Extension de l'architecture active AMAM pour le support des services de sécurité multicast

Hassen Sallay, Abdelkader Lahmadi, Olivier Festor, Isabelle Chrisment

Extension de l'architecture active AMAM pour le support des services de sécurité multicast

Hassen Sallay, Abdelkader Lahmadi, Olivier Festor, Isabelle Chrisment

LORIA - INRIA Lorraine - Université Henri Poincaré
615 rue du Jardin Botanique
F-54602 Villers-lès-Nancy, France
{Hassen.Sallay,Abdelkader.Lahmadi,Olivier.Festor,Isabelle.Chrisment}@loria.fr

RÉSUMÉ. *Dans cet article nous présentons le support de sécurité multicast dans l'architecture active pour la gestion de services multicast AMAM. Cette extension supporte la dynamique de l'arbre de distribution et résiste au facteur d'échelle. Elle offre les fonctionnalités de contrôle d'accès ainsi que la protection du contenu.*

ABSTRACT. *In this paper we present the security extension within the active management architecture dedicated to IP multicast services AMAM. This extension supports the dynamics of a multicast tree and the scale factor. It offers the two main securtiy functionnality, access control and content protection. This extension is implemented using active technology.*

MOTS-CLÉS : *Multicast IP, Architecture de supervision, sécurité , réseau actif*

KEYWORDS: *multicast, network and service management, Security, active network*

1. Introduction

La supervision des services multicast dans les réseaux IP est aujourd'hui un élément clef dont la disponibilité conditionne le déploiement à grande échelle des services de communication de groupes. Pour cela, les fournisseurs de services cherchent à faire évoluer des solutions de supervision de certains services spécifiques tels que des VPNs en point à point qui s'appuient sur des technologies de niveaux inférieurs, e.g. VP ATM, vers des services plus complexes tels que les services mutlicast sur IP. Les services multicast engendrent de nombreux défis pour la supervision. Le premier est certainement de définir dans le contexte de la gestion de services, un modèle commercial viable sur lequel vont pouvoir s'appuyer les solutions de supervision au travers d'agréments et de contrats de services. Le second défi est un défi technologique. En effet, contrairement à une communication point à point, la communication de groupes fait intervenir de multiples terminaux (potentiellement plusieurs milliers voire millions). Ce qui pose un problème crucial de passage à l'échelle pour la supervision. De plus, la dynamique des groupes ne permet pas une configuration statique de composants de supervision, les deux échelles temporelles étant incompatibles. Sur ces deux points (passage à l'échelle & dynamique) les architectures de supervision standard, ou du moins certains de leurs composants et paradigmes atteignent leurs limites.

Les fonctions de gestion telles que la comptabilité, la sécurité et la gestion de fautes doivent prendre en considération la nature des services multicast et ses spécificités. Par exemple, le caractère dynamique multicast influence énormément la façon d'implanter la fonction de sécurité. En effet, à chaque abonnement ou désabonnement des clients, une nouvelle génération et diffusion de clefs devient nécessaire pour limiter les accès aux seuls clients autorisés et au seul trafic demandé.

Dans [SAL 03], nous avons développé une architecture qui satisfait au mieux ces critères. Cette architecture, basée sur un modèle hiérarchique à trois niveaux, distribue les données et les fonctions de gestion tout en ayant la capacité de composer et coupler la nature dynamique du multicast et ses fonctions de gestion. Elle pousse l'exécution des tâches de gestion dans les routeurs frontaux de l'arbre multicast pour résister au mieux au facteur d'échelle. AMAM[1] est l'implantation de cette architecture à l'aide de la technologie active. L'objet de cet article est de présenter l'extension de cette architecture avec le support de la fonction de sécurité. Pour cela, l'article est organisé comme suit : la section 2 recense les différentes fonctions de sécurité et approches proposées pour le support de la gestion de sécurité du multicast. La section 3 décrit AMAM notre architecture de gestion. La section 4 détaille l'architecture interne du composant de sécurité et la section 5 présente les fonctionnalités de sécurité qu'il offre. L'implantation à l'aide de la technologie active de la composante de sécurité dans AMAM est décrite dans la section 6. Une conclusion et quelques perspectives terminent la contribution.

1. Active-based Management Architecture for IP Multicast

2. État de l'art

Afin de sécuriser une communication multicast, différentes fonctions telles que l'authentification, l'intégrité, la confidentialité ou la protection du contenu sont nécessaires [FOR 94].

