

WHISPER : communications confidentielles dans un monde décentralisé[†]

Valerio Schiavoni et Etienne Rivière

Institut d'Informatique, Université de Neuchâtel, Suisse.

De nombreuses applications réparties à grande échelle nécessitent de garantir la confidentialité des communications parmi des groupes de processus. Les messages échangés parmi le groupe légitime participant à une application doivent être indéchiffrables pour les autres nœuds du réseau, tout comme l'appartenance même des nœuds à un groupe doit être cachée. Les approches fondées sur l'utilisation d'une solution centralisée de type VPN ne passent que difficilement à l'échelle, et nécessitent la mise à disposition d'une infrastructure dédiée. Ce cadre n'est pas adapté à la fourniture d'applications et services à la demande, de manière auto-organisante et passant à l'échelle. Ce court article présente les grandes lignes de l'intergiciel WHISPER, une solution totalement décentralisée, ne nécessitant pas d'infrastructure dédiée ni d'autorité de certification, et permettant le support de la gestion de l'appartenance et des communications au sein d'un groupe de nœuds membres d'un grand réseau, tout en assurant la confidentialité à la fois des communications et de l'identité des membres du groupe. Plus particulièrement, nous considérons le cas où les autres nœuds peuvent observer les communications, que ce soit par l'observation d'un lien, ou lorsque ces nœuds servent de relais pour pallier les difficultés de communication dues au mécanismes de translation d'adresse (NAT). Les évaluations du prototype de WHISPER mettent en évidence sa propension à protéger la confidentialité des membres du groupe à un coût raisonnable.

Mots-clés : Réseaux à grande échelle, Gestion de groupe, Échantillonnage de pairs (*peer sampling*), Confidentialité.

1 Introduction

De nombreuses applications requièrent que les communications au sein d'un groupe de nœuds autorisés soient cachées au reste du réseau. Des salons de conversations privés au sein d'un réseau social mis en œuvre de façon répartie, des systèmes de diffusion d'information participatifs assurant la liberté d'expression en présence de censeurs, ou enfin des mécanismes de gestion de flux et d'admission pour de la télévision à la demande, constituent quelques exemples. La confidentialité des échanges dans un système réparti est fondée traditionnellement sur le cryptage des messages émis entre les pairs : seuls les pairs disposant de la clé associée au groupe privé peuvent obtenir le contenu. Néanmoins, le cryptage seul n'est pas suffisant dans le cadre d'applications réparties à grande échelle. Il est tout aussi nécessaire de protéger l'identité du groupe, c'est à dire sa composition. Afin de prévenir la possibilité d'attaques ciblées contre un groupe privé particulier, il ne doit pas être possible pour un nœud malveillant de déterminer l'appartenance d'un nœud à un groupe donné, ou même de déterminer l'existence d'un des groupes.

Les solutions centralisées, de type réseau privé virtuel (VPN) par exemple, permettent de gérer l'appartenance et la légitimité des membres d'un groupe privé, et de crypter les communications point-à-point entre ceux-ci. Toutefois, ces mécanismes passent difficilement à l'échelle, nécessitent une infrastructure dédiée et hautement disponible, et peuvent constituer la cible d'attaques contre le groupe lui-même en tant que point unique de défaillance. De plus, un attaquant qui peut observer les communications d'un nœud donné peut déterminer la composition du groupe lui-même.

Système considéré et modèle de fautes. Nous considérons des réseaux à grande échelle et auto-organisés, c'est-à-dire ne nécessitant pas la présence d'une autorité de confiance particulière avec un rôle d'arbitre par rapport aux nœuds ordinaires. De la même manière, le réseau ne comporte pas de nœud omniscient, et la gestion de l'appartenance, que ce soit au réseau dans son ensemble ou à chaque groupe privé, est effectuée de manière décentralisée. Le modèle de faute est celui de nœuds honnêtes mais curieux : nous considérons que par défaut, les nœuds cherchent à glaner de l'information sur la composition des groupes et sur les

[†]Les travaux présentés dans cet article apparaîtront dans les actes de la conférence ICDCS 2011.

