XII

Sécurité, protection de la vie privée et disponibilité[•]

XII.1- Introduction

L'émergence de l'informatique diffuse laisse entrevoir une société où la technologie disparaît dans l'environnement physique afin de la rendre aussi efficace que possible car 'invisible' à l'utilisateur (122). Or, cet objectif de transparence ne peut être atteint que si la technologie est suffisamment sûre de fonctionnement pour que les utilisateurs puissent effectivement l'oublier. Ainsi, les utilisateurs doivent avoir une totale confiance que :

- les malveillances éventuelles ne peuvent pas porter atteinte à la confidentialité ou à l'intégrité de leurs données et transactions ;
- la technologie ne peut pas être détournée pour dévoiler à leur insu des données intimes ou leurs moindres faits et gestes ;
- les services offerts sont toujours accessibles là où et quand ils en ont besoin.

Ce chapitre comporte trois sections principales consacrées respectivement à l'état de l'art et des recherches relatifs à ces trois objectifs de confiance.

Nous portons une attention particulière aux spécificités de l'informatique diffuse, caractérisée par un traitement embarqué sur des objets physiques (appelés *dispositifs* dans ce qui suit) souvent mobiles, et communiquant sans fil et sans connectivité permanente à une infrastructure fixe.

XII.1.1- Menaces vis-à-vis de la sûreté de fonctionnement

Les dispositifs de l'informatique diffuse sont sujets aux mêmes sources de dysfonctionnement ou fautes que tout autre système informatique (11), mais ces fautes sont aggravées par plusieurs spécificités. Nous traiterons successivement des fautes accidentelles ou non malveillantes, puis des malveillances.

L'environnement physique peut accroître significativement le taux de défaillance physique des dispositifs. Les dispositifs (surtout dans les réseaux de capteurs), peuvent être appelés à fonctionner dans des conditions sévères de vibration, d'humidité, de température, de rayonnement ou en présence de produits chimiques. La détérioration physique et l'usure des dispositifs, conduisant à une

[•] Ce chapitre a été rédigé par Yves DESWARTE, David POWELL et Yves ROUDIER.

dégradation plus ou moins progressive de leur fonctionnement, ne doivent pas être négligées.

La communication sans fil introduit des aléas importants du fait des interférences possibles, que ce soit dû à des sources de bruit externes, au partage des fréquences avec d'autres systèmes, ou à des conflits avec les émissions de dispositifs pairs. La mobilité des dispositifs ajoute une source d'aléa supplémentaire en raison de la portée limitée de la communication sans fil et la présence éventuelle d'obstacles à la transmission (murs, bâtiments, terrain accidenté…).

Le développement de logiciels pour l'informatique diffuse doit faire face à plusieurs difficultés qui nuisent à la production de logiciels de qualité. D'une part, de tels systèmes sont sujets à une *dynamique* importante en raison de la communication non fiable, voire limitée dans le temps (mobilité), et des changements de contexte d'utilisation (dispositifs portables). Les logiciels systèmes et applicatifs doivent donc être capables de s'adapter dynamiquement à des situations en perpétuelle mutation. D'autre part, la diversité des types de dispositifs pouvant interagir et l'évolution fulgurante des technologies de l'informatique diffuse concourent à une *hétérogénéité* inévitable. La pérennité des composants logiciels et la compatibilité syntaxique et sémantique de leurs interfaces logiques sont alors particulièrement problématiques. Enfin, l'évolution rapide des technologies et la forte concurrence commerciale entre fabricants concourent à un *raccourcissement des cycles de vie* des produits, voire à leur déploiement prématuré, avant une validation suffisante.

Les erreurs accidentelles liées à l'interaction homme-système constituent potentiellement une source majeure de défaillances de l'informatique diffuse ou, du moins, d'échecs à son déploiement massif. Malgré la taille réduite des dispositifs utilisés, les interfaces doivent être adaptées à des utilisateurs de tous âges et qui n'ont pas nécessairement reçu de formation technique. La diversité des contextes d'utilisation et la furtivité d'une informatique qui se veut « diffuse » accentuent la potentialité de surprises pour ses utilisateurs. Les incompréhensions et les échecs d'utilisation soulignent l'importance de centrer la conception de tels systèmes autour de leurs utilisateurs finaux (*cf.* chapitres VI et VII).

Les possibilités d'attaques et d'utilisations malveillantes de dispositifs d'informatique diffuse sont innombrables, du fait même de leur grande diffusion, de leur utilisation dans des espaces non protégés et de la communication sans fil. Cela concerne aussi bien les malveillances physiques (vol des objets physiques, vandalisme sur des dispositifs disséminés dans la ville ou dans la nature, brouillage des canaux radio) que les attaques logiques hélas déjà devenues chose commune dans les systèmes informatiques plus traditionnels (Internet). Dans cette dernière catégorie de malveillance, on peut mentionner quelques spécificités de l'informatique diffuse : la potentialité de reprogrammer un dispositif physique subtilisé temporairement à son utilisateur dans un endroit public ; les possibilités d'interception, voire d'interposition, offertes par une communication sans fil insuffisamment protégée ; le déni de service par non-coopération entre dispositifs pairs (ex. routage ad hoc). Enfin, la furtivité de l'informatique diffuse, le port d'objets personnels identifiables à distance (ex. étiquettes RFID[1]), la mise en place

[1] RFID : Radio Frequency IDentification

de services géolocalisés ou autres services contextuels, etc., constituent autant de nouvelles menaces pour la vie privée des utilisateurs.

XII.1.2- Contraintes liées à l'informatique diffuse

Au-delà des limitations évidentes de coût, de poids et de volume nécessaires pour des dispositifs portables diffusés en masse, la mise en place de protections contre les différentes menaces (classiques ou nouvelles) est complexifiée par les contraintes imposées par les technologies et les applications de l'informatique diffuse.

Au niveau technologique, les protections à mettre en place sont soumises à des limitations importantes de ressources en terme d'énergie, de bande passante et de capacité de traitement (rendant rédhibitoire, par exemple, l'utilisation de certaines techniques cryptographiques). À ces limitations s'ajoutent d'autres difficultés, représentant autant de défis ardus pour la conception de mécanismes et d'algorithmes de protection adéquats : le dynamisme (défaillances, mobilité, populations de dispositifs de taille variable), la mise à l'échelle (populations non-bornées a priori), la difficulté voire l'impossibilité de distinguer une défaillance d'une perte de contact par mobilité, l'autonomie (modes de fonctionnement déconnectés de toute infrastructure fixe), l'hétérogénéité technologique (matériel, logiciel système, types de connectivité réseau) et fonctionnelle des dispositifs. Enfin, il ne faut pas oublier que les utilisateurs finaux de l'informatique diffuse ne sont pas nécessairement férus de technologie, ce qui constitue un défi supplémentaire quant à leur sensibilisation vis-à-vis des menaces en présence (dichotomie entre ignorance et peur excessive), à l'ergonomie des protections mises en place, ou à la perception de l'efficacité de ces dernières (confiance).

XII.2- Sécurité

Augmenter la confiance des utilisateurs vis-à-vis des technologies, fréquemment invisibles pour l'utilisateur, mises en œuvre dans le cadre de l'informatique diffuse nécessite en premier lieu d'assurer la sécurité de leur utilisation. Au-delà des classiques problèmes liés à la sécurité des environnements d'exécution, qui trouvent ici aussi de nouvelles illustrations comme par exemple la possibilité de transmission de virus par l'utilisation d'étiquettes RFIDs (107), la sécurité de l'informatique diffuse concerne d'abord et avant tout celle des communications et des interactions entre les dispositifs utilisés. En particulier, l'usage généralisé des communications sans fil pour assurer la transparence d'utilisation des dispositifs d'informatique diffuse rend possible la multiplication d'attaques invisibles, aussi bien actives (déni de service, modification des messages échangés) que passives (écoutes). L'auto-organisation de nombreuses structures de communication sans fil, comme les réseaux ad-hoc à sauts multiples (mobiles ou non) et les réseaux de capteurs, nécessite bien évidemment de sécuriser les fonctionnalités de ce type d'organisation (54), en particulier en ce qui concerne le routage comme de nombreux travaux l'ont relevé.

Les utilisations de l'informatique diffuse supposent des scénarios d'utilisation très dynamiques, dans lesquels un utilisateur découvre services et dispositifs dans son environnement immédiat. Cette dynamicité pose deux problèmes spécifiques :

- l'absence de lien entre identité logique (surtout cryptographique, matérialisée par une clé ou un secret) et dispositif physique : comment un humain peut-il être convaincu que le matériel qu'il utilise ou manipule est associé à l'entité logique avec laquelle il pense interagir ou inversement que le dispositif de l'entité se trouve bien devant lui ? Dans beaucoup de scénarios de l'informatique diffuse, l'authentification doit permettre de vérifier la localisation des clés cryptographiques utilisées lors de leur établissement, en particulier en s'assurant de leur proximité.
- l'absence de confiance *a priori* : alors que la sécurité traditionnelle lie la confiance à l'authentification d'une entité, l'absence ou à tout le moins le faible nombre de référentiels de sécurité commun basés sur l'identification des entités logiques découvertes dans l'environnement immédiat pose un problème d'autant plus aigu que de nombreux scénarios supposent des interactions justement très ouvertes.

Les sections suivantes détaillent les approches utilisées pour résoudre ces deux problèmes.

XII.2.1- Établissement d'associations sécurisées

Les différentes solutions proposées jusqu'à maintenant pour assurer l'association sécurisée de dispositifs, c'est-à-dire pour lever toute ambiguïté sur le lien entre entité physique manipulée et identité logique, sont le résultat d'un compromis entre :

- la sécurité effectivement obtenue : il s'agit très souvent de l'assurer par des moyens cryptographiques appropriés.
- la facilité de mise en œuvre de la technologie : une solution peut-elle être intégrée à un dispositif, notamment lorsqu'il est très petit ?
- l'interface homme-machine : la possibilité d'utilisation par des personnes non expertes est critique pour limiter la gêne de l'utilisateur et assurer une intégration aussi transparente que possible dans l'environnement.
- la facilité de déploiement : les solutions détaillées ci-après ne nécessitent pas pour la plupart de distribuer à l'avance un moyen d'établir un secret avec d'autres dispositifs, mais il peut être nécessaire de distribuer par ailleurs des connaissances, même indirectes, sur un dispositif, pour assurer d'autres objectifs de sécurité (voir notamment XII.2.2.2).

XII.2.1.1- Appairage de dispositifs interactifs

Le but de l'appairage ou couplage physique de dispositifs interactifs, notamment les dispositifs personnels de type téléphone mobile ou PDA, est d'assurer la communication sécurisée d'un appareil détenu par un utilisateur avec un dispositif soit personnel, soit disponible dans l'environnement, mais qui ne partage en tout cas pas de contexte ou de secret au préalable. Cette opération est parfois appelée « connexion initiale sûre » (*secure first connect*). Un utilisateur souhaite par exemple s'assurer que son téléphone sans fil sera relié à son point d'accès Wifi mais pas celui de son voisin, ou que ses photos de vacances apparaîtront sur son écran de télévision et pas dans l'appartement d'à côté. Dans l'approche par couplage physique, le dispositif est identifié par une manipulation des appareils identifiables qui soit

simple pour le propriétaire du premier dispositif. De l'appairage résulte l'établissement d'un canal sécurisé entre deux dispositifs.

Le protocole d'établissement de clés de Diffie et Hellman (52) constitue généralement la technique de base pour construire un secret partagé, mais il est d'une part relativement coûteux en calculs, et est d'autre part exposé à une classe d'attaque dénommée attaque par le milieu (ou attaque « *Man-In-The-Middle* ») dans laquelle un adversaire s'authentifie en lieu et place de l'entité attendue. La technique généralement employée consiste en une authentification de chaque partie, qui s'avère généralement impossible en informatique diffuse. Les solutions développées dans ce cadre et présentées ci-dessous visent à s'assurer que l'entité logique avec qui le dispositif personnel interagit est bien associée à un dispositif identifié dans l'environnement de l'utilisateur et non pas à certifier son identité.

S'inspirant des observations éthologiques sur l'imprégnation des animaux, le « caneton qui ressuscite » (116) fut l'une des premières solutions au problème du couplage entre dispositifs sans identification préalable : une phase d'initialisation par connexion filaire entre les deux dispositifs permet d'établir un canal sécurisé de communication, avant que les dispositifs ne puissent communiquer sans fil. Une clé secrète, partagée entre les deux dispositifs, est générée pendant la phase d'initialisation, constituant ainsi un mécanisme d'imprégnation au travers duquel les deux dispositifs se reconnaissent. La connexion physique permet évidemment de supprimer toute possibilité d'attaque par le milieu entre deux boîtiers à condition que le câble utilisé soit correctement blindé. En cas de vente ou de ré-affectation d'un dispositif, il est nécessaire de le reconnecter de manière filaire au nouveau dispositif avec lequel il doit être associé afin de le réimprégner (mort et « résurrection » du caneton). En termes industriels, cette solution simple souffre surtout du besoin de standardiser les connecteurs employés. Cette approche est déjà mise en œuvre, notamment par des fournisseurs d'accès Internet, lors d'une première utilisation de certains appareils multimédia domestiques : le branchement filaire permet de distribuer un secret, par exemple entre un modem ADSL WiFi et une station multimédia.

Balfanz *et al*. (13) proposent un mécanisme d'appairage similaire basé sur l'utilisation de canaux de communication infrarouge pour la connexion initiale entre deux appareils. Le dispositif visé peut ainsi être désigné par l'utilisateur à l'aide de son dispositif personnel, sans qu'il ne soit nécessaire de transporter un câble. Cette approche se révèle cependant moins sûre que la précédente, dans la mesure où il est possible à un attaquant dans la même pièce de détecter des réflexions des échanges infrarouges entre les deux dispositifs et ainsi de monter des attaques par le milieu. Cette technique impose aussi que les ports infrarouges soient en ligne de visibilité mais permet une visée à distance avec des usages établis par la généralisation des télécommandes.

XII.2.1.2- Appairage de dispositifs interactifs avec preuve de proximité

Les approches précédentes permettent à l'utilisateur de s'assurer qu'il a bien ouvert un canal sécurisé avec un dispositif connu et désigné par l'utilisateur. Si elles permettent de se protéger des attaques par le milieu liées au média radio, elles sont cependant sujettes à des attaques par le milieu sur le canal secondaire de

communication : elles ne prouvent notamment pas que le dispositif désigné contienne l'entité logique avec laquelle le dispositif personnel dialogue. Par exemple, si on présente à l'utilisateur un dispositif qu'il n'est pas capable d'identifier pour connecter le câble servant à l'imprégnation (voir plus haut), il y a possibilité que ce dispositif constitue en fait un relais vers le véritable dispositif qui se trouve en un tout autre lieu. Ce type d'attaque, dénommée fraude mafieuse (*mafia fraud*), ouvre notamment la porte à la contrefaçon de dispositifs et met en danger la confidentialité des communications effectuées avec le dispositif authentique.

Les protocoles de vérification de proximité (*distance bounding protocols*) dont le prototype est décrit par Brands et Chaum dans (23) constituent l'approche la plus intéressante pour résoudre le problème de confiance quant au dispositif désigné. Ce type de protocole s'appuie sur la mesure du temps total mis pour envoyer un message de défi à l'entité possédant un secret et pour que la réponse à ce défi soit calculée et renvoyée. Ces protocoles mettent en œuvre une série de défis-réponses successifs afin de diminuer la probabilité de succès d'attaques par un intermédiaire ne connaissant pas le secret. La technique permet ainsi de vérifier que la distance à laquelle on estime se trouver d'un dispositif contenant l'entité logique avec qui une communication est établie est effectivement bornée supérieurement. Cette mesure s'appuie sur la vitesse de propagation des messages, et est mesurée indirectement par le temps écoulé pour répondre à un défi. Il faut noter que cette technique impose une précision de la mesure très importante, surtout dans le cas de mesures basées sur des ondes électromagnétiques. Clulow *et al.* (45) présentent quelques autres protocoles de preuve de proximité et en fournissent une évaluation.

