Vers un modèle de confiance pour les objets communicants : une approche sociale
-DRAFT-

Véronique Legrand et Stéphane Ubéda
Centre d'Innovations en Télécommunications & Intégration de services
CITI INRIA ARES, INSA de Lyon, Bâtiment Léonard de Vinci
21 Avenue Jean Capelle, 69621 Villeurbanne Cedex

Joël Morêt-Bailly et Agnes Rabagny
Centre de Recherches Critiques sur le Droit
CERCRID UMR5137, Université Jean Monnet
6, rue basse des Rives, 42023 Saint-Etienne cedex 2

Laurent Guihéry
Laboratoire d'Economie des Transports
LET - ISH CNRS UMR6554, Université Lumière (Lyon II)
14 Av Berthelot, 69363 Lyon Cedex 7

Jean-Philippe Neuville
Centre de sociologie des organisations
CSO UMR7116, 19 Rue Amélie, 75007 Paris

1er mars 2004

Résumé

La question de la confiance s'est appliquée dans le monde des télécommunications avec des modèles reposant sur la connaissance *au préalable* des identités. Si aucune information n'est transmise au préalable, la confiance ne s'établit pas : elle n'est pas adaptative. C'est bien cette condition qui rend ces modèles contraignants et binaires, inadaptés aux *écosystèmes d'objets communicants*.

Actuellement, les objets autonomes sont sous le contrôle total de leur propriétaire. Pour établir une communication entre deux objets, la participation active des utilisateurs des deux objets est requise. Ce concept de *confiance* est extrêmmement primitif et ne permet pas l'explosion de l'usage des objets communicants.

La confiance, avant d'être un problème technique, est avant tout un problème social. En effet, les mécanismes techniques doivent être au service de la politique de sécurité imposé par l'usage et non le contraire ! Une politique trop restrictive n'offrira que très peu de possibilités d'interaction et donc rendra le système inopérant ; il en va de même d'une politique très permissive qui n'engendrera aucune confiance des utilisateurs dans le système, le rendant non pas inopérant, mais plutôt *inopéré* !

Nous avons proposé une architecture de confiance hybride, combinant des éléments classiques d'authentification et des éléments plus subjectifs nourris par les interactions de l'objet avec son environnement. Ces éléments subjectifs devront s'inspirer des modèles mis en place par les sociétés humaines pour gérer les interactions.

1 Introduction

On nous prédit depuis un certain temps déjà l'émergence d'un univers peuplé d'objets *intelligents* et dotés de capacités de communications. Mr Jawad Khaki, vice-président Windows Networking & Commu-

nications de Microsoft n'hésite pas à parler de *"devices ecosystems"*. Il est vrai que cette vision commence à devenir réalité, même si l'aspect intelligent reste limité à une découverte très sommaire de son environnement. Par contre, les technologies de communications prennent un essor tous à fait considérable et permettent maintenant d'envisager des *écosystèmes d'objets communicants*.

Actuellement nous assistons à une très forte accélération de l'impact des télécommunications dans la société. A l'heure où la convergence commence à prendre tout son sens autour de l'Internet Protocol (IP), les révolutions actuelles à l'œuvre ne reposent plus sur des innovations technologiques majeures, mais sur des usages dont on ne commence qu'à entrevoir les effets et sur lesquelles les acteurs classiques des technologies de l'information et de la communication n'ont que très peu de prise. Actuellement, nous assistons à une urbanisation des technologies d'accès haut débit à l'Internet combinée à l'explosion des communications sans fil. Si l'UMTS mettra probablement plus de temps à s'imposer que ce à quoi on pouvait s'attendre, les technologies de radiocommunication à courte et moyenne portée viennent compléter cet arsenal : explosion des Wireless Local Area Network grâce au WiFi, réalité des Personnal Area Network grâce au Bluetooth. Cet ensemble de technologies de radiocommunications doit permettre, dans un avenir proche, de voir un autre concept devenir réalité : l'*Internet ambiant*. Dans cette vision, l'accès à Internet sera disponible en tout lieu, aussi naturellement que l'on s'attend à trouver l'électricité dans toutes les pièces d'un bâtiment ou l'éclairage public dans toutes les zones habitées. L'Internet ambiant permettrait aux objets communicants de puiser des ressources et des services dans le réseau des réseaux. Les éléments d'une révolution sociale en matière de télécommunications sont donc réunis.

L'objet communicant n'en est encore qu'à ses débuts, se limitant actuellement à quelques niches, mais dont le nombre ne cesse de croître. Actuellement, ces objets communicants permettent des échanges de données avec d'autres objets, des ordinateurs personnels ou Internet, essentiellement dans les domaines de la gestion des agendas personnels (agenda proprement dit, mais également cartes de visite, fichiers d'adresses etc...), les documents multimédias (sons, images, vidéos). Mais on prendra très vite l'habitude d'échanger des horaires de transports, des informations sur le trafic automobile etc... On dépassera rapidement le stade de l'échange d'informations pour aller vers l'échange de *services* entre objets. Mais au-delà de la révolution technologique, il faut souligner celle des comportements. L'appréhension face à un objet doté de capacités de communication s'est fortement réduite et des scénarios d'usage tels que celui où un usager combine les services d'un téléphone cellulaire et d'un portable PC pour spontanément créer une extension de l'Internet pour l'offrir à ses proches via une connexion WiFi ou bluetooth, sans être courant, effraie de moins en moins.

Les réseaux de télécommunications de seconde génération ne sont pas les seuls à familiariser un nombre croissant d'usagers à un éventuel futur Internet ambiant. Les acteurs classiques de l'Internet ont été débordés par le concept du pair-à-pair et ils ne mesurent pas encore parfaitement l'impact que cette révolution a eu sur l'usager. Ces réseaux ont permis à un très grand nombre de renforcer leur rôle d'acteur de l'Internet en créant un espace d'échange sans aucune administration centralisée. Ceci a permis l'avènement d'un usage renforcé pour les objets communicants permettant le stockage et l'échange de documents multimédia. Des concepts tels que les formats de stockage de données, le stockage sur des supports multiples, l'archivage de documents ne sont plus l'apanage d'informaticiens chevronnés, mais apparaissent de plus en plus dans les usages de monsieur tout le monde.

La prochaine étape sera de doter ces systèmes autonomes que sont les objets communicants de la capacité à s'organiser de façon plus ou moins spontanée en pico-réseaux : c'est le concept de Personnal Area Network. Ces pico réseaux sont de moins en moins *personnal* puisqu'impliquant des équipements qui ne sont pas sous une autorité commune. Ces pico-réseaux établiront des relations, éventuellement spontanées, entre eux pour s'offrir mutuellement des ressources et des services : ils seront dotés d'une capacité de communication dite *ad hoc*, c'est à dire de la capacité à communiquer en mode pair-à-pair, éventuellement en se servant d'autres objets communicants comme intermédiaires et sans l'aide d'aucune infrastructure. En unifiant toutes ses visions, on peut imaginer un écosystème d'objets communicants s'appuyant sur un support

réseau hybride.

