Système de réputation préservant la vie privée

Paul Lajoie Mazenc

Système de réputation distribué préservant la vie privée

Paul Lajoie-Mazenc
EPC CIDER / EPC CIDre
Rennes, France
paul.lajoie-mazenc@irisa.fr

I. Introduction

Dans les grands réseaux, la grande majorité des interactions sont effectuées entre des inconnus, ce qui pose problème lorsque les membres du réseau placent dans ces interactions une certaine valeur, monétaire ou autre. Dans le cas du commerce électronique par exemple, un acheteur n'a aucune idée de l'état réel du bien vendu, qui peut être un produit d'occasion au lieu d'un produit neuf ou être plus abîmé qu'annoncé. Parallèlement, le vendeur ne peut pas être certain qu'il sera payé après avoir expédié le bien. De ce fait, l'acheteur et le vendeur aimeraient tous deux savoir avant de s'engager définitivement s'ils peuvent faire confiance à l'autre et si le risque qu'ils encourent est grand.

Pour répondre à ce problème, il est possible d'utiliser un système de réputation. Un système de réputation permet à ses utilisateurs d'estimer la réputation des autres utilisateurs afin de les aider à décider si oui ou non ils peuvent leur faire confiance et s'il est prudent de conclure une transaction. La réputation (ou *score de réputation*) d'un membre d'un réseau est généralement représentée par un objet mathématique (un nombre dans $\{-1, 0, 1\}$ dans le cas du système de commerce électronique de eBay ou une fonction bayesienne dans [1] par exemple) qui donne une représentation synthétique des différents avis ou *témoignages* des clients ayant déjà eu une interaction avec le fournisseur.

Resnick et al. [2] expliquent qu'un système de réputation doit au moins respecter les trois contraintes suivantes :

1) Les durées de vie des identifiants des utilisateurs et des objets doivent être assez longues pour leur permettre de se construire une réputation ;
2) Les informations sur les comportements des utilisateurs et les états des objets doivent pouvoir être collectées, agrégées et distribuées de façon à ce qu'elles soient visibles par tous les utilisateurs concernés ;
3) Ces informations doivent guider les actions futures des utilisateurs.

Dans ce travail, nous considérons le cas d'un réseau dans lequel des *fournisseurs de services* fournissent des services aux autres membres du réseaux que nous appelons les *clients*. Nous proposons un système de réputation permettant aux clients de décider s'ils peuvent en toute confiance interagir avec un fournisseur de service. Ce système de réputation est *distribué* afin qu'il n'existe pas de point unique de défaillance sur lequel un attaquant pourrait focaliser ses efforts. De plus, pour des raisons de vie privée notre proposition garantit l'*anonymat* des clients : il est impossible de lier l'identité d'un agent avec les interactions qu'il a eu avec différents fournisseurs de service ni avec les différents témoignages qu'il a pu émettre.

Dans la Section II, nous précisons la terminologie employée et définissons formellement les termes utilisés. La Section III fait un état des lieux concernant les systèmes de réputation préservant la vie privée. La Section IV présente le fonctionnement du système de réputation proposé. La section V décrit le protocole suivi lorsqu'un client désire interagir avec un fournisseur de service. Nous montrons dans la Section VI quelles attaques sont atténuées grâce à l'utilisation de ce protocole. La Section VII explique en quoi notre système respecte la vie privée des clients. Finalement, nous concluons dans la Section VIII et proposons les principaux travaux futurs.

II. Terminologie et définitions

Les fonctionnalités d'un système de réputation peuvent être classées en trois catégories : *la collecte de témoignages*, *le calcul du score de réputation*, *l'utilisation de ce score*.

Un *témoignage* est un ensemble de données permettant d'évaluer une transaction. Il comporte l'opinion d'un client à propos d'un fournisseur de service, fondé sur ses interactions passées avec lui et l'opinion du fournisseur de service sur les transactions auxquelles il a participé avec ce même client.

