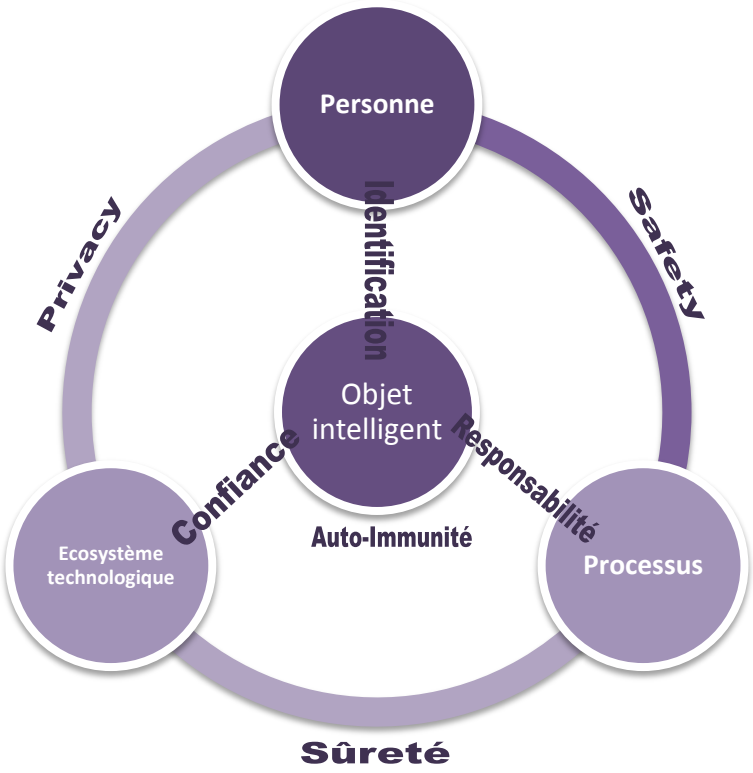
Sécurité de l'Internet des Objets : vers une approche cognitive et systémique

Yacine Challal

Par

M. Yacine CHALLAL

Sécurité de l'Internet des Objets : vers une approche cognitive et systémique



Au vu d'obtenir le diplôme

d'Habilitation à Diriger des Recherches

Devant le jury composé de :

M Abdelmadjid Bouabdallah, Professeur, *Université de Technologie de Compiègne*
M Jacques Carlier, Professeur, *Université de Technologie de Compiègne*
M Bernard Cousin, Professeur, *Université de Rennes 1*
M Walid Dabbous, Directeur de recherche, *INRIA*
Mme Maryline Laurent, Professeur, *Telecom & Management SudParis*
M Jean-Frédéric Myoupo, Professeur, *Université de Picardie Jules Verne*

Soutenance : Juin 2012
Option : Technologies de l'Information et des Systèmes

Résumé

La prolifération des réseaux ad hoc mobiles, pair-à-pair et de capteurs ont encouragé le développement des concepts d'une informatique autonome avec potentiellement un large éventail d'applications. Or, la vulnérabilité inhérente de ces réseaux autonomes introduit de nouveaux challenges de sécurité, telles que des attaques internes menées par des entités malveillantes. Plusieurs de ces attaques sont difficiles à détecter et à contrarier en raison de leur comportement asymptotique au comportement de processus légitimes des systèmes en interaction. Par ailleurs, la limitation des ressources de certains réseaux autonomes (réseaux de capteurs sans fil, réseaux mobiles ad hoc) constitue un autre grand challenge pour leur robustesse qui englobe à la fois la tolérance aux défaillances et la sécurité.

Dans ce contexte, nos travaux se sont articulés autour de deux axes de recherche qui se situent à deux limites de la connaissance contemporaine sur la sécurité des systèmes : *la sécurité collaborative des systèmes complexes en interaction et la sécurité des systèmes à fortes contraintes de ressources*. Nous nous sommes fixés comme objectif le développement de solutions algorithmiques aptes à satisfaire les besoins des utilisateurs en termes de performance et de robustesse tout en leur permettant de faire abstraction de la complexité sous-jacente. Nous avons démontré à travers nos travaux que l'interaction robuste et sécurisée entre ces systèmes atypiques est possible. Elle est possible grâce à une nouvelle appréhension de la sécurité basée sur la collaboration de processus de confiance, et la prévention à base de mécanismes proactifs de tolérance aux disfonctionnements.

Nous avons mené une recherche à la fois scientifique, technologique et intégrative dans le cadre de projets pluridisciplinaires, qui s'inscrivent dans des domaines aussi variés que la santé, l'agriculture, la gestion du trafic urbain, les systèmes embarqués, les réseaux et la sécurité des échanges.

L'évolution de nos axes de recherche est principalement motivée par la prise en compte de nouvelles évolutions technologiques et de leur usage, pour lesquelles nous proposerons des solutions algorithmiques de sécurité tout en optimisant les coûts inhérents. En l'occurrence, une évolution majeure qui s'inscrit dans la continuité des développements récents des technologies de l'information et de la communication et des systèmes embarqués, est *« l'internet des objets (IdO)»*. Cette évolution technologique sera accompagnée d'une évolution des usages et de l'écosystème technologique environnant dans toute sa complexité. Nous allons montrer que cette nouvelle *« technologie de rupture »* à enjeux socioéconomiques importants suscite ses propres challenges de sécurité et de « privacy ». Nous présenterons une évolution de la thématique de sécurité de l'IdO en trois phases : *la sécurité efficace pour une informatique embarquée miniaturisée, la sécurité et « privacy » centrée sur l'utilisateur selon le contexte, et une approche cognitive et systémique de la sécurité de l'IdO.* En effet, nous montrerons que l'évolution des objets vers plus d'autonomie à percevoir et à agir sur l'environnement, accentuera les enjeux de la sécurité et de la « privacy ». En conséquence, la sécurité de l'Internet des objets devrait aussi évoluer vers plus d'autonomie perceptive et actionnelle en se basant sur une approche cognitive et systémique centrée sur les objets intelligents.

Remerciements

En préambule à ce manuscrit, je souhaitais adresser mes remerciements les plus sincères aux personnes qui m'ont apporté leur aide et qui ont contribué à l'élaboration de ce rapport ainsi qu'à la réussite de ces années postdoctorales.

J'adresse mes plus cordiaux remerciements à Abdelmadjid BOUABDALLAH pour m'avoir autant impliqué dans les activités de son équipe, pour la confiance dont il fait preuve à mon égard et pour l'expérience qu'il m'a permis d'acquérir dans bien des domaines au cours de ces dernières années. Sans son soutien indéfectible, ses encouragement et ses conseils et orientations, je n'aurais accompli ces travaux.

J'adresse mes plus respectueux remerciements à Madame Maryline LAURENT, Professeur à SudParis Telecom & Management, et Messieurs Bernard COUSIN, Professeur à l'Université de Rennes 1, Walid DABBOUS, Directeur de Recherche à *inria*® et Jean-Frédéric Myoupo, Professeur à l'Université de Picardie Jules Verne pour avoir accepté d'être rapporteurs de mon Jury. Qu'ils soient assurés de ma plus profonde reconnaissance pour l'attention qu'ils ont portée à ce manuscrit et pour le temps qu'ils ont consacré à son évaluation. Conscient du travail qu'il me reste encore à effectuer et de ce qui est perfectible, je m'attacherai à suivre humblement leurs conseils et recommandations avisés.

Je tiens à exprimer toute ma gratitude à Monsieur Jacques CARLIER, Professeur à l'Université de Technologie de Compiègne qui me fait l'honneur de participer à ce Jury en tant qu'examinateur.

J'adresse mes plus sincères remerciements à Messieurs Ali CHARARA, Directeur du laboratoire HEUDIASYC et Aziz MOUKRIM, Directeur du département de Génie Informatique de l'UTC et responsable du domaine « Réseaux et Optimisation » pour leur soutien sans faille de mes activités de recherche et de pédagogie.

Je tiens à exprimer toute ma sympathie à la mémoire de notre cher défunt Hatem BETTAHAR, Maître de conférences à l'UTC et membre de notre équipe de recherche pour la qualité de la relation humaine que nous avons tissée mutuellement au fil des ans, pour toutes ses contributions à ces travaux, et qui nous a quittés tragiquement un certain 13 janvier 2011, une date qui marquera à jamais nos esprits.

Je remercie chaleureusement A. Babakhouya, M. Bagaa, W. Bechkit, A. Bencheikh, J. Alfredo Guerrero Mata, A. Hadjidj, S. Hatahet, N. Lasla, B. Maala, M. Omar, A. Ouadjaout, ainsi que tous les étudiants que j'ai encadrés et qui ont contribué aux travaux présentés dans ce mémoire.

Je remercie enfin toute ma famille, ma femme, mes enfants, mes parents et frères et sœurs, pour leur soutien continu et leurs encouragements.

Table des matières

Chapitre 1 : Introduction générale

1.1 Contexte

La prolifération des réseaux ad hoc mobiles, pair-à-pair et de capteurs ont encouragé le développement des concepts d'une informatique *autonome* avec potentiellement un large éventail d'applications. Nous signifions par « *informatique autonome* » l'ensemble des applications réseau où l'infrastructure de communication matérielle et/ou logicielle est construite par les entités participantes d'une façon autonome.
L'avantage de former un réseau mobile ad hoc est d'assurer une communication sans fil entre des dispositifs hétérogènes, n'importe quand et n'importe où, sans aucune infrastructure de communication préétablie. Ces dispositifs communiquent avec les autres nœuds qui sont à leur portée radio. Chaque nœud participant fournit des services tels que le transfert des messages, la signalisation d'information de routage, l'authentification, etc. pour former un réseau avec d'autres nœuds. Les capacités de mobilité, d'adaptation à toute situation même dégradée, d'auto-organisation et d'auto-recouvrement de routes après pannes, et de résilience, rendent cette technologie favorite pour des applications civiles et militaires diverses comme : la coordination des opérations de sauvetage dans des zones sans infrastructures opérationnelles, les réseaux véhiculaires, les réseaux de drones aériens et sous-marins, le partage de contenus et le divertissement dans des réseaux spontanés etc.
D'une façon assez similaire, dans un réseau pair-à-pair (P2P), chaque pair participe au fonctionnement du réseau « *overlay* » auquel il appartient en partageant des contenus et/ou des ressources et en participant à la signalisation de routage « *overlay* ». Cette technologie a encouragé à son tour un tas d'applications comme : le partage de fichiers et de contenus, le stockage distribué, le calcul réparti, le travail collaboratif, etc.
En outre, l'évolution continue des concepts fondateurs des réseaux ad hoc, et les progrès en matière de communication sans fil et de systèmes embarqués ont permis le développement d'un type particulier de réseaux ad hoc composés de nœuds capteurs sans fil. Ces nœuds capteurs, à faible coût et à ressources limitées, forment un réseau communément appelé un réseau de capteurs sans fil (RCSF). Cette technologie prometteuse permet la mesure de grandeurs physiques du milieu, la collecte de ces informations en temps réel, et leur transmission vers une station de supervision afin de surveiller une zone spécifique. Son faible coût et sa facilité de déploiement en font une solution attrayante pour une pléthore d'applications dans divers domaines, tels que : *le contrôle de chaînes de production et logistique, la surveillance de patients ou personnes âgées à distance, l'agriculture de précision, la détection et la poursuite d'objets, la détection et la surveillance de la propagation d'incendies, etc*.
Ces réseaux de capteurs sont caractérisés par de fortes contraintes dues à la limitation de ressources comme l'énergie, les capacités de stockage, de calcul et de bande passante. En outre, de nombreuses applications nécessitent le déploiement de capteurs dans des zones difficilement accessibles et en grande quantité, ce qui rend très difficile le contrôle manuel et le suivi individuel des capteurs.

La vulnérabilité inhérente des réseaux mobiles ad hoc et des réseaux de capteurs, qui sont généralement plus enclins à des menaces de sécurité physiques, introduit de nouveaux challenges de sécurité. La possibilité d'écoute, le déni de service, et les attaques

d'usurpation d'identité sont plus faciles à mener dans ce type de réseaux sans fil et sans infrastructure. Toutefois, les solutions de sécurité utilisées pour protéger les réseaux filaires classiques ne sont pas adéquates en raison des caractéristiques atypiques des réseaux mobiles ad hoc et des réseaux de capteurs. En plus de leur vulnérabilité intrinsèque s'ajoutent de nouvelles menaces, telles que les attaques internes menées par des nœuds malveillants. Plusieurs de ces attaques sont difficiles à détecter et à contrarier en raison de leur comportement asymptotique au comportement de processus légitimes du réseau. Par ailleurs, étant donné la sensibilité des applications potentielles des réseaux de capteurs sans fil qui sont étroitement liées au monde physique et même à des personnes, un déploiement à grande échelle de cette technologie dépendra de leur robustesse. En particulier, la sécurité apparaît comme un problème difficile en raison des contraintes de ressources qui entourent leur conception.

1.2 Axes de recherche et synthèse des contributions

Dans ce contexte, nos travaux se sont articulés autour de deux axes de recherche qui se situent à deux limites de la connaissance contemporaine sur la sécurité des systèmes : *la sécurité collaborative des systèmes et la sécurité des systèmes à fortes contraintes de ressources*.

Le premier axe est *l'approche collaborative pour la sécurité des systèmes communicants.* Cet axe de recherche émerge quand les mécanismes de sécurité actuels atteignent leur limite devant des attaques de plus en plus sophistiquées. Des attaques basées sur des comportements asymptotiques aux comportements des processus légitimes d'un système, ce qui rend le diagnostic d'une attaque très difficile en s'appuyant uniquement sur les outils actuels de la sécurité des systèmes. Ces comportements nécessitent une nouvelle appréhension de la sécurité qui s'appuiera sur la collaboration et la réputation. En effet, les solutions cryptographiques ont démontré leur limite quant à la protection des systèmes contre des processus malveillants et/ou malicieux s'appuyant sur des comportements « mensongers » tout en respectant les protocoles de communication. Dans ce cadre, nous avions exploré le couplage de la cryptographie à la collaboration de processus de confiance afin de protéger nos réseaux contre ce type d'attaques malicieuses et difficiles à contrarier.
Comme ce type de solutions repose sur des entités de confiance, nous avons entamé notre investigation par une analyse des modèles de confiance existants pour les réseaux mobiles ad hoc. En particulier, nous nous sommes intéressés aux modèles à base de certification électronique qui se caractérisent par leur capacité à s'adapter au facteur d'échelle et/ou à tolérer les pannes des serveurs de certification. Nos conclusions nous ont conduits à proposer une nouvelle approche basée sur la notion de confiance partielle que nous avons introduite. Pour mettre en œuvre cette nouvelle notion de confiance partielle, nous nous sommes servis de la cryptographie à seuil, où les entités du réseau délivrent des certificats partiels, et l'obtention d'un *quorum* de certificats permettrait de reconstituer un certificat complet conférant une adhésion totale au système. Nous avons démontré que notre modèle de confiance est plus robuste que les modèles existants. Notre modèle ne nécessitant pas d'infrastructure particulière est en parfaite adéquation avec la nature variable de la connectivité dans l*es réseaux mobile ad hoc.*
Nous avons par ailleurs, proposé une nouvelle approche de routage sécurisé reposant sur des entités de confiance qui coopèrent pour la vérification des messages de signalisation de routes. Notre approche permet ainsi de considérer une nouvelle métrique dans la

construction de route : *la confiance*. En effet, les protocoles de routage existants ont pour objectif, en général, de construire les routes les *« plus courtes »*. Or, notre approche permet de construire les routes les « *plus sûres »*, grâce à l'introduction de cette nouvelle métrique mesurée par les entités de confiance du réseau.
Toujours en se basant sur la notion de confiance et de coopération, nous avons proposé une solution de détection et de confinement de vers dans les réseaux pairs-à-pairs BitTorrent. Notre solution exploite le fonctionnement du protocole BitTorrent pour accélérer la propagation d'alertes de sécurité et le confinement de vers dans ce type de réseau. Elle repose sur la coopération d'un ensemble d'agents de confiance qui s'introduisent d'une façon transparente dans le processus de partage de fichiers et coopèrent dans la propagation d'alertes de sécurité éventuelles. Nous avons modélisé notre système *overlay* d'agents de confiance et démontré qu'il permet de réduire le taux d'infection dans le réseau d'une façon remarquable.

Le deuxième axe de nos travaux est *la sécurité dans les systèmes à fortes contraintes de ressources* en général et les réseaux de capteurs sans fil en particulier. Cet axe de recherche émerge à son tour quand la cryptographie moderne voit ses limites devant des systèmes dépourvus des ressources nécessaires (mémoire, puissance de calcul, etc.) à sa mise en œuvre. Nous avons considéré en particulier les réseaux de capteurs sans fil (RCSF) caractérisés par des limitations de ressources sévères en termes d'énergie, de mémoire, et de bande passante. Ces fortes contraintes, nécessitent une nouvelle appréhension de la sécurité basée sur des mécanismes proactifs et résilients contre la compromission de certains composants du réseau. En effet, vu la sensibilité des applications potentielles, un déploiement à grande échelle de RCSF dépend de la fiabilité qu'offre cette technologie. En particulier, la sécurité émerge comme une question difficile en raison de la limitation des ressources.
Un des composants fonctionnels indispensables dans toute architecture de communication sécurisée est le *sous-système de gestion de clés*. Ce sous-système revêt une importance particulière dans les réseaux de capteurs étant donné leurs contraintes de ressources. Nous avons traité en particulier la problématique de la résilience du sous-système de gestion de clés dans les réseaux de capteurs. Nous avons proposé une nouvelle approche de pré-distribution de clés résiliente à la compromission d'un ensemble de nœuds du réseau. Notre approche permet en effet de dissimuler les trousseaux de clés pré-distribuées aux nœuds du réseau de telle sorte que la compromission de certains nœuds ne met pas en péril tous les liens où leurs clés seraient utilisées pour sécuriser les échanges. Nous avons démontré que cette nouvelle approche améliore effectivement la résilience du sous-système de gestion de clés sans autant induire de surcoûts majeurs. En outre, nous avons proposé une nouvelle solution de pré-distribution de clés déterministe et scalable. Cette nouvelle solution est basée sur la théorie de la conception combinatoire, et tout en particulier sur la construction dite « unital design ». Nous avons montré qu'un pré-chargement judicieux des trousseaux de clés construits grâce à cette technique permettait d'assurer une couverture sécurisée de réseaux à très grande échelle avec un surcoût de stockage des clés très réduit.
Nous avons par ailleurs traité les problèmes de résilience et de sécurité du routage multi-chemins. Nous avons proposé une nouvelle solution sécurisée de construction de routes multi-chemins. La résilience est améliorée naturellement grâce aux routes multiples construites pour acheminer les données des sources vers le collecteur (*« sink »*). Ce paradigme permet en effet de réduire le temps de recouvrement en cas de panne ou d'attaque, en basculant le flux sur une route alternative préalablement construire. Il permet

aussi, d'améliorer la robustesse d'une façon proactive en transmettant les données redondantes sur les chemins alternatifs. Notre approche utilise des mécanismes d'authentification légers et efficaces. Nous avons analysé les propriétés de sécurité de notre solution et évalué ses performances à travers des simulations. Les résultats de cette analyse et de ces simulations montrent l'efficacité de notre approche de construction de routes multi-chemins, sa résilience en cas de présence d'intrus et sa robustesse en cas de pannes.
Les contraintes d'énergie sont l'une des problématiques clés des réseaux de capteurs sans fil. De ce fait, étant donnée la redondance potentielle des mesures effectuées par le réseau, l'agrégation est l'un des moyens les plus efficaces pour l'économie de l'énergie. Il s'agit donc d'apporter une transformation aux données brutes reçues par un nœud à travers une fonction d'agrégation (min, max, moyenne, …) pour n'en retransmettre que l'information utile. Cette façon de procéder permet de réduire le nombre de messages transmis dans le réseau ce qui économise l'énergie qui aurait été consommée pour effectuer ces transmissions. Néanmoins, si l'agrégation élimine les redondances, elle rend la vérification de l'intégrité des données plus difficile. En effet, ce procédé autorise les nœuds intermédiaires à modifier les données initiales, et à travers l'élimination de la redondance, pourrait effacer les « données témoins » qui auraient pu être utilisées pour la vérification de l'intégrité des données reçues.
Nous avons traité cette problématique de vérification de l'intégrité des données avec agrégation dans les réseaux de capteurs. Grâce à une nouvelle technique de partage de clés que nous avons introduite, nous avons proposé une solution d'agrégation avec vérification de l'intégrité des données. Cette vérification s'effectue de proche en proche dans le réseau ce qui permet d'éviter le transport inutile de données « polluées » par un intrus : un phénomène dont souffrent les solutions existantes. Nous avons implémenté notre solution pour vérifier certaines hypothèses de délais, et nous avons évalué ses performances à travers des simulations. Les résultats ont montré que notre approche permet effectivement de réaliser une agrégation sécurisée sans induire des surcoûts importants en termes d'énergie, de bande passante ou de stockage.

