ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية
---

(12) BREVET D'INVENTION

(11) N° de publication :
MA 39223 A1

(51) Cl. internationale :
H04L 9/00; H04L 29/00

(43) Date de publication :
31.01.2018

(21) N° Dépôt :
39223

(22) Date de Dépôt :
26.07.2016

(71) Demandeur(s) :
Université Mohammed V Rabat, Avenue des Nations Unies, Agdal, bp 8007 NU Rabat, 10000 (MA)

(72) Inventeur(s) :
ECH-CHERIF EL Kettani Mohamed Dafir ; Baddi youssef

(74) Mandataire :
FATIMA ZAOUI

(54) Titre : **Methode d'adaptation du protocole PIM-SM pour le partage dynamique des clés de cryptage dans le multicast mobile IPv6**

(57) Abrégé : La gestion des clés représente un élément majeur dans la sécurisation des communications de groupe, elle areçu une attention particulière au niveau des communautés de recherche universitaires ainsi que dans l'industrie.Cela est dû à la pertinence économique des applications basées sur les communications de groupe telles que,IPrV, vidéoconférence, jeux de groupe. La gestion des clés concerne la distribution et la mise à jour des clés àchaque fois qu'un membre rejoint ou quitte le groupe. L'aspect dynamique des applications de groupe qui offre laliberté aux membres de rejoindre et de quitter un ou plusieurs groupes de communication, en plus de la mobilitédes membres rend la conception des protocoles de gestion des clés efficaces et évolutives un souci difficile. Pourdéployer avec succès de nombreux services basés sur les communications de groupe dans un environnementmobile, l'infrastructure et les protocoles de gestion des clés doivent être développées a fin de gérer les clés decryptage nécessaires pour fournir un contrôle d'accès au contenu partage.

Abrégé

La gestion des clés représente un élément majeur dans la sécurisation des communications de groupe, elle a reçu une attention particulière au niveau des communautés de recherche universitaires ainsi que dans l'industrie. Cela est dû à la pertinence économique des applications basées sur les communications de groupe telles que, IPTV, vidéoconférence, jeux de groupe. La gestion des clés concerne la distribution et la mise à jour des clés à chaque fois qu'un membre rejoint ou quitte le groupe. L'aspect dynamique des applications de groupe qui offre la liberté aux membres de rejoindre et de quitter un ou plusieurs groupes de communication, en plus de la mobilité des membres rend la conception des protocoles de gestion des clés efficaces et évolutives un souci difficile. Pour déployer avec succès de nombreux services basés sur les communications de groupe dans un environnement mobile, l'infrastructure et les protocoles de gestion des clés doivent être développées a fin de gérer les clés de cryptage nécessaires pour fournir un contrôle d'accès au contenu partage.

Titre : Méthode d'adaptation du protocole PIM-SM pour le partage dynamique des clés de cryptage dans le multicast mobile IPv6

Description

Notre invention est une combinaison modifiée et adaptée de trois domaines informatiques : les communications de groupe (multicast IP), le mobile IPv6 et la gestion des clés de cryptage de groupe (Group Key Management). Dans le but de réaliser une session multicast sécurisée dans un environmenet mobile.

La croissance phénoménale de l'Internet au cours des dernières années et l'augmentation de la bande passante dans les réseaux d'aujourd'hui ont fourni à la fois source d'inspiration et de motivation pour le développement de nouvelles applications et services pour répondre à de nouveaux besoins combinant voix, vidéo et texte "sur IP", tels que la télévision sur Internet, la diffusion de news, la vidéoconférence, les jeux multijoueurs sur internet, et l'apprentissage interactif à distance. Ces applications ont un caractère de groupe où le contenu doit être diffusé à plusieurs parties pour former une communication de groupe. Ce mode de communication complexe a été réalisé avec des liaisons point-a-point supportées par les réseaux informatiques classiques. Ces derniers ne sont pas optimaux pour ce type d'applications.

Le concept de communication de groupe et le multicast IP ont vu le jour lors des études de recherche doctorale de Deering vers la fin des années 80 et plus précisément en 1988 où le premier tunnel de diffusion multicast a été établi entre l'université de Stanford 1 et BBN 2. Le premier modèle de communication multicast a été proposé à la communauté de l'IETF par Steve Deering et David Cheriton. Il a étendu le protocole IP pour permettre d'identifier un "groupe" associé à une classe d'adresses IP. Les révisions ultérieures et raffinements de ce modèle ont été spécifiés dans la RFC 1112, qui est la référence définitive du modèle communément appelé ASM. Ces travaux de spécifications ont été suivis par un essai à grande échelle au cours de la diffusion audio de la réunion qui a eu lieu dans les bureaux de l'IETF à San Diego en 1992.

Plutôt que d'envoyer des données à un récepteur unique (le mode unicast), ou à tous les récepteurs sur un réseau donné (mode broadcast), le mode de communication multicast ou de groupe, comme défini par Steve Deering, vise à fournir des données à un ensemble de nœuds envoyés par une source en un seul exemplaire; le réseau duplique alors le paquet tant que cela s'avère nécessaire jusqu'à ce qu'une copie de chaque paquet atteigne l'un des récepteurs visés. Cela évite des frais supplémentaires de traitement associés à la réplication des paquets au niveau de la source et ceux de la bande passante à cause de l'envoi de paquets dupliqués sur le même lien.

