Équipe d'ingénierie de l'Internet (IETF)
Request for Comments: 5677
Catégorie : Sur la voie de la normalisation
ISSN: 2070-1721

Traduction Claude Brière de L'Isle

T. Melia, éditeur, Alcatel-Lucent
G. Bajko, Nokia
S. Das, Telcordia Technologies Inc.
N. Golmie, NIST
JC. Zuniga, InterDigital Communications, LLC
décembre 2009

Conception du cadre des services de mobilité (MSFD) IEEE 802.21

Résumé
Le présent document décrit un concept de cadre de services de mobilité (MSFD, *mobility services framework design*) pour le protocole IEEE 802.21 de transfert inter cellulaire indépendant du support (MIH, *Media Independent Handover*) qui vise les problèmes identifiés associés au transport des messages de MIH. Le document décrit aussi les mécanismes pour la découverte des services de mobilité (MoS, *Mobility Services*) et les mécanismes de couche de transport pour la livraison fiable des messages de MIH. Ce document ne fournit pas de mécanisme pour sécuriser la communication entre un nœud mobile (MN, *mobile node*) et le serveur de mobilité. Il est plutôt supposé que les mécanismes de sécurité de couche inférieure (par exemple, la couche de liaison) ou que des solutions de sécurité propriétaires globales spécifiques du système sont utilisées.

Note de l'IESG
Comme décrit plus loin dans cette spécification, ce protocole ne fournit pas de mécanismes de sécurité. Dans certaines situations de déploiement, les services de sécurité de couche inférieure peuvent être suffisants. D'autres situations exigent des mécanismes propriétaires ou des mécanismes standard encore incomplets, comme ceux actuellement considérés par l'IEEE. Pour cette raison, la spécification recommande une analyse attentive avant d'envisager son déploiement.

L'IESG souligne l'importance de ces recommandations. L'IESG note aussi que cette spécification dévie de l'exigence traditionnelle de l'IETF que la prise en charge de la sécurité dans l'environnement Internet ouvert soit une partie obligatoire de toute spécification de protocole sur la voie de la normalisation. Une exception a été faite pour cette spécification, mais cela ne devrait pas être compris comme signifiant que d'autres futures spécifications peuvent s'affranchir de cette exigence.

Table des matières

1. Introduction

Le présent document propose une solution aux questions identifiées dans le document de déclaration de problème [RFC5164] pour le transport de couche 3 des protocoles de MIH IEEE 802.21.

Le problème du transport de couche 3 de MIH est divisé en deux parties principales : la découverte d'un nœud qui prend en charge les services de mobilité (MoS) spécifiques et le transport des informations entre un nœud mobile (MN) et le nœud découvert. Le processus de découverte est exigé pour que le MN obtienne les informations nécessaires à la communication du protocole de MIH avec un nœud homologue. Les informations incluent l'adresse de transport (par exemple, l'adresse IP) du nœud homologue et les types de MoS fournis par le nœud homologue.

Le présent document fait la liste des scénarios de déploiements majeurs de MoS. Il décrit la solution d'architecture, incluant le modèle de référence MSFD et les identifiants de MIHF. Les procédures de découverte de MoS expliquent comment le MN découvre les serveurs de mobilité dans son réseau de rattachement, dans un réseau visité ou dans un réseau tiers. Le reste de ce document décrit l'architecture de transport MIH, des exemples de flux de messages pour plusieurs scénarios de signalisation, et les questions de sécurité.

Le présent document ne fournit pas de mécanisme pour sécuriser la communication entre un nœud mobile et le serveur de mobilité. À la place, il est supposé que des mécanismes de sécurité d'une couche inférieure (par exemple, la couche de liaison) ou des solutions de sécurité propriétaires globales spécifiques du système, sont utilisés. Les détails de tels mécanismes de couche inférieure et/ou propriétaires sortent du domaine d'application de ce document. Il est RECOMMANDÉ d'utiliser ce protocole après avoir analysé attentivement si ces mécanismes satisfont les exigences désirées, et on encourage à de futurs travaux de normalisation dans ce domaine. Le groupe de travail IEEE 802.21a a récemment commencé des travaux sur les questions de sécurité de MIH qui pourraient fournir une solution dans ce domaine. Pour plus d'informations, voir la Section 8.

2. Terminologie

Les acronymes et termes suivants sont utilisés dans ce document :

Transfert inter-cellulaire indépendant du support (MIH, *Media Independent Handover*) : l'architecture de prise en charge du transfert inter-cellulaire défini par le groupe de travail IEEE 802.21 qui consiste en la fonction de MIH (MIHF), en entités réseau de MIH, et en messages du protocole MIH.

Fonction de transfert inter-cellulaire indépendant du support (MIHF, *Media Independent Handover Function*) : fonction de commutation qui fournit des services de transfert inter-cellulaire incluant le service d'événement (ES, *Event Service*) le service d'information (IS, *Information Service*) et le service de commande (CS, *Command Service*) à travers des points d'accès de service (SAP, *service access point*) définis par le groupe de travail IEEE 802.21 [IEEE80221].

Utilisateur MIHF : entité qui utilise les SAP MIH pour accéder aux services MIHF, et qui est chargé d'initier et terminer la signalisation MIH.

Identifiant de fonction de transfert inter-cellulaire indépendant du support (MIHFID, *Media Independent Handover Function Identifier*) : identifiant exigé pour identifier de façon univoque les points d'extrémité de MIHF pour livrer les services de mobilité (MoS) ; il est mis en œuvre comme FQDN ou NAI.

Mobilité de service (MoS, *Mobility of Service*) : composé de service d'information, de service de commande, et de service d'événement fournis par le réseau aux nœuds mobiles pour faciliter la préparation du transfert inter-cellulaire et la décision de transfert inter-cellulaire, comme décrites dans [IEEE80221] et la [RFC5164].

MoSh : mobilité de service fournie par le réseau de rattachement du nœud mobile.

MoSv : mobilité de service fournie par le réseau visité.

MoS3 : mobilité de service fournie par un réseau tiers, qui n'est ni le réseau de rattachement ni le réseau visité courant.

Nœud mobile (MN, *Mobile Node*) : appareil Internet dont la localisation change, avec son point de connexion au réseau.

Protocole de transport de services de mobilité (MSTP, *Mobility Services Transport Protocol*) : protocole utilisé pour livrer les messages du protocole MIH d'une MIHF aux autres nœuds à capacité MIH dans un réseau.

Service d'informations (IS, *Information Service*) : MoS qui a son origine aux couches inférieures ou supérieures de la pile de protocoles et envoie des informations aux couches locales inférieures ou supérieures de la pile de protocoles. L'objet de l'IS est d'échanger des éléments d'information (IE, *information element*) relatifs aux diverses informations sur les réseaux du voisinage.

Service d'événements (ES, *Event Service*) : MoS qui a son origine à une MIHF distante ou aux couches inférieures de la pile locale de protocoles et envoie des informations à la MIHF locale ou aux couches supérieures locales. L'objet de l'ES est de rapporter les changements de l'état de liaison (par exemple, des messages disant que la liaison locale est morte) et divers événements de couche inférieure.