Ce type de protocole a été appliqué à différentes techniques d'appairage. Bussard et Roudier (26, 27) ont d'abord montré comment employer ce type de protocole pour remplacer la technique d'imprégnation du caneton ressuscité et l'intérêt de résoudre les problèmes de fraudes mafieuses dans les systèmes d'informatique diffuse. Ce travail suggère également l'utilisation d'un *token* (un objet physique d'authentification) personnel pour remplacer la connexion de dispositif à dispositif tout en assurant une meilleure mesure de la distance que dans le cas d'utilisation du seul lien radio, notamment en réduisant les erreurs de communication.

La même technique de Brands et Chaum (23) a été appliquée dans (34) puis (35) à la preuve mutuelle de proximité pour deux nœuds exécutant le protocole de Diffie-Hellman. Ce travail vise à n'utiliser que le canal radio et dans ce cadre, la sécurité de l'appairage est légèrement moindre que lorsque la preuve de distance est effectuée par contact comme suggéré dans le cas précédent, puisque l'utilisateur n'a que l'assurance que le dispositif contacté se trouve à l'intérieur d'une sphère centrée sur l'utilisateur et de diamètre connu.

Certains travaux (110, 120) ont proposé d'autres solutions reposant sur des protocoles de preuve de proximité similaires mais s'appuyant sur des messages transmis par ultrasons. L'avantage principal de ces approches est la précision de la mesure qui est de l'ordre du centimètre au lieu de la vingtaine de centimètres comme dans les techniques présentées plus haut.

Contrairement à l'approche décrite ci-dessus, les solutions proposées par les systèmes mobiles et multimédia actuels reposent très largement sur l'authentification

via un canal de communication secondaire, éventuellement de moindre bande passante, mais perceptible par l'utilisateur qui est impliqué dans l'appairage, une approche introduite par Rivest et Shamir (108). En particulier, la tâche de vérifier la proximité de deux appareils est dévolue à l'utilisateur, dans la mesure où il est effectivement capable de s'en assurer par ses propres moyens. Un tel canal de communication secondaire est alors utilisé pour échanger des mots de passe. Naor *et al*. (93) ont montré comment déterminer une taille adéquate pour ces mots de passe, méthode qui peut s'appliquer aux différentes techniques décrites ci-dessous.

L'appairage de dispositifs Bluetooth emploie ce type de mécanisme, bien que cette solution n'est cependant pas adaptée à la plupart des dispositifs utilisés en informatique diffuse, par exemple à cause de la nécessité de disposer d'un écran et d'un clavier simultanément. De plus, dans le cas de dispositifs sans moyen d'entrer de mot de passe, un mot de passe fixe est utilisé, ce qui, indépendamment des faiblesses du protocole, ne protège plus vraiment des attaques par le milieu dès lors qu'on le connaît (par la documentation de l'appareil par exemple).

La comparaison visuelle de chaînes de caractères échangées après un engagement (*commitment*) et simultanément affichées par deux dispositifs comme proposée par (60) ou (32) constitue une variation intéressante mais peu employée de cette approche, notamment parce qu'elle ne nécessite pas de clavier.

SiB (91) propose également une approche analogue, plus simple à mettre en œuvre que les protocoles à preuve de proximité, mais aussi moins contraignante que l'entrée ou la comparaison de mots de passe sur les dispositifs appairés. Ce travail adopte les principes utilisés pour l'appairage Bluetooth, mais en simplifiant l'interface pour la saisie d'un secret partagé. Selon la formule des auteurs, « voir c'est croire » : le premier dispositif, qui doit disposer d'un écran ou d'un moyen d'impression dynamique, y affiche un code barre contenant le condensat (*hash*) de sa clé publique. Le deuxième dispositif, qui doit lui disposer d'une caméra, doit être approché du premier pour photographier son écran, et ainsi récupérer une image interprétable du code barre. Enfin, le premier dispositif transmet au second sa clé publique par le canal de communication radio, clé qui peut alors être vérifiée grâce au condensat récupéré. Ainsi dans ce cas, le canal de communication secondaire est visuel et traduit par l'alignement de la caméra d'un dispositif avec l'écran d'un autre. Cette opération conduit à une authentification unidirectionnelle ou bidirectionnelle selon le nombre d'interactions réalisées. Cette solution n'est évidemment pas applicable aux situations où prendre une photo est impossible ou interdit. Dans une version moins sécurisée, il est possible de coller des étiquettes portant un code-barre sur ou à proximité de chaque appareil avec le risque qu'une telle étiquette soit remplacée par un attaquant. Une version améliorée (112) permet une authentification utilisant non plus un écran mais le clignotement d'une simple diode électroluminescente.

Des approches similaires ont été suivies utilisant des canaux de communication secondaires sonores, puisque microphones et haut-parleurs équipent très souvent toutes sortes de dispositifs. Ainsi on peut transmettre le condensat de la clé publique d'un premier dispositif sous une forme audible par l'utilisateur (par exemple une succession de mots d'un dictionnaire) que ce dernier doit alors comparer au condensat généré à partir de la transmission de la clé publique sur le

canal de communication radio. C'est l'approche suivie par LoudAndClear (65). Cependant, de même que toute solution visuelle est inadaptée aux malvoyants, de par la nature du canal de communication secondaire utilisé, cette technique est inadaptée aux malentendants. Les tentatives d'attaque par le milieu dans ces approches sonores se solderont au pire par un déni de service si les deux dispositifs sont suffisamment près, l'émission de sons simultanés empêchant par exemple la vérification du condensat de la clé publique. D'autres travaux ont au contraire porté sur la transmission sonore directe d'une clé secrète (88) pour sécuriser des communications sans fil ultérieures. Dans ce cas, la sécurité dépend de l'absence d'écoutes dans la zone où se déroule l'échange. Une partie importante de ces travaux porte sur le codage des données sous une forme sonore mélodieuse pour des utilisateurs humains afin d'éviter le rejet de la solution en raison de la gêne qu'elle causerait alors.

XII.2.1.3- Dispositifs non-interactifs

Au-delà des dispositifs bien équipés en termes d'interface homme-machine, l'informatique diffuse concerne aussi de nombreux dispositifs qui en sont dépourvus. Un des thèmes de l'informatique diffuse est justement la disparition de l'ordinateur en tant que machine identifiée et sa diffusion dans toutes sortes d'artefacts. Par conséquent, un grand nombre de dispositifs ambiants, avec qui l'utilisateur doit communiquer ou qui doivent communiquer entre eux, ne peuvent employer les techniques décrites plus haut, alors que cette communication doit aussi être sécurisée. Les nœuds de réseaux mobiles ad hoc ou des réseaux de capteurs constituent par exemple des infrastructures nécessaires dans le cadre des applications d'informatique diffuse nécessitant l'acheminement de données en de multiples sauts. Dans de nombreux cas, les capacités de calcul de ce type de matériel imposent l'utilisation de cryptographie symétrique plutôt que celle de la cryptographie asymétrique combinée à l'authentification du canal établi.

Ce domaine de recherche très actif a notamment abouti à la création de solutions visant à établir un canal sécurisé entre deux dispositifs qui ont été disposés à proximité par l'intervention humaine. L'établissement de telles associations sécurisées nécessite alors une phase d'initialisation préliminaire dans la plupart de ces solutions. Cette phase peut s'appuyer sur la prédistribution de plusieurs clés, de sorte que deux appareils voisins partagent statiquement au moins une clé comme dans (57), ou encore la gestion de clés par grappes sous l'autorité d'un nœud comme dans Secure Pebblenets (15), pour ne citer que quelques-unes des nombreuses propositions faites dans ce domaine. Des techniques non symétriques ont aussi été proposées pour la gestion de clés qui s'appuient sur la prédistribution des clés d'une autorité de nommage et l'utilisation de chiffrement basé sur l'identité (*IBE*) (20).

Une implication plus importante d'un utilisateur humain a aussi été suggérée : l'utilisation de mouvements synchronisés a notamment été expérimentée comme moyen d'appairer deux dispositifs avec l'aide d'un utilisateur dans le système Smarts-It (71) : deux ou plus dispositifs équipés d'accéléromètres s'appairent s'ils partagent les mêmes mouvements, par exemple s'ils se trouvant simultanément dans la poche d'un utilisateur qui marche, ce qui peut être considéré comme une forme d'authentification faible.

Inspiré par cette idée, Casteluccia et Mutaf (37) essayent au contraire d'assurer une authentification forte des deux dispositifs associés. Une version adaptée du protocole d'Alpern et Schneider (5) permet d'établir une clé partagée par les deux dispositifs secoués simultanément. Ce protocole se déroule en une série d'échanges durant lesquels chacun des deux dispositifs envoie à l'autre un message dans un ordre aléatoire. Les deux dispositifs échangent des bits à 1 lorsque la source indiquée dans le message est effectivement le dispositif émetteur et à 0 lorsqu'il indique comme source son partenaire. Le mouvement des dispositifs permet d'empêcher un attaquant éventuel de déterminer lequel des deux nœuds est en train d'émettre en se basant sur la puissance de réception des signaux de l'un et de l'autre. En l'absence de cette connaissance, l'attaquant est incapable de déterminer la valeur du bit échangé puisqu'il ne sait pas lequel des deux dispositifs est en train d'émettre, contrairement au deuxième dispositif récepteur. Il faut noter que l'utilisateur qui appaire les deux dispositifs doit être capable de synchroniser les deux nœuds et de comprendre comment agiter les dispositifs pour éviter à un attaquant de distinguer les deux dispositifs (mouvements qui peuvent être plus complexes que de déplacer les deux nœuds en même temps). Cette technique suppose aussi qu'aucune signature ne caractérise les deux radios (même puissance d'émission en particulier).

Les systèmes d'étiquettes RFID sont encore plus petits et moins puissants que des capteurs. Des protocoles adaptés à ce type de système commencent cependant à apparaître, par exemple Kancke et Kahn (66) décrivent un protocole de preuve de proximité adapté aux systèmes RFID. De nombreux autres problèmes de sécurité liés à l'authentification de ces dispositifs existent, liés en particulier à la protection de la vie privée des utilisateurs (de nombreux exemples sont fournis dans (76)).

XII.2.2- Établissement de la confiance

L'établissement de la confiance repose traditionnellement sur la reconnaissance d'une entité et l'association d'attributs décrivant la confiance qui lui est accordée. Les infrastructures de clé publiques (PKI[2]) qui fournissent ce type de mécanisme jouent ainsi un rôle central dans les réseaux classiques. Les scénarios évoqués dans le cadre du déploiement de l'informatique diffuse suggèrent que dans de très nombreux cas :

- soit il existe des autorités communes capables de certifier des caractéristiques des utilisateurs ou de leurs dispositifs, mais l'identité ne doit pas être dévoilée, de façon à protéger la vie privée des utilisateurs (comme détaillé au XII.3) ;
- soit l'identité des parties en présence n'est d'aucun secours car les entités qui interagissent ne sont pas sous la même autorité et n'ont donc aucune base commune pour établir la confiance.

De nouvelles techniques doivent être appliquées dans ces deux situations :

- pour le premier type de scénario, de nombreux travaux suggèrent l'utilisation de preuves indirectes du contexte ambiant de l'utilisateur ou de son dispositif, en faisant éventuellement appel à des autorités multiples, pour fonder un jugement sur la confiance que l'on peut accorder à un dispositif ou à une entité ;

[2] PKI : Public Key Infrastructure

- la construction de la confiance en s'appuyant sur une évaluation de la coopération de chaque nœud voire l'évaluation du comportement de l'utilisateur humain répondent aux besoins du deuxième type de scénario.

XII.2.2.1- Confiance basée sur des preuves du contexte ambiant

La plupart des mécanismes d'établissement de la confiance adaptés à l'informatique diffuse s'appuient sur l'obtention de preuves d'un certain contexte ambiant. Ces éléments de preuve constituent ainsi généralement des éléments permettant d'évaluer la confiance vis-à-vis d'une entité de manière indirecte sans passer par son identité, mais plutôt par sa localisation, par l'heure d'un accès, par l'identité ou le rôle des nœuds qui l'entourent, etc. On assiste en effet à la naissance d'approches fédératives pour le contrôle d'accès s'appuyant sur des éléments autres que l'identité. Établir des preuves liées à ce type d'éléments peut impliquer l'introduction d'autorités supplémentaires pouvant établir la véracité de telles assertions, ce qui se réalise soit par la collection de « tickets de contexte », soit par l'obtention d'une signature d'une de ces autorités, soit la combinaison de plusieurs de ces preuves. Cette approche peut par exemple permettre d'assurer la présence d'un individu sur un lieu donné à une heure particulière. Les schémas mis en place doivent dans la mesure du possible empêcher que ce type de preuve soit transférable une fois obtenue, ce qui peut nécessiter de les lier à un secret non divulgable.

Cette approche a notamment été très utilisée pour assurer un contrôle d'accès contextuel dans des systèmes d'informatique diffuse. Covington *et al*. (48) s'appuient par exemple sur la définition d'un modèle de contrôle d'accès à base de rôles généralisé (GRBAC[3]) qui crée de nouveaux types de rôles associés aux états du système, appelés rôles environnementaux. Les droits d'un sujet ne sont alors activés que pourvu que les conditions décrites dans les rôles environnementaux associés soient évaluées à vrai : il est par exemple possible de définir un rôle environnemental correspondant à chaque jour de la semaine.

Le système Cerberus (4) vise à sécuriser l'espace intelligent Gaia et fournit des outils supplémentaires pour raisonner sur le contexte, en particulier un moteur d'inférence, et d'accorder un crédit plus ou moins grand à certaines sources de contexte. Les politiques de sécurité y sont, quant à elles, exprimées par des ensembles de règles en logique du premier ordre.

Le raisonnement sur le contexte s'appuie de plus en plus fréquemment sur l'utilisation de descriptions sémantiques élaborées, notamment à base d'ontologies. C'est par exemple le cas du contrôle d'accès dans le système MOSQUITO (64) qui introduit des critères d'activation de règles XACML[4] s'appuyant sur une description du contexte écrite dans le langage d'ontologie CoOL[5].

Le contrôle d'accès nécessite également la gestion de délégations afin d'assurer que les autorisations ne se diffusent dans le système que selon le principe du moindre privilège, en particulier en ce qui concerne leur durée de validité notamment afin de limiter les besoins de révocation de certificats. On constate ainsi

[3] GRBAC : Generalized Role-Based Access Control

[4] XACML : eXtensible Access Control Markup Language

[5] CoOL : Context Ontology Language

le développement de systèmes de délégation décentralisés comme ceux décrits par exemple dans (123).

Asokan et Ginzboorg proposent l'utilisation du chiffrement pour assurer le contrôle d'accès à des documents au sein d'un groupe constitué de manière ad-hoc. La proposition (9) suggère le chiffrement faible basé sur le partage d'un mot de passe pour permettre aux personnes présentes dans une même pièce d'établir une clé partagée entre les dispositifs des membres du groupe. Les utilisateurs sont donc responsables de vérifier le contexte et notamment si les personnes qui les entourent sont effectivement dignes de confiance et peuvent participer au groupe. La sécurité de la solution dépend aussi des risques liés au mode d'échange du mot de passe initial (et suppose en particulier que seules les personnes visibles dans la pièce puissent connaître le mot de passe) mais aussi de ceux liés à son mode de saisie (les caractères tapés sur un clavier génèrent des signaux électromagnétiques pouvant être détectés dans une pièce voisine (82)). D'autre part, si cette solution convient bien à des ordinateurs portables ou assistants personnels, elle n'est pas adaptée aux dispositifs sans clavier par exemple.

L'utilisation de systèmes de navigation mondiaux tels le GPS (*Global Positioning System*) est fréquemment évoquée comme moyen de récupérer la localisation, élément le plus important pour définir le contexte. Son utilisation nécessite cependant des précautions, d'autant qu'il peut être sujet à des attaques comme décrit par exemple dans (75). De nombreuses approches ont été proposées (voir (70)) et la sécurisation de cette fonction commence à trouver des solutions comme décrit dans (35).

