Systèmes Multi-Agents Hippocratiques

Gestion de la sphère privée au sein des systèmes multi-agents

Ludivine Crépin[1,2,3], Laurent Vercouter[1], Yves Demazeau[2], François Jacquenet[3], Olivier Boissier[1]

[1] *Ecole Nationale Supérieure des Mines de Saint-Etienne - Centre G2I*
158 cours Fauriel - 42023 Saint-Étienne Cédex 2 – France
{ludivine.crepin, laurent.vercouter, olivier.boissier}@emse.fr

[2] *CNRS - Laboratoire d'Informatique de Grenoble*
46, avenue Félix Viallet - 38031 Grenoble Cédex – France
yves.demazeau@imag.fr

[3] *Université Jean Monnet - Laboratoire Hubert Curien*
18 rue Benoit Lauras - 42023 Saint-Etienne cedex 2 – France
francois.jacquenet@univ-st-etienne.fr

RÉSUMÉ. *L'évolution actuelle de l'informatique nous amène vers un traitement automatique des données privées (l'identité des utilisateurs du Web...) qui transitent dans les systèmes informatiques. Ces informations transitent souvent à l'insu des entités concernées ou sans leur consentement. Cet article présente un modèle de SMA, le HiMAS, qui gère la privacy grâce à un modèle de confiance.*

ABSTRACT. *The current computer science evolution leads to a more and more automatic private data (web user's idendity...) processing which transits in information processing systems. Those informations often spread out without the knowledge of the entities concerned nor their consent. This article presents a model of SMA, the HiMAS, which manages the privacy thanks to a trust model.*

MOTS-CLÉS : *Sphère privée, système multi-agents, confiance, confidentialité*

KEYWORDS: *Privacy, multi-agents system, trust, confidentiality*

1. Introduction

Les systèmes d'informations requièrent de plus en plus de données *sensibles* pour l'authentification ou encore l'accès aux ressources. Ces données circulent souvent à l'insu des entités concernées, sans que cette *sensibilité* soit prise en compte. Le Web étant décentralisé, nous proposons d'étudier ce problème à travers les systèmes multi-agents (SMA) qui possèdent la même caractéristique. Cet article expose les bases de notre modèle, les Systèmes Multi-Agents Hippocratiques, HiMAS.

Les informations dites *sensibles* sont généralement associées à l'existence d'un utilisateur. Par exemple, dans (Demazeau *et al.*, 2006), l'utilisateur transmet à un agent son emploi du temps et c'est à l'agent de garantir la protection de ces données. Certaines informations *sensibles* pour un agent ne se réfèrent pas forcément à celles d'un utilisateur. Par exemple, dans un système modélisant un jeu de stratégie, l'information *sensible* à protéger est la stratégie de l'équipe, information qui ne fait pas partie du domaine privé d'un utilisateur. Les HiMAS permetttent de considérer ces deux types d'informations dites *sensibles*.

Nous introduisons ici la notion de privacy dans les SMA. Cette notion n'ayant pas de définition communément acceptée (intimité, confidentialité, vie privée...), nous l'associons au concept de sphère privée.

2. Sphère privée

La sphère privée concerne toutes les informations qu'une entité désire protéger des autres. Le propriétaire des informations *sensibles* est l'entité concernée par ces informations. Cette sphère a comme particularité le fait d'être personnelle et personnalisable : l'entité concernée juge de ce qu'elle doit contenir et son contrôle est entièrement à sa charge. Elle est également contextuelle et sensible : elle change selon le contexte et ses éléments n'ont pas tous la même importance.

Au sein des SMA, cette sphère peut être attachée à différentes entités. En effet, il peut s'agir de celle de l'utilisateur, de celle d'un agent ou encore de celle d'un agent représentant la sphère privée d'un utilisateur. A l'heure actuelle, et pour plus de simplifications dans le cadre du modèle, nous ne faisons pas de distinction entre ces types de sphère : la sphère privée d'un agent représente ces trois types.

3. Approches informatiques

En informatique, certains moyens ont été mis en œuvre pour garantir une gestion de ces informations en fonction des souhaits des utilisateurs. Parmi eux le P3P notamment (W3C, 2002) permet aux utilisateurs de définir des contraintes sur leurs données personnelles et aux sites de définir leur politique envers ces données. Cependant, de nombreux problèmes subsitent encore comme le contrôle de la diffusion, de l'utilisation ou encore l'intégrité de ces données.