Service de commandes (CS, *Command Service*) : MoS qui envoie des commandes de la MIHF distante ou des couches locales supérieures aux couches inférieures distantes ou locales de la pile de protocoles pour commuter des liaisons ou pour obtenir l'état de la liaison.

Nom de domaine pleinement qualifié (FQDN, *Fully Qualified Domain Name*) : nom de domaine complet pour un hôte sur l'Internet, montrant (dans l'ordre inverse) le chemin de délégation complet de la racine du DNS et du domaine de niveau supérieur jusqu'au nom de l'hôte (par exemple, monexemple.exemple.org).

Identifiant d'accès réseau (NAI, *Network Access Identifier*) : identifiant d'utilisateur qu'un utilisateur soumet durant l'authentification d'accès au réseau [RFC4282]. Pour les usagers mobiles, le NAI identifie l'utilisateur et aide à acheminer le message de demande d'authentification.

Traducteur d'adresse réseau (NAT, *Network Address Translator*) : appareil qui met en œuvre la fonction de traduction d'adresse réseau décrite dans la [RFC3022], dans laquelle les adresses locales ou privées de couche réseau sont transposées en adresses réseau et numéros d'accès acheminables (en dehors du domaine du NAT).

Protocole de configuration dynamique d'hôte (DHCP, *Dynamic Host Configuration Protocol*) : protocoles décrits dans les [RFC2131] et [RFC3315] qui permettent aux appareils de l'Internet d'obtenir des adresses respectivement IPv4 et IPv6, des gabarits de sous réseau, des adresses de passerelle par défaut, et autres informations de configuration IP des serveurs DHCP.

Système des noms de domaine (DNS, *Domain Name System*) : protocole décrit dans la [RFC1035] qui traduit les noms de domaines en adresses IP.

Authentification, autorisation, et comptabilité (AAA, *Authentication, Authorization, and Accounting*) : ensemble de services de gestion de réseau qui déterminent respectivement la validité de l'identifiant d'un utilisateur, déterminent si un utilisateur est autorisé à utiliser les ressources du réseau, et retracer l'utilisation des ressources du réseau par un utilisateur.

AAA de rattachement (AAAh, *Home AAA*) : serveur AAA situé sur le réseau de rattachement du nœud mobile.

AAA visité (AAAv, *Visited AAA*) : serveur AAA situé dans un réseau visité qui n'est pas le réseau de rattachement du nœud mobile.

Accusé de réception de MIH (MIH ACK, *MIH Acknowledgement*) : message de signalisation d'un MIH qu'une MIHF envoie en réponse à un message MIH provenant d'une MIHF envoyeuse.

Point de service (PoS) : instance de MIHF côté réseau qui échange des messages MIH avec une MIHF fondée sur le MN.

Serveur d'accès réseau (NAS, *Network Access Server*) : serveur auquel un MN se connecte initialement quand il essaye d'obtenir la connexion à un réseau et qui détermine si le MN est autorisé à se connecter au réseau du NAS.

Protocole de datagrammes d'utilisateur (UDP, *User Datagram Protocol*) : protocole de couche transport sans connexion utilisé pour envoyer des datagrammes entre une source et une destination à un accès donné, défini dans la RFC 768.

Protocole de contrôle de transmission (TCP, *Transmission Control Protocol*) : protocole de couche transport en mode flux qui fournit un service de livraison fiable avec contrôle d'encombrement, défini dans la RFC 793.

Délai d’aller retour (RTT, *Round-Trip Time*) : estimation du temps exigé pour qu'un segment voyage d'une source à une destination et qu'un accusé de réception retourne à la source, qui est utilisé par TCP dans les connexions avec expirations de temporisateurs pour déterminer quand un segment est considéré comme perdu et devrait être renvoyé.

Unité maximale de transmission (MTU, *Maximum Transmission Unit*) : plus grande taille d'un paquet IP qui peut être envoyée sur un segment de réseau sans exiger de fragmentation [RFC1191].

MTU de chemin (PMTU, *Path MTU*) : plus grande taille d'un paquet IP qui peut être envoyée sur un chemin de réseau de bout en bout sans exiger de fragmentation IP.

Protocole de sécurité de la couche transport (TLS, *Transport Layer Security Protocol*) : protocole de couche application qui assure principalement la confidentialité et l'intégrité des données entre deux entités de réseau communicantes [RFC5246].

Taille maximum de segment d'envoyeur (SMSS, *Sender Maximum Segment Size*) : taille du plus grand segment que l'envoyeur peut transmettre conformément à la [RFC5681].

2.1 Langage des exigences

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].

3. Scénarios de déploiement

Cette section décrit les divers scénarios de déploiement possibles pour le MN et le serveur de mobilité. Le positionnement relatif du MN et du serveur de mobilité affecte la découverte de MoS ainsi que les performances du service de signalisation de MIH. Le présent document vise les scénarios mentionnés dans la [RFC5164] et spécifie les options de transport pour porter le protocole MIH sur IP.

3.1 Scénario S1 : MoS de réseau de rattachement

Dans ce scénario, le MN et les services sont situés dans le réseau de rattachement. On se réfère à cet ensemble de services sous le nom de MoSh comme montré à la Figure 1. Le MoSh peut être situé au réseau d'accès que le MN utilise pour se connecter au réseau de rattachement, ou il peut être situé ailleurs.

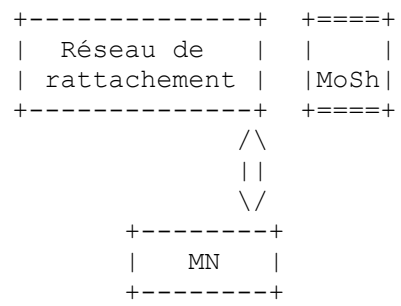


Figure 1 : MoS dans le réseau de rattachement

3.2 Scénario S2 : MoS dans le réseau visité

Dans ce scénario, le MN est dans le réseau visité et les services de mobilité sont fournis par le réseau visité. On appelle cela le MoSv comme montré à la Figure 2.

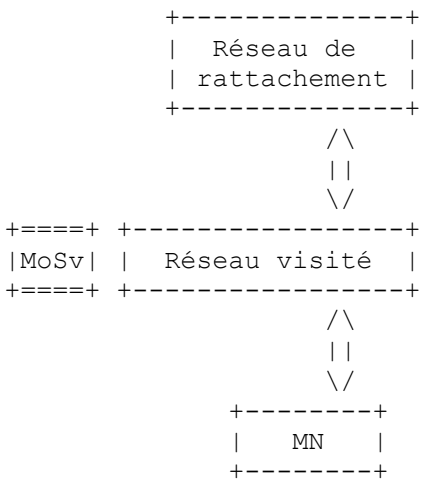


Figure 2 : MoSv dans le réseau visité

3.3 Scénario S3 : MoS tiers

Dans ce scénario, le MN est dans son réseau de rattachement ou dans un réseau visité et les services sont fournis par un réseau tiers. On appelle cette situation MoS3 comme montré à la Figure 3. (Noter que le MoS peut exister à la fois dans le réseau de rattachement et dans les réseaux visités.)