Actuellement, le protocole PIM-SM spécifié dans la RFC4601 est le protocole favori dans le réseau MBONE pour des raisons de performance et d'efficacité. Le protocole PIM-SM, contrairement aux autres protocoles de routage multicast (DVMRP et MOSPF et PIM-DM), construit un arbre partagé avec Point de Rendez-vous commun à toutes les sources et récepteurs de la topologie pour router les paquets multicast. C'est pour cette raison que nous accordons une attention particulière au protocole PIM-SM.

Après plusieurs années d'adaptation du modèle de Deering pour les réseaux informatiques statiques, la mobilité est devenue une technologie clé de la prochaine génération d'Internet et a été normalisée au sein de l'IETF.

Le protocole Mobile IP définit des mécanismes pour supporter des nœuds mobiles dans les réseaux de communication. Il fonctionne en utilisant deux adresses IP pour chaque nœud mobile : une première adresse IP statique, appelée Home-of-address (HoA) lié au réseau d'origine appelé Home Network permettant l'identification; et une deuxième adresse IP, appelée Care-of-Address (CoA) dynamique pour le routage. De cette façon, quand un nœud mobile NM se déplace vers un autre réseau, il sera toujours en mesure de communiquer avec d'autres hôtes.

Vu l'incompatibilité des communications de groupe standardisées avec le protocole mobile IPv6), l'IETF propose deux approches pour intégrer les protocoles de routage multicast dans les réseaux mobiles IP : Home

Subscription et RemoteSubscription. Ces deux techniques présentent une solution pour rendre les communications multicast possibles dans un environmenet mobile, sauf qu'ils ne traitent pas la question de la sécurité de ces communications.

En effet, dans un environnement mobile où les membres peuvent se déplacer à l'intérieur et l'extérieur du réseau d'origine, le protocole de gestion des clés de cryptage doit prendre en considération non seulement une gestion d'appartenance dynamique à un ou plusieurs groupes multicast (rejoindre et quitter), mais aussi avec l'emplacement de membre dynamique. Lorsqu'un membre multicast (source ou récepteur) se déplace d'un sous-réseau à un autre, la complexité de gestion des clés augmente puisque le membre multicast n'a pas identifié de la même façon dans le nouveau sous-réseau.

Dans toutes les solutions proposées, un handover introduit une mise à jour totale des clés de cryptage dans le nouveau et l'ancien sous-réseau. Vu que le membre multicast est considéré comme un membre multicast quittant la session multicast dans l'ancien sous-réseau et comme un nouveau membre multicast joignant la même session multicast dans le nouveau sous-réseau.

Description des dessins

Figure 1: présente un arrangement de 4 zones intercouplés constituant un domaine de routage multicast

Figure 2: les états d'un récepteur multicast mobile durant une session multicast en mobile IPv6

Figure 3: la structure de l'architecture réseau proposée avec les agents et les messages de signalisation et données

Erreur ! Source du renvoi introuvable.: diagramme d'échange de messages entres les agents du domaine de routage multicast

Description du procédé

Description fonctionnelle

La confidentialité dans les communications de groupe exige que seuls les membres du groupe puissent lire et traiter les données multicast même si les données sont diffusées dans l'ensemble du réseau.

Généralement, la diffusion des données ayant une valeur commerciale ou de l'État contenu des informations top-secret nécessite l'utilisation de mécanismes appropriés pour empêcher les destinataires nonlégitimes d'avoir accès au contenu. Afin de garantir la confidentialité des communications de groupe, seuls les clients autorisés pour le service auraient accès au contenu pour seulement la durée correspondant à leur autorisation.

Une solution simple consiste à crypter les données destinées au groupe multicast par la source avec une clé de groupe, appelé TrafficEncryption Key (TEK), commun à tous les récepteurs multicast autorisés. Par conséquent, ce chiffrement symétrique devrait empêcher les autres utilisateurs d'avoir accès au contenu. Cette clé est générée par un agent appelé Domaine Key destributor DKD.

Ces fonctionnalités en relation avec la confidentialité font partie d'un système de gestion des clés de cryptage ou Group Key Management protocol (GKM). Le rôle d'un protocole GKM est de générer, mettre à jour et distribuer les clés TEKsaux membres du groupe légitimes.

La gestion des clés de cryptage des groupes de communication multicast dans un environnement mobile est totalement influencée par les informations d'appartenance au groupe. Par conséquent, il existe plusieurs critères pour évaluer une solution de gestion des clés de cryptage de groupe multicast telles que l'évolutivité, la sécurité de rejoindre / quitter une session multicast, le nombre de clés de crypatege nécessaire par agent oucontrôleur, le

nombre de clés nécessaire au niveau des membres du groupe multicast, et le temps de traitement nécessaire pour la gestion des clés.

Pour assurer une parfaite confidentialité en amont et en aval, un système de mise a jour de clés, appelé aussi une fonction de rekeying, doit être effectuée chaque fois qu'il ya des changements d'appartenance dans le groupe : lorsque la durée autorisée pour un récepteur multicast expire, un récepteur multicast quitte explicitement une session multicast, ou un récepteur multicast mobile change de sous réseau. Consuquent, il est nécessaire de modifier la clé de groupe commun vers une nouvelle clé pour empêcher le récepteur en question d'avoir accès au contenu.

L'impact de ce processus de rekying sur les membres du groupe multicast, communément appelé le phénomène 1-affecte-n, mesure le nombre de membres touchés par un processus de requin. Ce phénomène est un problème difficile dans la conception de protocoles de gestion des clés de groupe. Si la taille du groupe ne cesse d'augmenter, un tel phénomène sera significativement sur la qualité de la performance du système de la diffusion multicast.

