# Etude et évaluation d'un service de connexions mobiles sécurisées à l'aide d'outils de virtualisation de réseaux mobiles

30 novembre 2012

## 1 Informations générales

**Responsable :** Damien MAGONI

Lieu : LaBRI

Téléphone : 05.40.00.35.40

E-mail : magoni@labri.fr

Equipe : LSR

Thème : Comet

Projet : CAPE

**Mots-clés :** protocoles de mobilité et de sécurité, réseau mobile virtuel

## 2 Description du sujet

L'objectif de ce travail de recherche est d'étudier, d'étendre et d'évaluer un service permettant de créer des connexions applicatives mobiles sécurisées. Ce service, nommé MUSeS, a été défini dans [2] et s'appuie sur l'architecture de réseau recouvrant CAPE/CLOAK [1]. La sécurisation du réseau recouvrant se fait à deux niveaux : au niveau des connexions systèmes et au niveau des connexions applicatives. Les connexions systèmes seront négociées entre les équipements voisins du réseau recouvrant en utilisant les identifiants des machines, définis dans ce même réseau. Les connexions applicatives seront négociées entre les entités utilisatrices du réseau recouvrant en utilisant les identifiants des entités, définis dans ce même réseau. Il faudra compléter ce service afin qu'il fournisse des services pour l'authentification des membres et pour la sécurisation des liens entre voisins. Il faudra compléter l'interface de programmation applicative et le module logiciel MUSeS écrit en C et permettant de gérer cette sécurisation. Ce module devra être capable de gérer la distribution des clés publiques des éléments tels qu'équipements et entités en utilisant éventuellement la DHT fournie par l'architecture CAPE.

Ce service permet d'interrompre une connexion système utilisant un protocole de transport sécurisé (e.g. SSL, SSH, etc) puis de la rétablir avec d'autres paramètres de sécurité sans interrompre la connexion applicative correspondante. Cette faculté permet, au cours d'une même connexion applicative, de déplacer l'équipement entre différents réseaux de manière transparente (i.e. sans avoir à utiliser Mobile IP) ou bien encore de changer de protocole de sécurité selon les caractéristiques du réseau.

Les performances de ce service complété seront évaluées par prototypage à l'aide du logiciel *nemo* [3] qui permet de scénariser en temps réel l'activité d'un réseau mobile composé de machines virtuelles. Il faudra donc définir plusieurs scénarios de mobilité puis évaluer les performances du service face à l'évolution de la connectivité du réseau. Il sera aussi nécessaire d'évaluer sur ces mêmes scénarios, d'autres solutions similaires telles que IPsec+MobileIP, MOBIKE [4] et N2N [5] afin de les comparer à MUSeS.

# 3 Références bibliographiques


1. Virtual Connections in P2P Overlays with DHT-Based Name to Address Resolution.
   *Telesphore Tiendrebeogo, Daouda Ahmat, Damien Magoni, Oumarou Sie.* International Journal on Advances in Internet Technology, 5(1) :11-25, 2012.
2. MUSeS : Mobile User Secured Session.
   *Daouda Ahmat, Damien Magoni.* WD'12 - IFIP Wireless Days International Conference, 6 pp., November 21-23, 2012, Dublin, Ireland.
3. Network Emulator : a Network Virtualization Testbed for Overlay Experimentations. *Vincent Autefage, Damien Magoni.* CAMAD'12 - IEEE International Workshop on Computer-Aided Modeling Analysis and Design of Communication Links and Networks, pp. 38-42, September 17-19, 2012, Barcelona, Spain.
4. MOBIKE http ://www.rfc-editor.org/rfc/rfc4621.txt
5. N2N : A Layer Two Peer-to-Peer VPN.
   *Deri, Luca and Andrews, Richard.* Proceedings of the 2nd international conference on Autonomous Infrastructure, Management and Security : Resilient Networks and Services, 2008, Bremen, Germany, pages = 53-64, doi = 10.1007/978-3-540-70587-1_5
6. Building and Managing Policy-Based Secure Overlay Networks.
   *Perez, G.M. ; Clemente, F.J.G. ; Skarmeta, A.F.G. ;* Parallel, Distributed and Network-Based Processing, 2008. PDP 2008. 16th Euromicro Conference on, Digital Object Identifier : 10.1109/ PDP.2008.92, Publication Year : 2008 , Page(s) : 597 - 603.
7. Securing Overlay Activities of Peers in Unstructured P2P Networks.
   *Jun-Cheol Park ; Geonu Yu ;* Computational Intelligence and Security, 2006 International Conference on, Volume : 2, Digital Object Identifier : 10.1109/ ICCIAS.2006.295433, Publication Year : 2006 , Page(s) : 1105 - 1108.
8. Wheel of Trust : A Secure Framework for Overlay-Based Services.
   *Guor-Huar Lu ; Zhi-Li Zhang ;* Communications, 2007. ICC '07. IEEE International Conference on, Digital Object Identifier : 10.1109/ ICC.2007.195, Publication Year : 2007 , Page(s) : 1148 - 1153.
9. STORM : A Secure Overlay for P2P Reputation Management.
   *Ravoaja, A. ; Anceaume, E. ;* Self-Adaptive and Self-Organizing Systems, 2007. SASO '07. First International Conference on, Digital Object Identifier : 10.1109/ SASO.2007.57, Publication Year : 2007 , Page(s) : 247 - 256.
10. Improving Messaging Security in Structured P2P Overlay Networks.
    *Yu, H. ; Buford, J. ; Merabti, M. ;* Multimedia and Expo, 2007 IEEE International Conference on, Digital Object Identifier : 10.1109/ ICME.2007.4284673, Publication Year : 2007 , Page(s) : 408 - 411.