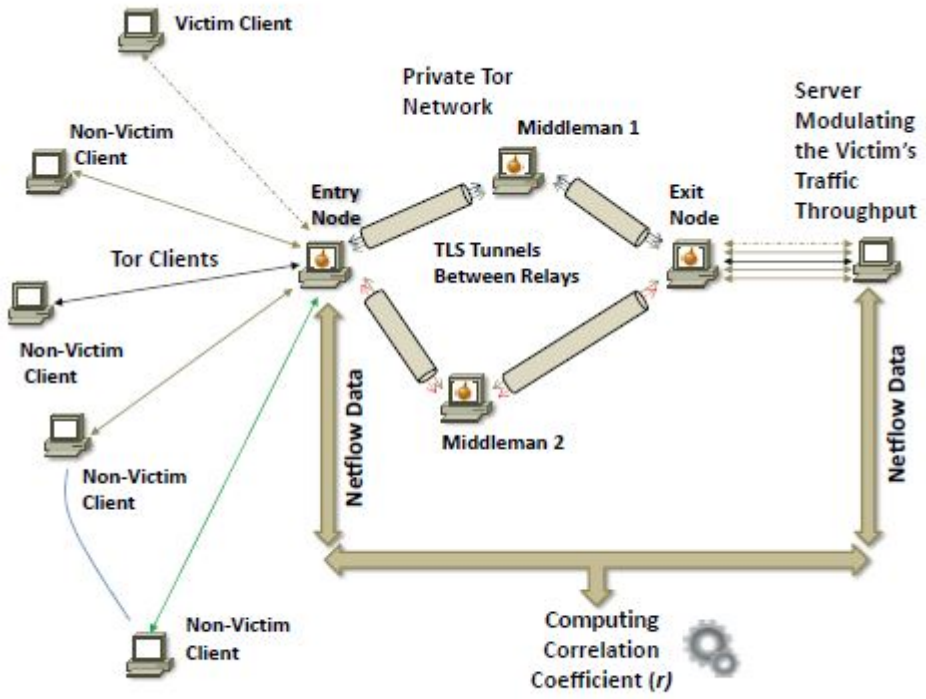
Tor : 8 utilisateurs sur 10 pourraient être identifiés

Selon des travaux de recherche dirigés par le professeur Sambuddah Chakravarty, de l'université Columbia aux Etats-Unis, l'anonymat offert par un outil comme Tor serait en partie illusoire. En se basant sur des techniques d'analyse de trafic fondées sur les caractéristiques intrinsèques des réseaux de communication à faible taux de latence comme Tor, les chercheurs parviennent à identifier 100 % des sources de trafic en laboratoire, et **81,4 % des utilisateurs d'un nœud public** (avec toutefois un taux de faux positifs de 6,4 %).

La détection du trafic Tor repose sur les caractéristiques du réseau d'anonymisation qui, pour fournir une qualité de service acceptable, veille notamment au délai séparant l'arrivée de deux paquets de données. Conséquence : un adversaire doté de moyens importants peut mettre sur pied une **attaque basée sur l'observation du trafic en quelques points du réseau**. « *Si la capacité actuelle des réseaux rend, à cette échelle, complexe le monitoring réseau au niveau des paquets, des assaillants peuvent potentiellement utiliser des fonctions de monitoring certes moins fiables, mais prêtes à l'emploi* », écrivent les chercheurs.

Tor : « pas de panique »

C'est tout l'intérêt de leur étude : montrer que l'identification d'utilisateurs Tor est **possible avec un outil aussi largement diffusé que Cisco NetFlow**. La méthode mise au point se base sur une perturbation du trafic côté serveur et sur la détection de ces perturbations côté client, via des analyses statistiques (voir schéma ci-dessous).



Dans un billet

posté sur le blog de Tor, **Roger Dingledine**, le responsable du projet, minimise la portée de ces travaux. « *C'est très bien de voir de nouvelles recherches sur les attaques par analyse de trafic, mais il ne s'agit pas d'un domaine nouveau. Donc ne paniquez pas avant d'avoir lu les notes de recherche sur le sujet, et celle-là en particulier qui, bien que soignée ne vient pas supplanter toutes les recherches précédentes* ». Et de pointer ce qui lui apparaît comme **une des principales faiblesses** des travaux conduits par Sambuddah Chakravarty : le **taux de faux positifs**. « *Il est facile de voir que, à grande échelle, ce problème de taux d'erreur devrait ôter toute utilité à l'attaque* », plaide Roger Dingledine. Qui note une des autres limitations de l'attaque : « *la capacité à mener cette attaque est liée à la part du trafic Internet qu'un assaillant est en mesure de mesurer ou de contrôler* ».

A lire aussi :
Anonabox, le routeur Tor déchu de Kickstarter
Tor : l'anonymat n'est pas toujours synonyme de sécurité