Afin de garantir leur anonymat, les clients agiront sous le couvert de pseudonymes. Les témoignages seront stockés sur des agents bien identifiés fournissant un service de *boîte aux lettres*. Nous préciserons ces deux notions en Section IV.

Définition 1 (Contenu d'un témoignage)**.** *Afin d'obtenir un score de réputation pertinent, le témoignage d'un agent utilisant un pseudonyme p sur un fournisseur de service FS doit porter plusieurs informations :*

- *la note donnée par p sur le comportement de FS ;*
- *la note donnée par FS sur le comportement de p ;*
- *une estampille pour rendre compte de la date à laquelle la transaction a lieu ;*
- *la valeur de la transaction pour accorder plus d'importance aux transactions importantes.*

Paul Lajoie-Mazenc est actuellement en stage de Master 2 dans les équipes INRIA conjointes CIDre/CIDER encadré par E. Anceaume, G.Guette, N.Prigent et V. Viet Triem Tong.

Les différents témoignages concernant un fournisseur de service FS sont agrégés par chaque nouveau client désirant se forger une opinion sur FS. Plus précisément, ces témoignages sont agrégés pour calculer un *score de réputation* dont la pertinence dépend à la fois de la quantité des témoignages collectés et de leur qualité. Un témoignage est dit *de qualité* si chacun des deux avis portés reflète les comportements des deux agents concernés.

Le comportement d'un agent (client ou fournisseur de service) se divise en deux parties : la conformité et l'honnêteté.

Définition 2 (Conformité)**.** *Un agent est dit* correct *s'il suit le protocole du système tout au long de l'interaction, et* incorrect *sinon.*

C'est une donnée objective et binaire : soit le protocole est suivi, soit il n'est pas suivi – un agent quittant le réseau au milieu d'une interaction est incorrect.

Définition 3 (Honnêteté)**.** *Un client est dit* honnête *si chaque témoignage qu'il émet reflète son jugement du comportement du fournisseur de service concerné. Un fournisseur de service est dit* honnête *si son comportement pour chaque transaction est tel qu'il l'aurait jugé bon si lui même avait été son propre client.*

L'honnêteté est une donnée subjective dont l'interprétation se rapproche de la notion juridique de *bonus pater familias* – « bon père de famille » –, qui représente la norme comportementale d'un individu mais n'est pas formellement définie. Plus globalement, on dira d'un agent qu'il est *bienveillant* s'il est à la fois honnête et correct, et *malveillant* dans le cas contraire.

Nous considérons ici que les attaquants sont des agents du système (clients, fournisseurs de service ou boîtes aux lettres). Un attaquant peut vouloir *médire* sur un autre agent en apportant des témoignages de mauvaise qualité, ou bien en sélectionnant ou augmentant le nombre des témoignages défavorables concernant cet autre agent. Ces attaques par *médisance* peuvent être amplifiées si l'attaquant peut se créer de nombreuses identitées. A l'inverse, l'attaquant peut aussi vouloir filtrer l'ensemble des témoignages le concernant pour augmenter la proportion de témoignages favorables et ainsi augmenter sa réputation. Ces attaques par filtrage peuvent être menées de deux manières différentes. L'attaquant peut effectuer une attaque dite *de l'homme au milieu*. Lorsqu'un client demande la réputation d'un fournisseur de service, l'attaquant intercepte la réponse de la boîte aux lettres et expurge les témoignages négatifs de la réponse avant de la faire suivre vers son destinataire naturel. L'impact est alors local, seul le client ayant demandé la réputation du fournisseur obtient une fausse information. L'attaquant peut aussi réussir à se faire désigner comme sa propre boîte aux lettres afin de ne stocker que les témoignages qui lui sont favorables. Dans ce cas, l'impact est global car les témoignages fournis par cette boîte aux lettres seront incomplets. Comme nous le verrons en Section V ces attaques sont mitigées par notre protocole. Par ailleurs, nous expliquerons pourquoi notre système de réputation protège la vie privée des clients.