Bien évidemment, nos objets communicants actuels n'en sont pas encore rendus là et quiconque a bataillé un peu pour configurer deux équipements Bluetooth jugera aisément du chemin qu'il reste à parcourir. Toutefois, les réseaux ambiants, et leur support réseau hybride - c'est à dire combinant des capacités de communication multiples [1], constituent un champ d'investigation d'une extrême importance. Il est difficile de savoir si cette vision est réaliste ou non, optimiste ou pas, mais on peut être sûr d'une chose : elle ne verra le jour que si les problèmes liés à la sécurité sont traités efficacement.

Actuellement, les objets autonomes sont sous le contrôle total de leur propriétaire. Pour établir une communication entre deux objets, les techniques actuelles de sécurité nécessitent la participation active des utilisateurs des deux objets. Leur accord respectif est obtenu sous la forme d'une manipulation à réaliser sur chacun des objets. Ce concept ne permet pas l'explosion de l'usage des objets communicants. Les objections majeures que l'on peut opposer aux techniques actuelles sont doubles. En tout premier lieu, l'intervention systématique de l'usager restreint fortement les scénarios dans lesquels on autorise l'accès à l'objet dont on est le contrôleur ; on n'imagine pas arrêter son véhicule sur le bord d'une route pour taper les commandes permettant à son assistant de navigation d'échanger des informations avec celui d'un autre véhicule. On n'imagine toutefois pas non plus laisser complétement ouvert aux communications provenant de l'extérieur son système d'aide à la navigation, avec les risques de piratages, ou de virus qui pourraient apparaître ! L'opération permettant d'autoriser un accès s'effectue généralement sans aucune information permettant d'évaluer la confiance que l'on peut faire à une telle requête ; elle repose donc généralement sur un contact physique avec le propriétaire de l'objet pour laquelle est faite la requête. A ce manque d'information vient s'ajouter un autre problème majeur : l'absence de graduation dans la nature de l'échange (on laisse l'accès ou non) et la non répudiation de l'accord que l'on octroie. Les mécanismes d'établissement de la confiance actuellement déployés dans les réseaux fixes s'appliquent mal au concept d'objets communicants parce qu'ils nécessitent l'usage d'un tiers de confiance au moment de l'établissement de celle-ci.

L'objet de cet article est de discuter d'un modèle de sécurité proposé pour des écosystèmes d'objets communicants. Le modèle proposé n'a pas la prétention de correspondre à toutes les situations d'usage de tels environnements et pose encore plus de questions qu'il n'apporte de réponse. En effet, il aborde non pas un problème spécifique de la sécurisation de ces réseaux ambiants, mais propose une architecture globale de sécurité, dynamique et auto adaptable, permettant de gérer la mise en relation d'objets communicants. L'architecture que nous avons proposée dans [2] sera brièvement décrite à la section 3. Cette architecture repose sur la définition de la notion de *confiance* entre les objets désirant entrer en collaboration de façon spontanée. Cette notion peut correspondre à des concepts très différents suivant le contexte dans lequel on l'emploi. L'ambiguïté de cette notion devra doit être levée pour permettre la définition d'une instance opérationnelle de notre architecture. Il s'agit du thème de cet article. La section 2 décrit sommairement quelques exemples pris dans l'état de l'art des recherches sur cette notion d'établissement de la confiance. Notre article survolera les différents modèles sociaux de la confiance qui peuvent servir à la fois de base à l'implantation d'une instance de l'architecture de sécurité proposée, mais ouvrent également de nouvelles voies pour compléter le modèle initiale. La confiance, avant d'être un problème technique, est avant tout un problème social. En effet, dans un scénario d'usages, les mécanismes techniques doivent permettre de mettre en œuvre la politique de sécurité et d'établissement des interactions désirées par les communautés qui utilisent ces environnements. Une politique trop restrictive n'offrira que très peu de possibilités d'interaction et donc rendra le système inopérant ; il en va de même d'une politique très permissive qui n'engendrera aucune confiance des utilisateurs dans le système, le rendant non pas inopérant, mais plutôt *inopéré* ! La dernière section, sans donner de solution définitive, tirera quelques conclusions des éléments provenant des règles sociales d'établissement de la confiance qui peuvent être transposées dans notre architecture de sécurité pour réseaux ambiants.

2 Etat de l'art de la confiance dans les réseaux ad hoc

La question de la confiance s'est appliquée dans le monde des télécommunications avec des modèles reposant sur la connaissance *au préalable* des identités. Si aucune information n'est transmise au préalable, la confiance ne s'établit pas : elle n'est pas adaptative. C'est bien cette condition qui rend ces modèles contraignants et binaires, imposant que les objets communicants soient d'abord connus (identification) puis reconnaissables (authentification) tout au long de l'échange (maintien de la confiance). Si la connaissance préalable des identités est possible pour des réseaux maîtrisés, elle ne peut naturellement s'imposer à des réseaux dont les caractéristiques sont tout le contraire : topologie réseaux fortement dynamique, passage à l'échelle incontrôlé, population anonyme. Dans un tel environnement, comment valider une identité ? Cette question de l'identification et de l'authentification des objets communicants à forte mobilité est largement traitée par la recherche dans de nombreux travaux regroupés plus en détail dans [3].

Certaines approches [4, 5] proposent des architectures inspirées des infrastructures traditionnelles à clé publique, CA (Certificate Authority), établissant la confiance *au préalable*. Par l'emploi de la cryptographie à seuil, la clé privée, véritable clé de voûte d'une CA, est divisée en n parts, puis distribuée à t participants mobiles du réseau. Lors d'une demande de certificat par un nœud client, un des participants doit rassembler *à la volée* $t + 1$ parties de la clé privée, l'habilitant ainsi à signer le certificat. Le seuil de $t + 1$ garantit la robustesse du système. D'autres adaptations de protocoles ont été étudiées comme les protocoles de Key Agreement, efficaces traditionnellement pour définir un canal sûr *au préalable* entre deux objets [6]. Les versions modernes proposées vont admettre que le canal évolue graduellement de peu sûr à sûr [7] ; l'initialisation de l'échange se réalise avec un secret préalable peu sûr, connu publiquement, par exemple un mot diffusé par messagerie, puis au fur et à mesure les objets s'échangeront de nouvelles informations pour forger mutuellement un secret *fort* : lien mathématique unique entre ces deux objets. Ce concept introduit plusieurs notions fondamentales telles que l'établissement de la confiance sur le doute - l'échange s'initialise malgré tout - ou telle que l'adaptabilité du niveau de confiance par la divulgation progressive de secrets, visant au final une authentification forte. Le modèle ATN [8] appliquent ces notions et présentent un scénario de négociation de l'authentification où le secret graduel de chaque objet est une *lettre de change* constituée d'une chaîne de certificats multi-identité : ici un identifiant bancaire, là un identifiant d'un club de golf ; au moment de l'initialisation, chaque objet présente jusqu'à obtention d'un accord mutuel tout ou partie de sa lettre de change, en rapport avec la vie *sociale* des objets communicants ; le modèle prévoit ensuite un accès discrétionnaire aux ressources régi par la politique de sécurité de l'objet sollicité.

