Identification pour les réseaux spontanés[1]

V. Legrand, S Galice, S. Ubéda
Laboratoire CITI – INRIA ARES
21 Avenue Jean Capelle F-69621 Villeurbanne
{veronique.legrand,samuel.galice, stephane.ubeda}@insa-lyon.fr

J-P. Neuville
Institut d'Études Politiques de Paris
CSO Centre de sociologie des organisations
UMR7116,
19 Rue Amélie, 75007 Paris

Résumé – – Dans un futur proche, à la mobilité toujours croissante des mobiles viendra s'ajouter la spontanéité de la création de réseaux Ils devront être capables d'interconnecter des mobiles, à la volée et de bout en bout, mais leur succès dépendra grandement de la confiance qu'ils apporteront à leurs usagers. Les modèles de confiance électroniques traditionnels ne répondent pas aux nouvelles exigences de tels réseaux dont les caractéristiques les rapprochent de plus en plus des modèles sociaux. Notre approche consiste à étudier les modèles de confiance sociaux pour en concevoir des modèles de confiance électroniques. L'identification, clé de voûte d'un modèle de confiance, reste un problème difficile. Dans cet article, nous proposons un état de l'art opposant modèles de confiance électroniques et sociaux, puis notre formalisme de l'identification et la proposition d'un modèle d'identification adapté aux réseaux dynamiques et correspondant aux modèles sociaux de type famille et réseau.

Mots-clés: Modèle de confiance, approche sociale, protocole de distribution de clé, clé cryptographique.

1. Introduction

Les réseaux spontanés annoncent les réseaux de communication du futur où la mobilité en est l'idée maîtresse. Leur succès dépendra sans aucun doute de leur capacité à interconnecter des mobiles, à la volée et de bout en bout, pour leur fournir des services de manière omniprésente. Pour ce faire, les mobiles devront coopérer de proche en proche et relayer des services. De tels réseaux possèdent une forte dynamique et formeront spontanément des communautés de services. Nous pouvons imaginer une prolifération de nœuds de mobiles coopérant et mutualisant leurs ressources pour fournir par exemple un service d'accès à Internet (Entité B *figure 1*) ou encore tout autre service de proximité guidé au fur et à mesure par les besoins de l'usager : l'adresse des urgences locales ou de la pharmacie de garde, horaire adapté des transports en commun, distribution de ticket de train, etc.…

Si la dynamique du réseau rend, par ses mobiles particulièrement aisé le déploiement de services réseau, elle en diminue sans aucun doute la fiabilité du fait de la fragilité des liens réseaux, de leur facilité d'accès ou encore des déplacements incontrôlés des mobiles. De même, si ces communautés ambiantes réunissent un ensemble de mobiles autour d'un même intérêt qui est de former une communauté de service, comme la mutualisation d'une connexion Internet (figure 1), elles sont exposées à des mouvements imprévisibles : *naissance*, *partitionnement, jointure* et leur taille, leur population évoluent au rythme de ces changements d'état. Ce sont dans ces conditions d'échange difficiles que le service devra fonctionner coûte que coûte et sans même se laisser rompre par le seul doute sur l'honnêteté d'un nœud. En outre, l'utilisation de toute infrastructure, de toute administration centralisée ou plus encore d'un tiers de confiance est impossible, la confiance par conséquent devra s'adapter et s'établir dynamiquement à l'échelle de la communauté tout comme les autres

[1] - *Cet article est une contribution au projet KAA (Knowledge Authentication Ambiant) projet multidisciplinaire pour la recherche de la confiance dans les réseaux spontanés supporté par l'ACI Sécurité.*

services. Les modèles communicants dynamiques, sociaux ou électroniques, vont poser la question essentielle de la confiance pour échanger spontanément, sans risque et sans paralyser la circulation d'information. Comment instaurer la confiance lors d'un échange, comment se connaître ou se reconnaître ? Car au sein de telles communautés, les entités en mouvement ont peu de chance de posséder une identité reconnue ou des connaissances préalables, rendant aussi inutiles ou inopérants les mécanismes d'identification et à tiers de confiance traditionnels. Finalement la forte dynamique des réseaux spontanés confère des comportements de plus en plus proches des modèles sociaux et de plus en plus éloignés des modèles électroniques, fondés au contraire sur des règles rigides administrées manuellement par des tiers.

Dans cet article, la section 2 propose un état de l'art opposant modèles de confiance électroniques et sociaux, puis la section 3 décrit notre vision du formalisme de la confiance et la section 4 la proposition d'un modèle d'identification de type *famille* et *réseau*. Enfin, la section 6 présente nos prospectives.

Deux entités, A de C1 et B de C2, étrangères l'une à l'autre ont toutes deux l'intérêt commun d'accéder à la ressource distante R (FAX). Le membre A appartient à un type « famille» C1 ayant accès à la ressource et le membre B à un type famille C2 ayant l'accès Internet ; si les deux familles fusionnent et coopèrent, A et B pourront accéder à la ressource R.