Des travaux comme (94) ou (79) ont également suggéré l'utilisation de la proximité plutôt que de la localisation absolue : la possession de *tokens* personnels permettrait ainsi de donner accès à une machine seulement quand l'utilisateur s'en approche. Disposer de preuves robustes dans ce domaine suppose vraisemblablement d'intégrer des preuves de proximité aux protocoles développés. S'il s'agit de contrôler l'accès d'un utilisateur, les techniques décrites plus haut sont cependant vulnérables aux attaques dites de fraude terroriste (*terrorist fraud*), non évitables par le seul protocole de Brands et Chaum (23) par exemple. Dans ce type d'attaque, le relais et le dispositif distant sont en collusion pour soumettre une fausse preuve concernant la localisation du dispositif autorisé, mais en réalité distant. Certains travaux (29, 30, 113) montrent comment intégrer des preuves de proximité qui ne sont pas vulnérables à ce type d'attaque. Certains chercheurs comme Kevin Warwick[6] ont même poussé ce concept jusqu'à expérimenter l'implantation de dispositifs RFID sous la peau pour contrôler l'accès à des pièces ou à des bâtiments, allumer la lumière, etc. Cette dernière technique soulève cependant de sérieux problèmes éthiques et de protection de la vie privée.

XII.2.2.2- Confiance basée sur l'évaluation de la coopération

L'informatique diffuse s'appuie sur des infrastructures auto-organisées offrant des ressources traditionnellement centralisées (réseaux ad hoc multisauts fournissant routage ou acheminement de paquets comme décrit au XII.4.4, stockage, sauvegarde, etc.). En particulier, on note dans ce cadre l'apparition d'un nouveau

[6] http://www.kevinwarwick.com/

type d'attaque, l'attaque par égoïsme, dans laquelle un nœud de l'infrastructure essaie de profiter des ressources collaboratives sans y apporter sa contribution. C'est par exemple le cas d'un nœud qui cherche à économiser ses ressources énergétiques et qui n'achemine pas les paquets qu'un voisin lui transmet. Évaluer et inciter à la coopération constituent évidemment un préalable important pour pouvoir assurer que de telles infrastructures peuvent fonctionner. On distingue essentiellement deux grands mécanismes d'incitation : la réputation (bonne ou mauvaise) et la rémunération (ou l'amende dans sa version punitive).

De nombreux travaux ont employé des techniques de réputation, assez simples à mettre en œuvre, afin de sécuriser le routage dans les réseaux mobile ad hoc ces dernières années. On peut citer de manière non exhaustive Watchdog/Pathrater (89), CORE (92) ou CONFIDANT (25).

La rémunération est une approche qui nécessite souvent plus de précision dans la détermination du prix d'un service. Cette technique a par exemple été proposée sous le nom de Nuglets (31) pour assurer l'acheminement de paquets dans des réseaux mobiles ad hoc : l'envoi de paquets suppose d'évaluer la distance à parcourir et de provisionner un nombre suffisant de crédits pour assurer l'acheminement de paquets de nœud en noeud. Ce travail suppose par contre l'utilisation de noyaux sécurisés (*tamper-resistant hardware*) afin d'assurer un échange équitable.

Au niveau applicatif, une approche entièrement algorithmique est proposée dans (28), basée sur les schémas de monnaie électronique de Chaum (40) qui consiste à distribuer des certificats utilisables en une seule occurrence par des utilisateurs, par ailleurs complètement inconnus. En cas de double présentation de ce type de certificat, de l'argent qui a été caché dans le certificat devient récupérable et son prélèvement sert à punir l'utilisateur. Le versement préalable d'un dépôt constitue donc la seule base de la confiance et la seule incitation à la coopération pour l'utilisateur.

XII.2.2.3- Confiance basée sur l'évaluation du comportement

Une dernière approche vise à évaluer le comportement de l'utilisateur ou de ses dispositifs à l'aune d'un « standard social », alors que dans l'approche précédente, on vise plutôt à inciter l'utilisateur à adopter une certaine attitude vis-à-vis de services coopératifs, en l'éliminant éventuellement du système par le jeu des incitations utilisées. L'observation du comportement peut porter sur les dispositifs utilisés (suivi d'une trajectoire d'étiquette RFID par exemple) voire sur leurs utilisateurs humains. La confiance dépend alors de l'établissement d'un profil standard de comportement : des travaux sur la surveillance des lieux et des personnes ont notamment été l'objet d'investigation s'appuyant sur l'analyse de trajectoires physiques (par exemple (102)). Ces travaux soulèvent cependant d'importantes questions concernant la protection de la vie privée, en particulier si les informations comportementales recueillies sont croisées avec des moyens d'identification numériques, comme discuté dans la section suivante.

XII.3- Protection de la vie privée

L'article premier de la loi « Informatique et libertés » (86) établit que « *L'informatique doit être au service de chaque citoyen.* […] *Elle ne doit porter*

atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». Ceci doit s'appliquer à l'informatique diffuse comme à l'informatique plus traditionnelle. D'ailleurs le droit au respect de la vie privée est considéré, dans nos sociétés, comme un droit fondamental (38, 97), ce qui a conduit à une réglementation internationale riche sur la protection des données personnelles (53, 86 , 95, 98). Pourtant, malgré cette réglementation, les citoyens et les consommateurs considèrent que les nouvelles technologies représentent un danger pour leur vie privée, et le développement de l'informatique diffuse risque d'être perçu par le public comme un instrument au service de « *Big Brother* » (99). Il est donc nécessaire de développer des technologies qui permettent de garantir la protection des données personnelles, et ainsi regagner la confiance du public.

À première vue, la vie privée devrait pouvoir être protégée par des moyens classiques de sécurité informatique : au fond, il ne s'agit de garantir que la confidentialité de données ou de méta-données personnelles[7] (50), et la section précédente (*cf.* XII.2) a montré qu'il existe de nombreuses techniques pour protéger la confidentialité des informations dans l'informatique diffuse. Mais « *le diable se niche dans les détails* » des techniques de sécurité : ainsi, pour contribuer à prouver qu'une action est légitime (ou non), il faut parfois collecter et conserver beaucoup d'informations qui peuvent nuire à la vie privée. D'autre part, le développement actuel des techniques de traçabilité et d'authentification forte se justifie par un souci d'améliorer la sécurité, mais il met en danger la vie privée des utilisateurs.

Les *critères communs* (73) définissent la protection de la vie privée (*privacy*) comme une classe de fonctionnalité, avec quatre sortes d'exigences :

- l'*anonymat* (*anonymity*) exige que d'autres utilisateurs ou sujets soient incapables de déterminer l'identité d'un utilisateur associé à un sujet ou à une opération ;
- la *possibilité d'agir sous un pseudonyme* (*pseudonymity*) exige qu'un ensemble d'utilisateurs ou de sujets soit incapable de déterminer l'identité d'un utilisateur associé à un sujet ou à une opération, mais que cet utilisateur réponde quand même de ses actions ;
- l'*impossibilité d'établir un lien* (*unlinkability*) exige que des utilisateurs ou des sujets soient incapables de déterminer si le même utilisateur a déclenché certaines opérations spécifiques dans le système ;
- la *non-observabilité* (*unobservability*) exige que des utilisateurs ou des sujets ne puissent pas déterminer si une opération est en cours d'exécution.

Ce sont ces exigences que devraient permettre de satisfaire les technologies de protection de la vie privée (PET[8]) pour améliorer la confiance des utilisateurs, et nous verrons que certaines de ces technologies pourraient exploiter de nouveaux dispositifs personnels issus de l'informatique diffuse. L'informatique diffuse

[7] Les méta-données sont des informations (gérées par les systèmes d'information et de communication) qui ne sont pas directement accessibles ou manipulables par les utilisateurs : par exemple, des adresses informatiques, des identifications de processus, l'instant auquel se déroule une opération, etc. Certaines de ces informations peuvent avoir un caractère personnel : par exemple, une adresse IP permet souvent d'identifier une personne.

[8] *Privacy-Enhancing Technologies*

présente donc des menaces nouvelles vis-à-vis de la vie privée (*cf.* XII.1.1), mais elle offre aussi des opportunités pour mieux la protéger.

L'implémentation de ces technologies ne doit bien sûr pas aller à l'encontre d'autres exigences critiques, comme la lutte contre la criminalité. Par exemple, l'usage de pseudonymes (avec les propriétés indiquées ci-dessus) doit être préféré à un anonymat total : les PET devraient protéger les utilisateurs légitimes vis-à-vis d'entreprises ou d'agences qui tenteraient de violer leur vie privée, mais ne doivent pas aider des criminels à perpétrer des actions illégales en toute impunité. Cela est possible si les PET sont fournies et maintenues sous le contrôle de citoyens honnêtes, qui coopèrent avec les autorités judiciaires dûment habilitées, mais qui refuseraient de divulguer des informations personnelles de façon abusive à d'autres parties.

Les technologies de protection de la vie privée visent donc à empêcher quiconque d'utiliser de façon abusive les données et méta-données qui se rapportent à une personne. Avant de décrire plus en détail ces technologies, nous allons d'abord établir les principes fondamentaux qui les sous-tendent (51).

XII.3.1- Principes fondamentaux

Il est important de considérer que les données personnelles appartiennent à la personne à laquelle elles se rapportent, et qu'elles n'appartiennent pas au propriétaire du système qui stocke ou traite ces données. Par exemple, on reconnaît généralement, au moins en Europe, que le dossier médical appartient au patient, et non pas au médecin qui le crée ou le met à jour, ni à l'hôpital qui le conserve dans ses fichiers. En tant que propriétaire de ses données personnelles, tout individu doit pouvoir exercer sa souveraineté sur ces informations. Ceci signifie que les données personnelles ne devraient être stockées que sur des dispositifs directement sous son contrôle, plutôt que sur des serveurs ou des dispositifs qu'il ne contrôle pas. Ceci ouvre des champs d'application nouveaux à l'informatique diffuse, par le développement de dispositifs personnels (ordinateurs portables, assistants numériques personnels, téléphones portables, cartes à puce), suffisamment sûrs pour stocker des informations personnelles sensibles et contrôler efficacement leurs accès[9].

Bien sûr, pour profiter de certains services, il faut parfois divulguer des données personnelles à un tiers, mais une telle divulgation doit se limiter au *besoin d'en connaître :*

- Ne devraient être divulguées que les seules données strictement nécessaires pour l'accomplissement de la tâche décidée ou acceptée par la personne (principe de *minimisation des données personnelles*).
- Le tiers devrait garder confidentielles ces informations, ne devrait y accéder que pour réaliser la tâche désignée par la personne, et devrait les effacer dès qu'elles ne sont plus nécessaires à l'accomplissement de cette tâche. Plus

[9] Ce stockage de données sur un dispositif personnel n'exclut pas une sauvegarde sur un serveur distant, de façon à permettre de réinitialiser un tel dispositif en cas de perte, de destruction ou de vol. Mais cette sauvegarde doit être protégée (par exemple, par chiffrement) pour empêcher que même le serveur de sauvegarde puisse accéder à des données personnelles sensibles.

généralement, le tiers doit respecter les exigences posées par le propriétaire des données (principe de *souveraineté sur les données personnelles*).

XII.3.1.1- Minimisation des données personnelles

La première mesure de minimisation consiste, pour l'utilisateur, à ne divulguer que les informations qui sont réellement nécessaires pour remplir la tâche considérée, et ces informations ne devraient être divulguées qu'aux seules parties qui en ont besoin. Prenons un exemple simplifié d'une transaction d'achat sur Internet, impliquant un client, un marchand, une entreprise de livraison, la banque du client et celle du marchand. Le marchand a besoin de savoir ce qui est acheté, et il doit être sûr qu'il sera payé pour cet achat (validité du moyen de paiement), mais il n'a pas besoin de connaître l'identité de l'acheteur, la banque de cet acheteur, l'adresse de livraison, etc. L'entreprise de livraison doit connaître l'adresse de livraison et éventuellement l'identité du destinataire (qui n'est pas nécessairement l'acheteur), ainsi que les caractéristiques physiques de l'objet acheté (poids, dimension, si c'est fragile ou pas, etc.), mais elle n'a pas à en connaître le prix d'achat, qui l'a acheté, etc. La banque du marchand doit savoir quel montant doit être viré et depuis quelle banque, mais n'a pas à connaître l'identité de l'acheteur ni même son numéro de compte, ce qui a été acheté, etc. La banque de l'acheteur doit connaître le montant à virer ainsi que la banque et le numéro de compte du marchand, mais pas ce qui a été acheté, ni l'adresse de livraison, etc. Dans cet exemple, aucune des parties n'a besoin de collecter toutes les informations personnelles relatives à cette transaction ; ces informations sont fragmentées et distribuées entre les parties, et ceci contribue à la confidentialité des données personnelles (58).

Ce principe de minimisation doit aussi s'appliquer à l'informatique diffuse. Si on prend l'exemple d'un réseau de capteurs biométriques collectant des informations liées à la santé (taille, poids, température, pression artérielle, etc.), ces informations ne devraient pas être enregistrées dans le réseau, mais de préférence transmises et stockées sur un dispositif personnel, sous le contrôle de l'individu auquel elles se rapportent.

Même quand l'identité d'une personne est nécessaire et doit être vérifiée (authentification), cette personne doit pouvoir sélectionner laquelle de ses identités elle désire divulguer (voir XII.3.2.1), de façon à se prémunir contre des liens qui pourraient être établis abusivement. Mais très souvent, des données personnelles sont collectées, traitées et redistribuées alors qu'il n'y a pas d'utilité à les relier à une personne identifiée. C'est le cas, par exemple, quand des données médicales sont rassemblées dans un but de recherche sur l'efficacité de nouveaux traitements, ou pour procéder à des études épidémiologiques, ou encore pour améliorer les ratios efficacité/coût des soins médicaux. De telles données médicales sont des informations personnelles très sensibles, et doivent donc être anonymisées pour protéger la vie privée des patients : l'étude qui utilise ces données peut avoir besoin d'informations très détaillées sur les trajectoires de soins, voire les antécédents familiaux, etc., mais pour autant il n'est pas nécessaire de connaître la personne à qui ces données se rapportent. Dans certains cas, les données d'un même patient peuvent devoir être collectées par des établissements différents (hôpitaux, cabinets médicaux, …), et à différents moments, et pourtant être identifiées comme reliées au

même patient, sans pour cela divulguer l'identité réelle de ce patient. Ceci nécessite la création d'un *identifiant anonyme*, unique pour chaque patient, qui soit commun aux différents lieux et instants de collecte des informations. Un tel identifiant anonyme devrait être généré de façon à empêcher toute inversion abusive du processus d'anonymisation, c'est-à-dire la ré-identification d'une personne à partir de son identifiant anonyme. Pourtant, dans certains cas, il peut être utile, voire vital, de « désanonymiser » l'identifiant pour réidentifier le patient, par exemple quand un nouveau traitement a été découvert pour une maladie diagnostiquée à partir des données médicales anomymisées. Une technique d'anonymisation a été développée (1) pour contrôler la possibilité d'établir un lien entre les données anonymiseées correspondant à un même patient et pour donner au patient le contrôle sur le processus de désanonymisation.

Les données personnelles anonymisées doivent elles-mêmes parfois être minimisées, en particulier pour empêcher des attaques par inférence, qui permettraient d'identifier une personne à partir de données anonymes. Par exemple, la connaissance des semaines de naissance de deux frères ou sœurs suffit pour identifier de façon unique leur mère dans une grande population (celle de la France, par exemple). Il peut donc être nécessaire de réduire la précision de données personnelles anonymes, par appauvrissement des données ou par filtrage. Par exemple, il peut être souhaitable de remplacer une date de naissance par un âge ou une tranche d'âge, un code postal par un code de région, etc. Bien sûr, il faut établir un bon compromis entre la protection de la vie privée et la nécessité d'avoir des informations suffisamment précises pour réaliser l'étude pour laquelle elles sont collectées (selon aussi le principe du besoin d'en connaître). Le filtrage et l'appauvrissement peuvent s'appliquer à toutes sortes de données personnelles, de façon à permettre à un utilisateur de ne transmettre que la quantité d'information nécessaire pour réaliser une transaction acceptable par l'ensemble des parties impliquées.

