cela dans le calcul de l'authentifiant pour le message de mise à jour de lien. Le message de mise à jour de lien est dans ce cas "précoce".

- Si le nœud mobile n'a pas un jeton de génération de clé d'entretien valide dans son entrée de liste de mise à jour de lien pour le nœud correspondant, le nœud mobile PEUT choisir de récupérer un jeton de génération de clé d'entretien par l'échange d'un message Initiation d'essai d'entretien et un message Essai d'adresse d'entretien, comme défini dans la [RFC3775], sans envoyer de message de mise à jour de lien précoce. Dans ce cas, le nœud mobile attend la réception du message Essai d'adresse d'entretien et utilise le jeton de génération de clé d'entretien qui y est contenu pour calculer l'authentifiant pour un message de mise à jour de lien complet. Cette approche augmente cependant la latence de transfert, et n'est donc PAS RECOMMANDÉE.

Pour réduire les délais de transfert, le nœud mobile DEVRAIT simultanément initier les enregistrements de rattachement et de correspondant pour une adresse d'entretien particulière. Le nœud mobile DEVRAIT aussi poursuivre en parallèle les désenregistrements de rattachement et de correspondant si il souhaite arrêter le service IPv6 pendant qu'il est éloigné de sa liaison de rattachement. Cependant, quand le nœud mobile commet les désenregistrements de rattachemement et de correspondant après être retourné sur la liaison de rattachement après une période d'itinérance, le nœud mobile DOIT initier d'abord le désenregistrement de rattachement, et il DOIT attendre un message d'accusé de réception de lien indiquant un désenregistrement de rattachement réussi avant d'initier le désenregistrement de correspondant. Ce comportement assure que l'agent de rattachement ne mandate pas l'adresse de rattachement du nœud mobile alors que le nœud mobile est sur la liaison de rattachement, donc empêchant l'interférence entre le nœud mobile et l'agent de rattachement durant la détection d'adresse dupliquée. Comme un désenregistrement de rattachement consomme seulement un délai d'aller-retour de liaison locale quand le nœud mobile l'effectue à partir de la liaison de rattachement, le coût de ne pas le faire en parallèle avec un désenregistrement de correspondant est normalement négligeable, en termes d'augmentation du délai de transfert.

De plus, quand le message de mise à jour de lien pour l'enregistrement de correspondant est à authentifier sur la base de la propriété de CGA de l'adresse de rattachement du nœud mobile ou par une preuve d'accessibilité à l'adresse de rattachement, le nœud mobile DEVRAIT initier l'échange des messages Initiation d'essai de rattachement et Essai de rattachemement avant le transfert afin de choisir de façon proactive un jeton de génération de clé de rattachement frais provenant du nœud correspondant. Cela réduit encore les délais de transfert. Un message Initiation d'essai de rattachement peut être envoyé périodiquement chaque fois que le jeton de génération de clé de rattachement acquis précédemment du nœud correspondant est sur le point d'expirer. Les jetons sont valides pendant 3,5 minutes [RFC3775], de sorte que l'intervalle entre les messages Initiation d'essai de rattachement successifs devrait être un petit peu moins. Autrement, le nœud mobile peut être capable d'envoyer le message Initiation d'essai de rattachement juste à temps si sa couche de liaison fournit un déclencheur qui annonce un transfert imminent. Les essais proactifs d'essai d'adresse de rattachement sont techniquement faisables parce que une adresse de rattachement ne change pas à travers les transferts.

Si le nœud mobile initie l'essai d'adresse de rattachement à partir de la liaison de rattachement, il DOIT adresser le message Initiation d'essai de rattachement directement au nœud correspondant. Le message Essai de rattachement va alors être reçu directement du nœud correspondant. Si l'essai d'adresse de rattachement est initié à partir d'une liaison visitée, le nœud mobile DOIT tunneler le message Initiation d'essai de rattachement à l'agent de rattachement. Le message Essai de rattachement va alors être tunnelé en retour au nœud mobile par l'agent de rattachement. Un essai d'adresse de rattachement NE DEVRAIT PAS se chevaucher avec un enregistrement ou désenregistrement de rattachement car il pourrait en résulter la perte du message Initiation d'essai de rattachement ou Essai de rattachement.

Si le message de mise à jour de lien est précoce, le nœud mobile DOIT ajouter une option Initiation d'essai d'entretien (paragraphe 5.4) au message, pour demander au nœud correspondant de retourner un nouveau jeton de génération de clé d'entretien. L'option Initiation d'essai d'entretien DOIT suivre les options Paramètres de CGA et Signature, si elles existent dans le message de mise à jour de lien. Une fois qu'un message d'accusé de réception de lien en réponse avec une option Essai d'adresse d'entretien (paragraphe 5.5) est reçu, le nœud mobile DOIT utiliser le jeton de génération de clé d'entretien qui y est contenu pour calculer l'authentifiant pour un message de mise à jour de lien complet et envoyer ce message au nœud correspondant.

Si le message de mise à jour de lien est authentifié sur la base de la propriété de CGA de l'adresse de rattachement du nœud mobile, le nœud mobile PEUT ajouter une option Demande de paramètres de CGA (paragraphe 5.6) au message de mise à jour de lien afin de demander au nœud correspondant de prouver la possession de son adresse IP au sein du message d'accusé de réception de lien. Cette preuve de possession permet au nœud mobile de vérifier que le jeton permanent de génération de clé de rattachement retourné dans le message d'accusé de réception de lien a été généré par le bon nœud correspondant.

Le nœud mobile comporte les indices de nom occasionnel associés aux jetons choisis de génération de clé de rattachement et d'entretien dans le message de mise à jour de lien en utilisant une option Indices de nom occasionnel [RFC3775]. L'indice de nom occasionnel de rattachement est ainsi déterminé comme suit :

- Si le message de mise à jour de lien est à authentifier sur la base de la propriété de CGA de l'adresse de rattachement du nœud mobile, le nœud mobile utilise un jeton temporaire de génération de clé de rattachement pour calculer l'authentifiant pour le message de mise à jour de lien, et l'indice de nom occasionnel de rattachement associé DOIT être pris dans le message Essai de rattachement avec lequel le jeton de génération de clé de rattachement a été obtenu.

- Si le message de mise à jour de lien est à authentifier par la preuve de la connaissance par le nœud mobile d'un jeton permanent de génération de clé de rattachement, l'indice de nom occasionnel de rattachement DOIT être réglé à zéro.

- Si le message de mise à jour de lien est à authentifier par une proeuve de l'accessibilité du nœud mobile à l'adresse de rattachement, le nœud mobile utilise un jeton temporaire de génération de clé de rattachement pour calculer l'authentifiant du message de mise à jour de lien, et l'indice de nom occasionnel de rattachement associé DOIT être pris dans le message Essai de rattachement avec lequel le jeton de génération de clé de rattachement a été obtenu.

L'indice de nom occasionnel d'entretien est déterminé selon les règles suivantes :

- Si le message de mise à jour de lien est complet, l'indice de nom occasionnel d'entretien est pris dans l'option Essai d'adresse d'entretien ou le message Essai d'adresse d'entretien avec lequel le jeton de génération de clé d'entretien (utilisé pour calculer l'authentifiant pour le message de mise à jour de lien) a été obtenu.

- Si le message de mise à jour de lien est précoce, l'indice de nom occasionnel d'entretien DOIT être réglé à zéro.

- Si l'objet du message de mise à jour de lien est de supprimer un lien au nœud correspondant, l'indice de nom occasionnel d'entretien DOIT être réglé à zéro.

L'option Indices de nom occasionnel suit les options Paramètres de CGA, Signature, Initiation d'essai d'entretien, et Demande de paramètres de CGA si elles sont incluses aussi dans le message de mise à jour de lien.

Le nœud mobile calcule finalement un authentifiant pour le message de mise à jour de lien sur la base des jetons choisis de génération de clé de rattachement et d'entretien, suivant les règles décrites aux paragraphes 5.2 et 6.2.7 de la [RFC3775]. Pour un message de mise à jour de lien qui demande la suppression d'un lien existant avec le nœud correspondant, l'authentifiant est calculé sur la base de seulement un jeton de génération de clé de rattachement, et il n'incorpore pas de jeton de génération de clé d'entretien. L'authentifiant est placé dans le champ Authentifiant d'une option Données d'autorisation de lien [RFC3775], que le nœud mobile ajoute au message de mise à jour de lien comme dernière option.

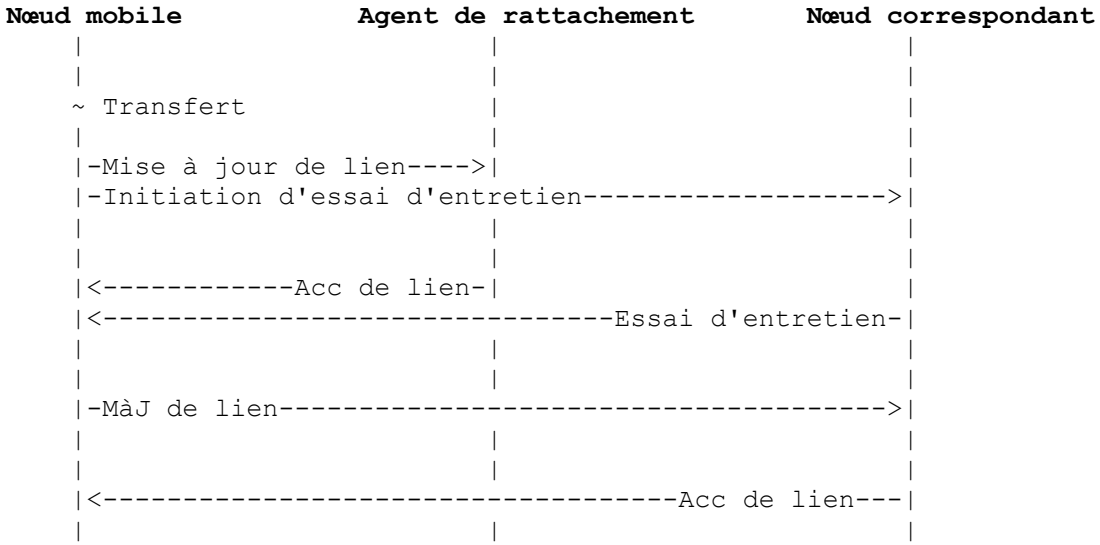


Figure 3 : Enregistrement de correspondant avec authentification par la preuve de la connaissance du nœud mobile d'un jeton permanent de génération de clé de rattachement ; essai explicite d'adresse d'entretien

Les diagrammes de séquence temporelle des Figures 1 à 3 illustrent le fonctionnement de l'optimisation de chemin améliorée sur la base de quelques échanges de messages choisis. La Figure 1 montre les messages échangés pour un enregistrement de correspondant où un message de mise à jour de lien précoce est authentifié par une preuve de la connaissance par le nœud mobile d'un jeton permanent de génération de clé de rattachement. Une option Initiation d'essai d'entretien dans le message de mise à jour de lien précoce demande au nœud correspondant d'ajouter au message d'accusé de réception de lien un jeton frais de génération de clé d'entretien dans une option Essai d'adresse d'entretien. Le nœud mobile conclut finalement l'enregistrement de correspondant avec un message de mise à jour de lien complet. La Figure 2 montre la procédure d'un enregistrement de correspondant où le message de mise à jour de lien est authentifié avec une preuve d'accessibilité à l'adresse de rattachement. L'essai d'adresse de rattachement est effectué de façon proactive avant le transfert, permettant au nœud mobile de produire un message de mise à jour de lien directement après le transfert. Le message de mise à jour de lien est là encore précoce, et un jeton de génération de clé d'entretien est livré au nœud mobile avec le message d'accusé de réception de lien. La Figure 3 décrit un enregistrement de correspondant où le nœud mobile obtient initialement un jeton frais de génération de clé d'entretien par l'échange dédié de messages Initiation d'essai d'entretien et Essai d'entretien. Il produit ensuite un message de mise à jour de lien complet qui est authentifié avec la propriété de CGA de l'adresse de rattachement.

4.2 Réception des messages de mise à jour de lien

Quand le nœud correspondant reçoit un message de mise à jour de lien, il doit d'abord vérifier si le nœud mobile envoyeur est le possesseur légitime de l'adresse de rattachement spécifiée dans le message. Le nœud correspondant choisit la méthode d'authentification sur la base de l'indice de nom occasionnel de rattachement donné dans l'option Indices de nom occasionnel du message de mise à jour de lien, et sur l'existence des options Paramètres de CGA et Signature dans le message de mise à jour de lien :

- Si l'indice de nom occasionnel de rattachement est réglé à une valeur non nulle et si le message de mise à jour de lien inclut une ou plusieurs options Paramètres de CGA suivies par une option Signature, le nœud correspondant DOIT authentifier le message de mise à jour de lien sur la base de la propriété de CGA de l'adresse de rattachement du nœud mobile.

- Si l'indice de nom occasionnel de rattachement est zéro et si le message de mise à jour de lien n'inclut pas une ou plusieurs options Paramètres de CGA suivies par une option Signature, le nœud correspondant DOIT authentifier le message de mise à jour de lien par une preuve de la connaissance du nœud mobile d'un jeton permanent de génération de clé de rattachement.

- Si l'indice de nom occasionnel de rattachement est réglé à une valeur non nulle et si le message de mise à jour de lien n'inclut pas une ou plusieurs options Paramètres de CGA suivies par une option Signature, le nœud correspondant DOIT authentifier le message de mise à jour de lien par une preuve de l'accessibilité du nœud mobile à l'adresse de rattachement.