Les réseaux de pairs font appel à ces notions et nous conduisent aujourd'hui vers des modèles plus modernes, de plus en plus proche des modèles sociaux : le modèle de communauté. Tout d'abord, les travaux de [3] introduisent les protocoles de recommandation et de réputation propices à la propagation des informations de confiance. Les objets, responsables de leur propre confiance, émettent un jugement sur la *qualité* de leur police de confiance en maintenant des notes sur la réputation des autres objets du réseau. En appliquant ce modèle de recommandation aux réseaux ad hoc, [9] montre l'évolution des nœuds réseaux à l'image d'une communauté et complète le modèle par un système de répression et de publication des fautes.

Au-delà de ce concept fort de communauté, l'authentification reste un point extrêmement difficile notamment pour appréhender les mouvements des objets au sein de la communauté tels que leur départ, leur adhésion, leur retour ou leur faute. Pour traiter cet aspect, les travaux de [10] proposent un protocole de Key Agreement de groupe où le secret partagé est une clé secrète calculée sur l'identité des objets de la communauté. Dans ce modèle, chaque mouvement d'objet induit un nouveau calcul du secret imposant par conséquent d'appliquer ce modèle à l'échelle d'un réseau local ou domotique SOHO (Small Office or Home Office). En revanche, les travaux de [11] ne proposent pas une approche globale de groupe mais un modèle coopératif où chacun des objets véhicule ses propres informations d'authentification et d'identification. Chaque nœud joue le rôle d'une autorité de confiance, capable de construire sa base de certificats annotés

chacun d'indices de recommandations et de réputations comme dans PGP ou [6]. Un client présente son certificat que l'autorité de confiance de l'objet sollicité valide ou non ; la confiance est le résultat de l'évaluation de relations passées ou de recommandations, elle n'est plus requise au préalable.

En revanche, [12] traduisent leur vue du concept d'identification et d'authentification en une métaphore du lien unissant biologiquement un caneton et sa maman : une relation forte et hiérarchique. La maman, le maître décide tout de la vie de la relation : la naissance, la renaissance, la durée et la fin. Pour créer ce lien, les auteurs décrivent un nouveau concept, appelé *imprégnation* qui, par transmission physique des informations d'identification des deux objets, rendra la relation maître-esclave indélébile. La renaissance possèdera la propriété d'être spontanée sur la simple reconnaissance des informations d'identification.

La cryptographie vit en ce début de 21ème siècle une innovation importante par l'avènement de la cryptographie basée sur l'identité où il s'agit de créer un lien mathématique fort entre l'identité et le matériel cryptographique. [13] applique ce nouveau concept avec l'utilisation du protocole MobileIP qui en situation de mobilité ne garantit pas à un objet l'identité de son correspondant. L'idée est donc d'associer au couple clé privée-publique l'identité du groupe MultiCast IPv6 en l'occurrence l'adresse IP publique, lieu commun de chacun des objets communicants d'un même groupe. Pour ce, le nœud-contrôleur dérive la valeur de l'identifiant publique - l'adresse de MultiCast et d'Anycast IPv6 - en valeurs de clé privée-clé publique du groupe établissant ainsi le lien mathématique entre l'identité du groupe et les clés du groupe. Cette proposition suppose cependant la distribution du secret par canal sécurisé au sein du groupe.

Enfin les travaux de [14] augurent un concept original, détaché de la contrainte identité-identifiant pour introduire une nouvelle dimension, la monnaie virtuelle, efficace pour créer des relations entre les membres d' une communauté. Ce système monétaire, dont l'unité est le *nuglet*, régit l'achat et la vente des ressources réseau. Se posent alors les questions liées à la gestion globale et individuelle de cette monnaie.

Ce panorama des divers approches dresse non seulement les problématiques de confiance en réseaux ambiants mais surtout un tableau assez restreint des solutions proposées pour de tels réseaux. Il laisse en tout cas présager l'avènement de nouveaux modèles développés autour des concepts de communautés de plus en plus proches des modèles sociaux comme la réputation, le crédit, ou la recommandation.

3 Une architecture de sécurité pour les objets communicants

Nous avons proposé une architecture pour le support et la mise en œuvre de tels réseaux hybrides [15]. Cette architecture globale doit permettre à des objets communicants aux capacités de communication hybride d'évoluer et d'interagir entre eux et avec l'Internet. L'architecture ne se limite pas à un simple support *réseau*, mais offre également un ensemble de services élémentaires nécessaires à l'avènement des objets communicants autonomes. Parmi ces services, on peut citer l'auto configuration du terminal et la gestion des environnements multi interfaces[1]. Mais d'autres fonctions telles que la découverte de services, l'administration de terminaux, le déploiement dynamique de services sont également à l'étude.

Le service qui nous concerne dans cet article est le service de sécurité. Et nous devrions plutôt parler de *services de sécurité*, car il est difficilement envisageable que, dans un contexte aussi complexe, une solution unique de sécurité puisse satisfaire aux exigences de l'ensemble des situations. Comme pour les services *réseaux*, nous donnons à notre architecture de sécurité les caractéristiques d'auto configuration, d'auto organisation et d'auto adaptation permettant à des objets communicants autonomes de spontanément mettre en place une infrastructure de sécurité correspondant à une situation donnée. Par auto configuration nous entendons que l'intervention de l'usager devra être limitée aussi bien en ce qui concerne le nombre de sollicitations qu'en ce qui concerne la complexité des opérations qui lui sont demandées. Par auto organisation nous pensons à des systèmes où coexistent des objets appartements à des usagers différents, sans aucune autorité centrale de régulation, construisant de façon spontanée un réseau de communication de façon sécurisée. Enfin, par auto adaptable nous envisageons une architecture qui devra être capable de proposer un

niveau de sécurité adapté à l'enjeu de la communication et dont le niveau pourra évoluer dans le temps en fonction du contexte.