L'objectif de notre invention est de présenter une solution au problème de rekiying lorsqu'un membre multicast mobile change de location d'un réseau ou sous-réseau à un autre. En se basant sur le protocole de routage multicast PIM-SM pour créer des sous-systèmes de routage multicast local ce qui limite l'impacte de la mobilité d'un récepteur multicast à ce dernier et sans impacter tout le système de routage multicast.

Nous introduisons une entité de sécurité appelée Mobile Area Key Destributor (MAKD) qui a un certain nombre de rôles dans le réseau de visite (Forign Network), dont l'un est de gérer les clés de cryptage multicast pour les membres mobiles dans le réseau de visite.

Notre invention propose une architecture qui se base sur l'utilisation du protocole de routage multicast PIM-SM, elle utilise une emelioration de ce protocole pour qu'il support l'utilisation de plusieurs Points de Rendez-vous RPs au lieu d'un seul selon les spécifications de l'IETF dans les RFCs 4601, 5059, 5796, et 6226.

Notre Invention propose l'utilisation de plusieurs Points de Rendez-vous actifs simultanément dans une session multicast pour la livraison des clés de ceyptges aux membres mobiles dans une session multicast.

Nous avons choisi le protocole de routage multicast PIM-SM comme protocole de transmission de clés de cryptage en raison de son efficacité de gestion des fonctionsd'abonnement et désabonnement des membres des groupes multicast couver en utilisant un routeur Point Rendezvous RP pour stocker les états de routage multicast.

Nous utilisons deux types de clés, des clés de cryptage pour les membres multicast lorsqu'ils sont en mobilité et les clés de cryptage pour les membres multicast lorsqu'ils sont fixes.

Nous distinguons deux scénarios de rekeying : rekeying des clés pour les membres fixes et rekeying des clés des membres mobiles. Chaque scénario n'affecte pas l'autre.

Description technique

Exposé de la solution

La figure 1 présente un arrangement de 4 zones intercouplés constituant un domaine de routage multicast domain_1 (1) : network_1 au network_4 (2 - 5). Une zone représente un système autonome qui peut être un réseau d'entreprise. Le réseau network_1 (2) constitue le cœur du domaine et nous nous ne proposons pas de modifica-

tion dans ce réseau et spécialement sur le protocole de routage unicast utilise ainsi que le protocole de routage multicast implémente.

Le domaine_1 (1) contient deux types de réseaux : réseau avec des noeuds mobiles et réseau avec des noeuds fixes.

Le réseau network_3 (4) estun réseau avec des nœuds mobile appelé aussi dans le protocole mobile IP « home Networks : home network_1 (6), avec un agent de mobilité « Home Agent » : HA_1 (7).

Comme illustré dans la figure 2, notre approche distingue un récepteur multicast mobile en trois états différents : avant, durant, aprèshandover. Nous présentons la réaction de notre invention selon les états d'un récepteur mobile RM_1 (8). Après un état initial (9) initier par la réception du trafic multicast après une jointure, l'état avant handover (10) représente un étatde stabilité du système avec tous les récepteurs mobile dans leur réseau d'origine, l'état durant handover (11) représente l'état d'un récepteur en mobilité, l'état aprèshandover (12) représente un l'état d'un récepteur après la réussite d'un handover mobile IPv6, le dernier état (13) représente l'état final ou le récepteur multicast quitte la session multicast.

Le réseau network_4 (5) estun réseau de visite où le récepteur multicast mobile RM_1 (8) va visiter, appelé aussi dans le protocole mobile IP « foeing Network » :foreing network_1 (14).

Tous les réseaux du domain_1 (1) sont interconnectés par un ou plueireurs lien (15 à 18)

Tous les agents et les nœuds du réseau ont la possibilité de détecter les états des autres nœuds ou agents en utilisant le protocole Mobile IPv6

a) avant handover (10)

Quand un récepteur RM_1 (8) est connecté à son réseau d'origine home_network_1(6), il reçoit les paquets multicast avec le multicast IP natif et il est directement lié à l'arbre de routage multicast primaire comme illustré dans la figure 1.

À cet instant la gestion des clés de cryptage est réalisée par le protocole de gestion de clés utilisé dans l'arbre de routage multicast primaire MT_1 avec un Point de Rendez-vous RP_1 (20) si nous donnons comme exemple l'utilisation du protocole de routage multicast PIM-SM pour la création de l'arbre de routage multicast primaire.

La source S_1 (21) dans ce cas envoie en unicast les paquets multicast vers son routeur designer local DR_1 (22), ce dernier se charge de les envoyer en unicast avec le message PIM-register (23) vers l'arbre de routage multicast primaire, et le Point de Rendez-vous RP_1 (20) est responsable de diffuser ces paquets vers tous les routeurs multicast dans le domaine de routage, ces derniers dupliquant les donner selon le nombre de récepteurs, par exemple le routeur multicast MR_1 (24) envoie une copie au routeur multicast MR_2 (25), ce dernier envoie directement la copie au routeur designer DR_2(26) du récepteur multicast mobile MR_1 (8). Le rôle de ce routeur multicast disinger dans une session multicast est très important vu que tout le trafic multicast distignerà ce récepteur sera envoyé à ce routeur disinger DR_2 (26).

Tout le trafic multicast diffusé durant cette session est crypté en utilisant une clé de cryptage TEK généré par le DKD_1 (27).

b) Durant handover (11)

Dès que le récepteur mobile passe de l'état avant handover(10) à l'état durant handover (11) et en cours d'exécution du handover_1 (28), il ne peut plus recevoir les données multicast à travers le Routeur Multicast MR_2 (25) et le DR_2 (26) local dans l'ancien réseau home network_1 (6), ni aussi Routeur Multicast MR_3 (29) et le DR_3 (30) local dans nouveau réseau de visite foreign network_1 (14), ce qui entraine 100% de perte de paquets multicast destinés à ce récepteur.