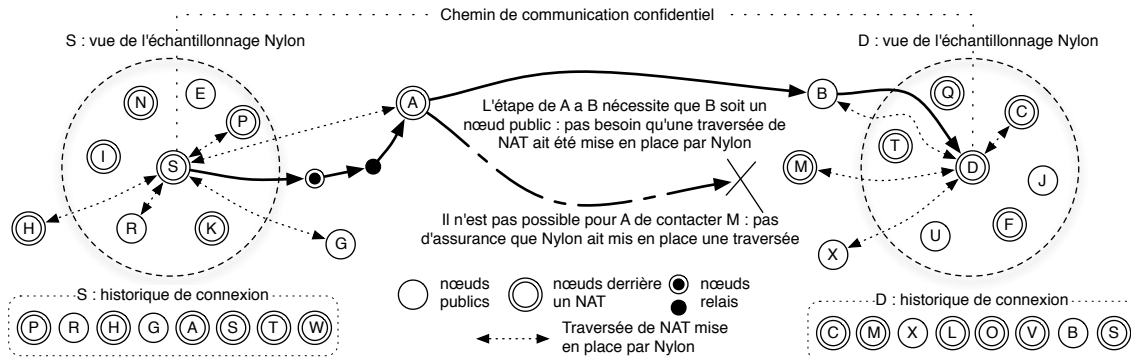


FIGURE 1: Construction d'un chemin de communication confidentiel à partir des historiques de connexion $\mathcal{N}ylon$.

messages échangés, mais respectent la définition du protocole et ne peuvent forger, rejouer ou omettre les messages. Nous considérons en outre que les liens ne sont pas fiables, que ce soit dû à l'existence de nœuds relais (voir ci-dessous) ou parce que le lien peut-être lui-même observé.

Gestion de l'appartenance globale par échantillonnage de pairs. L'ensemble des nœuds du réseau participent au réseau global (et public), qui forme un réseau logique (*overlay*) connecté. Ce réseau logique est construit et maintenu par un protocole d'échantillonnage de pairs [JVG⁺07] (pour *peer sampling*). Chaque nœud du réseau connaît un petit sous-ensemble d'autres nœuds appelé sa *vue*. L'ensemble des vues forment un graphe proche d'un graphe aléatoire. La gestion de l'appartenance est assurée par l'insertion rapide des nouveaux nœuds dans les vues d'autres nœuds du réseau et par la suppression des nœuds défaillants de ces vues après un temps borné. Cette maintenance se fonde généralement sur l'utilisation de protocoles épidémiques, qui sont ceux que nous considérons dans le cadre de cet article : périodiquement, chaque nœud sélectionne un nœud de sa vue et procède à un échange, ou brassage, de liens. Les protocoles d'échantillonnage de pairs servent de fondation à de nombreux protocoles épidémiques ou non : dissémination fiable, construction de réseaux logiques structurés, aggrégation, etc. [RBLP07]

Échantillonnage de pairs et translation d'adresse. Le modèle considéré par [JVG⁺07], où chaque nœud peut contacter directement n'importe quel autre, ne correspond pas à la réalité. En effet, une majorité (plus de 60% d'après [CF07]) des nœuds résident derrière des mécanismes de translation d'adresse (NAT) ou des pare-feux, qui empêchent toute communication entrante si une communication sortante préalable n'a pas été mise en place. Dans le reste de ce document, nous appellerons un P-nœud un nœud qui n'est pas derrière un NAT et donc joignable directement, et N-nœud celui qui est derrière un NAT.