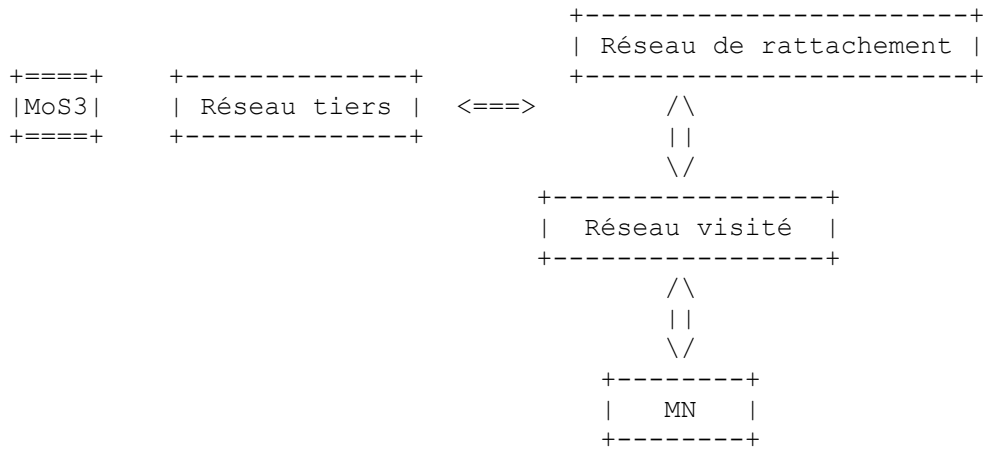


Figure 3 : MoS provenant d'un tiers

3.4 Scénario S4 : MoS en itinérance

Dans ce scénario, le MN est situé dans le réseau visité et tous les services de MIH sont fournis par le réseau de rattachement, comme montré à la Figure 4.

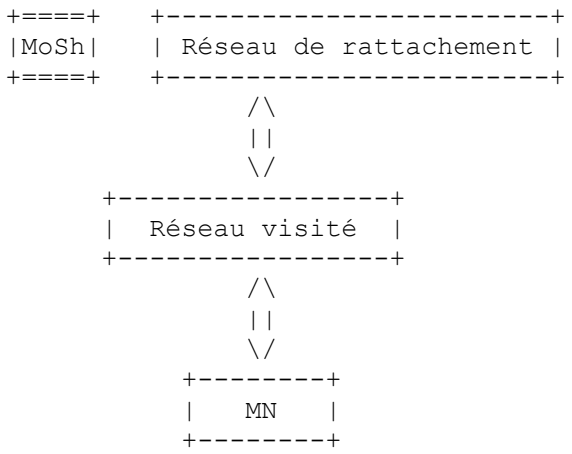


Figure 4 : MoS fourni par le rattachement pendant une visite

Différent types de MoS peuvent être fournis indépendamment des autres types et il n'y a pas de relation stricte entre ES, CS, et IS, ni d'exigence que les entités qui fournissent ces services devraient être co-localisées. Cependant, alors que IS tend à impliquer une grande quantité d'informations statiques, ES et CS sont des services dynamiques et certaines relations entre eux peuvent être attendues, par exemple, une commande de transfert inter-cellulaire (CS) pourrait être produite à réception d'un événement de liaison (ES). Le présent document ne fait aucune hypothèse sur la localisation du MoS (bien qu'il pourrait y avoir des configurations préférées) et vise une MSFD souple pour découvrir les différents services dans les différentes localisations pour optimiser les performances de transfert inter cellulaires. La découverte de MoS est discutée plus en détails dans la Section 5.

4. Vue d'ensemble de la solution

Comme mentionné à la Section 1, l'espace de solutions est divisé en deux domaines fonctionnels : découverte et transport. Les hypothèses suivantes ont été faites :

- La solution vise principalement à prendre en charge les services de MIH de IEEE 802.21 -- à savoir, le service d'informations (IS), le service d'événements (ES), et le service de commandes (CS).

- Si le MIHFID est disponible, le domaine du FQDN ou du NAI est utilisé pour la découverte de service de mobilité.

- Les solutions sont choisies pour couvrir tous les scénarios de déploiement possibles comme décrit à la Section 3.

- La découverte de MoS peut être effectuée durant le rattachement initial au réseau ou à tout instant ensuite.

Le MN peut connaître le domaine du serveur de mobilité à découvrir. Le MN peut aussi être pré-configuré avec l'adresse du serveur de mobilité à utiliser. Dans le cas où le MN ne connaît pas le domaine / serveur de mobilité à interroger, des méthodes d'allocation dynamique sont décrites dans la Section 5.

Il est exigé que la découverte du serveur de mobilité (et la configuration en rapport au niveau MIHF) lie deux homologues MIHF (par exemple, MN et serveur de mobilité) avec leurs adresses IP respectives. La découverte DOIT être exécutée dans les conditions suivantes :

- Amorçage : quand le rattachement à la couche 2 du réseau réussit, il PEUT être exigé que le MN utilise DHCP pour la configuration d'adresse. Ces procédures peuvent porter les informations exigées pour la configuration de MoS dans les options DHCP spécifiques.

- Si le MN ne reçoit pas les informations de MoS durant le rattachement au réseau et si le MN n'a pas de serveur de mobilité pré-configuré, il DOIT faire une procédure de découverte lors de la configuration initiale d'adresse IP.

- Si le MN change son adresse IP (par exemple, sur un transfert inter cellulaire) il DOIT rafraîchir les liens d'homologue MIHF (c'est-à-dire, le processus d'enregistrement de MIHF). Dans le cas où le serveur de mobilité utilisé n'est plus convenable (par exemple, un RTT trop grand a été subi) le MN PEUT devoir effectuer une nouvelle procédure de découverte.

- Si le MN est un appareil multi-rattachements et si il communique avec le même serveur de mobilité via différentes adresses IP, il PEUT lancer les procédures de découverte si une des adresses IP change.

Une fois que l'homologue MIHF a été découvert, les informations de MIH peuvent être échangées entre les homologues MIH sur un protocole de transport comme UDP ou TCP. L'usage des protocoles de transport est décrit à la Section 6 et la mise en paquets des messages de MIH n'exige pas de tramage supplémentaire car le protocole MIH défini dans [IEEE80221] contient déjà un champ Longueur.

4.1 Architecture

La Figure 5 décrit le modèle de référence MSFD et ses composants au sein d'un nœud. La couche du sommet est l'utilisateur MIHF. Cet ensemble d'applications consiste en un ou plusieurs clients MIH qui sont responsables d'opérations comme de générer des interrogations et des réponses, de traiter les déclencheurs de couche 2 au titre de l'ES, et d'initier et traiter les opérations de transfert inter cellulaires au titre du CS. Derrière l'utilisateur MIHF est la MIHF elle-même. Cette fonction est chargée de la découverte de MoS, ainsi que de créer, maintenir, modifier, et détruire les associations de signalisation MIH avec les autres MIHF situées dans les nœuds MIH homologues. En dessous de la MIHF sont divers protocoles de couche transport ainsi que des fonctions de découverte d'adresse.