Bien entendu, une solution complètement opérationnelle respectant l'ensemble de ces critères n'existe pas encore. Notre architecture, décrite dans [2], respecte déjà une partie de ces contraintes et doit être encore améliorée. Lors de ce travail initial, il est très vite apparu que la notion de confiance constitue le levier incontournable à l'émergence d'une solution globale au problème de la sécurité dans des réseaux d'objets autonomes. En effet, il est admis que la construction d'une relation de confiance entre deux entités autonomes, en l'absence de tiers, est un enjeu très complexe. L'architecture de sécurité que nous proposons repose sur trois concepts. Le premier correspond à la notion d'**imprégnation**. Le deuxième est basé sur la notion d'**historique** du couple terminal/utilisateur. Et enfin, le troisième est basé sur l'**auto-organisation** de communauté d'objets communicants en fonction du contexte.

Imprégnation Ce concept fut décrit dans le cadre des objets communicants dans un article célèbre appelé "The resurrecting duckling: security issues for ad hoc wireless networks" [12]. L'imprégnation consiste à créer un couple objet/utilisateur qui ne pourra être rompu que par *reprogrammation* de l'objet lui même. L'imprégnation a plusieurs avantages parmi lesquels celui de lever les ambiguïtés du problème de l'authentification de l'objet et de l'utilisateur : laquelle réaliser en premier, quel contrôle donner à l'objet lui-même, à l'utilisateur, comment l'objet modifie-t-il les droits d'un utilisateur etc... La dissociation de ces deux concepts engendre de nombreux problèmes, des failles de sécurité et des paradoxes. Dans notre approche, nous parlerons du couple objet/utilisateur qui aura été scellé lors de l'opération d'imprégnation.

Dans notre modèle, la mise en œuvre de l'imprégnation nécessite trois éléments fonctionels. Outre l'objet lui-même, nous aurons une *station d'imprégnation*, c'est à dire un dispositif matériel permettant de réaliser l'opération et une clé d'identification de l'utlisateur, dispositif portatif contenant à la fois les données et des algorithmes permettant la mise ne œuvre du modèle. Actuellement, dans nos travaux, la station d'imprégnation est un PC disposant de toutes les interfaces de communication sans fil permettant d'entrer en contact avec des objets communicants. Cette station d'imprégnation dispose également d'une partie des éléments du modèle. La clé d'authentification est actuellement une clé USB équipée d'un processeur embarqué (type JAVA Card). Il est important de noter qu'elle ne dispose pas de technologie de communication sans fil, le contact physique étant nécessaire pour activer les différentes étapes de l'imprégnation. On notera également que dans notre modèle qu'aucune imprégnation n'est réalisable sans une clé d'authentification.

Un dernier élément optionel peut entrer en jeu lors de l'imprégnation. Il s'agit d'un serveur d'authentification classique permettant à la station d'imprégnation de compléter le profil de l'utilisateur déjà présent dans la clé d'authentification. Il s'agit là d'un serveur *classique*, mais dont les caractéritiques ne sont connues que dynamiquement au moment de l'imprégnation. Les serveurs peuvent implanter des modèles très différents et ne sont sous l'autorité d'aucune administration centrale.

L'opération d'imprégnation a pour objectif de configurer l'objet en fonction de son utilisateur et de déposer ce que nous appelons dans notre modèle un **germe de confiance**. Cet élément est central dans l'établissement de la confiance entre deux objets. Son usage est décrit au paragraphe suivant.

Historique Le couple terminal/utilisateur créé par l'imprégnation va nouer de très nombreuses relations, possédant toutes un niveau de confiance variable en fonction du contexte, des services invoqués et d'une manière générale de la dynamique du réseau. En quelque sorte, la naissance du couplage terminal/utilisateur lors de la phase intiale d'imprégnation est la première intéraction et c'est de loin la plus importante. C'est lors de cette phase qu'un historique minimal est inscrit dans l'objet, cet historique associant de manière étroite l'objet à son utilisteur. La mémoire de ces intéractions constitue une identité forte qui caractérise chacun des élements de notre système. Cet historique se modifie avec le temps en se renforçant lors de nouvelles intéractions ou diminuant lorsque des informations se périment. L'idée est que ce germe doit être *entretenu*

durant la vie du couple objet/utilisateur. Cet historique, associé à des algorithmes liés à la sécurisation des protocoles et à une politique de sécurité localement définie pour le couple objet/utilisateur, constitue ce que nous appelons le **germe de confiance**.

Lors de l'interaction spontanée de deux objets (on utilisera aussi bien le terme objet ou utilisateur pour faire référence au couple objet/utilisateur), les germes de confiance établiront de façon spontanée, en fonction le leur politique de sécruité individuelle, le niveau de confiance qu'ils accordent à cette relation. Sans entrer dans les détails, il s'agira essentiellement d'un échange incrémental d'éléments publics de l'histoirique permettant aux objets de construire leur historique commun. Cette construction ne se fondera que sur les éléments *publics* de ces historiques, les éléments privés permettant de certifier que ces historiques n'ont pas été usurpés. En fonction de la valeur que chacun des objets donne à cet historique commun, les objets négocieront un niveau de confiance qui, s'il est suffisant pour l'invocation du service, déclanchera celui-ci sans l'intervention de l'utilisateur. Notons au passage, que les deux objets peuvent générer une clé de session à partir des parties privées des historiques communs qui sont les seuls à pouvoir calculer (d'un point de vue purement opérationnel, cette opération peut être plus délicate que ce que le texte laisse supposer, mais ce n'est pas l'objet de cet article). Si le niveau de confiance n'est pas suffisant, une intervention des utilisateurs est nécessaire. Elle prendra la forme de l'utilisation de la clé d'un des utilisateurs qui devra être insérée dans l'objet pour lequel on veut autoriser une interaction. Dans cette opération, le principe d'un contact physique est obligatoire. Chaque interaction acceptée ou refusée peut venir nourrir l'historique.

Ambiances Enfin, la dernière notion que l'on utilisera est celle que nous appelons **ambiance**. Le principe général est simple : si un regroupement d'objets ayant des interactions deux à deux découvre suffisamment d'éléments dans l'historique commun (celui-ci peut être également bâti de façon volontaire par un groupe désirant des interactions de groupe), pour en construire un certain niveau de confiance, une ambiance peut être créée. Les objets participant à une ambiance utilisent pour un certain temps l'historique commun de l'ambiance et non plus le leur lors de l'interaction avec des terminaux appartenant ou non à l'ambiance. Les mécanismes de mise à jour de l'historique de l'ambiance peuvent être différents de ceux de la mise à jour d'un historique local. Il constitue également un domaine de recherche qui dépasse très largement le cadre de cet article.

Un modèle hybride de confiance Notons que l'historique de l'objet se nourrira également des interactions spontanées avec des points d'accès à des réseaux fixes ou à l'Internet. Lors d'interactions avec des éléments ayant accès à un réseau fixe, des mécanismes classiques de sécurité pourront être mis en œuvre, mais l'autorisation d'accès à un service par un élément de l'Internet sera un élément important de l'historique d'un terminal dont il pourra se servir plus tard lors d'une interaction avec un objet pour *donner crédit* à sa demande de service.