Vu que même si le récepteur mobile se connecte et envoie un message BU (31) pour enregistrer son adresse CoA dans le nouveau réseau de visite il ne peut pas recevoir les paquets multicast tant qu'il n'est pas enregistré une autre fois à la session multicast et reçois les permissions d'accès.

c) Apres handover (12)

À ce niveau on distingue entre deux cas de figure, le cas où le Récepteur Mobile RM_1 (8) se déplace vers un réseau contenant déjà des membres multicast mobiles et le cas où le Récepteur Mobile RM_1 (8) se déplace vers un réseau sans récepteurs multicast mobiles.

i. Réseau sans membres mobiles

Avec le multicast IP, le récepteur mobile RM_1 (8) qui a rejoint un groupe multicast et qui se déplace vers un nouveau réseau ou sous-réseau : si ce dernier ne contient pas d'autres membres du même groupe multicast ce qui implique le manque d'un arbre de routage multicast pour la transmission du trafic multicast, ce scénario est représenté dans le réseau network_4 (5).

Dans ce cas le récepteur mobile ne sera pas capable de recevoir le trafic multicast, jusqu'à ce que l'arbre de routage multicast atteigne la nouvelle liaison de ce récepteur. Le Récepteur Mobile RM_1 (8) doit exécuter un protocole de gestion de groupe multicast, généralement c'est le protocole MLD, qui lui permet d'informer le premier routeur DR_3 (30) (ou BS dans les cas des réseaux sans fil) pour joindre les groupes multicast ce qui entraine unlong délai pour l'authentification du RM_1 (8), ainsi qu'il sera considéré comme étant un nouveau récepteur.

Pour résoudre ce problème, quand Le Récepteur Mobile RM_1 (8) entre dans un nouveau domaine ou un réseau étranger de visite, il doit toujours joindre le groupe multicast associé à l'agent HA_1 (7)créer temporiarmentpour obtenir les paquets provenant des sources multicastà partir de son agent HA_1 (7). Il initie une jointure par l'envoi d'un message d'enregistrement MLD vers le routeur multicast DR_3 (30) et rejoint l'arbre de routage multicast temporaire MT_2 (32) avec le Point de Rendez-vous RP_2 (33) dans son sous-réseau de visite foreing network_1 (14).

Nous montrons dans la section suivant comment cette jointure est faite.

ii. Réseau avec des membres mobiles déjà connecte

Lorsque le récepteur mobile RM_1 (8) se déplace dans un nouveau réseau de visite foreing network_1 (14), il utilise deux types de messages de signalisation : messages de signalisation pour le mobile IP et messages de signalisation pour le multicast IP, ces derniers inclut les messages de gestion des clés de groupe multicast.

La figure 3 et 4 présente les messages de signalisations possibles entre les agents du domaine domain_1 (1), le récepteur mobile RM_1 (8) envoie sa nouvelle adresseCoA à son agent d'accueil en utilisant le message BU_1 (31) qui fait partie du standard Mobile IPv6.

À la réception de ce message de signalisation, BU_1 (31), le home agent HA_1 (7) génère un message (36) qui contient une clé que nous appelons clé de chiffrement de trafic TEK_2 (35). Le home agent HA_1 (7) crypte via la clé publique du MAKD_1 (34) l'ensemble de la signature numérique de la TEK_2 (35) avec la clé secrète du home agent et la clé publique KP du home agent :

HA_1 (7) → MAKD_1 (34)

$(36) = CR[PK_{MAKD\_1}]\ \{S[S[K_{HA\_1}]\{TEK\_2\}, PK_{HA\_1})\}$

Le home agent envoie ce message en multicast au MAKD du réseau de visite foreing network_1 (14).

Le MAKDa son tour décrypte le message en utilisant sa clé secret pour en sortir la signature numérique de la TEK_2 avec la clé secrète du home agent et la clé publique KP du home agent. Ce dernier enregistre dans sa table de correspondance un état de correspondance entre le home agent et sa clé publique [HA_1 (7), PK_{HA_1}].

Ensuite, le MAKD_1 (34) recrypte le message (37) qui inclut cette fois la signature de la clé TEK, sa clé publique, et une clé de cryptage local a ce réseau de visite généré par le MAKD que nous appeloms FNEK (Foreing Network Encryption Key) FNEK,cemessage (37) est recryptéen utilisant la clé publique PK_1 du récepteur multicast mobile RM_1 (8).

MAKD_1 (34) →RM_1 (8)
(37)= CR[PK_{RM_1}] {S[SK_{HA_1}]{TEK_2},FNEK}

Le récepteur multicast mobile RM_1 (8) déchiffre avec sa clé prive le message reçu pour ensortir le TEK, la clé publique de MKD, le FNEK.

Quand un récepteur multicast mobile veut intégrer une autre fois ses groupes multicast, et avant d'envoyer un message de jointure à son routeur désigné DR_3 (30), le récepteur mobile demande les informations d'authentification auprès du serveur MAKD_1 (34) local via une requête (38).

Ensuite, le routeur designer DR_3 (30) transmet ses informations (information d'identification et la clé publique du récepteur multicast mobile RM_1 (8)) au MAKD_1 (34).

L'agent MAKD_1 (34) vérifie ces informations et atteste si le récepteur mobile est apte d'intégrer la session multicast ou non.