1.3 Méthodologie

Nous avons mené une recherche à la fois scientifique, technologique et intégrative dans le cadre de projets pluridisciplinaires. Des projets qui s'inscrivent dans des domaines aussi variés que la santé, l'agriculture, la gestion du trafic urbain, les systèmes embarqués, les réseaux et la sécurité des systèmes.
Pour chacun des axes de nos travaux, nous avons proposé un ensemble de solutions efficaces. Nous avons suivi une méthodologie à la fois conceptuelle et expérimentale selon un processus itératif qui permet une meilleure insertion des solutions dans leur domaine d'application. Ce processus itératif s'est souvent reposé sur l'expertise de nos partenaires dans le cadre de projets pluridisciplinaires comme l'INRA (Institut National de Recherche en Agronomie), BMBI (Laboratoire de Biomécanique et Bioingénierie), équipe ASER (Automatique, Systèmes Embarqués, Robotique) du laboratoire Heudiasyc, etc. En outre, ce processus passe par une phase de modélisation en utilisant les outils adéquats : processus stochastiques, réseaux de Pétri, programmation linéaire, etc. Nous avons également évalué les performances de nos solutions en utilisant des simulateurs à événements discrets ou itératifs largement approuvés dans la communauté, comme Network Simulator (NS2) [63], TinyOS/TOSSIM [64], et PeerSim [65]. Le cas échéant, nous avions effectué une spécification puis une validation de la sécurité de nos protocoles en utilisant un moteur de

vérification automatique AVISPA [66]. Enfin, nous avons aussi réalisé des expérimentations et développé des prototypes de preuve de concept (plateformes de réseaux de capteurs sans fil pour l'agriculture et la rééducation fonctionnelle).
Nous avons mené une recherche intégrative dans le cadre de projets pluridisciplinaires. Comme l'illustre la Figure 1, ces projets couvrent un vaste spectre de domaines d'applications (sécurité des communications de groupe, sécurité des systèmes embarqués, réseaux de capteurs, rééducation fonctionnelle, agriculture de précision, communication inter-drones, et gestion du trafic urbain). Ces projets ont contribué ainsi à l'avancement des connaissances sur des sujets difficiles avec des challenges scientifiques et technologiques complexes. En outre, j'ai assuré des responsabilités de certains projets (AGROSENS, SIRENE) où j'ai eu l'occasion d'appréhender les tâches de gestion de projet et leurs difficultés. Par ailleurs, durant ces années, j'ai participé à l'encadrement de plusieurs stages de master, magisters (1ère post-graduation à l'étranger), et trois thèses de doctorat dont une achevée en mai 2011 et deux autres qui devraient s'achever à la fin de l'année 2012. Ces encadrements ont donné lieu à des résultats sous forme de développements intégrés aux projets et publications dans des revues et conférences de renommée. La Figure 1 résume mon parcours et l'ensemble des projets auxquels j'ai participé depuis ma thèse, ainsi que les encadrements de stages et doctorats auxquels j'ai participé.

1.4 Structure du document

Dans la suite de ce document, nous allons détailler davantage nos contributions scientifiques et technologiques autour des deux axes présentés ci-dessus. Ce rapport sera structuré comme suit : dans le chapitre 3, nous présenterons nos travaux autour des approches collaboratives pour la sécurité des systèmes. Nous présenterons en particulier les résultats de nos travaux autour des modèles de confiance robustes et distribués, la propagation de vers dans BitTorrent, leur détection et leur confinement à travers un réseau « *overlay* » d'agents de confiance coopératifs, et une nouvelle approche de routage sécurisé à base d'entités de confiance coopératives.
Dans le chapitre 4, nous présenterons nos travaux autour de la sécurité dans les réseaux de capteurs sans fil. Nous présenterons en particulier les résultats de nos travaux autour de la gestion de clés résiliente et « *scalable* », le routage multi-chemins robuste et sécurisé, et l'agrégation de données avec contrôle d'intégrité.
Dans le chapitre 5, nous présenterons les résultats de quelques projets de recherche technologique et partenariale auxquels j'ai participé. En particulier, nous présenterons le projet AGROSENS (FEDER, Picardie) autour des réseaux de capteurs pour l'agriculture, le projet SUPGEST (Fédération SHIC) qui porte sur les réseaux de capteurs pour la rééducation fonctionnelle, et le projet SIRENE (CARNOT) portant sur la communication inter-drones robuste et sécurisée.
Enfin, dans le chapitre 6, nous présenterons des perspectives de nos travaux motivées par l'évolution de l'Internet vers une nouvelle technologie de rupture qu'est l'*Internet des objets*. Après une présentation des enjeux socioéconomiques et les questions sécuritaires que soulève l'Internet des objets, nous présenterons notre vision de l'évolution de la thématique et de ses perspectives.

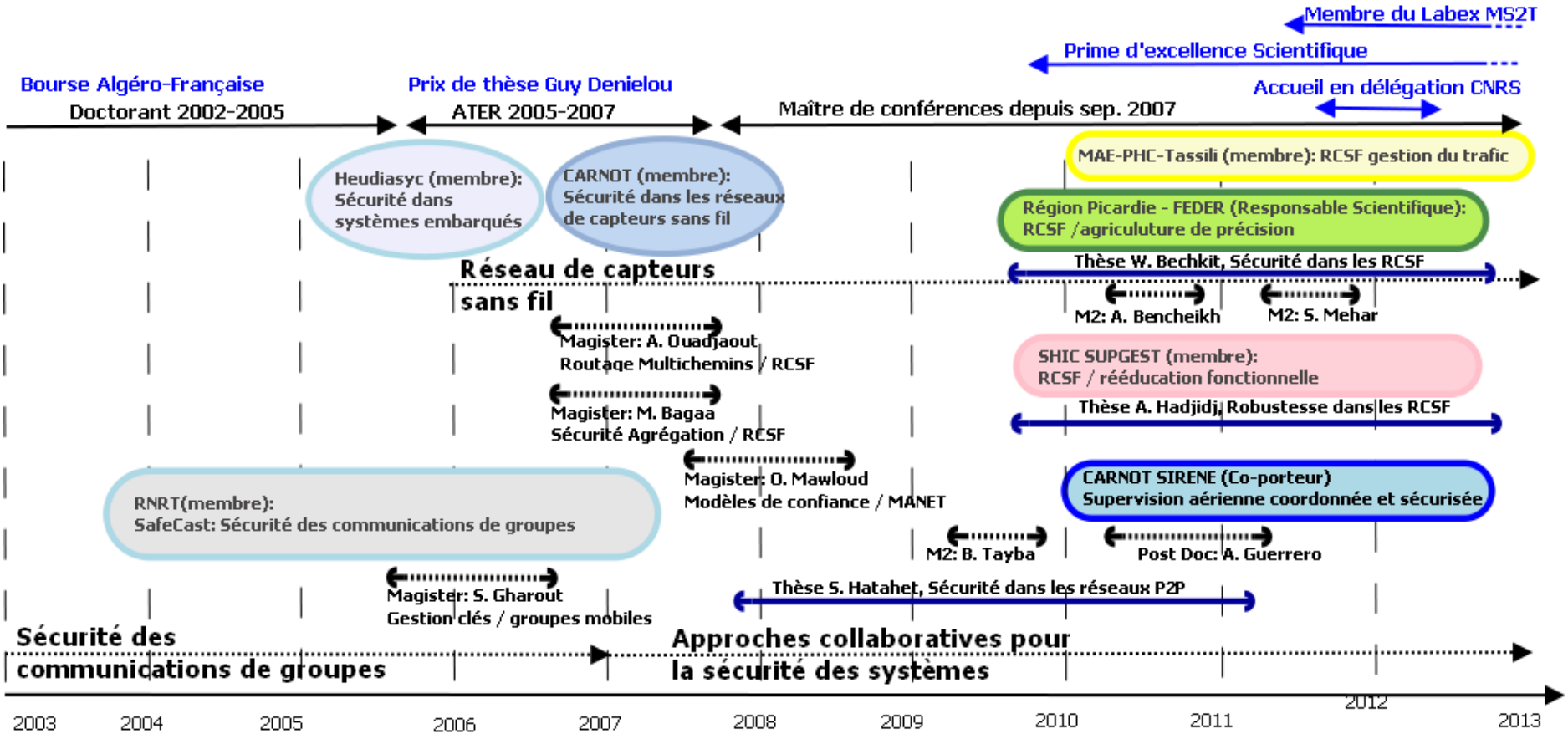


Figure 1 Projets et encadrement effectués ces dernières années

Chapitre 2 : Approches collaboratives pour la sécurité des réseaux

La sécurité revêt une importance stratégique pour nos entreprises et institutions de plus en plus connectées au réseau mondial Internet. Les solutions cryptographiques ont montré leur limite quant à la protection des systèmes contre des processus malveillants et/ou malicieux s'appuyant sur des comportements byzantins et/ou « mensongers » tout en respectant les protocoles de communication. Dans cet axe de recherche nous explorons le couplage de la cryptographie avec la collaboration de processus de confiance. Ceci pour protéger nos réseaux contre ce type d'attaques malicieuses et difficiles à contrarier en se basant uniquement sur la cryptographie. Dans cette thématique nous nous intéressons aux méthodes collaboratives pour la gestion de la confiance et la sécurité du routage, et la détection et le confinement d'attaques dans les réseaux pair-à-pair.

2.1 Modèles de confiance à base de certification dans les MANET

Les réseaux ad hoc mobiles sont composés d'un ensemble d'entités autonomes et auto-organisées. Ces réseaux sont très vulnérables aux attaques en raison de l'absence d'infrastructure et l'utilisation des liens sans fil. Des entités malveillantes peuvent entraver le bon fonctionnement du réseau. Par ailleurs, les entités légitimes doivent les détecter et les isoler du réseau en les évitant par exemple lors de l'acheminement des messages. Ceci nécessite la mise au point d'un modèle de confiance qui permet de définir qui fait confiance à qui et comment. Ce dernier fournit un cadre de travail pour la construction et l'administration de la relation de confiance entre les nœuds dans un réseau. Selon l'ITU-T (International Telecommunication Union - Telecommunication standardization sector), le terme « confiance » est défini comme suit : «On dit qu'une entité fait confiance à une deuxième entité si et seulement si cette dernière se comporte exactement comme la première le prévoit » [66].

La gestion de la confiance dans les réseaux ad hoc fait l'objet de deux grandes catégories de modèles: les modèles de confiance à base de réputation ([68][69][70][71][72][73][74]), et les modèles de confiance à base de certification ([75][76][77][78][79][80][81][82][83]). Dans la première catégorie, la confiance est basée sur la notion de réputation. La réputation d'un nœud augmente quand il effectue correctement les tâches qui correspondent au bon fonctionnement du réseau, tel que le routage. Chaque nœud observe le comportement de ses voisins et déclare une *accusation* s'il estime qu'un nœud est *suspect*, ce qui permet d'isoler l'ensemble des nœuds malicieux.

Dans la deuxième catégorie, la gestion de la confiance se fait essentiellement par une tierce partie de confiance qu'elle soit centrale ou distribuée. Si cette dernière estime qu'un nœud donné est digne de confiance, elle lui délivre un certificat qui va lui permettre de prouver sa légitimité envers les autres nœuds du réseau. Un certificat, est une structure de données dans laquelle une clé est liée à une identité (et éventuellement à certains autres attributs) délivrée et signée par la tierce partie de confiance dite *« autorité de certification »*.

Nous nous sommes intéressés à la deuxième catégorie : les modèles de confiance à base de certification.

2.1.1 Modèles de confiance à base de certification pour MANET : état de l'art

Après une revue approfondie des solutions existantes dans la littérature, nous avons proposé une taxonomie des modèles de confiance à base de certification dans les réseaux mobiles ad hoc (cf. Figure 2) [1]. Nous avons identifié deux catégories selon l'existence ou pas des autorités centrales : (i) Modèles autoritaires : dans cette catégorie, il existe une ou plusieurs autorités de confiance dans le réseau. Selon le nombre d'autorités, nous divisons cette catégorie en modèles monopolistes et modèles oligopolistiques. (ii) Modèles anarchiques : dans cette catégorie de modèles, il n'y a aucune autorité centrale. Chaque utilisateur dans le système agit en tant qu'autorité de certification. La propagation de la confiance dans le réseau forme un graphe entre les utilisateurs, appelé graphe de confiance (ou « web-of-trust »), qui est géré par les utilisateurs eux-mêmes. Ce modèle est décentralisé par nature, ce qui est adapté pour les réseaux ad hoc mobiles. Dans cette catégorie de modèles, deux opérations principales sont nécessaires : (1) la construction du graphe de confiance initial, et (2) la découverte des chaînes de certificats. Ainsi nous distinguons deux sous-catégories: (a) Modèles proactifs : dans cette sous-catégorie, le protocole d'échange de certificats est exécuté systématiquement entre les nœuds voisins. Ainsi, si le nœud client a besoin d'une chaîne de certificats, il la récupère directement à partir de son dépôt. (b) Modèles réactifs : dans cette sous-catégorie, le protocole de collection des certificats s'exécute à la demande. Quand le nœud aura besoin de vérifier un certificat, à cet instant il collecte à travers un protocole distribué la chaîne de certificats appropriée.

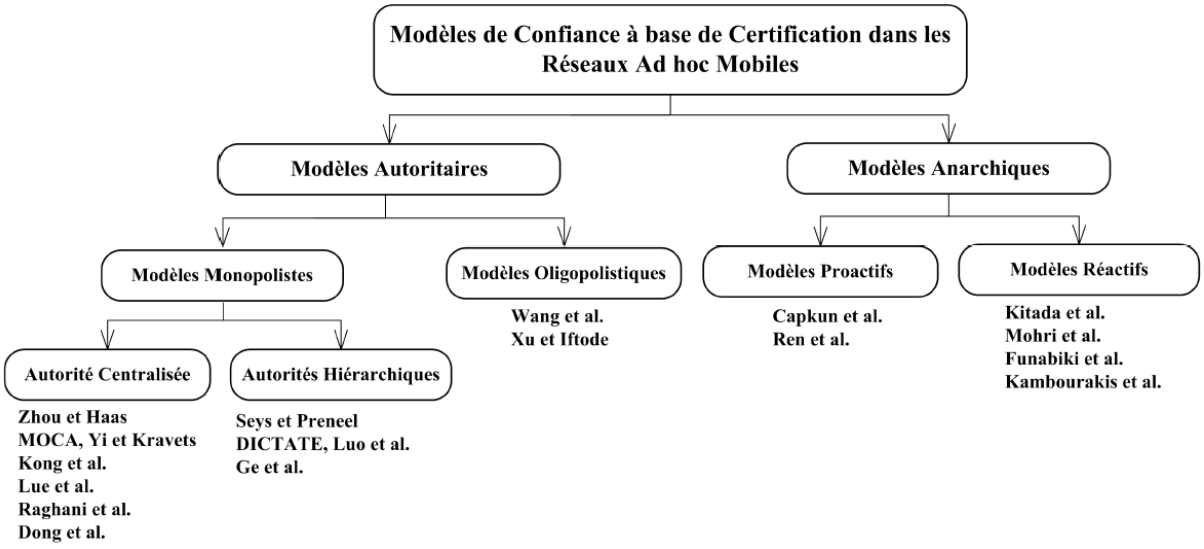


Figure 2 Classification des modèles de confiance à base de certification dans les réseaux ad hoc mobiles

En plus de l'analyse détaillée des solutions existantes et de la taxonomie que nous avons proposée, nous avons réalisé une étude comparative en considérant un ensemble de critères de performance qualitatifs et quantitatifs. Ainsi nous avons modélisé ces solutions avec des « Réseaux de Pétri Stochastiques » qui nous ont permis d'évaluer pour chaque solution la disponibilité du service de certification, l'adaptation au facteur d'échelle, et le dimensionnement de certains paramètres de ces solutions.

2.1.2 Un modèle de confiance robuste pour les réseaux ad hoc mobiles

Suite à notre analyse des modèles existants [1], nous avons proposé un modèle de confiance complètement distribué [2]. Au lieu d'appliquer la règle simpliste de transitivité de

la confiance, nous avons introduit une nouvelle règle de confiance plus robuste : "si A fait confiance à B et B fait confiance à C, alors A peut faire confiance à C, seulement s'il existe k-1 entités qui font confiance à C" (cf. Figure 3).

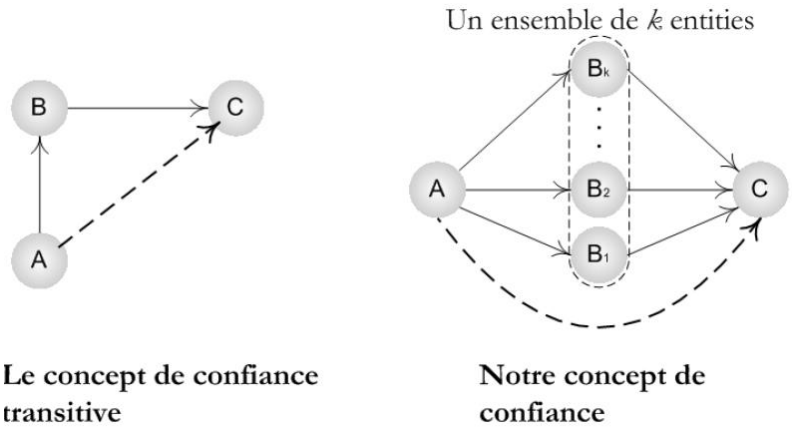


Figure 3 Relation de confiance

Afin de mettre en œuvre ce concept, nous avons proposé une solution basée sur un schéma de cryptographie à seuil (k, n), où n représente le nombre d'utilisateurs dans le système et k (k < n) représente le quorum de confiance.

Rappel : Cryptographie à seuil

Le concept de la cryptographie à seuil est inventé par Shamir [84] qui a proposé un mécanisme basé sur l'interpolation polynomiale. Il permet le calcul et le partage d'une valeur secrète S à un ensemble de n serveurs, sans que chacun d'eux connaisse sa valeur. A partir, d'au moins k serveurs on peut reconstruire le secret. Si le nombre de serveurs est inférieur à k aucune information n'est obtenue sur le secret S. Cette technique de cryptographie a été combinée avec le système cryptographique asymétrique RSA pour avoir un système qui permet de partager le pouvoir de signature à un ensemble de serveurs [85].

Le protocole de partage de secret de Shamir

Le protocole proposé par Shamir [84] permet de mettre en commun un secret S entre plusieurs serveurs (s_1, s_2, ..., s_n) de telle sorte qu'à partir de seulement k parts on peut reconstruire le secret S. On crée un polynôme F(x) de degré k-1, avec des coefficients aléatoires, en mettant $a_0 = S$. On choisit ensuite publiquement n points distincts X_i, tel que $X_i \neq 0$, et on distribue secrètement à chaque serveur s_i une part privée (X_i, $F(X_i)$). Le point X_i pourrait être n'importe quelle valeur publique qui identifie le serveur s_i d'une manière unique. Pour simplifier la notation, on met $X_i = i$, en conséquence les parts privées sont dénotées par F(1), F(2), … ,F(n).

Le protocole de reconstruction du secret

Ce protocole permet de reconstruire le secret S à partir d'un sous-ensemble de k parts : F(1), F(2),…,F(k). Etant donné k paires de points distincts (i, F(i)), il existe un polynôme unique F(x) de degré k-1 passant par tous les points. Ce polynôme peut être calculé à partir des points (i, F(i)) en utilisant l'interpolation de Lagrange [84].

Nous avons réalisé des simulations pour mesurer la robustesse de notre modèle et sa résilience face aux nœuds malicieux. Comme le montre la Figure 4, notre modèle améliore

cette résilience grâce au mécanisme de certification à seuil et la notion de confiance partielle que nous avons introduite. Nous avons également étudié l'impact du partitionnement du réseau. Comme le montre la Figure 5, notre modèle résiste mieux à cet éventuel changement de topologie induit par la mobilité des nœuds.

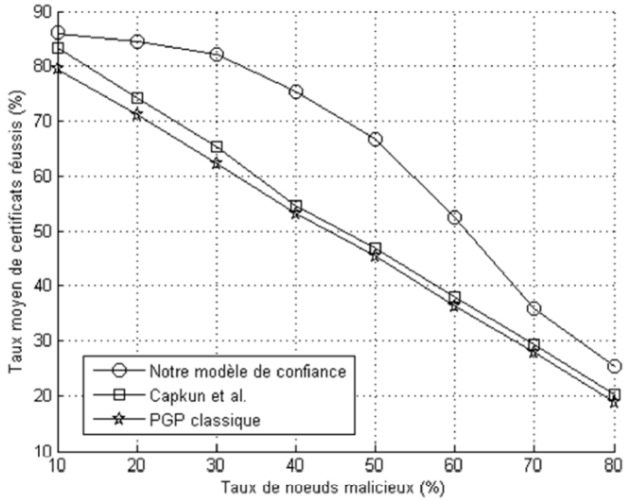


Figure 4 Impact du nombre de nœuds malicieux sur le taux moyen de certificats réussis

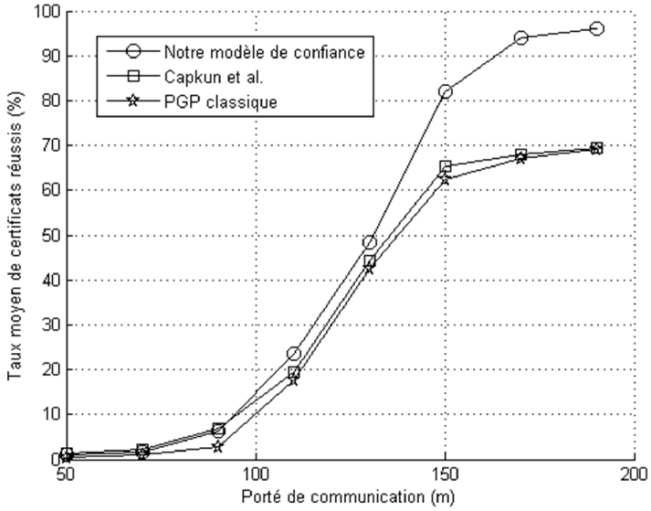


Figure 5 Impact du partitionnement du réseau sur le taux moyen de certificats réussis

2.1.3 Architecture de Confiance dans les réseaux mixtes

Nous avons également proposé une architecture d'un modèle de confiance [3][4] pour le cas des réseaux mixtes composés d'une partie avec infrastructure (filaire, cellulaire, etc.), et une autre sans infrastructure (ad hoc mobile) (cf. Figure 6). L'architecture repose sur l'utilisation de deux types d'autorités de certification, qui assurent la gestion des certificats X509v3: des autorités centrales CCA (Central Certification Authority), qui se trouvent dans la partie du réseau ayant une infrastructure, et des autorités mobiles MCA (Mobile Certification Authority), qui se trouvent dans la partie du réseau sans infrastructure. Les autorités MCA émulent le rôle du service de certification en utilisant un schéma de cryptographie à seuil (k,n) pour augmenter la disponibilité du service de certification, tandis que, les autorités CCA délèguent le pouvoir de certification aux autorités MCA en utilisant un schéma de cryptographie à seuil (t,m), et garantissent ainsi la disponibilité de serveurs de certification dans la partie sans infrastructure du réseau.