Notre architecture est basée sur une notion hybride. D'une part des éléments classiques d'authentification, obtenus lors de l'impregnation ou lors de l'interaction avec des services de l'Internet. D'autre part des éléments plus subjectifs correspondant aux interactions que l'objet a eu avec son environnement. Tout ceci doit être réalisé sans administration centrale.

Evidemment, la protection du mécanisme complet que l'on vient de décrire est loin d'être trivial et fait l'objet d'études. Mais ce qui nous intéresse ici dans cet article est plutôt comment construire l'historique d'un objet, quelles informations y placer, quels crédits accorder à une information. Enfin, comment la dynamique du système peut être garantie ? Toutes ces questions sont des préalables à l'élaboration d'une solution technique et ne sont pas des questions techniques. Il s'agit bel et bien de définir un modèle de confiance avant de proposer une solution technique. L'objetif des paragraphes suivants est de chercher dans les modèles mis en place par les sociétés humaines pour gérer les interactions, ce qui pourrait entrer dans un modèle, de confiance entre des écosystèmes d'objets autonomes désirant s'échanger des services.

4 Approche sociale de la confiance

4.1 La confiance et la société

La question de la confiance dans les échanges entre individus peut porter sur quatre aspects [16] :

1) les échangistes (X échange avec Y car X a confiance en Y et réciproquement),
2) les choses échangées (X a confiance dans la qualité de ce qu'il reçoit de Y et réciproquement, sinon il n'y a plus échange !),
3) les moyens de l'échange (X a confiance dans le procédés qui permet d'échanger avec Y et réciproquement),
4) les tiers-garants institutionnels (X échange avec Y car tout deux ont confiance dans les institutions censées garantir leurs échanges).

La sociologie ne se pose jamais la question des moyens. Elle élude volontiers la question de la qualité des choses échangées en *traitant* le problème de cette incertitude qualitative via les deux autres supports de confiance que sont la confiance institutionnelle (X et Y ne doutent pas de la qualité des choses qu'ils échangent car ils font confiance aux institutions qui régulent leurs échanges) et la confiance à autrui (X et Y ne doutent pas de la qualité des choses échangées parce qu'ils se font confiance mutuellement). Ces deux notions d'institution et d'inter-connaissance sont au cœur des analyses de l'échange en sciences sociales.

L'échange est un objet aussi central que traditionnel au sein des sciences sociales, notamment en économie où il est question d' *échange économique* pour analyser toute circulation de biens et services entre agents, ainsi qu'en sociologie et en anthropologie où le concept clé est celui d'*échange social*, concept qui recouvre l'ensemble des situations d'échange non-économique entre individus. Les sciences sociales ont pour tradition d'inscrire l'échange au sein de quatre institutions idéales-typiques :

1) la *famille*, ou encore le périmètre de la socialité primaire qui permet d'ajouter les amis, voire les voisins ;
2) l'*organisation*, qui comprend toute forme d'action collective coordonnée, depuis l'entreprise jusqu'à l'hôpital en passant par un club sportif ou un ministère ;
3) le *marché*, lieu réel ou virtuel de rencontre entre une offre et une demande de biens, services ou informations ;
4) le *réseau*, qui définit toute communauté d'individus unis par le partage d'une expérience (réseau d'anciens de...), d'un intérêt (réseau de développeurs de logiciels libres...), d'un attribut (réseau de détenteurs d'un QI supérieur à 150...), etc.

Ces quatre institutions se distinguent sur deux variables fortement discriminantes. En premier lieu, la *distance sociale* qui sépare deux individus qui échangent, cette distance sociale pouvant être forte dans le cas du marché et de l'organisation (d'où la nécessité du contrat - d'achat ou de salaire - pour produire l'échange entre inconnus) ou, au contraire, faible, comme souvent dans le cas de la famille et du réseau où l'inter-connaissance, la familiarité innée (les liens du sang de la famille) ou acquise (le partage dans le réseau), permettent l'échange sans contrat, entre des individus qui se sentent d'une façon ou d'une autre proches. En second lieu, le *degré de structuration* de l'institution, qui définit les degrés de liberté dont disposent les acteurs pour échanger (notamment choix du partenaire de l'échange et choix des choses échangées) ; ce degré peut être faible, comme dans le réseau et le marché où les individus ont toute latitude pour se choisir et échanger ce qu'ils veulent, ou fort comme dans la famille et l'organisation, institutions où l'échange est

davantage contraint par une hiérarchie et des règles. Au sein de chacune de ces quatre institutions, l'échange serait, en théorie, réglé par un mécanisme dominant :

1) l'échange dans la famille est principalement réglé par le *don*, sous-entendu qu'il n'y a pas de calcul, d'équivalence, de dette... ;
2) l'échange en organisation est principalement réglé par l' *autorité*, sous-entendue que c'est la hiérarchie, ses règles de subordination et les procédures qui régulent l'échange ;
3) l'échange dans le réseau est principalement réglé par la *confiance*, sous-entendu que c'est le fait de partager quelque chose qui permet à deux inconnus d'échanger ; et
4) l'échange sur le marché est principalement réglé par le *prix*, sous-entendu qu'il y aura transaction si et seulement si offreur et demandeur trouvent un prix d'équilibre.

Don, autorité, confiance et prix, associés respectivement à la famille, à l'organisation, au réseau et au marché, sont des mécanismes de régulation des échanges qui peuvent, du coup, être également discriminés selon les deux paramètres que sont la distance sociale et le degré de structuration, ce qui nous donne le tableau suivant :

		Distance sociale	
		Forte	**Faible**
Degré de structuration	**Fort**	Organisation/autorité	Famille/don
	Faible	Marché/prix	Réseau/confiance

On s'aperçoit dès lors que susciter des échanges de choses incertaines entre des inconnus (marché) n'est possible qu'en présence d'un prix. Dans un autre registre, on constate que l'échange en confiance est davantage approprié aux situations faiblement structurée et au sein desquelles les individus sont plutôt proches, non pas en raison de liens familiaux ou d'amitié, mais simplement du fait de partager quelque chose en commun (le réseau). En l'absence de prix des choses échangées, la condition pour faire échanger en confiance des individus soumis à peu - pas ? - de règles est celle de la pré-existence du partage d'une chose commune. Sinon, l'échange devra reposer sur davantage de règles de structuration des rapports sociaux et des relations inter-individuelles.