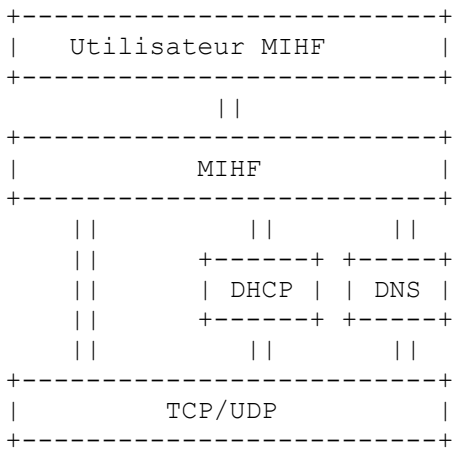


Figure 5 : Pile de MN

La MIHF s'appuie sur les services fournis par TCP et UDP pour transporter les messages de MIH, et s'appuie sur DHCP et le DNS pour la découverte d'homologues. Dans les cas où l'adresse IP de l'homologue MIHF n'est pas pré-configurée, la source MIHF a besoin de la découvrir soit via DHCP, soit par le DNS, comme décrit à la Section 5. Une fois que l'homologue MIHF est découvert, la MIHF doit échanger des messages avec son homologue sur UDP ou TCP. Les recommandations spécifiques concernant le choix des protocoles de transport sont fournies dans la Section 6.

Il n'y a pas de caractéristiques de sécurité actuellement définies au titre du protocole de MIH. Cependant, la sécurité peut être fournie à la couche transport ou à la couche IP lorsque nécessaire. La Section 8 donne des lignes directrices et des recommandations pour la sécurité.

4.2 Identifiants MIHF (FQDN, NAI)

Le MIHFID est exigé pour identifier de façon univoque les points d'extrémité de MIHF pour livrer les services de mobilité (MoS). Donc un identifiant de MIHF doit être unique au sein d'un domaine où des services de mobilité sont fournis et indépendant de la ou des adresses IP configurées. Un MIHFID DOIT être représenté dans la forme d'un FQDN [RFC2181] ou d'un NAI [RFC4282]. Un MIHFID peut être pré-configuré ou découvert par les méthodes de découverte décrites à la Section 5.

5. Découverte de MoS

La méthode de découverte de MoS dépend de si le MN tente de découvrir un serveur de mobilité dans le réseau de rattachement, dans le réseau visité, ou dans un réseau tiers distant qui n'est ni le réseau de rattachement ni le réseau visité. Dans le cas où le MN a déjà une adresse de serveur de mobilité pré-configurée, il n'est pas nécessaire de lancer la procédure de découverte. Si le MN n'a pas un serveur de mobilité pré-configuré, la procédure suivante s'applique.

Dans le cas où un serveur de mobilité est fourni localement (scénarios S1 et S2) les techniques de découverte décrites dans les [RFC5678] et [RFC5679] sont toutes deux applicables comme décrit aux paragraphes 5.1 et 5.2.

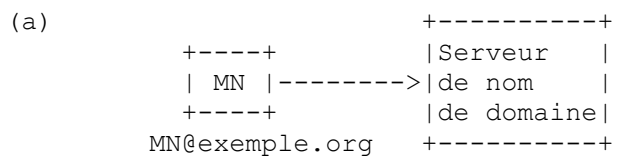
Dans le cas où un serveur de mobilité est situé dans le réseau de rattachement alors que le MN est dans le réseau visité (scénario S4) la découverte fondée sur le DNS décrite dans la [RFC5679] est applicable.

Dans le cas où un serveur de mobilité est situé dans un réseau tiers différent du réseau visité courant (scénario S3) seule la méthode de découverte fondée sur le DNS décrite dans la [RFC5679] est applicable.

On devrait noter que l'autorisation d'un MN d'utiliser un serveur de mobilité spécifique n'est ni dans le domaine d'application du présent document ni actuellement spécifiée dans [IEEE80221]. On suppose de plus que tous les appareils peuvent accéder au MoS découvert. Au cas où de futurs déploiements mettraient en œuvre des politiques d'autorisation, les nœuds mobiles devraient revenir aux autres MoS appris si l'autorisation est refusée.

5.1 Découverte de MoS quand MN et MoSv sont dans le réseau de rattachement (scénario S1)

Pour découvrir un serveur de mobilité dans le réseau de rattachement, le MN DEVRAIT utiliser la méthode de découverte de MoS fondée sur le DNS décrite dans la [RFC5679]. Pour utiliser ce mécanisme, le MN DOIT avoir son domaine de rattachement pré-configuré (c'est-à-dire, que l'abonnement soit lié à un réseau). L'option d'interrogation du DNS est montrée à la Figure 6a. Autrement, le MN PEUT utiliser les options DHCP pour la découverte de MoS [RFC5678] comme montré dans la Figure 6b (dans certains déploiements, un relais DHCP peut n'être pas présent).



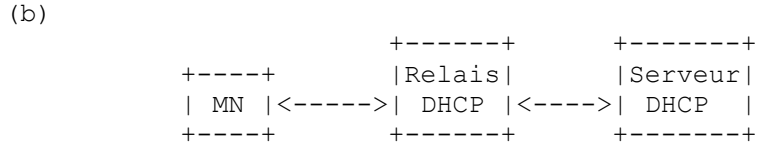


Figure 6 : Découverte de MoS (a) avec interrogation du DNS, (b) avec les options DHCP

5.2 Découverte de MoS quand MN et MoSv sont dans un réseau visité (scénario S2)

Pour découvrir un serveur de mobilité dans le réseau visité, le MN DEVRAIT tenter d'utiliser les options DHCP pour la découverte de MoS [RFC5678] comme montré dans la Figure 7.

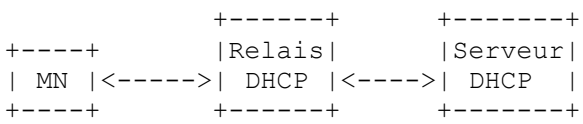


Figure 7 : Découverte de MoS en utilisant les options DHCP

5.3 Découverte de MoS quand les services MIH sont dans un réseau tiers distant (scénario S3)

Pour découvrir un serveur de mobilité dans un réseau distant autre que le réseau de rattachement, le MN DOIT utiliser la méthode de découverte de MoS fondée sur le DNS décrite dans la [RFC5679]. Le MN DOIT d'abord apprendre le nom de domaine du réseau contenant le MoS qu'il cherche. Le MN peut interroger son serveur de mobilité courant pour trouver le nom de domaine d'un réseau spécifique ou le nom de domaine d'un réseau à une localisation spécifique (comme dans la Figure 8a). IEEE 802.21 définit des éléments d'information tels que OPERATOR ID *(identifiant d'opérateur)* et SERVICE PROVIDER ID *(identifiant de fournisseur de service)* qui peuvent être un nom de domaine. Une interrogation d'IS peut fournir cette information, voir [IEEE80221].

Autrement, le MN PEUT interroger un serveur de mobilité connu précédemment pour apprendre le nom de domaine du réseau désiré. Finalement, le MN DOIT utiliser les mécanismes de découverte fondés sur le DNS pour trouver un serveur de mobilité dans le réseau distant comme dans la Figure 8b. On devrait noter que l'étape b peut seulement être effectuée quand on a obtenu le nom de domaine du réseau distant.