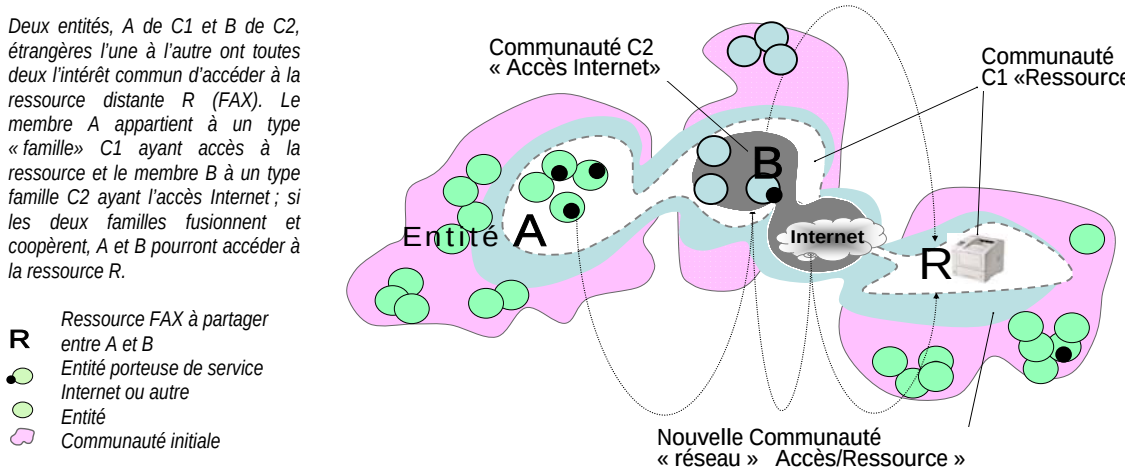

Figure 1 Accès mutualisé à une ressource distante

2. Etat de l'art : identification et identité dans les communautés

Dans cette section « état de l'art », nous nous intéressons aux modèles d'identification employés dans les réseaux à forte dynamique : les réseaux spontanés, les réseaux hybrides, les réseaux ad hoc, les réseaux pervasifs ou les réseaux ambiants appartiennent à cette catégorie de réseaux. La spontanéité imposera en plus au réseau la capacité de fournir un service d'identification à la demande ; or les modèles classiques imposent trois contraintes qui vont nuire à la dynamique du réseau : l'habilitation des identités au préalable, la distribution du secret au préalable et sa validation par un tiers de confiance. Idéalement, une habilitation spontanée, une distribution de secret à la volée et une protection totale aux attaques d'usurpation permettrait un modèle d'identification totalement dynamique et spontané. Nous proposons ici de classifier les modèles d'identification électroniques ou sociaux en fonction de ces contraintes.

2.1. Modèles traditionnels : comment se fait l'identification ?

Les modèles de confiance traditionnels ont pour rôle essentiel de certifier la confiance sous réserve de vérifier cinq propriétés fondamentales [MZ97] : identification, authentification, confidentialité, intégrité et non répudiation, qui, combinées entre elles, élèvent plus ou moins le degré de robustesse. Par exemple, un simple login/mot de passe (identité et preuve) est moins sûr qu'un certificat puisqu'il ne vérifie pas la propriété d'imputabilité. L'objectif d'un modèle de confiance est donc de garantir que l'information ne soit connue que des seules entités habilitées et ce, sans falsification, sans détournement, sans divulgation de l'information ou sans usurpation de leur identité.

L'identification [DoD83] est la condition de tout échange ; couplée à l'authentification, l'identification va initialiser un échange asymétrique entre un « prouvant » et un « vérifieur » en trois phases distinctes : 1) la gestion d'identités associant identité et secret, 2) le processus de *preuve* où le « *prouvant* » convainc le « *vérifieur* » de son identité à l'aide de son secret, enfin, 3) le processus de *vérification* où le « *vérifieur* »,vérifie le secret du « *prouvant* ».

Identification pour les réseaux spontanés

La *gestion d'identité* initialise une entité de moyens indispensables pour engager un échange et nécessaires à sa reconnaissance. Une entité peut être un mobile, une personne ou un terminal au moins doté de capacités de communication et d'une identité logique unique, créée elle durant le processus d'habilitation. La gestion d'identité distingue deux processus : *habilitation* et *distribution de secrets*.

- *L'habilitation* est une phase préalable à l'échange sous le contrôle de l'administrateur système. Elle permet grâce à une autorité tierce d'associer à l'identité diverses propriétés comme la preuve, le secret personnel, le secret de groupe, un ou plusieurs identifiants. En somme, l'habilitation permet d'assigner tout signe distinctif ou tout critère extérieur d'appartenance à une même communauté.
- *La distribution du secret* représente le processus d'attribution du secret aux seules entités habilitées à initialiser entre elles l'échange de confiance. Un secret délivré pour un échange « paire à paire » est un secret personnel qui, dans la cryptographie, se distingue d'un secret partagé de groupe ou clé de groupe. Pour un groupe, il faudra en plus distinguer les entités habilitées des « non-habilitées » par des critères extérieurs. Du point de vue social, les *critères extérieurs* définissent un signe distinctif d'appartenance à la communauté, une connaissance commune, sorte de trait d'union entre plusieurs entités véhiculant ainsi la confiance entre elles. Du point de vue électronique, le critère extérieur est un secret que des entités dites cryptographiquement compatibles partagent pour assurer confidentialité et authentification et exclure toute entité n'ayant pas la connaissance de ce secret. Toute la difficulté de la distribution du secret réside en la transmission du secret et en la distinction des entités habilitées (prouvant et vérifieur).

Deux modes d'échange sont alors possibles pour distribuer le secret : soit « face à face » et au préalable (PSK = pre shared key), soit durant l'échange et de manière dynamique (KAP :Key Agreement Protocol). KAP utilise le concept essentiel de la cryptographie asymétrique où toute entité est dotée d'un couple clé publique/clé privée tel que seul le possesseur d'une clé privée peut déchiffrer ce qui a été chiffré avec sa clé publique correspondante, et que tout flux chiffré avec une clé privée sera déchiffré avec sa clé publique correspondante. Pour pallier néanmoins aux attaques d'usurpation ou de Man In The Middle [MZ97]. il faut garantir reconnaissance mutuelle et imputabilité de l'« émetteur/destinataire » [MZ97] : c'est le rôle des protocoles de « Key Establishment ». Une autorité de certification interfère dans l'authentification des entités de son domaine en délivrant à chacune un certificat d'identité [X.509] qu'elle doit impérativement signer avec sa clé privée ; c'est sur celle-ci que repose la robustesse des infrastructures à clé publique.

2.2. Modèles traditionnels d'identification

Nous proposons de classer les modèles d'identification traditionnels selon leur mode d'échange « paire à paire » ou de groupe, leur mode d'habilitation et de gestion du secret : distribution du secret et vérification de la preuve. Nous distinguons en premier les modèles d'identification qui, pour négocier l'échange, imposent une identité propre *(à identité)*, une identité de groupe *(coopératifs, partagés*) ou restent indépendants (*autonomes*). Nous distinguons ensuite, en mode paire à paire ou de groupe, un secret distribué (modèles « *à identité», « partagés* ») d'un secret calculé (*coopératifs*, *autonomes*) qui sera pour le groupe plus résistant à l'usurpation puisque chaque entité contribue au calcul du secret [DH76][STW]. Le secret peut être une simple preuve d'identité, d'une entité ou d'un groupe mais peut aussi être une fonction commune du groupe, le critère extérieur discriminant.