4.2 De la confiance dans la théorie économique

La question de la confiance a été globalement bien traitée par les sciences économiques, dans différents champs d'analyse (économie monétaire et rôle de la *confiance* dans la monnaie, économie de l'information et nouvelle micro-économie, théorie des jeux, économie des convention, institutionnalisme,...). L'économie des contrats et des conventions ont aussi contribué à l'analyse de la confiance, de même que la nouvelle sociologie économique [17]. Plus récemment des apports intéressants viennent de l'économie expérimentale et de la théorie des jeux où la confiance est traitée par un modèle de réputation. La réputation vise à canaliser spontanément l'opportunisme et contribuer à le réduire. Dans cette perspective, les relations de confiance entre les contractants sont réduites à une estimation des coûts / avantages concernant les actions à conduire pour maintenir une bonne réputation. On peut même aller plus loin en prétendant que le marché est auto-producteur de confiance. Cette thèse du marché comme *inducteur de confiance* suppose que ce cadre d'échange produit lui-même ses propres règles de loyauté profitables à toutes les parties [18, 19].

De manière synthétique, on peut dire que la confiance révèle un double intérêt pour les économistes :

– réduire l'incertitude (qui s'exerce sur la concurrence et sur l'évolution des marchés en réduisant les coûts de transactions)
– atténuer l'asymétrie d'information entre les individus, par exemple entre les fournisseurs et les clients.

Le point central des développements les plus récents sur ces questions s'intéresse à la question des asymétries informationnelles entre les agents. En situation d'information parfaite, la confiance s'établit de facto entre les agents car il y a une parfaite connaissance informationnelle d'autrui et de son environnement. Par contre, en situation d'information imparfaite, le problème de la confiance est central car les agents ont tendance à masquer leurs préférences et à dissimuler les risques inhérents à une transaction (l'exemple le plus évident concerne le marché des voitures d'occasion traité par Akerlof [20]). En général, ces travaux partent de l'impossibilité d'application pratique du modèle d'équilibre général et de l'écart de ce modèle avec la pratique et les expériences économiques : en effet, si l'on considère que les acteurs ne sont plus omniscients et que leur rationalité est imparfaite, l'information étant considérée comme asymétrique, alors l'efficacité de la régulation par le marché pure devient délicate, sous-optimale et voire *incomplète*. C'est souvent en partant de l'analyse du don que les travaux débouchent sur les questions de confiance [20].

La question de confiance a été aussi particulièrement étudiée par les néo-institutionnalistes qui considèrent que la confiance constitue un élément central de réduction des coûts de transaction entre les agents (cf. O. Williamson) : pour lui, la confiance ne s'oppose pas au calcul rationnel de l'intérêt, elle en découle. Du côté de l'Ecole des Conventions, la confiance est perçue comme réductrice d'incertitude et s'exprime dans des règles, des conventions et permettent de fixer un ordre social stable. Pour certains économistes, la confiance ne peut se comprendre uniquement par le seul jeu des intérêts et par la relation marchande. Ces auteurs soulignent que la confiance et les conventions sont en fin de compte des solutions efficaces de nombreux problèmes économiques, notamment face à l'incomplétude des marchés. Chez Coase (1937), initiateur du courant de la Nouvelle Economie Institutionnelle, la confiance se place au delà du débat marché / intégration, car elle pose la question du mode de coordination des transactions le plus efficace. Certaines transactions sont en effet retirées du marché et retirées de la régulation par les prix pour être organisées dans la firme et soumises au principe coordinateur de l'autorité afin d'économiser sur les coûts de transaction. Comme on peut l'entrevoir dans ce texte trop succinct et réducteur, les économistes ont bien analysé le concept de confiance qu'il place au centre des mécanisme de marché et de réductions des incertitudes, des asymétries d'information et des coûts de transaction.

4.3 Droit, confiance et prévisibilité ou comment le droit peut-il instaurer la confiance ?

Weber et l'*expectation raisonnable* des actions Pour le sociologue, juriste et économiste Max Weber [21], le droit moderne, organisé dans le cadre de l'Etat et dont l'application est garantie par lui, permet aux acteurs une *expectation raisonnable* des actions des autres. En effet, un acteur peut raisonnablement anticipé la prise en compte de la règle de droit par un autre, du fait que si ce dernier ne la respecte pas, le premier peut avoir recours aux institutions étatiques (notamment les tribunaux) pour la faire appliquer. Notamment, un acteur peut raisonnablement penser que son cocontractant va respecter les règles en vigueur, puisqu'il est de son intérêt, à court ou moyen terme, de le faire (à peine d'application de la règle par les tribunaux, de mauvaise publicité, de frais supplémentaires etc.). Evidemment, si l'intérêt du cocontractant est autre (par exemple, son attitude lui permet de ruiner son concurrent qui ne pourra dorénavant plus agir contre lui), il pourra adopter une attitude différente. Dans ce modèle, la confiance ne renvoie pas à une qualité que l'on reconnaît à autrui, mais à une prévisibilité de son comportement, du fait du contexte institutionnel dans lequel se déroule l'activité. En résumé, dans le droit moderne, ce qui fait la confiance, c'est l'Etat.

Confiance et sanction Si l'on se place dans un autre contexte *juridique* ou de *régulation*, c'est-à-dire dans une société sans autorité publique pour faire respecter le droit, un élément inhérent à toute régulation perdure : la sanction, contrainte sociale chez les sociologues, contrainte juridique chez les juristes. C'est ici se placer dans la situation suivante : que se passe-t-il si on trahit la confiance ? C'est justement dans ce contexte que le terme confiance est utilisé actuellement en droit pénal français dans le cadre de l'infraction

d'*abus de confiance*. Celle-ci prévoit la répression du *"détournement ou de la dissipation d'une chose remise dans le cadre d'un contrat"*. On constate que le droit prévoit ici une action a posteriori. Le fait que l'on veut éviter est avéré : on sanctionne. Ce système intègre, en outre, la dimension suivante : on espère que le citoyen tenté par la commission de l'infraction saura s'abstenir du fait des sanctions qui le frapperont s'il passe à l'acte.

Confiance et déontologie Un autre mode de régulation, qui a à voir avec la confiance est à l'oeuvre dans le cadre de la régulation déontologique [22]. Il s'agit, ici, dans une situation de déséquilibre de compétence - donc de pouvoir - entre deux acteurs, typiquement un client et un médecin ou un avocat, de ne pas seulement donner des droits au client, puisque celui-ci aura beaucoup de mal à les mettre en oeuvre du fait de son incompétence, mais de faire peser des devoirs sur la tête de celui qui se trouve en situation de pouvoir : le professionnel. Dans cette perspective, la relation entre les médecins et le patient est notamment théorisée, par les professionnels intéressés à, comme la rencontre entre une confiance et une conscience.