En plus de la procédure de validation pour les messages de mise à jour de lien spécifiée dans la [RFC3775], le nœud correspondant doit suivre les étapes supplémentaires suivantes pour rejeter les messages de mise à jour de lien qui ne sont pas authentifiés de façon appropriée :

- Si le message de mise à jour de lien inclut une ou plusieurs options Paramètres de CGA suivies par une option Signature et si l'indice de nom occasionnel de rattachement est zéro, le nœud correspondant DOIT envoyer un message d'accusé de réception de lien avec le code d'état 150 ("Indice de nom occasionnel de rattachement attendu non nul"). Cela assure qu'un message de mise à jour de lien qui est authentifié sur la base de la propriété de CGA de l'adresse de rattachement du nœud mobile doit aussi fournir une preuve de l'accessibilité du nœud mobile à l'adresse de rattachement.

- Si le message de mise à jour de lien est à authentifier par une preuve de la connaissance par le nœud mobile d'un jeton permanent de génération de clé de rattachement, le nœud correspondant DOIT vérifier qu'il a une entrée d'antémémoire de liens pour le nœud mobile qui inclut un jeton permanent de génération de clé de rattachement. Au cas où le nœud correspondant n'aurait pas d'entrée d 'antémémoire de liens pour le nœud mobile, ou si l'entrée existante d'antémémoire de liens pour le nœud mobile n'inclut pas de jeton permanent de génération de clé de rattachement, le nœud correspondant DOIT rejeter le message de mise à jour de lien par l'envoi d'un message d'accusé de réception de lien avec le code d'état 147 ("Jeton permanent de génération de clé de rattachement indisponible").

- Si le message de mise à jour de lien est à authentifier par une preuve de l'accessibilité du nœud mobile à l'adresse de rattachement, le nœud correspondant DOIT vérifier qu'il n'a pas de jeton permanent de génération de clé de rattachement dans son entrée d'antémémoire de liens pour le nœud mobile. Si le nœud correspondant a un jeton

permanent de génération de clé de rattachement dans son entrée d'antémémoire de liens pour le nœud mobile, il DOIT rejeter le message de mise à jour de lien en envoyant un message d'accusé de réception de lien avec le code d'état 149 ("Jeton permanent de génération de clé de rattachement existant"). Cela assure qu'un attaquant ne peut pas dégrader la méthode d'authentification pour capturer le lien d'un nœud mobile légitime.

L'authentifiant pour le message de mise à jour de lien est calculé sur la base d'un jeton permanent ou temporaire de génération de clé de rattachement. Le type de jeton de génération de clé de rattachement que le nœud correspondant utilise dans la validation de l'authentifiant, et comment il restitue ou recalcule le jeton de génération de clé de rattachement, dépend de la méthode d'authentification :

- Si le message de mise à jour de lien est à authentifier sur la base de la propriété de CGA de l'adresse de rattachement du nœud mobile, le nœud correspondant DOIT recalculer le jeton temporaire de génération de clé de rattachement défini par l'indice (non nul) de nom occasionnel de rattachement dans l'option Indices de nom occasionnel du message de mise à jour de lien, et il DOIT utiliser ce jeton recalculé pour valider l'authentifiant du message.

- Si le message de mise à jour de lien est à authentifier par une preuve de la connaissance par le nœud mobile d'un jeton permanent de génération de clé de rattachement, le nœud correspondant DOIT utiliser le jeton permanent de génération de clé de rattachement qu'il a dans son entrée d'antémémoire de liens pour le nœud mobile dans la validation de l'authentifiant du message de mise à jour de lien.

- Si le message de mise à jour de lien est à authentifier par la vérification de l'accessibilité du nœud mobile à l'adresse de rattachement, le nœud correspondant DOIT recalculer le jeton temporaire de génération de clé de rattachement défini par l'indice (non nul) de nom occasionnel de rattachement dans l'option Indices de nom occasionnel du message de mise à jour de lien, et il DOIT utiliser ce jeton recalculé pour valider l'authentifiant du message.

Sauf si l'objet du message de mise à jour de lien est de supprimer un lien existant au nœud correspondant, l'authentifiant est aussi calculé sur la base d'un jeton de génération de clé d'entretien. Quel jeton de génération de clé d'entretien le nœud correspondant utilise pour valider l'authentifiant dépend de si le message de mise à jour de lien est complet ou précoce :

- Si l'indice de nom occasionnel d'entretien dans l'option Indices de nom occasionnel du message de mise à jour de lien est réglé à une valeur non nulle, le message de mise à jour de lien est complet. Dans ce cas, le nœud correspondant DOIT recalculer le jeton de génération de clé d'entretien qui est identifié par l'indice de nom occasionnel d'entretien, et il DOIT utiliser ce jeton recalculé pour valider l'authentifiant du message.

- Si l'indice de nom occasionnel d'entretien dans l'option Indices de nom occasionnel du message de mise à jour de lien est zéro, le message de mise à jour de lien est précoce. Le jeton de génération de clé d'entretien à utiliser par le nœud correspondant pour valider l'authentifiant du message de mise à jour de lien est zéro dans ce cas.

Le nœud correspondant valide finalement l'authentifiant dans le message de mise à jour de lien sur la base des jetons de génération de clé de rattachement et d'entretien choisis, suivant l'algorithme décrit au paragraphe 9.5.1 de la [RFC3775].

Si la validation échoue, le nœud correspondant DOIT éliminer le message de mise à jour de lien. Le nœud correspondant peut avoir à envoyer un message d'accusé de réception de lien avec un code d'état indiquant l'échec, comme décrit dans la [RFC3775].

Si la validation de l'authentifiant dans le message de mise à jour de lien réussit, le nœud correspondant enregistre la nouvelle adresse d'entretien du nœud mobile, soit en mettant à jour une entrée d'antémémoire de liens existante, si il en existe une, soit en créant une nouvelle entrée d 'antémémoire de liens. La durée de vie accordée au lien dépend de la durée de vie demandée par le nœud mobile dans le champ Durée de vie du message de mise à jour de lien et de la méthode par laquelle le message de mise à jour de lien est authentifié. Si le message de mise à jour de lien est authentifié sur la base de la propriété de CGA de l'adresse de rattachement du nœud mobile ou par une preuve de la connaissance par le nœud mobile d'un jeton permanent de génération de clé de rattachement, la durée de vie pour le lien DEVRAIT être réglée au minimum de MAX_CGA_BINDING_LIFETIME et de la valeur spécifiée dans le champ Durée de vie du message de mise à jour de lien. Si le message de mise à jour de lien est authentifié par une preuce de l'accessibilité du nœud mobile à l'adresse de rattachement, alors la durée de vie pour le lien DEVRAIT être réglée au minimum de MAX_RR_BINDING_LIFETIME [RFC3775] et de la valeur spécifiée dans le champ Durée de vie du message de mise à jour de lien. Le nœud correspondant PEUT dans l'un et l'autre cas accorder une durée de vie encore plus réduite, mais NE DOIT PAS accepter une durée de vie plus longue.

L'état de la nouvelle adresse d'entretien dépend de si le message de mise à jour de lien est complet ou précoce :

- Si le message de mise à jour de lien est complet, la nouvelle adresse d'entretien est réglée à l'état VÉRIFIÉ. Le nœud correspondant peut alors immédiatement envoyer des paquets à la nouvelle adresse d'entretien sans restriction.

- Si le message de mise à jour de lien est précoce, la nouvelle adresse d'entretien est réglée à l'état NON VÉRIFIÉ. Le nœud correspondant DOIT alors suivre les règles définies au paragraphe 4.10 pour l'envoi des paquets à cette adresse d'entretien jusqu'à ce que l'adresse d'entretien soit réglée à l'état VÉRIFIÉ.

Si le message de mise à jour de lien contient une ou plusieurs options Paramètres de CGA, le nœud mobile demande au nœud correspondant d'accepter les paramètres de CGA inclus pour établir un nouveau jeton permanent de génération de clé de rattachement partagé entre le nœud mobile et le nœud correspondant, ou pour en renouveler un existant. Le nœud correspondant DOIT dans ce cas vérifier si les options Paramètres de CGA sont directement suivies par une option Signature et, si c'est le cas, valider les paramètres de CGA et la signature comme décrit au paragraphe 4.6.

Si l'option Paramètres de CGA n'est pas directement suivie par une option Signature, ou si la validation des paramètres de CGA et de signature inclus échoue, le nœud correspondant DOIT éliminer le message de mise à jour de lien et envoyer un message d'accusé de réception de lien avec le code d'état 148 ("Échec de vérification de CGA et signature") au nœud mobile.

Si la signature incluse dans l'option Signature est correcte, le nœud correspondant génère un jeton permanent de génération de clé de rattachement à partager avec le nœud mobile et il le mémorise dans son entrée d'antémémoire de liens pour le nœud mobile. Le jeton permanent de génération de clé de rattachement est envoyé au nœud mobile dans un message d'accusé de réception de lien comme décrit au paragraphe 4.3.

4.3 Envoi des messages d'accusé de réception de lien

À réception d'un message de mise à jour de lien valide, le nœud correspondant retourne au nœud mobile un message d'accusé de réception de lien dans tous les cas suivants :

- Le fanion Accusé de réception dans le message de mise à jour de lien est établi.

- Le message de mise à jour de lien contient une ou plusieurs options Paramètres de CGA directement suivies par une option Signature, et la signature incluse dans cette dernière a été déterminée être correcte.

- Le message de mise à jour de lien est précoce et inclut une option Initiation d'essai d'entretien.

Si le message de mise à jour de lien contient de plus une option Demande de paramètres de CGA et si l'adresse IP du nœud correspondant est une CGA, le nœud correspondant DOIT inclure ses paramètres de CGA et sa signature dans le message d'accusé de réception de lien en ajoutant une ou plusieurs options Paramètres de CGA directement suivies par une option Signature. Les paramètres de CGA et la signature du nœud correspondant permettent au nœud mobile de vérifier que le jeton permanent de génération de clé de rattachement reçu dans le message d'accusé de réception de lien a été généré par le bon nœud correspondant. Si le message de mise à jour de lien contient une option Demande de paramètres de CGA, mais si l'adresse IP du nœud correspondant n'est pas une CGA, le nœud correspondant ignore l'option Demande de paramètres de CGA et traite le message de mise à jour de lien comme décrit ci-dessous.

Si le message de mise à jour de lien contient une ou plusieurs options Paramètres de CGA directement suivies par une option Signature, et si la signature incluse dans cette dernière a été déterminée être correcte, le nœud correspondant DOIT ajouter une option Jeton permanent de générateur de clé de rattachement (voir le paragraphe 5.3) avec un nouveau jeton permanent de génération de clé de rattachement au message d'accusé de réception de lien. Le nœud correspondant mémorise aussi ce jeton permanent de génération de clé de rattachement dans son entrée d'antémémoire de liens pour le nœud mobile.

Si le message de mise à jour de lien inclut une option Initiation d'essai d'entretien, le nœud correspondant DOIT ajouter au message d'accusé de réception de lien une option Essai d'adresse d'entretien avec une valeur pseudo aléatoire dans le champ Jeton de génération de clé d'entretien. L'option Essai d'adresse d'entretien DOIT apparaître après l'option Jeton permanent de générateur de clé de rattachement si les deux options sont présentes dans le message d'accusé de réception de lien.

Une option Données d'autorisation de lien doit être ajoutée au message d'accusé de réception de lien comme dernière option, comme décrit aux paragraphes 5.2 et 6.2.7 de la [RFC3775].

4.4 Réception des messages d'accusé de réception de lien

Un nœud mobile vérifie d'abord si un message d'accusé de réception de lien reçu est conforme aux règles spécifiées dans la [RFC3775]. Pourvu que le message d'accusé de réception de lien ne soit pas rejeté sur la base de ces règles, le nœud mobile suit les étapes supplémentaires suivantes.

Si le nœud mobile incluait une option Demande de paramètres de CGA dans le message de mise à jour de lien et si le message d'accusé de réception de lien contient une option Jeton permanent de générateur de clé de rattachement, le nœud mobile traite d'abord toutes les options Paramètres de CGA et Signature dans le message d'accusé de réception de lien de la manière suivante. Si le message d'accusé de réception de lien contient une ou plusieurs options Paramètres de CGA qui sont directement suivies par une option Signature, le nœud mobile DOIT vérifier la possession par le nœud correspondant de son adresse IP en vérifiant les paramètres de CGA et la signature inclus comme décrit au paragraphe 4.6. Si la validation des paramètres de CGA et de la signature échoue, le nœud mobile DOIT éliminer en silence le message d'accusé de réception de lien. Le nœud mobile DOIT aussi éliminer en silence le message d'accusé de réception de lien si le message inclut une ou plusieurs options Paramètres de CGA qui ne sont pas directement suivies par une option Signature, ou si le message d'accusé de réception de lien manque d'options Paramètres de CGA en présence d'une option Signature.

Si le nœud mobile n'incluait pas d'option Demande de paramètres de CGA dans le message de mise à jour de lien ou si le message d'accusé de réception de lien ne contient pas d'option Jeton permanent de générateur de clé de rattachement, le nœud mobile ignore toutes les options Paramètres de CGA et Signature que le message d'accusé de réception de lien peut contenir. Une utilisation prudente de l'option Demande de paramètres de CGA dans les messages de mise à jour de lien permet au nœud mobile de contrôler les ressources de traitement qu'il consomme dans la vérification d'une CGA de nœud correspondant ainsi que de désactiver une telle vérification dans le cas d'échecs persistents de vérification, qui peuvent être dus à un logiciel de CGA mal configuré ou périmé [RFC4992] sur le côté du nœud correspondant ou au nœud mobile lui-même. Précisément, si le nœud mobile échoue de façon répétée à recevoir un message d'accusé de réception de lien incluant des options Paramètres de CGA et Signature valides en réponse à l'envoi d'un message de mise à jour de lien avec une option Demande de paramètres de CGA, le nœud mobile DEVRAIT s'abstenir d'inclure une option Demande de paramètres de CGA dans les futurs messages de mise à jour de lien pour le même nœud correspondant.

