Authentification et distribution de clés pour les communications Multicast*

EL KIRAM Moulay Ahmed

Laboratoire d'Informatique et d'Ingénierie des systèmes, Univ. Cadi Ayyad
Faculté des Sciences SEMLALIA - Département d'Informatique.
Bd. Prince My Abdellah, B.P. 2390, 40000 Marrakech. Maroc
kiram@ucam.ac.ma

Résumé. *L'importante augmentation de la bande passante ces dernières années a permis l'émergence et la mise en place de nouveaux services combinant toutes sortes de données : voix, vidéo et texte. L'apparition des applications à participants multiples, comme la téléconférence, l'enseignement à distance, les jeux vidéo distribués, le télé travail coopératif a conduit les fournisseurs d'accès ou les distributeurs de contenus à s'intéresser au communication de groupe, aussi appelé communication multipoint ou mulicast. La diffusion d'information à un groupe peut être réalisée, en utilisant plusieurs liaisons point à point. Mais cette solution est peu efficace sur un réseau à cause de la duplication de l'information émise. IP multicast est de plus en plus utilisé comme mécanisme de communication efficace pour les applications de groupe sur Internet. En revanche, le déploiement à grande échelle du multicast est bloqué par les problématiques de sécurité. Il faut donc sécuriser les applications de communication multipoint. Dans ce papier, nous montrerons d'abord les problèmes et les exigences en matière de sécurité pour un environnement multicast. Nous présenterons ensuite les services de sécurité pour un tel environnement. Nous présenterons aussi les différentes approches de distribution de clés pour les communications multicast et nous proposerons en fin un protocole d'authentification et de distribution de clés à caractère centralisé pour les communications de groupe.*

Abstract. *Data networks are spreading with increasingly high flows. This has lead to the appearance of applications to multiple participants, like the teleconference, the e-learning, the distributed video games, the electronic cooperative work... The diffusion of information to a group can be carried out, by using several peer to peer connections (Unicast). But this solution is not very effective on a network because of the duplication of emitted information. IP multicast is more and more used as effective mechanism of communication for the applications of group on Internet. On the other hand, the deployment on a large scale of the multicast is blocked by security problems. Thus, it is necessary to make secure the applications of multipoint communication. This represents an important economic and trategic stake. In this paper, we will first show initially the problems and the security requirements for an environment multicast. Than we will present security services for such environment. We will also present the various approaches of keys distribution for multicast communication and in the end, we will propose a protocol of authentication and centralized keys distribution for the group communications.*

Mots clés : *Sécurité ; authentification ; distribution de clés ; multicast*

Keywords: *Security, authentication, key distribution, multicast*

* Authentication and key distribution for multicast communications.

© 2010. Revue RIST, vol. 18, n° 2, p. 89-101

1. Le multicast

Le multicast apparaît comme un des services de communication le plus efficace pour l'acheminement des données entre de multiples parties. L'avantage principal de ce mode de communication est d'optimiser la consommation des ressources de réseaux, principalement en réduisant la consommation de la bande passante et des ressources des routeurs et en optimisant le temps d'acheminement des flux de données (Deering, 1991).

L'évolution des réseaux de communication et principalement des plates formes et les applications, les communications de groupe ou les transmissions multipoint ou multicast deviennent de plus en plus populaires et ont suscité beaucoup d'intérêt ces dernières années. Elles correspondent à des modèles adéquats pour beaucoup d'applications de groupe.

Un groupe multicast est un ensemble de stations dont le nombre varie de zéro à l'infini. La composition du groupe est dynamique ; une station peut joindre (Join) ou quitter (Leave) le groupe à tout moment.

Une application de groupe peut être :

- une application de diffusion à source unique (un à plusieurs) où une seul membre diffuse à plusieurs destinataires tel que la diffusion TV, la diffusion des valeurs de bourses…
- une application de diffusion multi sources (certains à plusieurs) où un sous ensemble des membres diffusent vers plusieurs destinataires tel que le télé-enseignement, les consultations distribuées, la téléconférence…
- une application de collaboration (plusieurs à plusieurs) dans laquelle tous les membres du groupe sont égaux. Chaque membre peut être à la fois source et destination tel que le télé-travail coopératif…

2. L'IP multicast

Dans le monde d'Internet, le multicast, appelé service de diffusion, repose sur l'utilisation d'une extension du protocole IP : IP multicast défini par DEERING dans (1991). Cette extension multicast du modèle IP est appelée aussi modèle ASM (Any Source Multicast).

