République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A/Mira de Béjaïa
Faculté des Sciences et des Sciences de l'Ingénieur
Département d'Informatique
École Doctorale Réseaux et Systèmes Distribués

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

Soutenu le 16/11/2005

Devant le jury composé de :

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

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