Si le nœud mobile incluait une option Demande de paramètres de CGA dans le message de mise à jour de lien, mais si le message d'accusé de réception de lien ne contient pas d'options Paramètres de CGA ou Signature, le nœud mobile ne peut pas être sûr que l'adresse IP du nœud correspondant ne soit pas simplement une CGA, ou si le message d'accusé de réception de lien n'a pas été généré par un attaquant sur le chemin du nœud mobile au nœud correspondant. Pour éviter d'accepter un jeton permanent de génération de clé de rattachement provenant d'un attaquant sur le chemin, le nœud mobile DOIT donner la préséance aux messages d'accusé de réception de lien qui incluent des options Paramètres de CGA et Signature valides sur les messages d'accusé de réception de lien sans de telles options. Un algorithme possible à suivre pour le nœud à cet égard est de toujours accepter d'abord le message d'accusé de réception de lien reçu, et si ce message ne contient pas d'options valides de Paramètres de CGA ou de Signature et qu'un autre message d'accusé de réception de lien incluant de telles options est reçu plus tard, de revenir sur tous les changements d'état impliqués par l'acceptation du premier accusé de réception de lien en faveur de ce message d'accusé de réception de lien ultérieur. Donner la présance aux messages d'accusé de réception de lien avec des options Paramètres de CGA et Signature valides sur les messages d'accusé de réception de lien sans de telles options permet au nœud mobile de communiquer avec les nœuds correspondants qui n'utilisent pas une CGA, et en même temps de protéger contre la plupart des attaquants sur le chemin. Cette stratégie ne protège pas contre un attaquant qui peut intercepter les messages d'accusé de réception de lien provenant du nœud correspondant, mais un tel attaquant pourrait de toutes façons empêcher la gestion de mobilité entre le nœud mobile et le nœud correspondant. Quand le nœud mobile a accepté de façon permanente le message d'accusé de réception de lien sans options Paramètres de CGA et Signature valides, le nœud mobile DEVRAIT s'abstenir d'inclure une option Demande de paramètres de CGA dans les futurs messages de mise à jour de lien pour le même nœud correspondant.

Si le message d'accusé de réception de lien contient une option Jeton permanent de générateur de clé de rattachement, le nœud mobile extrait le jeton permanent de génération de clé de rattachement inclus dans cette option et le mémorise dans son entrée de liste de mise à jour de lien pour le nœud correspondant. Les futurs messages de mise à jour de lien vont alors être authentifiés par une preuve de la connaissance par le nœud mobile de ce jeton permanent de génération de clé de rattachement.

Si le message d'accusé de réception de lien contient une option Essai d'adresse d'entretien, le nœud mobile extrait le jeton de génération de clé d'entretien inclus dans cette option, mémorise le jeton dans son entrée de liste de mise à jour de lien pour le nœud correspondant, et envoie au nœud correspondant un message de mise à jour de lien complet comme défini au paragraphe 4.1. Noter que le message de mise à jour de lien complet va être authentifié sur la base de la propriété de CGA de l'adresse de rattachement du nœud mobile si le message d'accusé de réception de lien comporte aussi une option Jeton permanent de générateur de clé de rattachement. Ceci est indépendant de la méthode d'authentification qui a été utilisée

pour le message de mise à jour de lien précoce correspondant.

Un nœud mobile DOIT s'assurer que, lorsque il a un lien pour une certaine adresse de rattachement à un nœud correspondant, il a aussi un lien valide à son agent de rattachement pour la même adresse de rattachement. Ceci peut parfois exiger que le nœud étende la durée de vie du lien à l'agent de rattachement, demande à un nœud correspondant d'utiliser une durée de vie de lien de moins que le maximum permis, ou de désenregistrer explicitement un lien existant à un nœud correspondant.

Si le nœud mobile authentifie les messages de mise à jour de lien pour un nœud correspondant particulier en prouvant sa connaissance d'un jeton permanent de génération de clé de rattachement, mais si les enregistrements à ce nœud correspondant échouent de façon persistante, le nœud mobile DEVRAIT renouveler le jeton permanent de génération de clé de rattachement en envoyant un message de mise à jour de lien qui est authentifié sur la base de la propriété de CGA de son adresse de rattachement. Ce message de mise à jour de lien inclut les paramètres de CGA et la signature du nœud mobile, et il demande au nœud correspondant de générer un nouveau jeton permanent de génération de clé de rattachement et il envoie cela au nœud mobile dans un message d'accusé de réception de lien.

Si le nœud mobile reçoit de façon persistante des messages d'accusé de réception de lien avec le code d'état 148 ("Échec de vérification de CGA et signature") de la part d'un nœud correspondant, le nœud mobile DEVRAIT authentifier les futurs messages de mise à jour de lien pour les mêmes nœuds correspondants par une preuve de son accessibilité à l'adresse de rattachement. Cela permet au nœud mobile de récupérer d'un logiciel de CGA mal configuré ou perimé [RFC4992] sur le côté du nœud correspondant ou au nœud mobile lui-même.

4.5 Envoi des paramètres de CGA

Un nœud mobile inclut ses paramètres de CGA et sa signature dans un message de mise à jour de lien pour un nœud correspondant dans toutes les situations suivantes :

- Pour acquérir un jeton permanent de génération de clé de rattachement si l'adresse de rattachement du nœud mobile est une CGA, et si le nœud mobile n'a pas déjà un jeton permanent de génération de clé de rattachement provenant du nœud correspondant.

- Pour étendre la durée de vie d'un lien existant si le nœud mobile a déjà un jeton permanent de génération de clé de rattachement provenant du nœud correspondant, et si la durée de vie du lien au nœud correspondant est sur le point d'expirer.

- Pour renouveler un jeton permanent de génération de clé de rattachement existant pour empêcher des attaques en répétition dans un événement imminent de retour à zéro du numéro de séquence, ou pour une protection améliorée contre la cryptanalyse.

Un nœud correspondant dont l'adresse IP est une CGA inclut ses paramètres de CGA et sa signature dans un message d'accusé de réception de lien pour le nœud mobile quand il reçoit un message de mise à jour de lien avec une option Demande de paramètres de CGA.

Les paramètres de CGA sont transmis dans le format de la structure de données de paramètres de CGA définie dans la [RFC3972]. La structure de données de paramètres de CGA est partagée sur une ou plusieurs options Paramètres de CGA comme décrit au paragraphe 5.1. La dernière option Paramètres de CGA DOIT être directement suivie par une option Signature.

La valeur du champ Signature dans l'option Signature est calculée en accord avec l'algorithme de génération de signature défini à la Section 6 de la [RFC3972]. La valeur est calculée avec la clé privée du nœud mobile ou correspondant sur la séquence d'octets suivante :

données de mobilité = adresse d'entretien | adresse IP de nœud correspondant | données d'en-tête de mobilité

où "|" note l'enchaînement, "adresse d'entretien" est l'adresse d'entretien du nœud mobile, et "adresse IP de nœud correspondant" est l'adresse IP du nœud correspondant qui est visible aux couches de protocole au dessus de IP. Dans le cas où le nœud correspondant est mobile, "adresse IP de nœud correspondant" se réfère à l'adresse de rattachement du nœud correspondant. "données d'en-tête de mobilité" est le contenu du message Mise à jour de lien ou Accusé de réception de lien incluant l'en-tête de mobilité et toutes les options jusqu'à la dernière option Paramètres de CGA. C'est-à-dire, "données d'en-tête de mobilité" exclut l'en-tête IPv6 et tous les en-têtes d'extension IPv6 autres que l'en-tête de mobilité lui-même.

Les "données de mobilité" constituent ce qui est appelé le "message" à la Section 6 de la [RFC3972].

La valeur du champ Signature est calculée comme si le champ Somme de contrôle dans l'en-tête de mobilité était zéro. Le champ Somme de contrôle dans le paquet transmis est encore calculé de la manière usuelle, avec la valeur calculée dans le champ Signature faisant partie du paquet protégé par la somme de contrôle.

4.6 Réception des paramètres de CGA

Les nœuds mobiles et correspondants qui reçoivent un message Mise à jour de lien ou Accusé de réception de lien incluant une ou plusieurs options Paramètres de CGA directement suivies par une option Signature traitent d'abord le message comme décrit dans la [RFC3775]. Cela inclut une vérification de l'authentifiant dans le champ Authentifiant de l'option Données d'autorisation de lien. Si le message Mise à jour de lien ou Accusé de réception de lien est rejeté à cause d'un authentifiant incorrect ou pour toute autre raison, le traitement du message s'arrête.

Autrement, si la validation du message Mise à jour de lien ou Accusé de réception de lien réussit, le nœud mobile ou nœud correspondant réassemble la structure de données de paramètres de CGA à partir des options Paramètres de CGA incluses dans le message comme décrit au paragraphe 5.1, et il exécute l'algorithme de vérification de CGA défini à la Section 5 de la [RFC3972]. L'algorithme de vérification de CGA prend la CGA à vérifier et la structure de données de paramètres de CGA réassemblée comme entrée. La CGA à vérifier est l'adresse de rattachement du nœud mobile quand l'algorithme de vérification de CGA est exécuté par le nœud correspondant. Quand le nœud mobile exécute l'algorithme de vérification de CGA, la CGA à vérifier est l'adresse IP du nœud correspondant qui est visible aux couches de protocole au dessus de IP. C'est l'adresse de rattachement du nœud correspondant dans le cas où le nœud correspondant est mobile. Les étapes suivantes sont sautées si la vérification de CGA échoue.

Si la vérification de CGA réussit, le nœud mobile ou correspondant effectue une vérification plus consommatrice de temps de la signature. Il extrait la signature du champ Signature dans l'option Signature et exécute l'algorithme de vérification de signature défini à la Section 6 de la [RFC3972]. L'algorithme de vérification de signature prend en entrée la CGA à vérifier comme défini ci-dessus, la structure de données de paramètres de CGA réassemblée, les données d'en-tête de mobilité comme défini au paragraphe 4.5, l'étiquette de type de message de CGA de l'optimisation de chemin améliorée comme définie à la Section 7, et la signature elle-même.

4.7 Envoi de jetons permanents de génération de clé de rattachement

Un nœud correspondant alloue à un nœud mobile un nouveau jeton permanent de génération de clé de rattachement après qu'il a reçu du nœud mobile un message de mise à jour de lien avec des options Paramètres de CGA et Signature incluses, et que ces options ont été bien validées comme décrit au paragraphe 4.6. Le jeton permanent de génération de clé de rattachement est une valeur de 64 bits générée de façon aléatoire par le nœud correspondant. Le nœud correspondant mémorise le jeton permanent de génération de clé de rattachement dans l'entrée d'antémémoire de liens qu'il tient pour le nœud mobile.

Le nœud correspondant envoie le jeton permanent de génération de clé de rattachement au nœud mobile sous une forme chiffrée au sein d'une option Jeton permanent de générateur de clé de rattachement dans un message d'accusé de réception de lien. Il envoie ce message même si le fanion Accuser réception dans le message de mise à jour de lien correspondant était à zéro. Le nœud correspondant chiffre le jeton permanent de génération de clé de rattachement avec la clé publique du nœud mobile en utilisant le format RSAES-PKCS1-v1_5 [RFC3447], et place le texte chiffré dans le champ Jeton permanent de générateur de clé de rattachement de l'option Jeton permanent de générateur de clé de rattachement.

L'option Données d'autorisation de lien DOIT être la dernière option dans le message d'accusé de réception de lien. C'est-à-dire, l'authentifiant dans l'option Données d'autorisation de lien couvre l'option Jeton permanent de générateur de clé de rattachement.

4.8 Réception des jetons permanents de génération de clé de rattachement

Un nœud mobile qui reçoit un message d'accusé de réception de lien traite d'abord le message comme décrit dans la [RFC3775], indépendamment de si le message inclut une option Jeton permanent de générateur de clé de rattachement. Cela inclut une vérification de l'authentifiant dans le champ Authentifiant de l'option Données d'autorisation de lien. Si le message d'accusé de réception de lien est rejeté à cause d'un authentifiant incorrect ou pour toute autre raison, le nœud mobile arrête le traitement du message.

Autrement, si le nœud mobile accepte le message d'accusé de réception de lien et si le message inclut une option Jeton permanent de générateur de clé de rattachement, le nœud mobile extrait le texte chiffré du champ Jeton permanent de générateur de clé de rattachement dans cette option et le déchiffre avec sa clé privée en utilisant le format RSAES-PKCS1-v1_5 [RFC3447]. Le résultat du chiffrement est le jeton permanent de génération de clé de rattachement à utiliser dans les enregistrements ultérieurs avec le nœud correspondant. Le nœud mobile mémorise le jeton permanent de génération de clé de rattachement dans l'entrée de liste de mise à jour de lien qu'il tient pour le nœud correspondant.

4.9 Renouvellement des jetons permanents de génération de clé de rattachement

Un nœud mobile qui partage un jeton permanent de génération de clé de rattachement avec un nœud correspondant NE DOIT PAS utiliser deux fois le même numéro de séquence avec ce jeton permanent de génération de clé de rattachement afin de se protéger contre les attaques en répétition. Le nœud mobile DOIT renouveler le jeton permanent de génération de clé de rattachement en incluant ses paramètres de CGA et sa signature dans un message de mise à jour de lien pour le nœud correspondant quand un retour à zéro des numéros de séquence est imminent. De plus, le nœud mobile PEUT renouveler son jeton permanent de génération de clé de rattachement à tout moment. Le renouvellement périodique du jeton permanent de génération de clé de rattachement fournit une protection accrue contre la cryptanalyse. Finalement, le nœud mobile peut dans la plupart des cas vouloir renouveler le jeton permanent de génération de clé de rattachement quand la durée de vie de son lien au nœud correspondant expire.