Afin de pallier l'effet des N-nœuds sur la structure du réseau issu de l'échantillonnage, une amélioration des protocoles épidémiques appelée $\mathcal{N}ylon$ a été proposée [KPQS09]. La vue de chaque nœud contient non seulement l'identifiant du nœud lié mais aussi les informations nécessaires pour établir une connexion vers ce nœud. En particulier, dans de nombreux cas il n'est pas possible d'utiliser UPnP pour établir une route à travers le NAT de l'autre nœud, et il est nécessaire d'utiliser un nœud relais qui est déjà en contact avec ce nœud, et qui pourra le cas échéant retransmettre les communications point-à-point.

WHISPER : gestion de groupe privés. Notre proposition d'intergiciel pour la gestion de groupe privés dans les grands réseaux, nommée WHISPER, est composée des deux couches suivantes :

- la couche de communications confidentielles permet d'assurer la communication point-à-point entre deux nœuds en cachant à la fois le contenu du message échangé ainsi que les partenaires de l'échange ;
- la couche d'échantillonnage privée met en œuvre la gestion de l'appartenance au sein de chaque groupe privé, et propose la même interface que le protocole d'échantillonnage au sein du groupe global.

2 Communications confidentielles point-à-point

La couche de communication point-à-point (WCL, pour WHISPER *Communication Layer*) permet à deux pairs de communiquer sans qu'un pair intermédiaire (par ex., un pair relais pour passer un NAT) ne puisse connaître la source et la destination du message, ainsi que son contenu. Chaque nœud conserve un historique de connexion qui contient les identifiants des nœuds avec lesquels un échange de vue $\mathcal{N}ylon$ a été effectué récemment. Cet échange a nécessité que $\mathcal{N}ylon$ ouvre la connexion, et mette en place des relais et des ou-

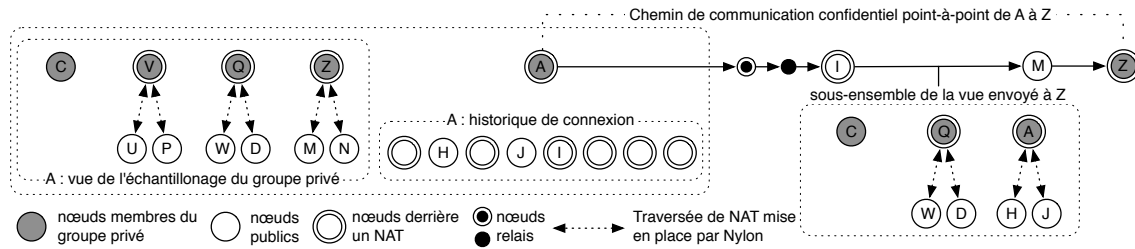


FIGURE 3: Échange de vues pour un groupe privé entre A et Z membres du groupe (I et M ne sont pas membres).

ouvertures de NAT qui persistent pour un temps dépendant du constructeur du NAT, mais qui par construction dépasse largement le temps de présence d'un pair dans l'historique de connexion. La figure 1 présente le principe de construction d'un chemin WCL. Il se fonde sur l'utilisation des historiques de connexion afin de construire un chemin anonymisant en oignon [Cha81, DMS04] entre S et D.