Les modèles *à identité* comme les infrastructures à clé publique [PKI99] sont aujourd'hui les plus répandus et réputés les plus sûrs puisqu'ils permettent à chaque entité de se référer pour les quatre processus à une autorité unique qui garantit l'identité de chaque entité par un *certificat d'identité* (détaillé ci-dessus en $ 2.1). L'autorité agit selon deux modèles : centralisé ou distribué. Le modèle distribué offre une meilleure disponibilité du service du fait de la décentralisation des informations de confiance mais se heurte cependant à la difficulté de répartir la clé privée avec cohérence et confidentialité entre chaque membre référent. Bien que le besoin de tiers de confiance prive ce modèle d'une forte dynamique, certains travaux [ZH99][KO01] proposent l'adaptation du modèle en réseau ad hoc répartissant l'autorité centralisée en plusieurs autorités de certification. La problématique de la cohérence et de la confidentialité des répliques de la clé privée est traitée par l'emploi de la cryptographie à seuil. L'ensemble de ces modèles ne s'adapte pas aux réseaux spontanés car ils ne gèrent pas l'identification dynamique d'entités ou de communautés, de distribution dynamique de secrets puisque seuls certains membres détiennent la même clé privée d'une communauté [LNU03].

Les modèles *partagés* ne gèrent pas l'identité d'entité mais proposent le secret commun *partagé* comme critère discriminant ; le secret, distribué au préalable, identifie le groupe et se partage entre l'ensemble des membres. L'authentification se réalise par la simple reconnaissance de ce secret partagé. Les modèles

partagés sont statiques et impose généralement une distribution au *préalable*, ce qui réduit leur intérêt pour une utilisation plus large. La faiblesse d'un seul membre met en danger l'ensemble du groupe, ces mécanismes ne sont donc pas sûrs et utilisables dans le cadre de grands réseaux même si chaque membre peut vérifier le secret présenté par un autre. Quelques modèles suivent cette architecture dont le plus réputé aujourd'hui est le WEP [IEE11].

Les modèles *coopératifs* définissent un mode d'échange de groupe qui le différencie du modèle précédent parce que chaque entité contribue au calcul du secret du groupe (secret S) [STW] [PB+03] ; S, secret commun du groupe, est calculé en général avec [DH76] et à partir du secret privé de l'entité combiné au secret privé du groupe. S constitue le critère extérieur, comme dans les modèles précédents, pour retenir les seules entités habilitées à coopérer autour d'un même intérêt, d'un même service. L'intérêt du mode coopératif réside dans le degré de liberté que possède une entité pour coopérer ou non en fonction d'un critère extérieur définit par le groupe. Mais ces mécanismes extrêmement consommateurs [A+01] devront être réservés au cas de communautés imposant une forte cohérence du secret.

Les modèles *autonomes* libèrent l'entité de la présence du tiers de confiance pour engager un échange sûr mais imposent la connaissance de l'autre sous forme par exemple d'une base de certificats embarquée. Ces modèles n'imposent pas en revanche la contribution de chacune des entités à l'élaboration du secret de la communauté ; l'échange se réalise de manière dynamique et spontanée, tout en gardant la possibilité de construire un échange ou une communauté avec d'autres nœuds autonomes et étrangers ; dans ce cas les entités devront introduire un critère extérieur commun puisqu'il n'existe pas de connaissances communes préalables. Ces modèles induisent d'autres problématiques liées à la performance ou encore à la cohérence des bases au moment des opérations de fusion ou de recherches de connaissances communes [HBC01]. Ce modèle est coopératif et autonome nécessite un algorithme d'évaluation des relations de confiance pour chaque entité.

2.3. Les modèles de confiance électronique

Certains travaux introduisant de plus en plus de critères extérieurs rendant ces modèles ou propositions de plus en plus proches des modèles sociaux. [BH01] propose la monnaie virtuelle (nuggets) comme liant, [FST04] étudient et évaluent des mécanismes de micro paiement pour le commerce électronique paire à paire et les travaux de [ARH97] [WW04] introduisent la notion de recommandation comme régulateur des entités via des agents véhiculant les informations de confiance.

Cependant, il est important de fournir un modèle plus complet comme [WT01], modèle de confiance distribué et dynamique portant sur le cycle complet de la confiance : prévention, répression et réaction. [AG99] propose d'appliquer au groupe son protocole d'établissement progressif de la confiance, passant au cours de l'échange d'un canal progressivement peu sûr à sûr [LNU03].

[FS86] propose les méthodes pour calculer la preuve sans jamais la révéler et initialise le concept du Zero Knowledge repris dans les travaux de [WW04]. Les auteurs analysent la confiance et le comportement humain, sur les aspects du commerce « peer to peer » où la confiance se construit par chaque entité sur l'ensemble de ses relations mises à jour dans sa liste de références. Ces mécanismes de recommandation et de réputation, « les amis de mes amis sont mes amis » utilise [ARH97].

[C99] soulève en tout premier lieu la nécessité de communiquer sous plusieurs modes et de se détacher des modèles traditionnels binaires monomodes. Il décrit l'identité sous deux formes d'échange avec l'anonymat associé au *marché* et le pseudonyme à la notion de *réseau* de confiance : il introduit le concept du « nym », identité définie par l'organisation et son mode d'échange [C99]. Il montre l'intérêt de définir un identifiant de l'échange.

Il en résulte que ce schéma correspond à un modèle complet doté d'une forte autonomie. Les deux mécanismes (répression et recommandation) s'adaptent aux exigences des réseaux spontanés.

2.4. Vision sociale de la confiance

Il est important de distinguer les objectifs fixés par l'identification car elle pourrait en cas d'ambiguïté nuire à la constitution d'une communauté de service pour finalement paralyser le réseau. En effet, une identification forte peut être requise pour délivrer un passeport mais une connaissance plutôt qu'une identification est suffisante pour coopérer à l'accès d'un service Internet ou échanger librement au sein d'un simple groupe de discussion.