L'***authentification*** est une fonction intégrante de tout protocole de distribution de clefs [MAU 97]. Elle est essentiellement déployée pour contrôler l'accès à un service de multicast. En effet, les mécanismes d'authentification servent (1) à identifier les clients du service et (2) s'assurer que seuls les abonnés sont autorisés à recevoir le trafic multicast. Elle sert également à limiter l'accès aux clefs de chiffrement du trafic seul aux abonnés si on utilise des techniques de cryptographie pour sécuriser le service multicast. Les sources de trafic multicast sont également identifiées grâce à des protocoles d'authentification tel que AH[2] [KEN 98a] qui identifie la source de chaque paquet IP multicast.

L'***intégrité*** sert à s'assurer que les données n'ont pas été altérées lors de leur cheminement. Dans quelques applications multicast telles que les application VoIP où des données corrompues peuvent être facilement détectées, cette fonction n'est pas essentielle. Cependant, elle devient vitale pour parer les attaques de spoofing dans les services basés sur des protocoles de gestion de clefs pour la sécurisation de multicast [BEL 89].

La ***confidentialité*** ou protection du contenu est essentielle pour créer des sessions privées de multicast. Bien que le chiffrement soit typiquement employé pour fournir cette fonction, une forme plus faible de confidentialité peut être réalisée en limitant le cheminement des paquets IP d'une session multicast donnée. Les protocoles de transport tels que RTP supportent ces mécanismes de chiffrement. ESP[3][KEN 98b] fournit cette fonction de confidentialité au niveau réseau. Cette fonction doit s'appliquer lors de la distribution de clefs de chiffrement pour un service multicast donné. Le protocole ISAKMP [MAU 97] offre un échange confidentiel de clefs de chiffrement.

En fait, ces fonctions de sécurité ne sont pas spécifiques aux services multicast. Elle s'applique pour tout service déployé dans un environnement ouvert tel que l'Internet. Cependant la spécificité du service multicast, surtout son caractère dynamique, rend ces fonctions difficiles à implanter. Par exemple, on devrait générer et diffuser des clefs de chiffrement à chaque abonnement ou désabonnement des membres pour limiter les accès aux seuls membres autorisés et au seul trafic demandé. Ce fait pose un véritable défi pour le passage à l'échelle pour un service multicast sécurisé et conditionne ainsi ses solutions de gestion. En effet, si la dynamicité d'un groupe est très forte, on risque de surcharger le réseau uniquement par les messages de signalisation pour la distribution des clefs régénérées ou rafraîchies. Des architectures de gestion qui s'adaptent à la dynamicité et résistent au mieux au facteur d'échelle sont alors des éléments clefs pour une commercialisation réussie d'un service multicast sécurisé.

2. Authentication Header
3. Encapsulating Security Payload

Différents protocoles et architectures sont définis pour fournir ces fonctions de sécurité. Ces solutions architecturales tentent de résoudre efficacement le problème de gestion de clefs dans les services multicast. [WAL 97] propose une centralisation de la génération de clès par un KDC (Key Distribution Center) qui distribue ces clefs aux abonnés qui sont connus à priori. Cette distribution de clefs reste trop lente pour les sessions dynamiques de multicast où l'adhésion n'est pas définie à priori. Cependant, dans quelques environnements, cette solution peut être la plus facile à mettre en place. [HAR 97, OPP 96, BAL 96] proposent des solutions décentralisées qui distribuent la gestion de clefs sur les différentes entités impliquées. [CHA 01a, CHA 01b] propose une solution basée sur une gestion décentralisée avec une seule clé partagée entre les membres du groupe. Ces architectures distribuées passent mieux à l'échelle.

Il est important de noter qu'une solution efficace pour une application particulière de multicast peut ne pas l'être pour une autre. De plus, la solution idéale devrait être transparente à l'utilisateur et fonctionner efficacement avec d'autres protocoles de diffusion multicast. Au sein de l'équipe MADYNES, nous avons conçu une architecture de gestion de multicast qui distribue les données et les fonctions de gestion pour mieux maîtriser la dynamicité et le facteur d'échelle. Cette architecture implante des fonctions intéressantes de sécurité via une gestion efficace des clefs de chiffrement.

3. Description de l'architecture AMAM

L'architecture intègre différentes tâches de gestion et distribue les données et les fonctions de gestion tout en ayant la capacité de composer et de coupler la nature dynamique du multicast et ses fonctions de gestion. Elle pousse l'exécution des tâches de gestion aux routeurs frontaux de l'arbre multicast pour résister au mieux au facteur d'échelle surtout en terme de nombre de membres abonnés à un service multicast donné.