4.10 Traitement des paquets de charge utile

L'échange immédiat d'un message de mise à jour de lien précoce après un transfert du côté du nœud mobile permet aux nœuds mobiles et correspondants de rétablir rapidement les communications à chemin optimisé via la nouvelle adresse d'entretien du nœud mobile. Le nœud mobile peut envoyer des paquets de charge utile au nœud correspondant à partir de la nouvelle adresse d'entretien aussitôt qu'il a expédié le message de mise à jour de lien précoce. Le nœud correspondant redirige les paquets de charge utile sortants pour le nœud mobile à la nouvelle adresse d'entretien une fois qu'il a reçu le message de mise à jour de lien précoce et enregistré la nouvelle adresse d'entretien. Ici, un "paquet de charge utile" est défini comme un paquet dont l'origine est à une couche de protocole au dessus de IP.

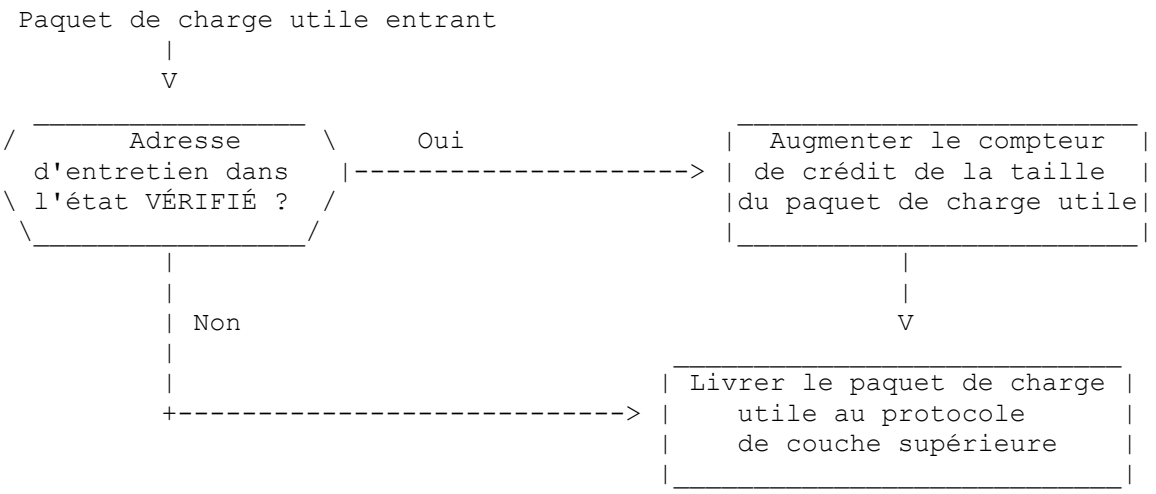


Figure 4 : Traitement des paquets de charge utile sortants

Une nouvelle adresse d'entretien qui a été enregistrée avec un message de mise à jour de lien précoce est conservée dans l'état NON VÉRIFIÉ par le nœud correspondant jusqu'à ce qu'il reçoive un message de mise à jour de lien complet du nœud mobile. Le nœud correspondant envoie alors l'adresse d'entretien à l'état VÉRIFIÉ. L'état de l'adresse d'entretien détermine la quantité maximum de données qu'il est permis au nœud correspondant d'envoyer à l'adresse d'entretien, comme il est nécessaire pour empêcher les attaques amplifiées d'inondation fondées sur la redirection. Dans ce but, le nœud correspondant tient un "compteur de crédit" pour chacun des nœuds mobiles qui a une entrée dans son antémémoire de liens. Chaque fois qu'un paquet de charge utile arrive d'un nœud mobile avec une adresse d'entretien dans l'état VÉRIFIÉ, le nœud correspondant DEVRAIT augmenter le compteur de crédit du nœud mobile de la taille du paquet de charge utile reçu. Le nœud correspondant PEUT être contraint par sa politique d'augmenter le compteur de crédit d'une valeur inférieure ou de ne pas augmenter du tout le crédit. Le compteur de crédit ne change pas quand un paquet de charge utile entrant est reçu d'une adresse d'entretien dans l'état NON VÉRIFIÉ. La Figure 4 montre un diagramme de cette procédure.

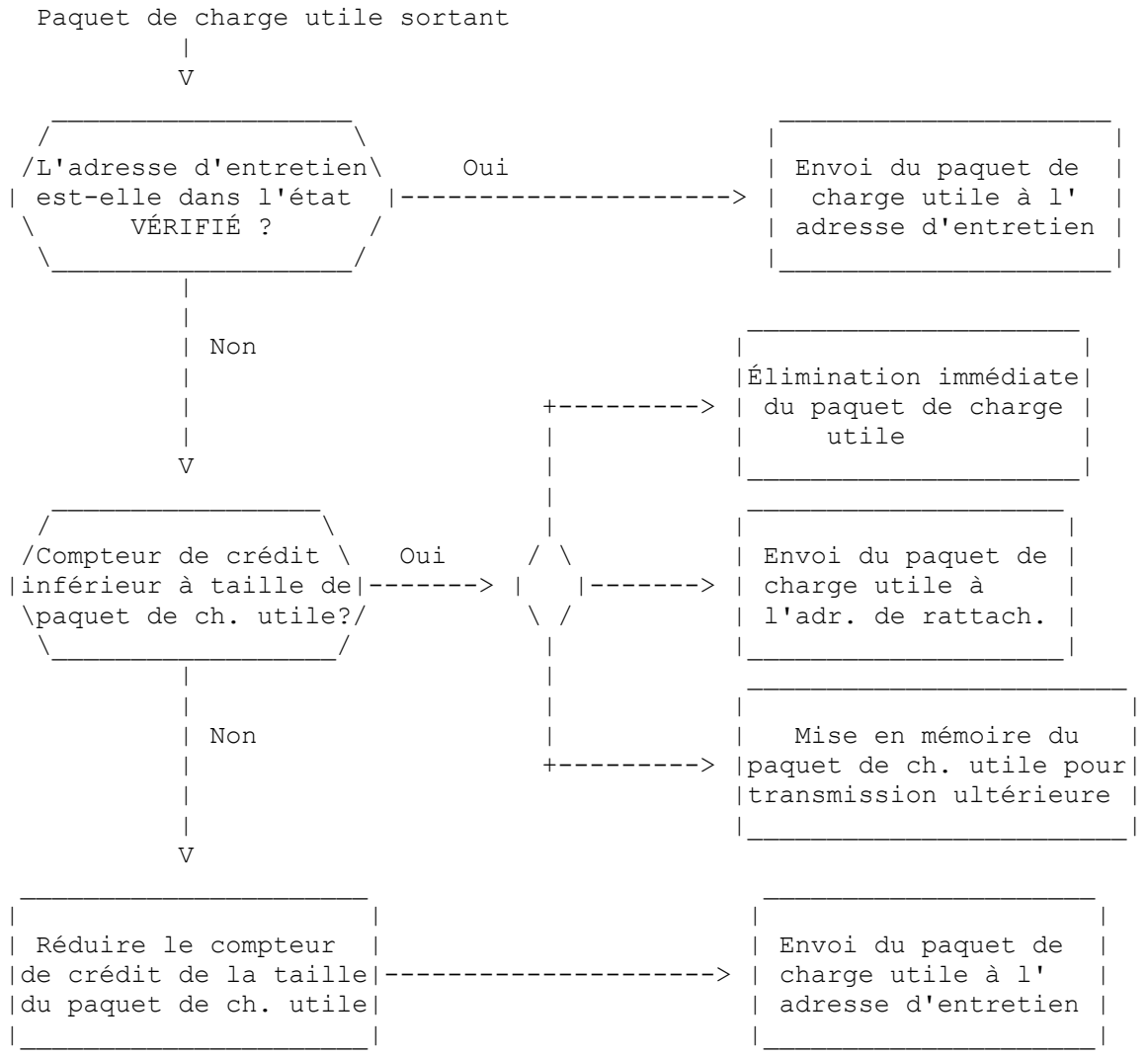


Figure 5 : Traitement des paquets de charge utile sortants

Quand le nœud correspondant a un paquet de charge utile à envoyer au nœud mobile, la suite du traitement du paquet de charge utile dépend de l'état de l'adresse d'entretien du nœud mobile et de la valeur actuelle du compteur de crédit du nœud mobile, comme illustré à la Figure 5 : le nœud correspondant DOIT envoyer le paquet de charge utile à l'adresse d'entretien du nœud mobile si l'adresse d'entretien est dans l'état VÉRIFIÉ. Si l'adresse d'entretien est dans l'état NON VÉRIFIÉ et si la valeur du compteur de crédit est supérieure ou égale à la taille du paquet de charge utile, le nœud correspondant DOIT réduire le compteur de crédit du nœud mobile de la taille du paquet de charge utile et envoyer aussi le paquet de charge utile à l'adresse d'entretien. Cependant, si l'adresse d'entretien est dans l'état NON VÉRIFIÉ et si le compteur de crédit est inférieur à la taille du paquet de charge utile, le paquet de charge utile NE DOIT PAS être envoyé à l'adresse d'entretien du nœud mobile. Le nœud correspondant DEVRAIT alors éliminer le paquet de charge utile, bien qu'il PUISSE aussi mettre le paquet de charge utile en antémémoire jusqu'à ce que l'adresse d'entretien passe à l'état VÉRIFIÉ, ou envoyer le paquet de charge utile à l'adresse de rattachement du nœud mobile. Le compteur de crédit du nœud mobile ne change pas quand le nœud correspondant envoie un paquet de charge utile à l'adresse d'entretien du nœud mobile alors que l'adresse d'entretien est dans l'état VÉRIFIÉ.

La quantité de données que le nœud mobile peut envoyer au nœud correspondant n'est jamais restreinte à cause de l'état de l'adresse d'entretien du nœud mobile. L'état de l'adresse d'entretien ne change pas non plus l'adressage ni l'acheminement des paquets de charge utile dans l'une ou l'autre direction du trafic : tous les paquets de charge utile qui sont générés du nœud mobile ont l'adresse d'entretien dans le champ Adresse de source de l'en-tête IPv6 et l'adresse de rattachement dans l'option Adresse de rattachement de l'en-tête d'extension Options de destination IPv6. Vice versa, tous les paquets de charge utile provenant du nœud correspondant ont l'adresse d'entretien dans le champ Adresse de destination de l'en-tête IPv6 et l'adresse de rattachement dans l'en-tête d'extension Acheminement IPv6.

4.11 Vieillissement de crédit

Un nœud correspondant s'assure que tous les compteurs de crédit qu'il tient diminuent graduellement au fil du temps. Chaque compteur de crédit est multiplié par un facteur, CreditAgingFactor *(facteur de vieillissement de crédit)* de moins de un dans des intervalles de temps fixés de longueur CreditAgingInterval *(intervalle de vieillissement de crédit)*. Un tel "vieillissement de crédit" limite le crédit total qu'un nœud mobile peut gagner, pourvu que le taux de remplisssage du crédit soit constant ou presque constant. Cela applique une limite supérieure au taux auquel le nœud correspondant peut durablement envoyer à l'adresse d'entretien du nœud mobile lorsque l'adresse d'entretien est dans l'état NON VÉRIFIÉ. En l'absence de vieillissement du crédit, un nœud malveillant avec une faible capacité de liaison en amont pourrait adopter le rôle d'un nœud mobile, construire un crédit à très bas débit et sur une longue période, et dépenser ce crédit durant une période beaucoup plus courte à rediriger une salve de paquets de charge utile à l'adresse IP d'une victime.

Choisir les valeurs appropriées pour CreditAgingFactor et CreditAgingInterval est important pour faciliter les applications où le nœud correspondant envoie à un plus haut débit que le nœud mobile. Si CreditAgingFactor ou CreditAgingInterval est trop petit, le compteur de crédit peut de façon persistente empêcher la transmission des paquets de charge utile à une adresse d'entretien dans l'état NON VÉRIFIÉ. Les valeurs données à la Section 7 sont RECOMMANDÉES car elles fonctionnent bien quand le nœud correspondant transfère un fichier au nœud mobile via une connexion TCP et que le délai d'aller-retour de bout en bout n'excède pas 500 millisecondes.

4.12 Mouvements simultanés

Comme spécifié dans la [RFC3775], les messages de mise à jour de lien sont envoyés à l'adresse de rattachement d'un nœud mobile correspondant. Cela rend possible que deux nœuds mobiles continuent les communications même si tous deux changent leur connexité IP au même moment.