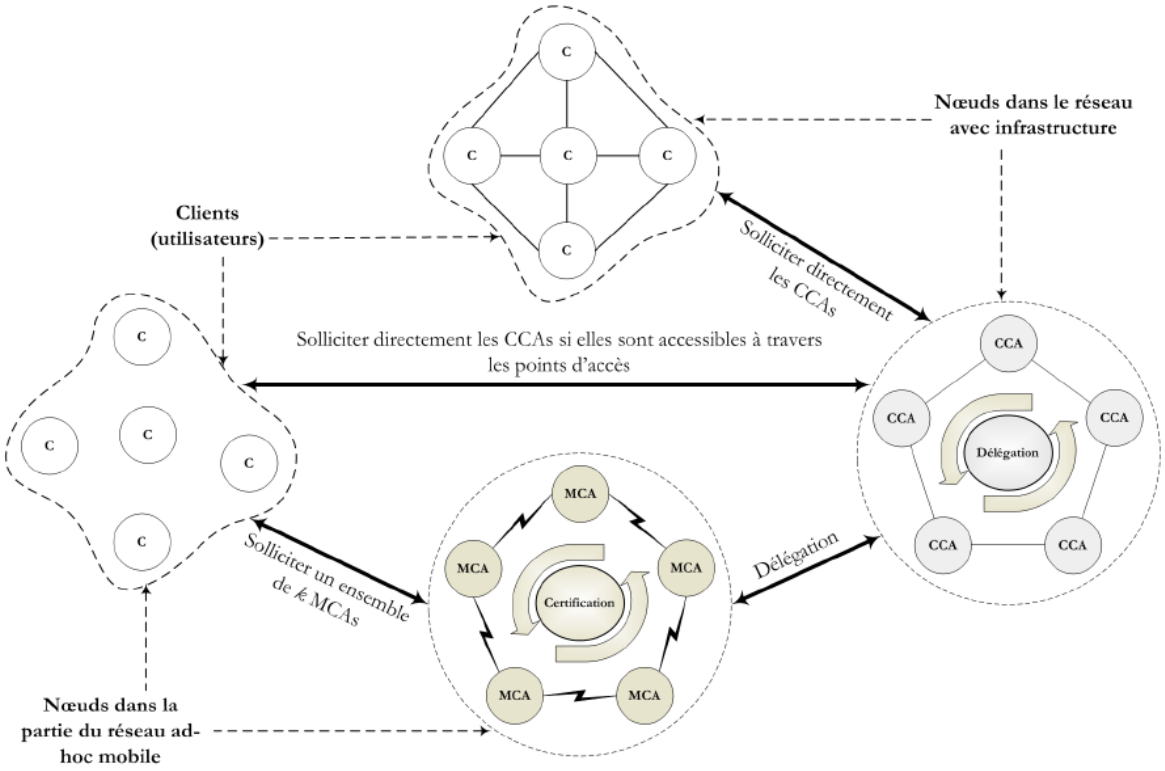


Figure 6 Modèle de confiance à seuil pour réseaux mixtes

L'architecture proposée est décentralisée, partiellement distribuée, et supporte la mobilité des nœuds et la défaillance de, jusqu'à, n-k parmi n autorités MCA. Pour mettre en valeur les qualités de performance de notre modèle, nous avons effectué des simulations intensives, qui ont montré que notre modèle fournit une grande flexibilité et plusieurs paramètres pour faire adapter l'architecture pour répondre aux besoins de l'application utilisée. En effet, nous avons montré qu'il est possible d'atteindre des compromis satisfaisant en termes de disponibilité du service de certification, temps de réponse du service, et taux de succès de certification, en ajustant certains paramètres de la solution, comme le seuil de cryptographie à seuil utilisée et le nombre de serveurs MCA (cf. Figure 7), la possibilité d'accès à l'infrastructure (cf. Figure 8), etc.

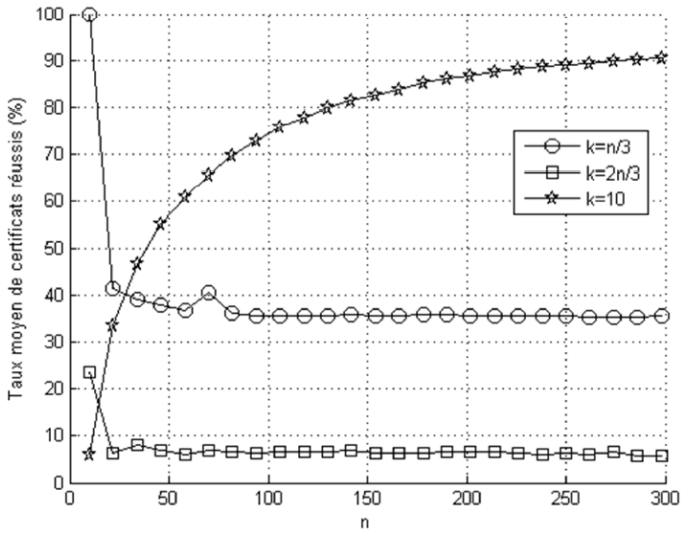


Figure 7 Impact du nombre de serveurs MCA et choix du seuil k sur le taux moyen de certificats réussis

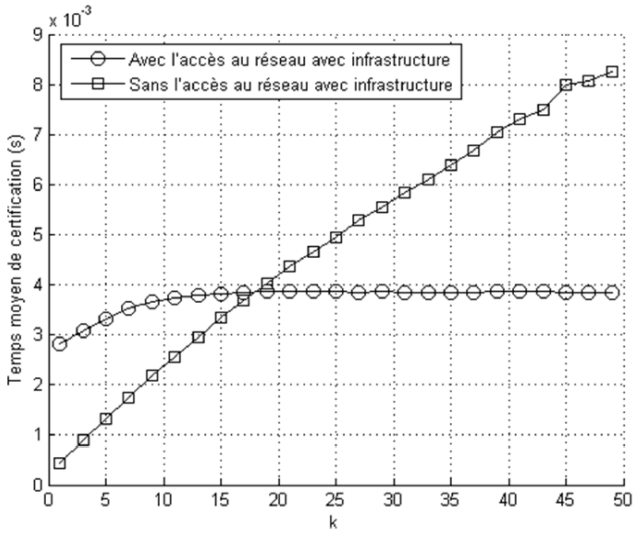


Figure 8 Comparaison du service avec et sans accès à la partie du réseau avec infrastructure par rapport au temps moyen de certification

2.2 La sécurité dans les réseaux pair-à-pair

Les réseaux pair-à-pair (P2P) offrent plusieurs avantages tels qu'un meilleur passage à l'échelle et une meilleure résistance aux pannes et par conséquent une meilleure qualité de service. Ces apports ont largement favorisé l'apparition de nouvelles applications qui offrent des services divers et variés tels que : le e-commerce, l'e-learning, le travail collaboratif, le stockage de fichiers, la voix sur IP, le partage de fichiers et le calcul intensif réparti.

Les applications P2P peuvent être sujettes à différents types d'attaques qui cherchent à nuire à leur fonctionnement. Les systèmes P2P sont vulnérables aux traditionnelles attaques réseaux comme le déni de service distribué (DDoS) [87], la propagation des virus/vers informatiques [88][89][90], les *« botnets »* [91][92][93], etc. En outre, les systèmes P2P sont particulièrement vulnérables à d'autres attaques spécifiques du fait du fonctionnement des systèmes P2P eux-mêmes qui s'appuient sur la collaboration et la coopération de ses pairs [94]. L'abus de confiance entre pairs peut poser de sérieuses menaces de sécurité sur un système P2P. De plus, dans un réseau P2P, des informations topologiques sous forme de tables de routage, et de listes de voisins sont partagées entre les pairs du système afin de répartir la charge de travail. Des nœuds malveillants peuvent exploiter ces informations afin de compromettre un réseau P2P [95].

De ce fait, la sécurité des réseaux P2P est remarquablement complexe et difficile à appréhender en prenant en considération leur nature décentralisée et ouverte. La garantie des services de sécurité devient elle-même un verrou scientifique et un défi technologique très important.

La complexité de ce défi a motivé un grand nombre de travaux de recherche qui ont abouti au développement de solutions de sécurité pour les réseaux P2P. La littérature dans ce domaine rapporte trois tendances principales. La première tendance est la conception de systèmes P2P résistants aux comportements malveillants. Il existe deux grandes approches pour renforcer la résilience d'un système P2P : l'intégration de système de réputation [96][97], et le développement de services d'identification de pairs [98][99]. Le principe de la deuxième tendance est de veiller à l'intégrité des données et le routage [101][100] au sein du système. Enfin, la troisième tendance concerne la sécurisation des communications P2P en temps réel, soit en appliquant des mécanismes cryptographiques aux données échangées entre pairs afin de protéger l'anonymat des utilisateurs [101], soit par l'intégration

de mécanismes d'incitation d'échange pour assurer l'équité entre les pairs [102][103], ou encore par la diffusion de patchs de sécurité pour prévenir les menaces de sécurité potentielles [104].

2.2.1 Propagation de vers dans BitTorrent

Il y a deux grandes caractéristiques qui distinguent les applications de partage de fichiers « pair-à-pair » (P2P). La première caractéristique est leur nature *ouverte* : ces applications sont conçues pour accueillir le plus grand nombre de pairs possible. Par conséquent, des pairs malveillants peuvent activement rejoindre un réseau P2P et attaquer le système de l'intérieur. La deuxième caractéristique est leurs simplicité et performance, souvent au détriment de la sécurité.

Notre objectif était d'analyser et d'identifier de nouvelles attaques sur les réseaux P2P. Nous nous sommes notamment intéressés à la sécurité du réseau BitTorrent. Des rapports récents [105] ont indiqué que près de 70% de tout le trafic Internet actuel P2P est dû à BitTorrent.

Rappel : BitTorrent

BitTorrent est un protocole P2P pour la distribution de contenu, conçu pour une réplication de données rapide, efficace et équitable [107]. BitTorrent est organisé en groupes d'utilisateurs, appelés « essaims » ou « swarms », intéressés par le téléchargement d'un fichier spécifique. Les utilisateurs d'un « swarm » coopèrent pour accélérer le processus de partage du fichier. Un « swarm » est composé de deux entités : un « tracker » et des pairs :

1. Un « tracker » maintient une trace de tous les pairs intéréssés par un fichier spécifique. Chaque « swarm » est géré par un « tracker ».
2. La deuxième entité est l'ensemble des pairs actifs : les « seeds » et « leechs ». Un « seed » est un pair qui a téléchargé l'intégralité d'un fichier partagé. Un « leech » est un pair qui est en cours de téléchargement d'un fichier partagé.

Un serveur, le plus souvent un serveur web, est aussi important dans le fonctionnement de BitTorrent. Le rôle de ce serveur est de fournir un fichier dit « torrent » pour les clients intéressés par le téléchargement d'un fichier spécifique. Le fichier « torrent » contient l'information nécessaire pour les clients pour préparer le téléchargement et joindre les « swarms ». La Figure 9 illustre le fonctionnement de BitTorrent et résume la terminologie utilisée dans le cadre de ce protocole P2P.

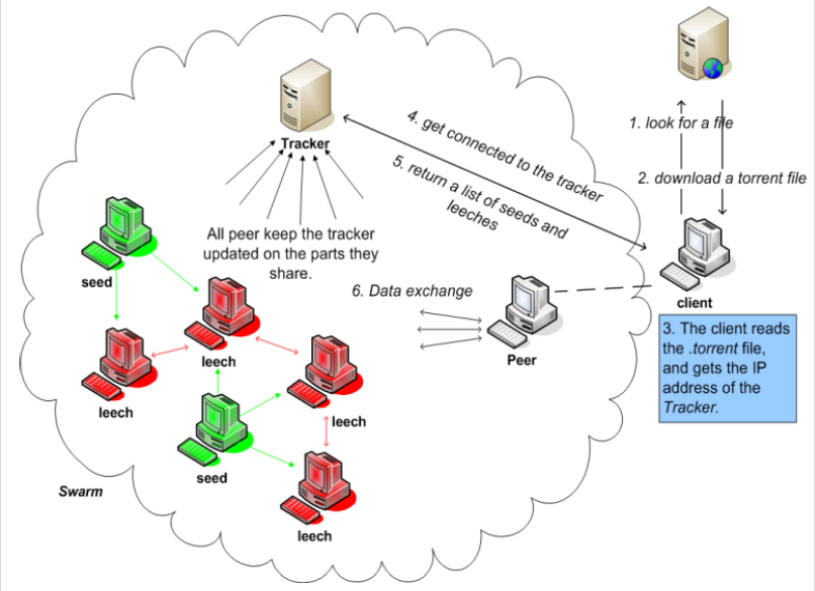


Figure 9 Fonctionnement de BitTorrent

Après avoir analysé les différentes attaques qui menacent les réseaux P2P dans un premier temps, et après avoir étudié les causes et les conséquences de chaque attaque dans un second temps, nous estimons que la propagation de vers actifs est l'une des attaques les plus dangereuses. Un ver informatique est un programme malveillant qui se propage d'une manière autonome sur un réseau, en se reproduisant d'une machine à une autre. Les effets des vers sur le fonctionnement d'Internet sont dévastateurs. Il a été signalé dans le rapport CSI Computer Crime and Security Survey 2010 [106] que près de 52% des attaques détectées sur Internet ont été les attaques des virus (vers / spyware).
Nous avons mené une étude et avons identifié des vulnérabilités dans le système de partage de fichiers P2P le plus utilisé aujourd'hui [5][6]: BitTorrent. Ces vulnérabilités encouragent la propagation d'un nouveau type de vers, que nous avons appelés BTW (BitTorrent Worm) [6]. BTW est un ver topologique, c'est-à-dire qu'il exploite les informations topologiques trouvées sur sa victime pour attaquer d'autres pairs. BTW augmente continuellement la taille de son voisinage et donc ses victimes potentielles. En effet, les pairs infectés par BTW se déclarent « seeds » pour attirer de nouveaux voisins « leechs », ce qui augmente la taille du voisinage du pair infecté.
Contrairement aux vers topologiques existants, BTW renforce sa propagation grâce à une coopération entre ses pairs infectés en se partageant des informations sur leurs victimes. Cette coopération se manifeste à deux niveaux : au niveau des « swarms » et au niveau du réseau BitTorrent. Au niveau d'un « swarm », quand un pair infecté réussit à infecter une nouvelle victime, il lui donne une liste des machines déjà « scannées » pour lui éviter de perdre sa capacité d'attaque sur des machines déjà scannées. La coopération au niveau du réseau BitTorrent passe par la construction d'une « hitlist » (liste de cibles) de « trackers » qui gèrent les « swarms » les plus peuplés. Un pair infecté, rejoint continuellement les « swarms » sur cette liste et attaque leurs membres. Le pair infecté, communique la moitié de sa « hitlist » à sa victime, et ainsi de suite. Quand la « hitlist » est épuisée, les pairs infectés attaquent le réseau Internet aléatoirement. L'algorithme détaillé de BTW est illustré dans les Figure 10 et Figure 11:

Algorithm 1 BTW Infection

```
P = 0 {list of peers to infect}
C = constant {attack capacity}
Cr = C {remaining attack capacity}
Cu = 0 {used attack capacity}
i = 0 {last index retrieved in tracker Hitlist}
N = 0 {list of neighbors}
HT {the Hitlist of popular swarm}
while true do
   N = new neighbors
   if !empty(N) then
      Cu = min(Cr, capacityOfAttack(N))
      P = peersToAttack(Cu)
      startAttack(P)
      Cr = C − Cu {see algorithm 2}
   end if
   if i < HT.length AND Cr > 0 then
      joinSwarmAtHT(i)
      i = i + 1
      if Cr > 0 then
         randomAttack(Cr) {see algorithm 2}
      end if
   end if
end while
```

Figure 10 Algorithme de propagation de BTW

Algorithm 2 startAttack(N)

```
for each n in N do
  if n is vulnerable and non-infected then
    I passes HT/2 to n
    I passes the list of scanned nodes to n {so n does not waste its C scanning them again}
    Cr++
  end if
end for
```

Algorithm 3 randomAttack(int i)

```
while i > 0 do
  randomly choose n
  if n is vulnerable and non-infected then
    I passes the list of scanned nodes to n
    Cr++
    i--
  end if
end while
```

Figure 11 Algorithme de propagation de BTW (suite)

Nous avons modélisé la propagation de BTW [5] et notre analyse montre que BTW est doté d'une capacité de propagation trois fois plus rapide que les autres vers connus comme l'illustre la Figure 12.

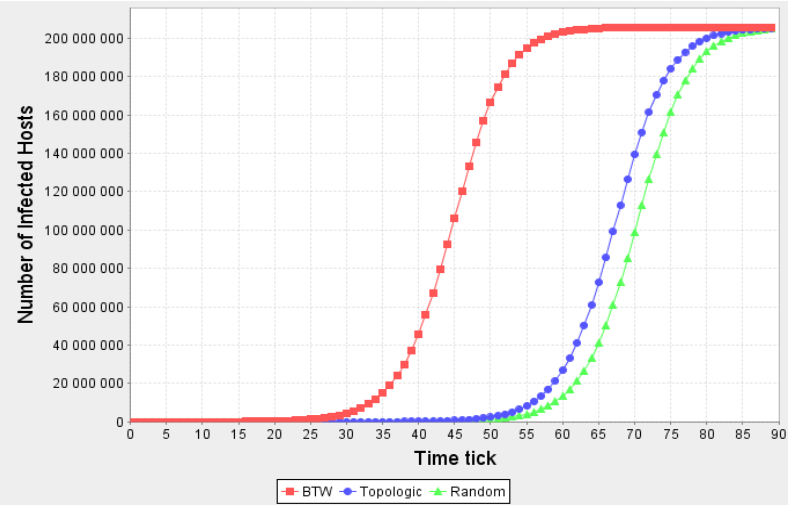


Figure 12 Rapidité de propagation selon différentes stratégies d'attaque.

2.2.2 Détection et confinement de vers dans BitTorrent

Ces résultats nous ont poussé à mettre au point une solution collaborative de détection et de confinement pour arrêter la propagation de BTW et de tout autre vers à travers BitTorrent. Un tel système de détection et de confinement de vers doit être discret, robuste et rapide pour être efficace. Dans cette optique, nous avons opté pour une solution distribuée. Notre système nommé BitTorrent Worm Sensor Network (BWSN) [6] est un réseau « overlay » d'agents d'inspection d'intrusion immunisés opérant au-dessus de BitTorrent. L'objectif de ces agents est de détecter une propagation de vers. Une fois l'attaque détectée par un agent, ce dernier envoie une alerte à tous les autres agents, qui à leur tour alerteront les machines voisines. La Figure 13 illustre les différentes actions entreprises par ce réseau de sentinelles dans le cas de détection d'une infection par un ver.