Le processus de diffusion multipoint sur un réseau local est relativement simple. La machine émettrice spécifie une adresse de destination IP multicast. Cette adresse est de classe D dans IPv4 et de préfixe FF00 :/8 dans IPv6. Puis après conversion de cette adresse en une adresse physique (par exemple de type Ethernet), le système d'exploitation diffuse les paquets de données. Les machines réceptrices doivent notifier à leur couche réseau qu'elles veulent recevoir des datagrammes destinés à une adresse multipoint donnée. Cette procédure appelée « adhésion à un groupe » est réalisé par un protocole de

gestion des adhésions au groupe nommé IGMP (Deering, 1989) pour IPv4 ou MLD (Vida, Costa, 1999) pour IPv6.

3. Facteurs à considérer dans le multicast sécurisé

Il existe plusieurs facteurs ou aspects ayant une influence sur les approches et mécanismes utilisés pour la sécurisation des communications multicast (Chrisment, 2005) :

- Passage à l'échelle : La taille de groupe peut varier d'une dizaine de participants dans les petits groupes de discussion à plusieurs centaines voire plusieurs milliers. Le facteur d'échelle dans le multicast sécurisé signifie la possibilité d'étendre les mécanismes de sécurité à un groupe plus important en taille sans dégradation des performances.
- Caractéristiques des membres : Les éléments matériels ou d'infrastructure réseaux dans le multicast, peuvent différer d'un membre à l'autre impliquant des besoins de communications différents.
- Dynamisme : La taille du groupe peut évoluée durant une session. Tout membre peut joindre ou quitter le groupe à tout moment. La sécurité est alors influencée par la fréquence des requêtes « join » et « leave » des membres du groupe.
- Contrôle du groupe : Il n'y a pas toujours un système central bien informé de l'état de groupe. Ceci est une conclusion du facteur de dynamisme du groupe.
- Durée de vie : Le groupe peut exister de manière temporaire ou permanente.

4. Vulnérabilités des communications de groupe

Dans le IP multicast, les groupes sont identifiés par une adresse de groupe et n'importe quel nœud du réseau peut joindre ou quitter le groupe quant il le souhaite. Cette simplicité, qui fait la puissance du routage multipoint, présente cependant des vulnérabilités (Ballardie, Crowcroft, 1995) :

- IP multicast (Deering, 1988) ne supporte pas la notion du groupe fermé. En effet, les adresses multicast sont publiques : adhérer à un groupe ou quitter un groupe sont des opérations qui ne nécessitent pas des permissions particulières (Fenner, 1997). Cela permet donc à n'importe quel utilisateur d'adhérer à un groupe et recevoir les messages destinés à celui-ci.
- Les accès au groupe ne sont pas contrôlés : un intrus peut envoyer des données au groupe sans en faire partie, perturber la session multipoint, et éventuellement causer des congestions dans le réseau.
- Les données destinées au groupe peuvent traverser plusieurs canaux non sécurisés avant d'atteindre tous les membres du groupe. Cela augment les opportunités d'écoute aux intrus éventuels.

- Les communications de groupe présentent plus d'opportunités pour l'interception des communications, proportionnelle au nombre de participants.
- Un point vulnérable du groupe met en cause la sécurité de tous les membres du groupe.
- La publication à large échelle de l'identité et de l'adresse du groupe aide les intrus à focaliser leurs attaques.
- Les attaquants peuvent usurper l'identité des membres légitimes du groupe.

Pour contrecarrer ces attaques, la communication de groupe nécessite des services de sécurité tels que, l'authentification, la confidentialité de données, la confidentialité du flux de trafic…

Ces services trouvent des définitions légèrement différentes de celles utilisées dans les communications classiques.

5. Services de sécurité dans le multicast

Dans les communications de groupe, le potentiel des attaques est beaucoup plus significatif que lors des transmissions dans les communications classiques. Les services de sécurités destinés pour les communications point à point ne seront donc plus appropriés aux communications de groupes.

