

République Algérienne Démocratique et Populaire.
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique.

Université A. Mira de Béjaia.
Faculté des Sciences et des Sciences de l'Ingénieur

Mémoire de Magistère

En Informatique
Option
Réseaux et Systèmes Distribués

Thème

**Gestion de clés Scalable pour des
Communications de Groupe Sécurisées**

**Présenté par
Saïd GHAROUT**

Devant le jury composé de :

Pr M. Abmed Nacer	Président	USTHB, Alger, Algérie
Pr N. Badache	Examineur	USTHB, Alger, Algérie
MC F. Naït Abdesselam	Examineur	USTL, Lille, France
Pr A. Bouabdallah	Directeur de Thèse	UTC, Compiègne, France
Dr Y. ChaUal	Invité	UTC, Compiègne, France

Promotion 2004 2005

Résumé

Le manque de sécurité empêche le déploiement à grande échelle des communications multicast, pour lesquelles la demande ne cesse pas d'augmenter chez les fournisseurs de services Internet et les distributeurs du contenu multimédia. La nature dynamique des sessions multi-parties complique le service de *confidentialité*. En effet, chaque changement d'adhésion induit une redistribution d'une nouvelle clé de chiffrement du trafic à tous les membres légitimes. Les solutions proposées pour faire face à cette limitation, connue sous le nom du phénomène *1 affecte n*, consistent à organiser les membres en sous-groupes, où chaque sous-groupe utilise une *clé de trafic* indépendante. Cependant, ces solutions présentent un nouveau défi qui est le besoin de la *traduction* du flux chiffré à chaque fois qu'il passe d'un sous-groupe à un autre. Ceci est considéré comme un inconvénient pour les applications qui exigent une transmission en temps réel telle que la vidéo-conférence. Dans cette thèse de Magistère, nous proposons une nouvelle approche adaptative pour la gestion de clé de groupe qui tient en compte l'aspect dynamique du groupe. Notre approche, appelée DSGK, emploie un regroupement adaptatif des zones de chiffrement en clusters pour utiliser la même *clé de chiffrement du trafic*. Le partitionnement de groupe en clusters de zones est réalisé d'une manière qui réduit au même temps les charges dues à la *redistribution de clé* et à la *traduction de flux*. Les résultats de simulation confirment la convenance de DSGK aux groupes fortement dynamiques en temps et en espaces par rapport à d'autres approches dans la littérature.

Mots clés : Multicat, Sécurité, Gestion de clés, Scalabilité, Dynamisme.

Abstract

The lack of security obstructs the effective large scale deployment of multicasting, for which the demand is increasing from both Internet service providers and content distributors. The dynamic nature of multiparty sessions complicates the *confidentiality* service. Indeed, each membership change induces a re-distribution of a new traffic encryption key to all legitimate members. The proposed solutions to cope with this limitation, commonly called *1 affects n* phenomenon, consist of organizing group members into subgroups that use independent traffic encryption keys. This kind of solutions introduce a new challenge which is the requirement of *key translation* of the encrypted flow whenever it passes from one subgroup to another. This is a serious drawback for applications that require real-time transmission such as video-conferencing. In this Magister thesis, we propose a novel adaptive approach which is dynamism aware. Our approach, called DSGK, uses adaptive clustering of encryption areas into clusters that use the same *traffic encryption key*. The partitioning is made in a way that reduces both *re-keying* and *key translation* overheads. Simulation results confirm the suitability of DSGK to highly dynamic groups with *space and time dependent dynamism*, compared to other approaches in the literature.

Keywords : Multicat, Security, Key Management, Scalability, Dynamism.

Table des matières

Glossaire	i
Table des matières	ii
Liste des figures	v
Liste des tableaux	vii
Liste des algorithmes	viii
Introduction	1
Contribution	2
Plan du mémoire	2
1 Le Multicast	3
1.1 Introduction	3
1.2 La diffusion multicast	4
1.3 La notion de groupe multicast	4
1.4 IP Multicast	5
1.5 Le protocole IGMP	6
1.6 Vulnérabilité de IP Multicast	7
1.7 Conclusion	8
2 Sécurité dans le Multicast	9
2.1 Introduction à la cryptographie	9
2.2 Confidentialité	9

2.3	Le chiffrement	10
2.3.1	Le chiffrement symétrique	10
2.3.2	Le chiffrement asymétrique	11
2.4	Protocole de Diffie-Hellman	13
2.5	Clé de groupe	13
2.6	Gestion de clés de groupe	14
2.7	Propriétés d'une clé de groupe	14
2.8	La scalabilité dans la gestion de clé de groupe	15
2.9	Conclusion	15
3	Taxonomie sur la gestion de clé de groupe	16
3.1	Approche à clé commune	17
3.1.1	Architectures centralisées	17
3.1.1.1	Approche paires point-à-point	17
3.1.1.2	Approches hiérarchiques (Arborescentes)	19
3.1.1.3	Comparaison	23
3.1.2	Architectures décentralisées	24
3.1.2.1	Comparaison	29
3.1.3	Protocoles d'accord de clés distribués	30
3.1.3.1	Coopération en anneau (<i>Ring-based cooperation</i>)	31
3.1.3.2	Approche de diffusion (<i>Broadcast-based approach</i>)	37
3.1.3.3	Comparaison	39
3.1.4	Conclusion	39
3.2	Approche TEK par sous-groupe	40
3.2.1	Comparaison et conclusions	46
3.3	Conclusion	47
4	Approche scalable pour la gestion de clé de groupe	48
4.1	Motivations	48
4.2	Généralités sur DSGK	49
4.3	Formalisation du problème	50
4.4	Nomenclature	51
4.5	Propriétés d'un agent	52
4.6	Stratégies de mise à jour de clé	53
4.6.1	Redistribution lors d'une adhésion	54
4.6.2	Redistribution lors d'un départ	54
4.6.3	Accord sur une TEK commune	55
4.6.4	Mise à jour de clé lors d'une division	56
4.6.5	Mise à jour de clé lors d'une fusion	57
4.7	Fonction de coût d'un cluster	58
4.8	Conclusion	62

5	Description et preuve du protocole DSGK	63
5.1	Le protocole DSGK	63
5.1.1	Les différents messages utilisés	65
5.1.2	Comportement dynamique des agents	66
5.1.2.1	Envoi des messages sur le dynamisme	67
5.1.2.2	Réception d'un message NEW_DYN_INF	69
5.1.2.3	Réception d'un message NEW_TEQ_RQ	69
5.1.2.4	Réception d'un message IM_ACTIVE	70
5.1.2.5	Réception d'un message NEW_TEQ	70
5.1.2.6	Traitement des changements d'adhésion	71
5.2	Preuves d'optimalité	72
5.2.1	Nombre de partitions possibles	72
5.2.2	Ré-écriture de l'impact mutuel	73
5.2.3	Optimalité de la division	74
5.2.4	Optimalité de la fusion	75
5.2.5	Stabilité de la partition	76
5.3	Conclusion	77
6	Simulation de DSGK et mesures de performances	78
6.1	Introduction	78
6.2	Modèle de simulation	79
6.3	Résultats de simulation	81
6.3.1	Impact des facteurs de poids (α, β)	81
6.3.2	Impact de la taille du groupe	83
6.3.2.1	Impact des inter-arrivées	84
6.3.2.2	Impact de la durée de séjour	85
6.3.3	Impact de la fréquence des opérations de division / fusion (split / merge)	86
6.4	Conclusion	87
	Conclusion et perspectives	90
	Bibliographie	92