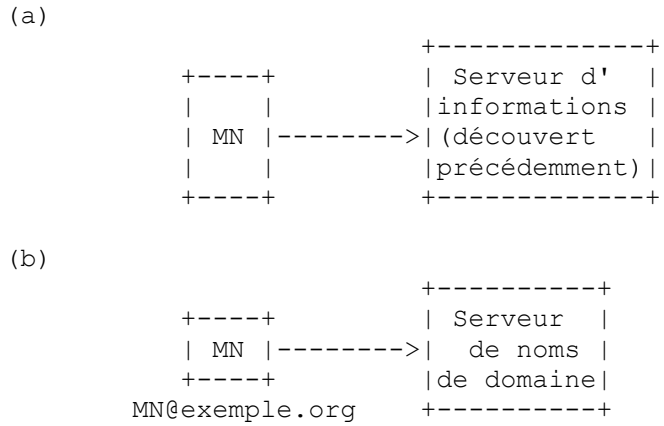


Figure 8 : Découverte de MoS en utilisant (a) l'interrogation d'IS sur un serveur IS connu, (b) l'interrogation DNS

5.4 Découverte de MoS quand le MN est dans un réseau visité et les services dans le réseau de rattachement (scénario S4)

Pour découvrir un serveur de mobilité dans le réseau visité quand les services de MIH sont fournis par le réseau de rattachement, la méthode de découverte fondée sur le DNS décrite dans la [RFC5679] est applicable. Pour découvrir le serveur de mobilité au réseau de rattachement pendant qu'il est dans un réseau visité en utilisant le DNS, le MN DEVRAIT utiliser les procédures décrites au paragraphe 5.1.

6. Options de transport de MIH

Une fois le MoS découvert, les homologues de MIH font une procédure de découverte de capacité et d'abonnement comme spécifié dans [IEEE80221]. Les homologues de MIH PEUVENT échanger des informations sur TCP, UDP, ou tout autre transport pris en charge à la fois par le serveur et le client. Le client PEUT utiliser le mécanisme de découverte du DNS pour découvrir quels protocoles de transport sont supportés par le serveur en plus de TCP et UDP qui sont recommandés dans ce document. Bien que l'un et l'autre protocole puisse fournir la fonction de transport de base exigée, il y a des compromis sur les performances et des caractéristiques uniques associées à chacun qui doivent être considérés dans le contexte des services de MIH pour les différentes conditions de perte et d'encombrement sur le réseau. Les objectifs de cette section sont de discuter ces compromis pour les différents réglages de MIH comme la taille et le débit de message de MIH, et les paramètres de retransmission. De plus, des facteurs comme la traversée de NAT sont aussi discutés. Étant données les exigences de fiabilité pour le transport de MIH, il est supposé dans cette discussion que le mécanisme MIH ACK est à utiliser en conjonction avec UDP, alors qu'il NE DOIT PAS être utilisé avec TCP car TCP inclut des fonctions d'accusé de réception et de retransmission.

6.1 Taille de message de MIH

Bien que la taille de message de MIH varie largement entre 30 octets (pour une demande de découverte de capacité) et environ 65000 octets (pour une primitive de réponse IS MIH_Get_Information) une taille normale de message de MIH pour le ES ou CS va de 50 à 100 octets [IEEE80221]. Donc, la considération des effets de la taille de message de MIH sur les performances du protocole de transport nous amène à discuter deux questions principales, relatives à la fragmentation des longs messages dans le contexte de UDP et à l'enchaînement des messages courts dans le contexte de TCP.

Comme le transport de longs messages de MIH peut exiger la fragmentation qui n'est pas disponible dans UDP, si le MIH utilise UDP, une limite DOIT être établie sur la taille du message MIH fondée sur la PMTU pour la destination (ou la MTU minimum lorsque la PMTU n'est pas mise en œuvre). La MTU minimum dépend de la version IP utilisée pour la transmission, et est le moindre de la MTU du premier bond, et 576 octets pour IPv4 [RFC1122] ou 1280 octets pour IPv6 [RFC2460], respectivement, bien que les applications puissent réduire ces valeurs pour tenir compte de la présence de tunnels.

Conformément à [IEEE80221], quand un message de MIH est envoyé en utilisant la couche L3 ou une couche de transport supérieure, L3 tient compte de tout problème de fragmentation et le protocole MIH ne traite pas la fragmentation dans ce cas. Donc, la fragmentation de couche MIH NE DOIT PAS être utilisée avec la fragmentation de couche IP et NE DOIT PAS être utilisée quand des paquets de MIH sont portés sur TCP.

La perte d'un fragment IP conduit à la retransmission d'un message MIH entier, ce qui à son tour conduit à de mauvaises performances de délai de bout en bout en plus de gaspiller la bande passante. Des recommandations supplémentaires dans la [RFC5405] s'appliquent pour limiter la taille de message MIH quand on utilise UDP et en supposant la fragmentation à la couche IP. Pour ce qui concerne le traitement des messages courts, TCP a la capacité d'enchaîner de très courts messages afin de réduire les frais généraux de bande passante. Cependant, ces frais généraux réduits sont au prix d'un délai supplémentaire pour achever une transaction de MIH, ce qui peut n'être pas acceptable pour CS et ES. Noter aussi que TCP est un protocole en mode flux et mesure les flux de données en termes d'octets, non de messages. Donc, il est possible de partager des messages sur plusieurs segments TCP si ils sont assez longs. Même de courts messages peuvent être étalés sur deux segments. Cela peut aussi causer des délais inacceptables, en particulier si la qualité de la liaison est sévèrement dégradée comme cela va probablement arriver quand le MN sort d'une zone de couverture d'accès sans fil. L'utilisation de l'option TCP_NODELAY peut alléger ce problème en déclenchant la transmission d'un segment plus tôt que le SMSS. (On devrait noter que la [RFC4960] vise ces deux problèmes, mais la discussion de SCTP est omise ici, car il n'est généralement pas utilisé pour les services de mobilité discutés dans le présent document.)

6.2 Débit de messages de MIH

La fréquence des messages de MIH varie conformément au type de service de MIH. On suppose que les messages de CS/ES arrivent à un taux de un par centaine de millisecondes afin de capturer des changements rapides dans les commandes de transfert intercellulaire d'environnement et/ou de processus. Par ailleurs, des messages IS sont échangés principalement chaque fois qu'un nouveau réseau est visité, ce qui peut être de l'ordre d'heures ou de jours. Donc, une salve de courts messages CS/ES ou de longs échanges de messages IS (dans le cas où plusieurs nœuds de MIH demandent des informations) peut conduire à l'encombrement du réseau. Bien que les commandes de limitation de débit incorporées

disponibles dans TCP puissent être bien adaptées pour traiter ces conditions d'encombrement, il peut en résulter de gros délais de transmission qui peuvent être inacceptables pour la livraison en temps utile des messages ES ou CS. Par ailleurs, si UDP est utilisé, un effet de limitation de débit similaire à celui obtenu avec TCP DEVRAIT être obtenu en ajustant de façon adéquate les paramètres d'un régulateur de baquet de jetons comme défini dans les spécifications de MIH [IEEE80221]. Les recommandations pour les réglages de paramètres de baquet de jetons sont comme suit :

- Si la MIHF connaît le RTT (par exemple, fondé sur les échanges de demande/réponse du protocole de MIH entre deux homologues MIH) le débit peut être fondé sur lui comme spécifié dans [IEEE80221].