5.1. L'authentification

Le service de l'authentification se présente sous plusieurs formes :

a. Authentification de l'entité

C'est une fonction permettant d'être sûr qu'une entité est bien celle qu'elle a déclarée être lors de la phase d'identification. Elle permet d'assurer que seules les entités autorisées ont le droit de joindre les groupes sécurisés. Ce service constitue une partie essentielle du contrôle d'accès aux groupes.

b. Authentification de l'origine de données

C'est une fonction qui permet à une entité d'être sûre de la source des données reçues. Ce service permet alors à une entité d'être sûre que les données qu'elle vient de recevoir proviennent bien d'une entité qu'elle connaît, qu'aucun déguisement ne vient masquer l'identité réelle de la source de ces données.

Ce type d'authentification se divise en deux sous types lorsqu'il s'agit de communication multicast (Boussida, Chrisment, 2004) :

- Authentification de la source : Cette propriété de sécurité garantit que les membres d'un groupe multicast s'assurent de l'identité de la source à chaque fois qu'ils reçoivent le flux émis en multicast.

– Authentification du groupe : Cette propriété de sécurité requiert que les membres d'un groupe multicast s'assurent que la source du flux multicast est bien adhérente au groupe.

5.2. Confidentialité de données

Ce service permet de restreindre la lecture des messages d'une source vers un groupe de destinataires, à un ensemble d'entités connues.

Ce service est la brique fondamentale pour la création de sessions multipoints privées qui fait intervenir une ou plusieurs clés de groupe.

La gestion des clés de groupe, à savoir, leur création, leur distribution et leur mise à jour, constitue l'élément de base pour les applications de groupe sécurisées.

Une clé de groupe est une clé de cryptage connue uniquement par les membres courants du groupe, elle doit satisfaire les propriétés suivantes :

a. Confidentialité du passée

Ce service permet d'écarter le fait qu'un intrus puisse stocker le trafic antérieur d'un groupe, puis rejoint le groupe pour s'acquérir des clés nécessaires pour le déchiffrement de ce flux passé.

Afin d'assurer la confidentialité passée, il peut être nécessaire de renouveler la clé de chiffrement après chaque arrivée (backward confidentiality). Cela pour assurer qu'un nouveau membre ne soit pas capable d'accéder à l'ancien trafic du groupe.

b. Confidentialité du future

Ce service permet d'empêcher tout membre ayant quitté le groupe multicast à un instant, de disposer des clés pour déchiffrer le trafic multicast ultérieur (forward confidentiality)

Afin de réaliser cette fonction, il peut être nécessaire, après chaque départ, de modifier les clés et les redistribuer à tous les membres du groupe.

5.3. Confidentialité de flux de trafic

L'accroissement de flux d'information entre les membres d'un groupe, ou le simple fait de savoir que des entités d'un groupe sont en communication peut révéler un secret et donc, être significatif pour un intrus.

Le service de confidentialité de flux de trafic, nommé de cette façon pour le distinguer de la confidentialité de données, à pour objet de masquer le fait qu'il y'a échange d'informations entre les membres d'un groupe.

5.4. Contrôle d'accès des membres du groupe

Ce service de sécurité garantit que l'adhésion au groupe est assurée via une liste de contrôle d'accès ACL (Access Control List), contenant toutes les entités autorisés à joindre le groupe

5.5. Intégrité de données

Le service d'intégrité de données est le moyen qui assure que les données reçues sont celles qui ont été transmises et non des données qui auraient pu être transformées par des entités tierces inconnues. En communication multicast, ce service assure que le trafic multipoint n'a pas été altéré pendant la transmission.

Le service d'intégrité de données n'est pas en général efficace sans l'assurance de l'authentification de l'origine de données. En effet, dans certaines circonstances, il n'est pas intéressant de recevoir les données intègres sans être informé de leur origine.

6. Authentification et gestion de clés dans le multicast sécurisé

6.1. Cryptage

Le mécanisme de cryptage joue un rôle très important pour la sécurité dans un environnement réseau. Il permet de réaliser des services de sécurité tels que l'authentification, la confidentialité, l'intégrité de données, le contrôle d'accès…

Le cryptage d'un message, aussi appelé chiffrement, est l'opération qui permet de transformer à l'aide d'opérations mathématiques (substitutions, transpositions) (figure 1) un texte en clair P (pour Plaintext) en un texte chiffré C (pour Ciphertext) de telle sorte qu'il ne soit plus compréhensible par une entité non accréditée.