XII.3.1.2- Souveraineté sur les données personnelles

Quand des données personnelles se trouvent sur un système d'information qui n'est pas sous le contrôle direct de la personne concernée (typiquement, un serveur d'une entreprise ou administration), soit pour un court moment (par exemple l'exécution d'une simple transaction), soit pour plus longtemps (par exemple des dossiers médicaux dans un hôpital), l'accès à ces données devrait être strictement limité à l'usage souhaité par leur propriétaire, c'est-à-dire la personne correspondant à ces données. Cela signifie que le propriétaire des données doit pouvoir imposer une politique de protection de la vie privée sur ses données et que le serveur qui conserve et traite ces données doit mettre en œuvre cette politique par des mécanismes de contrôle des accès adéquats. La politique en question peut définir des permissions et des interdictions précisant qui peut ou ne peut pas réaliser quelle opération sur ces données personnelles. Mais cette politique peut aussi définir des obligations précisant, par exemple, que les données expirent (et donc doivent être effacées) après un délai donné suivant la terminaison de la transaction, ou que la divulgation de ces données à un tiers doit être notifiée au propriétaire par courriel, etc. Bien sûr, la politique de vie privée imposée par le propriétaire des données doit être compatible avec la politique de sécurité qui protège les biens de l'entreprise et

gouverne l'exécution de l'application, et donc les accès effectifs aux données. La compatibilité entre ces deux politiques doit être vérifiée avant la divulgation par l'utilisateur de ses données personnelles[10].

Rappelons que, légalement (86), le propriétaire du serveur est responsable de la sécurité des données personnelles qu'il héberge, et peut être poursuivi s'il ne protège pas correctement ces données contre des malveillances (internes ou externes). Il est donc important d'implémenter des mécanismes de sécurité capables de mettre en œuvre efficacement à la fois les exigences de vie privée des utilisateurs et la politique de sécurité de l'entreprise. Ceci peut se faire en utilisant des mécanismes de contrôle d'accès conventionnels, et une conception rigoureuse des logiciels d'applications et des procédures d'opération. Mais cela peut aussi être facilité par des mécanismes dédiés, tels que des médiateurs d'accès aux données, capables de mettre en œuvre des *politiques indétachables* (*sticky policies*) associées à chaque donnée personnelle élémentaire, sous forme d'une étiquette indétachable. L'article (36) présente une telle architecture, utilisant un chiffrement basé sur l'identité (*Identity-Based Encryption*), alors que la thèse (12) propose une technique similaire, basée sur les politiques.

Il est important de donner confiance à l'utilisateur que ses données sont bien gérées conformément à ses exigences. Ceci peut être obtenu si une organisation de contrôle, indépendante et digne de confiance, réalise un audit du serveur et de ses procédures opérationnelles, puis émet un certificat garantissant que le serveur respecte la politique de protection de la vie privée qu'il proclame. Mais cela peut aussi être supporté par du matériel et du logiciel dignes de confiance, comme ceux qui sont promus par le *Trusted Computing Group*[11]. Ainsi, avec un dispositif matériel résistant aux attaques physiques, tel que le *Trusted Platform Module* (TPM), il est possible pour un utilisateur distant de vérifier qu'un TPM est utilisé, et que le serveur n'exécute aucun logiciel autre que des logiciels certifiés comme satisfaisant les exigences de protection de la vie privée.

XII.3.2- Technologies pour protéger la vie privée

Nous présentons ici quatre types de technologies permettant de mieux protéger la vie privée, en particulier dans l'informatique diffuse.

XII.3.2.1- Gestion d'identités virtuelles multiples

Pour qu'une personne puisse protéger sa vie privée, il est important de cacher ou de réduire autant que possible les liens entre cette personne et les actions et données correspondantes. Par exemple, si une personne est le seul utilisateur d'un ordinateur connecté à Internet avec une adresse IP fixe[12], il est possible pour un observateur de relier toutes les informations émises depuis cette adresse IP à cette personne : l'adresse IP peut alors être considérée comme un identifiant unique, c'est-à-dire qu'il est propre à une seule personne. De tels identifiants uniques permettent d'établir un lien entre différentes actions indépendantes réalisées par la même

[10] Voir, par exemple, l'action P3P <http://www.w3.org/TR/P3P/>.

[11] https://www.trustedcomputinggroup.org/home/

[12] Le fait qu'un utilisateur a toujours (ou souvent) la même adresse IP peut s'observer facilement, par exemple dans les en-têtes des courriels qu'il envoie.

personne, ou entre des ensembles d'informations liées à la même personne. C'est donc une menace directe contre la vie privée, et en particulier contre la troisième exigence des critères communs présentés en début de section XII.3.

Un moyen pour réduire les risques d'établissement de tels liens consiste à utiliser des communications anonymes (voir XII.3.2.2) et des accès anonymes aux services (*cf.* XII.3.2.3). Mais bien souvent c'est insuffisant, puisque pour obtenir un service personnalisé, l'utilisateur doit se faire reconnaître avec une *identité*. L'identité peut être définie comme la représentation d'une personne pour un service. Cette fois encore, si une personne accède à plusieurs services sous la même identité, il est possible d'établir un lien entre ces accès. Aussi est-il souhaitable d'avoir des identités virtuelles[13] (ou *pseudonymes*) multiples pour accéder à des services multiples. Bien sûr, chaque personne doit pouvoir sélectionner quelle identité utiliser pour chaque service, et doit pouvoir gérer la validité temporelle de ses identités : si la même identité est utilisée pour plusieurs accès à un ou plusieurs services, il est possible d'établir une correspondance entre ces accès, et cette correspondance peut être plus ou moins sensible du point de vue de la vie privée. L'utilisateur devrait donc pouvoir définir une date d'expiration pour chacune de ses identités, les deux choix extrêmes étant une *identité valide une fois* (une nouvelle identité doit être générée à chaque accès) et une *identité permanente*.

Différentes identités peuvent être utilisées pour différents niveaux d'exigences vis-à-vis de la vie privée. Par exemple, certaines identités virtuelles ne servent qu'à permettre d'enregistrer certaines préférences de l'utilisateur, sans que ce soit des données personnelles directement identifiantes (ou *à caractère nominatif*). Pour un service de météo par exemple, ce sera la ville préférée, ou les unités à utiliser par défaut (degrés Celsius ou Fahrenheit, miles ou kilomètres, etc.). En revanche, d'autres identités pourraient être dédiées aux accès à des services sensibles, tels que ceux de déclaration d'impôts ou de vote électronique, etc. La vérifiabilité des identités doit être directement liée à la sensibilité des services : aucune authentification n'est utile pour accéder à un service non sensible qui ne stocke ni ne gère aucune donnée personnelle, alors qu'une authentification forte devrait être exigée pour des services sensibles, de façon à empêcher toute usurpation d'identité. De plus, un utilisateur devrait sélectionner des identités différentes pour accéder à des services sensibles différents. Par exemple, il faudrait utiliser des identités différentes, sans lien direct mais à forte authentification, pour déclarer ses impôts et pour s'inscrire sur des listes électorales, de façon à se prémunir contre d'éventuels abus de certaines administrations ou gouvernements. En particulier, les citoyens ne devraient pas utiliser les mêmes certificats à clés publiques (par exemple stockés sur une carte d'identité nationale électronique) pour l'accès à ces deux services publics.

La gestion, par un utilisateur, de ses multiples identités est un problème qui peut être complexe (72), et pourtant elle doit être rendue suffisamment facile pour être utilisable et compréhensible par chaque individu, quelles que soient ses aptitudes techniques. Ceci est l'un des défis majeurs du projet européen PRIME (*Privacy and Identity Management for Europe*)[14]. Dans ce cadre, les technologies

[13] On parle d'identité *virtuelle*, par opposition avec l'identité *réelle*, c'est-à-dire celle qu'on a dans le monde réel, celle de l'état-civil par exemple.

[14] <http://www.prime-project.eu/>

d'informatique diffuse (en particulier grâce aux nouvelles formes d'interaction homme-machine, *cf*. chapitre VI) devraient pouvoir être utilisées pour développer des dispositifs personnels permettant à n'importe qui de gérer facilement ses identités virtuelles multiples.

XII.3.2.2- Communications anonymes

L'écoute passive de communications est une menace importante contre la vie privée puisque, même si le contenu d'une communication peut être chiffré, la simple observation des adresses source et destination (dans les paquets IP, par exemple) peut révéler des informations sensibles. En effet, une adresse IP identifie à un instant donné une machine qui peut n'avoir qu'un seul utilisateur ou un petit nombre d'utilisateurs, et donc identifie une personne ou un petit groupe de personnes. D'autre part, cette adresse est utilisée pour le routage des paquets dans le réseau, et correspond donc à une localisation géographique. Il est donc aisé, en observant simplement un paquet, de savoir qu'une personne est présente à un moment donné en un lieu donné. Ce risque est encore plus important dans le cadre de l'informatique diffuse, puisque les communications sans fil sont faciles à capter, et qu'une personne peut posséder de nombreux dispositifs personnels, chacun pouvant avoir une adresse IP fixe[15]. Il suffit dès lors de capter un paquet émis par l'un de ces dispositifs pour déduire que la personne est présente à proximité.

En 1981, David Chaum a introduit le problème de l'analyse de trafic dans les réseaux comme Internet, en soulignant que la vie privée des utilisateurs était en danger dès lors qu'un observateur peut déterminer l'existence d'une communication ou identifier deux personnes qui communiquent entre elles (39). Pour empêcher l'analyse de trafic, il a présenté un protocole utilisant des routeurs qu'il a appelés *MIX*, qui cachent le lien entre les messages entrants et sortants. Dans ce cas, si Alice veut communiquer avec Bob de façon anonyme, elle chiffrera son message avec la clé du MIX et l'enverra au MIX, qui le déchiffrera, identifiera le destinataire, Bob, et lui redirigera le message déchiffré. Un attaquant qui observerait toutes les communications ne pourrait dès lors distinguer Alice des autres personnes qui émettent des messages vers le MIX, ni Bob des autres destinataires de messages issus du MIX[16].

David Chaum a aussi proposé de réaliser des communications anonymes à l'aide de réseaux pair à pair, les DC-nets (41). De tels réseaux pourraient bénéficier des communications par diffusion offertes par les réseaux sans fil, mais leur mise en œuvre pratique nécessiterait des protocoles complexes si les communications sont peu fiables ou si les connexions/déconnexions sont fréquentes (2), ce qui est le cas général dans l'informatique diffuse (*cf*. XII.4.2 et XII.4.4).

Il existe une autre solution pour garantir que les adresses IP ne puissent être utilisées pour établir des liens entre les personnes et les actions qu'elles réalisent : l'adressage dynamique. Dans ce cas, l'adresse d'un dispositif doit être générée dynamiquement (tirée de préférence aléatoirement dans un large espace d'adressage,

[15] Par exemple, IPv6 propose que chaque dispositif ait une adresse IP implicite fixe, dérivée de l'adresse MAC de l'interface réseau utilisée, cette adresse MAC étant généralement unique et fixée par le fabricant de l'interface.

[16] Ceci suppose que le MIX mélange (d'où son nom) les différents messages qu'il reçoit avant de les réémettre dans un ordre aléatoire.

partagé avec de nombreux autres utilisateurs), lorsque le dispositif se connecte. Cette allocation dynamique d'adresse peut être réalisée soit par un serveur (par exemple DHCP), soit par le dispositif lui-même (à condition de pouvoir garantir l'unicité de cette adresse dans le réseau considéré). Ceci conduit à séparer totalement identification et adressage.

Pour illustrer certaines de ces techniques, prenons un exemple simple, où un utilisateur nomade veut établir une connexion entre son ordinateur portable et son fournisseur d'accès Internet (FAI) sans que ce dernier ne puisse connaître sa localisation. Dans ce scénario, l'ordinateur se connecte par WiFi à une borne publique d'un autre fournisseur d'accès, dans lequel l'utilisateur n'a pas confiance, sinon pour relayer ses communications. On suppose aussi l'existence de mandataires (*proxies* en anglais), tiers de confiance indépendants des fournisseurs d'accès, auxquels chaque utilisateur peut s'abonner pour garantir certaines propriétés de protection de la vie privée. Dans ce cas, la connexion entre l'utilisateur et son FAI peut s'établir de la façon suivante :

1. L'ordinateur portable génère aléatoirement une adresse MAC qui sera utilisée pendant toute la session par son interface 802.11.
2. L'ordinateur établit une connexion sans fil à la borne et reçoit une adresse IP temporaire (générée par le serveur DHCP de la borne).
3. Utilisant cette connexion IP, l'ordinateur établit un tunnel (par exemple SSH) vers le mandataire qu'il a choisi. L'authentification de l'utilisateur par le mandataire (et réciproquement) est incluse dans la négociation de session du tunnel.
4. Le mandataire établit (à la demande de l'utilisateur) une nouvelle connexion avec le FAI de l'utilisateur, et sert de relais entre le tunnel et le FAI.
5. L'utilisateur s'authentifie auprès de son FAI (à travers le relais du mandataire). À partir de ce moment, le FAI est sûr de l'identité de l'utilisateur, mais ne peut déduire de la connexion IP quelle est la localisation du client : il ne connaît que l'adresse IP du mandataire, pas celle de la borne ni de l'utilisateur. De même, le fournisseur de la borne n'a aucune information sur l'identité de l'utilisateur (ni sur ses équipements à part le protocole utilisé, ni sur son fournisseur d'accès), il peut seulement identifier qu'un utilisateur nomade inconnu se connecte au mandataire et communique avec lui.

XII.3.2.3- Accès anonyme à des services

Utiliser des communications anonymes ne suffit pas pour obtenir un accès anonyme à un service : les messages envoyés au fournisseur de service peuvent contenir des informations identifiantes, qui doivent être effacées ou transformées par un mandataire (voir plus haut) avant qu'elles ne soient transmises au fournisseur. Cette transformation dépend de la sémantique du message (c'est-à-dire de la signification de son contenu), et la tâche peut donc être très ardue. Si le mandataire est dédié à un service spécifique, il est relativement aisé d'analyser la syntaxe des en-têtes, par exemple, pour éliminer une partie des informations sensibles.

Cependant, la structure des messages requis par la plupart des services peut être très variable, et donc très difficile à anonymiser.

Décider quelle partie du message devrait être modifiée est une première difficulté quand on essaie d'anonymiser un message d'application. Une autre difficulté est de savoir comment le modifier. Certaines informations peuvent être simplement effacées ou remplacées par des valeurs génériques. Par exemple, pour les accès Web, des informations comme le type de système d'exploitation ou de navigateur Web, la dernière page visitée, etc., peuvent être remplacées par des informations génériques non sensibles. Les informations à caractère nominatif peuvent souvent être remplacées par des pseudonymes (voir XII.3.2.1), ce qui est fait, par exemple, par les relais d'anonymisation de courrier électronique lorsqu'ils remplacent les adresses de courriel par des alias. Mais certains contenus doivent être maintenus tels quels, par exemple pour l'autorisation, et ne peuvent donc pas être remplacés (ce qui peut ne pas poser de problèmes si les mécanismes d'autorisation préservent la vie privée, comme ceux qui sont proposés dans la section suivante).

En pratique, il faut développer des mandataires spécifiques à chaque type d'application. Prenons l'exemple d'un service basé sur la localisation[17] pour des utilisateurs de téléphones GSM. Un tel service pourrait par exemple indiquer comment se rendre à la pharmacie la plus proche, ou consulter les menus des restaurants du quartier et réserver une table dans l'un d'entre eux, ou encore fournir les programmes des cinémas et réserver une place, etc. Dans un tel scénario, les différentes parties sont :

1. L'*utilisateur* avec son téléphone GSM.
2. L'*opérateur de télécommunications GSM*, qui peut identifier le client (par la carte SIM du téléphone), et qui connaît la localisation du client (par l'identification de la cellule), mais ne devrait rien connaître du service de localisation demandé par son client (information sensible).
3. Un *fournisseur de service lié à la localisation*, qui ne doit pas connaître l'identité du client (directement ou indirectement, pas même l'identification de l'opérateur), mais seulement la localisation pour laquelle on lui demande un service.
4. Un *mandataire* (tiers plus ou moins de confiance), qui connaît le numéro de téléphone du client et l'adresse IP du fournisseur de service, mais pas la localisation du client, ni les contenus de la requête de service et de la réponse correspondante[18].