- Sinon, alors en moyenne elle NE DEVRAIT PAS envoyer plus d'un message UDP toutes les 3 secondes.

6.3 Retransmission

Pour TCP, la temporisation de retransmission est ajustée conformément au RTT mesuré. Cependant du fait du mécanisme de retard exponentiel, le délai associé aux temporisations de retransmission peut augmenter significativement avec l'augmentation de la perte de paquets.

Si UDP est utilisé pour porter les messages de MIH, MIH DOIT utiliser les accusés de réception MIH. Un message MIH est retransmis si son MIH ACK correspondant n'est pas reçu par le nœud générateur dans un intervalle de temporisation établi par la MIHF. Le nombre maximum de retransmissions est configurable et la valeur du temporisateur de retransmission est calculé conformément à l'algorithme défini dans la [RFC2988]. Le nombre maximum par défaut de retransmissions est réglé à 2 et le temporisateur de retransmission initial (TMO) est réglé à 3 s quand le RTT n'est pas connu. Le TMO maximum est réglé à 30 s.

6.4 Traversée de NAT

Il n'y a pas de problème connu pour la traversée de NAT en utilisant TCP. La fin de temporisation de connexion par défaut de 2 heures 4 minutes [RFC5382] (en supposant un maintien en vie de TCP de deux heures) est considérée comme adéquate pour le transport de MIH. Cependant, des problèmes avec la traversée de NAT en utilisant UDP sont documentés dans la [RFC5405]. Des défaillances de communication sont rencontrées quand des boîtiers de médiation détruisent l'état par flux associé à une session d'application durant les périodes où l'application n'échange pas de trafic UDP. Donc, la communication entre le MN et le serveur de mobilité DEVRAIT être capable de traiter en douceur de telles défaillances et de mettre en œuvre des mécanismes pour rétablir leurs sessions UDP. De plus et afin d'éviter de telles défaillances, les messages MIH PEUVENT être envoyés périodiquement, comme les messages de maintien en vie, pour tenter de rafraîchir l'état du boîtier de médiation. Comme la [RFC4787] exige une temporisation d'état minimum de 2 minutes ou plus, les messages MIH qui utilisent UDP comme transport DEVRAIENT être envoyés toutes les 2 minutes. Les messages de réenregistrement ou d'indication d'événement comme définis dans [IEEE80221] PEUVENT être utilisés à cette fin.

6.5 Lignes directrices générales

Les messages ES et CS sont petits par nature et ont des exigences de latence strictes. Par ailleurs, les messages IS sont plus résilients en termes de contraintes de latence, et certains longs messages IS pourraient excéder la MTU du chemin vers la destination. TCP DEVRAIT être utilisé comme transport par défaut pour tous les messages. Cependant, UDP en combinaison avec l'accusé de réception de MIH DEVRAIT être utilisé pour transporter les messages ES et CS qui sont plus courts que, ou égaux à la MTU de chemin comme décrit au paragraphe 6.1.

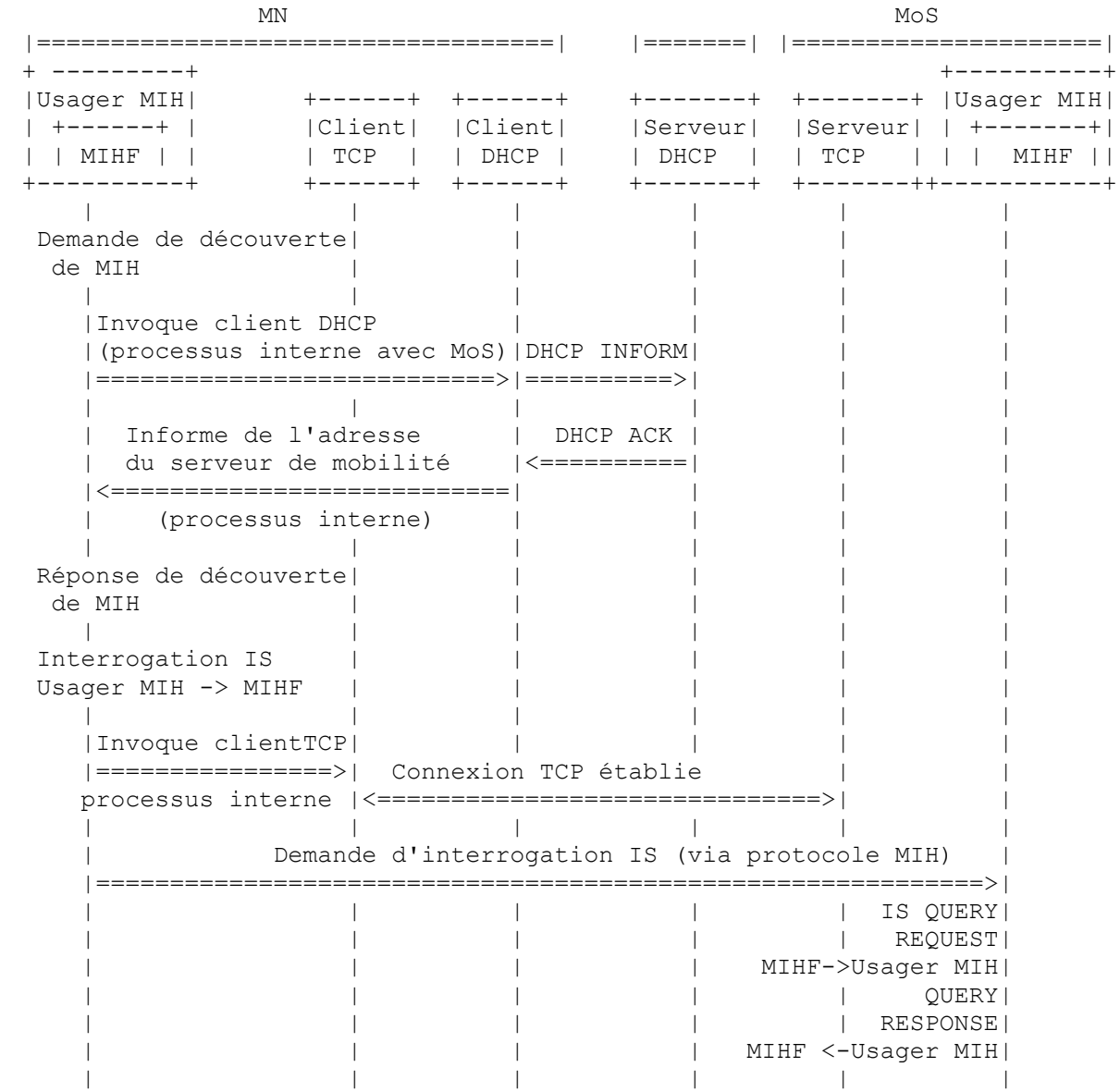
Dans les deux cas de UDP et TCP, si un numéro d'accès n'est pas explicitement alloué (par exemple, par le SRV du DNS) les messages de MIH envoyés sur UDP, TCP, ou autre transport pris en charge DOIVENT utiliser le numéro d'accès par défaut défini à la Section 9 pour ce transport particulier.