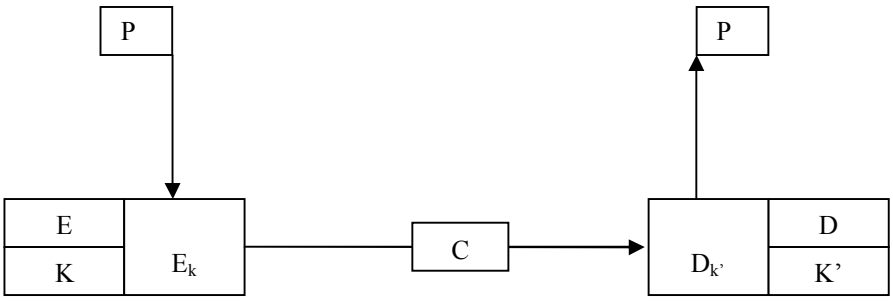

Figure1. *Mécanisme de cryptage*

Le texte en clair P est transformée en texte chiffré C par une fonction de cryptage Ek qui n'est autre qu'un algorithme de cryptage E (pour Encryption) paramétré par une clé de cryptage K (C = Ek(P)). Le texte chiffré C transite sur la ligne de transmission et est décrypté du coté du récepteur légitime par une fonction de décryptage Dk' qui n'est autre qu'un algorithme de décryptage D (pour Decryption) paramétré par une clé de décryptage de données K' pour retrouver le texte en clair P (P= Dk'(C)).

Les systèmes cryptographiques ou cryptosystèmes sont de deux types :

- Les cryptosystèmes symétriques, appelés aussi cryptosystèmes conventionnels ou cryptosystèmes à clés secrètes dans lesquels l'algorithme de décryptage est paramétré par une clé qui se déduit facilement de la clé paramètre de l'algorithme de cryptage.
- Les cryptosystèmes asymétriques, appelés aussi cryptosystèmes à clés publiques dans lesquels les algorithmes de cryptage et de décryptage sont paramétrés par des clés différentes et la connaissance de l'une ne permet pas de déduire l'autre, l'une appelée clé secrète et l'autre clé publique.

6.2. Distribution de clés dans le multicast

a. Approches centralisées. GKMP

Dans cette approche, une seule clé symétrique appelée TEK (Traffic Encryption Key) est utilisée par la source pour crypter le flux multicast et par les récepteurs pour le décrypter. La plupart des protocoles de cette approche centralisent les tâches de gestion de clés dans une seule entité. GKMP (Group Key Management Protocol) (Harney, Muckenhirn, 1997) en est un exemple.

GKMP utilise un centre de distribution de clé appelé SKDC (Single Key Distributor Center). Ce centre est une entité participante au groupe, et non une entité tierce, qui coopère avec le premier membre pour créer la clé du groupe. La clé générée est ensuite distribuée aux autres membres du groupe par des tunnels sécurisés en point à point, via des clés de session.

Pour garantir la confidentialité du passé, l'ajout (join) d'un nouveau membre oblige la génération d'une nouvelle clé. Cette clé est remise en point à point au nouveau membre, et en multicast aux autres membres.

Ensuite, et en vue de garantir la confidentialité du futur, le retrait (leave) d'un membre, oblige à réaliser n (n taille du groupe) tunnels sécurisés pour distribuer la nouvelle clé, ce qui revient à créer un nouveau groupe.

Le nombre de messages requis pour la mise à jour de la TEK est de l'ordre n (O(n)), ce qui laisse cette solution inadaptée au facteur d'échelle mais pratique pour les groupes non dynamiques ou stables.

b. Approche hiérarchique

Le caractère localisé de l'approche centralisée rend le contrôleur du groupe une cible privilégiée pour les attaques. Aussi, cette approche souffre du problème du goulot d'étranglement.

L'approche centralisée peut être améliorée en subdivisant le groupe en sous groupes utilisant des TEK différentes (Hassan, 2005). Chaque sous groupe est géré par un contrôleur du sous groupe et partage une clé symétrique local-TEK. Lors d'un changement dans la composition du groupe, seul le sous-groupe concerné met à jour sa clé locale et son contrôleur la distribue uniquement aux membres du sous groupe. Cependant, le fait d'avoir plusieurs sous groupes nécessite le décryptage et le récrypatage du flux multicast à chaque passage d'un sous groupe vers un autre.