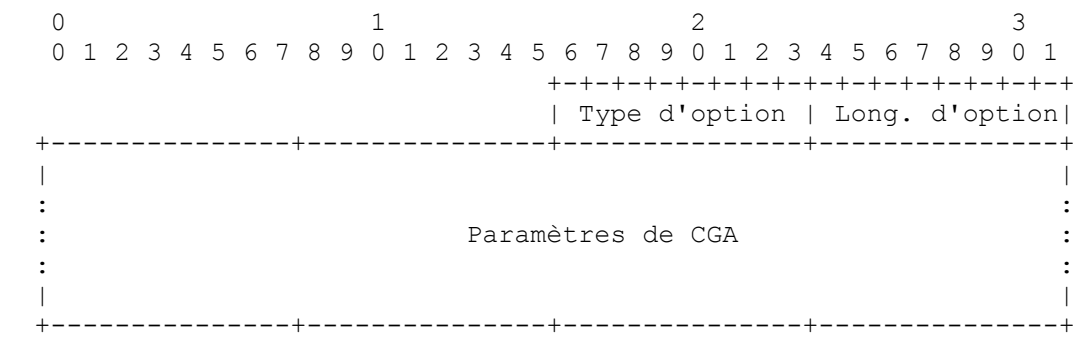
5. Formats d'option et codes d'état

L'optimisation de chemin améliorée utilise un ensemble de nouvelles options de mobilité et de nouveaux codes d'état en plus des options de mobilité et codes d'état définis dans la [RFC3775]. Ils sont décrits ci-dessous.

5.1 Option Paramètres de CGA

L'option Paramètres de CGA est utilisée dans les messages Mise à jour de lien et Accusé de réception de lien. Elle contient une partie des paramètres de CGA du nœud mobile ou correspondant. La [RFC3775] limite les options d'en-tête de mobilité à une longueur maximum de 255 octets, excluant les champs Type d'option et Longueur d'option. Comme les paramètres de CGA vont probablement excéder cette limite, plusieurs options Paramètres de CGA peuvent devoir être enchaînées pour porter tous les paramètres de CGA.

Le format de l'option Paramètres de CGA est comme suit :



Type d'option : identifiant de 8 bits du type de cette option de mobilité. Sa valeur est 12.

Longueur d'option : entier non signé de 8 bits représentant la longueur du champ Paramètres de CGA en octets.

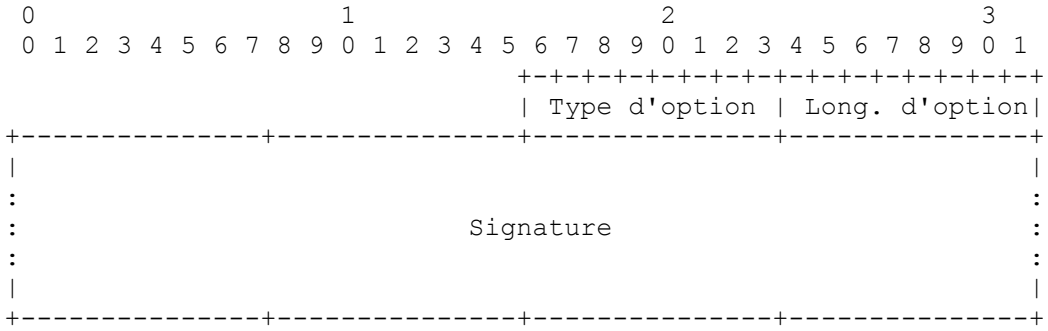
Paramètres de CGA : ce champ contient jusqu'à 255 octets de la structure de données de paramètres de CGA définie dans la [RFC3972]. L'enchaînement de toutes les options Paramètres de CGA dans l'ordre où elles apparaissent dans le message

de mise à jour de lien DOIT résulter en la structure originale de données de paramètres de CGA. Toutes les options Paramètres de CGA dans le message de mise à jour de lien sauf la dernière DOIVENT contenir exactement 255 octets dans le champ Paramètres de CGA, et le champ Longueur d'option DOIT être réglé à 255 en conséquence. Toutes les options Paramètres de CGA DOIVENT apparaître directement les unes après les autres, c'est-à-dire, une option de mobilité d'un type différent NE DOIT PAS être placée entre deux options Paramètres de CGA.

5.2 Option Signature

L'option Signature est utilisée dans les messages Lien et Accusé de réception de lien. Elle contient une signature que le nœud mobile ou correspondant génère avec sa clé privée sur une ou plusieurs options Paramètres de CGA précédentes.

Le format de l'option Signature est comme suit :



Type d'option : identifiant de 8 bits du type de cette option de mobilité. Sa valeur est 13.

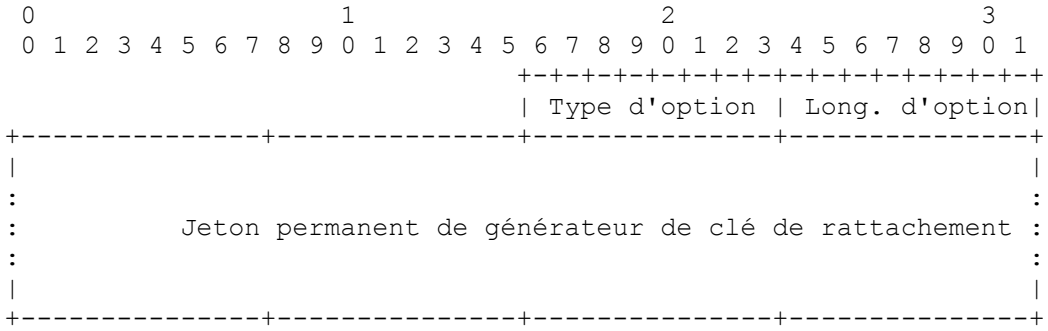
Longueur d'option : entier non signé de 8 bits représentant la longueur du champ Signature en octets.

Signature : ce champ contient la signature du nœud mobile ou correspondant, générée avec la clé privée du nœud mobile ou correspondant comme spécifié au paragraphe 4.5.

5.3 Option jeton permanent de générateur de clé de rattachement

L'option Jeton permanent de générateur de clé de rattachement est utilisée dans les messages d'accusé de réception de lien. Elle contient un jeton permanent de génération de clé de rattachement que le nœud correspondant envoie au nœud mobile après qu'il a reçu un message de mise à jour de lien contenant une ou plusieurs options Paramètres de CGA directement suivies par une option Signature provenant du nœud mobile.

Le format de l'option Jeton permanent de générateur de clé de rattachement est comme suit :



Type d'option : identifiant de 8 bits du type de cette option de mobilité. Sa valeur est 14.

Longueur d'option : entier non signé de 8 bits représentant la longueur du champ Jeton permanent de générateur de clé de rattachement en octets.

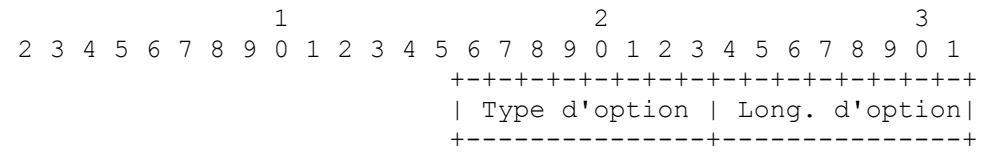
Jeton permanent de générateur de clé de rattachement : ce champ contient le jeton permanent de génération de clé de rattachement généré par le nœud correspondant. Le contenu de ce champ DOIT être chiffré avec la clé publique du

nœud mobile, comme défini au paragraphe 4.7. La longueur du jeton permanent de génération de clé de rattachement est 8 octets avant chiffrement, bien que le texte chiffré [RFC3447] et, donc, le champ Jeton permanent de générateur de clé de rattachement puisse être plus long.

5.4 Option Initiation de vérification d'adresse d'entretien

L'option Initiation d'essai d'entretien est incluse dans les messages de mise à jour de lien. Elle demande à un nœud correspondant de retourner une option Essai d'adresse d'entretien avec un jeton frais de génération de clé d'entretien dans le message d'accusé de réception de lien.

Le format de l'option Initiation d'essai d'entretien est comme suit :



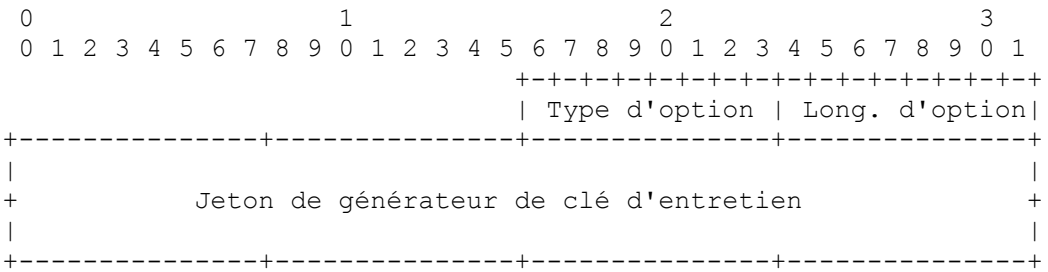
Type d'option : identifiant de 8 bits du type de cette option de mobilité. Sa valeur est 15.

Longueur d'option : ce champ DOIT être réglé à zéro.

5.5 Option Essai d'adresse d'entretien

L'option Essai d'adresse d'entretien est utilisée dans les messages d'accusé de réception de lien. Elle contient un jeton frais de génération de clé d'entretien, que le nœud correspondant envoie au nœud mobile après qu'il a reçu une option Initiation d'essai d'entretien dans un message de mise à jour de lien.

Le format de l'option Essai d'adresse d'entretien est comme suit :



Type d'option : identifiant de 8 bits du type de cette option de mobilité. Sa valeur est 16.

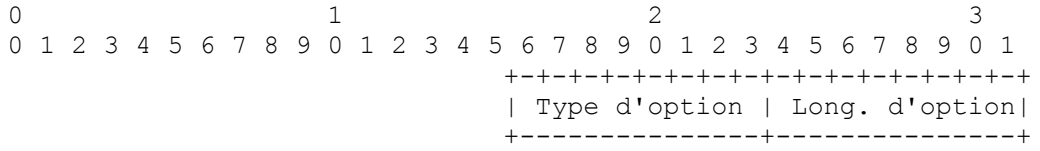
Longueur d'option : ce champ DOIT être réglé à 8. Il représente la longueur du champ Jeton de générateur de clé d'entretien en octets.

Jeton de générateur de clé d'entretien : ce champ contient le jeton de génération de clé d'entretien généré par le nœud correspondant, comme spécifié au paragraphe 4.3.

5.6 Option Demande de paramètres de CGA

L'option Demande de paramètres de CGA est incluse dans les messages de mise à jour de lien qui sont authentifiés sur la base de la propriété de CGA de l'adresse de rattachement du nœud mobile. Elle demande au nœud correspondant de retourner ses paramètres de CGA et sa signature dans le message d'accusé de réception de lien, permettant au nœud mobile de vérifier que le jeton permanent de génération de clé de rattachement retourné dans le message d'accusé de réception de lien a été généré par le bon nœud correspondant.

Le format de l'option Demande de paramètres de CGA est comme suit :



Type d'option : identifiant de 8 bits du type de cette option de mobilité. Sa valeur est 11.

Longueur d'option : ce champ DOIT être réglé à zéro.

5.7 Codes d'état

L'optimisation de chemin améliorée utilise les quatre nouveaux codes d'état suivants pour les messages d'accusé de réception de lien en plus des codes d'état définis dans la [RFC3775]:

Jeton permanent de génération de clé de rattachement indisponible (147)
: Un nœud correspondant retourne un message d'accusé de réception de lien avec le code d'état 147 à un nœud mobile si il a reçu du nœud mobile un message de mise à jour de lien qui a été authentifié par la propriété de CGA de l'adresse de rattachement du nœud mobile, mais le nœud correspondant n'a pas d'entrée d'antémémoire de liens pour le nœud mobile, ou l'entrée d'antémémoire de liens existante pour le nœud mobile ne contient pas de jeton permanent de génération de clé de rattachement. Un message d'accusé de réception de lien avec le code d'état 147 indique au nœud mobile qu'il devrait demander un nouveau jeton permanent de génération de clé de rattachement au nœud correspondant en envoyant au nœud correspondant un message de mise à jour de lien incluant ses paramètres de CGA et sa signature. Cela permet en particulier au nœud mobile de récupérer rapidement d'une perte d'état chez le nœud correspondant. La [RFC3775] ne permet pas à un nœud correspondant d'envoyer un message d'accusé de réception de lien avec un code d'état indiquant une défaillance quand l'authentifiant d'un message de mise à jour de lien reçu se trouve être incorrect. Cela cause une latence de transfert supplémentaire avec une forte probabilité parce que le nœud mobile ne peut détecter le problème qu'après l'expiration d'un temporisateur de retransmission. Le nœud mobile va de plus probablement suppoer une perte de paquet et renvoyer plusieurs fois le message de mise à jour de lien incorrectement authentifié. Un message d'accusé de réception de lien avec le code d'état 147 aide le nœud mobile à identifier le problème sous-jacent de façon plus efficace quand le nœud correspondant pourrait ne pas vérifier la propriété de CGA de l'adresse de rattachement du nœud mobile.

Échec de vérification de CGA et de signature (148)
: Un nœud correspondant retourne un message d'accusé de réception de lien avec le code d'état 148 à un nœud mobile si il a reçu du nœud mobile un message de mise à jour de lien qui inclut une ou plusieurs options Paramètres de CGA directement suivies par une option Signature, mais la propriété de CGA de l'adresse de rattachement ne peut pas être vérifiée sur la base du contenu des options Paramètres de CGA, ou la vérification de la signature dans l'option Signature a échoué.

Jeton permanent de génération de clé de rattachement existant (149)
: Un nœud correspondant retourne un message d'accusé de réception de lien avec le code d'état 149 à un nœud mobile si il a reçu du nœud mobile un message de mise à jour de lien qui a été authentifié par la vérification de l'accessibilité du nœud mobile à l'adresse de rattachement et n'inclut pas une ou plusieurs options Paramètres de CGA directement suivies par une option Signature, mais le nœud correspondant a un jeton permanent de génération de clé de rattachement dans son entrée d'antémémoire de liens pour le nœud mobile. Le message de mise à jour de lien est traité plus avant si il inclut une ou plusieurs options Paramètres de CGA directement suivies par une option Signature. Cela permet au nœud mobile d'obtenir un nouveau jeton permanent de génération de clé de rattachement du nœud correspondant au cas où il aurait perdu celui existant, par exemple, à cause d'un réamorçage. Que le nœud correspondant accepte le message de mise à jour de lien dans ce cas dépend de la vérification des paramètres de CGA et de la signature fournis dans le message de mise à jour de lien.