Le principe d'un tel chemin est illustré par la figure 2. Un chemin en oignon permet de cacher à la fois le contenu, la source et la destination d'un message. Le message initial est crypté avec une clé symétrique (AES) k et le nœud source sélectionne un nombre $m \geq 2$ de "mixes" afin de former un chemin vers la destination empruntant ces mixes. La clé AES k est ensuite cryptée successivement avec la clé asymétrique RSA de la destination D (notée $pubk_D$), puis dans le sens inverse du chemin jusqu'au premier mix. À chaque étape, l'identifiant du nœud suivant est encrypté avec la clé k (elle même encryptée sur plusieurs niveaux ou couches, d'où le nom d'*oignon*). Comme seul le nœud destination peut obtenir k , le contenu du message est protégé. Comme un mix ne peut pas savoir à quel position dans la chaîne de mixes il se situe, il n'est pas en mesure de déterminer si le nœud qui lui a transmis le message est, ou non, la source du message. De la même manière, un mix ne peut pas déterminer si le nœud suivant dans la chaîne est la destination ou un autre mix. Comme nous ne considérons pas de nœuds collaborant pour observer les communications et les partenaires, il est suffisant d'utiliser deux mix dans le chemin. Le choix de ces deux mix est illustré par la figure 1. Le premier mix peut être choisi parmi tous les membres de l'historique de connexion du nœud S. Toutefois, et comme explicité par la figure, il est nécessaire pour le choix du second mix, d'utiliser un P-nœud. En effet, il n'y a pas d'assurance que la couche *Nylon* aura ouvert une connexion de S vers B dans un passé récent : il faut donc que B soit directement joignable à partir du premier mix A. Notons qu'il est nécessaire pour la création du chemin que A connaisse les clés RSA publiques des mixes ainsi que de D. Les clés des nœuds de l'historique de connexion de S (par exemple, celle de A) sont simplement obtenues en les ajoutant aux échanges de vues *Nylon*. Celles de l'historique de D sont obtenues, comme l'historique de D lui-même, par le mécanisme d'échantillonnage privé.

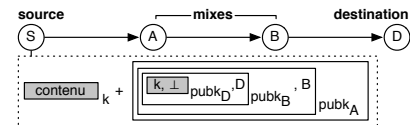


FIGURE 2: Chemin anonymisant en oignon.

3 Échantillonnage de pairs au sein d'un groupe confidentiel

Utilisant la construction de routes WCL décrite dans le précédent paragraphe, l'échantillonnage au sein d'un groupe privé permet à chaque nœud participant à un groupe privé d'obtenir un sous-ensemble des membres du groupe ainsi que les informations nécessaires et à jour pour établir une connexion vers ceux-ci. Ceci est assuré par un protocole d'échantillonnage standard [JVG⁺07], où les informations échangées sont : les pairs connus dans le groupe et le pair courant ainsi que les P-nœuds de leur historique de connexion nécessaire pour les contacter, et leurs clés publiques RSA. Notons qu'un mécanisme, non décrit dans ce document, permet d'assurer qu'il existe toujours un P-nœud dans l'historique de chaque nœud. Les nœuds du groupe privé sont ensuite utilisés de la même manière que ceux donné par le protocole d'échantillonnage global, néanmoins, une logique de session prévaut car les routes WCL doivent être maintenues tant que la connexion est susceptible d'être utilisée. WHISPER fait en sorte que ces connexions, ainsi que les ouvertures de NAT correspondantes, soient maintenues de manière transparente pour l'application.

La gestion de la légitimité de l'appartenance à un groupe est réalisée par l'utilisation de *passports*, signés par une clé privée de groupe. Celle-ci est conservée par les administrateurs du groupe. Par défaut l'ensemble des membres sont administrateurs et peuvent signer un nouveau membre. L'ajout au groupe se fait par un moyen externe (par ex., un site web, un courriel, etc.), qui renvoie l'adresse d'un administrateur

et une autorisation temporaire d'ajout. Une fois les pairs ajoutés, la gestion du va-et-vient (*churn*) dans le groupe ne nécessite pas d'autorité externe.