Définition 4 (Protection de la vie privée des clients)**.** *La vie privée d'un client est préservée si les trois conditions suivantes sont satisfaites.*

- **pseudonymat** *un client est connu uniquement via des pseudonymes ;*
- **non-tracabilité des identités** *un client ne peut être relié à tout ou partie de ses pseudonymes ;*
- **non-tracabilité des pseudonymes** *deux pseudonymes ne peuvent pas être reliés.*

III. Etat de l'art

Carrara et Hogben [3] présentent de nombreux exemples d'utilisations de systèmes de réputation, en commençant par des systèmes de commerce électronique tels que eBay [4], un site web d'enchères électronique, PGP (Pretty Good Privacy), un logiciel de signature cryptographique permettant l'établissement de chaînes de signature de confiance, ou encore le réseau pair à pair Gnutella. Dans eBay, un vendeur propose un objet à la vente. Les acheteurs potentiels vont enchérir afin de remporter cet objet. Après chaque transaction, le vendeur et l'acheteur peuvent se noter l'un l'autre avec un retour positif, négatif ou neutre (c'est-à-dire $+1$, -1 ou 0) tout en laissant des commentaires associés à cette transaction. Une fois ces témoignages (notes et commentaires) envoyés à un serveur eBay, le score de chaque utilisateur est calculé en sommant tous les retours. Dans ce premier exemple, le score de réputation est la somme des notes obtenues. Celle-ci a pour but d'aider les acheteurs potentiels à se faire une idée du comportement passé du vendeur. Dans ce système, les témoignages des acheteurs et des vendeurs sont accessibles (lisibles) par l'autre partie une fois déposés sur le serveur. Carrara et Hogben affirment qu'il existe une forte corrélation entre les retours des acheteurs et du vendeur : un acheteur sera tenté de ne pas déposer de note ou commentaire négatif afin ne pas se voir lui même attribuer une note ou un commentaire négatif (et réciproquement).

Ce premier système de réputation est un système centralisé puisque toutes les évaluations sont stockées par les serveurs de eBay. Ce système est intéressant car il propose un *pseudonymat* des différents clients du système : une personne utilise un pseudonyme pour s'authentifier sur le système, et il n'est pas possible de relier les différents pseudonymes d'une même personne. Néanmoins, ce système permet de tracer les actions effectuées par un même pseudonyme : une recherche simple permet de connaître l'historique des achats et des ventes avec leurs évaluations. Par ailleurs, la gestion de ce *pseudonymat* n'est pas automatique puisque l'obtention de n pseudonymes passe par la création de n comptes Ebay. Ces différents pseudonymes auront alors des scores de réputation différents (un score étant relié à un pseudonyme) ce qui fausse la portée d'un score de réputation. Il serait souhaitable que toutes les évaluations d'une même personne soient prises en compte dans le calcul du score de réputation de tous ses différents pseudonymes et que l'historique d'un pseudonyme soit difficile à connaître.

Pour répondre à ce problème, Androulaki *et al.* [5] ont proposé une architecture de commerce électronique assurant

l'anonymat des clients et des vendeurs. Cette architecture est une fois encore centralisée car elle repose essentiellement sur un agent particulier : une banque connaissant l'identité de chacun des agents du système et leur attribuant des jetons. Ces jetons constituent la monnaie d'échange pour les transactions entre les vendeurs et les clients et représentent le score de réputation : plus un agent possède de jetons, meilleur est son score. Les agents (clients et vendeurs) discutent entre eux via des pseudonymes et n'utilisent leur identité réelle que pour communiquer avec la banque. Le contenu des transactions entre les agents et la banque étant protégé par des moyens cryptographiques (signature en aveugle et chiffrement asymétrique), l'anonymat des agents est garanti.

Nous proposons ici une architecture de commerce électronique permettant d'assurer l'anonymat des clients. Contrairement aux travaux présentés ci-dessus, notre architecture est entièrement distribuée. À notre connaissance, en dehors de cette proposition, il n'existe aucun système de réputation distribué préservant l'anonymat des agents.