[JC94] explique l'importance de l'identification au sens social en tant que mécanisme initial de la

reconnaissance. Pour [JC94], l'identification permet de reconnaître des entités contribuant à la constitution d'une communauté selon des « signes distinctifs communs » qui vont permettre d'élaborer une communauté réunie autour de ces marques permettant ainsi de favoriser le processus de l'authentification. [TDE02] assure en outre que, en définitive certains composants d'un individu comme des valeurs, des fragments de passé, appelés « signes distinctifs communs », «manifestent l'existence de traditions et de valeurs communes qui constituent un moyen privilégié de régulation du fonctionnement interne de l'organisation». Ces concepts sont intéressants, car ils encouragent l'idée que l'identification, née de la collecte des acquis ou de valeurs communes d'une communauté, a un sens, plus encore pourrait permettre la reconnaissance des identités.

L'approche sociale de [LU+04] définit quatre modèles sociaux de confiance se distinguant par leur mode de régulation, leur degré de structuration et la distance sociale de leurs membres [LU+04] : *famille*, *organisation*, *réseau* et *marché* (Tableau 1). Chaque communauté définit un contexte de confiance, c'est-à-dire les conditions de confiance dans lesquelles l'échange va se dérouler. Ces contextes ne constituent pas des découpages nets et peuvent mixer leurs propriétés : une personne de la même famille peut nouer un échange de type *marché* avec un membre de sa *famille*.

TYPOLOGIES	FAMILLE	RESEAU	ORGANISATION	MARCHE
REGULATION	DON	CONFIANCE	AUTORITE	PRIX
DISTANCE SOCIALE	FAIBLE	FAIBLE	FORTE	FORTE
DEGRE DE STRUCTURATION	FORT	FAIBLE	FORT	FAIBLE

Table 1.1 : Organisation des modèles de confiance sociaux

Le *marché* représente l'échange libre de tiers de confiance où seule la chose échangée compte, les « échangistes » sont transparents, il n'existera alors aucune notion d'habilitation, de connaissance et de reconnaissance comme par exemple de la vente par annonces ; le marché est alors régulé par la monnaie et la valeur de la chose.

La *famille* ne compte que des membres réunis par le lien du sang, un lien physique fort rendant presque totale l'espérance qu'un membre de la même famille ne trahisse la confiance déjà pré instaurée. De cette manière, l'habilitation sera automatique dès lors que le lien physique existe puisque qu'il permettra la reconnaissance dynamique des deux membres sans validation d'un tiers de confiance.

L'*organisation* traduit le contexte d'échange des membres d'une communauté très structurée, hiérarchique et régulée par une autorité unique. L'autorité garantit les identités des personnes à l'échelle de la communauté et même au-delà, dans certaines relations inter domaine pré établies (notion de frontière). Au sein du type *organisation* les entités sont socialement éloignées l'une de l'autre et devrait à priori refuser de se faire confiance. Mais chaque membre possède un lien de subordination avec l'autorité, si bien que la confiance se certifie par l'autorité mais ne se construit pas par les membres. La structure de la communauté est entretenue par le lien de subordination régi par l'autorité. Ce lien fort réduit considérablement l'incertitude que pourrait avoir un membre sur un autre ou même sur son autorité. La distribution des habilitations et des pièces justificatives de l'identité des membres est réalisée au préalable entre l'autorité et les membres.

A la différence des autres modèles, le *réseau* regroupe des membres motivés par les mêmes intérêts ou partageant la même expérience [JC94]. Les intérêts communs constituent le critère extérieur partagé par la communauté et de ce critère, il est possible de dériver des identités temporaires (pseudonyme) dans le seul but d'engager l'échange et de ne pas le bloquer ; un échange utilisant un pseudonyme constitue une sorte d'habilitation dynamique. Une fois les critères communs partagés par les membres, les entités vont se reconnaître spontanément par leur appartenance au même réseau d'intérêt. Le degré de structuration est faible mais est compensé par l'espérance que l'intérêt développé par les entités est plus fort que celui de compromettre le réseau de confiance.

2.5. Modèles sociaux et modèles électroniques

La vision de l'identification pour les modèles sociaux puis électroniques nous conduit à une opposition de ces deux modèles et il en ressort plusieurs constats. En *premier*, la confiance gérée par les modèles électroniques se traduit par la recherche de sécurité maximale délivrée par un tiers de confiance alors que les modèles sociaux de type *réseau* évaluent le risque et ne visent pas la sécurité maximale. La gestion des niveaux de confiance en fonction des risques et des incertitudes devient alors essentielle pour réduire la faiblesse des

critères discriminants : niveau de confiance faible pour un critère discriminant faible et fort pour un critère discriminant fort et la notion « je fais confiance en », mesurant enjeux et risques, constitue finalement une approche purement sociale. En *second*, il ressort une notion très forte, la notion d'initialisation (figure 2a) qui différencie nettement les modèles sociaux des modèles électroniques puisque l'on constate qu'une personne initialise l'échange coûte que coûte, même avec un étranger, ce qui n'est pas possible dans les modèles électroniques. Une personne essaiera dans ce seul but de corréler progressivement les identités de son interlocuteur, en cherchant leurs connaissances communes. Lors de cette phase, l'entité va tenter de rechercher des critères discriminants comme des connaissances communes, des intérêts communs : c'est la notion de « faire connaissance » figure 2a. Plus encore, si la personne ne parvient à corréler une identité, elle créera alors une identité temporaire de la relation (pseudonyme) : il s'agit là de la notion d'habilitation dynamique. En *troisième*, lors de l'échange type « réseau », on constate que l'unicité n'est pas garantie car au travers de communautés disjointes, sans gestion d'identité commune, l'unicité ne veut rien dire. Une gestion d'identité universelle qui fait aujourd'hui défaut serait adaptée. Si ce point est un verrou du point de vue de la recherche, il n'est pas bloquant pour notre problématique puisque l'échange peut commencer sans identité par la phase « faire connaissance ».