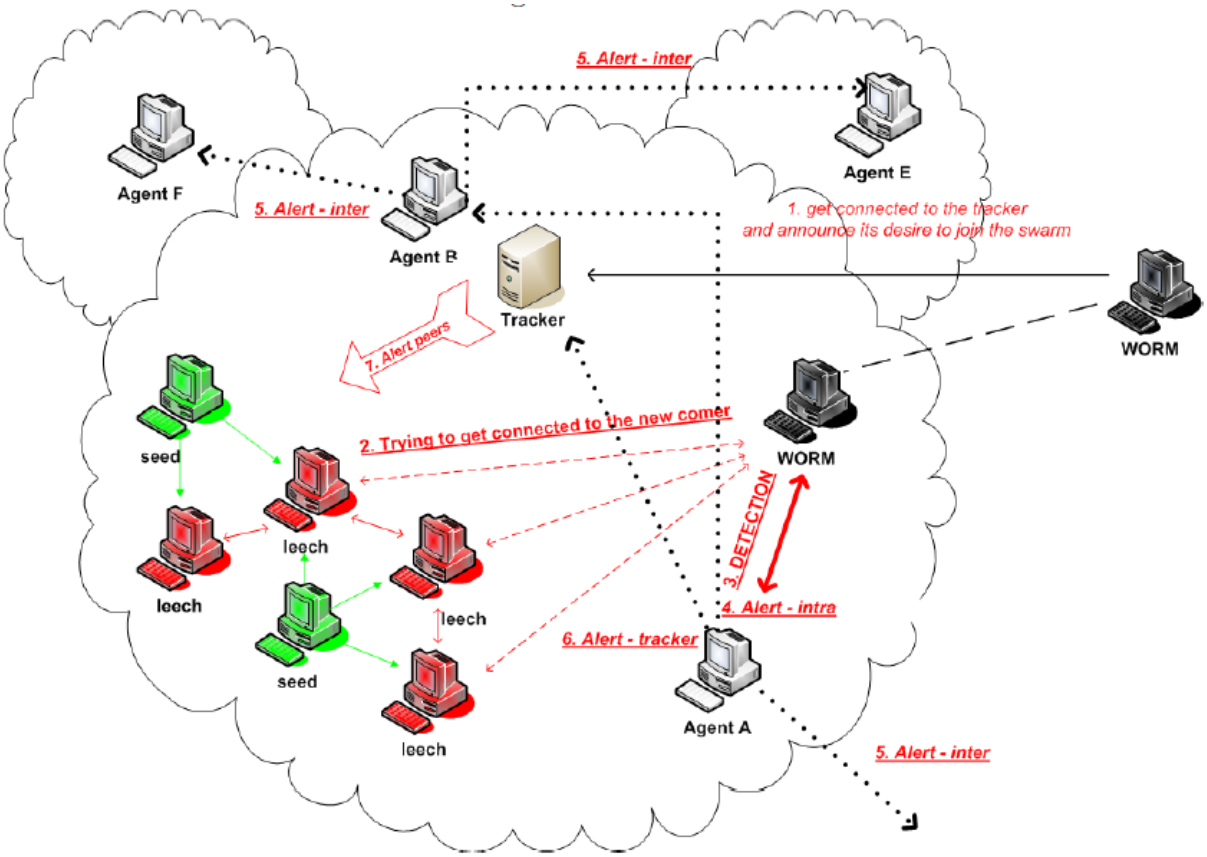


Figure 13 Coordination des agents BWSN pour la diffusion d'alertes

Nos analyses montrent que l'intervention de BWSN permet une réduction de 95% du taux d'infection global et sous une heure dans le pire des cas comme l'illustrent les Figure 14, Figure 15 et Figure 16.

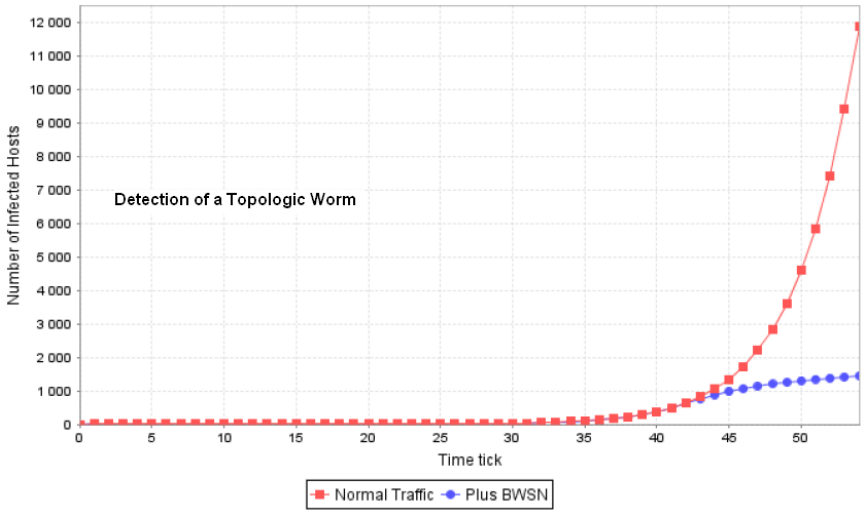


Figure 14 Impact de BWSN sur la propagation de vers topologiques

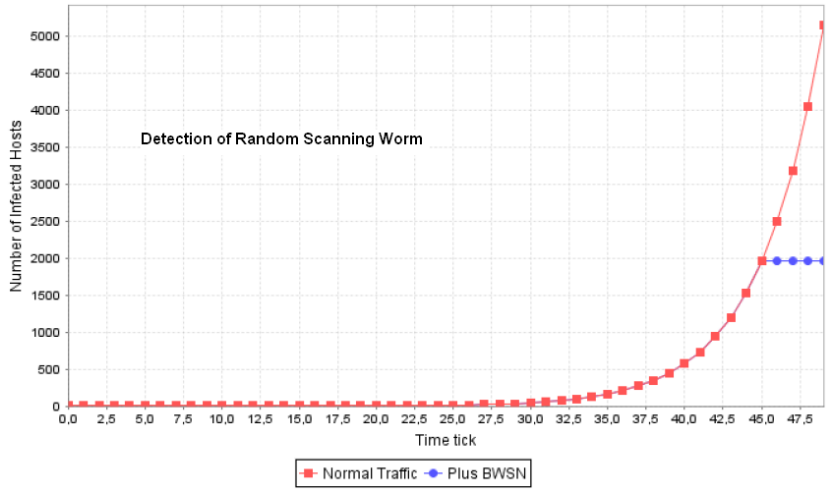


Figure 15 Impact de BWSN sur la propagation de vers aléatoires

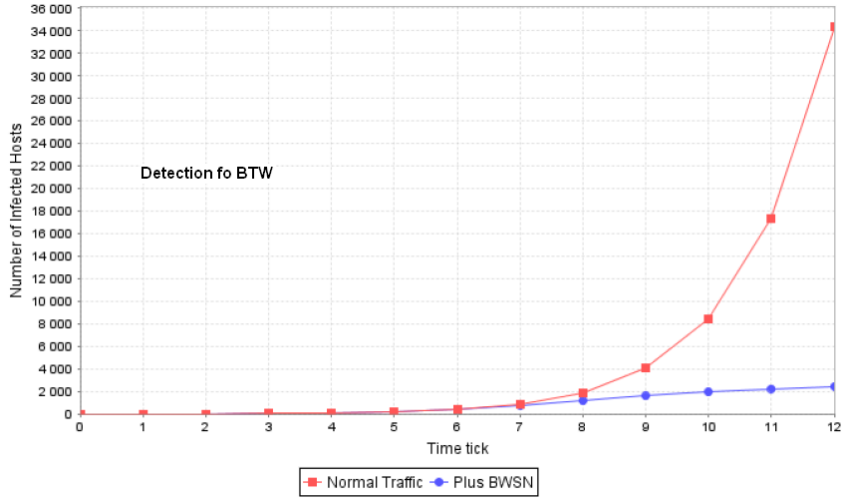


Figure 16 Impact de BWSN sur la propagation de BTW

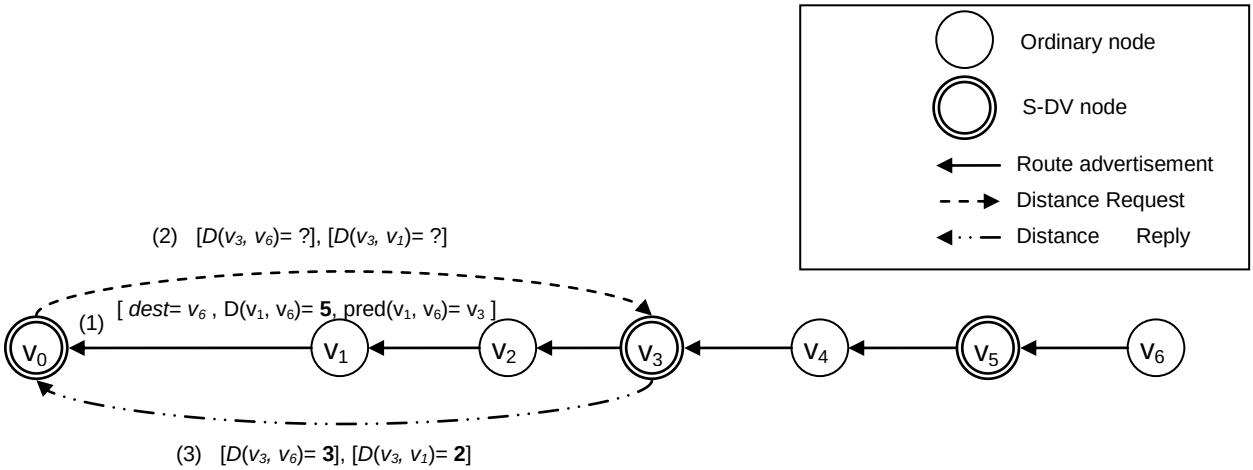
2.3 Approche collaborative pour la sécurité du routage

Les protocoles de routage ont été conçus pour maintenir dynamiquement des routes entre n'importe quelles entités communicantes malgré les changements potentiels de la topologie du réseau. La majorité des applications réseaux reposent sur cette fiabilité hypothétique des protocoles de routage. De ce fait, une anomalie (faute, panne, attaque, …) au niveau du routage peut compromettre la fiabilité d'applications critiques sur Internet et causer des dommages collatéraux importants [109].

Nous nous sommes intéressés en particulier à la sécurité du routage à base de vecteurs de distance. Cette catégorie de protocoles est connue pour sa vulnérabilité à cause de la vue partielle, limitée au voisinage immédiat, que peuvent avoir les routeurs. Une menace majeure est le fait qu'un seul routeur malicieux pourrait interrompre la fonction de routage en envoyant des messages incorrects de mise à jour de la table de routage. Ces messages erronés peuvent isoler certains routeurs du réseau ou favoriser certaines routes au profit des nœuds malicieux. Ces mises à jour malicieuses peuvent être envoyées par des attaquants externes et internes. Un attaquant externe peut injecter des messages de routage erronés, rejouer d'anciens messages de routage, ou modifier des messages valides. Par conséquent, le message erroné injecté se propage dans le réseau où il pourrait perdurer durant une

période relativement longue et ainsi entraver le bon fonctionnement de plusieurs routeurs. Un attaquant interne est un routeur qui aurait été fiable initialement puis serait compromis ou qui aurait tout simplement altéré son comportement initialement fiable. Ce type d'attaquant peut causer des dommages plus importants. En effet, ils peuvent envoyer à leurs voisins des messages de signalisation erronés. Ces messages changent la vue locale de la topologie, de leurs voisins, ce qui pourrait isoler certains routeurs du réseau ou favoriser certaines routes au profit des nœuds malicieux.

Dans ce contexte, nous avons proposé une nouvelle approche collaborative pour sécuriser le routage à base de vecteurs de distances « Secure Distance Vector routing protocols (S-DV) » [8]. L'idée principale est de désigner certains routeurs de confiance, que nous avons appelé routeurs S-DV, qui collaborent dans le contrôle de cohérence des messages de mise à jour du routage. Cette approche repose notamment sur un mécanisme de contrôle que nous avons appelé « Distance Request and Distance Reply Protocol » (cf. Figure 17). Ce mécanisme offre une détection déterministe de la fraude sur la valeur du vecteur de distance. Par ailleurs, les routeurs S-DV utilisent une nouvelle métrique que nous désignons par « Security Indicator ». Cette métrique permettra de préférer une route plus sécurisée à une route plus courte mais soumise à des attaques fréquentes.



Cette figure illustre le vecteur de distance envoyé de v_1 à v_0 composé de 3 champs: [*dest, D(v_1, dest), pred(v_1, dest)*] qui désignent respectivement: la destination, la distance et le prédécesseur de cette route. Quand v_1 reçoit cette mise-à-jour, il vérifie sa consistance en envoyant un message « Distance Request » au prédécesseur v_3 de cette route, lui demandant ses distances locales *D(v_3, dest)* et *D (v_3, v_1)*. Ce prédécesseur v_3 consulte sa table de routage et répond à cette requête avec un message « Distance Reply ». Quand v_0 reçoit ce message, il vérifie si la somme de ces distances est égale à la distance annoncée dans le vecteur de distance (formule 1). Si c'est le cas, la route est acceptée sinon elle est rejetée.

$$D(v_1, dest) = D(v_3, dest) + D(v_3, v_1) \qquad (1)$$

Figure 17 Scénario de vérification S-DV

Notre analyse du protocole contre les menaces de sécurité, notamment avec le moteur de vérification de protocoles de sécurité AVISPA [66], montre l'efficacité de notre approche contre les comportements malicieux. Le protocole de vérification de la consistance des routes est exécuté uniquement par quelques routeurs de confiance (routeurs S-DV). Ceci réduit le surcoût de la solution et facilite l'adaptation au facteur d'échelle.

En outre, contrairement aux protocoles de routage conventionnels, grâce à notre mécanisme de vérification des annonces de vecteurs de distance, les nœuds du réseau peuvent être évalués avec un indicateur de sécurité dont la valeur dépend de la fréquence des annonces incorrectes émanant du routeur. Cet indicateur peut être utilisé pour sélectionner des routes plus sûres.

Nous avons appliqué notre solution à une architecture de communication à base d'un réseau « mesh », comme illustré par la Figure 18. Nous avons considéré le protocole de routage DSDV [108] auquel nous avons rajouté notre mécanisme de vérification des routes. Nous avons appelé cette nouvelle version Trusted-DSDV (T-DSDV) [27].

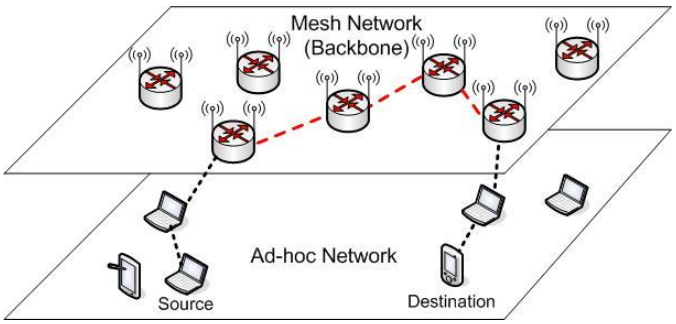


Figure 18 Hybrid Wireless Mesh network

Les résultats de simulation que nous avons obtenus à l'aide du simulateur NS-2 [63] montrent que les surcoûts de notre protocole T-DSDV sont moins importants que d'autres solutions de la littérature comme S-DSDV [110] (cf. Figure 19), tout étant résilient aux attaques à base de faux messages de signalisation.

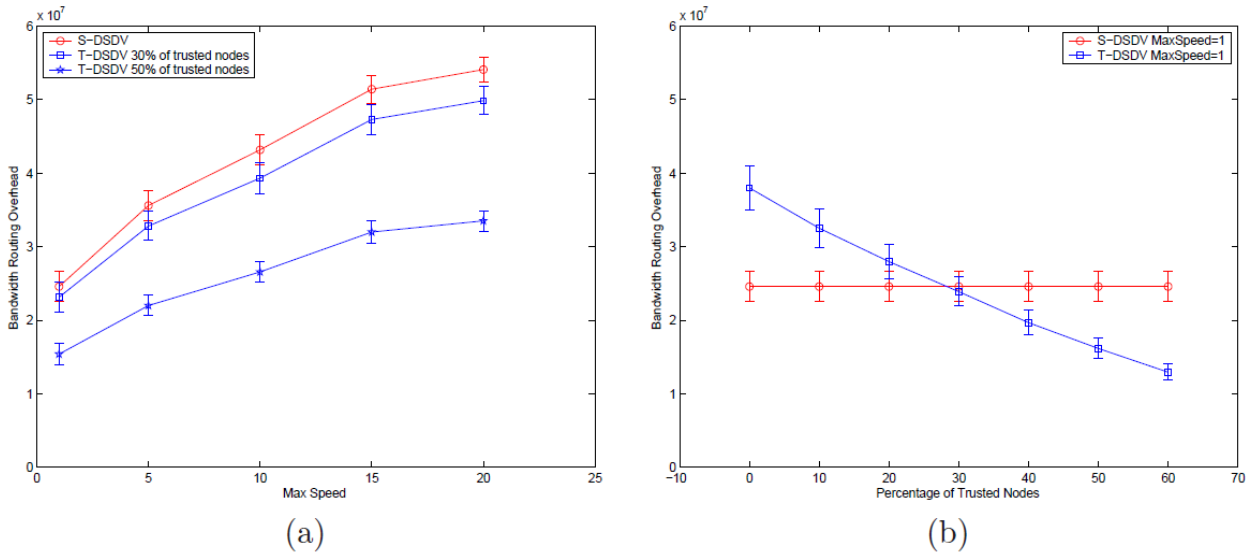


Figure 19 (a) Surcoût de bande passante vs vitesse maximale des nœuds, (b) Surcoût de bande passante vs pourcentage de nœuds de confiance

2.4 Conclusion

Dans ce chapitre nous avons présenté nos travaux autour de la sécurité coopérative des systèmes. Nous avons montré que les attaques de plus en plus sophistiquées des systèmes, et les attaques internes qui sont naturellement asymptotiques aux comportements légitimes des processus d'un système nécessitent une nouvelle appréhension de la sécurité de ces systèmes. Cette une nouvelle approche est basée sur la coopération d'entités de confiance et la réputation. Cette coopération permet d'un côté de garantir le bon déroulement des fonctions vitales du système : le routage dans un réseau, le partage de fichiers dans un système pairs-à-pairs, la gestion de clés, etc. En outre elle permet de renforcer la sécurité du système en détectant et en confinant d'éventuelles attaques : falsification de messages de signalisation du routage, propagation de vers dans un système pairs-à-pairs, etc.

Nous avons ainsi, abordé cet axe en définissant un nouveau modèle de confiance distribué et robuste. Nous avons également proposé des solutions basées sur des entités de confiance pour la sécurité du routage et la détection et le confinement de vers dans les réseaux BitTorrent.

Nous croyons que la *sécurité à travers la coopération d'entités de confiance* est une évolution assez naturelle de la sécurité des systèmes. En effet, la nature *« envahissante » et quasi omniprésente* des attaques de sécurité et l'aspect « *heuristique »* des outils de détection et de confinement des attaques a fait émerger cette approche basée sur la coopération et la réputation, approche à la fois proactive et réactive, qui vient combler les limites des outils contemporains de la sécurité.

Chapitre 3 : La sécurité dans les réseaux de capteurs sans fil

Depuis une décennie, nous assistons à une prolifération des domaines d'application potentielle des réseaux de capteurs sans fil (RCSF). Par conséquent, un nombre important de travaux de recherche ont été menées par les communautés universitaires et industrielles. Cependant, vu la sensibilité des applications potentielles qui sont généralement étroitement liées au monde physique et même aux êtres humains, un déploiement à grande échelle de RCSF dépend de la fiabilité qu'offre cette technologie émergente. En particulier, la sécurité émerge comme une question difficile dans les RCSF en raison de la limitation des ressources (énergie, mémoire, bande passante, etc.) dans ce type de réseaux.

3.1 Sécurité dans les réseaux de capteurs sans fil : état de l'art

Nous avons étudié les problèmes de sécurité et de fiabilité dans les RCSF [9][8][18]. Nous avons conclu que ces menaces sont héritées de la nature même des RCSF comme illustré sur la Figure 20 :

Limitation de ressources: la contrainte d'énergie est l'une des principale limitations qui impactent sévèrement la fiabilité et l'intégrité des données dans un RCSF. Des techniques de mise en veille, d'agrégation [113] et de « clustering » [111] sont proposées pour la conservation de l'énergie. Néanmoins, une attention particulière est requise pour la détection d'injection de données erronées et/ou fausse notamment dans le cas de dissémination de données avec agrégation [114][115][116][117].

Communication multi-sauts et sans fil : la portée radio des nœuds capteurs est limitée à cause de la limitation de l'énergie. Une communication multi-sauts est alors indispensable dans un RCSF. Cette nature multi-saut des communications ouvre lavoie à des menaces d'attaques de sécurité à deux niveaux : attaques contre la construction et la maintenance des routes [118][119][120], et attaques d'altération de données à travers l'injection, la modification et la suppression de paquets [121][122][123]. En outre, la communication sans fil introduit de nouvelles vulnérabilités au niveau des couches réseaux basses (liaison et physique) comme des attaques de type déni de service : « jamming » [124] et épuisement de l'énergie des nœuds récepteurs [125].

Absence de protection physique: les applications de RCSF nécessitent un déploiement à proximité ou à l'intérieur du milieu physique à superviser. Ceci engendre une compromission fréquente accidentelle ou intentionnelle des nœuds du réseau. Comme le succès de ces applications est aussi lié à leur bas coût, il est difficile de conférer une protection physique à tous les nœuds du réseau. En conséquence, les nœuds d'un RCSF sont sujets à des attaques physiques où un adversaire (avec suffisamment de moyens) peut extraire des nœuds des informations sensibles (clés cryptographiques, par exemple). Ce type d'attaque est d'autant plus plausible que les nœuds sont généralement déployés dans un environnement ouvert sans surveillance.

La Figure 20 résume les problèmes de sécurité qui découlent des caractéristiques des RCSF, ainsi que les fonctionnalités requises pour une meilleure sécurité et robustesse de cette technologie.

Nous avons travaillé, ces dernières années, sur plusieurs blocs fonctionnels indispensables pour la sécurité et la robustesse des RCSF : gestion de clés distribuée et résiliente, routage sécurisé multi-chemins, et agrégation de données avec contrôle d'intégrité, que nous présenterons dans les sections suivantes.