5 Analyse et conclusion

Notre approche était double : travailler sur l'historique et amender le modèle. Le germe de confiance travaille à partir de l'historique du couple objet/utilisateur. Il est bien évidemment difficilement envisageable de stocker l'ensemble de toutes les interactions entre objets. Alors lesquelles stocker ? Quelles valeurs donner à un élément ? Comment hiérarchiser les informations ? Concernant le modèle lui même, nous nous posons des questions sur sa pertinence ? A quels scénarii d'usages cette architecture de sécurité s'adapte-t-elle ?

On peut, en outre, se demander ce que l'on transpose des modèles sociaux d'établissement de la confiance dans le domaine des télécommunications et des sevices qui y sont associés. Si l'on reprend le tableau donné à la section 4.1, on peut facilement considérer que la majorité des architectures de sécurité dans le monde des réseaux sont de la forme *degré structure* **Fort** et *distance sociale* **Forte**. En effet, ils sont organisés autour d'un système d'administration de réseau dont les acteurs appartiennent à une organisation hiérarchique qui gère différentes classes d'utilisateur parfaitement identifiées. C'est bien évidemment le cas dans les réseaux d'opérateurs et même le cas dans l'Internet actuel, même si le degré de structuration est légèrement plus faible. Dans tous les cas, la régulation est faite dans le cadre d'un système fondé sur l'autorité.

Si l'on se réfère à présent aux services particuliers de l'Internet dans le cadre du E-commerce, on relâche fortement la structure. Les acteurs se multiplient, mais leur distance sociale reste forte. La régulation des échanges dans ce type de système est imposée par le prix de services. Il s'agit d'un système économique classique.

Les systèmes pair-à-pair a contrario entrainent un niveau de proximité des acteurs beaucoup plus important. Les liens qu'ils tissent spontanément proviennent de centres d'intérêts communs (de l'échange de données multimédia à la lutte contre la mondialisation) qui correspondent à une organisation en *réseau*. La régulation des échanges se fait par une confiance naturelle en les acteurs du réseau. La sécurité des réseaux pair-à-pair est encore empirique et les études sont encore à mener.

Enfin, il est très dificile de faire entrer un système technologique d'échange basé sur la notion de *famille* (au sens large, puisqu'on y inclut les amis, les connaissances proches au sens physique) dont la régulation est basée sur un système de *don*. Dans les systèmes pair-à-pair, si l'on exclut un comportement de type *militantisme* qui reste marginal, nous ne sommes pas en présence d'un système de don, la motivation implicite des participants étant que le réseau offrira en retour des données aussi intéressantes que celles qui lui sont offertes.

Si l'on cherche à savoir à quel modèle appartient notre architecture de sécurité, on peut la voir comme *degré structure* **Faible** et *distance sociale* **Faible**, comme les systèmes pair-à-pair. Cependant, les interactions entre objets communicants impliquant une proximité physique, notre architecture remplit une partie

des conditions de la classe *degré structure* **Fort** et *distance sociale* **Faible**. La distance sociale s'affaiblit puisqu'une mise en présence physique répétée est nécessaire pour faire naître des interactions et donc générer un niveau de confiance important. Cependant, deux couples objets/utilisateurs n'ayant aucune rencontre physique dans le passé peuvent très bien générer spontanément une interaction d'un très haut niveau de confiance, simplement parce que leur historique commun correspond à un comportement similaire (même banque, même habitude de E-commerce, même club, même entreprise etc...). Si l'on aborde maintenant le système de régulation des échanges, il est difficile de penser qu'il tient de don pur, puisque la motivation d'offrir des services à des inconnus est clairement d'attendre le même comportement dans le futur des acteurs du système. Cependant, a contrario du système pair-à-pair, un utilisateur n'a pas accès à l'ensemble du système et les relations sont beaucoup plus individualisées. Le système peut être vu simplement comme un moyen de limiter le risque lors d'un échange et non de susciter des échanges.

Pour susciter des échanges, tout en posant la gestion de la confiance comme base de la sécurité, il est nécessaire de doter notre architecture d'éléments susceptibles d'encourager les échanges. La création de monnaie électronique au sein du système pourrait être envisageable [14] mais serait un frein important au modèle et ajouterait beaucoup de problèmes de sécurité supplémentaires (comment gérer une transaction en l'absence de tiers, comment éviter la fausse monnaie etc...). La seule autre motivation que l'on peut trouver tient au fait que si l'on rend des *services* aux gens de la communauté, on peut espérer que la communauté fera de même pour nous. Mais à la différence des systèmes pair-à-pair, l'offre de service consomme des ressources et nécessite d'augmenter son degré d'exposition. Partant de ce principe, la mise en relation de deux entités présuppose une confiance qui ne peut être garantie par un tiers.

On pense naturellement à la mise en place d'un modèle de **réputation**. Notre architetcure permet un mode très dégradé de la notion de réputation : si un objet réussit très régulièrement des interactions avec le même objet, sa réputation peut devenir plus importante et donc autoriser des accès à des services plus évolués. Dans un tel système, la notion de réputation est limitée à des interactions deux à deux et n'aura que très peu d'impact sur le système. Pour augmenter la portée d'un tel système, il est nécessaire d'introduire un système de **recommandation**. La réputation locale pour une entité peut donc être transmise, l'acceptation d'une recommandation étant assujettie également au degré de confiance que l'on accorde à l'entité qui propose cette recommandation. Ce système est compatible avec notre modèle, ajoutant seulement au **germe de confiance** les moyens techniques de gérer cela. On augmente ainsi l'impact de la notion de réputation, sans atteindre le niveau existant dans les interactions économiques classiques où la réputation est visible de tous. Pour atteindre un tel niveau, il faudrait rendre cette notion de réputation publique, comme cela se fait sur certains sites de ventes aux enchères. Cependant, notre modèle excluant toute administration centralisée, comment publier la réputation, qui garantit la validité de celle-ci et surtout comment y accéder lors d'une interaction locale ? Une autre solution serait que chaque couple objet/utilisateur *publie* sa réputation spontanément dans son environnement sous réserve que l'intégrité de ces informations de réputations soit garantie. Cette solution serait idéale mais reste très difficilement réalisable et engendre de nouvelles informations à protéger.

On peut imaginer contourner le problème via la création de groupes d'utilisateurs. Comme nous l'apprend le droit, tout système juridique repose sur la notion de sanction. En effet, la prédictibilité de comportement d'une entité face au risque encouru lors du non respect des règles communes nécessite un organisme central pour ériger ces règles et une *police* pour les faire respecter. Nous n'aborderons pas les problèmes de responsabilité des personnes dans l'usage d'objets qui ne déroge en rien aux règles de droit classique : si votre action est répréhensible aux yeux de la loi, l'usage d'une technologie particulière ne change pas cet état de fait, mais peut simplement complexifier la constitution de la preuve de l'acte reprochable. Par contre, il serait nécessaire de posséder un système de sanction pour des actes non répréhensibles aux yeux de la loi, mais contraires à la philosophie même du système. On a déjà proposé le mécanisme de réputation, un comportement contraire aux règles entrainant la diminution de la réputation de l'entité. Mais comme on l'a

vu, l'absence de centralisation de l'information de réputation rend la sanction peut efficace.