L'approche hiérarchique réduit considérablement le phénomène 1 affecte n. Cependant, elle souffre de la tache coûteuse de décryptage et de récryptage ce qui la rend inefficace pour les groupes stables.

c. Approche Adaptative AKMP

L'approche adaptative AKMP (Adaptative Key Management Protocol for Secure multicast) (Bettahar, Bouabdallah, Challal, 2002) profite des avantages de l'approche centralisée et de l'approche hiérarchique. L'idée principale de l'approche AKMP est d'adopter l'approche centralisée si les membres sont peu dynamiques et de basculer vers l'approche hiérarchique si les membres deviennent assez dynamiques.

Dans l'approche AKMP, plusieurs routeurs AKMP sont utilisés. Le protocole commence par construire un seul groupe partageant une TEK unique. Durant la session multicast sécurisé, si un routeur AKMP détecte une augmentation de dynamicité locale, il initie un sous groupe avec une clé locale indépendante.

Les approches que nous avons présentées ci-dessus sont des approches de distribution de clés sans authentification préalable. Ceci constitue une fragilité importante des protocoles sous jacents. Aussi, ces protocoles n'offrent pas de moyens pour garantir l'authenticité de l'origine des clés distribués. En effet une entité malhonnête peut distribuer des clés en se faisant passé pour un contrôleur de groupe.

Le protocole que nous présenterons ci-dessous est un protocole de distribution de clés. Les clés sont distribuées uniquement aux entités préalablement authentifiées avec possibilité de garantir l'authenticité de leur origine.

Notre choix est porté sur le caractère centralisé visant les groupes peu dynamiques.

7. Authentification et distribution de clé dans GKMP

Nous proposons dans ce qui suit une amélioration de l'approche GKMP avec une authentification préalable.

Notre solution met en jeu deux serveurs :

- Un serveur d'authentification AS chargé d'authentifier tous les membres du groupe (même ceux qui avaient quitté le groupe).
- Un contrôleur de groupe CG, nommé SKDC dans GKMP, chargé d'authentifier les membres effectifs du groupe G et leur distribuer la clé K_G de ce groupe.

Chaque membre du groupe U détient une clé privée K_U qu'il partage uniquement avec le serveur d'authentification AS.

Notre protocole d'authentification et de distribution de clé est illustré dans la figure suivante (fig.2) :

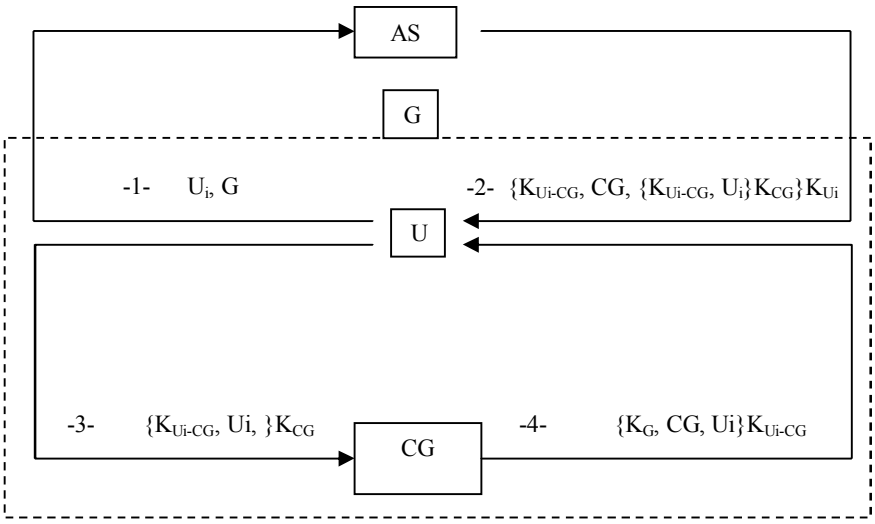

Figure2 : *Approche centralisée d'authentification et de distribution de clés*

Le protocole que nous proposons se déroule comme suit :

1. l'utilisateur Ui communique son identité ainsi que celle du groupe au serveur d'authentification AS.
2. Le serveur d'authentification génère une clé de session K_{Ui-CG} qui sera partagée entre Ui et le contrôleur du groupe CG. Cette clé est remise à l'utilisateur Ui protégée par sa clé secrète. Un deuxième exemplaire de cette clé lui est aussi remis, mais protégé par la clé secrète du contrôleur du groupe.