4 Résultats expérimentaux

Nous présentons ici quelques résultats de l'évaluation du prototype de WHISPER, écrit en C et en Lua, sur la plateforme mondiale PlanetLab (400 nœuds sur des machines séparées) et sur un cluster de 12 nœuds hébergeant 1000 instances. La figure 4 présente en haut la décomposition du temps d'aller retour pour un échange de 20 Ko entre deux nœuds de groupe privés. On observe que les délais de cryptage sont deux ordres de grandeurs plus faibles que les délais d'acheminement sur le réseau, et ce même en comptant les décryptages RSA sur les nœuds mixés. En bas, nous présentons le coût en bande passante selon le nombre de groupes pour chaque nœud, sur 400 nœuds sur PlanetLab et parmi 120 groupes. La proportion de P-nœuds est de 30%. Nous présentons la distribution de la bande passante (BP) utilisée avec un temps de cycle d'échantillonnage global de 10 secondes, et 1 minute pour les groupes privés, ce qui constitue une fréquence relativement élevée. La distribution pour chaque expérience est donnée par les différents quantiles : la médiane de la consommation moyenne par seconde est donnée par le ton de gris intermédiaire. La consommation de BP est linéaire en le nombre de groupes pour chaque nœud. On observe aussi que les P-nœuds, de part leur rôle privilégié, contribuent plus au protocole. Nos autres observations montrent que le temps CPU utilisé sur les P-nœuds est entre 2 et 3 fois celui utilisé sur les N-nœuds, et constitue dans le pire cas $\sim 1\%$ du temps de cycle d'échantillonnage. Nos autres expériences montrent aussi que la résistance au va-et-vient est élevée : un taux de remplacement de 10% du réseau chaque minute implique l'essai d'une nouveau chemin de communication dans 2.83% des cas, et il n'existe pas de chemin viable (avant le prochain échange) dans seulement 0.77% des cas.

5 Conclusion et références

Ce bref article a présenté les grands principes de WHISPER, un intergiciel permettant le support de communications confidentielles au sein d'un groupe dans un réseau à grande échelle, de manière totalement décentralisée. WHISPER utilise des chemins de communications fondés sur le principe de mixes de Chaum [Cha81], qui ont été notamment utilisés pour le système d'accès anonyme à Internet TOR [DMS04], qui repose sur une infrastructure dédiée. WHISPER propose une interface d'échantillonnage de pair permettant aux applications fondées sur ce mécanisme de gestion d'appartenance d'utiliser de façon transparente les garanties de confidentialité. Les évaluations du prototype en conditions réelles montrent sa propension à fournir des garanties fortes sur la confidentialité à un coût raisonnable.

Remerciements. Ces travaux sont en partie financés par le Fond National Suisse (200021-127271/1).

- [CF07] Martin Casado and Michael J. Freedman. Peering through the shroud : The effect of edge opacity on IP-based client identification. In *NSDI'07*, April 2007.
- [Cha81] David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2) :84–90, 1981.
- [DMS04] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor : The second-generation onion router. In *Security'04 : 13th USENIX Security Symposium*, aug 2004.
- [JVG⁺07] Márk Jelasity, Spyros Voulgaris, Rachid Guerraoui, Anne-Marie Kermarrec, and Maarten van Steen. Gossip-based peer sampling. *ACM Transactions on Computer Systems*, 25(3), aug 2007.
- [KPQS09] Anne-Marie Kermarrec, Alessio Pace, Vivien Quema, and Valerio Schiavoni. Nat-resilient gossip peer sampling. In *ICDCS'09*, 2009.
- [RBLP07] Étienne Rivière, Roberto Baldoni, Harry Li, and José Pereira. Compositional gossip : a conceptual architecture for designing gossip-based applications. *ACM SIGOPS Op. Sys. Rev.*, 2007.

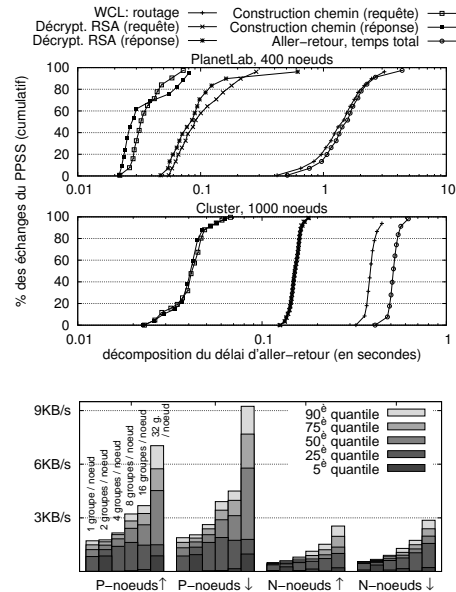


FIGURE 4: WHISPER : délais et bande passante.