IV. Fonctionnement du système de réputation

A. Organisation du réseau

Le système de réputation que nous proposons repose sur un réseau pair à pair structuré en anneau [6] qui permet aux clients de trouver rapidement les fournisseurs de service et leurs boîtes aux lettres (BaL) ainsi que de communiquer avec eux. Afin de garantir la disponibilité des témoignages, des grappes de boîtes aux lettres sont utilisées comme proposé initialement par Ravoaja *et al.* [7].

La figure 1 présente l'exemple d'un tel réseau où AD est l'autorité de démarrage responsable de l'insertion des nœuds dans le réseau et $FS_1 \dots FS_6$ sont six fournisseurs de service. La figure présente aussi les boîtes aux lettres ($BaL(FS_2, j)$ pour $j \in \{1, 2, 3\}$) de FS_2 organisées en grappes.

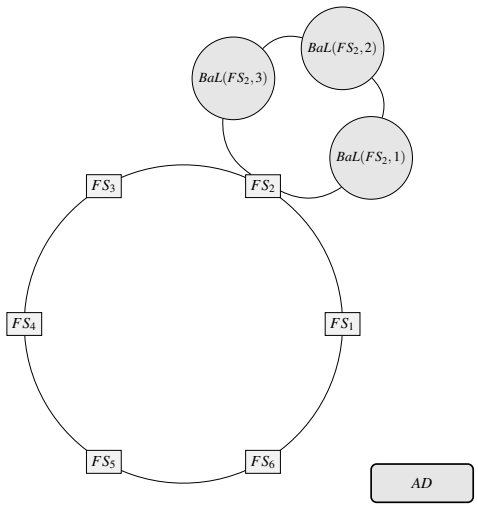

FIGURE 1: Forme générale du réseau : structure en anneau des agents et grappes de boîtes aux lettres

Comme expliqué à la Section II, notre système repose sur l'utilisation de boîtes aux lettres pour regrouper les témoignages concernant un même fournisseur de service. Les témoignages concernant le fournisseur de service FS sont stockés sur les boîtes aux lettres associées à FS.

Afin d'empêcher les attaques visant à augmenter artificiellement le nombre de témoignages (*bourrage d'urnes*), dès qu'une boîte aux lettres reçoit un nouveau témoignage concernant les deux mêmes participants (pseudonyme et fournisseur de service), l'ancien témoignage est remplacé. Ainsi, à tout instant, et pour chaque paire d'agents ayant interagi, une boîte aux lettres ne contient donc qu'une seule paire de témoignages entre ces agents.

B. Calcul des scores de réputation

Nous utilisons la méthode bayésienne décrite par Whitby et al. [1] reposant sur le système de beta-réputation proposé par Ismail et Jøsang [8] pour calculer la réputation d'un fournisseur. Cette méthode suppose que le comportement d'un agent suit une loi de probabilité bêta dont on ne connaît pas les paramètres. Sa fonction de calcul de score présente deux propriétés intéressantes. La première autorise des retours non-binaires alors que la seconde permet de « vieillir » les témoignages, c'est-à-dire de donner plus d'importance aux témoignages récents. Ces propriétés sont atteintes de la manière suivante : un témoignage n'est plus un retour positif ou négatif, mais est un vecteur : $\rho = \begin{bmatrix}\rho_+ & \rho_-\end{bmatrix},\ \rho_+, \rho_- \in [0,1] \mid \rho_+ + \rho_- = 1$, où ρ_+ représente la partie positive du témoignage et ρ_- sa partie négative. Le vieillissement d'un témoignage se fait en introduisant une « fonction de vieillissement » $f(t)$. Si t_ρ représente le temps écoulé depuis l'émission du témoignage ρ, positif – ou nul si le témoignage vient d'être émis –, le nouveau témoignage sera : $\rho_t = \rho \times f(t_\rho)$.