Le déroulement d'une transaction serait le suivant[19] :

1. Le téléphone du client obtient sa localisation (soit par GPS, soit par l'identification de la cellule GSM à portée de laquelle il se trouve), et ainsi construit sa requête vers le fournisseur de service de localisation. Il génère

[17] Cet exemple est une simplification d'un service opérationnel développé dans le cadre du projet PRIME.

[18] Si le service de localisation est payant, ce mandataire peut aussi servir d'intermédiaire pour garantir le paiement au fournisseur de service de localisation, soit par débit d'un compte prépayé du client auprès du mandataire, soit sur la facture GSM du client (avec bien sûr l'accord du client et de l'opérateur).

[19] Pour simplifier, on suppose ici que le service est gratuit, mais il serait relativement peu complexe d'insérer dans ce protocole des fonctions de paiement.

aussi aléatoirement une clé symétrique de session K_s, avec laquelle il chiffre la requête. Enfin, il chiffre K_s à l'aide de la clé publique K_p du service pour constituer un ticket $T = \{K_s\}_{K_p}$.

2. Le client appelle (par GSM) le mandataire, et lui transmet (par SMS ou MMS) l'identification du service de localisation, le ticket T et la requête chiffrée.
3. Le mandataire se connecte par Internet au site du service de localisation et lui transmet le ticket et la requête chiffrée. Le serveur déchiffre le ticket avec sa clé privée, récupère ainsi K_s qu'il utilise pour déchiffrer la requête. Il construit sa réponse en conséquence, et la chiffre avec K_s avant de la renvoyer au mandataire.
4. Le mandataire retransmet la réponse chiffrée au client (par SMS ou MMS).
5. Le téléphone du client déchiffre la réponse (avec K_s) et l'affiche.

S'il faut créer une transaction complémentaire, par exemple pour réserver une table ou acheter un ticket de cinéma, cette nouvelle transaction se déroulera de la même façon.

XII.3.2.4- Autorisation préservant la vie privée

L'autorisation consiste à n'accorder des services qu'à certains utilisateurs, en fonction de leurs privilèges. L'aspect le plus important pour une autorisation préservant la vie privée est de séparer l'autorisation de l'authentification. En particulier, il ne devrait pas toujours être nécessaire de s'authentifier (c'est-à-dire de s'identifier et de prouver son identité) pour obtenir des privilèges. Par exemple, l'accès à un magazine en ligne peut être restreint à ceux qui ont payé un abonnement. Une façon d'implémenter cela tout en préservant la vie privée pourrait être pour l'utilisateur de souscrire son abonnement en payant avec de la monnaie électronique anonyme (*e-cash*, (40)) auprès d'un kiosque en ligne, qui lui transmettrait une preuve individuelle d'abonnement (avec une date de validité), et avec cette preuve, il pourrait récupérer depuis le site de l'éditeur du magazine tous les numéros qui couvrent la période de son abonnement. S'il paie par e-cash, et si ses connexions sont anonymes (*cf.* XII.3.2.2), son identité n'est transmise ni au kiosque, ni à l'éditeur. Dans cet exemple, l'éditeur accorde ou refuse l'accès, en fonction de la preuve présentée par l'utilisateur. Cette preuve d'abonnement est donc une *garantie anonyme* (en anglais, *anonymous credential*), et en tant que telle, la preuve doit présenter certaines propriétés, dont l'infalsifiabilité (l'éditeur doit être sûr que l'abonnement a bien été payé) et l'intransférabilité (seul l'abonné peut utiliser l'abonnement). On peut imaginer d'utiliser des garanties anonymes pour prouver de nombreuses autres propriétés, comme par exemple l'adhésion à une association, la citoyenneté, le permis de conduire, la carte d'électeur, etc. Dans certaines circonstances, l'anonymat doit pouvoir être révoqué par l'émetteur de la garantie, par exemple en cas de fraude ou de falsification. Dans ces cas-là, la garantie doit être « pseudonyme » plutôt qu'anonyme.

IDEMIX (*Identity Mixer*) (33) est un projet du laboratoire d'IBM à Zurich qui développe des algorithmes pour créer des garanties qui puissent être vérifiées de manière « *aveugle* ». Avant d'accéder à un service, l'utilisateur choisit un pseudonyme et obtient, auprès d'une autorité compétente, certaines garanties signées pour ce pseudonyme. Quand il veut accéder à un service, il lui suffit de prouver qu'il possède les garanties suffisantes, sans avoir à les montrer. En effet, si l'utilisateur montrait la même garantie chaque fois qu'il accède à un service, il serait facile d'établir un lien entre ces accès. L'idée de base d'IDEMIX consiste à ce que l'utilisateur transmette au serveur le pseudonyme et les garanties sous une forme chiffrée aléatoirement et utilise une preuve dite « *sans apport de connaissance* » pour garantir que le message chiffré contient les garanties nécessaires. La preuve sans apport de connaissance est basée sur une primitive cryptographique appelée « *signature de groupe* ». Ce schéma de signature permet aux membres d'un groupe de signer numériquement un document que n'importe qui pourra vérifier comme signé par un membre du groupe, mais sans pouvoir distinguer lequel des membres du groupe a réellement signé le document (10). Avec une telle preuve, le serveur peut être sûr que l'utilisateur a le droit d'accéder au service (en tant que membre du groupe autorisé), mais est incapable d'obtenir aucune autre information du message chiffré. De plus, puisque le chiffrement est aléatoire, le serveur est également incapable de reconnaître si deux requêtes distinctes utilisent la même garantie, et donc proviennent du même utilisateur. En cas de fraude ou d'autre nécessité, une tierce partie de confiance (par exemple, l'autorité émettrice de la garantie) peut déchiffrer les messages et extraire de la garantie les informations nécessaires pour contacter l'utilisateur ou lancer une procédure judiciaire.

Il est souhaitable que la gestion de telles garanties anonymes soit intégrée dans des dispositifs personnels suffisamment sûrs. Fabrice Boudot a ainsi proposé d'implémenter dans une carte à puce des algorithmes cryptographiques permettant de garantir des réponses binaires sur des attributs secrets certifiés, sans pour autant révéler aucune autre information sur ces attributs (21). Ces dispositifs personnels devraient intégrer des moyens biométriques d'authentification de leur propriétaire, pour empêcher qu'ils ne soient utilisés par d'autres (en cas de prêt ou de vol de ces dispositifs), et ainsi garantir l'intransférabilité des garanties anonymes.

XII.4- Disponibilité

Dans cette section, nous considérons les moyens permettant aux technologies de l'informatique diffuse d'être résilientes par rapport aux fautes accidentelles et aux autres menaces casuelles auxquelles elle doit faire face en vie opérationnelle (*cf.* XII.1.1). Nous ne traitons ici ni des erreurs et problèmes liés aux interactions avec les utilisateurs (*cf.* chapitres VI et VII), ni de la problématique de la vérification et du test par rapport aux fautes introduites pendant leur développement.

Nous nous focalisons sur la disponibilité de traitements embarqués sur des dispositifs mobiles, communicant sans fil et sans connectivité permanente à une infrastructure fixe, ou sur les réseaux de capteurs (fixes ou mobiles).

XII.4.1- L'épuisement d'énergie

Le problème de l'épuisement d'énergie se pose pour tout dispositif d'informatique diffuse à source d'énergie autonome ne pouvant être rechargée qu'occasionnellement[20], voire pas du tout. Dès lors, la première protection consiste bien évidemment à épargner au maximum l'énergie disponible par l'utilisation de technologies peu voraces, la mise en place de mécanismes de gestion de l'énergie (59, 81, 96), et la sélection des algorithmes en fonction de leur consommation énergétique au même titre que de leurs performances temporelles et de leur encombrement mémoire (14, 69, 104). Cependant, dans les environnements pour lesquels la recharge ou le remplacement des sources d'énergie ne peuvent être envisagés (par exemple, dans un réseau de capteurs disséminés dans la nature), de telles techniques ne font que repousser l'instant à partir duquel le dispositif en question ne pourra plus fonctionner, faute d'énergie. L'épuisement d'énergie constitue donc une cause importante des défaillances pour lesquelles des mécanismes de tolérance peuvent être mis en place au niveau logiciel. Modélisable comme un phénomène d'usure, de telles défaillances sont relativement prévisibles. Une procédure de tolérance peut même être envisagée de façon proactive par une détection de l'épuisement imminent de l'énergie.

XII.4.2- La communication sans fil

La notion même d'informatique diffuse est indissociable de la communication sans fil car c'est elle qui rend possible la coopération entre dispositifs pouvant se mouvoir indépendamment. Mais les menaces introduites par cette technologie (*cf.* XII.1.1) peuvent fortement nuire à la qualité et à la disponibilité du service de communication offert.

Pour lutter contre les interférences accidentelles et les brouillages malveillants, les normes de communication sans fil font appel aux techniques de codage pour la correction des erreurs, et aux techniques de dispersion spectrale (par exemple, dispersion par séquence directe dans la norme IEEE 802.11b ou dispersion par saut de fréquence dans la norme Bluetooth 1.2) ou encore à d'autres techniques avancées de modulation ainsi qu'à des protocoles de transmission fiabilisés. Néanmoins, la transmission sans fil reste intrinsèquement fragile. Par exemple, une étude expérimentale (43) sur la communication IP mise en œuvre sur des réseaux personnels (PAN[21]) Bluetooth a dénombré en 18 mois quelques 20854 erreurs observables au niveau utilisateur. Une proportion non négligeable de ces erreurs (0,7%) échappait à la détection par le code utilisé au niveau physique. Dans une application réelle, de telles erreurs non signalées pourraient être catastrophiques. Sur la base des erreurs détectables, les expériences démontrent un temps moyen jusqu'à défaillance (MTTF[22]) de seulement 10 minutes. En considérant une stratégie de rétablissement manuel par redémarrage, les auteurs estiment une disponibilité des

[20] Il faut cependant noter à ce sujet les progrès remarquables récents sur la récupération de l'énergie « ambiante » (rayonnements, vibrations, potentiels thermiques...) qui permettent d'entrevoir l'avènement de (micro-)dispositifs auto-alimentés (6).

[21] PAN : Personal Area Network

[22] MTTF : Mean Time To Failure

dispositifs de seulement 69%. Les auteurs proposent alors des techniques de tolérance aux fautes transitoires par répétition systématique ou par reprise après détection qui permettent d'augmenter un peu le MTTF (jusqu'à 30 minutes) et d'obtenir une disponibilité de 94%. Les auteurs ont observé une distribution non uniforme de certaines défaillances selon les équipements hétérogènes utilisés dans leurs expériences. Une partie des défaillances observées est ainsi imputable à des fautes de développement (en l'occurrence, dans la couche d'abstraction du matériel).

XII.4.3- Les défaillances des dispositifs

Les contraintes de coût et d'encombrement des dispositifs de l'informatique diffuse militent contre la mise en place de redondances à l'intérieur même d'un dispositif pour tolérer ses propres fautes. En général, on considère le dispositif tout entier comme une unité atomique de défaillance[23]. Ce point de vue est d'autant plus pertinent que l'épuisement des ressources énergétiques, la détérioration physique, voire le vol, sont probablement les sources principales de défaillance. Se pose alors le problème général de la tolérance aux défaillances des dispositifs.

Ce problème se confond souvent avec celui de la tolérance à la dynamique due à la mobilité. En effet, il semble impossible dans le cas général de distinguer la défaillance par arrêt d'un dispositif de son déplacement hors portée de communication, ou encore d'une mise hors tension volontaire.

Dans le cas d'ensembles de dispositifs dissimilaires, l'hétérogénéité des fonctionnalités ne permet pas d'envisager en général le maintien d'un fonctionnement non dégradé lorsqu'un dispositif devient indisponible. La tolérance revient alors à minimiser les conséquences de la perte du dispositif sur le système ou sur la communauté de dispositifs dont il faisait partie. Kindberg et Fox (80) mettent en avant un *principe de volatilité* pour guider la conception d'applications d'informatique diffuse. Ce principe préconise une conception prenant comme hypothèse que les utilisateurs, les matériels et les logiciels constituent un ensemble très dynamique et imprévisible, et propose la définition d'invariants (par exemple, l'absence de blocage) sur l'exécution globale du système malgré cette volatilité. Cependant, dans le cadre de Gaia, un espace intelligent peuplé de dispositifs hétérogènes, Ranganathan et Campbell (105) proposent une approche de tolérance originale, orientée par les objectifs et basée sur la planification. La planification vise à définir dynamiquement les tâches à accomplir pour atteindre les objectifs courants et d'activer automatiquement des services alternatifs offerts par les dispositifs hétérogènes disponibles.

À l'inverse, lorsqu'il s'agit de dispositifs similaires, la population de dispositifs peut être vue comme un réservoir de redondance permettant de tolérer les défaillances de dispositifs, sans dégradation du fonctionnement, par des techniques de duplication de fonctions, de données ou de services. Dans la suite de cette section, nous nous plaçons principalement dans ce contexte de dispositifs similaires.

[23] Une exception peut toutefois être trouvée dans le cadre de l'intergiciel *Impala* (85) qui considère la tolérance en interne pour les ressources de communication dans un réseau de capteurs.

XII.4.4- Les réseaux ad hoc

Indépendamment des fautes, des interférences et des brouillages, la transmission sans fil est limitée par la portée des émissions. Dès que les dispositifs communicants se déplacent de façon non coordonnée, il est impossible de garantir une communication directe fiable, à moins de prendre en compte le positionnement et la vitesse maximale relative des entités avant d'entamer une communication (100).

Pour s'affranchir partiellement de la limitation de portée en communication directe, les dispositifs communicants peuvent faire appel à des dispositifs tiers pour relayer leurs messages. En l'absence d'une infrastructure fixe de communication, cela conduit à la notion de réseaux sans fil multi-sauts, habituellement dénommés *réseaux (mobiles) ad hoc* (MANET[24]) pour des nœuds mobiles, ou *réseaux de capteurs sans fil* (WSN[25]) pour des nœuds sensoriels (fixes ou mobiles). De très nombreux travaux théoriques ont été consacrés à la problématique du routage dans les MANET (18, 24, 46, 61, 74, 90, 101), mais, à notre connaissance, peu de réalisations pratiques existent à ce jour (les applications potentielles annoncées sont les communications pour les armées, les services d'urgence, les robots mobiles, la sécurité routière, voire les événements sportifs en extérieur). Les protocoles sont classés principalement en protocoles proactifs ou réactifs selon qu'ils visent à maintenir des tables de routage en permanence ou, au contraire, qu'ils recherchent de nouveaux chemins à la demande, conduisant à des performances et des consommations énergétiques différentes selon le degré de mobilité des nœuds. En général, les protocoles réactifs sont préférables car ils ne gaspillent pas de ressources pour maintenir des chemins inutilisés. Ils sont en plus partiellement tolérants à la dynamique du réseau (qu'elle soit due à la mobilité ou à l'arrêt de nœuds) par leur principe de recherche de chemins à la demande (fondé principalement sur l'inondation). Cependant, ces protocoles peuvent induire un retard de communication important en raison justement de cette recherche dynamique de chemins. En conséquence, les chemins découverts sont conservés temporairement en mémoire cache afin de pouvoir les réutiliser tant que la topologie du réseau reste suffisamment stable. Des protocoles tolérants aux fautes sont étudiés pour repousser encore plus loin le besoin de recourir à l'inondation pour découvrir des chemins nouveaux (49, 118).

La communication sans fil par ondes hertziennes permet d'utiliser les propriétés offertes par la diffusion locale (non-fiable) pour mettre en place la détection d'erreur et le diagnostic. Par exemple, Michiardi et Molva (92) exploitent la diffusion locale pour surveiller l'activité de nœuds voisins dans un réseau ad hoc afin de détecter d'éventuelles erreurs ou « mauvais comportements ». De façon similaire, Chessa et Stanti (42) profitent de la diffusion locale pour espionner les réponses des voisins aux requêtes de test de nœuds tiers afin d'améliorer l'efficacité du diagnostic.