3. L'utilisateur Ui envoi $\{K_{Ui\text{-}CG}, Ui, \}K_{CG}$ au contrôleur du groupe CG. Ce dernier décrypte ce message avec sa clé secrète K_{CG} pour trouver la clé de session $K_{Ui\text{-}CG}$ ainsi que l'identité Ui. CG vérifie dans la liste des membres qu'il détient si l'utilisateur Ui est bien membre effectif du groupe G . Si c'est la cas, CG forme le message $\{K_G, CG, Ui\}K_{Ui\text{-}CG}$ et le retourne à Ui.
4. Ui décrypte le message $\{K_G, CG, Ui\}K_{Ui\text{-}CG}$ qu'il vient de recevoir du contrôleur du groupe avec la clé qu'il avait reçu du serveur d'authentification AS pour finalement retrouver le clé du groupe K_G .

Ce protocole peut être amélioré en utilisant le timestamps, ou des nonces, pour lutter contre de potentielles attaques de type rejeu.

8. Authentification et distribution dans l'approche hiérarchique

Notre proposition d'authentification et de distribution de clé qui améliore l'approche hiérarchique consiste à utilisée un seul serveur d'authentification AS. Chaque groupe Gi est géré par un contrôleur de groupe CGi (Fig.3).

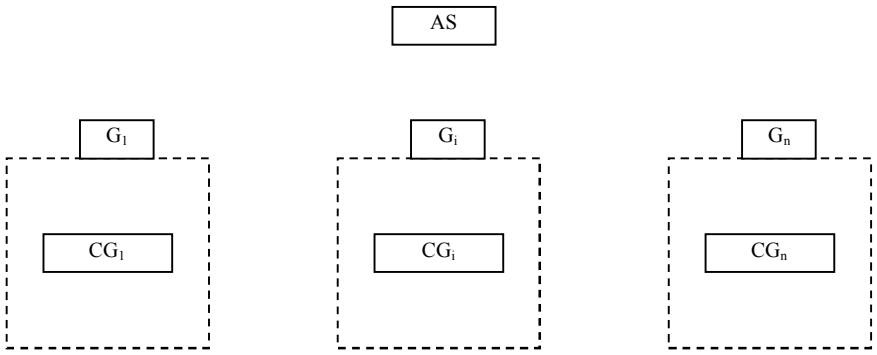

Figure3 : *Approche hiérarchique d'authentification et de distribution de clés*

Un utilisateur Ui est authentifié dans le sous groupe CGi, et la clé KGi du sous groupe Gi lui est remise comme dans l'approche centralisée. Cependant, l'échange entre deux sous groupe nécessite un décryptage et encryptage au niveau des contrôleurs des sous groupes.

9. Authentification et distribution lors d'un ajout

9.1. Ajout d'un membre

Nous distinguons deux cas lors de l'ajout d'un membre au groupe :

– Cas d'ajout d'un nouveau membre : Dans ce cas, ce membre doit être enregistré au niveau du serveur d'authentification AS et du contrôleur du groupe. Ceci est réalisé en ajoutant une ligne au niveau du serveur d'authentification, contenant l'identité du nouveau membre ainsi que sa clé

secrète et aussi en déclarant cet utilisateur dans le contrôleur du groupe. Puis la clé du groupe lui est remise.

- Cas ou le membre retourne au groupe : C'est le cas ou un membre à quitter temporairement son groupe et souhaite le regagner. Dans ce cas, ce membre reste toujours reconnu au niveau du serveur d'authentification par sa clé secrète et ce membre est rajouté au groupe au niveau du contrôleur du groupe dans la liste des membres du groupe qu'il détient. Puis une clé de groupe lui est remise.

9.2. Remise de clé de groupe

Lors de l'ajout d'un membre, et en vue de garantir la confidentialité du passé, une nouvelle clé doit être distribuée à tous les membres du groupe. Cette distribution peut se faire, au niveau du contrôleur du groupe, en multicast à l'aide de l'ancienne clé du groupe. Cependant, cette solution largement employée ne permet pas de garantir l'authentification de l'origine de la clé. En effet, une entité malhonnête du groupe peut générer une nouvelle clé et la distribuer aux autres membres à la place du contrôleur du groupe.