L'architecture se base sur un modèle hiérarchique à trois niveaux : niveau nœud source, niveau noeud intermédiaire et niveau nœud frontal[4] (voir les figures 1, 2). Elle repose sur la coopération des trois types d'agents de gestion associés à ces niveaux ; MSA[5](Agent Source), MNA[6] (Agent Noeud), MEA[7] (Agent Frontal) placés respectivement à chaque niveau. Les agents MNA et MEA se déploient et se retirent dynamiquement suivant l'expansion et la contraction de l'arbre de distribution multicast (i.e. join/leave d'un routeur). MEA collecte les informations de gestion pour chaque groupe via une interface générique capable de coopérer avec IGMP [CAI 01] ou MLD [HAB 01]. MNA interagit aussi avec les protocoles de routage de multicast à travers des interfaces bien définies pour collecter les informations sur la topologie de l'arbre de distribution. Ces informations collectées par un MEA et un MNA sont

4. Nous considérons les noeuds frontaux de l'arbre de distribution multicast sont les routeurs qui possèdent en local des membres abonnés sous leur responsabilité
5. Multicast Source Agent
6. Multicast Node Agent
7. Multicast Edge Agent

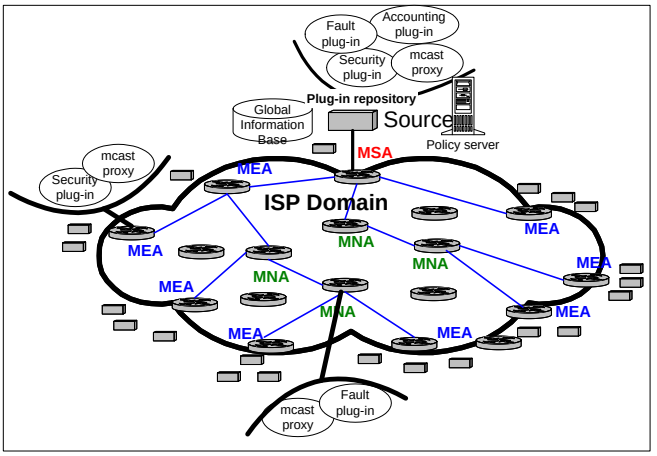


Figure 1. *L'architecture globale de gestion AMAM*

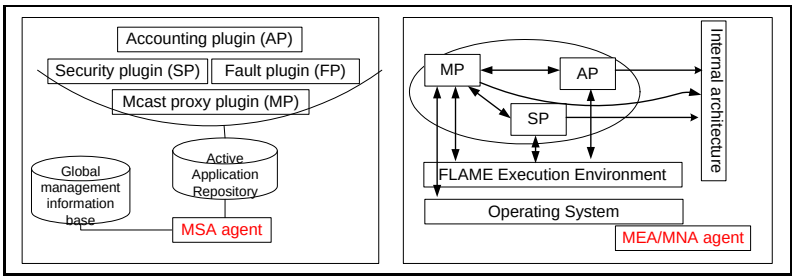


Figure 2. *L'architecture AMAM*

envoyées au MSA. Ce dernier est responsable des tâches de gestion. Il possède une base de données servant à stocker les informations de gestion, une base de politiques et un dépôt contenant différents greffons (plugin) spécialisés de gestion. Ces applications de gestion sont des applications réalisées comme applications actives et peuvent être téléchargées au besoin et sur demande par les MNA et MEA.

La communication entre les différentes entités (différents greffons dans les différents agents) se base sur un protocole unifié. Ce protocole définit un format générique pour les messages échangés. Les greffons utilisent ces messages pour se communiquer et échanger les données de gestion entre les différents agents sur lesquels ils résident. Chaque greffon définit ses propres messages et spécifie le contenu de ses enregistrements de données.

AMAM représente l'implantation à l'aide de la technologie active de notre architecture distribuée pour la gestion de multicast sur IP. Le choix de l'implantation en

actif vise à tirer profit des avantages de flexibilité et d'extensibilité que la technologie active offre [SCH 99],[TEN 97],[FES 00].