Enfin, lorsqu'un client A veut utiliser les services du réseau, il doit initier une communication avec l'autorité de démarrage et payer le coût d'inscription, que celui-ci soit monétaire ou calculatoire. L'autorité de démarrage fournit alors n pseudonymes permettant à A de rester anonyme et que nous notons $p(A, 1), \dots, p(A, n)$. Enfin, A prend place dans le réseau, sous la forme des n pseudonymes. Si jamais un agent désire obtenir plus de pseudonymes, il lui suffit de contacter à nouveau l'autorité de démarrage.

V. Protocole d'interaction

Dans cette section, nous détaillons le protocole permettant à un agent A possédant les pseudonymes $p(A, i),\ i \in I$ d'interagir avec un fournisseur de service FS, associé aux boîtes aux lettres $BaL(FS, j)$ pour $j \in J$ (cf. figure 2). Nous supposons que les boîtes aux lettres sont honnêtes.

Le protocole se découpe en trois parties. La première permet à A d'obtenir le score de réputation de FS. Notons que le protocole s'arrête dès la fin de la première partie si A n'est pas satisfait de la valeur du score de réputation de FS. La seconde partie du protocole établit la communication permettant la transaction entre A et FS. Enfin, la troisième partie décrit comment A et FS déposent leur témoignage sur les boîtes aux lettres.

Partie 1 : Calcul de la réputation de FS par un agent A. L'agent A utilisant le pseudonyme $p(A, i)$ choisit aléatoirement un ensemble J_m de m boîtes aux lettres du fournisseur de