Indice de nom occasionnel de rattachement non nul attendu (150)
: Un nœud correspondant retourne un message d'accusé de réception de lien avec le code d'état 150 à un nœud mobile si il a reçu du nœud mobile un message de mise à jour de lien qui inclut une ou plusieurs options Paramètres de CGA directement suivies par une option Signature, mais l'indice de nom occasionnel de rattachement spécifié dans l'option Indices de nom occasionnel est zéro. Ce comportement assure qu'un message de mise à jour de lien qui est authentifié sur la base de la propriété de CGA de l'adresse de rattachement du nœud mobile doit aussi fournir une preuve de l'accessibilité du nœud mobile à l'adresse de rattachement.

6. Considérations sur la sécurité

L'optimisation de chemin améliorée diffère de l'IPv6 mobile de base en ce qu'elle applique un ensemble d'optimisations pour des performances de transfert accrues, une plus forte sécurité, et des frais généraux de signalisation réduits. Ces optimisations entraînent les changements conceptuels suivants au modèle de sécurité [RFC4225] de IPv6 mobile de base :

- L'IPv6 mobile de base effectue des essais périodiques de l'accessibilité d'un nœud mobile à l'adresse de rattachement comme preuve de la possession de l'adresse de rattachement. L'optimisation de chemin améliorée applique une preuve initiale cryptographique de possession de l'adresse de rattachement en combinaison avec une vérification de l'accessibilité du nœud mobile à l'adresse de rattachement afin d'échanger en toute sécurité un jeton secret permanent de génération de clé de rattachement. Le jeton permanent de génération de clé de rattachement est utilisé pour l'authentification cryptographique du nœud mobile durant les enregistrements de correspondant suivants, afin que ces enregistrements de correspondant ultérieurs puissent être liés en toute sécurité à la preuve de possession initiale de l'adresse de rattachement. Aucune autre vérification périodique d'accessibilité à l'adresse de rattachement n'est effectuée.

- L'IPv6 mobile de base exige d'un nœud mobile qu'il prouve son accessibilité à une nouvelle adresse d'entretien durant un enregistrement de correspondant. Cela implique que le nœud mobile et le nœud correspondant doivent échanger des messages Initiation d'essai d'entretien et Essai d'entretien avant que le nœud mobile puisse initier correctement la mise à jour de lien. L'optimisation de chemin améliorée permet au nœud mobile d'initier d'abord la mise à jour de lien et de suivre avec une preuve d'accessibilité à l'adresse d'entretien. Les nœuds mobiles et correspondants peuvent ainsi reprendre les communications plus tôt après un transfert, alors que la vérification d'accessibilité s'effectue concurremment. La quantité de données qu'il est permis au nœud correspondant d'envoyer à l'adresse d'entretien jusqu'à ce que la vérification d'accessibilité s'achève est dictée par l'autorisation fondée sur le crédit.

- La durée de vie maximum de lien pour les enregistrements de correspondant est de 7 minutes dans l'IPv6 mobile de base. Un nœud mobile doit donc périodiquement rafraîchir un enregistrement de correspondant dans les cas où il ne change pas sa connexité IP pendant un certain temps. Le présent protocole augmente la durée de vie maximum de lien à 24 heures, réduisant le besoin de rafraîchissements périodiques à un degré négligeable.

La suite de l'exposé vise les implications de ces changements conceptuels du modèle de sécurité de IPv6 mobile. Elle devrait être vue dans le contexte des considérations sur la sécurité des [RFC3775], [RFC3972], et [RFC4225].

6.1 Propriété de l'adresse de rattachement

L'optimisation de chemin améliorée exige d'un nœud mobile qu'il donne une forte preuve cryptographique [RFC3972] qu'il est le possesseur légitime de l'adresse de rattachement qu'il souhaite utiliser. La preuve se fonde sur la connaissance par le vrai possesseur de l'adresse de rattachement du composant privé d'une paire de clés publique/privée avec les deux propriétés suivantes :

- Comme entrée à une fonction irréversible de génération de CGA avec un ensemble de paramètres auxiliaires de CGA, la clé publique résulte en l'adresse de rattachement du nœud mobile.

- Parmi les paramètres de CGA qui sont fournis à la fonction de génération de la CGA se trouve un modificateur qui, comme entrée à une fonction irréversible d'extension de hachage avec la clé publique, résulte en une chaîne avec un certain nombre minimum de zéros en tête. Trois bits réservés dans l'adresse de rattachement codent ce nombre minimum.

La première propriété lie cryptographiquement l'adresse de rattachement à la clé publique du nœud mobile et, par la vertu du chiffrement à clé publique, à la clé privée. Elle permet au nœud mobile de revendiquer la possession de l'adresse de rattachement en prouvant sa connaissance de la clé privée. La seconde propriété augmente le coût d'une recherche en force brute d'une paire de clés publique/privée qui suffise pour la première propriété. Cela augment la sécurité d'une adresse de rattachement générée cryptographiquement en dépit de sa limitation à 59 bits de signification cryptographique. Appliquer seulement la première propriété permettrait à un attaquant de trouver une paire de clés publique/privée convenable en O(2^59) étapes. En ajoutant la seconde propriété, la complexité d'une recherche en force brute peut être augmentée à O(2^(59+N)) étapes, où N est le nombre minimum de zéros en tête que le résultat de la fonction d'extension du hachage est obligée d'avoir.

En pratique, pour qu'un nœud mobile légitime génère cryptographiquement une adresse de rattachement, le nœud mobile

doit d'abord accomplir une recherche en force brute d'un modificateur convenable, et ensuite utiliser ce modificateur pour exécuter la fonction de génération de CGA. Un attaquant qui voudrait usurper l'adresse de rattachement du nœud mobile, dans ce qu'on appelle un "vol d'adresse IP" [RFC4225], a alors deux options : il pourrait générer sa propre paire de clés publique/privée et effectuer une recherche en force brute d'un modificateur qui, en combinaison avec la clé publique générée, satisfasse les deux propriétés initialement décrites ; ou il pourrait mettre en facteurs entiers la clé publique du nœud mobile, déduire la clé privée correspondante, et copier le modificateur du nœud mobile sans recherche en force brute. Le coût de l'attaque peut être déterminé par le nœud mobile dans l'un et l'autre cas : mettre en facteurs entiers une clé publique devient d'une complexité croissante avec la longueur de la clé publique, et la longueur de clé est à la discrétion du nœud mobile. Le coût d'une recherche en force brute pour un modificateur convenable augmente avec le nombre de zéros en tête que le résultat de la fonction d'extension de hachage doit avoir. Ce nombre est lui aussi un paramètre que le nœud mobile peut choisir. Les attaques en dégradation, par lesquelles l'attaquant réduit le coût d'usurpation d'une adresse de rattachement générée cryptographiquement en choisissant un ensemble de paramètres de CGA qui sont moins sûrs que les paramètres de CGA que le nœud mobile a utilisés pour générer l'adresse de rattachement, sont donc impossibles.

La spécification de la CGA [RFC3972] exige l'utilisation de clés publique et privées RSA, et elle stipule une longueur minimum de clé de 384 bits. Cette exigence a été faite sur mesure pour la découverte sécurisée de voisin IPv6 [RFC3971], l'application originale de la CGA. L'optimisation de chemin améliorée n'augmente pas la longueur minimum de clé parce que, en l'absence d'attaque en dégradation comme expliqué ci-dessus, la capacité d'utiliser des clés courtes ne compromet pas la sécurité des adresses de rattachement qui ont été générées cryptographiquement en utilisant de plus longues clés. De plus, des extensions à la [RFC3972] peuvent éventuellement permettre l'utilisation de classes de clés publique/privées autres que RSA. De telles extensions sont compatibles avec l'application de CGA de l'optmisation de chemin améliorée. On doit cependant faire attention en choisissant la classe et longueur de clé appropriée. Les adresses de rattachement sont normalement plutôt stables par nature, de sorte que les paramètres choisis doivent être sûrs pour une durée de vie d'adresse de rattachement potentiellement longue. Lorsque des clés RSA sont utilisées, une longueur minimum de clé de 1024 bits est donc RECOMMANDÉE.

Bien que la fonction de génération de CGA lie cryptographiquement l'identifiant d'interface d'une adresse de rattachement au préfixe de sous réseau de l'adresse de rattachement, la fonction accepte tout préfixe de sous réseau et donc n'empêche pas un nœud de générer cryptographiquement une adresse de rattachement avec un préfixe de sous réseau usurpé. Par conséquent, la propriété de CGA d'une adresse de rattachement ne garantit pas l'accessibilité du possesseur à l'adresse de rattachement. Ce pourrait être utilisé pour une "attaque d'inondation par retour à la maison" [RFC4225], où l'attaquant utilise sa propre clé publique pour générer cryptographiquement une adresse de rattachement avec un préfixe de sous réseau provenant d'un réseau victime, demande à un nœud correspondant de lier cela à l'adresse d'entretien atuelle de l'attaquant, initie le téléchargement d'un gros fichier via l'adresse d'entretien, et finalement désenregistre le lien ou le laisse expirer. Le nœud correspondant va alors rediriger les paquets téléchargés sur le réseau victime identifié par le préfixe de sous réseau de l'adresse de rattachement usurpée par l'attaquant. Le protocole défini dans le présent document effectue un essai d'accessibilité pour l'adresse de rattachement au moment du premier enregistrement de l'adresse de rattachement avec le nœud correspondant. Cela empêche l'inondation par retour à la maison.

La vérification de la propriété de CGA de l'adresse de rattachement d'un nœud mobile implique un chiffrement à clé publique asymétrique, qui est relativement complexe comparé à la cryptographie symétrique. L'optimisation de chemin améliorée atténue cet inconvénient par l'utilisation de la cryptographie symétrique après une vérification initiale fondée sur la clé publique de l'adresse de rattachement du nœud mobile. Précisément, le nœud correspondant alloue au nœud mobile un jeton permanent de génération de clé de rattachement durant l'enregistrement de correspondant initial sur la base duquel le nœud mobile peut s'authentifier auprès du nœud correspondant durant les enregistrements de correspondant suivants. Une telle authentification permet au nœud correspondant de relier un enregistrement de correspondant suivant à la vérification initiale fondée sur la clé publique de l'adresse de rattachement du nœud mobile. Le jeton permanent de génération de clé de rattachement n'est jamais envoyé en clair ; il est chiffré avec la clé publique du nœud mobile quand il est initialement alloué, et haché de façon irréversible durant les enregistrements de correspondant suivants.

6.2 Propriété de l'adresse d'entretien

Une preuve sûre de possession d'adresse de rattachement peut atténuer la menace de vol d'adresse IP, mais un attaquant peut quand même lier une adresse de rattachement correcte à une fausse adresse d'entretien et par là amener un nœud correspondant à rediriger des paquets, qui autrement seraient livrés à l'attaquant lui-même, sur un tiers. Négliger de vérifier l'accessibilité d'un nœud mobile à l'adresse d'entretien revendiquée pourrait donc causer la contribution involontaire d'un ou plusieurs nœuds correspondants à une attaque d'inondation fondée sur la redirection contre une victime choisie par l'attaquant.

Les attaques d'inondation fondée sur la redirection peuvent cibler un seul nœud, une liaison, ou un routeur ou autre appareil

réseau critique en amont d'un réseau entier. Par conséquent, l'adresse d'entretien usurpée de l'attaquant peut être l'adresse IP d'un nœud, une adresse IP aléatoire d'un préfixe de sous réseau d'une liaison particulière, ou l'adresse IP d'un routeur ou autre appareil du réseau. Une attaque contre un réseau impacte potentiellement un plus grand nombre de nœuds qu'une attaque contre un nœud spécifique, bien que les voisins d'un nœud victime sur une liaison de diffusion souffrent normalement des mêmes dommages que la victime elle-même.

Exiger des nœuds mobiles qu'ils génèrent cryptographiquement les adresses d'entretien de la même façon qu'ils génèrent les adresses de rattachement n'atténuerait que de façon marginale la menace d'inondation fondée sur la redirection. Bien qu'elle empêcherait un attaquant d'enregistrer comme son adresse d'entretien l'adresse IP d'un nœud victime spécifique, l'attaquant pourrait quand même générer une adresse d'entretien différente fondée sur la CGA avec le même préfixe de sous réseau que l'adresse IP de la victime. Les paquets d'inondation redirigés vers cette adresse d'entretien n'auraient pas à être reçus et traités par un nœud spécifique, mais ils impacteraient une liaison ou réseau entier et causeraient donc des dommages comparables. Les adresses d'entretien fondées sur la CGA ont donc peu d'efficacité à l'égard de la protection contre l'inondation. Par ailleurs, elles exigeraient une preuve de possession fondée sur la clé publique d'un coût de calcul élevé à chaque changement de l'adresse d'entretien. Pour ces raisons, l'optimisation de chemin améliorée utilise les adresses d'entretien régulières de IPv6.