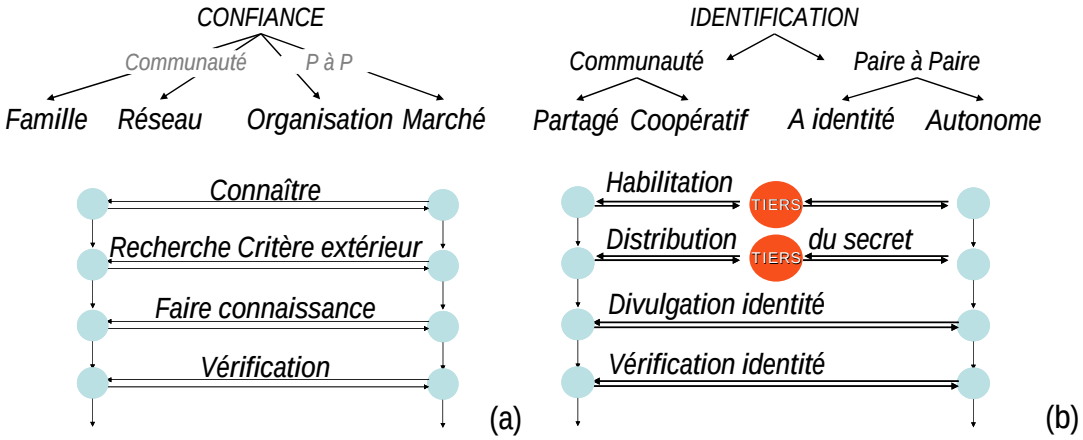

Figure 2 *Modèles et étapes comparées de l'initialisation pour les modèles sociaux (a) et électroniques (b)*

Le modèle *réseau* se révèle particulièrement nécessaire dans le cas d'échange sans connaissance préalable ; il est un véritable apport aux modèles électroniques donc si l'on concevait un modèle technologique en respectant les propriétés des modèles *famille* et *réseau*, il serait possible de concevoir un modèle apportant la confiance en environnement spontané, besoin qui n'est pas couvert aujourd'hui.

L'identification comme nous l'avons vu joue un rôle fondamental dans un modèle de confiance puisqu'elle contribue pour beaucoup à réduire l'incertitude qu'une entité peut ressentir sur l'autre et vice et versa. Du point de vue des sciences sociales, l'identification favorise les chances de succès de l'échange alors que du point de vue des technologies l'identification initialise l'échange sûr. Cette nuance est importante car elle définit qu'une entité « sociale » serait en mesure de choisir son contexte de confiance de l'échange, un apport des modèles sociaux aux modèles électroniques à étudier. Nous allons définir les propriétés que nous souhaitons développer pour un modèle de confiance, et plus particulièrement pour un modèle d'identification dans un contexte dynamique.

3. Propriétés de la confiance et de l'identification

Des quatre processus étudiés (section 2.1), nous proposons maintenant d'en définir leurs divers composants: entité, identité, identifiant, communauté, secret.

Entité et identité

Une entité est un objet mobile doté de capacités de communication indispensables pour entreprendre un échange : elle désigne une personne, son mobile ou tout terminal connecté. Notamment, on suppose qu'au sein de sa communauté l'entité est capable d'émettre des messages de diffusion pour signaler sa présence et de les recevoir. Ces messages sont des informations qui vont lui permettre de détecter l'environnement de sécurité auquel elle appartient. Lorsqu'elle appartient à un ensemble **E** communicant, l'entité doit posséder une caractéristique physique liée au réseau comme sa localisation géographique et son adresse réseau ainsi qu'une

identité logique. La mobilité entraîne que sa localisation géographique et son adresse réseau évoluent alors que son identité est figée. **E** désigne l'ensemble des entités notées ***a, b, c*** (***a*** ∈ **E**). A chaque entité ***a*** on associe une identité notée $\mathbf{Id_a}$, un secret $\mathbf{S_a}$, un ensemble d'identifiants **I** (login par exemple) et un ensemble de méthodes destinées à calculer la confiance, $\mathbf{M_a}$ [confidentialité, identification, authentification, intégrité, non-répudiation,...]. Il existe des sous-ensembles de **E** qu'on note ***G,*** définis par des critères extérieurs. Par commodité, on désignera ces sous ensembles des *communautés*. Une entité ***a*** est définie comme suit tel que ***a*** possède une identité, un secret, des méthodes et les deux points « **::** » signifient « *possède* »:

(1) $a :: \{ Ida , Sa , [Ma] \}$

Notion de secret de l'entité

Le secret d'une entité ***a***, noté ***Sa*** est la condition nécessaire pour procéder au processus de preuve ; il contribue notamment à répondre aux critères d'authentification requis dans les modèles traditionnels (notamment le modèle « à identité ») en respectant au mieux les trois règles suivantes [MZ97] : ce que je suis - défini par un ou plusieurs éléments physiques de l'individu (biométrie,...), ce que je connais - valeur apprise (mot de passe, code, etc.)-, et ce que je possède - valeur affectée sous forme par exemple d'une carte à puce. En présentant le secret ***Sa***, l'entité va convaincre son interlocuteur qu'elle est bien ce qu'elle dit être, sachant que le mode de distribution du secret est donc un point essentiel pour qu'il ne soit transmis qu'aux seules entités habilitées.

Notion de secret de communauté

L'intérêt du secret de la communauté est de favoriser le calcul de clés cryptographiques (clé de session ou d'authentification). Nous avons vu que la distribution du secret aux seules entités habilitées est une phase particulièrement critique pour les réseaux spontanés démunis de tiers de confiance puisqu'elle cherche à fournir sans connaissance préalable et de manière spontanée les clés initiales à chaque entité. Nous désignons par **S** le secret de la communauté et définirons la communauté par l'ensemble des entités qui partagent le même secret commun **S** constituant finalement la preuve d'appartenance à la communauté.

Unicité

L'identification constitue un processus au préalable pour habiliter une identité en lui associant des propriétés et des fonctions de sécurité, notamment des preuves d'identité ou d'appartenance à une communauté. Ces fonctions de base seront la création, la mise à jour, la suppression d'identité et les fonctions supplémentaires comme les autorisations, les rôles. Cependant le modèle de confiance respectera le principe de l'unicité : une identité est unique et se distingue de toute autre. Nous définissons qu'une entité ***a*** appartient à un ensemble **E** :

(2) $a :: Ida \text{ et } b :: Idb \text{ si } a \neq b \text{ alors } Ida \neq Idb$

Notion de communauté

Les entités vont utiliser leurs capacités de communications pour coopérer avec d'autres entités à construire un service pour l'usager. Par exemple, plusieurs mobiles ou communautés autonomes vont se réunir pour porter un service de routage ou former un groupe de « news » pour ouvrir une discussion sur l'intérêt du logiciel libre ou encore construire comme le montre la figure 1, une nouvelle communauté de FAX, Cl. Ces réseaux s'unissent autour d'un intérêt commun, les critères d'appartenance. Le résultat de cette union constitue un sous ensemble de **E** que nous appellerons une communauté désignée **C**. extérieur et dans ce cas c'est le secret S qui constitue le critère d'appartenance : c'est parce que chaque entité possède S qu'on parlera de communauté.