4. Sécurité dans AMAM

Cette architecture nous permet de réaliser une solution qui résiste au facteur d'échelle pour la gestion de clefs. Elle se base sur le principe de génération d'une seule clef globale par la source et de plusieurs clefs locales par les routeurs frontaux. Elle s'implante comme suit :

– l'agent MSA genère une clef globale et la distribue à tous les nœuds de l'arbre multicast. Cette clef est utilisée pour crypter le trafic à délivrer. La clef globale est générée une seule fois mais elle peut être rafraîchie régulièrement pour plus de sécurité. La fréquence de rafraîchissement de cette clef reste un choix politique de l'ISP ou un paramètre du contrat de service avec l'exploitant de service ;

– si un routeur possédant la clef globale quitte l'arbre de distribution multicast, le greffon de sécurité disparaît et par conséquent la clef globale est systématiquement détruite ;

– chaque agent MEA génère en local une clef locale et la distribue sur ses membres en local ;

– l'agent MEA décrypte le trafic avec la clef globale, le chiffre avec la clef locale et le diffuse à ses membres ;

– les membres déchiffrent le trafic avec la clef locale qu'ils ont reçue ;

– à chaque nouvel abonnement/désabonnement enregistré, l'agent MEA régénère une nouvelle clef locale et la diffuse sur ses membres en local. Il chiffre ensuite le trafic avec cette nouvelle clef.

Le rafraîchissement de clef local rend la solution plus résistante au facteur de l'échelle vu que la dynamique n'affecte plus la totalité de membres abonnés mais uniquement les membres en local[8].

4.1. *Architecture du greffon de sécurité*

Le greffon de sécurité se compose de trois modules principaux (voir figure 3) :

– ***module de communication :*** son rôle est d'assurer la communication entre les différents greffons de sécurité déployés sur les différents agents de gestion sur l'arbre de distribution multicast. Il interagit aussi avec le greffon MP (multicast proxy)[9] pour collecter les informations de sécurité fournies dans les requêtes d'abonnement.

8. Cette solution engendre un surcoût dû au chiffrement/déchiffrement de trafic mais une implantation des algorithmes de chiffrement/déchiffrement sous forme matérielle peut limiter l'impact temporel.

9. Ce greffon possède des interfaces avec les protocoles de gestion de membres IGMP et MLD aussi bien qu'avec les protocoles de routage multicast tel que PIM-SSM

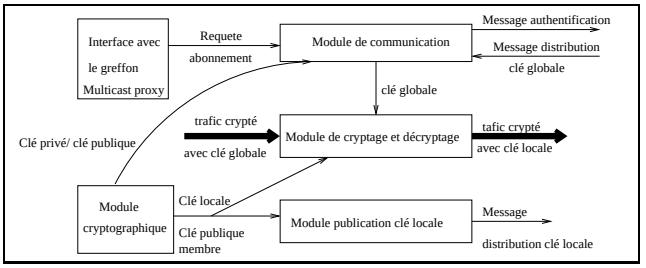


Figure 3. *Différents modules du greffon de sécurité*

– ***module de chiffrement et de déchiffrement :*** Ayant la clef globale fournie par le module de communication et la clef locale générée en local, ce module effectue le chiffrement et le déchiffrement de trafic multicast. Ce module n'est fonctionnel qu'aux agents MEA

– ***module de publication :*** ce module sert principalement à publier les clefs générées localement aux différents membres abonnés au service multicast mais il peut servir également à communiquer, en temps réel, d'autres informations de notification sur la validité de la permission d'accès au service dû à l'expiration de son crédit[10] ou alors à une éventuelle expulsion.

– ***module cryptographique :*** ce module permet la génération des différentes clefs et gère l'infrastructure PKI pour retrouver les différentes clefs publiques des membres et des différents agents (voir figure 3).

4.2. *Messages de communication*

La communication entre les différents greffons situés sur les différents agents utilise le protocole d'échange de messages spécifié dans AMAM. Le protocole définit un format générique de messages (Figure 4). Chaque greffon spécifie le contenu de ses enregistrements de données pour définir ses propres messages.

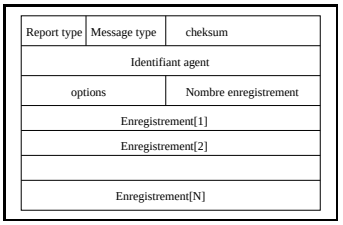


Figure 4. *Le format du message générique d'AMAM*

10. Les informations concernant la comptabilité de service pour chaque membres sont fournies par le greffon de comptabilité défini dans AMAM.