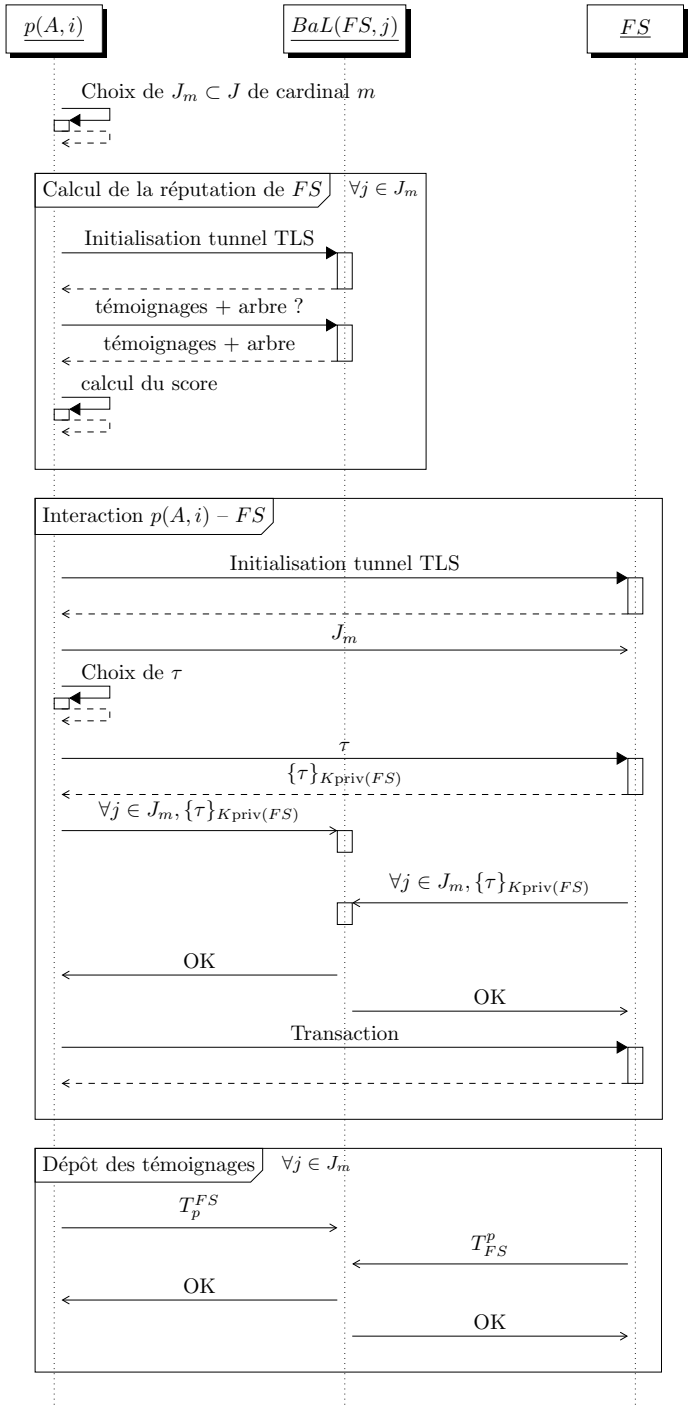

FIGURE 2: Interaction entre un utilisateur A sous le pseudonyme $p(A,i)$, un fournisseur de service FS et ses boîtes aux lettres $BaL(FS,j)$

service FS avec lesquelles il communiquera. Il réduit ainsi le nombre de messages envoyés en ne choisissant qu'une fraction des boîtes aux lettres disponibles. Si les boîtes aux lettres choisies se révèlent indisponibles alors l'agent peut en utiliser d'autres. Notons que dans la suite, on supposera qu'il existe parmi les m boites aux lettres un quorum de boîtes aux lettres disponible jusqu'à la fin de la transaction. Une fois ce choix effectué, A établit un tunnel TLS [9] avec chacune des boîtes aux lettres qu'il a choisi. Ces tunnels garantissent l'authentification des boîtes aux lettres, la confidentialité et l'intégrité des données échangées. Une fois ces tunnels disponibles, le client demande à chacune des boîtes aux lettres les témoignages correspondants au fournisseur de service FS. Les boites aux lettres fournissent tous les témoignages, dans la limite d'un par pseudonyme (le plus frais s'il y en avait plusieurs). Notons que A n'a besoin de connaître ni le pseudonyme ayant déposé le témoignage, ni l'identifiant de la transaction, ces informations sont donc purgées des témoignages par les boîtes aux lettres.

Une fois les témoignages expurgés récupérés, A agglomère les différentes notes et calcule le score de réputation de FS selon la méthode de calcul décrite précédemment. A choisit ensuite s'il désire ou non continuer l'interaction.

Partie 2 : Interaction entre FS et $p(A,i)$. Si A choisit d'interagir avec FS, il établit un tunnel TLS avec lui pour bénéficier comme précédemment d'un canal de communication sécurisé. Il l'informe ensuite des m boîtes aux lettres qu'il a choisi en lui envoyant J_m pour que les deux participants puissent communiquer avec ces mêmes boîtes aux lettres. $p(A,i)$ choisit un identifiant de transaction τ – par exemple en calculant une empreinte de $(p||FS||\text{timestamp})$ [1] où timestamp représente le moment auquel cet échange a lieu– et le transmet à FS qui lui renvoie le même identifiant, signé avec sa clé privée. $p(A,i)$ informe ensuite les m boîtes aux lettres de l'interaction en leur envoyant cette signature. FS fait de même de son côté. Les boîtes aux lettres en accusent réception dès qu'elles ont reçu les deux exemplaires. Cela permet d'assurer aux deux participants que l'autre s'est lui aussi engagé à poursuivre l'interaction.

S'ensuit la transaction entre le client sous le pseudonyme $p(A,i)$, et le fournisseur de service FS. Nous ne faisons aucune hypothèse sur la nature ou le déroulement de cette transaction.

Partie 3 : dépots des témoignages de FS et $p(A,i)$ sur les boîtes aux lettres de J_m Une fois la transaction terminée, les participants déposent leurs témoignages sur toutes les boîtes aux lettres de J_m en utilisant les tunnels de communication crées en première partie du protocole. Les boîtes aux lettres les informent quand les deux témoignages sont récupérés. Si après un certain temps T, les boîtes aux lettres n'ont reçu qu'un seul des deux témoignages, elles considèrent le témoignage manquant comme étant neutre vis à vis de la transaction. Si le témoignage manquant est celui du client alors elles le considèrent comme un avis positif à propos de FS. Si le témoignage manquant est celui de FS alors elle le considère comme un avis négatif à propos de la transaction. Après ce temps T les témoignages sont rendus disponibles à tous.