Un serveur de mobilité DOIT prendre en charge UDP et TCP pour le transport de MIH et le MN DOIT prendre en charge TCP. De plus, le serveur et le MN PEUVENT prendre en charge des mécanismes de transport supplémentaires. Le MN PEUT utiliser les procédures définies dans la [RFC5679] pour découvrir des protocoles de transport supplémentaires pris en charge par le serveur (par exemple, SCTP).

7. Flux d'opérations

La Figure 9 donne un exemple de flux d'opérations entre des homologues MIHF quand un utilisateur de MIH demande un IS et que le MN et le serveur de mobilité sont tous deux dans le réseau de rattachement du MN. DHCP est utilisé pour la découverte des services de mobilité (MoS) et TCP est utilisé pour établir une connexion de transport pour porter les messages IS. Quand le serveur de mobilité n'est pas pré-configuré, l'utilisateur MIH a besoin de découvrir l'adresse IP du serveur de mobilité pour communiquer avec la MIHF distante. Donc, l'utilisateur MIH envoie un message de demande de découverte à la MIHF locale comme défini dans [IEEE80221].

Dans cet exemple (on pourrait décrire des mécanismes similaires avec DHCPv6) on suppose que la découverte de MoS est effectuée avant l'établissement d'une connexion de transport avec la MIHF distante, et le processus de client DHCP est invoqué via des API internes. Le client DHCP envoie un message DHCP INFORM conformément au DHCP standard et avec l'option MoS comme défini dans la [RFC5678]. Le serveur DHCP répond via un message DHCP ACK avec l'adresse IP du serveur de mobilité. L'adresse du serveur de mobilité est alors passée à la MIHF locale via des API internes. La MIHF génère le message de réponse de découverte et le passe à l'utilisateur MIH correspondant. L'utilisateur MIH génère une interrogation IS adressée au serveur de mobilité distant. La MIHF invoque le client TCP sous-jacent, qui établit une connexion de transport avec l'homologue distant. Une fois la connexion de transport établie, la MIHF envoie l'interrogation IS via un message REQUEST de protocole MIH. Le message et l'interrogation arrivent à la MIHF et utilisateur MIH de destination, respectivement. Le serveur de mobilité de l'utilisateur MIH répond à l'interrogation IS correspondante et le serveur de mobilité de la MIHF envoie la réponse IS via un message RESPONSE de protocole MIH. Le message arrive à la MIHF de source, qui passe la réponse IS à l'utilisateur MIH correspondant.



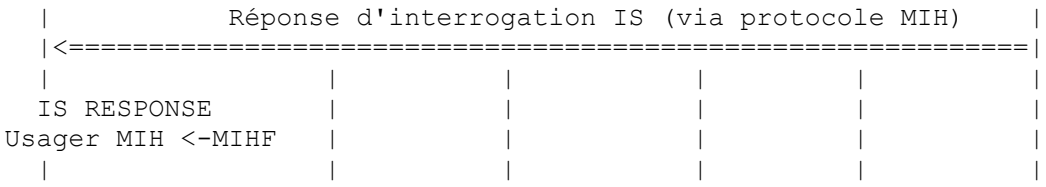


Figure 9 : Exemple de flux d'opérations impliquant l'utilisateur de MIH

8. Considérations sur la sécurité

Il y a deux composantes des considérations sur la sécurité : la découverte de MoS et le transport de MIH. Pour la découverte de MoS, les recommandations de DHCP et du DNS sont fournies ici selon les lignes directrices de l'IETF. Pour le transport de MIH, on décrit les menaces pour la sécurité et on s'attend à ce que le système ait les moyens d'atténuer de telles menaces quand des informations sensibles sont échangées entre le nœud mobile et le serveur de mobilité. Comme la spécification de base IEEE 802.21 ne fournit pas de sécurité au niveau du protocole MIH, on suppose qu'une sécurité de couche inférieure (par exemple, la couche de liaison) ou des solutions de sécurité spécifiques du système (par exemple, propriétaires) sont disponibles. Le présent document ne fournit aucune ligne directrice à cet égard. On souligne que le groupe de travail IEEE 802.21a a récemment commencé un travail sur les questions de sécurité de MIH qui pourrait fournir des solutions dans ce domaine. Finalement, l'autorisation d'un MN d'utiliser un serveur de mobilité spécifique, comme déclaré à la Section 5, n'est ni dans le domaine d'application du présent document ni actuellement spécifié dans [IEEE80221].

8.1 Considérations sur la sécurité pour la découverte de MoS

Un certain nombre de problèmes de sécurité doivent être pris en compte durant la découverte de nœud. Dans le cas où DHCP est utilisé pour la découverte de nœud et où l'authentification de la source et du contenu des messages est exigée, les administrateurs de réseau DEVRAIENT utiliser l'option d'authentification DHCP décrite dans la [RFC3118], lorsque disponible, ou s'appuyer sur la sécurité de couche de liaison. La [RFC3118] fournit des mécanismes pour l'authentification d'entité et de message. Dans le cas où le mécanisme d'authentification DHCP n'est pas disponible, les administrateurs peuvent devoir s'appuyer sur la sécurité de la couche de liaison sous-jacente. Dans ce cas, la liaison entre le client DHCP et le point de terminaison de couche 2 peut être protégée, mais la source du message DHCP et ses messages ne peuvent pas être authentifiés ni l'intégrité de ces derniers vérifiée sauf si il existe un lien de sécurité entre la couche de liaison et la couche DHCP.

Dans le cas où le DNS est utilisé pour découvrir le MoS, des fausses demandes et réponses du DNS peuvent causer, respectivement, des dénis de service (DoS) et l'incapacité du MN à effectuer un transfert inter cellulaire approprié. Lorsque les réseaux sont exposés à de telles attaques de DoS, il est RECOMMANDÉ que les fournisseurs de service DNS utilisent les extensions de sécurité du système des noms de domaines (DNSSEC, *Domain Name System Security Extensions*) comme décrites dans la [RFC4033]. Les lecteurs peuvent aussi se référer à la [RFC4641] pour considérer les aspects des pratiques de fonctionnement de DNSSEC.

8.2 Considérations sur la sécurité pour le transport MIH

La communication entre un MN et un serveur de mobilité est exposée à un certain nombre de menaces pour la sécurité:

- Usurpation d'identité de serveur de mobilité. Un faux serveur de mobilité pourrait fournir au MN des données boguées et le forcer à choisir le mauvais réseau ou à prendre une mauvaise décision de transfert inter cellulaire.

- Altération. L'altération des informations fournies par un serveur de mobilité peut résulter en ce que le MN prenne de mauvaises décisions de choix de réseau ou de transfert inter cellulaire.

- Attaques en répétition. Comme les services de mobilité définis dans [IEEE80221] prennent en charge un modèle "PUSH", ils peuvent envoyer de grandes quantités de données aux MN chaque fois que le serveur de mobilité pense que les données sont pertinentes pour le MN. Un attaquant peut intercepter les données envoyées par le serveur de mobilité au MN et les répéter ultérieurement, causant au MN la prise de décisions de choix de réseau ou de transfert inter cellulaire qui ne sont pas valides à ce moment.