Le greffon de sécurité nécessite trois types de messages :

– ***Message d'authentification*** émis d'un MEA vers un MNA ou d'un MNA vers un MSA. Le champ option contient le jeton de l'émetteur signé avec sa clef privé. Chaque enregistrement de ce message contient l'identification du canal sollicité par les abonnés ;

– ***Message de distribution de la clef globale*** émis d'un MNA vers un MEA ou d'un MSA vers un MNA. Un enregistrement de ce message contient l'identifiant du canal et sa clef globale. Le champ option contient le jeton signé de l'émetteur pour assurer son authentification. Ce message sera chiffré avec la clef publique du destinataire.

– ***Message de distribution de la clef locale*** émis d'un MEA vers un membre abonné. Un enregistrement de ce message contient la clef locale délivrée par le MEA à un abonné.

Pour tous ces messages, le champ `type Report` est mis à l'identificateur du greffon de sécurité spécifié dans AMAM. À la réception d'un de ces messages, l'agent actif le transmet au `PluginManager` qui va assurer que le greffon de sécurité est bien présent et instancié. Si tel est le cas, le message lui est transmis.

5. Fonctionnalités du greffon de sécurité

Les fonctionnalités offertes par le greffon de sécurité sont le contrôle d'accès au canal de diffusion et la protection du contenu.

5.1. *Le contrôle d'accès*

Le contrôle d'accès se fait en deux étapes :

– l'authentification de l'abonné et des agents s'ils ne sont pas encore deployés.

– la vérification de la validité de l'abonnement d'un abonné. Cette vérification est réalisée par le MEA.

Avant d'accepter des abonnés à un canal de diffusion, le MSA crée la clef globale du canal qui sert pour le chiffrement du trafic en cas de trafic sécurisé. Avant d'accéder au canal de diffusion, chaque entité de notre architecture, que se soit un agent de supervision ou un abonné, doit être authentifiée. Un agent est délégué dès qu'il possède, après authentification, ces deux clefs. L'authentification est assurée grâce à un jeton signé. Ce jeton est composé de :

– `Ns` : nombre spécifique attribué par le prestataire de services lors de la souscription au service de diffusion du canal.

– le tuple `(S, ch)`, avec `S` l'adresse de la source et `ch` l'adresse du canal.

– une estampille.

– l'adresse IP du récepteur.

Dans le cas d'un jeton signé d'un agent, le champ `Ns` sera ignoré ou mis à zéro. Deux scénarios se présentent lors de l'abonnement d'un client au canal de diffusion. Dans le premier scénario, l'agent MEA est délégué c'est à dire qu'il possède la clef globale du canal. Dans le deuxième scénario, l'agent MEA est non délégué et son MNA en amont ne l'est pas non plus. Il s'agit de la phase de déploiement des agents sur l'arbre de distribution multicast.

5.1.1. *MEA délégué*

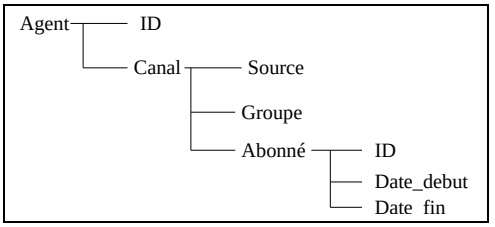


Figure 5. *La PIB maintenue par l'agent frontal MEA*

Cette situation se produit lorsque les agents sont déjà déployés sur l'arbre multicast, et qu'un nouveau client veut s'abonner au canal. Le client qui veut joindre le canal envoie une requête d'abonnement à son MEA qui contient son jeton signé avec sa clef privée. À la réception de la requête, le MEA authentifie le client. Si l'authentification réussit, le MEA vérifie la validité de l'abonnement du client en vérifiant dans sa base d'information de politiques (PIB) l'entrée correspondante à cet abonné [CHA 01c]. Une entrée dans la PIB d'un abonné (Figure 5) contient son adresse IP et deux dates date_début, date_fin qui indiquent le commencement et l'expiration de la validité de la souscription. Ces deux dates sont interprétées par le MEA comme suit :

– `SI (date_fin > date_début ET TIME < date_fin) ALORS` l'abonné peut recevoir la clef de déchiffrement. Le MEA lui envoie le message de distribution de la clef locale.

– `SI (date_fin > date_début ET TIME > date_fin) ALORS` la demande d'abonnement est ignorée ou redirigée vers un service de souscription suivant une politique prédéfinie.