VI. Attaques atténuées

Avant toute interaction avec la boîte aux lettres (resp. le fournisseur de service), le client établit un tunnel TLS qui garantit l'authentification de la boîte aux lettres (resp. celle du fournisseur de service) et permet d'effectuer des échanges confidentiels et intègres. Ainsi, toute usurpation d'identité ou tentative de rejeu de messages par un attaquant potentiel est empêchée.

Une boîte aux lettres peut envoyer des témoignages obsolètes ou fallacieux. L'utilisation de grappes de boîtes aux lettres permet d'atténuer l'effet de ce type attaque. Intuitivement, si le nombre de boîtes aux lettres sélectionnées est suffisamment grand, le client peut détecter avec une forte probabilité les boîtes aux lettres malveillantes. Nous projetons de prouver cette propriété dans un travail futur.

Un des deux participants peut également essayer de réfuter une transaction afin d'augmenter son score ou de diminuer celui de l'autre. Si $p(A,i)$ interagit avec un fournisseur FS bienveillant mais ne veut pas augmenter la réputation de FS, il peut se déconnecter volontairement du réseau une fois la transaction effectuée mais avant d'avoir déposé son témoignage. La boîte aux lettres aura reçu son engagement sur la transaction – $\{\tau\}_{K\text{priv}(FS)}$ – et, après un certain temps T passé à l'attendre, la boîte aux lettres attribue d'elle-même un témoignage positif pour FS. Un client est ainsi incité à témoigner lorsqu'une transaction s'est mal déroulée. De même, si FS se déconnecte après s'être mal comporté sans émettre de témoignage, la boîte aux lettres attribue un témoignage négatif sur la transaction, incitant ainsi FS à témoigner. L'avantage de cette méthode est qu'elle pallie toutes les tentatives de réfutation. Par contre, les déconnexions (involontaires) du réseau sont également détectées comme des tentatives de réfutation.

VII. Respect de la vie privée

D'après la définition 4, la vie privée d'un client est préservée si trois conditions sont respectées : le pseudonymat, la non-traçabilité des identités et la non-traçabilité des pseudonymes.

Un client utilise son identité réelle uniquement lorsqu'il rejoint le réseau : en effet, il n'a pas encore de pseudonymes et communique avec l'autorité de démarrage afin d'en obtenir. Afin d'assurer l'authentification de cette autorité et une confidentialité des messages échangés, le client et l'autorité de démarrage peuvent également utiliser un tunnel TLS pour toutes leurs communications. Ainsi, seule l'autorité connaît les identités des agents. Nous supposons que cette entité est suffisamment protégée pour qu'on puisse formuler l'hypothèse de fiabilité de l'autorité de démarrage.

Hypothèse (Fiabilité de l'autorité de démarrage)**.** *Nous supposons que l'autorité de démarrage est fiable et que les liens identité-pseudonymes qu'elle stocke sont confidentiels.*

Cette même hypothèse nous permet de garantir que seule l'autorité de démarrage est à même de faire un lien entre une identité et des pseudonymes puisque pendant chaque interaction avec un fournisseur, un client utilise uniquement ses pseudonymes lors de ses communications avec un fournisseur de service ou une boîte aux lettres.

La propriété la plus intéressante est la non-traçabilité des pseudonymes. En effet, celle-ci garantit que l'on ne peut pas savoir si deux pseudonymes différents appartiennent à la même identité ou pas. Il existe de nombreuses attaques par inférence, où l'on s'intéresse à des comportements révélateurs. Un exemple significatif est celui présenté par Barbaro et Zeller [10] : en 2006, après le dévoilement par AOL de données de recherches des utilisateurs sur son moteur de recherche, certaines personnes furent retrouvées. Notamment, Thelma Arnold, grâce à quelques unes de ses recherches révélatrices : recherches généalogiques, de commerces de proximité, etc.