La mobilité et les arrêts de nœuds peuvent conduire à un *partitionnement* d'un réseau ad hoc en plusieurs sous-réseaux disjoints. Différentes stratégies permettent

[24] MANET : Mobile Ad-hoc NETwork

[25] WSN : Wireless Sensor Network

de faire face au partitionnement. Dans (17), on suppose une densité suffisamment élevée de nœuds dans une même zone géographique de façon à réduire le problème du partitionnement à celui de la déconnexion de composants singletons au bord de cette zone. Une autre stratégie consiste à minimiser la probabilité ou la durée d'un partitionnement en déployant automatiquement des nœuds supplémentaires (83) ou en tirant profit de la mobilité des nœuds (19, 84, 117). Dans (68), les auteurs proposent une technique de détection de partitionnements imminents afin de permettre à la couche de logiciel supérieure (intergiciel ou application) de déclencher une procédure d'adaptation adéquate.

Une autre stratégie consiste à admettre le partitionnement comme un mode de fonctionnement inévitable et de gérer des duplicata des données (*cf.* XII.4.6) de telle façon à autoriser des accès concomitants dans des sous-réseaux disjoints du réseau partitionné.

Dans beaucoup d'applications d'informatique diffuse, le partitionnement n'est pas seulement inévitable, il constitue le mode de fonctionnement principal. La notion de système global partitionné s'estompe alors en faveur d'une notion de communauté de dispositifs quasi-autonomes. Les éventuelles rencontres avec d'autres dispositifs peuvent alors être mises à profit pour créer des *systèmes d'information spontanés* (121).

XII.4.5- Les réseaux de capteurs

Bien qu'ils héritent de certaines caractéristiques des réseaux ad hoc, les réseaux de capteurs (*cf.* chapitre XI) présentent une problématique spécifique de disponibilité et de fiabilité car ils supportent des applications de très longue durée dans des environnements où la maintenance manuelle est difficile, voire impossible. Les défaillances des capteurs et l'épuisement de leurs ressources énergétiques doivent alors impérativement être pris en compte. Les réseaux de capteurs doivent aussi faire face aux incertitudes liées au calibrage, à la précision et au positionnement des capteurs.

Un réseau de capteurs doit être vu dans son ensemble comme un *système* destiné la perception de phénomènes physiques. Les différents capteurs effectuent des observations locales de l'environnement et coopèrent pour produire un *résultat global* qui reflète une caractéristique de la zone couverte, ou d'une partie de cette zone. Pour économiser l'énergie nécessaire à la transmission des données, on peut faire appel à des techniques d'agrégation des données au fur et à mesure de leur propagation.

Les capteurs dans un même voisinage sont aptes à percevoir les mêmes phénomènes physiques locaux de leur environnement, éventuellement selon des modalités différentes. Il est alors naturel d'envisager des techniques de fusion et de vote des données afin de tolérer (par masquage) les imprécisions de perception et les défaillances des capteurs.

Par exemple, Clouqueur *et al.* (44) considèrent la tolérance aux fautes dans un réseau de capteurs de présence destiné à la détection de cibles (surveillance militaire). Ils proposent et comparent des approches permettant aux capteurs non défaillants d'atteindre un consensus sur la présence ou non d'une cible. Ce consensus doit être obtenu malgré des imprécisions de perception et des défaillances

arbitraires[26] (mais sans collusion) des capteurs. Les auteurs considèrent deux approches de consensus décentralisées (respectivement sur les perceptions ou sur les décisions), ainsi qu'une approche hiérarchique permettant de diminuer les coûts énergétiques imposées par la communication.

Basile *et al*. (16) proposent la notion d'un « cercle des initiés », composé des capteurs voisins d'un capteur donné, pour mettre en œuvre de façon locale la tolérance aux défaillances arbitraires (sans collusion). Dans cette approche, un capteur propose une valeur qui doit être vérifiée et signée par une majorité de ses voisins, utilisant les techniques de cryptographie à seuil. Deux variantes sont proposées selon que la valeur vérifiée est la valeur propre du capteur ou celle qui résulte d'une fusion multi-sensorielle de cette valeur avec celles de ses voisins.

Zhao *et al*. (124) abordent le problème du *diagnostic* dans les réseaux de capteurs afin de fournir à un administrateur extérieur des mesures continues de l'état du réseau, appelés résumés (« *digests* »). Cette introspection de l'état du réseau utilise, comme pour les données de perception de l'environnement, des techniques d'agrégation progressive des données afin de minimiser la consommation d'énergie. Les *digests* sont complétés, le cas échéant, par des synthèses d'enquêtes « régionales » ou par des rapports détaillés sur l'état des capteurs. Staddon *et al*. (115) traitent de la *localisation* de nœuds défaillants pour reconfigurer des arbres de routage des données vers une base centrale et pour déclencher des alarmes si la qualité de la surveillance ne peut plus être assurée.

Un autre aspect spécifique aux réseaux de capteurs est la *couverture géographique* de la zone surveillée. Un déploiement inégal des capteurs, la présence d'obstacles, l'occurrence de fautes ou l'épuisement des ressources énergétiques concourent tous à la production de *trous de couverture* et donc à une dégradation de la qualité de la surveillance. Ahmed *et al*. (3) présentent une étude de différentes techniques envisageables pour pallier les trous de couverture, avec en particulier l'exploitation de l'éventuelle mobilité des capteurs ou d'un sous-ensemble des capteurs, ou encore le contrôle de la topologie ou de la densité du réseau par l'activation opportune de capteurs mis auparavant en sommeil pour minimiser la consommation énergétique.

Nous avons déjà souligné le problème posé par la maintenance dans les réseaux de capteurs. Cela concerne non seulement la difficulté, voire l'impossibilité, de réparer une multitude d'éléments matériels éparpillés dans la nature mais aussi la difficulté de mettre à jour le logiciel d'application dont ils sont équipés. Par exemple, Liu et Martonosi (85) présentent un intergiciel basé sur des événements et capable de supporter la mise à jour incrémentale et à distance des modules du code d'application d'un réseau de capteurs embarqués sur des animaux sauvages. Cet intergiciel permet aussi l'adaptation automatique ou « autonomique » de l'application pour minimiser la consommation d'énergie ou maximiser les performances. Les auteurs donnent aussi un exemple d'adaptation en vue de tolérer la défaillance de ressources physiques internes à un dispositif En l'occurrence, la défaillance d'un des deux émetteurs-récepteurs radio peut être tolérée par la

[26] La notion de défaillances arbitraires admet tous les comportements erronés imaginables, y compris des comportements malveillants.

commutation automatique sur un protocole de communication qui utilise seulement l'émetteur-récepteur restant.

XII.4.6- La duplication de données

La duplication de données est une technique classique de tolérance aux fautes dans les systèmes répartis (56, 63, 114) qui prend un intérêt particulier dans le cas de dispositifs mobiles pour faire face aux défaillances, aux déconnexions et aux partitionnements. Deux principales catégories d'approches existent, appelées « optimistes » ou « pessimistes » selon que l'on admet ou non la mise à jour de copies auxquelles il n'est pas possible d'accéder simultanément. Dans l'approche optimiste, des mises à jour concomitantes sont admises, au risque de devoir détecter et résoudre les conflits sémantiques qui peuvent en résulter.

La duplication optimiste de données a été beaucoup étudiée dans le cadre de l'informatique mobile ou « nomade », où des clients souhaitent accéder à leurs données même lorsque leurs dispositifs mobiles sont déconnectés de l'infrastructure fixe qui supporte leurs serveurs de stockage des données. Par exemple, Coda (111) est un système de fichiers dupliqués qui supporte des clients mobiles. Il distingue les copies « serveurs », qui sont des copies primaires stockées sur des serveurs redondants reliés par l'infrastructure fixe, et des copies « clients », qui sont des copies secondaires qui ne peuvent être synchronisées qu'avec les copies serveurs. D'autres systèmes de fichiers à duplication optimiste et adaptés à la mobilité ont été proposés, dont Ficus (103) et Roam (106).

Des approches similaires, mais mono-utilisateurs, existent maintenant en standard dans les systèmes d'exploitation commerciaux tels que Mac OS X, qui comportent des fonctions de synchronisation de fichiers et de données d'application personnelles entre ordinateurs au travers d'un serveur sur l'infrastructure fixe (7, 8). L'utilisateur peut spécifier une synchronisation manuelle ou automatique de ses données dupliquées sur ses différents ordinateurs, voire sur son téléphone ou son assistant numérique portable.

Des travaux récents se focalisent sur la duplication et le partage de données dans le contexte de groupes d'utilisateurs reliés par un réseau ad hoc (à un ou plusieurs sauts).

Boulkenafed et Issarny considèrent dans AdHocFS (22) le cas d'utilisateurs mobiles qui veulent travailler en groupe lorsqu'ils sont déconnectés de leurs serveurs de fichiers fixes. Dans ce système, la duplication optimiste est adoptée pour les copies mobiles dans des groupes disjoints et par rapport aux copies sur les serveurs fixes, mais une gestion pessimiste et donc stricte des copies est assurée pour les copies mobiles au sein d'un même groupe (par le biais d'un protocole d'écrivain exclusif).

Hara et Madria (67) considèrent la duplication de données sur des dispositifs mobiles ayant des capacités limitées de stockage. Ils proposent alors une technique d'allocation des copies permettant d'optimiser leur accessibilité lors d'un partitionnement. La technique proposée considère que la mise à jour d'une donnée ne peut se faire qu'au travers de son exemplaire principal. Une lecture concomitante d'une copie secondaire dans un autre composant du réseau partitionné reste possible, mais devra alors être invalidée par la suite, lorsque le partitionnement cessera. Wang

et Li (119) considèrent une approche similaire pour dupliquer des services d'information mais en tenant compte d'un modèle de mobilité de groupes de dispositifs afin de ne dupliquer les données que lorsqu'un partitionnement est imminent.

Gianuzzi (62) étudie l'efficacité de la duplication de données ou de *fragments* de données dans un réseau ad hoc pouvant se partitionner. Il évalue la probabilité de l'accessibilité de k copies ou fragments dans le même composant du réseau que les clients intéressés, et cela en fonction de la « densité de portée » du réseau (le nombre moyen de nœuds dans la zone de portée des nœuds, supposée circulaire). Une telle évaluation permet de juger de la pertinence d'une duplication pessimiste gérée par des quorums, ou bien de l'utilisation de codes d'effacement (redondance k parmi n) pour des données à lecture seule.

Rodrig et LaMarca (109) proposent une variante du schéma de votes pondérés de Gifford (63) adaptée aux applications d'informatique diffuse. L'allocation des votes aux dispositifs permet de spécifier la composition des quorums nécessaires pour la lecture ou l'écriture des données et donc les comportements autorisés lors du partitionnement. Il s'agit d'une approche stricte (et donc pessimiste) qui exige l'exclusion entre une écriture et toute autre opération (écriture ou lecture) afin de garantir la cohérence des copies. Dans cette approche, il est possible d'assigner un nombre suffisant de votes à un dispositif privilégié pour l'autoriser à modifier la donnée même lorsqu'il est partitionné des autres dispositifs. Cependant, en cas de défaillance de ce dispositif, la donnée deviendrait inaccessible pour les dispositifs restants. Pour éviter cela, un mécanisme de « bail » est employé pour invalider des copies déconnectées depuis trop longtemps. Il se pose alors le difficile problème de choisir la durée du bail car c'est elle qui permet de distinguer la situation « dispositif déconnecté » de celle de « dispositif défaillant ».

D'autres travaux s'intéressent au problème de la sauvegarde de données saisies ou modifiées sur des dispositifs portables fonctionnant principalement de façon déconnectée par rapport à l'infrastructure fixe. Se pose alors le problème de la protection de ces nouvelles données en attendant l'occasion de pouvoir créer des copies sur un serveur fixe.

Dans Flashback, Loo *et al.* (87) proposent de relier les dispositifs appartenant à un même utilisateur par un réseau PAN et de mutualiser leurs capacités de stockage en un système de sauvegarde pair à pair privé. Les dispositifs sont supposés être de confiance et sont authentifiés par un schéma simple de certificats. Afin de sauvegarder ses données critiques, un dispositif « propriétaire » de données à sauvegarder établit des relations point à point avec des voisins choisis selon une heuristique de coût tenant compte de leur capacité de stockage, de l'énergie dont ils disposent et du niveau d'activité corrélée avec le dispositif propriétaire. Un dispositif défaillant peut être remplacé par un nouveau dispositif ayant le même identifiant, qui peut alors récupérer les données sauvegardées dans le réseau PAN.

Dans MoSAIC, Killijian *et al.* (47, 77) adoptent une approche similaire. Au contraire de Flashback, un dispositif propriétaire de données à sauvegarder ne fait pas appel à des dispositifs appartenant au même utilisateur, mais à des dispositifs inconnus qui sont rencontrés fortuitement au gré de leurs déplacements respectifs. Dans cette approche, les dispositifs mettent en œuvre une sauvegarde coopérative

intermédiaire, la sauvegarde finale des données s'effectuant lors de la re-connexion des dispositifs à l'infrastructure fixe, qui permet alors l'accès à un serveur de stockage sûr. Le fait de faire appel à des dispositifs inconnus soulève des défis quant à la gestion de la confiance (*cf.* XII.2.2) et à la prise en compte des malveillances, défis qui sont abordés par des techniques de réputation et de récompense, et par la fragmentation et la duplication des données.

XII.4.7- La duplication de serveurs

La duplication de serveurs vise à fournir des services à haute disponibilité dans une architecture logicielle de type client-serveur. Pour un serveur *sans état* ne pouvant défaillir que par arrêt, la gestion de serveurs dupliqués consiste essentiellement à mettre en place des mécanismes permettant à un client venant de subir une déconnexion de rechercher un autre exemplaire du serveur. La prise en compte de défaillances autres que des arrêts nécessite en plus un vote sur une pluralité de réponses venant de plusieurs exemplaires du serveur.

Pour un serveur *avec état*, la duplication est moins simple, car elle nécessite des mécanismes pour garantir que les états des exemplaires restent cohérents.

Si le serveur est considéré comme une « boîte noire » (telle qu'un automate, voire un processus), tout message reçu par le serveur peut potentiellement modifier son état. La cohérence des états nécessite alors la mise en place d'un protocole de diffusion atomique pour assurer que tous les exemplaires du serveur traitent les messages reçus dans le même ordre. La mise en place d'un tel protocole dans un réseau mobile dynamique impose des hypothèses sur la densité minimale et la vitesse relative des nœuds mobiles supportant les duplicata. Par exemple, Dolev *et al*. (55) présentent un algorithme permettant de définir un nœud virtuel mobile pouvant se déplacer dans une zone géographique comportant suffisamment de nœuds physiques pour supporter des copies de son état. Le nœud virtuel mobile défaille lorsqu'il entre dans une région insuffisamment peuplée.

Une situation intermédiaire se présente lorsque le serveur est considéré comme une « boîte blanche » dont l'état consiste en un ensemble de variables typées visibles depuis l'extérieur. Dans ce cas, il n'est pas nécessaire de garder strictement identiques les états globaux des exemplaires, mais seulement les états des variables effectivement dupliquées, c'est-à-dire, appartenant aux ensembles de variables gérées par différents exemplaires du serveur. Il ne s'agit plus alors de serveurs dupliqués au sens strict mais de serveurs multiples gérant des données dupliquées. Par exemple, Kim *et al*. (78) présentent une architecture de découverte de services supportant une multiplicité de serveurs de répertoire de services. Tout nœud (mobile) peut se porter candidat pour jouer le rôle de serveur de répertoire ; tout nœud qui joue ce rôle est appelé *volontaire*, les autres nœuds sont des *clients* (du service de répertoire de services). Tout volontaire maintient un répertoire des services offerts par des nœuds dans une région donnée, ainsi qu'un répertoire des autres volontaires dont il a connaissance. Tout client tente de s'enregistrer auprès de k volontaires, qui maintiennent chacun un enregistrement correspondant aux services proposés par ce client. Ces k volontaires forment ainsi un serveur dupliqué de répertoire de services, tolérant aux fautes et aux déconnexions, vis-à-vis des services proposés par ce client. Les nœuds jouant le rôle de volontaires et les volontaires vis-

à-vis d'un client donné se reconfigurent automatiquement selon la dynamique du réseau (mobilité et défaillance des nœuds).