5.1.2. *MEA non délégué*

Dans ce cas, le MEA vient d'être deployé par l'administrateur sur un routeur frontal. À son initialisation, le MEA va instancier sa PIB, pour avoir la liste de ses abonnés locaux ainsi que leurs permissions d'accès au canal de diffusion. À la réception d'une requête d'abonnement, le MEA calcule un RPF[11] vers la source et essaye de joindre l'arbre multicast en remontant la requête d'abonnement au premier MNA délégué.

11. Reverse Path Forwarding

Cette requête contient le jeton signé du MEA. Le MNA va authentifier le MEA. En cas de réussite il lui envoie le message de distribution de la clef globale chiffrée avec sa clef publique. À la réception de ce message, le MEA devient délégué et génère sa clef locale, et effectue la vérification de validité de l'abonnement du client. En cas de réussite, il lui envoie la clef locale chiffrée avec sa clef publique.

5.2. *Protection du contenu*

La protection du contenu est assurée par le chiffrement du trafic à l'aide d'une clef secrète partagée entre le MSA et le MEA. Sur réception du trafic, le MEA le décrypte puis le chiffre avec sa clef locale avant de le renvoyer aux abonnés. Le changement de la clef globale est assuré par le MSA en diffusant, pour tous les MEA, un message de renouvellement contenant la nouvelle clef cryptée avec l'ancienne clef globale. L'agent frontal MEA à son tour procède à un changement de la clef locale si l'un des cas suivants se présente :

– la réception d'une nouvelle demande d'abonnement dans un service où l'entrante doit pas pouvoir accéder à l'ancien trafic du canal. L'exemple d'un tel service est celui de la diffusion d'un communiqué (à tous) après déliberation (d'un sous-ensemble) eg, jury de festival de cinéma.

– l'expiration de la permission d'accès d'un abonné ou l'expulsion d'un abonné.

– la périodicité du renouvellement de la clef locale.

Dans tout ces cas, l'agent frontal (le MEA) crée une nouvelle clef et la diffuse par le message de distribution clef locale.

– Dans le cas d'un nouveau abonné, le MEA envoie le message de renouvellement aux anciens membres crypté avec l'ancienne clef locale et au nouveau abonné crypté avec sa clef publique.

– A l'exclusion d'un abonné, le message de renouvellement de la clef locale sera envoyé à tous les membres crypté avec leurs clefs publiques excepté le membre qui vient d'être exclu.

– Le renouvellement périodique de la clef locale s'effectue avec une période de rafraîchissement qui est spécifiée dans la PIB de l'agent.

Le message de renouvellement sera envoyé à chaque membre crypté avec la clef publique du récepteur.

6. Intégration dans FLAME

Nos agents de supervision sont implantés sous forme d'applications actives dans l'environnement d'exécution FLAME[12].

12. Full-Fledged Loria- Alcatel Active Management Environment

6.1. *Description de FLAME*

FLAME est une plate-forme active de supervision des réseaux IP [D'A 02]. Cet environnement d'exécution se base sur un gestionnaire de nœud et sur des instances d'applications actives. Le gestionnaire a en charge le téléchargement de code, la réception des paquets, les connexions vers les agents d'administration, le lancement et l'arrêt des applications actives. Les applications quand à elle sont des processus qui font partie de l'Environnement d'Exécution (EE) dont elles exploitent les services tout en hébergeant leur propre code. Tout paquet actif est reçu et mis en forme par le gestionnaire. Si l'application active correspondante est bien présente et instanciée, le paquet lui est transmis. Sinon son code sera téléchargé sur le nœud avant d'être instancié et le paquet lui est transmis. FLAME possède plusieurs caractéristiques avancées qui sont utiles pour l'implantation de nos agents de supervision. Ces caractéristiques sont :