Certaines travaux, tels que les bases de données hippocratiques (Agrawal *et al.*, 2002), se sont intéressés à ces problèmes en proposant un nombre plus important de principes à respecter. Dix principes définissent une ligne directrice qui indique que l'utilisateur doit être au courant de tout ce qui concerne les données lui étant relatives. L'utilisateur doit également avoir accès aux données le concernant afin de connaître ce qui est encore présent, d'avoir la possibilité d'effectuer des mises à jour et d'en assurer l'exactitude. Pour finir, le système doit garantir la sécurité (au niveau du stockage et de la diffusion) ainsi que la conformité des données mais aussi de se limiter en terme de collection, diffusion, utilisation et rétention des données recueillies.

Les problématiques liées à la sphère privée dans les SMA concerne deux points : sa gestion par les agents et sa protection, toutes deux, à la fois par les agents et la société d'agents.

4. HiMAS, Système Multi-Agents Hippocratique

Un HiMAS introduit la sphère privée dans les SMA en adaptant aux SMA neuf des principes fondamentaux des bases de données hippocratiques. L'agent qui fournit la donnée doit être *consentant* et *connaître les objectifs* de cette récolte. L'agent qui récolte la donnée doit *demander le minimum en terme de collection de données, de diffusion, d'utilisation et de conservation de ces données*. De plus, ce dernier doit assurer la *conformité* et l'*ouverture* des données à l'agent ayant fourni les données. Le système doit assurer la *sécurité* au niveau des communications et de l'autonomie des agents.

Le principe des bases de données hippocratiques qui n'a pas été retenu pour les HiMAS est celui qui impose le respect de l'exactitude. En effet, un agent doit avoir la possibilité de mentir pour protéger sa sphère privée.

Les agents d'un HiMAS assurent la gestion de leur sphère privée en commençant par se la représenter. Une première sécurité apparaît du fait de l'autonomie des agents : aucune entité ne peut connaître ce que contient leur sphère privée si elle n'est pas communiquée. De plus, les agents étant des entités cognitives, ils doivent pouvoir raisonner sur leur interlocuteur et le contexte courant pour décider ou non de communiquer des informations relatives à leur sphère privée. Nous appelons transaction une telle communication.

Lors de la transaction, la première protection qui est appliquée concerne la sécurité : les agents doivent utiliser un canal sécurisé afin que l'information sensible ne soit pas interceptée. L'ajout d'une préférence et d'une politique à une transaction représente le consentement de l'agent qui fournit la donnée et l'engagement de celui qui la récolte. Cette définition d'un échange d'une donnée permet d'appliquer les principes de sécurité, de consentement, de la connaissance des objectifs, de la conformité et de la limitation de la collection.

Après une transaction, les HiMAS assurent les principes de limitation de l'utilisation, de la diffusion, de conservation et de récolte ainsi que celui d'ouverture. Les applications Web étant décentralisées, aucune vision globale ne peut être obtenue. Les agents sont des entités capables de communications, de jugement, en terme de confiance et réputation par exemple, et d'observations. Dans une société, les agents sont donc capables de collaborer afin de contrôler le respect des principes. Un tel contrôle est appelé contrôle social.

L'introduction du contrôle social et le jugement d'un agent par un autre nous amène à étudier les liens entre la confiance et la sphère privée en utilisant cette notion comme première barrière de protection.

5. Sphère privée & Confiance

La décentralisation empêche la mise en place d'un niveau de sécurité suffisant pour le respect de ces différentes règles. Dans ce contexte, la notion de confiance et de réputation jouent un rôle essentiel. En effet, lorsqu'un service ne garantit pas une parfaite sécurité, nous le jugeons en fonction de sa réputation afin de décider de l'utiliser ou non.

Mais, même si le système dans lequel se trouvent les agents présente une sécurité infaillible au niveau des transactions et de l'autonomie, rien ne garantit le comportement des agents, d'où l'intervention de la confiance qui permet un calcul des risques encourus envers la sphère privée.

Dans le cas du respect de la sphère privée, la confiance est étroitement liée aux mécanismes de détection de comportement mais aussi à la fonction de jugement d'un agent par un autre.

Remerciement : Ludivine Crépin est soutenue par une ADR Web Intelligence, financé par le cluster ISLE de la région Rhône-Alpes.

6. Bibliographie

Agrawal R., Kiernan J., Srikant R., Xu Y., « Hippocratic Databases. », *VLDB*, Morgan Kaufmann, p. 143-154, 2002.

Demazeau Y., Melaye D., Verrons M.-H., « A Decentralized Calendar System Featuring Sharing, Trusting and Negotiating. », *IEA/AIE*, p. 731-740, 2006.

W3C, « Plateform for Privacy Preferences, http ://www.w3.org/P3P/ », 2002.