Après avoir reçu les clés de cryptage, le récepteur mobile envoie un autre message de jointure MLD_2 (39) à son routeur désigner DR_3 (30) dans son réseau de visite. Ce dernier intègre l'arbre de routage multicast temporaire avec le Point de Rendez-vous RP_2 (33).
Il envoie le message rejoindre demande qui comprend ses informations d'identification et sa clé publique a son routeur designer DR_3 (30) avec un message de jointure MLD_1 (39).

Après avoir établi un plus court chemin entre le récepteur mobile et le point de Rendez-vous RP_2 (33), le récepteur mobile reçoit le trafic multicast nativement en utilisant une communication multicast IP normale.

Certaines adaptations et modifications supplémentaires sont nécessaires au niveau du protocole MLD pour répondre aux exigences spécifiques des récepteurs mobiles. En fait, pour une détection précoce de la présence ou l'absence des membres mobiles du groupe multicast, nous suggérons l'accélération du processus de jointure au groupe multicast en diminuant l'intervalle des requêtes. C'est à ce niveau que le rôle du Routeur désigné RD intervient : le Routeur Désigné RD peut utiliser le protocole MLD pour gérer les groupes multicast actifs dans son sous-réseau et mettre à jour la liste des groupes en envoyant périodiquement un message MLD-request. Quand un RD détecte tout changement dans la liste des groupes actifs, il doit notifier les Points des Rendez-vous RPs autour des Récepteurs mobiles RMs qui veulent rejoindre ou quitter un groupe multicast.

Applications indistruelles

L'invention objet de la présente est susceptible -entre autres- d'application industrielle dans les domaines suivants :

- La télévision sur Internet
- La diffusion de news
- La vidéoconférence
- Les jeux multijoueurs sur internet
- L'apprentissage interactif à distance

Le procédé objet du brevet permet d'offrir les avantages suivants :

- Aucune modification n'est faite au niveau de la partie fixe contenant l'arbre de routage multicast primaire, les routeurs membres et les nœuds membres des groupes multicast fixes.
- Dans notre solution, la question de la mobilité des membres est traitée sans processus de mise à jour total des clés appelé "rekeyingprocess » vu que le membre mobile est toujours valide durant la session.
- Le système n'a pas besoin d'exécuter un process de mise a jours si un membre mobile quitte la session multicast vu que sa clé utilise est valide pour une seule utilisation et il expire des quel envoie un message pour quitter la session multicast ou son routeur DR détecte qu'il a quitté la session en se basant sur le protocole MLD

Revendication

1. Un procédé de multicast mobile dans le IPv6 qui utilise des liens unicast pour assurer la mobilité des membres des groupes multicast, caractresé en se qu'il se base sur des liens multicast dynamiques.
2. Garantir qu'un intrus qui connaît un ensemble de clés ne peut déduire les clés antérieures de groupe. Cette propriété permet d'assurer qu'un nouveau membre du groupe ne peut déchiffrer les messages envoyés au groupe avant son adhésion, et ne peut pas prendre l'identité d'un récepteur mobile visitant un réseau de visite.
3. Un membre mobile se déplaçant d'une zone à une autre peut intégrer sa session de diffusion multicast sans affecter l'ensemble de la session multicast et évitant le phénomène de 1-affect-n.