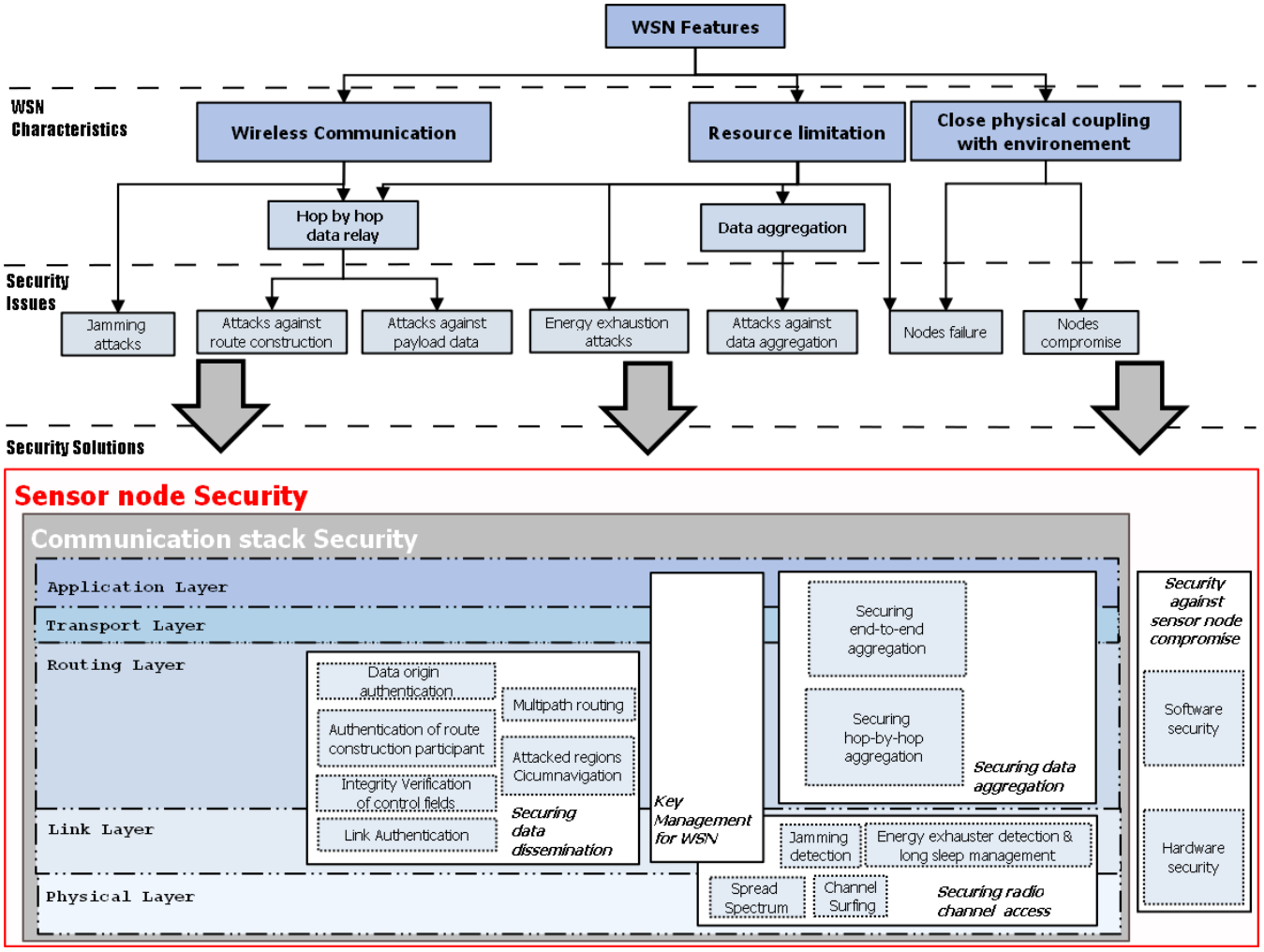


Figure 20 Les challenges de sécurité dans les réseaux de capteurs sans fil

3.2 Gestion de clés dans les réseaux de capteurs sans fil

La gestion de clé est une fonction indispensable dans tout système cryptographique pour assurer des services de sécurité comme la confidentialité, l'authentification, la non-répudiation, etc. C'est un des aspects les plus difficiles de la configuration d'un système cryptographique de sécurité. Pour qu'un tel système fonctionne et soit sécurisé, chacun des nœuds communicants doit disposer d'un ensemble de clés secrètes (dans un système à clés secrètes) ou de paire de clés publiques/privés (dans un système à clés publiques). Ceci implique la génération des clés, leur distribution de manière sécurisée aux utilisateurs, et leur stockage. Dans les systèmes à clés publiques, la gestion des clés comprend la capacité à vérifier et à gérer les clés publiques des autres utilisateurs qui sont signées sous formes de certificats numériques (cf. Figure 21).

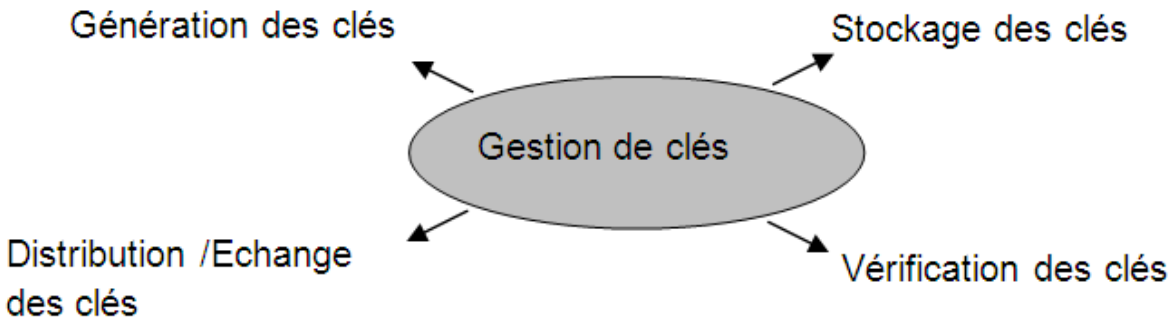


Figure 21 Les fonctions de gestion de clés

Si les fonctions de gestion des clés présentées dans la figure ci-dessus semblent assez simples, plusieurs problèmes de sécurité se posent.
Si les clés secrètes ou privées ne sont pas générées de manière sécurisée, un adversaire peut deviner la clé en utilisant un algorithme de génération. Si un nœud du réseau ne peut pas stocker ses clés de manière sécurisée, elles peuvent être mises en péril. Un tiers peut décrypter les données ou les communications du nœud ou signer faussement des objets comme s'ils provenaient de ce nœud. C'est particulièrement significatif si les clés sont enregistrées sur un nœud sans protection physique ou surveillance humaine. Si le système de gestion des clés employé dans un RCSF fait qu'il puisse perdre la trace de ses clés et ne gère pas la récupération des clés, des informations importantes cryptées peuvent devenir inaccessibles. C'est souvent aussi grave que de voir des données détruites à cause des failles dans le système de gestion des clés. Si le système de gestion des clés ne permet pas à un nœud de vérifier leur authenticité, il peut être possible de se faire passer pour quelqu'un d'autre.

3.2.1 Gestion de clés dans les réseaux de capteurs : classification

Les communications dans un réseau de capteurs ne peuvent pas se fonder sur la disponibilité d'une infrastructure fixe ou d'un administrateur central, ce qui nécessite des techniques de gestion de clés décentralisées. Par ailleurs, les solutions à base de clés publiques, qui offrent une gestion de clés efficace dans les réseaux conventionnels, sont inadaptées aux RCSF à cause des limitations de ressources. Ainsi, l'établissement de clés symétriques est une alternative plausible pour assurer des services de sécurité dans les RCSF.

Le problème de gestion des clés dans les réseaux de capteurs sans fil a été largement étudié dans la littérature et plusieurs solutions ont été proposées [9]. Nous distinguons deux grandes catégories de systèmes de gestion de clés dans les RCSF (cf. Figure 22): les systèmes déterministes et les systèmes probabilistes. Dans les systèmes déterministes [132][133][134][135][136], deux nœuds voisins peuvent établir un lien sécurisé ce qui garantit une couverture sécurisée totale du réseau. Dans les systèmes probabilistes [126][127][128][129][130][131], la connectivité sécurisée n'est pas garantie et dépend de l'existence de clés partagées entre les nœuds voisins.
Dans les deux catégories, une approche basée sur la pré-distribution de clés se distingue. En effet, la pré-distribution de clés symétriques est une catégorie de gestion de clés prometteuse pour les RCSF en raison de leur limitation de ressources. Dans cette catégorie, les nœuds sont pré-chargés d'un trousseau de clés à partir d'un lot commun de clés. Puis, au déploiement, les nœuds découvrent des clés communes qui seront utilisées pour

sécuriser les échanges. Cette manière de pré-charger les nœuds avec des clés, permet de minimiser les échanges de messages qui auraient été nécessaires pour établir ces clés communes. Par conséquent, l'énergie des nœuds qui aurait été consommée par la transmission de ces messages sera préservée.

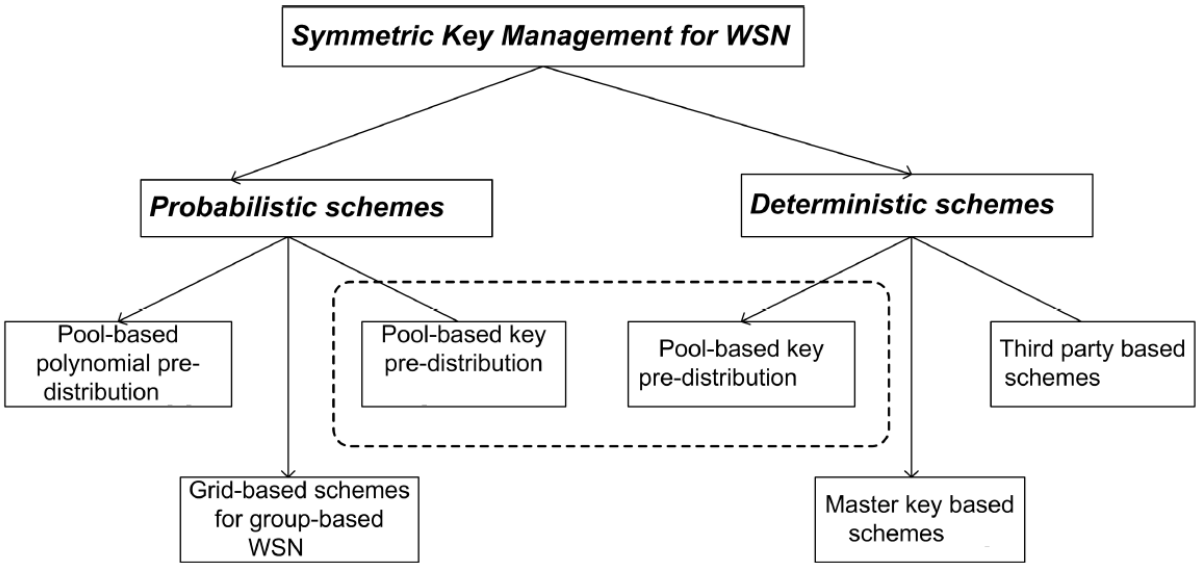


Figure 22 Classification des systèmes de gestion de clés pour les RCSF

3.2.2 Gestion de clés efficace et résiliente dans les RCSF

Nous nous sommes intéressés particulièrement à la *résilience* des protocoles de pré-distribution de clés contre la compromission de nœuds du réseau. Nous définissons la « résilience » dans ce contexte par la capacité du système à se reconstruire après une attaque ou une panne.

Nous avons proposé une nouvelle classe d'un schéma de pré-distribution de clés [10][11]. Nous dénotons cette nouvelle classe par HC(x) où x est un schéma de pré-distribution de clés. Ce nouveau schéma peut être appliqué à toute solution existante basée sur une pré-distribution de clés. Nous avons démontré que notre approche améliore considérablement la résilience de cette catégorie de solutions. Le principe de notre schéma repose sur une transformation des clés identiques se trouvant sur des nœuds différents, de telle sorte que la compromission du trousseau de clés d'un nœud ne mette pas en péril tous les liens sécurisés avec les clés de ce trousseau. Dans notre schéma, avant le déploiement des nœuds du réseau, on applique à chacune de ses clés pré-chargées une fonction de hachage h, *i* fois (*i* étant un paramètre variable qui peut être l'identifiant du nœud par exemple). Une des caractéristiques des fonctions de hachage est qu'elles sont à sens unique. Ainsi, si un attaquant découvre le trousseau de clés d'un nœud, il ne pourra déduire que les versions dérivées de ces clés. Ce qui améliore la résilience à la compromission de nœuds.

Considérons deux nœuds voisins i et j. Le nœud i (resp. j) applique i mod L (resp. j mod L) fois la fonction de hachage h à chacune des clés de son trousseau de clés. Quand les nœuds i et j découvrent un identifiant de clé commun id, leur clé commune sera alors $h^{max(i \bmod L, j \bmod L)}(K_{id})$. Le nœud min(i, j) peut alors calculer la clé commune en appliquant la fonction de hachage h |i mod L- j mod L| fois à K_{id} (cf. Figure 23).

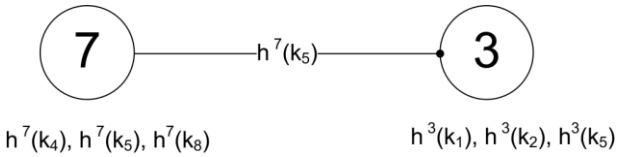


Figure 23 Illustration de l'approche à base de fonction de hachage

Dans la Figure 24, nous appliquons notre schéma de transformation des clés avec les opérations de hachage (Figure 24(b)). Dans le schéma basique sans cette transformation (Figure 24(a)), la compromission des nœuds 4 et 7 entraîne la compromission de tous les liens. Avec notre schéma, la compromission des mêmes nœuds n'entraînera la compromission que du lien entre ces deux nœuds (4,7).

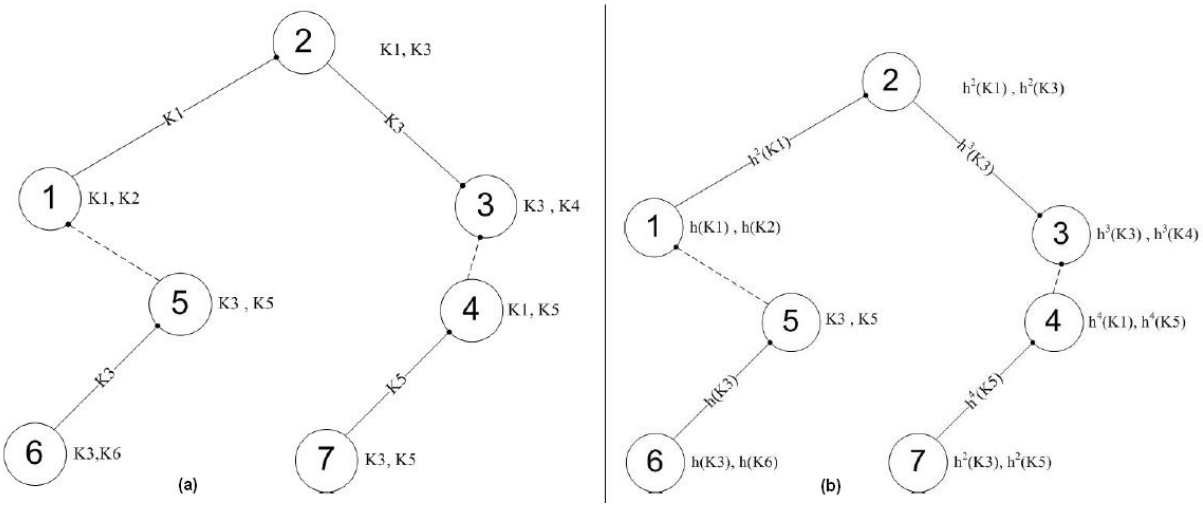


Figure 24 Exemple illustrant l'amélioration de la résilience avec notre schéma de gestion de clés

Nous avons appliqué notre approche à plusieurs schémas de pré-distribution de clés et nous avons montré à travers des calculs combinatoires et probabilistes que notre approche améliore la résilience de ces solutions. La Figure 25 illustre l'amélioration de la résilience et la connectivité sécurisée dans le cas de notre solution HC(Q-composite) en comparaison à une solution de la littérature Q-composite [128].

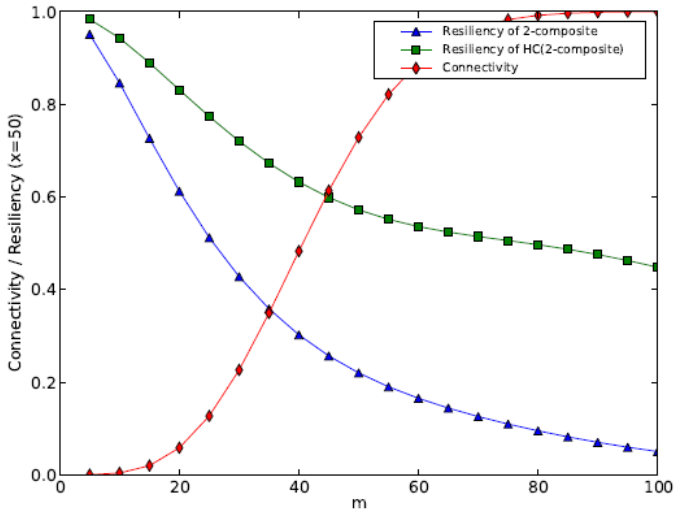


Figure 25 Connectivité et résilience vs. Taille du trousseau de clés.

Comme notre solution nécessite le calcul de fonctions de hachage plusieurs fois sur les trousseaux de clés de tous les nœuds, nous nous sommes intéressés à la consommation d'énergie induite par ces calculs. Pour cela, nous avons implémenté la fonction de hachage SHA-1 [137] et nous l'avons compilé pour le processeur des nœuds Mica2 [138] en utilisant TinyOS [64]. Puis nous avons utilisé le simulateur AVRORA [139] qui permet de faire une évaluation assez précise de l'énergie consommée. La Figure 26 illustre l'énergie consommée par les fonctions de hachage effectuées par notre solution HC(Q-Composite) pour Q=1,2,3 et les compare à l'énergie consommée induite par l'émission de 128 octets. Nous constatons que l'énergie consommée par notre solution est négligeable.

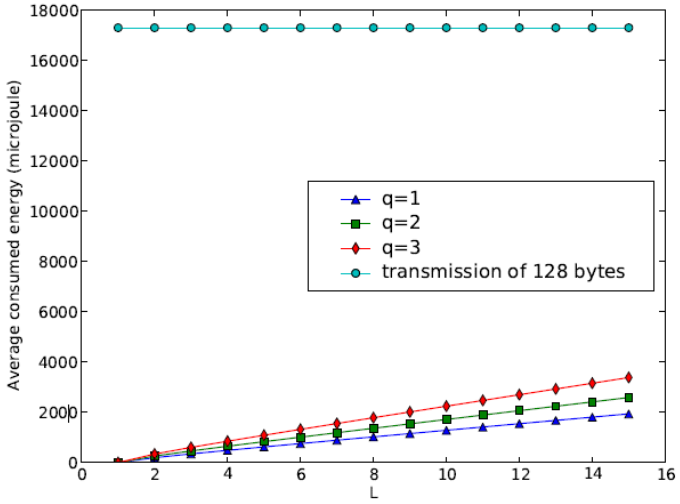


Figure 26 Surcoût de consommation d'énergie de HC(q-composite)

3.2.3 Nouvelle approche de pré-distribution de clés déterministe et scalable

Nous avons proposé une nouvelle approche [12][13] de pré-distribution de clés déterministe et scalable basée sur la théorie de la conception combinatoire. Cette théorie traite de l'existence et de la construction d'ensembles finis dont l'intersection jouit de propriétés spécifiques. Notre solution se base en particulier sur la construction dite « unital design ».

Définition : Unital Design
Un "unital design" consiste en un ensemble de $b = m^2(m^3 + 1)/(m + 1)$ sous-ensembles, appelés blocs, d'un ensemble de $v = m^3 + 1$ points. Chaque bloc contient $k = m + 1$ points et chaque point est contenu dans $r = m^2$ blocs. Chaque paire de points est contenue dans exactement un bloc.
On note un « unital design » par le triplet (m^3+1, m+1, 1). Sans perte de généralité, nous considérons dans notre solution les « unitals » hermitiens [14] qui existent pour tout m puissance d'un nombre premier.

3.2.3.1 Version naïve de pré-distribution de clés basée sur les « unitals » (NU-KP)

Dans une première version de notre solution, dite naïve, nous proposons de faire un simple mappage entre l' « unital design » et la pré-distribution de clés comme suit :

- on associe à chaque point de l' « unital » une clé distincte
- on associe à l'ensemble des points, le lot commun des clés
- on associe à chaque bloc de l' « unital » un trousseau de clés

Nous pouvons, ainsi, générer à partir d'un lot global de |S| = m^3+ 1 clés, n = $m^2(m^3+1)/(m+1)$ trousseaux de clés contenant chacun m+1 clés.
Avant le déploiement, on génère les trousseaux de clés, qui correspondent aux blocs de l' « unital », puis on pré-charge chaque nœud d'un trousseau distinct ainsi que les identifiants des clés qui le composent. Après le déploiement, les nœuds échangent les identifiants de leurs clés pour déterminer les éventuelles clés communes.
Cette version naïve de notre solution est très scalable dans le sens où elle permet de couvrir de très grands réseaux, de l'ordre de $O(m^4)$, alors que les solutions existantes basées sur la théorie du « design » se limitent à des réseaux de l'ordre de $O(m^2)$ (m+1 étant la taille d'un trousseau de clés). Ceci signifie aussi que pour un réseau de taille n, notre solution réduit remarquablement la taille des trousseaux de clés (surcoût de stockage dû aux clés) : de l'ordre de $O(\sqrt[4]{n})$, alors que les solutions comparables de la littérature nécessitent le stockage de trousseaux de clés de l'ordre de $O(\sqrt{n})$.
Cependant, cette solution naïve n'assure pas une grande probabilité de partage de clés pré-chargées. En effet, nous avons démontré que cette probabilité tend vers O(1/m) pour m très grand ce qui est insuffisant.