(3) $C(a,b,c) \equiv \{ a :: \{Ida , Sa , S , Ma\} , \ b :: \{Idb , Sb , S , Mb\} , \ c :: \{Idc , Sc , S , Mc\} \}$

4. Identification: une nouvelle approche

4.1. KAA: rappel des fonctions

Le projet de recherche KAA (Knowledge Authentication Ambient) a pour objectif de proposer un modèle de confiance pour les objets communicants. Pour KAA, la confiance est une valeur graduée de « aucune » à « maximale » que les actions de sécurité vont plus ou moins renforcer selon les objectifs de sécurité fixés par les transactions des usagers. Le concept du modèle KAA est d'intégrer le mode de gestion de la confiance des communautés sociales aux communautés électroniques. Le point de départ repose sur les quatre familles sociales qui définissent quatre protocoles de confiance négociés selon le besoin de deux entités.

Nous faisons l'hypothèse que l'implémentation des protocoles autorise qu'une entité KAA existe à condition qu'elle soit équipée d'un package cryptographique minimum, le package KAA qui la rendra compatible avec tout autre entité KAA. Ce package intègre le matériel cryptographique et les données initiales. Le matériel cryptographique regroupe un ensemble d'algorithmes et de méthodes cryptographiques requises qui définissent la confiance (section 2) : habilitation, distribution du secret, recherche de critères communs, d'intégrité, de confidentialité, de divulgation de preuve et de vérification de preuve. Si l'ensemble de ces fonctions atteignait une valeur maximale, le calcul de la confiance apporterait un niveau de confiance maximal. Les données de confiance, dynamiques et propres à chaque entité KAA, se présente sous forme d'un ensemble de certificats appelé liste de connaissances qui, créée à l'initialisation de l'entité, va assurer l'accès aux familles connues et certifier les données de confiance. Equipée de cet ensemble, elle peut engager un échange dans l'un ou l'autre des contextes.

Modèle KAA

Famille	*Réseau*	*Organisation*	*Marché*
Imprégnation	-	*Identité*	*Chose échangée*
Secret Sp	*Critères communs*	*Divulguer le certificat*	*Valeur de la chose*
Reconnaissance	*Mutualiser les ressources*	*Vérification du certificat*	*Chose échangée*
Certificat de Famille	*Certificat de confiance*	***Certificat d'identité***	*Certificat vente*

Figure 3 *Positionnement de KAA*

Nous avons commencé nos travaux par l'étude de deux contextes de confiance : *famille* et *réseau* et nous présentons dans la suite de cet article deux modèles communicants KAA : un échange entre deux entités issues de communautés type *famille* : le modèle d'imprégnation et la phase d'habilitation spontanée entre deux entités étrangères du type *réseau* (figure 2). Mais, avant de présenter ces deux modèles, nous proposons notre première formalisation de la confiance et de l'identification.

Fonction de confiance

Nous avons vu que KAA définit la confiance comme une valeur graduée entre deux entités **a** et **b**, c'est donc une fonction que nous notons CONF capable de calculer l'espérance que **a** possède sur **b** tel que **b** respecte les politiques de confiance notées **Pa** mises en œuvre par **a.** L'espérance est notée **n** où **n** est la valeur graduelle de **0** à **1** pour définir la confiance entre **a** et **b.**

(4) $\forall (a, b) \mid CONF(a, b)=\{0,1\}$ et $CONF(a, a)= 1$

La **«** politique de confiance » **Pa** possède les valeurs de **0** à **1** selon qu'elles ont été respectées ou non. La politique de confiance contient l'objectif de sécurité défini qui lie une entité et ses actions : par exemple pour l'action payer alors l'objectif de l'entité est la signature et l'entité possède une signature notée Sign**a.**

(5) *Soit Pa={0,1}, si Pa=1 alors CONF(a, b)=1*

Notion d'identification et d'objectif de sécurité

L'identification contribue à élever la confiance d'une entité vers l'autre dès lors qu'elle respecte les contraintes d'habilitation (unicité), de distribution du secret (en milieu sûr), propriétés définies en sections 3 (3.2, 3.3 et 3.4). Chacune des propriétés d'identification respectées élève le niveau de confiance à son maximum. Si les cinq propriétés de la confiance [MZ97] (identification, authentification, confidentialité, intégrité et non répudiation) qui décrivent les objectifs de sécurité sont atteintes alors CONF(a, b)=1.

4.2. Modèle de communauté de type famille : Imprégnation KAA

Le type *famille* doit la confiance entre les membres d'une même famille au lien du sang. Le concept d'imprégnation de [SA99] définit la relation physique (imprégnation) indispensable pour distribuer un secret en toute confidentialité lors de la phase d'initialisation et propice à des mécanismes de reconnaissance robustes. Nous associons ce concept au type social *famille* pour lequel le lien physique représente le lien du sang. Ce modèle constitue la distribution du secret et du package d'initialisation de toute entité KAA.

Le modèle propose une phase d'initialisation proposant les services d'habilitation et de distribution du secret au préalable et par voie physique.