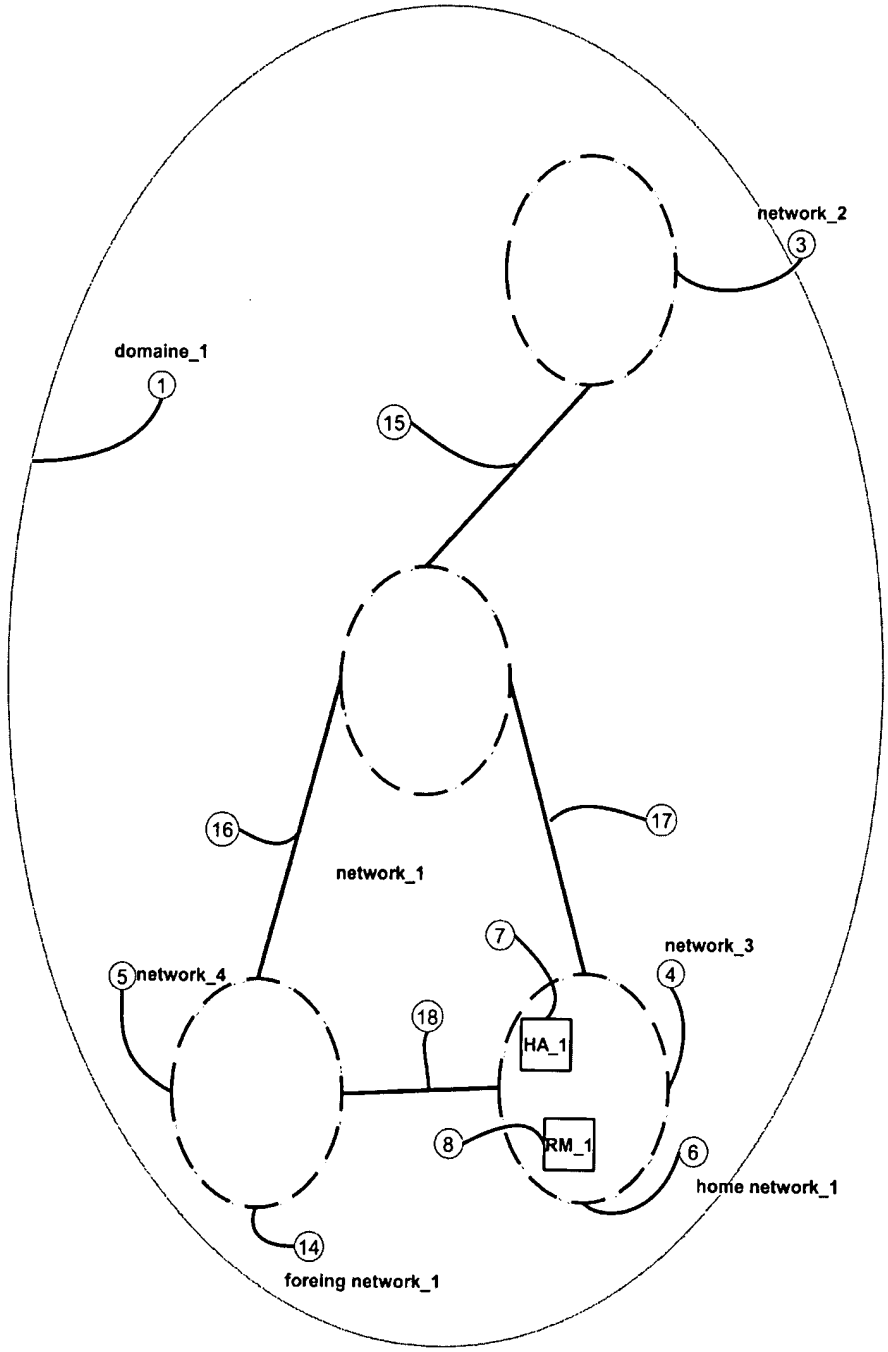

Figure 1

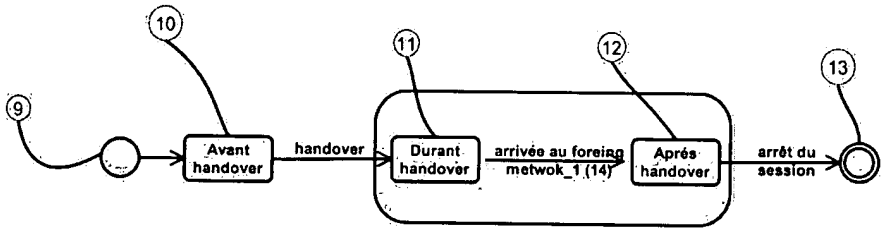

Figure 2

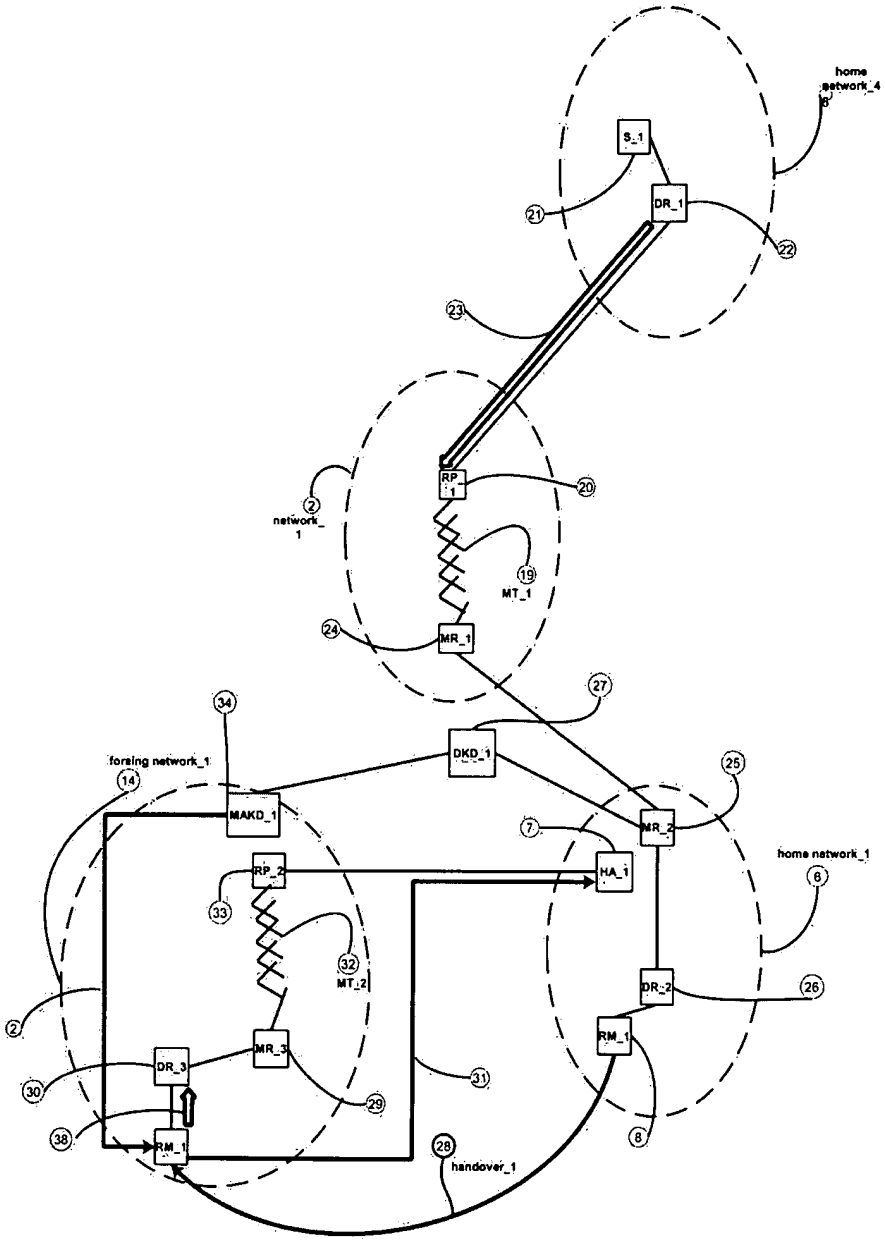
home network_4
6
S_1
21
DR_1
22
23
RP_1
20
2
network_1
19
MT_1
24
MR_1
27
34
DKD_1
25
foreign network_1
14
MAKD_1
7
MR_2
home network_1
6
RP_2
HA_1
33
32
MT_2
DR_2
26
2
RM_1
MR_3
DR_3
30
31
29
38
RM_1
28
handover_1
8

