

Acronyme du projet	DOCTOR		
Nom	Deployment and securisation of new functionalities in virtualized networking environments		
Financement et labellisation			
Dates	Début : 1 er décembre 2014		Fin : 30 septembre 2018
Consortium : Coordonné par Orange			
			

Résumé de la présentation du projet :

Les réseaux ICN (*Information Centric Networking*) définissent un paradigme dans lequel les contenus échangés sont au cœur du fonctionnement du réseau, depuis le nommage des paquets jusqu'au routage. Apparues en 2006, les solutions actuelles sont suffisamment matures pour envisager leur déploiement et c'est notamment le cas de NDN (*Named Data Networking*), architecture largement étudiée dans la littérature scientifique qui possède une implémentation fonctionnelle et maintenue. Toutefois, pour un opérateur de l'Internet, envisager de déployer une telle solution protocolaire n'est pas envisageable pour deux raisons. La première est le coût associé à son déploiement qui nécessite un changement d'infrastructure ; la seconde est le manque de solutions pour sa surveillance et sa sécurité.

Le projet DOCTOR vise à fournir des solutions scientifiques et techniques pour le déploiement des réseaux ICN en utilisant la virtualisation des fonctions réseaux (*NFV – Network Function Virtualisation*). Dans ce cadre, différentes contributions issues du projet seront présentées. La première est une passerelle qui permet de traduire les requêtes et réponses du protocole HTTP en paquets ICN, permettant de montrer l'utilisation d'un réseau ICN en conditions réelles. La seconde est la conception et la mise en œuvre d'un plan de monitoring et d'algorithmes de détection qui permettent de détecter deux attaques majeures du paradigme ICN : l'attaque par inondation d'intérêts et l'empoisonnement de cache. La dernière contribution est une architecture d'orchestration qui permet le déploiement virtualisé d'un réseau NDN et la mise en œuvre de contre-mesures automatiques face à l'empoisonnement de cache.

Pour chacune de ces contributions, une démonstration des solutions du projet sera faite avec les outils qui ont été mis en œuvre : Déploiement d'une topologie virtuelle NDN, acheminement de trafic réel HTTP, empoisonnement de contenu HTTP et mise en œuvre d'une contre-mesure automatique.

Contacts : Bertrand Mathieu (bertrand2.mathieu@orange.com), Orange Labs
Guillaume Doyen (guillaume.doyen@utt.fr), UTT/Institut Charles Delaunay