Nous supposons que de telles attaques peuvent être menées dans notre système de réputation, en comparant les différents éléments des témoignages : date et heure des transactions, valeur des transactions, portée des notes. Cependant, seules les boîtes aux lettres et les fournisseurs de service connaissent

1. || est l'opérateur de concaténation.

une partie de l'historique des pseudonymes. Une boîte aux lettres dispose de différents témoignages portés par un même pseudonyme sur le fournisseur de service avec lesquels le pseudonyme a interagit. Un fournisseur peut établir qu'un même pseudonyme a interagit plusieurs fois avec lui. Par contre, lorsqu'un client demande les témoignages concernant un fournisseur de service, il aura seulement les notes des différents client puisque les pseudonymes sont expurgés des témoignages rendus publics. Afin de pouvoir mener efficacement de telles attaques, il faut qu'un attaquant connaisse les historiques de nombreux fournisseurs – soit en formant une collusion à grande échelle, soit en inondant le réseau de boîtes aux lettres ou de fournisseurs de service sous son contrôle – afin de pouvoir comparer les différents paramètres. Pour l'instant nous formulons l'hypothèse que les conditions nécessaires à la mise en place d'une attaque par inférence visant à relier plusieurs pseudonymes rendent ces types d'attaques presque impossibles. Dans la suite de ce travail nous affinerons cette hypothèse en calculant les paramètres nécessaires permettant de résister à une telle attaque.

VIII. Conclusion et travail futur

Nous avons proposé dans cet article un système de réputation distribué respectant la vie privée des utilisateurs et robuste aux attaques. Sous l'hypothèse que l'autorité de démarrage n'est pas corrompue, notre système de réputation garantit le respect de la vie privée des clients, des applications construites au-dessus de notre système, en combinant à la fois des outils cryptographiques standards et la distribution des traitements sur un ensemble d'agents, appelés *boites aux lettres*.

Pour poursuivre ce travail, nous pensons tout d'abord formaliser la preuve que le protocole garantit l'anonymat des clients de l'architecture. Nous nous attacherons ensuite à montrer formellement que l'architecture proposée est résistante à d'autres attaques. Par exemple, nous montrerons qu'un client peut toujours obtenir un témoignage précis dès que le nombre de témoignages stockés est assez grand et que les témoignages de mauvaise qualité restent limités. Nous aimerions aussi mettre en évidence la possibilité d'obtenir un score de réputation pertinent tant que la proportion de boîtes aux lettres malicieuses est inférieure à une certaine borne.

Références

[1] Whitby, A., Jøsang, A., Indulska, J. : Filtering out unfair ratings in bayesian reputation systems. In : Proc. 7th Int. Workshop on Trust in Agent Societies. (2004)

[2] Resnick, P., Zeckhauser, R., Friedman, E., Kuwabara, K. : Reputation systems. Communications of the Association for Computing Machinery (CACM) **43**(12) (2000) 45–48

[3] Carrara, E., Hogben, G. : Reputation-based systems : a security analysis. ENISA Position Paper (2007)

[4] : eBay. http://www.ebay.com

[5] Androulaki, E., Choi, S., Bellovin, S., Malkin, T. : Reputation systems for anonymous networks. In : Privacy Enhancing Technologies, Springer (2008) 202–218

[6] Stoica, I., Morris, R., Karger, D., Kaashoek, M.F., Balakrishnan, H. : Chord : A scalable peer-to-peer lookup service for internet applications. In : Proceedings of the ACM SIGCOMM '01 Conference, San Diego, California (August 2001)

[7] Ravoaja, A., Anceaume, E. : Storm : A secure overlay for p2p reputation management. In : Proceedings of the International Conference on Self-Autonomous and Self-Organizing Systems (SASO). (2007)

[8] Jøsang, A., Ismail, R. : The beta reputation system. In : Proceedings of the 15th Bled Electronic Commerce Conference. (2002)

[9] Dierks, T., Rescorla, E. : The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard) (August 2008) Updated by RFCs 5746, 5878, 6176.

[10] Barbaro, M., Zeller, T. : A face is exposed for AOL searcher no. 4417749. The New York Times (2006)