Une erreur de conception courante est qu'une forte preuve de possession de l'adresse de rattachement pourrait atténuer la menace d'inondation fondée sur la redirection et par conséquent éliminer le besoin de vérifier l'accessibilité du nœud mobile à une nouvelle adresse d'entretien. Cette notion peut venir de la spécification d'un enregistrement de rattachement dans l'IPv6 mobile de base [RFC3775], qui invite à l'authentification d'un nœud mobile sur la base d'une association de sécurité IPsec, mais n'exige pas qu'elle soit complétée par une vérification de l'accessibilité du nœud mobile à l'adresse d'entretien. Cependant, la raison pour ne pas rendre obligatoire la vérification d'accessibilité pour un enregistrement de rattachement est dans ce cas l'existence d'une relation administrative entre l'agent de rattachement et le nœud mobile, plutôt que le fait que l'agent de rattachement puisse vérifier de façon sûre la possession de l'adresse de rattachement du nœud mobile, ou que l'enregistrement de rattachement soit protégé par IPsec. La relation administrative avec le nœud mobile permet à l'agent de rattachement, d'abord de faire confiance à la correction de l'adresse d'entretien d'un nœud mobile et, ensuite, d'identifier rapidement le nœud mobile si il devait commencer à se comporter de façon malveillante, par exemple, à cause d'une infection par un "malgiciel". Le paragraphe 15.3 de la [RFC3775] et le paragraphe 1.3.2 de la [RFC4225] expliquent ces conditions.

En supposant la confiance, une relation administrative entre le nœud mobile et son agent de rattachement est viable, étant donné que l'agent de rattachement est une partie intégrante des services de mobilité auxquels un utilisateur mobile s'abonne normalement, établit lui-même, ou reçoit sur la base d'une relation d'affaires. Une extension IPv6 mobile [RFC4449] qui développe une clé d'authentification partagée, préconfigurée sur le nœud mobile et le nœud correspondant, présuppose la même relation entre le nœud mobile et un nœud correspondant. Bien que cette hypothèse limite l'applicabilité du protocole (la Section 2 de la [RFC4449] recconnaît cela) elle permet l'omission de la vérification d'accessibilité de l'adresse d'entretien comme dans le cas de l'enregistrement de rattachement. L'optimisation de chemin améliorée ne fait pas d'hypothèse sur la relation entre les nœuds mobiles et correspondants. Cela rend le protocole applicable dans des scénarios arbitraires, mais nécessite que les nœuds correspondants véerifient l'accessibilité du nœud mobile à chaque nouvelle adresse d'entretien.

6.3. Autorisation fondée sur le crédit

L'optimisation de chemin améliorée permet aux nœuds mobiles et correspondants de reprendre des communications bidirectionnelles après un transfert sur le côté nœud mobile avant qu'ait été vérifiée l'accessibilité du nœud mobile à la nouvelle adresse d'entretien par le nœud correspondant. Une telle concurrence en l'absence de la protection appropriée réintroduirait la menace d'inondation fondée sur la redirection, que la vérification d'accessibilité a été à l'origine conçue pour éliminer : étant donné que le nœud correspondant est en général ignorant du délai d'aller-retour au nœud mobile, et comme la vérification d'accessibilité peut échouer due à des pertes de paquets, le nœud correspondant doit accepter une période de concurrence suffisamment longue pour que la vérification d'accessibilité s'achève. Un attaquant pourrait mésuser de cela pour tromper temporairement le nœud correspondant pour qu'il redirige des paquets sur l'adresse IPd'une victime. L'attaquant peut aussi réussir à différer la vérification d'accessibilité en s'enregistrant à nouveau avec le nœud correspondant, éventuellement avec une adresse d'entretien usurpée différente, peu avant que la période de concurrence maximum permise au nœud correspondant ne s'achève et que le nœud correspondant passe ce temps à attendre l'achèvement de la vérification d'accessibilité sans envoyer d'autres paquets. Ce comportement ne peut pas nécessairement être considéré comme malveillant du côté du nœud correspondant car même l'accessibilité d'un nœud mobile légitime peut échouer à être vérifiée avant que l'adresse d'entretien du nœud mobile change à nouveau. Ce peut être dû à une forte mobilité du côté du nœud mobile, ou à des pertes de paquet persistantes sur le chemin entre le nœud mobile et le nœud correspondant. Il n'est généralement pas trivial de décider du côté du nœud correspondant si la partie à l'autre extrémité se

comporte de façon légitime dans des conditions difficiles, ou de façon malveillante.

L'optimisation de chemin améliorée élimine la menace d'inondation fondée sur la redirection en dépit de la vérification d'accessibilité concurrente par l'utilisation de l'autorisation fondée sur le crédit. L'autorisation fondée sur le crédit gère les efforts d'un nœud correspondant pour l'envoi de paquets de charge utile à une adresse d'entretien dans l'état NON VÉRIFIÉ. Ceci est réalisé sur la base des trois hypothèses suivantes :

1. Une attaque d'inondation cherche normalement à glisser à un tiers la charge d'assembler et envoyer les paquets d'inondation. La bande passante est une ressource ample pour de nombreuses victimes attirantes, de sorte que l'effort pour envoyer le fort taux de paquets d'inondation exigé pour entraver la capacité de communication de la victime peut excéder les propres capacités de l'attaquant.

2. L'attaquant peut toujours inonder une victime directement en générant lui-même des paquets bogués et en les envyant à la victime. Une telle attaque n'est pas amplifiée, de sorte que l'attaquant doit être provisionné à générer un flux de paquets suffisant pour mettre la victime à terre.

3. Par conséquent, l'effort supplémentaire pour établir et coordonner une attaque d'inondation fondée sur la redirection n'est payant pour l'attaquant que si le nœud correspondant peut être trompé pour l'amener à contribuer et amplifier l'attaque.

L'inondation fondée sur la redirection non amplifiée n'est donc, du point de vue d'un attaquant, pas plus attractive qu'une pure inondation directe, où l'attaquant envoie lui-même des paquets bogués à la victime. Elle est en fait moins intéressante étant donné que l'attaquant a besoin de maintenir un contexte pour la gestion de la mobilité afin de coordonner la redirection. Sur cette base, l'autorisation fondée sur le crédit annule le motif de l'inondation fondée sur la redirection en empêchant l'amplification qui pourrait être réalisée par elle, plutôt que d'éliminer la redirection des paquets malveillants en premier lieu. La capacité d'envoyer des paquets non désirés est une propriété inhérente des réseaux en mode paquet, et l'inondation directe est une menace qui en résulte. Comme l'inondation directe existe avec et sans la prise en charge de la mobilité, cela constitue une mesure raisonnable en comparaison de la sécurité fournie par l'optimisation de chemin améliorée à la sécurité de l'Internet non mobile. Par l'utilisation de l'autorisation fondée sur le crédit, l'optimisation de chemin améliorée satisfait l'objectif de fournir un niveau de sécurité comparable à celui de l'Internet non mobile.

Comme l'exécuteur d'une attaque d'inondation fondée sur la redirection va jouer le rôle d'un nœud mobile, l'autorisation fondée sur le crédit doit être appliquée sur le côté du nœud correspondant. Le nœud correspondant surveille continuellement les efforts que fait le nœud mobile pour communiquer avec le nœud correspondant. L'effort du nœud mobile est pris comme limite de l'effort que le nœud correspondant peut dépenser pour l'envoi des paquets de charge utile quand l'adresse d'entretien du nœud mobile est dans l'état NON VÉRIFIÉ. La permission du nœud correspondant d'envoyer une quantité limitée de paquets de charge utile à une adresse d'entretien dans l'état NON VÉRIFIÉ permet une reprise immédiate des communications bidirectionnelles une fois que nœud mobile a enregistré une nouvelle adresse IP avec le nœud correspondant après un transfert.

Si ce qui paraît être un nœud mobile est en fait un attaquant qui trompe le nœud correspondant pour rediriger les paquets de charge utile à l'adresse IP d'une victime, l'autorisation fondée sur le crédit assure que le flux de paquets d'inondation cesse avant que l'effort effectué par le nœud correspondant pour générer le flux excède l'effort que l'attaquant a récemment effectué lui-même. L'attaque d'inondation est donc au plus aussi efficace qu'une attaque d'inondation directe, et par conséquent échoue à produire une amplification.

Une autre propriété de l'autorisation fondée sur le crédit est qu'elle n'alloue pas à un nœud mobile de crédit tant que son adresse d'entretien est dans l'état NON VÉRIFIÉ. Cela mérite une justification car il serait techniquement faisable d'allouer un crédit indépendant de l'état de l'adresse d'entretien du nœud mobile. Cependant, l'allocation de crédit pour les paquets reçus d'une adresse d'entretien dans l'état NON VÉRIFIÉ introduirait une vulnérabilité à des attaques soutenues de réflexion. Spécifiquement, un attaquant pourrait causer la redirection de paquets par un nœud correspondant pour l'attaquant à l'adresse IP d'une victime, et la poursuite du flux de paquets vers la victime en reconstituant continuellement son crédit en envoyant des paquets au nœud correspondant. Bien qu'une telle attaque en réflexion fondée sur la redirection échouerait à produire une amplification, elle peut encore être attirante pour un attaquant qui souhaite poursuivre un accueil initial de protocole de transport avec le nœud correspondant – ce qui exige normalement que l'attaquant reçoive des données non devinables -- et redirige le téléchargement après coup sur l'adresse IP de la victime. L'autorisation fondée sur le crédit assure que l'attaquant dans ce cas ne peut pas acquérir de crédit supplémentaire une fois que le téléchargement a été redirigé, et force ainsi l'attaque à se terminer rapidement.

6.4 Attaques de glissement de temps

L'IPv6 mobile de base limite la durée de vie d'un enregistrement de correspondant à 7 minutes et s'arrange ainsi pour que l'accessibilité d'un nœud mobile à ses adresses de rattachement et d'entretien soit revérifiée périodiquement. Cela assure que la vulnérabilité à l'espionnage de la procédure d'acheminement de retour ne peut pas être exploitée par un attaquant qui est seulement temporairement sur le chemin entre le nœud correspondant et l'adresse usurpée de rattachement ou d'entretien. De telles "attaques glissantes dans le temps" [RFC4225] pourraient autrement être mésusées pour un vol d'adresse IP hors du chemin, une inondation sur le retour au point de rattachement, ou d'inondation contre les adresses d'entretien.

L'optimisation de chemin améliorée ne répète ni l'essai initial d'adresse de rattachement ni aucun essai d'adresse d'entretien pour réduire les délais de transfert et les frais généraux de signalisation. Cela ne limite pas la robustesse du protocole aux attaques de vol d'adresse IP parce que la preuve exigée de possession fondée sur la CGA pour les adresses de rattachement élimine déjà de telles attaques. La vérification d'accessibilité n'ajoute pas de protection supplémentaire à cet égard. Par ailleurs, la restriction à une vérification d'accessibilité initiale facilite les attaques d'inondation hors chemin en glissement de temps – soit contre les adresses de rattachement avec des préfixes incorrects, soit contre des adresses d'entretien usurpées -- si l'exécuteur peut s'interposer dans l'échange avant qu'il passe à une localisation différente.

Le choix de conception contre les essais répétés d'adresse de rattachement et d'entretien a été fait sur la base de l'observation que les attaques en glissement de temps sont déjà une menace existante dans l'Internet non mobile d'aujourd'hui. Spécifiquement, un attaquant peut temporairement passer sur le chemin entre une victime et un nœud correspondant, demander un flux de paquets au nœud correspondant au nom de la victime, et ensuite se déplacer à une localisation différente. La plupart des protocoles de transport ne vérifient pas l'accessibilité d'un initiateur à l'adresse IP prétendue après une vérification initiale durant l'établissement d'une connexion. Cela permet à un attaquant de participer seulement à l'établissement de la connexion et de se déplacer ensuite à une position hors du chemin, à partir de laquelle il peut imiter des accusés de réception pour feindre une présence continue à l'adresse IP de la victime. La menace de glissement dans le temps s'applique donc déjà dans l'Internet non mobile.

Il devrait cependant être reconnu que le moment auquel l'optimisation de chemin améliorée vérifie l'accessibilité d'un nœud mobile à une adresse de rattachement ou d'entretien peut bien être antérieur à l'établissement de toute connexion de couche de transport. Cela donne à un attaquant plus de temps pour sortir du chemin entre le nœud correspondant et la victime et ainsi rendre plus faisable une attaque de glissement de temps. Si l'absence de vérification périodique d'accessibilité est considérée être trop risquée, un nœud correspondant peut appliquer des essais supplémentaires d'adresse de rattachement ou d'entretien en limitant la durée de vie d'enregistrement, ou en envoyant des messages Demande de rafraîchissement de lien à un nœud mobile.

6.5 Attaques en répétition

Le protocole spécifié dans le présent document s'appuie sur les numéros de séquence de 16 bits de l'IPv6 mobile de base et les changements périodiques de clé pour éviter des attaques en répétition. Le changement de clés permet aux nœuds mobiles et correspondants de réutiliser les numéros de séquence sans s'exposer eux-mêmes à des attaques en répétition. Il doit être effectué au moins une fois toutes les 24 heures à cause de la durée de vie maximum permise aux liens pour les enregistrements de correspondant. Les nœuds mobiles et correspondants changent aussi de clé chaque fois qu'un retour à zéro de l'espace de numéros de séquence devient imminent. Il est peu probaable que cela arrive fréquemment, cependant, étant donné que les numéros de séquence disponibles sont suffisants pour jusqu'à 32 768 enregistrements de correspondant, chacun consistant en un message de mise à jour de lien précoce et complet. L'espace de numéros de séquence permet donc une moyenne de 22 enregistrements de correspondant par minute sans exposer de besoin de changement de clé pendant les 24 heures de la durée de vie du lien.