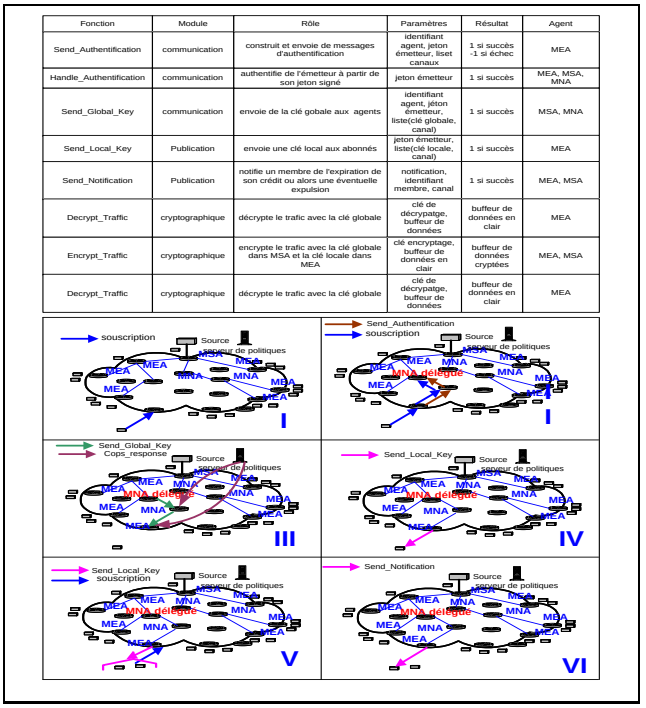
– l'extensibilité de ces fonctionnalités d'une façon dynamique. Ceci nous permet d'enrichir et de mettre à jour notre agent de supervision avec les greffons nécessaires sans interrompre son fonctionnement.

– l'administration des applications actives via des agents d'administration implantés dans l'environnement d'exécution accessible par telnet ou par l'intermédiaire de politiques en utilisant le protocole COPS [DUR 00]. L'environnement d'exécution implante un point d'enforcement de politiques (PEP) qui interagit avec un serveur COPS pour fournir aux applications actives un service d'approvisionnement et de contrôle d'accès. Ceci permettra à l'agent de supervision de s'approvisionner avec sa configuration et en particulier, le greffon de sécurité peut connaître les droits d'accès au canal de ces clients locaux.

6.2. *Spécification de l'API de sécurité*

Le greffon de sécurité est implanté sous forme d'une bibliothèque dynamique chargée à la volée par l'agent de supervision en cas de besoin. Grâce à l'extensibilité offerte par FLAME, notre agent de supervision est extensible que se soit un MEA, un MNA ou un MSA avec le greffon de sécurité sans interrompre son fonctionnement. Le greffon offre les différentes fonctions de sécurité. La figure 6 comporte la description des différentes fonctions ainsi que les différentes entités qui y font appel.

Dans la figure 6, un scénario de déploiement utilisant l'API de sécurité est explicité. Quand un membre s'abonne au service multicast, il sera authentifié par son MEA. Avant de rejoindre l'arbre de distribution, chaque routeur sur le chemin vers le premier routeur faisant partie de l'arbre multicast et renfermant un MNA délégué doit s'authentifier au près de ce MNA. Dès son authentification, le MNA authentifié reçoit la clé globale de ce MNA délégué et devient par conséquent délégué aussi. La clef globale est ensuite envoyée à chacun de ces routeurs situés entre le MEA et le responsable de son authentification. Disposant de sa PIB, le MEA authentifie le membre et lui envoie la clef générée en local. A l'arrivé d'un nouveau membre, le MEA l'au-



Fonction	Module	Rôle	Paramètres	Résultat	Agent
Send_Authentification	communication	construit et envoie de messages d'authentification	identifiant agent, jeton émetteur, liset canaux	1 si succès -1 si échec	MEA
Handle_Authentification	communication	authentifie de l'émetteur à partir de son jeton signé	jeton émetteur	1 si succès	MEA, MSA, MNA
Send_Global_Key	communication	envoie de la clé gobale aux agents	identifiant agent, jéton émetteur, liste(clé globale, canal)	1 si succès	MSA, MNA
Send_Local_Key	Publication	envoie une clé local aux abonnés	jeton émetteur, liste(clé locale, canal)	1 si succès	MEA
Send_Notification	Publication	notifie un membre de l'expiration de son crédit ou alors une éventuelle expulsion	notification, identifiant membre, canal	1 si succès	MEA, MSA
Decrypt_Traffic	cryptographique	décrypte le trafic avec la clé globale	clé de décrypatge, buffeur de données	buffeur de données en clair	MEA
Encrypt_Traffic	cryptographique	encrypte le trafic avec la clé globale dans MSA et la clé locale dans MEA	clé encryptage, buffeur de données en clair	buffeur de données crypées	MEA, MSA
Decrypt_Traffic	cryptographique	décrypte le trafic avec la clé globale	clé de décrypatge, buffeur de données	buffeur de données en clair	MEA

Figure 6. *Scénario de déploiement*

thentifie en local et régenère et diffuse une nouvelle clef locale. Le MEA envoie des messages de notification à un abonné donné sur la validité de la permission d'accès au service dû à l'expiration de son crédit ou alors à une éventuelle exclusion.