Identification pour les réseaux spontanés

Phase I « Habilitation et distribution du secret »

L'image du patriarche, maître de la famille se présente sous la forme d'un serveur d'imprégnation ◘ et reste le seul maître pour habiliter les entités telles que chaque identité ***Id*** soit unique dans son domaine. Le protocole d'imprégnation induit un lien physique fort et est obligatoire pour s'initialiser. L'entité KAA *famille* est imprégnée de méthodes **Ma**, de son secret individuel ***Sa***, du secret de la « *famille* » **Sp**. Les deux fonctions d'habilitation et de distribution respectent les propriétés suivantes :

(6) *a :: { Ida , Sa , Sp, [Ma]}.* *(définition de l'entité imprégnée)*

(7) *a :: Ida et b :: Idb si a ≠ b alors Ida ≠ Idb)* *(définition de l'unicité)*

(8) *P(a,b,c) ≡{a :: {Ida , Sa , Sp , Ma} , b :: {Idb , Sb , Sp , Mb} , c :: {Idc , Sc , Sp , Mc}}*
(définition de l'appartenance à la communauté « famille »)

L'idée est d'éviter l'insertion d'éventuelles membres et les pertes de cohérences du secret **Sp** de la « famille » comme le décrit [KPT01] en imposant pour chacun des membres leur contribution exclusive Sa dans le calcul de **Sp** [HM94]. Soient **Sp** le secret commun partagé par les entités et ⊗ un opérateur, le calcul s'exprime selon la base [DH76] et [HM94] :

(9) *Sp =Sa ⊗ Sb ⊗ Sc ⊗...⊗ Sn*
(définition [HM94] du secret de la communauté « famille »)

Le « lien du sang » est un lien physique où la confiance entre les membres de la même famille et leur patriarche P est à 1 :

(10) *∀ (a,b,c, P) | CONF(a, P) = 1, CONF(b, P) = 1, CONF(c, P) = 1*
(définition du lien patriarche/entité)

Phase II "Recherche du critère famille et Reconnaissance »

Dans le principe de KAA, deux entités à priori étrangères établissent la confiance par l'échange de leurs listes de connaissances [LU+ 04] où elles cherchent l'existence commune d'un certificat de famille signé par leur patriarche ; l'intérêt, dans ce cas, est qu'elles se reconnaissent dynamiquement toutes deux par la reconnaissance de leur secret commun, le critère extérieur Sp, signe de leur appartenance à la même famille. Il suffit alors de le vérifier, elles le peuvent puisqu'elles ont la connaissance de leur contribution ***Sa*** au calcul du secret **Sp** :

(11) *∀ (a,b,c, P) | CONF(c, P) = 1 CONF(a, P) = 1, alors CONF(c, a)=1 et CONF(a , c)=1*

4.3. Modèle de communauté de type Réseau

Nous avons défini un mécanisme d'établissement de la confiance pour un modèle électronique de type « *famille* », nous allons maintenant proposer la première étape pour un modèle de type « réseau » : comment générer une habilitation dynamique électronique. L'idée est de calquer sur le modèle social *réseau* l'échange entre deux entités **a** et **b** étrangères et en possession toutes deux du package KAA de base [LU+04]. Leur échange doit exister pour obtenir le service souhaité (un service FAX ou d'accès Internet par exemple en figure 1) faute de quoi leur communication serait coupée ; le concept KAA défend l'idée d'engager un échange même à risque en introduisant la notion de niveau de confiance pour l'évaluer par la suite. Nous décrivons ici le mécanisme « certificat de moment » qui apporte la preuve que ces deux entités se sont connues et sont en mesure de se reconnaître dans le futur.

Phase « Faire connaissance »

Tout comme deux « personnes », les entités vont tout d'abord chercher si elles se connaissent et acquérir pour ce leur données de confiance communes par l'échange de leur historique ; dans le cas où aucune connaissance commune n'est détectée, elles vont « faire connaissance » même si, tout comme dans une relation sociale, cette action les expose autant au risque de communiquer avec un intrus qu'au succès de l'échange : cet échange vécu par les deux entités devient un moment commun enrichi d'évènements communs. Est-il alors possible d'utiliser cette connaissance commune comme signe distinctif de leurs relations futures ? Autrement dit, lors de la phase de reconnaissance chacune des entités pourra présenter la preuve de leur rencontre. Mais si ce moment commun doit être compréhensible et prouvable par ces seules entités afin de

réaliser plus tard l'authentification, ce moment doit présenter les propriétés cryptographiques traditionnelles d'imputabilité, d'intégrité, de confidentialité, d'anti rejeu. Pour ce faire, nous utilisons les mécanismes destinés au calcul d'un secret commun par contribution des parties [KPT01]. L'idée est que chacune des entités fige les mêmes caractéristiques du *moment* noté Ξ.qu'elles ont eu l'occasion de partager, de figer les mêmes méthodes **M**, et de calculer chacune de leur côté ce secret commun partagé : le secret du moment noté **S**Ξ. Avec ce secret, il sera possible de signer le certificat du moment noté **Cert**Ξ pour le stocker et le transmettre.

(12) *Pour a : Ξ a/b::{ SΞa, Ida ,Sa, Evènement{€i,...,€j, Horodatage,DuréedeVie, Identifiant} ,*

et Pour b : Ξ b/a::{ SΞb,, Idb , Sb , Evènement{€i,...,€j, Horodatage,DuréedeVie, Identifiant}

Chacune des entités consigne le moment dans sa base de connaissances sous forme d'un certificat signé via le secret commun SΞ auquel contribuent les deux entités avec leur propre secret :

(13) *SΞ = SΞa = SΞb = Sa ⊗ Sb* *Le secret du moment commun à a et b est identique*

Il suffit de calculer le certificat *Cert* de la manière suivante avant de le stocker :

(14) *CertΞ a/b = SignΞ (Ida , Idb , Evènement, Horodatage, Identifiant)* *pour a*

(15) *CertΞ b/a = SignΞ (Ida , Idb , Evènement, Horodatage, Identifiant)* *pour b*

Bilan du « certificat de moment »

Le calcul **S**Ξ, secret du moment, permet de distribuer dynamiquement le secret entre les seules entités habilitées, c'est-à-dire ayant connu ce *moment*. Avec ce secret, chaque entité pourra chiffrer et déchiffrer le certificat de *moment* afin de vérifier dans l'échange ultérieur que son interlocuteur a partagé avec elle ce *moment* dans le passé. Ce certificat de moment viendra ainsi enrichir l'historique de chaque entité et sera affecté d'une évaluation de la relation passée, le niveau de confiance [LU+04].