Le protocole que nous avons proposé offre, en plus de la solution de distribution de clé en multicast, la possibilité de distribuer la nouvelle clé du groupe à l'aide de la clé partagée entre le contrôleur du groupe et les membres. En effet rappelons le, chaque membre du groupe avait reçu une clé de session du serveur d'authentification partagée avec le contrôleur du groupe.

10. Authentification et distribution lors d'un départ

10.1. Départ d'un membre

Un membre du groupe ayant quitté le groupe, ne pourra plus avoir accès aux flux multicast, ceci pour garantir la confidentialité du futur.

Le départ d'un membre dans notre proposition est réalisé par la suppression de l'identité de ce membre au niveau du contrôleur du groupe tout en gardant ce membre enregistré au niveau du serveur d'authentification. Cela permettrai à ce membre de s'authentifier s'il a regagne le groupe. Ceci ne signifie pas que ce membre aura la clé du groupe sans la réactivation de son appartenance à ce groupe au niveau de son contrôleur.

10.2. Remise de la clé du groupe

Cette fois ci, la remise de la clé ne pourra pas s'effectuer en multicast, sinon, le membre ayant quitté le groupe aura accès à cette clé.

Les clés de session partagées entre le contrôleur du groupe et les membres sont suffisants pour distribuer la nouvelle clé en point à point à tous les membres. Ceci garantie bien que seuls les membres effectifs du groupe (ceux inscrit au niveau du contrôleur) auront accès à la nouvelle clé du groupe.

11. Conclusion

Le déploiement large et sûr des applications de groupe repose sur l'emploi de mécanisme de sécurité dédié aux communications multicast. En effet, certaines applications de groupe telles que le télé-enseignement, la téléconférence…présentent plus de vulnérabilités et nécessitent des mécanismes de sécurité spécifiques aux communications multicast parfois différents à ceux employer pour sécuriser les communications point à point.

Dans ce papier, nous avons présenté les problèmes de sécurité lorsqu'il s'agit de communication de groupe. Nous avons aussi présenté les services de sécurité pour de tel environnement. Ceci a montré certaines exigences en matière de sécurité dans les communications multicast non exigés dans les communications point à point.

Nous avons aussi proposé un protocole d'authentification et de distribution de clé pour les communications de groupe. Notre protocole présente une solution plus complète en précédant la distribution de clés aux entités du groupe d'une phase d'authentification. En effet, on ne peut imaginer un protocole de distribution de clé sans une authentification préalable. Notre solution est une approche centralisée parfaitement adaptée aux groupes peu dynamique.

12. Références

Ballardie, T., Crowcroft, J. 1995. Multicats-specific Security Threats and conter-Measures. Syposium on «Network and Distributed system Security. San Diego», California. p. 2-16

Bettahar, H., Bouabdalla, A., Challal, Y. 2002. Multicast sécurisé : une solution adaptative. « SAR'02 »

Boussida, M.S., Chrisment, I. 2004. Méthodes d'authentification pour les communications de groupes : Taxonomie et évaluation dans les environnement Ad-Hoc. 3ième conférence sur « les architectures réseaux. SAR'04», La londe. p. 197-208**Deering, S. 1989.** *Host Extensions for IP Multicasting*. Rfc 1112. IETF

Chrisment, I. 2005. Maîtrise de la dynamique dans l'Internet: De l'adaptation des protocoles à la sécurité des services. These PH: Ecole doctorale IAEM Lorraine. UFR STMIA

Deering, S. 1991. Multicast Routing in a Datagram Internetwork. PhD thesis: Stanford Univesity,

Deering, S.E. 1988. *Multicast Routing in Internetwork and Extended LANs*. «ACM. SIGCOMM'88», Stanford, California

Fenner, W. 1997. *Internet Group Management protocol*. RFC 2236

Harjono, T., Tsudik, G. 2000. IP Multicast Security : Issues and Directions. *Annales de telecom*

Harney, H., Muckenhirn, C. 1997. *Group Key Management Protocol GKMP. Specification*. RFC 2093. SPARTA

Hassan, H. R. et al. 2005. Gestion de clés dans la communication de groupes hiérarchiques. « SAR'O5 »

Vida, R., Costa, L. 1999. *Mulicast Listener Discovery*. RFC 2004, IETF