3.2.3.2 Version avancée de pré-distribution de clés basée sur les « unitals » (t-UKP)

Afin d'augmenter la probabilité de partage de clés pré-chargées dans les nœuds, dans cette version avancée, nous pré-chargeons chaque nœud avec *t* blocs disjoints (*t* étant un paramètre du protocole). L'objectif de cette construction est d'améliorer la probabilité de partage de clés communes entre nœuds voisins tout en maintenant une forte scalabilité.
Dans l'algorithme suivant, nous proposons une technique de distribution aléatoire pour pré-charger chaque *t* blocs disjoints dans chaque nœud du réseau.

```
1  Generate B =< B_q >, key sets corresponding to
   blocks of a unital design of order m
2  foreach Node_i do
3      KR_i = {}
4      while (|KR_i| ≤ t(m + 1)) do
5          pick B_q from B
6          if ((KR_i ∩ B_q) = ∅) then
7              KR_i = KR_i ∪ B_q
8              B = B − B_q
           end
       end
   end
```

Figure 27 Algorithme de pré-distribution de blocs de clés

Après le déploiement, deux nœuds voisins échangent les identifiants de leurs clés pour déterminer les clés communes. Contrairement à la version naïve, deux nœuds pourraient partager plus qu'une clé commune en utilisant cette construction. En effet, en s'appuyant sur les propriétés des « unitals », on peut démontrer que deux nœuds peuvent avoir en commun jusqu'à t^2 clés.
Si deux nœuds partagent une ou plusieurs clés, nous proposons que la clé de session entre les deux nœuds soit le code de hachage calculé sur la concaténation de l'ensemble des clés communes. Cette façon de calculer la clé de session entre deux nœuds, permet par ailleurs d'augmenter la résilience du réseau en cas de compromission de nœuds. L'intrus aurait alors besoin de plusieurs trousseaux pour compromettre un lien sécurisé.

Quand deux nœuds ne partagent pas de clés communes, ils doivent en partager une à travers un chemin sécurisé composé de liens sécurisés successifs.

3.2.3.3 Analyse de performances et comparaisons

Nous avons analysé les performances de notre solution et nous les avons comparées à deux solutions de la littérature qui se basent sur la théorie du « design » : SBIBD [133] et Trade-KP [134].

Comme on peut le voir sur la Figure 28, notre solution basée sur le « unital design » est plus scalable que les solutions existantes. Le coût du stockage de clés est remarquablement réduit ce qui permet d'atteindre des tailles de réseaux très élevées.

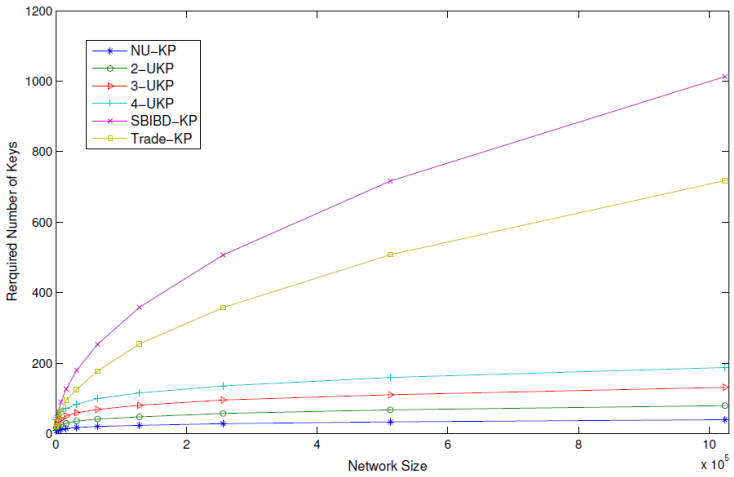


Figure 28 Surcoût de stockage en fonction de la taille du réseau

Nous avons évalué également la probabilité de partage de clés pré-chargées des trois solutions. Comme on peut le voir sur la Figure 29, SBIBD assure ce partage par construction. Dans le cas, de notre solution, t-UKP permet d'atteindre des probabilités élevées. En particulier, nous avons démontré que pour la configuration où $t = \sqrt{m}$, la probabilité de partage de clés a une borne inférieure égale à $1\text{-}e^{-1}$.

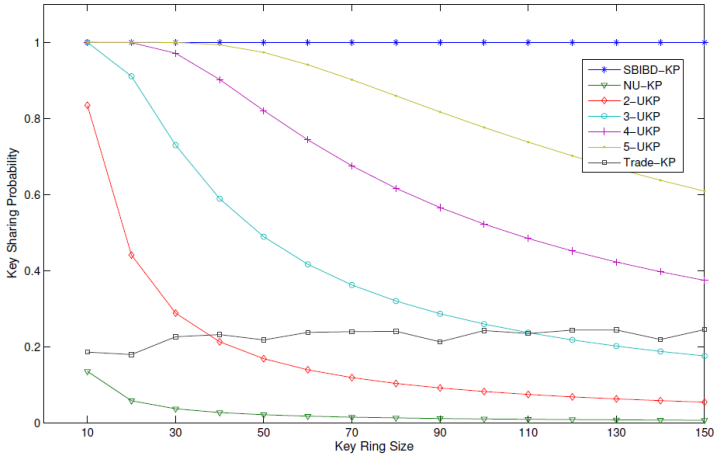


Figure 29 Probabilité de partage de clé en fonction de la taille du trousseau de clés

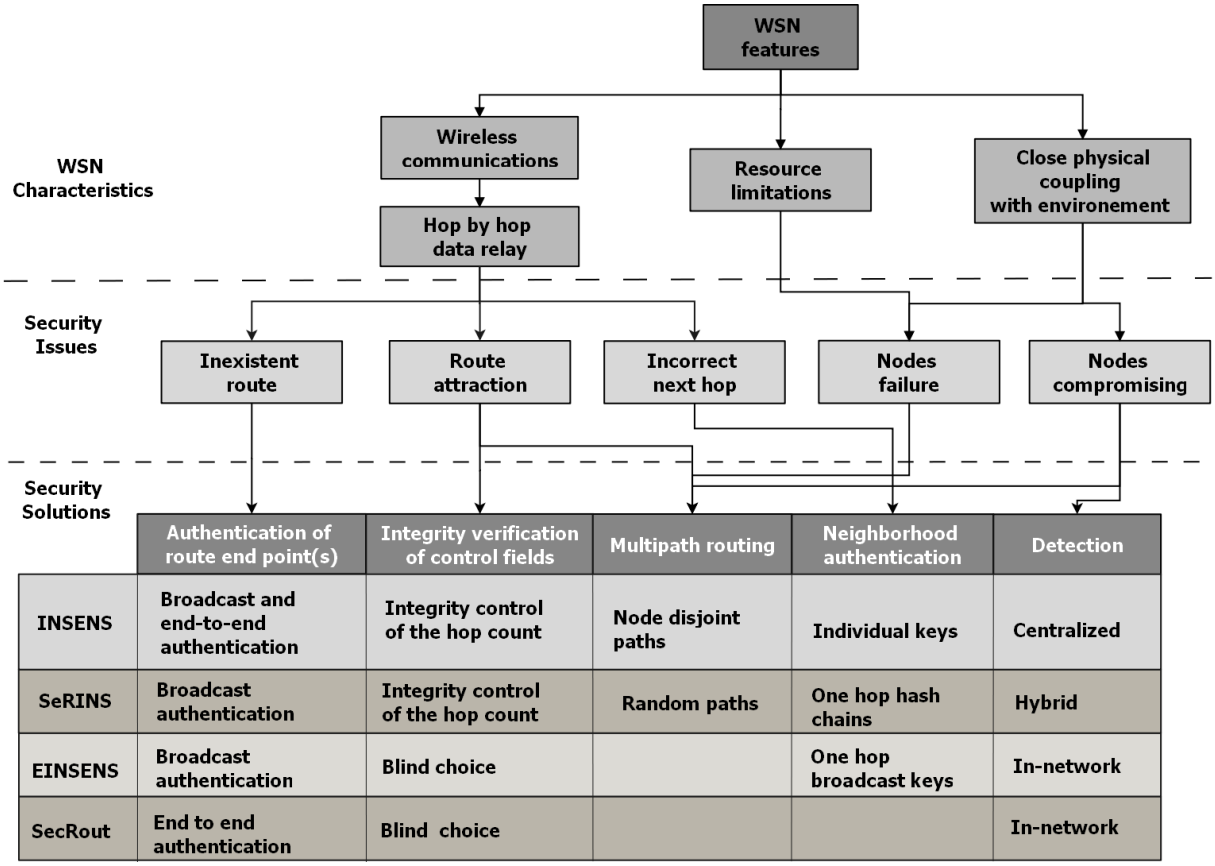
3.3 Sécurité du Routage dans les RCSF

Dans un système de communication multi-sauts, le routage est un service fondamental pour le fonctionnement du réseau. La position prédominante de ce service le rend une cible idéale

des attaques de sécurité. Par ailleurs, la limitation de ressources dans les RCSF les rend plus vulnérables aux menaces de sécurité.

3.3.1 Sécurité du routage dans les RCSF : état de l'art

La Figure 30 illustre les besoins de sécurité et les approches existantes pour sécuriser le routage.



	Authentication of route end point(s)	Integrity verification of control fields	Multipath routing	Neighborhood authentication	Detection
INSENS	Broadcast and end-to-end authentication	Integrity control of the hop count	Node disjoint paths	Individual keys	Centralized
SeRINS	Broadcast authentication	Integrity control of the hop count	Random paths	One hop hash chains	Hybrid
EINSENS	Broadcast authentication	Blind choice		One hop broadcast keys	In-network
SecRout	End to end authentication	Blind choice			In-network

Figure 30 Taxonomie de la sécurité du routage dans les RCSF

Pour protéger un RCSF contre les comportements malicieux qui entravent la fonction de routage, plusieurs mécanismes ont été proposés dans la littérature. Nous les classifions en trois grandes stratégies [9] : *évitement, détection et tolérance*.

L'*évitement* consiste à empêcher les intrus de prétendre la possession de meilleures routes. Certaines solutions (INSENS [118], SeRINS [120]) proposent de protéger les métriques utilisées (*« hop count »* par exemple) dans la signalisation de routes. D'autres solutions (EINSENS [118], SecRout [119]) optent pour une technique radicale en faisant un choix arbitraire des routes. La *détection* de routes corrompues nécessite une vérification continue des routes construites. Cette vérification peut être centralisée au niveau de la station de base qui devrait alors disposer d'une vue intégrale de la topologie (INSENS [118]). Comme elle peut être effectuée dans le réseau d'une façon distribuée par les nœuds capteurs (EINSENS [118]), ou encore, partagée entre la station de base et les capteurs qui jouent alors un rôle partiel dans la vérification (SeRINS [120]). De plus, les attaques de sécurité doivent être tolérées dans le fonctionnement du réseau. Parmi les techniques de *tolérance* aux intrusions et aux pannes figure le routage multi-chemins (INSENS [118], SeRINS [120]).

Ces deux protocoles ont adopté des approches assez différentes qui souffrent des inconvénients suivants: (i) INSENS [118] souffre principalement de sa lourdeur due à son approche centralisée. A chaque construction des routes, un nombre important de messages

de contrôle sont échangés entre les nœuds et la station de base (SB), ce qui fait qu'INSENS [118] ne peut être appliqué à de grands réseaux. Néanmoins, l'avantage primaire d'INSENS [118] est qu'il offre un contrôle total sur la qualité de la topologie de communication et sa fiabilité. SeRINS [120] essaye d'outrepasser l'inconvénient d'INSENS [118] en implémentant une détection semi-distribuée qui ne fait appel à la SB qu'en cas de comportements suspects. Toutefois, ce protocole ne permet pas la construction de routes disjointes. Ce choix fait que la topologie devient moins tolérante aux pannes et aux intrus vu la diminution du taux de redondance. Par conséquent, on peut dire que les solutions existantes n'offrent pas de compromis intéressant entre le niveau de tolérance du système et sa « scalabilité ».

3.3.2 Routage multi-chemins robuste et sécurisé pour RCSF

Nous avons proposé une nouvelle approche de routage multi-chemins, appelée SMRP (Sub-branch Multipath Routing Protocol) [17], qui améliore significativement la résilience du réseau comparée aux solutions existantes. Par ailleurs, notre solution ne nécessite qu'un seul message par nœud pour la construction d'une topologie fiable. Nous avons également proposé un protocole efficace sécurisé, appelé SEIF (Secure and Efficient Intrusion-Fault tolerant protocol) basé sur le protocole SMRP [17]. SEIF ne nécessite aucune référence à la station de base pour la construction de routes ou leur vérification.
Les solutions de routage multi-chemins disjoints existantes reposent sur la notion de branche. Une branche est l'arbre dont la racine est un voisin immédiat de la station de base (SB). Les chemins appartenant à des branches différentes sont donc disjoints. Après une étude approfondie avec des simulations, nous avons conclu que cette approche limite le nombre de chemins disjoints par nœuds et diminue la résilience du réseau. De ce fait, nous avons allégé la contrainte d'appartenance à deux branches différentes en n'exigeant que l'appartenance à des sous-branches différentes comme illustré sur la Figure 31.

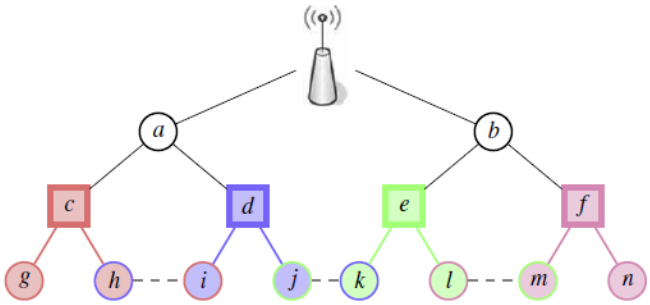


Figure 31 Construction de sous-branches avec SMRP. Le nœud i dispose de deux routes : une via d et l'autre via h. Dans une approche à base de routes entièrement disjointes, une seule des deux routes serait retenue.

De cette manière, les chemins disjoints que nous obtenons, *au regard de cette nouvelle définition*, sont beaucoup plus nombreux, ce qui améliore la résilience et la tolérance aux pannes. Bien évidemment, la contre-partie de cette approche est l'hypothèse que les nœuds voisins de la SB doivent être assez fiables. Cette hypothèse reste plausible vu qu'il n'est pas difficile de disposer d'un périmètre de sécurité autour de la SB où les nœuds sont protégés et dotés de plus de ressources (en énergie notamment) (cf. Figure 32).

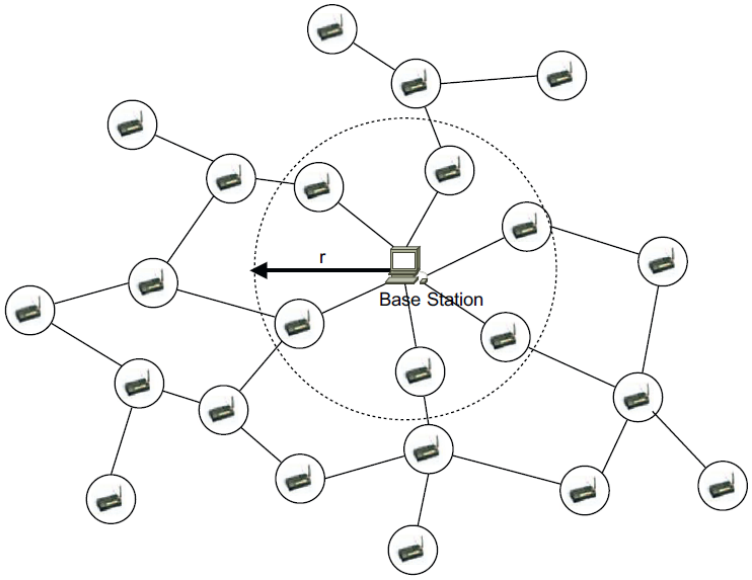


Figure 32 Périmètre de sécurité de rayon r autour de la SB.

Le problème principal du mécanisme basique de branches est l'utilisation des identificateurs des racines en tant que marque des branches. Cette information « en clair » permet à un attaquant de manipuler librement la vue de ses voisins et leurs décisions. Vu la présence éventuelle d'intrus internes, il n'est pas efficace d'utiliser un simple chiffrement pour protéger cette information (car les clés secrètes seront connues par l'intrus interne). Dans ce cas, le seul mécanisme efficace pouvant protéger les marques des branches est l'authentification d'origine. En effet, si on peut assurer que l'identificateur de la branche présumée provient réellement d'un voisin direct de la SB, un attaquant ne pourra plus injecter de fausses branches. Cependant, cette authentification doit vérifier les propriétés suivantes :

- Cette authentification doit suivre le modèle un-à-plusieurs, où la racine doit pouvoir produire une preuve vérifiable par n'importe quel capteur du réseau. Aucun autre capteur ne doit pouvoir générer à l'avance cette preuve, ce qui nécessite une certaine asymétrie rendant le mécanisme à sens unique.
- Elle doit être dynamique afin de résister aux attaques de re-jeu. Cela est nécessaire lorsque la topologie de routage doit être rafraichie périodiquement. Ainsi, les preuves d'authentification générées lors d'un tour i, doivent être invalides pour tout tour j > i.
- La solution choisie doit prendre en considération les contraintes des nœuds en conservant l'énergie et l'espace-mémoire.

Afin d'assurer ces trois propriétés, notre solution repose sur le concept de chaînes de hachage. Ce mécanisme permet d'offrir les propriétés requises, qui sont : l'asymétrie, le dynamisme et la préservation des ressources.

Rappel : Chaîne de hachage

Une chaîne de hachage à sens unique (*« One Way Hash Chain (OHC) »)* est utilisée comme générateur de nombres séquentiels à sens unique. Elle permet une authentification efficace d'une séquence de messages dans une communication un-à-plusieurs.

Elle consiste en une séquence de nombres $(K_i)_{0\le i\le n}$ générés à partir d'une graine aléatoire K_n comme suit : $K_i = F(K_{i+1})$, où F est une fonction de hachage à sens unique (cf. Figure 33). Cette chaîne est stockée au niveau du nœud source. Les éventuels nœuds récepteurs des futures messages de la source, sont chargés avec la première valeur uniquement : K_0 (appelée *vérificateur de la chaîne ou graine d'authentification*). Pour chaque message envoyé, le nœud source révèle une nouvelle valeur de la chaîne dans le sens inverse de la génération, i.e. $K_1, K_2, ..., K_n$ (cf. Figure 33). Comme les récepteurs sont chargés avec K_0, ils peuvent vérifier l'appartenance à la chaîne (et donc l'authenticité) de toute valeur reçue, en utilisant la propriété suivante : $K_0 = F^i(K_i), \forall 0 < i \le n$.

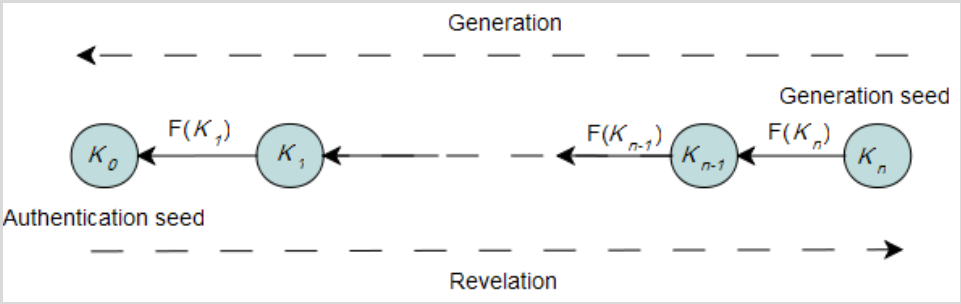


Figure 33 Chaîne de hachage à sens unique

Une authentification basée sur une chaîne de hachage nécessite que l'entité authentifiante possède au préalable une graine d'authentification de la chaîne. Dans le cas des sous-branches, chaque capteur du réseau doit connaître une telle graine pour chaque racine de sous-branche. Néanmoins, ces racines ne sont connues qu'après le déploiement du réseau, et leur nombre peut changer au cours du temps avec l'ajout ou départ des nœuds. Par conséquent, on ne peut pas établir une association de sécurité statique entre les racines et le reste du réseau. Pour contourner ce problème, nous avons utilisé la SB comme repère commun entre les racines et le reste du réseau. Avant le déploiement, un certain nombre de chaînes sont générées et sauvegardées au niveau de la SB. Chaque capteur est préchargé avec la première valeur non utilisée de chaque chaîne. Au début de chaque tour, la SB distribue pour chaque racine i sa « marque de branche » en divulguant la prochaine valeur d'une chaîne donnée. Cette marque sera utilisée par la racine afin de construire sa branche et prouver au reste du réseau son voisinage directe avec la SB, puisque seule la SB peut connaître la prochaine valeur d'une chaîne. Lorsqu'un capteur reçoit une telle marque, il pourra vérifier son appartenance à une des sous-chaînes de la SB, puisqu'il possède une valeur antécédente de la chaîne en question.