5. Bilan et perspectives

La problématique que nous avons traitée porte sur la capacité d'un réseau à assurer les échanges en environnement à priori hostile pour que les services se forment spontanément et que l'information circule même si des doutes sur le climat de confiance subsistent. Nous avons vu que les échanges n'appellent pas toujours un niveau de sécurité maximal et que le contexte de l'usager doit être adaptable. Notre étude a montré qu'il n'existait pas de modèles de confiance électroniques adaptés à ces nouveaux besoins mais que les modèles sociaux, eux, possèdent des caractéristiques qui permettraient de couvrir ces besoins. Le concept de KAA a été présenté comme une adaptation de ces concepts sociaux mais la conception d'un tel modèle reste une tâche à laquelle nous devons nous atteler pour implémenter notamment les modèles correspondants.

En formalisant notre modèle, nous devons aussi modéliser les attaques qui vont se calquer sur celles découlant des modèles sociaux en plus de celles existantes actuellement dans les modèles électroniques.

On pense naturellement à la mise en place d'un modèle de réputation pour apporter à notre architecture un mode de graduation de la confiance plus fin : 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. 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.

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. 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. De nombreux travaux, [ARH97] décrivent des mécanismes de réputation fondés sur la détection d'un comportement contraire aux règles, mais l'absence de centralisation de l'information de réputation rend la sanction peu efficace. Nos travaux actuels portent aussi sur la détection de comportements anormaux et normaux afin de détecter au même titre qu'un modèle social les écarts qui pourraient mettre un système de confiance en danger.

6. Bibliographie

[AG99] N. Asokan and P. Ginzboorg. "Key-agreement in ad-hoc networks". In Nordsec'99, 1999.

[ARH97] A. Abdul-Rahman and S. Hailes. "A Distributed Trust Model" -. New Security Paradigms Workshop 1997, ACM, 1997.

[A+01] Yair Amir, Yongdae Kim, Cristina Nita-Rotaru, Gene Tsudik ."On the Performance of Group Key Agreement Protocols". F30602-00-2-0526 from The Defense Advanced Research Projects Agency.

[BH01] L. Buttyan and J.-P. Hubaux. "Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks". Technical Report DSC/2001/001, Swiss Federal Institute of Technology – Lausanne, Department of Communication Systems, 2001.

[C99] Roger Clarke: Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice; in: Simone Fischer-Hübner, Gerald Quirchmayr, Louise Yngström (Eds.): User Identification & Privacy Protection: Applications in Public Administration & Electronic Commerce; Kista, Schweden; June 1999; IFIP WG 8.5 and WS 9.6; http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html.

[DH76] W. Diffie and M. E. Hellman. "New directions in Cryptography" -. IEEE Trans. Inform. Theory, IT-22:644–654, November 1976.

[DoD83] DoD Directive 5200.28-STD, Trusted Computer System Evaluation Criteria, 1983.

[FS86] A. Fiat, A. Shamir. "How to prove yourself: Practical solutions to identification and signature problems". In A.M. Odlyzko, editor, Advances in Cryptology —CRYPTO'86, volume 263 of Lecture Notes in Computer Science, pages 186–194.Springer-Verlag, 1987.

[FST04] Daniel R. Figueiredo, Jonathan K. Shapiro, Don Towsley. "Payment-based Incentives for Anonymous Peer-to-Peer Systems". Computer Science Technical Report 04-62, July 27, 2004.

[HBC01] J. Hubaux, L. Buttyan, and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks". In Proceeding of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Oct 2001.

[IEE11] IEEE 802.11 wireless local area networks: The working group for WLAN standards. http://grouper.ieee.org/groups/802/11/, 2002.

[JC94] J. Chevallier, « Identité, organisation, institution », in L'identité politique, PUF 1994, pp. 239-251.

[KO01] J. Kong et al. "Providing robust and ubiquitous security support for mobile ad-hoc networks". In Proc. IEEE ICNP, pages 251–260, 2001.

[KPT01] Y. Kim, A. Perrig, and G. Tsudik, "Communication-efficient group key agreement," in Proceedings of FIP SEC 2001, June 2001.

[LNU03] Véronique Legrand, Farid Naït-Abdesselam et Stéphane Ubéda – « Etablissement de la confiance et réseaux ad-hoc : Un état de l'art » - Laboratoire CITI – INRIA ARES - Conférence SAR 2003

[LU+04] V. Legrand, S. Ubéda, J. Morêt-Bailly, A. Rabagny, L. Guihéry, J-P. Neuville. "Vers un modèle de confiance pour les objets communicants : une approche sociale ». 3rd Conference on Security and Network Architectures, June 2004.

[LHU03] V. Legrand, D. Hooshmand and S. Ubéda. "Trusted Ambient community for self-securing hybrid networks".INRIA RR-5027, 2003.

[MZ97] A. Menezes, P. van Oorschot, and S. Vanstone. "Handbook of Applied Cryptography". CRC Press, 1997.

[PB+03] N.Prigent, C.Bidan, JP.Andreaux, O.Heen. "Secure Long Term Communities In Ad Hoc Networks". ACM SASN 2003.

[PKI99] Perlman R. "An Overview of PKI Trust Models", IEEE, 1999.

[RS00] R. Shirey, "Internet Security Glossary" - Network Working Group, Informational May 2000, 2828.txt.

[SA99] Frank Stajano, Ross Anderson,. "The resurrecting duckling: Security issues for ad-hoc wireless networks". In Proceedings of the 7th International Workshop on Security Protocols, Lecture Notes in Computer Science. Springler-Verlag, Berlin, Germany, April 1999. Available from http://www.cl.ac.uk/~fms27/duckling/duckling.htm

[SWS96] Bruce Schneier, John Wiley & Sons. "Applied Cryptography" Second Edition, 1996, ISBN 0-471-11709-9.

[TDE02] Thierry DELPEUCH, CERAT, Institut d'études politiques de Grenoble.

[WW04] Andre Weimerskirch, Dirk Westho -"Zero Common-Knowledge Authentications for Pervasive Networks" - Communication Security Group, Ruhr-University Bochum, Germany.

[X.509] ITU-T Recommendation X.509 (1997): Information technology - Open systems interconnection - The directory Authentication framework, June 1997. Also ISO/IEC 9594-8:1998.

[ZH99] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network, pp.24–30, December 1999.