En l'absence d'organisation de type *étatique*, c'est aux acteurs de s'autoréguler. L'un des mécanismes qui peut être transposé dans notre architetcure est le modèle à base de *déontologie*. On peut, en effet, imaginer qu'un groupe suffisamment important se constitue en *association* (sens référence à un quelconque statut adminsitratif) qui se dote de règles de comportement et d'un mécanisme de sanction en cas de non respect des règles : une déontologie. Ce groupe créérait ainsi un *"label"* qui pourrait être présenté sous forme électronique lors d'un échange (c'est donc un élément de l'historique) et qui permettrait de renforcer la confiance que l'on peut avoir dans l'interaction. Les entités du système qui font confiance à ce label doivent préalablement charger un programme permettant de vérifier la validé du label lors d'une interaction. Au moment d'une interaction, les entités n'ont aucun moyen technique permettant de vérifier que l'entité paire à laquelle on s'adresse respecte bien le code de déontologie associé au label, mais il sera possible, en cas de violation du code, de porter à la connaissance de l'association ce manquement aux règles, association pouvant prendre des décisions disciplinaires comme l'exclusion temporaire ou défintive [23]. Les membres d'une telle association doivent trouver un intérêt important à rester au sein de cette communauté, parce que ce label leur garantit la collaboration des entités qu'ils vont croiser et permet ainsi que les interactions aient lieu avec de hauts degrés de confiance. Un tel mécanisme est difficile a mettre en œuvre, mais entre dans le modèle de sécurité hybride tel que le suppose notre architecture.

Enfin, il existe un dernier système qui, en absence d'autorité au moment de l'échange, peut être mise en place : la **délégation d'autorité**. Certains objets peuvent recevoir une délégation d'autorité d'un organisme pour une certaine durée et pour un certain type de service. Par exemple, on peut imaginer que lors d'un salon commercial, des agents travaillant pour des banques embarquent une délégation d'autorité dans leur terminaux, pour garantir certaines transactions financières. Dans le cadre de la circulation automobile, on peut imaginer que le système d'aide à la navigation d'un véhicule puisse recevoir une délégation d'autorité lui permettant de contrôler les feux de circulation ou de demander la priorité pendant son déplacement. Un tel mécanisme serait également difficile a mettre en œuvre, le système devant en plus garantir que cette délégation d'autorité soit réellement applicable.

Références

[1] G. Chelius and E. Fleury, "Ananas: A new adhoc network architectural scheme," INRIA Research Report 4354, 2002.

[2] V. Legrand, D. Hooshmand, and S. Ubéda, "Trusted ambient community for self-securing hybrid networks," INRIA, Research Report 5027, 2003.

[3] V. Legrand, F. Nait-Abdesselam, and S. Ubéda, "Etablissement de la confiance et réseaux adhoc: un état de l'art," in *2eme rencontre francophone sur Sécurité et Architecture Réseaux*, Nancy, France, 2003.

[4] L. Zhou and Z. Haas, "Securing ad hoc networks," *IEEE Network*, pp. 24–30, 1999.

[5] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for mobile ad-hoc networks," in *International Conference on Network Protocols (ICNP)*, 2001, pp. 251–260.

[6] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, no. 22, pp. 644–654, 1976.

[7] N. Asokan and P. Ginzboorg, "Key-agreement in ad-hoc networks," *Computer Communications*, vol. 18, no. 23, pp. 1627–1637, 2000.

[8] W. Winsborough and N. Li, "Towards practical automated trust negotiation," in *IEEE 3rd Intl. Workshop on Policies for Distributed Systems and Networks*, 2002, pp. 88–102.

[9] A. Weimerskirch and G. Thonet, “A distributed light-weight authentication model for ad-hoc networks,” Electrical Eng. & Information Sciences Dept., Ruhr-Universität Bochum, Germany, Accenture Technology Labs, Sophia Antipolis, France,” Research report, 2001.

[10] N. Prigent, J.-P. Andreaux, C. Bidan, and O. Heen, “Secure long term communities in ad hoc networks,” in *1st ACM workshop on Security in Ad hoc and Sensor Networks (SASN)*, 2003.

[11] J.-P. Hubaux, T. Gross, J.-Y. Le Boudec, and M. Vetterly, “Towards self-organized mobile ad hoc networks : the terminode project,” *IEEE Communications Magazine - Special Issue on Telecomuunications Networking at the Start of the 21st Century*, January 2001.

[12] F. Stajano and R. Anderson, “The resurrecting duckling: Security issues for ad-hoc wireless networks,” in *7th International Workshop on Security Protocols*, L. Springer-Verlag, Ed., April 1999, pp. 172–194.

[13] C. Castelluccia and G. Montenegro, “Securing group management in ipv6 with cryptographically based addresses,” Institut National de Recherche en Informatique et en Automatique,” Research report, 2002.

[14] L. Buttyan and J.-P. Hubaux, “Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks,” Swiss Federal Institute of Technology - Lausanne, Department of Communication Systems,” Research Report, 2001.

[15] Projet commun INRIA Rhône-Alpes et INSA-Lyon, “Projet ares : Architectures de REseaux de Services,” http://www.inria.fr/recherche/equipes/ares.fr.html.

[16] J.-P. Neuville, “Le contrat de confiance : étude des mécanismes de coopération dans le partenariat industriel autour de deux grands constructeurs automobiles européens.” Ph.D. dissertation, IEP de Paris (sous la direction de E. Friedberg), 1996.

[17] ——, “La stratégie de la confiance. le partenariat observé depuis le fournisseur,” *Sociologie du travail*, no. 3, pp. 297–319, 1997.

[18] B. Baudry, “Incertitude et confiance : une réflexion sur les logiques de coordination dans la relation d’emploi,” *La confiance, approches économiques et sociologiques*, no. 22, pp. 237–261, 1999.

[19] ——, “De la confiance dans la relation d’emploi ou de sous-traitance,” *Sociologie du Travail*, vol. 26, no. 1, pp. 43–61, 1994.

[20] G. Akerlof, “The markets for lemon,” *Quarterly Journal of Economics*, no. 336, pp. 488–500, 1970.

[21] M. Weber, *Sociologie du droit*. Presses Universitaires de France, 1986.

[22] J. Moret-Bailly, *Les déontologies*. Presses universitaires d’Aix-Marseille, 2001.

[23] ——, *Les institutions disciplinaires*. Mission de recherche Droit et Justice - Collection Arrêt sur recherches, 2003.