Dans la Figure 34(a) on illustre la phase de distribution des marques de sous-branche dans une branche (celle délimitée par un rectangle en pointillé). Le même processus est exécuté dans les autres branches. La Figure 34(b) illustre la phase de construction de routes multi-chemins appartenant à des sous-branches disjointes. Les nœuds vérifient l'authenticité des requêtes à leur réception grâce au mécanisme de chaîne de hachage et les graines pré-chargées dans les nœuds.

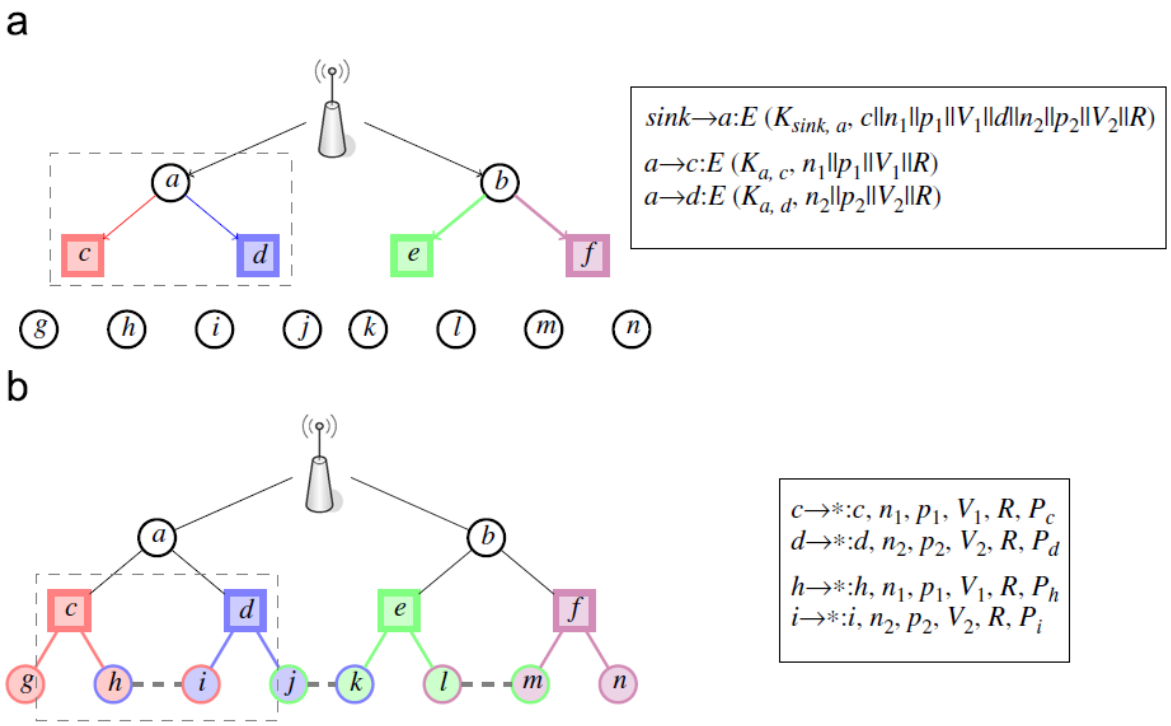


Figure 34 Exemple de construction de sous-branches sécurisées avec SEIF

Nous avons évalué et comparé les performances de notre protocole en le simulant dans un environnement TinyOS [64] et en analysant la fiabilité des topologies construites avec la librairie NetworX (Python). Nous avons considéré deux types de topologies : topologies uniformes et topologies de type « Albert Barabasi » [146] généralement utilisées pour la modélisation de réseaux Internet. Nous nous sommes intéressés en particulier à la consommation de l'énergie (cf. Figure 35), la résilience du réseau (cf. Figure 36, Figure 37), et le MTTF (Mean Time To Failure) où nous avions considéré le temps avant l'occurrence de la première panne d'un nœud (cf. Figure 38).

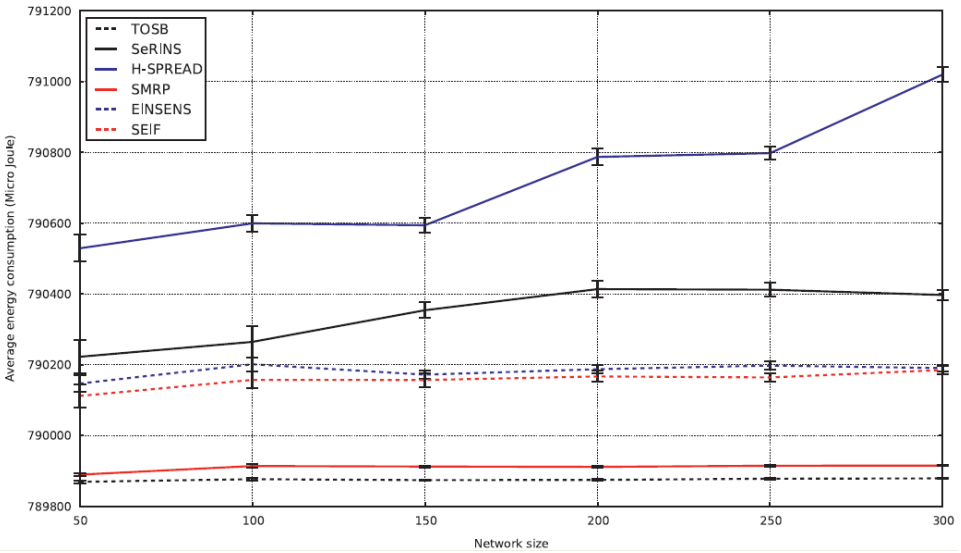


Figure 35 Consommation moyenne de l'énergie

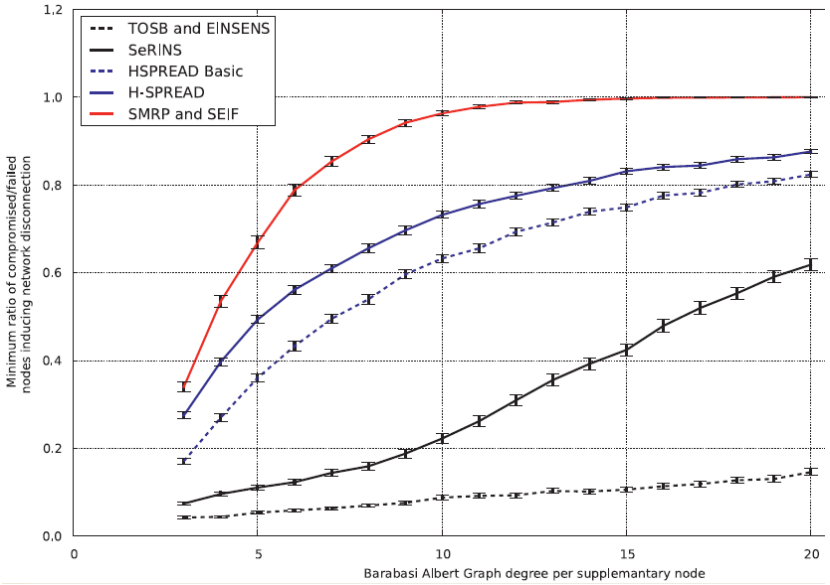


Figure 36 Résilience vs. degré du graphe. Taille du réseau égale à 100. Intervalle de confiance à 0.96

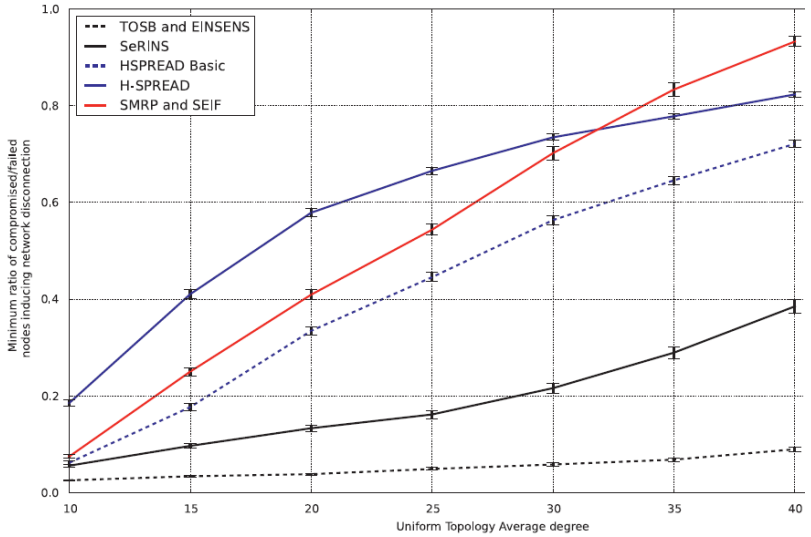


Figure 37 Résilience vs. degré du graphe. Taille du réseau égale à 100. Intervalle de confiance à 0.96

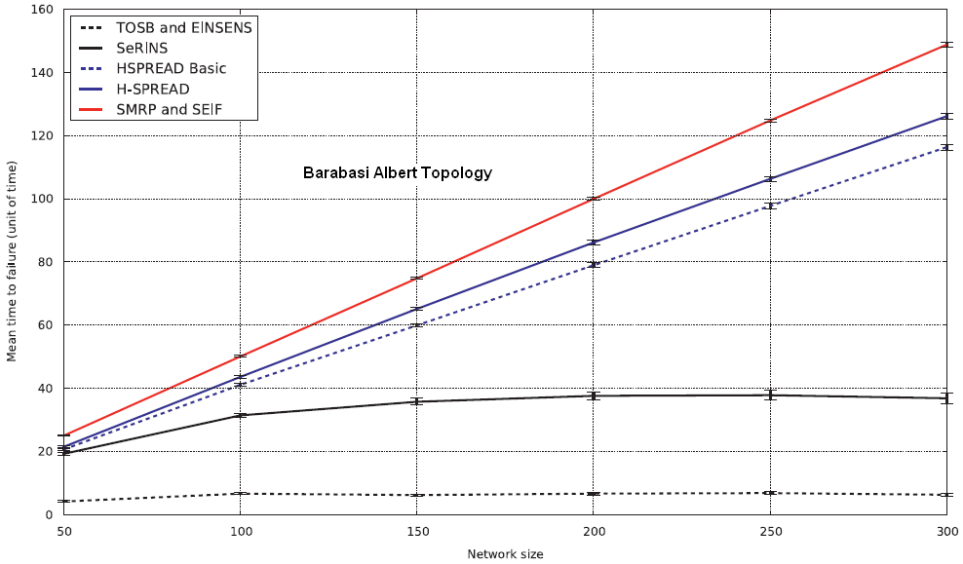


Figure 38 MTTF : degré moyen égal à 20, moyenne de 1000 itérations, intervalle de confiance à 0,96

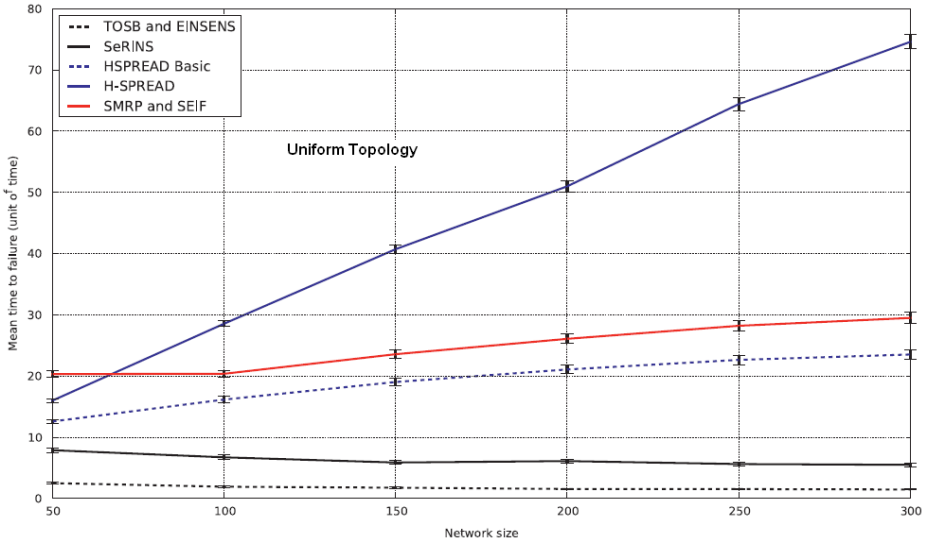


Figure 39 MTTF : degré moyen égal à 20, moyenne de 1000 itérations, intervalle de confiance à 0,96

3.3.3 Routage multi-chemins robuste pour RCSF hétérogènes

Nous avons par la suite étendu notre approche de construction de routes multi-chemins à des RCSF hétérogènes où certains nœuds du réseau (pas forcément des voisins de la SB) disposeraient de ressources plus abondantes notamment en termes d'énergie. L'idée de base de cette solution (appelée *« Heterogeneous Disjoint Multipath Routing Protocol* (HDMRP)» [19]) est de tenir compte de cette hétérogénéité du réseau, dans la construction de routes multi-chemins en favorisant le passage par les nœuds puissants dit « master nodes » (cf. Figure 40).

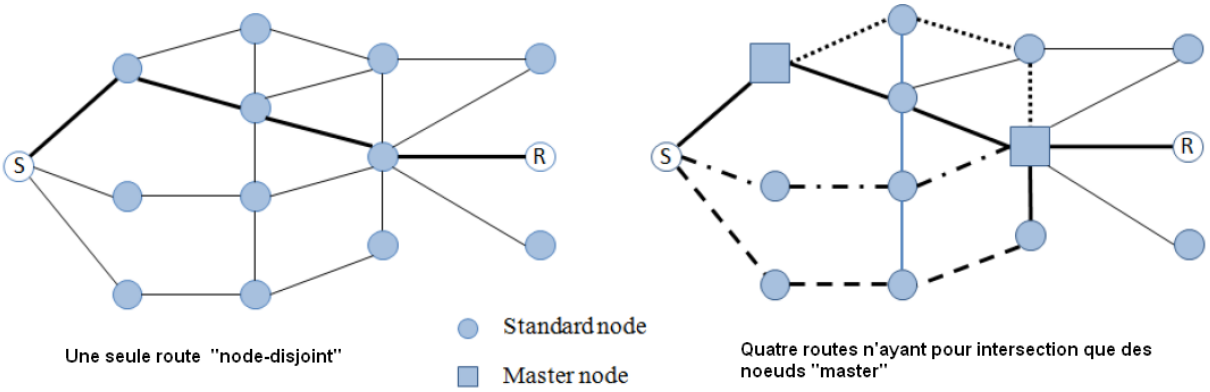


Figure 40 Construction de routes multi-chemins avec HDMRP

Nous avons réalisé des simulations de HDMRP, SMRP (décrit ci-dessus) et BRP (Branch Routing Protocol [147]). Les résultats de ces simulations ont démontré que cette approche permet effectivement d'augmenter le nombre de routes disjointes avec les seuls points d'intersection au niveau des nœuds « masters » (cf. Figure 41), et par conséquent résister davantage aux pannes dans le réseau (cf. Figure 42).

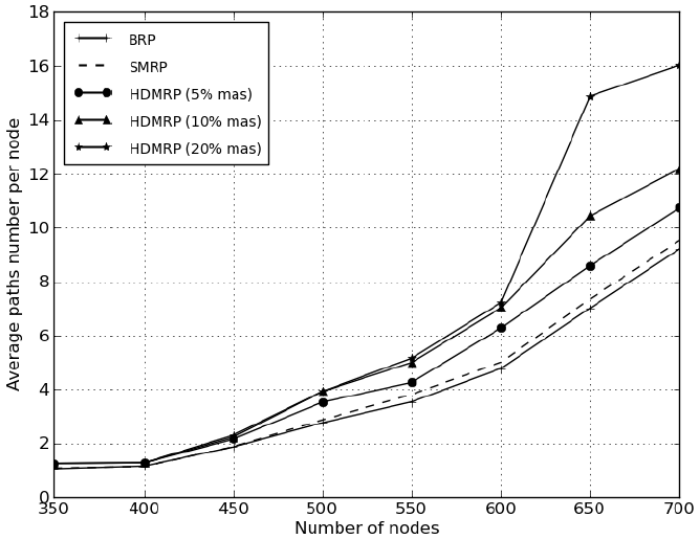


Figure 41 Nombre de nœuds multi-chemins avec HDMRP vs. SMRP et BRP

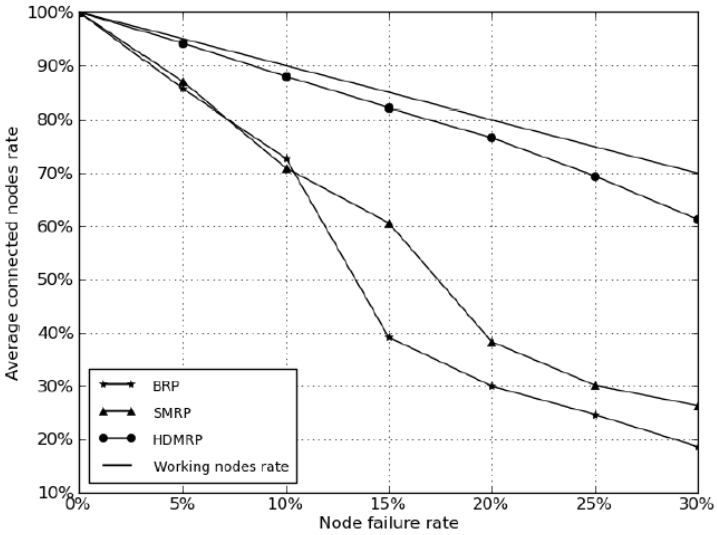


Figure 42 Impact des pannes sur la connectivité du réseau

3.4 Agrégation dans les RCSF et contrôle d'intégrité

L'énergie constitue une des plus fortes contraintes des réseaux de capteurs vu qu'elle s'épuise rapidement et en conséquence met en péril le bon fonctionnement du RCSF. Certaines études montrent que 70% de l'énergie consommée dans un RCSF est due aux communications sans fil. Etant donnée la proximité géographique des nœuds d'un RCSF, l'information captée est vraisemblablement redondante. De ce fait, une des techniques prometteuses d'économie de l'énergie est l'agrégation. L'agrégation consiste à appliquer une fonction (min, max, moyenne, etc.) à un ensemble de valeurs reçues pour n'en retransmettre qu'une information utile dans un seul paquet de données. En plus de l'économie de l'énergie, l'agrégation permet d'optimiser l'utilisation de la bande passante en réduisant le nombre de messages transmis et les collisions éventuelles. Cependant, si l'agrégation réduit la redondance, elle rend la vérification de l'intégrité des données plus complexe. En effet, l'introduction de l'agrégation stipule l'intervention de nœuds intermédiaires pour apporter des transformations aux données brutes, ce qui rend la tâche de leur vérification doublement complexe.

3.4.1 Sécurité de l'agrégation de données dans les RCSF: classification

Nous classifions les solutions de sécurité de l'agrégation dans les RCSF en deux grandes catégories [9] (cf. Figure 43): les approches distribuées où l'agrégation se fait dans un arbre de routage recouvrant les nœuds capteurs, et les approches centralisées où l'agrégation se fait dans des *clusters.* Nous raffinons davantage cette classification en sous-catégories selon les pairs qui établissent des associations de sécurité pour protéger l'agrégation : l'approche à base d'associations de sécurités saut-par-saut, l'approche basée sur des associations de sécurité de bout en bout, et l'approche basée sur des associations de sécurité hybrides.
Dans la première approche, la vérification de l'intégrité des données se fait par les nœuds capteurs eux-mêmes avec l'aide de la station de base (SDAP [148], SAWN [149], SecureDAV [151], RSDA [150]). Dans la seconde approche, c'est la station de base seule qui effectue tout le processus de vérification de l'intégrité des données (CMT [152], ASAP [153]). Dans la troisième approche, la station de base effectue le processus de vérification, et dans le cas d'agrégation erronée, tous les capteurs participent au processus de vérification et de localisation du nœud responsable de l'erreur (SumAgg [154]).

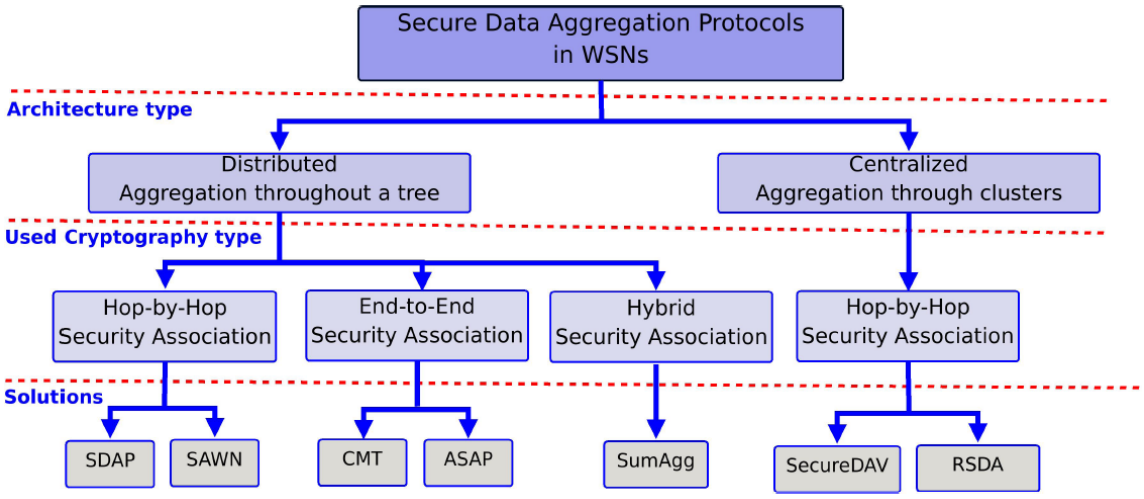


Figure 43 Classification de protocoles sécurisés d'agrégation de données dans les RCSF

Les principaux inconvénients des solutions existantes sont la centralisation du processus de vérification et/ou le « rejet aveugle » des données « polluées » par les nœuds malveillants.
Le problème de centralisation est dû à l'implication totale ou partielle de la station de base dans le processus de vérification. De ce fait, l'application RCSF n'est pas totalement distribuée et la vérification des données captées par le RCSF ne peut se faire qu'après réception par la station de base de l'intégralité des données agrégées. Le second problème est dû à la détection d'une valeur agrégée incorrecte (polluée). Etant donné la nature agrégée des données reçues par la station de base, ceci engendre le rejet « aveugle » de toutes les mesures transportées par le RCSF qui ont conduit à ces données agrégées. Les solutions existantes souffrent de leur incapacité à distinguer les données erronées des données correctes qui ont contribué au calcul d'une donnée agrégée qu'elle s'avère incorrecte.