Figure 3

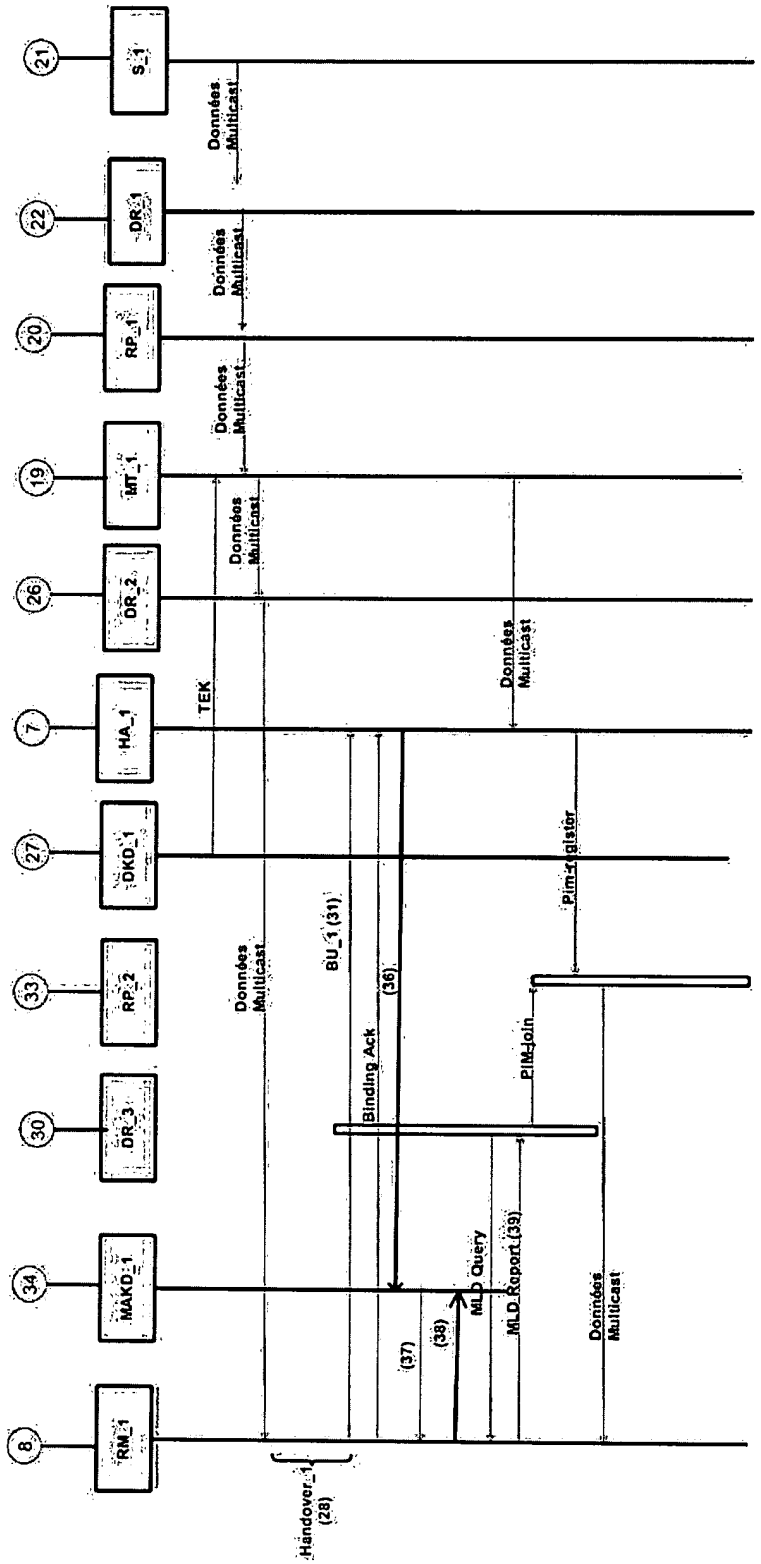
21
S_1
22
DR_1
20
RP_1
19
MT_1
26
DR_2
7
HA_1
27
DKD_1
33
RP_2
30
DR_3
34
MAKD_1
8
RM_1
Données Multicast
TEK
BU_1 (31)
(36)
Binding Ack
PIM-register
PIMJoin
MLD Query
MLD Report (39)
(37)
(38)
Handover_1 (28)

Figure 4

MA 39223A1

ROYAUME DU MAROC
****
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
****

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية

RAPPORT DE RECHERCHE AVEC OPINION SUR LA BREVETABILITE

(Conformément aux articles 43 et 43.2 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13)

Renseignements relatifs à la demande	
N° de la demande : 39223	Date de dépôt : 26/07/2016 ;
Déposant : Université Mohammed V Rabat	
Intitulé de l'invention : Methode d'adaptation du protocole PIM-SM pour le partage dynamique des clés de cryptage dans le multicast mobile IPv6	

Le présent document est le rapport de recherche avec opinion sur la brevetabilité établi par l'OMPIC conformément aux articles 43 et 43.2, et notifié au déposant conformément à l'article 43.1 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13.