- Espionnage. En espionnant les communications entre un MN et un serveur de mobilité, un attaquant peut être capable de retracer les mouvements d'un utilisateur entre les réseaux ou les cellules, ou prédire les futurs mouvements, en inspectant les messages de service de transfert inter cellulaire.

De nombreuses solutions de sécurité de système spécifiques du déploiement sont disponibles, qui peuvent être utilisées pour établir des contre-mesures aux menaces susmentionnées. Par exemple, pour les scénarios MoSh et MoSv (y compris les scénarios d'itinérance) la sécurité de couche de liaison peut être suffisante pour protéger la communication entre le MN et le serveur de mobilité. C'est un environnement typique d'opérateur mobile où la sécurité de la couche de liaison fournit l'authentification, la confidentialité, et l'intégrité des données. Dans d'autres scénarios, comme le MoS de tiers, les solutions de sécurité de couche de liaison peuvent n'être pas suffisantes pour protéger le chemin de communication entre le MN et le serveur de mobilité. Le canal de communication entre MN et serveur de mobilité doit être sécurisé par d'autres moyens.

Le présent document ne fournit pas de lignes directrices spécifiques sur la façon dont ces solutions de sécurité devraient être déployées. Cependant, si à l'avenir, le groupe de travail IEEE 802.21 amende la spécification avec de la sécurité au niveau du protocole MIH ou recommande le déploiement de scénarios, l'IETF pourra revisiter les considérations sur la sécurité et recommander une sécurité spécifique de la couche transport comme approprié.

9. Considérations relatives à l'IANA

Le présent document enregistre les accès TCP et UDP suivants auprès de l'IANA :

Mot-clé	**Décimal**	**Description**
ieee-mih	4551/tcp	Services MIH
ieee-mih	4551/udp	Services MIH

10. Remerciements

Les auteurs remercient Yoshihiro Ohba, David Griffith, Kevin Noll, Vijay Devarapalli, Patrick Stupar, et Sam Xia de leurs précieux commentaires, relectures, et des discussions fructueuses.

11. Références

11.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. DOI 10.17487/RFC2119, *(MàJ par* RFC8174)

[RFC2181] R. Elz et R. Bush, "Clarifications pour la spécification du DNS", DOI 10.17487/RFC2181, juillet 1997. *(P.S., MàJ par* RFC4035, RFC2535, RFC4343, RFC4033, RFC4034, RFC5452, RFC8767)

[RFC3118] R. Droms et W. Arbaugh, "Authentification des messages DHCP", juin 2001. *(P.S.)*

[RFC3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins et M. Carney, "Protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", juillet 2003. (*MàJ par* RFC6422 et RFC6644, RFC7227 *; rendue obsolète par* RFC8415)

[RFC4033] R. Arends, et autres, "Introduction et exigences pour la sécurité du DNS", mars 2005, DOI 10.17487/RFC4033

[RFC4282] B. Aboba et autres, "L'identifiant d'accès réseau", décembre 2005. *(P.S., Remplacée par* RFC7542)

[RFC5678] G. Bajko, S. Das, "Options du protocole de configuration dynamique d'hôte (DHCPv4 et DHCPv6) pour la découverte de services de mobilité IEEE 802.21", décembre 2009. *(P. S.)*

[RFC5679] G. Bajko, "Localisation des services de mobilité IEEE 802.21 avec le DNS" décembre 2009. *(P. S.)*

11.2 Références pour information

[IEEE80221] "IEEE Standard for Local and Metropolitan Area Networks - Part 21: Media Independent Handover Services", IEEE LAN/MAN Std 802.21-2008, janvier 2009. http://www.ieee802.org/21/private/Published%20Spec/802.21-2008.pdf (l'accès au document est réservé aux membres).

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", DOI 10.17487/RFC1035, STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604, 7766, 8482, 8767)

[RFC1122] R. Braden, "Exigences pour les hôtes Internet – couches de communication", STD 3, DOI 10.17487/RFC1122, octobre 1989. *(MàJ par* RFC6633, 8029, 9293)

[RFC1191] J. Mogul et S. Deering, "Découverte de la MTU de chemin", DOI 10.17487/RFC1191, novembre 1990.

[RFC2131] R. Droms, "Protocole de configuration dynamique d'hôte", mars 1997. *(DS) (Mà J par* RFC3396, RFC4361, RFC5494, et RFC6849)

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6)", décembre 1998. *(MàJ par* 5095, 6564 *; D.S ; Remplacée par* RFC8200, STD 86*)*

[RFC2988] V. Paxson, M. Allman, "Calcul du temporisateur de retransmission de TCP", novembre 2000. *(P.S.)(Obs., voir* RFC6298)

[RFC3022] P. Srisuresh, K. Egevang, "Traducteur d'adresse réseau IP traditionnel", janvier 2001. *(Information)*

[RFC4641] O. Kolkman, R. Gieben, "Fonctionnement pratique de DNSSEC", septembre 2006. *(Remplace* RFC2541*) (Information)*

[RFC4787] F. Audet, éd., C. Jennings, "Exigences sur le comportement des traducteurs d'adresse réseau (NAT) pour UDP en envoi individuel", janvier 2007, DOI 10.17487/RFC4787. (BCP0127) *(MàJ par* RFC7857)

[RFC4960] R. Stewart, éd., "Protocole de transmission de commandes de flux (SCTP)", septembre 2007. (*Remplace* RFC2960, RFC3309 ; *P.S. ; Remplacée par* RFC9260)

[RFC5164] T. Melia, "Transport des services mobiles : position du problème", mars 2008. *(Information)*

[RFC5246] T. Dierks, E. Rescorla, "Version 1.2 du protocole de sécurité de la couche Transport (TLS)", DOI 10.17487/RFC5246, août 2008. *(P.S.* ; *remplace* RFC3268, 4346, 4366 ; *MàJ* RFC4492 ; *rendue obsolète par la* RFC8446)

[RFC5382] S. Guha et autres, "Exigences sur le comportement des NAT pour TCP", octobre 2008, DOI 10.17487/RFC5382. (BCP0142) *(MàJ par* RFC7857)

[RFC5405] L. Eggert, G. Fairhurst, "Lignes directrices pour l'utilisation d'UDP en envoi individuel pour les concepteurs d'applications", novembre 2008. (BCP0145 *; MàJ par* RFC8085)

[RFC5681] M. Allman, V. Paxson, E. Blanton, "Contrôle d'encombrement de TCP", DOI 10.17487/RFC5681, septembre 2009. *(Remplace* RFC2581*) (D.S.)*

Adresse des auteurs

Telemaco Melia
Alcatel-Lucent
Route de Villejust
Nozay 91620
France
mél : telemaco.melia@alcatel-lucent.com

Gabor Bajko
Nokia
mél : Gabor.Bajko@nokia.com

Subir Das
Telcordia Technologies Inc.
mél : subir@research.telcordia.com

Nada Golmie
NIST
mél : nada.golmie@nist.gov

Juan Carlos Zuniga
InterDigital Communications, LLC
mél : j.c.zuniga@ieee.org