XII.5- Conclusion

La sûreté de fonctionnement des technologies de l'informatique diffuse constitue un défi majeur à relever avant un déploiement massif auprès du grand public ou dans des applications critiques. L'intégration de l'informatique à des dispositifs physiques, la mobilité de ces dispositifs et l'omniprésence de la communication sans fil soulèvent de nouveaux risques quant à la sécurité des interactions, la protection de la vie privée et la disponibilité des services.

Sur le plan de la sécurité, les technologies de l'informatique diffuse, en particulier l'omniprésence des communications sans fil et les besoins de localisation des dispositifs utilisés nécessitent l'utilisation de techniques cryptographiques particulières, en particulier liées à la preuve de proximité ou à l'existence d'un secret authentifiant une entité.

De nombreuses solutions ont d'ores et déjà été proposées au problème d'établissement d'associations sécurisées, mais l'adoption de moyens de protection adaptés va finalement dépendre à la fois de l'évolution des appareils employés, en particulier de leur facteur de forme, et de l'acceptation par les utilisateurs, en particulier le grand public. On peut cependant clairement voir que la diffusion des nouvelles technologies va rendre le déploiement de telles mesures indispensable de manière assez rapide : c'est même déjà le cas pour certaines des plus simples dans certains appareils multimédia communiquant sans fil.

Au-delà de ce premier problème, le choix de mesures d'établissement de la confiance sera nécessairement fonction des applications à protéger, mais on devine déjà la grande importance de l'accumulation d'informations sur le profil de l'utilisateur, en particulier faisant appel au stockage de preuves de leurs déplacements et interactions, dans l'élaboration de politiques de sécurité dans l'informatique diffuse. Ces dernières techniques peuvent par ailleurs poser problème pour la protection de la vie privée.

D'ailleurs, une certaine hostilité vis-à-vis des technologies nouvelles se développe dans une bonne partie du public, principalement par crainte d'atteintes à la vie privée. Il faut donc prendre en compte ce souci dès la conception de nouvelles applications, bien avant leur déploiement, de façon à y intégrer efficacement des technologies de protection de la vie privée (PET, pour « *Privacy-Enhancing Technologies* »). Ceci est particulièrement vrai pour l'informatique diffuse en raison de la multiplication des dispositifs personnels ou portant des informations personnelles sensibles. Il convient en particulier de soutenir le développement de PET génériques (par exemple, pour permettre aux individus de garder le contrôle de leurs informations personnelles) ou spécifiques d'applications particulières (par exemple, pour minimiser la divulgation d'informations personnelles).

Il est important aussi de soutenir des actions pluridisciplinaires sur les aspects légaux et techniques, entre autres sur la façon dont les dépositaires d'informations personnelles peuvent et doivent en protéger la confidentialité et contrôler leur

transmission éventuelle à des tiers, en particulier aux autorités judiciaires ou gouvernementales.

La disponibilité est une condition nécessaire pour l'acceptabilité de nouvelles applications informatiques diffuses ou pour leur déploiement dans des situations critiques. Aujourd'hui, l'informatique diffuse est souvent synonyme d'informatique nomade et la disponibilité des applications rime avec connectivité à une infrastructure fixe, par exemple, pour accéder à des serveurs disponibles sur Internet.

Cependant, à long terme, il serait intéressant de pouvoir réaliser des services à haute disponibilité sans faire appel à l'infrastructure fixe. Cela intéresse bien sûr les militaires, mais aussi les services d'urgence, qui doivent faire face à l'absence ou à l'indisponibilité d'une telle infrastructure[27]. Mais cela permet aussi d'entrevoir des applications nouvelles, bien loin de la téléphonie et de l'informatique nomade, conçues autour de réseaux autonomes de dispositifs intelligents (capteurs, actionneurs, véhicules, robots…), fixes ou mobiles, et de tailles diverses (macro-, micro-, nano-…).

Pour pouvoir réaliser des services à haute disponibilité à base de réseaux dynamiques de dispositifs communicants, des recherches sont à promouvoir selon au moins deux approches complémentaires :

- une approche orientée par les ressources (données, objets, serveurs…) : comment définir des ressources logiques à haute disponibilité à partir d'une multiplicité de ressources élémentaires sujettes aux défaillances et aux déconnexions ?
- une approche orientée par les objectifs : comment utiliser les ressources disponibles à un instant et à un endroit donnés pour satisfaire au mieux les objectifs courants ?

Cela nécessite bien sûr un soutien en recherche de base sur l'algorithmique des systèmes dynamiques. Mais, pour aller au-delà de théories et de concepts qui sont, le plus souvent aujourd'hui, validés uniquement par des simulations, il est important de promouvoir une recherche expérimentale et interdisciplinaire, autour de plateformes rassemblant des dispositifs programmables, équipés des dernières technologies de communication sans fil, et dotés de moyens de réglage de portée et d'animation mobile.

[27] Par exemple, lors de l'explosion de l'usine AZF à Toulouse en septembre 2001, tous les réseaux de téléphonie mobile étaient saturés et donc indisponibles.

Bibliographie

1. A. Abou El Kalam, Y. Deswarte, G. Trouessin et E. Cordonnier, “Une démarche méthodologique pour l’anonymisation de données personnelles sensibles”, in *2ème Symposium sur la Sécurité des Technologies de l’Information et des Communications (SSTIC 2004),* (Rennes, France), pp.91-115, 2004.
2. C. Aguilar-Melchor, “Les communications anonymes à faible latence”, Institut National des Sciences Appliquées de Toulouse, Thèse de doctorat, 4 juillet 2006.
3. N. Ahmed, S. S. Kanhere et S. Jha, “The Holes Problem in Wireless Sensor Networks: A Survey”, *Mobile Computing and Communications Review*, vol. 9, no. 2, pp. 4-18, 2005.
4. J. Al-Muhtadi, A. Ranganathan, R. Campbell et M. Dennis, “Cerberus: A Context-Aware Security Scheme for Smart Spaces”, in *1st IEEE Int. Conf. on Pervasive Computing and Communications (PerCom 2003),* pp.489-96, 2003.
5. B. Alpern et F. Schneider, “Key Exchange using Keyless Cryptography”, *Information processing letters*, vol. 16, no. 2, pp. 79-82, 1983.
6. Y. Ammar, A. l. Buhrig, M. Marzencki, B. t. Charlot, S. Basrour, K. Matou et M. Renaudin, “Wireless Sensor Network Node with Asynchronous Architecture and Vibration Harvesting Micro Power Generator”, in *2005 Joint Conf. on Smart Objects and Ambient Intelligence: Innovative Context-aware Services: Usages and Technologies,* (Grenoble, France), ACM International Conference Proceeding Series, 121, pp.287-92, ACM Press, 2005.
7. Apple Computer Inc., “Synchronisation .Mac”, http://www.apple.com/fr/macosx/features/dotmacsync/, accédé le 9 novembre 2006.
8. Apple Computer Inc., “iSync”, http://www.apple.com/fr/macosx/features/isync/, accédé le 9 novembre 2006.
9. N. Asokan et P. Ginzboorg, “Key-Agreement in Ad-hoc Networks”, *Computer Communications*, vol. 23, no. 17, pp. 1627-37, 2000.
10. G. Ateniese, J. Camenisch, M. Joye et G. Tsudik, “A Practical and Provably Secure Coalition-Resistant Group Signature Scheme”, in *Advances in Cryptology - CRYPTO 2000,* LNCS, 1880, pp.255-70, Springer-Verlag, 2000.
11. A. Avizienis, J.-C. Laprie, B. Randell et C. Landwehr, “Basic Concepts and Taxonomy of Dependable and Secure Computing”, *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11-33, 2004.
12. W. Bagga, “Cryptographie à base de politiques : théorie et applications”, École Nationale Supérieure des Télécommunications, Institut Eurécom, Thèse de doctorat, 8 décembre 2006.
13. D. Balfanz, D. Smetters, P. Stewart et H. Wong, “Talking to Strangers: Authentication in Ad-Hoc Wireless Networks”, in *Symp. on Network and Distributed Systems Security (NDSS '02),* (San Diego, CA, USA), 2002.
14. K. C. Barr et K. Asanović, “Energy-Aware Lossless Data Compression”, *ACM Transactions on Computer Systems*, vol. 24, no. 3, pp. 250-91, 2006.

15. S. Basagni, K. Herrin, D. Bruschi et E. Rosti, “Secure Pebblenet”, in *Int. Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc'01),* (Long Beach, CA), pp.156-63, 2001.
16. C. Basile, Z. Kalbarczyk et R. Iyer, “Neutralization of Accidental Errors and Malicious Activities in Wireless Ad Hoc Networks”, University of Illinois at Urbana-Champaign, 2005.
17. P. Bellavista, A. Corradi et E. Magistretti, “REDMAN: An Optimistic Replication Middleware for Read-only Resources in Dense MANETs”, *Pervasive and Mobile Computing*, vol. 1, pp. 279-310, 2005.
18. R. Beraldi et R. Baldoni, “A Caching Scheme for Routing in Mobile Ad Hoc Networks and Its Application to ZRP”, *IEEE Transactions of Computers*, vol. 52, no. 8, pp. 1051-62, 2003.
19. M. M. Bin Tariq, M. Ammar et E. Zegura, “Message Ferry Route Design for Sparse Ad hoc Networks with Mobile Nodes”, in *Int. Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc'06),* (Florence, Italy), pp.37-48, ACM, 2006.
20. D. Boneh et M. Franklin, “Identity-Based Encryption from the Weil Pairing”, *SIAM Journal of Computing*, vol. 32, no. 3, pp. 586-615, 2003.
21. F. Boudot, “Partial Revelation of Certified Identity”, in *4th Working Conference on Smart Card Research and Advanced Applications (CARDIS 2000)* (Bristol, UK), pp.257-69, Kluwer Academic Publishers, 2000.
22. M. Boulkenafed et V. Issarny, “AdHocFS: Sharing Files in WLANs”, in *2nd Int. Symp. on Network Computing and Applications (NCA'03),* (Cambridge, MA, USA), pp.156-63, IEEE CS Press, 2003.
23. S. Brands et D. Chaum, “Distance-Bounding Protocols (extended abstract)”, in *EUROCRYPT 93,* LNCS, 765, pp.23-27, Springer, 1993.
24. J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu et J. Jetcheva, “A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols”, in *Proc. of the ACM/IEEE Int. Conf. on Mobile Computing and Networking (MobiCom'98),* (Dallas, TX, USA), pp.98-97, ACM Press, 1998.
25. S. Buchegger et J. Y. Le Boudec, “Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes - Fairness In Distributed Ad-Hoc Networks”, in *Int. Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc'02),* (Lausanne, Switzerland), pp.226-36, IEEE, 2002.
26. L. Bussard et Y. Roudier, “Pervasive and Ubiquitous Computing Security”, in *Workshop on Security in Ubiquitous Computing at UBICOMP'2002,* (Göteborg, Sweden), 2002.
27. L. Bussard et Y. Roudier, “Embedding Distance Bounding Protocols within Intuitive Interactions”, in *Proceedings of the First International Conference on Security in Pervasive Computing (SPC'2003),* (Boppard, Germany), pp.143-56, 2003.
28. L. Bussard et R. Molva, “One-Time Capabilities for Authorizations without Trust”, in *2nd IEEE Int. Conf. on Pervasive Computing and Communications (PerCom'04),* (Orlando, FL, USA), pp.351-55, 2004.

29. L. Bussard, R. Molva et Y. Roudier, “History-Based Signature or How to Trust Anonymous Documents”, in *2nd Int. Conf. on Trust Management (iTrust 2004),* (St. Anne's College, Oxford, UK), LNCS, 2995, pp.78-92, Springer, 2004.
30. L. Bussard et W. Bagga, “Distance-bounding proof of knowledge to avoid real-time attacks”, in *Security and Privacy in the Age of Ubiquitous Computing, 20th IFIP International Information Security Conference (IFIP/Sec 2005),* (R. Sasaki, S. Qing et H. Yoshiura, Eds.), (Chiba, Japan), pp.223-38, 2005.
31. L. Buttyán et J.-P. Hubaux, “Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks”, *Mobile Networks and Applications*, vol. 8, no. 5, pp. 579-92, 2003.
32. M. Cagalj, S. Capkun et J.-P. Hubaux, “Key Agreement in Peer-to-Peer Wireless Networks”, *Proceedings of the IEEE (Special Issue on Security and Cryptography)*, vol. 94, no. 2, 2006.
33. J. Camenisch et E. V. Herreweghen, “Design and Implementation of the IDEMIX Anonymous Credential System”, in *9th ACM Conf. on Computer and Communications Security (CCS'02),* (Washington, DC, USA), pp.21-30, ACM, 2002.
34. S. Capkun, L. Buttyan et J.-P. Hubaux, “SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks”, in *ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN),* pp.21-32, 2003.
35. S. Capkun et J.-P. Hubaux, “Secure Positioning in Wireless Networks”, *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221-32, 2006.
36. M. Casassa Mont, S. Pearson et P. Bramhall, “Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services”, in *4th International Workshop on Database and Expert Systems Applications (DEXA'03),* (Prague, Czech Republic), pp.377-82, IEEE CS, 2003.
37. C. Castelluccia et P. Mutaf, “Shake Them Up! A Movement-Based Pairing Protocol for CPU-Constrained Devices”, in *3rd Int. Conf. on Mobile Systems, Applications and Services (Mobisys 2005),* (Seattle, WA, USA), pp.51-64, 2005.
38. CDFUE, *Charte des Droits Fondamentaux de l'Union Européenne*, articles 7 et 8, Journal officiel des Communautés européennes (2000/C 364/01-22), 18 décembre 2000.
39. D. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”, *Communications of the ACM*, vol. 24, no. 2, pp. 84-88, 1981.
40. D. Chaum, “Blind Signatures for Untraceable Payments”, in *Crypto'82,* pp.199-203, Plenum Press, 1983.
41. D. Chaum, “The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability”, *Journal of Cryptology*, vol. 1, pp. 65-75, 1988.
42. S. Chessa et P. Santi, “Comparison-based System-level Fault Diagnosis in Ad Hoc Networks”, in *Symp. on Reliable Distributed Systems,* (New Orleans, LA USA), pp.257-66, IEEE CS Press, 2001.

43. M. Cinque, D. Cotroneo et S. Russo, “Collecting and Analyzing Failure Data of Bluetooth Personal Area Networks”, in *IEEE/IFIP Int. Conf. on Dependable Systems and Networks,* pp.313-22, IEEE, 2006.
44. T. Clouqueur, K. K. Saluja et P. Ramanathen, “Fault Tolerance in Collaborative Sensor Networks for Target Detection”, *IEEE Transactions of Computers*, vol. 53, no. 3, pp. 320-33, 2004.
45. J. Clulow, G. P. Hancke, M. G. Kuhn et T. Moore, “So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks”, in *European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks (ESAS 2006),* LNCS, 4357, pp.83–97, 2006.
46. S. Corson et J. Macker, “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”, Internet RFC 2501, January 1999.
47. L. Courtès, M.-O. Killijian et D. Powell, “Storage Tradeoffs in a Collaborative Backup Service for Mobile Devices”, in *6th European Dependable Computing Conference (EDCC-6),* (Coimbra, Portugal), pp.129-38 IEEE CS Press, 2006.
48. M. J. Covington, P. Fogla, Z. Zhan et M. Ahamad, “A Context-Aware Security Architecture for Emerging Applications”, in *18th Annual Computer Security Applications Conference (ACSAC'02),* (Las Vegas, NV, USA), p.249, 2002.
49. L. Demoracski, “Fault-tolerant Beacon Vector Routing for Mobile Ad Hoc Networks”, in *19th IEEE Int. Conf. on Parallel and Distributed Processing Symposium (IPDPS'05),* p.279.2, IEEE, 2005.
50. Y. Deswarte, “La sécurité des systèmes d’information et de communication”, in *Sécurité des réseaux et systèmes répartis*, *Traité IC2*, Y. Deswarte et L. Mé, Eds., Hermès, 2003, pp. 15-48.
51. Y. Deswarte et C. Aguilar-Melchor, “Technologies de protection de la vie privée sur Internet”, in *Sécurité des systèmes d’information*, *Traité IC2*, L. Mé et Y. Deswarte, Eds., Hermès-Lavoisier, 2006, pp. 49-71.
52. W. Diffie et M. E. Hellman, “New Directions in Cryptography”, *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644-54, 1976.
53. Directive95/46/CE, Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, du 24 octobre 1995, Journal officiel des Communautés européennes (1995/L 281/0031-0050), 23 novembre 1995.
54. D. Djenouri, L. Khelladi et N. Badache, “A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks”, *IEEE Communications Surveys and Tutorials*, vol. 7, no. 4, pp. 2- 28, 2005.
55. S. Dolev, S. Gilbert, N. A. Lynch, E. Schiller, A. A. Shvartsman et J. Welch, “Virtual Mobile Nodes for Mobile Ad Hoc Networks (extended abstract)”, in *Distributed Computing (DISC),* (Amsterdam, Netherlands), LNCS, 3274, pp.230-44, Springer, 2004.
56. A. El Abbadi, D. Skeen et F. Cristian, “An Efficient Fault-Tolerant Protocol for Replicated Data Management”, in *4th ACM SIGACT-SIGMOD Symp. on Principles of Database Systems,* (Portland, OR, USA), pp.215-28, ACM, 1985.