6.6 Épuisement des ressources

Bien qu'une preuve de possession d'adresse de rattachement fondée sur la CGA fournisse une protection contre les messages de mise à jour de lien non authentifiés, elle peut exposer un nœud correspondant à des attaques de déni de service car elle exige un chiffrement à clé publique coûteux en calcul. L'optimisation de chemin améliorée limite l'utilisation du chiffrement à clé publique au seul premier enregistrement de correspondant et si/quand le changement de clé est nécessaire. Il est RECOMMANDÉ que les nœuds correspondants suivent en plus la quantité de ressources de traitement qu'elles dépensent sur la vérification de possession d'adresse de rattachement fondée sur la CGA, et qu'ils rejettent les nouveaux enregistrements de correspondant qui impliquent le chiffrement à clé publique quand ces ressources excèdent une limite prédéfinie. La [RFC3972] discute en détails de la faisabilité d'attaques d'épuisement de ressource fondées sur la CGA.

6.7 Possession d'adresse IP du nœud correspondant

L'optimisation de chemin améliorée permet aux nœuds mobiles d'authentifier un message d'accusé de réception de lien reçu sur la base de la propriété de CGA de l'adresse IP du nœud correspondant, pourvu que le nœud correspondant ait une CGA. Le nœud mobile demande cette authentification en incluant une option Demande de paramètres de CGA dans le message de mise à jour de lien qu'il envoie au nœud correspondant, et le nœud correspondant répond en ajoutant ses paramètres de CGA et sa signature au message d'accusé de réception de lien dans les options Paramètres de CGA et Signature. Prouver la possession par le nœud correspondant de son adresse IP protège le nœud mobile contre l'acceptation d'un message d'accusé de réception de lien usurpé et contre la mémorisation du jeton permanent de génération de clé de rattachement inclus pour être utilisé durant les futurs enregistrements de correspondant. Une telle attaque résulterait en un déni de service contre le nœud mobile parce qu'il l'empêcherait d'effectuer toute mise à jour de lien avec le jeton permanent de génération de clé de rattachement obtenu. L'optimisation de chemin améliorée recommande le renouvellement d'un jeton permanent de génération de clé de rattachement en cas de défaillances persistentes d'enregistrement de correspondant, permettant aux nœuds mobiles de récupérer des attaques de déni de service qui impliquent des jetons permanents de génération de clé de rattachement usurpés.

La menace d'attaque de déni de service décrite est dans une certaine mesure atténuée par les exigences de la localisation de l'attaquant : un message de mise à jour de lien qui demande à un nœud correspondant de fournir un jeton permanent de génération de clé de rattachement est authentifié sur la base de la propriété de CGA de l'adresse de rattachement du nœud mobile. Cette méthode d'authentification implique un essai d'adresse de rattachement, qui fournit au nœud mobile un jeton de génération de clé de rattachement sur la base duquel il peut calculer l'authentifiant du message de mise à jour de lien. Comme le nœud mobile s'attend à ce que l'authentifiant du message d'accusé de réception de lien en retour soit calculé avec le même jeton de génération de clé de rattachement, un attaquant qui voudrait usurper un message d'accusé de réception de lien qui inclut un jeton permanent de génération de clé de rattachement doit espionner l'essai d'adresse de rattachement. L'attaquant doit donc être présent sur le chemin du nœud correspondant à l'agent de rattachement du nœud mobile pendant que l'essai d'adresse de rattachement est effectué. De plus, si le message de mise à jour de lien qui demande le jeton permanent de génération de clé de rattachement est achevé, son authentifiant est calculé sur la base d'un jeton de génération de clé d'entretien. L'attaquant doit alors aussi connaître ce jeton de génération de clé d'entretien pour générer l'authentifiant du message d'accusé de réception de lien. Cela exige que l'attaquant soit sur le chemin du nœud correspondant à adresse IP de rattachement actuelle du nœud mobile au moment où le nœud correspondant envoie le jeton de génération de clé d'entretien au nœud mobile dans un message Essai d'adresse d'entretien ou dans l'option Essai d'adresse d'entretien d'un message d'accusé de réception de lien.

Comme un nœud mobile ne saît en général pas si l'adresse IP d'un nœud correspondant particulier est une CGA, le nœud mobile doit être prêt à recevoir un message d'accusé de réception de lien sans options Paramètres de CGA et Signature en réponse à l'envoi d'un message de mise à jour de lien avec une option Demande de paramètres de CGA incluse. En soi, ce comportement obligatoire peut permettre des attaques en dégradation par lesquelles l'attaquant enverrait, au nom du nœud correspondant, un message d'accusé de réception de lien sans options Paramètres de CGA et Signature, prétendant que l'adresse IP du nœud correspondant n'est pas une CGA. L'optimisation de chemin améliorée atténue cette menace en ce qu'elle invite les nœuds mobiles a donner la priorité aux messages d'accusé de réception de lien avec des options Paramètres de CGA et Signature valides sur les messages d'accusé de réception de lien sans ces options. Cela protège contre les attaques en dégradation sauf si l'attaquant peut intercepter les messages d'accusé de réception de lien provenant du nœud correspondant. Étant donné que l'attaquant doit être sur le chemin du nœud correspondant à l'agent de rattachement du nœud mobile à peu près en même temps comme expliqué ci-dessus, l'attaquant peut n'être pas capable d'intercepter les messages d'accusé de réception de lien du nœud correspondant. D'un autre côté, un attaquant qui peut intercepter les messages d'accusé de réception de lien provenant du nœud correspondant est de toutes façons dans une position où il peut poursuivre son déni de service contre le nœud mobile et le nœud correspondant. C'est une menace qui existe déjà dans l'Internet non mobile, et elle n'est pas spécifique de l'optimisation de chemin améliorée.

Des mécanismes externes peuvent permettre au nœud mobile d'obtenir la certitude que l"adresse IP d'un nœud correspondant particulier est une CGA. Le nœud mobile peut alors insister pour avoir la preuve de la possession d'une adresse IP de la part du nœud correspondant, et dans ce cas il va éliminer tous les messages d'accusé de réception de lien reçus qui ne contiennent pas d'options Paramètres de CGA et Signature valides. Un moyen concevable pour que les nœuds mobiles distinguent entre les adresses IPv6 standard et les CGA pourrait être une extension au système des noms de domaines.

7. Constantes et variables de configuration du protocole

La [RFC3972] définit un espace de noms de type de message de CGA à partir duquel les applications de CGA tirent des

étiquettes de type de message de CGA à utiliser dans les calculs de signature. L'optimisation de chemin améliorée utilise la constante suivante, générée de façon aléatoire du type de message de CGA :

0x5F27 0586 8D6C 4C56 A246 9EBB 9B2A 2E13

La [RFC3775] limite la durée de vie pour les liens qui ont été établis avec les nœuds correspondants au moyen de la procédure d'acheminement de retour à MAX_RR_BINDING_LIFETIME *(durée maximum de vie d'enregistrement de lien)*. L'optimisation de chemin améliorée adopte cette limite pour les liens qui sont authentifiés par une preuve de l'accessibilité du nœud mobile à l'adresse de rattachement. Cependant, la durée de vie de lien est limitée à la constante plus généreuse de MAX_CGA_BINDING_LIFETIME *(durée de vie maximum de lien de CGA)* quand le lien est authentifié par la propriété de CGA de l'adresse de rattachement du nœud mobile :

MAX_CGA_BINDING_LIFETIME 86400 seconds

Le vieillissement de crédit incorpore deux variables de configuration pour diminuer graduellement le compteur de crédit d'un nœud mobile au fil du temps. Il est RECOMMANDÉ qu'un nœud correspondant utilise les valeurs suivantes :

CreditAgingFactor : 7/8
CreditAgingInterval : 5 secondes

8. Considérations relatives à l'IANA

Le présent document définit les six nouvelles options de mobilité suivantes, à qui doivent être allouées des valeurs de type dans l'espace de numérotation d'option de mobilité de la [RFC3775] :
- option de mobilité de demande de paramètres de CGA (11)
- option de mobilité Paramètres de CGA (12)
- option de mobilité Signature (13)
- option de mobilité Jeton permanent de générateur de clé de rattachement (14)
- option de mobilité Initiation d'essai d'adresse d'entretien (15)
- option de mobilité Essai d'adresse d'entretien (16)

Le présent document alloue les quatre nouveaux codes d'état suivants pour les messages d'accusé de réception de lien :
- "Jeton permanent de génération de clé de rattachement indisponible" (147)
- "Échec de vérification de CGA et de signature" (148)
- "Jeton permanent de génération de clé de rattachement existant" (149)
- "Indice de nom occasionnel de rattachement non nul attendu" (150)

Les valeurs à allouer pour ces codes d'état doivent toutes être supérieures ou égales à 128, indiquant que le message de mise à jour de lien en question a été rejeté par le nœud correspondant receveur.

Le présent document définit aussi une nouvelle valeur de 128 bits dans l'espace de noms de type de message de CGA de la [RFC3972].

9. Remerciements

Les auteurs remercient Tuomas Aura, Gabriel Montenegro, Pekka Nikander, Mike Roe, Greg O'Shea, Vesa Torvinen (en ordre alphabétique) des précieuses et intéressantes discussions sur les adresses générées cryptographiquement.

Les auteurs remercient aussi Marcelo Bagnulo, Roland Bless, Zhen Cao, Samita Chakrabarti, Greg Daley, Vijay Devarapalli, Mark Doll, Lakshminath Dondeti, Francis Dupont, Lars Eggert, Eric Gray, Manhee Jo, James Kempf, Suresh Krishnan, Tobias Kuefner, Lila Madour, Vidya Narayanan, Mohan Parthasarathy, Alice Qinxia, et Behcet Sarikaya (en ordre alphabétique) pour leur relecture et leurs importants commentaires sur ce document et les prédécesseurs de ce document.

Finalement, les auteurs tiennent aussi à souligner que [Binding] a été le pionnier de l'utilisation des adresses générées cryptographiquement dans le contexte de l'optimisation de chemin IPv6 mobile, et que le présent document consiste largement en matériaux tirés de [CGA-OMI], [Early], et [CBA] et des contributions de leurs auteurs.

10. Références

10.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC3447] J. Jonsson et B. Kaliski, "Normes de cryptographie à clés publiques (PKCS) n° 1 : Spécifications de la cryptographie RSA version 2.1", février 2003. *(Obsolète, remplacée par* RFC8017) *(Information)*

[RFC3775] D. Johnson, C. Perkins, J. Arkko, "Prise en charge de la mobilité dans IPv6", juin 2004. *(P.S.) (Obs., voir* RFC6275)

[RFC3972] T. Aura, "Adresses générées cryptographiquement (CGA)", mars 2005. (*MàJ par* RFC4581, RFC4982) *(P.S.)*

10.1 Références pour information

[AUTHO] Arkko, J. et C. Vogt, "Credit-Based Authorization for Binding Lifetime Extension", Travail en cours, mai 2004.

[Binding] Roe, M., Aura, T., O'Shea, G., and J. Arkko, "Authentication of IPv6 mobile Binding Updates and Acknowledgments", Travail en cours, mars 2002.

[CGA-OMI] Haddad, W., Madour, L., Arkko, J., and F. Dupont, "Applying Cryptographically Generated Addresses to Optimize MIPv6 (CGA-OMIPv6)", Travail en cours, mai 2005.

[CBA] Vogt, C., Arkko, J., Bless, R., Doll, M., and T. Kuefner, "Credit-Based Authorization for IPv6 mobile Early Binding Updates", Travail en cours, mai 2004.

[CAM] O'Shea, G. and M. Roe, "Child-Proof Authentication for MIPv6 (CAM)", ACM SIGCOMM Computer Communication Review, ACM Press, Vol. 31, No. 2, avril 2001.

[DdoS] Mirkovic, J. and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", ACM SIGCOMM Computer Communication Review, Vol. 34, No. 2, ACM Press, avril 2004.

[DoS-AO] Nikander, P., "Denial-of-Service, Address Ownership, and Early Authentication in the IPv6 World", Revised papers from the International Workshop on Security Protocols, Springer-Verlag, avril 2002.

[Early] Vogt, C., Bless, R., Doll, M., and T. Kuefner, "Early Binding Updates for IPv6 mobile", Travail en cours, février 2004.

[IEEE] Vogt, C. and M. Doll, "Efficient End-to-End Mobility Support in IPv6", Proceedings of the IEEE Wireless Communications and Networking Conference, IEEE, avril 2006.

[RFC3971] J. Arkko et autres, "Découverte de voisin sûre (SEND)", mars 2005. (*MàJ par* RFC6494) *(P.S.)*

[RFC4225] P. Nikander et autres, "Fondements des concepts de sécurité de l'optimisation de l'acheminement d'IPv6 mobile", décembre 2005. *(Information)*

[RFC4449] C. Perkins, "Sécurisation de l'optimisation de chemin IPv6 mobile avec une clé partagée statique", juin 2006. *(P.S.)*

[RFC4651] C. Vogt, J. Arkko, "Taxonomie et analyse des améliorations à l'optimisation de l'acheminement IPv6 mobile", février 2007. *(Information)*

[RFC4982] M. Bagnulo, J. Arkko, "Prise en charge de plusieurs algorithmes de hachage dans les adresses générées

cryptographiquement (CGA)", juillet 2007. (*MàJ* RFC3972) *(P.S.)*

Adresse des auteurs

Jari Arkko
Ericsson Research NomadicLab
FI-02420 Jorvas
Finland
mél : jari.arkko@ericsson.com

Christian Vogt
Institute of Telematics
Universitaet Karlsruhe (TH)
76128 Karlsruhe
Germany
mél : chvogt@tm.uka.de

Wassim Haddad
Ericsson Research
8400, Decarie Blvd
Town of Mount Royal
Quebec H4P 2N2, Canada
mél : wassim.haddad@ericsson.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.