Les documents cités par l'examinateur dans la partie rapport de recherche sont joints au présent document

Le présent rapport contient des indications relatives aux éléments suivants :

Partie 1 : Considérations générales
- ☒ Cadre 1 : Base du présent rapport
- ☐ Cadre 2 : Priorité
- ☐ Cadre 3 : Titre et/ou Abrégé tel qu'ils sont définitivement arrêtés

Partie 2 : Rapport de recherche

Partie 3 : Opinion sur la brevetabilité
- ☒ Cadre 4 : Remarques de clarté
- ☒ Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle
- ☐ Cadre 6 : Observations à propos de certaines revendications dont aucune recherche significative n'a pu être effectuée
- ☐ Cadre 7 : Défaut d'unité d'invention

Examinateur: F.Belafkih	**Date d'établissement du rapport** : 05/10/2016
Téléphone: 212 5 22 58 64 14/00	

ROYAUME DU MAROC – OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE – Unité Brevets, Dessins et Modèles

Partie 1 : Considérations générales

Cadre 1 : base du présent rapport

Les pièces suivantes de la demande servent de base à l'établissement du présent rapport :

- Description
  7 Pages
- Revendications
  3
- Planches de dessin
  3 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : H04L9/08, H04L29/06
CPC : H04L63/104, H04L2209/80, H04L9/0822, H04L9/0833, H04L9/0891, H04L63/065

Bases de données électroniques consultées au cours de la recherche :

EPOQUE, Orbit

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
X	**Group Communication Security ;** Yacine Challal ; 13 Mai 2005 http://citeseerx.ist.psu.edu/viewdoc/download ?doi=10.1.1.78.875&rep+rep1&type=pdf Tout le document	1-3
X	**WO2005062951 A2 ;** Motorola, Inc., A Corporation Of The State Of Delaware ; 14 juillet 2005 Tout le document	1-3
X	**PIM-SM Protocol based architecture to transparent mobile sources in Multicast Mobile IPv6 diffusion ;** Mohamed Dafir ECH-CHRIF El KETTANI, Youssef BADDI ; Décembre 2012 Tout le document	1-3
X	**Key exchange process of PIM-SM-based for Multiple Group Communication in P2P;** Si-Jung Kim , Bong-Han Kim; 18 Décembre 2013 Tout le document	1-3

***Catégories spéciales de documents cités :**

-« **X** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
-« **Y** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
-« **A** » document définissant l'état général de la technique, non considéré comme particulièrement pertinent
-« **P** » documents intercalaires ; Les documents dont la date de publication est située entre la date de dépôt de la demande examinée et la date de priorité revendiquée ou la priorité la plus ancienne s'il y en a plusieurs
-« **E** » Éventuelles demandes de brevet interférentes. Tout document de brevet ayant une date de dépôt ou de priorité antérieure à la date de dépôt de la demande faisant l'objet de la recherche (et non à la date de priorité), mais publié postérieurement à cette date et dont le contenu constituerait un état de la technique pertinent pour la nouveauté

Partie 3 : Opinion sur la brevetabilité

Cadre 4 : Remarques de clarté

Les revendications 1-3 ne satisfont pas aux exigences de clarté car l'objet de la protection demandée n'est pas défini. Les revendications tentent de définir l'objet par le résultat recherché au lieu de le définir clairement en termes de caractéristiques techniques. En tout état de cause, cette formulation n'est pas acceptable en l'espèce, puisqu'il semble possible de définir l'objet en des termes plus concrets, c'est-à-dire en exposant comment l'effet peut être obtenu.

Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté (N)	Revendications aucune Revendications 1-3	Oui Non
Activité inventive (AI)	Revendications aucune Revendications 1-3 aucune	Oui Non
Possibilité d'application Industrielle (PAI)	Revendications 1-3 Revendications aucune	Oui Non

Il est fait référence aux documents suivants. Les numéros d'ordre qui leur sont attribués ci-après seront utilisés dans toute la suite de la procédure

D1 : Group Communication Security
D2 : WO2005062951 A2
D3 : PIM-SM Protocol based architecture to transparent mobile sources in Multicast Mobile IPv6 diffusion

1. Nouveauté (N) et Activité Inventive (AI) :

La phase initiale de la recherche a mis en évidence un très grand nombre de documents pertinents (voir les documents D1, D2 et D3 à titre d'exemple) quant à la question de la nouveauté. Le nombre de documents trouvés est tel qu'il est impossible de déterminer quelles parties de la revendication 1 peuvent être considérées comme définissant un objet pour lequel une protection pourrait être légitimement demandée. Pour ces raisons, une recherche significative n'a pu être effectuée au regard de l'ensemble de l'objet de la revendication 1.

En effet, tous les documents ci-dessus divulguent des procédés de multicast mobile qui utilisent les liens unicast pour assurer la mobilité des membres des groupes multicast, caractérisé en ce qu'ils se basent sur des liens multicast dynamiques. D'où l'objet de la revendication 1 n'est pas nouveau et n'implique pas une activité inventive au sens des articles 26 et 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

Les revendications dépendantes 2-3 ne contiennent aucune caractéristique qui, en combinaison avec les revendications auxquelles elles se réfèrent, définissent un objet satisfaisant aux exigences de la nouveauté et de l'activité inventive.

2. Possibilité d'application industrielle (PAI) :

L'objet de la présente invention est susceptible d'application industrielle au sens de l'article 29 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, parce qu'il présente une utilité déterminée, probante et crédible.