57. L. Eschenauer et V. Gligor, “A Key Management Scheme for Distributed Sensor Networks”, in *9th ACM Conf. on Computer and Communications Security (CCS'02),* (Washington D.C., USA), pp.41 - 47, ACM, 2002.
58. J.-C. Fabre, Y. Deswarte et L. Blain, “Tolérance aux fautes et sécurité par fragmentation-redondance-dissémination”, *Technique et Science Informatiques (TSI)*, vol. 15, no. 4, pp. 405-27, 1996.
59. L. M. Feeney, “A QoS Aware Power Save Protocol for Wireless Ad Hoc Networks”, in *1st Mediterranean Workshop on Ad Hoc Networks (Med-Hoc Net 2002),* (Sardenga, Italy), 2002.
60. C. Gehrmann, C. J. Mitchell et K. Nyberg, “Manual Authentication for Wireless Devices”, *RSA Cryptobytes*, vol. 7, no. 1, pp. 29-37, 2004.
61. M. Gerla, X. Hong et G. Pei, “Fisheye State Routing Protocol (FSR) for Ad Hoc Networks”, IETF MANET Working Group, Internet Draft, 17 June 2002.
62. V. Gianuzzi, “Data Replication Effectiveness in Mobile Ad-Hoc Networks”, in *1st ACM Int. Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubitiquitous Networks (PE-WASUN'04),* (Venice, Italy), pp.17-22, ACM, 2004.
63. D. K. Gifford, “Weighted Voting for Replicated Data”, in *7th Symp. on Operating System Principles,* (Asilomar, CA, USA), pp.150-62, 1979.
64. L. Gomez, L. Moraru, D. Simplot-Ryl et K. Wrona, “Using Sensor and Location Information for Context-Aware Access Control”, in *Int. Conf. on Computer as a Tool (EUROCON 2005)* (Belgrade, Serbia & Montenegro), 2005
65. M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik et E. Uzun, “Loud and Clear: Human Verifiable Authentication Based on Audio”, in *Int. Conf. on Distributed Computing Systems (ICDCS'2006),* p.10, 2006.
66. G. P. Hancke et M. G. Kuhn, “An RFID Distance Bounding Protocol”, in *1st Int. Conf. on Security and Privacy for Emerging Areas in Communications Networks (SecureComm'05),* (Athens, Greece), pp.67-73, IEEE, 2005.
67. T. Hara et S. K. Madria, “Data Replication for Improving Data Accessibility in Ad Hoc Networks”, *IEEE Transactions on Mobile Computing*, vol. 5, no. 11, pp. 1515-32, 2006.
68. M. l. Hauspie, D. Simplot et J. Carle, “Partition Detection in Mobile Ad-Hoc Networks”, in *Med-Hoc Net 2003 Workshop,* (Mahdia, Tunisia), p.6, 2003.
69. W. R. Heinzelman, A. Chandrakasan et H. Balakrishnan, “Energy-Efficient Communication Protocol for Wireless Microsensor Networks”, in *33rd Hawaii Int. Conf. on System Sciences,* p.8020, IEEE CS Press, 2000.
70. J. Hightower et G. Borriello, “Location Systems for Ubiquitous Computing”, *Computer*, pp. 57-66, 2001.
71. L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl et H.-W. Gellersen, “Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts”, in *3rd Int. Conf. Ubiquitous Computing (Ubicomp'01),* (Atlanta, GA, USA), LNCS, 2201, pp.116-22, Springer, 2001.

72. IMS2003, *Identity Management Systems (IMS): Identification and Comparison Study*, Independent Centre for Privacy Protection (ICPP) / Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein and Studio Notarile Genghini (SNG), 2003-09-07.
73. ISO/IEC15408-2-2005, *Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 2: Exigences fonctionnelles de sécurité*, Norme Internationale, ISO/IEC 15408-2:2005, 2ème édition, 2005-10-01.
74. A. Jardosh, E.M. Belding-Royer, K. C. Almeroth et S. Suri, "Towards Realistic Mobility Models for Mobile Ad hoc Networks", in *Int. Conf. on Mobile Computing and Networking (MobiCom'03),* (San Diego, CA, USA), pp.217-29, 2003.
75. R. G. Johnston et J. S. Warner, "Think GPS Cargo Tracking = High Security? Think Again." *Transport Security World*, 2003.
76. A. Juels, "RFID Security and Privacy: A Research Survey", *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381-94, 2006.
77. M.-O. Killijian, D. Powell, M. Banâtre, P. Couderc et Y. Roudier, "Collaborative Backup for Dependable Mobile Applications [Extended Abstract]", in *2nd Workshop on Middleware for Pervasive and Ad-Hoc Computing. Middleware 2004 Companion,* (Toronto, Canada), pp.146-49, ACM Press, 2004.
78. M. J. Kim, M. Kumar et B. A. Shirazi, "Service Discovery using Volunteer Nodes in Heterogeneous Pervasive Computing Environments", *Pervasive and Mobile Computing*, vol. 2, pp. 313-43, 2006.
79. T. Kindberg et K. Zhang, "Context Authentication Using Constrained Channels", Internet and Mobile Systems Laboratory, HP Laboratories, Palo Alto, CA, USA, Technical Report HPL-2001-84, 2 April 2001.
80. T. Kindberg et A. Fox, "System Software for Ubiquitous Computing", *IEEE Pervasive Computing Magazine*, vol. 1, no. 1, pp. 70-81, 2002.
81. R. Kravets et P. Krishnan, "Power Management Techniques for Mobile Communication ", in *Mobicom'98,* (Dallas, TX, USA), pp.157-68, ACM, 1998.
82. M. G. Kuhn et R. J. Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations", in *2nd Workshop on Information Hiding,* LNCS, 1525, pp.124-42, 1998.
83. A. LaMarca, D. Koizumi, M. Lease, S. Sigurdsson, G. Borriello, W. Brunette, K. Sikorski et D. Fox, "Making Sensor Networks Practical with Robots", Intel, Seattle, Report IRS-TR-02-004, 2002.
84. Q. Li et D. Rus, "Sending Messages to Mobile Users in Disconnected Ad-hoc Wireless Networks", in *MobiCom 2000,* (Boston, MA, USA), pp.44-55, ACM, 2000.
85. T. Liu et M. Martonosi, "Impala: A Middleware System for Managing Autonomic, Parallel Sensor Systems", in *ACM SIGPLAN Symp. on Principles and Practice of Parallel Programming (PPoPP 03),* pp.107-18, 2003.
86. Loi78-17, Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2004-801 du 6 août 2004 relative à la

protection des personnes physiques à l'égard des traitements de données à caractère personnel.

87. B. T. Loo, A. LaMarca et G. Borriello, “Peer-to-Peer Backup for Personal Area Networks”, Intel, Seattle, Report IRS-TR-02-015, May 2003.
88. C. V. Lopes et P. Q. Aguiar, “Acoustic Modems for Ubiquitous Computing”, *IEEE Pervasive Computing*, vol. 2, no. 3, pp. 62-71, 2003.
89. S. Marti, T. J. Giuli, K. Lai et M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”, in *6th Int. Conf. on Mobile Computing and Networking,* (Boston, MA, USA), pp.255-65, 2000.
90. M. Mauve, J. Widmer et H. Hartenstein, “A Survey on Position-Based Routing in Mobile Ad Hoc Networks”, *IEEE Network*, vol. 15, no. 6, pp. 30-39, 2001.
91. J. M. McCune, A. Perrig et M. K. Reiter, “Seeing-is-Believing - Using Camera Phones For Human-Verifiable Authentication”, in *IEEE Symp. on Security and Privacy,* (Oakland, CA, USA), pp.110-24, 2005.
92. P. Michiardi et R. Molva, “CORE: A Collaborative Reputation Mechanism To Enforce Node Cooperation In Mobile Ad Hoc Networks”, in *6th IFIP Communications and Multimedia Security Conference,* (B. Jerman-Blaszic et T. Klobucar, Eds.), (Portorosz, Slovenia), pp.107-21, Kluwer Academic, 2002.
93. M. Naor, G. Segev et A. Smith, “Tight Bounds for Unconditional Authentication Protocols in the Manual Channel and Shared Key Models”, in *Advances in Cryptology (CRYPTO '06),* pp.214-31, 2006.
94. A. J. Nicholson, M. D. Corner et B. D. Noble, “Mobile Device Security Using Transient Authentication”, *IEEE Transactions on Mobile Computing*, vol. 5, no. 11, pp. 1489-502, 2006.
95. OCDE2002, OCDE, *Recommandation concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, adoptée par le Conseil de l'OCDE en date du 23 septembre 1980 (OECD Doc. C(80)58/FINAL, ISBN 9264197192, 2002, 66p.).
96. C. M. Olsen et C. Narayanaswami, “PowerNap: An Efficient Power Management Scheme for Mobile Devices”, *IEEE Transactions on Mobile Computing*, vol. 5, no. 7, pp. 816-28, 2006.
97. ONU217A, Organisation des Nations Unies (ONU), *Déclaration universelle des droits de l’homme*, Résolution 217 A (III) adoptée par l'Assemblée Générale de l'Organisation des Nations Unies le 10 décembre 1948 à Paris.
98. ONU19901214, Organisation des Nations Unies (ONU), *Lignes directrices pour la réglementation des fichiers de données personnelles automatisés*, (Résolution n° 45/95 du 14 décembre 1990).
99. G. Orwell, *Nineteen Eighty-Four*, London: Secker and Warburg, 1949.
100. J. Pauty, “Rôle de la géométrie dans l'informatique diffuse : programmation des applications et navigation contextuelle”, Université de Rennes 1, Thèse de doctorat, 24 février 2006.
101. C. E. Perkins, E. Belding-Boyer et S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing”, Internet RFC 3561, July 2003.

102. J. H. Piater, S. Richetto et J. L. Crowley, “Event-based Activity Analysis in Live Video Using a Generic Object Tracker”, in *Performance Evaluation for Tracking and Surveillance (PETS-2002),* (Copenhagen, Denmark), 2002.
103. G. J. Popek, R. G. Guy, T. W. Page, Jr. et J. S. Heidemann, “Replication in Ficus Distributed File Systems”, in *Workshop on the Management of Replicated Data,* (Houston, TX, USA), pp.5-10, IEEE, 1990.
104. N. R. Potlapally, S. Ravi, A. Raghunathan et N. K. Jha, “A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols”, *IEEE Transactions on Mobile Computing*, vol. 5, no. 2, pp. 128-43, 2006.
105. A. Ranganathan et R. H. Campbell, “Autonomic Pervasive Computing based on Planning”, in *Int. Conf. on Autonomic Computing (ICAC'04),* pp.80-87, IEEE, 2004.
106. D. H. Ratner, “Roam: A Scalable Replication System for Mobile and Distributed Computing”, UC Los Angeles, PhD, January 1998 (162p).
107. M. R. Rieback, B. Crispo et A. S. Tanenbaum, “Is Your Cat Infected with a Computer Virus?” in *4th Annual IEEE Int. Conf. on Pervasive Computing and Communications (PerCom 2006),* (Pisa, Italy), pp.169-79, 2006.
108. R. L. Rivest et A. Shamir, “How to Expose an Eavesdropper”, *Communications of the ACM*, vol. 27, no. 4, pp. 393-95, 1984.
109. M. Rodrig et A. LaMarca, “Decentralized Weighted Voting for P2P Data Management”, in *3rd ACM. Int. Workshop on Data Engineering for Wireless and Mobile Access,* (San Diega, CA, USA), pp.85-92, ACM Press, 2003.
110. N. Sastry, U. Shankar et D. Wagner, “Secure Verification of Location Claims”, in *ACM Workshop on Wireless Security (WiSe),* pp.1-10, 2003.
111. M. Satyanarayanan, J. J. Kistler, P. Kumar, M. E. Okasaki, E. H. Siegel et D. C. Steere, “Coda: A Highly Available File System for a Distributed Workstation Environment”, *IEEE Transactions on Computers*, vol. 39, no. 4, pp. 447-59, 1990.
112. N. Saxena, J.-E. Ekberg, K. Kostiainen et N. Asokan, “Secure Distance Pairing based on a Visual Channel”, in *IEEE Symp. on Security and Privacy,* (Oakland, CA, USA), pp.306-13, IEEE CS, 2006.
113. D. Singelee et B. Preneel, “Location Verification using Secure Distance Bounding Protocols”, in *IEEE Int. Conf.on Mobile Adhoc and Sensor Systems,* p.7, 2005.
114. D. Skeen, “A Quorum-Based Commit Protocol”, in *6th Berkley Workshop on Distributed Data Management and Computer Networks,* (Berkeley, CA, USA), pp.69-80, 1982.
115. J. Staddon, D. Balfanz et G. Durfee, “Efficient Tracing of Failed Nodes in Sensor Networks”, in *Ast ACM Int. Workshop on Wireless Sensor Networks and Applications,* (Atlanta, GA, USA), pp.122-30, ACM Press, 2002.
116. F. Stajano et R. Anderson, “The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks”, in *7th Int. Workshop on Security Protocols,* (Berlin, Germany), LNCS, 1796, pp.172-94, Springer, 1999.

117. A. Vahdat et D. Becker, “Epidemic Routing for Partially-Connected Ad Hoc Networks”, Duke University, Technical Report CS-2000-06, 2000.
118. R. Venkatasubramanian et J. P. Hayes, “Discovering 1-FT Routes in Mobile Ad Hoc Networks”, in *IEEE/IFIP Int. Conf. on Dependable Systems and Networks (DSN'04),* (Florence, Italy), pp.627-36, 2004.
119. K. H. Wang et B. Li, “Efficient and Guaranteed Service Coverage in Partitionable Mobile Ad-Hoc Networks”, in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies.,* pp.1089- 98, IEEE, 2002.
120. B. Waters et E. Felten, “Secure, Private Proofs of Location”, Princeton University, Technical Report TR-667-03, January 2003.
121. F. Weis, “Mise en œuvre des systèmes d'informations spontanés (SIS)”, in *Colloque sur la mobilité,* (LORIA , Nancy), p.2, 2002.
122. M. Weiser, “Some Computer Science Issues in Ubiquitous Computing”, *Communications of the ACM*, vol. 36, no. 7, pp. 75-84, 1993.
123. D. Yao, R. Tamassia et S. Proctor, “On Improving the Performance of Role-Based Cascaded Delegation in Ubiquitous Computing”, in *1st Int. Conf. on Security and Privacy for Emerging Areas in Communications Networks (SecureComm'05),* (Athens, Greece), pp.157-70, IEEE, 2005.
124. J. Zhao, R. Govindan et D. Estrin, “Computing Aggregates for Monitoring Wireless Sensor Networks”, in *Int. Workshop on Sensor Network Protocols and Applications,* pp.139-48, IEEE CS Press, 2003.