7. Conclusion

Dans ce papier, nous avons décrit notre architecture à trois niveaux AMAM qui distribue les données et les fonctions de gestion. Cette architecture considère le caractère dynamique de services multicast, les spécificités de ses fonctions de gestion et les critères de passage à l'échelle et la facilité de déploiement. Nous avons présenté ensuite l'extension de cette architecture pour le support de services de sécurité de multicast. Cette extension vise à déléguer la gestion de renouvellement de clefs aux agents frontaux pour satisfaire les critères de la dynamique et de passage à l'échelle. Nous avons détaillé l'architecture interne du greffon de la sécurité ainsi que les fonctionnalités qu'il offre telles que l'authentification et le contrôle de contenu. Enfin une API pour l'intégration de ce greffon dans l'environnement d'exécution actif FLAME a été spécifiée. Un déploiement dans FLAME pour les services basés sur le schéma multicast SSM constitue notre travail futur. Une simulation du protocole d'échange de messages ainsi qu'une étude de performance de déploiement dans FLAME est également prévue.

8. Bibliographie

[BAL 96] BALLARDIE A., « Scalable Multicast Key Distribution, RFC 1949, Experimental », May 1996.

[BEL 89] BELLOVIN S., « Security Problems in the TCP/IP Protocol Suite », *ACM Computer Communications Review*, vol. 19, n° 2, 1989.

[CAI 01] CAIN B., DEERING S., FENNER B., KOUVELAS I., THYAGARAJAN A., « Internet Group Management Protocol, Version 3, RFC 1075 », March 2001.

[CHA 01a] CHADDOUD G., CHRISMENT I., SHAFF A., « Dynamic Group Communication Security », SaintPetersburg, Russie, Mai 2001.

[CHA 01b] CHADDOUD G., CHRISMENT I., SHAFF A., « Dynamic Group Key Management », ISCC Hammamet, Tunisie, Juillet 2001.

[CHA 01c] CHAN K., SELIGSON J., DURHAM D., GAI S., MCCLOGHRIE K., HERZOG S., REICHMEYER F., YAVATKAR R. SMITH A., « COPS Usage for Policy Provisioning (COPS-PR), RFC 3084, standard track », March 2001.

[D'A 02] D'ALU S., FESTOR O., « FLAME : une plate-forme active dédiée à la supervision des services de l'Internet », Proc. CFIP'2002, Montréal, Canada,, May 2002.

[DUR 00] DURHAM D., BOYLE J., COHEN R., HERZOG S., RAJAN R., SASTRY A., « The COPS (Common Open Policy Service) Protocol, RFC 2748, standard track », January 2000.

[FES 00] FESTOR O., CHRISMENT I., FLEURY E., « Les réseaux programmables », rapport n° 3913, Mars 2000, INRIA.

[FOR 94] FORD W., *Computer Communications Security : Principles, Standard Protocols and Techniques*, Prentice Hall, 1994.

[HAB 01] HABERMAN B., WORZELLA R., « IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol », RFC 3019, Janvier 2001.

[HAR 97] HARNEY H., MUCKENHIRN C., « Group Key Management Protocol (GKMP) Architecture, RFC 2094 , experimental », July 1997.

[KEN 98a] KENT S., ATKINSON R., « IP Authentication Header (AH), RFC 2402, standard track », november 1998.

[KEN 98b] KENT S., ATKINSON R., « IP Encapsulating Security Payload (ESP), RFC 2406, standard track », november 1998.

[MAU 97] MAUGHAN D., SCHERTLER M., SCHNEIDER M., TURNER J., « Internet Security Association and Key Management Protocol (ISAKMP) », Internet Draft, February 1997.

[OPP 96] OPPLIGER R., ALBANESE A., « Distributed Registration and Key Distribution (DiRK) », May 1996.

[SAL 03] SALLAY H., FESTOR O., « A Highly Distributed Dynamic IP Multicast Accounting and Management Framework », accepté à IM'03, Mars 2003.

[SCH 99] SCHÖNWÄLDER J., « Emerging Internet Management Technologies », IEEE IM'99 (Tutorial), October 1999.

[TEN 97] TENNENHOUSE D., SMITH J., SINCOSKIE W., WETHERALL D., MINDEN J., « A survey of Active Network Research », *IEEE Communications Magazine*, , 1997.

[WAL 97] WALLNER D., HARDER E., AGEE R., « Key Management for Multicast : Issues and Architecture », Internet Draft, july 1997.