3.4.2 Contrôle d'intégrité distribué et agrégation dans les RCSF

Nous avons proposé un nouveau protocole efficace de contrôle d'intégrité avec agrégation de données dans les RCSF. Dans notre solution, appelée SEDAN « Secure and Efficient Data Aggregation protocol for WSN » [20][21], chaque nœud peut vérifier immédiatement

l'intégrité des données de ses voisins à deux sauts, et l'agrégation effectuée par ses voisins immédiats. Ceci permet d'éviter le transport inutile de données « polluées » et donc la préservation des ressources en énergie des nœuds.

Comme on peut le voir sur la Figure 44, cette vérification se base sur un calcul de MAC sur l'agrégation effectuée par les nœuds voisins immédiats et les données brutes envoyées par les voisins à deux sauts.

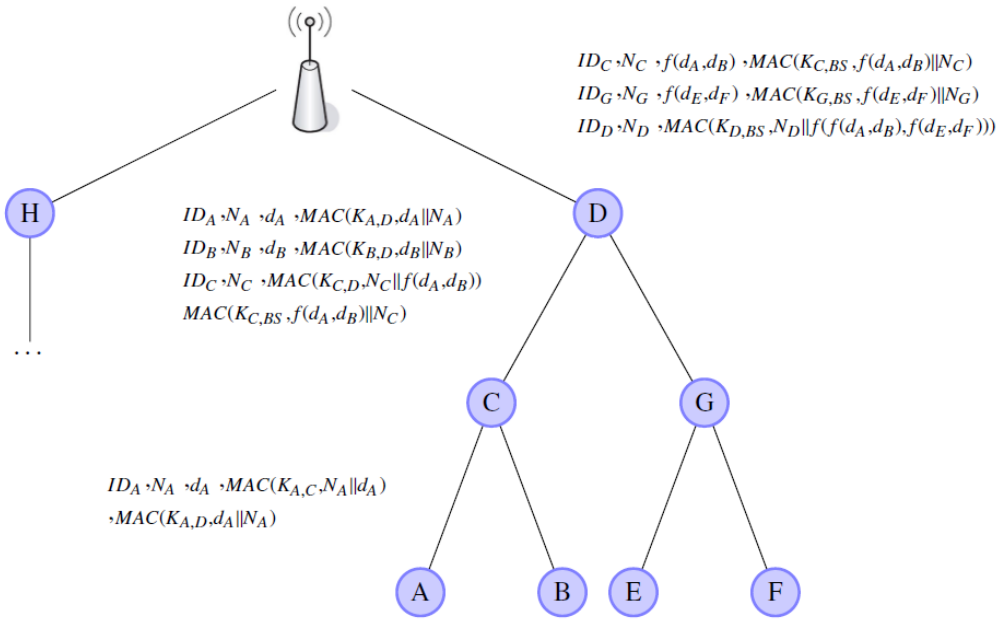


Figure 44 Processus d'agrégation dans SEDAN

Ceci est rendu possible grâce à la définition et à la gestion d'un nouveau type de clés que nous avons appelé clés à deux sauts « two hops pair-wise keys » [20]. Ce nouveau type de clés permet le partage d'un secret entre deux voisins à deux sauts, qui reste inconnu aux voisins à un saut qui participeraient à l'établissement de ces clés. De cette manière, tout nœud du réseau peut vérifier l'intégrité des données transmises par ses voisins à deux sauts et s'assurer que ces données n'ont pas été altérées par les nœuds intermédiaires à un saut.

Nous avons proposé alors un nouveau protocole (EPKE) pour l'établissement et la gestion de ce nouveau type de clés [20]. Notre protocole, comme d'autres dans la littérature (LEAP [132]), se base sur l'hypothèse d'existence d'une période de « trêve » au début du déploiement du réseau, pendant laquelle nous supposons qu'un intrus n'aurait pas le temps de compromettre un nœud et lire ses clés cryptographiques. Durant cet intervalle de temps, les nœuds du réseau établissent leurs clés à un saut, puis à deux sauts, qui sont des clés dérivées d'un secret pré-chargé commun à tous les nœuds. Ce secret commun est effacé de la mémoire des nœuds dès l'épuisement de la période de « trêve ». Pour démontrer le réalisme de cette hypothèse, nous nous sommes intéressés à évaluer la durée nécessaire pour établir toutes les clés dans le réseau. Pour cela, nous avons implémenté notre protocole avec TinyOS [64] et nous l'avons exécuté sur une topologie réelle composée d'un ensemble de nœuds de type MicaZ [138]. Comme l'illustre la Figure 45, une durée de l'ordre de 3 secondes suffit pour établir toutes les clés du réseau, et elle nous semble très insuffisante pour compromettre un nœud et lire le secret pré-chargé.

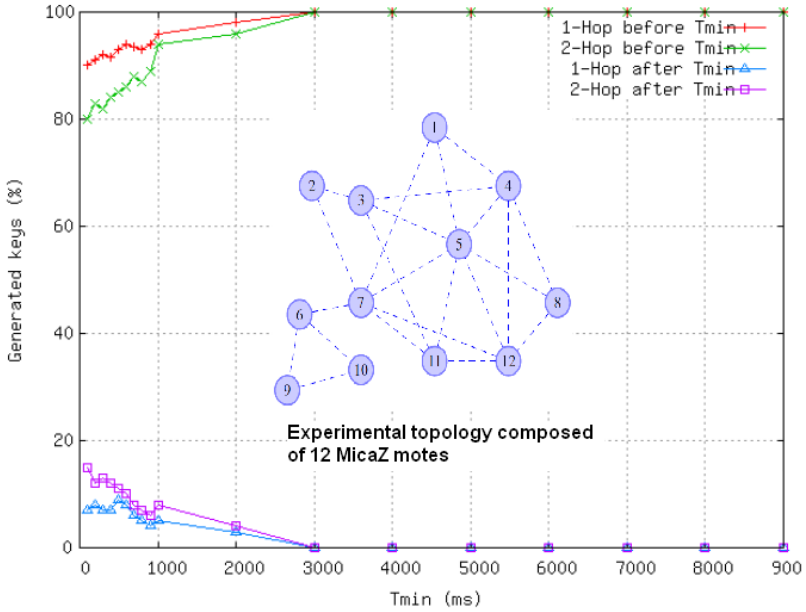


Figure 45 La proportion de clés générées vs. Tmin

Pour évaluer le degré du « rejet aveugle » de données agrégées, nous avons considéré un arbre binaire et nous avons calculé la proportion de données rejetées selon la position sur l'arbre du nœud compromis ayant « pollué » ces données. Comme l'illustre la Figure 46, notre solution SEDAN permet une détection instantanée des données altérées ce qui permet de réduire l'ampleur de ce phénomène de « rejet aveugle » quand le nœud malveillant n'est pas proche de la racine.

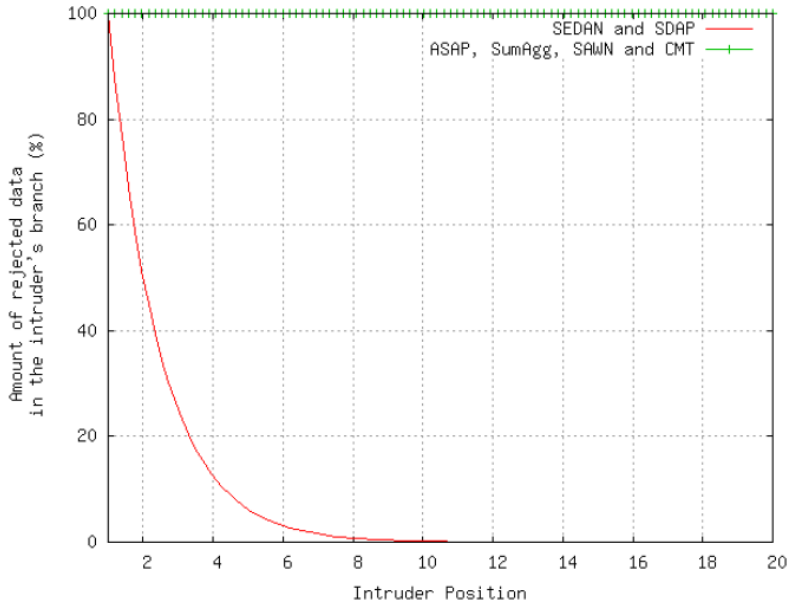


Figure 46 Proportion des données rejetées vs. position du nœud malveillant

Nous avons implémenté notre protocole SEDAN ainsi que d'autres protocoles de la littérature, sous TinyOS [64] pour les comparer et évaluer leurs performances. Nous nous sommes intéressés au temps moyen avant la détection de données agrégées « polluées » (MTTD : Mean Time To Detection). Comme l'illustre la Figure 47, cette durée est quasi nulle dans le cas de notre protocole SEDAN contrairement aux autres protocoles.

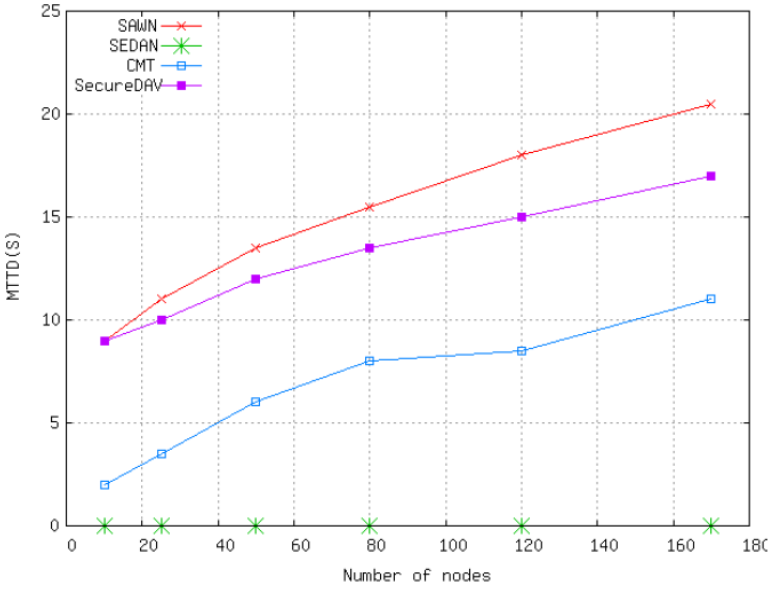


Figure 47 MTTD vs. taille du réseau

Par ailleurs, nous avons évalué la consommation de l'énergie avec le plugin PowerTOSSIM [155]. Comme on peut le voir sur la Figure 48, le surcoût en termes d'énergie est négligeable dans le cas de notre solution.

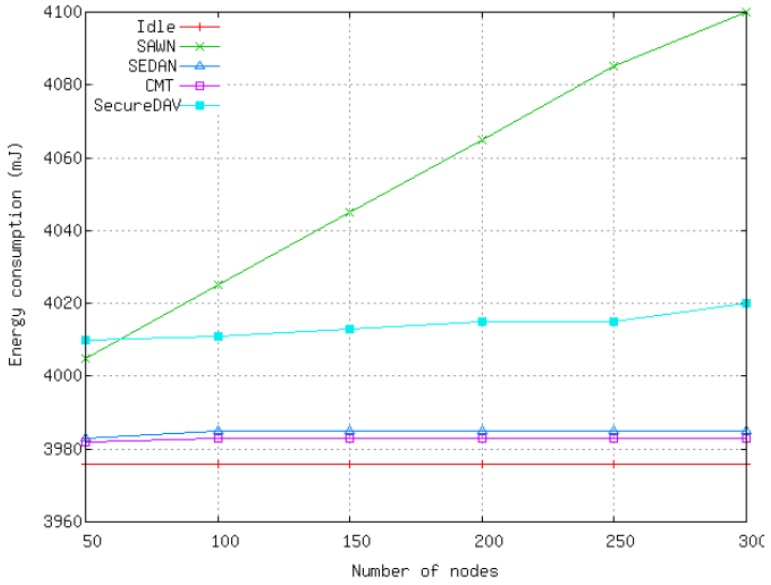


Figure 48 Consommation d'énergie vs. taille du réseau

3.5 Conclusion

Dans ce chapitre, nous avons présenté nos travaux autour de la sécurité dans les réseaux de capteurs sans fil. Nous avons montré que les contraintes sévères de ressources imposent certains choix pour assurer la sécurité des échanges dans un réseau de capteurs. Or, le niveau et les services de sécurité requis restent similaires aux services requis dans tout système en interaction. Partant de ce constat, nous avons montré qu'il était possible d'assurer des niveaux de sécurité élevés en améliorant la résilience des systèmes. Ainsi, nous avons montré qu'à travers une utilisation judicieuse des fonctions de hachage on pouvait améliorer la résilience de la gestion de clés : un sous-système vital pour toute architecture de communication sécurisée. Une pré-distribution ingénieuse des clés (en se basant sur la théorie de la conception combinatoire notamment), permet d'éviter des transmissions inutiles de messages pour l'établissement de clés. De même, en utilisant les chaînes de hachage, on pouvait sécuriser un mécanisme de construction de routes multi-chemins robuste. Enfin, en reposant sur des hypothèses raisonnables de délais pour mener une attaque, on pouvait utiliser un mécanisme de pré-distribution de clés pour sécuriser l'agrégation de données dans un réseau de capteurs.

Chapitre 4 : Recherche technologique et partenariale

Depuis mon arrivée à l'UTC en 2001, j'ai eu l'occasion de participer à plusieurs projets de recherche partenariale comme l'illustre la Figure 1. Ces projets pluridisciplinaires s'inscrivent dans des domaines aussi variés que la santé, l'agriculture, la gestion du trafic urbain, les systèmes embarqués, les réseaux et la sécurité des systèmes. Dans ce qui suit, nous présentons quelques projets et leurs résultats pour illustrer la complexité et la difficulté des chantiers entrepris dans le cadre de ces travaux de recherche durant ces dernières années.

4.1 AGROSENS : RCSF pour le contrôle de l'environnement et l'agriculture

AGROSENS (2009-2012) est un projet financé par le Fond Européen pour le Développement Régional (FEDER) et la région de Picardie. C'est un projet pluridisciplinaire dans le cadre d'une recherche partenariale entre Heudiasyc, l'Institut National de Recherche en Agronomie (INRA-Laon) et Agro-Transfert Ressources et Territoires. Dans ce projet, je suis responsable scientifique du côté de notre laboratoire (HEUDIASYC). Je co-encadre également la thèse de M. Walid Bechkit, financée dans le cadre de ce projet.
L'objectif du projet est le développement d'une plateforme de réseaux de capteurs sans fil, robuste et sécurisée, pour la supervision du milieu physique des cultures. L'utilisation des RCSF devrait permettre d'améliorer la capacité à réagir en temps réel aux évolutions du milieu et du couvert afin de garantir une meilleure production en termes de qualité et de quantité, tout en économisant les ressources en eau, en énergie et en limitant les intrants phytosanitaires.

L'étape de consolidation technologique avec nos partenaires a permis d'identifier l'ensemble des composants requis pour le champ d'application ciblé. Dans ce cadre, nous avons développé une plateforme [26] de RCSF. Les nœuds du réseau sont de types différents (TelosB, MicaZ) [138] compatibles avec la norme IEEE 802.15.4. Les nœuds MicaZ sont interfacés à des sondes EC5 [166] (pour la mesure de la teneur en eau du sol) à travers une carte d'acquisition MDA300 [138]. Par ailleurs ces deux types de nœuds (TelosB, MicaZ+MDA300) permettent de mesurer des paramètres de l'atmosphère : température, humidité et luminosité. Sur ces nœuds, nous avons implémenté un protocole d'interrogation et de dissémination des données captées. La Figure 49 illustre l'architecture logicielle de la plateforme.

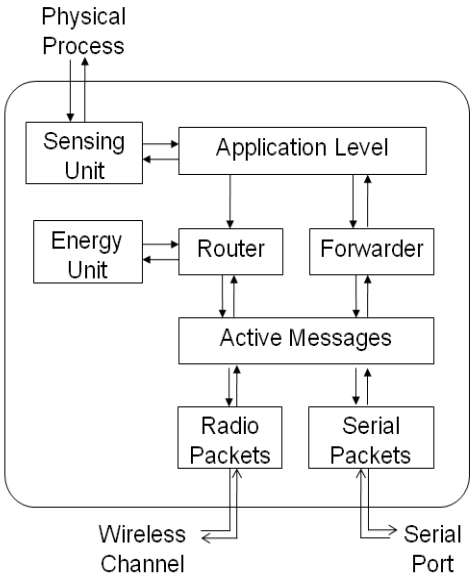


Figure 49 Architecture logicielle

Nous avons par ailleurs, développé une application [26] (cf. Figure 50) qui permet à l'utilisateur d'interroger le réseau, de visualiser les données captées en temps réel et via Internet, et de configurer la période d'échantillonnage, la mise en veille des nœuds pour l'économie de l'énergie, etc.
Nous avons testé ce prototype à l'échelle du laboratoire. Une fois déployés, les nœuds s'auto-organisent grâce au protocole de routage adaptatif que nous avons développé, et acheminent les données mesurées jusqu'à la station de base. Ces tests nous ont permis de vérifier avec succès des fonctionnalités importantes de la plateforme à savoir :

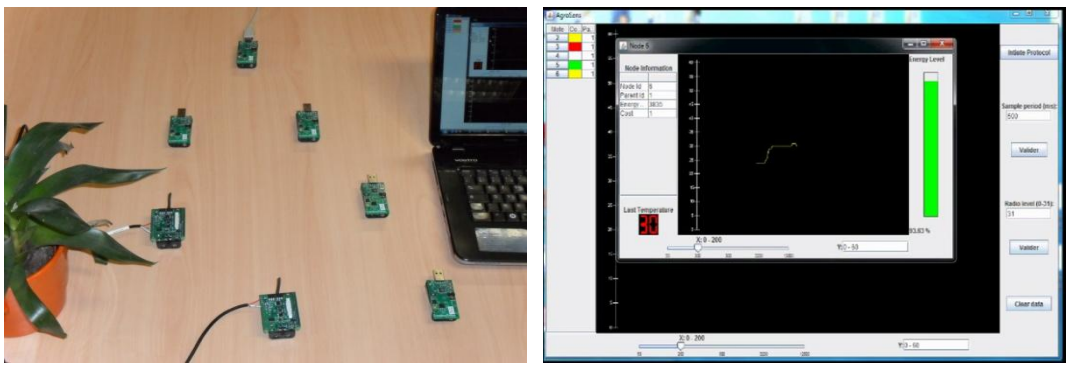


Figure 50 Plateforme AGROSENS

- la construction d'un arbre des chemins minimaux basée sur l'énergie résiduelle;
- la mise à jour automatique de l'arbre construit en cas de pannes des nœuds ;
- la reconstruction automatique de l'arbre en cas de mobilité des nœuds;
- l'allongement de la durée de vie du réseau grâce à la mise en veille des nœuds

4.2 SUPGEST : Supervision et optimisation du Geste à l'aide d'un RCSF

SUPGEST (2009-2012) est un projet soutenu par la fédération de recherche SHIC 3272 (Systèmes Hétérogènes en InteraCtion). C'est un projet pluridisciplinaire entre les trois laboratoires Heudiasyc, BMBI (Biomécanique et Bio-Ingénierie) et Roberval (Mécanique, Acoustique et vibrations, Matériaux). Je participe à ce projet et je coencadre la thèse de M. Abdelkrim Hadjidj qui travaille entre autres sur le développement de protocoles de communication fiables et sur une plateforme de RCSF dans le cadre du projet.
SUPGEST a pour objectif l'étude et la conception d'un système de capteurs sans fil embarqués sur une partie du système musculosqueletique. Ce système a pour rôle la supervision du ou des membres choisis afin d'optimiser les gestes à effectuer soit par le patient, le chirurgien, le kinésithérapeute à partir d'une évaluation objective de la rééducation fonctionnelle.

Nous avons développé une plateforme [22] de RCSF et une application qui permet de visualiser les signaux (accélération linéaire et angulaire) captés (cf. Figure 51). Ces signaux alimentent un modèle biomécanique pour l'aide à la décision en rééducation fonctionnelle.

Figure 51 Plateforme RCSF pour la rééducation fonctionnelle

Par ailleurs, nous avons développé un protocole de communication [23] pour transmettre ces signaux mesurés des capteurs vers la station de base, en exploitant toute les capacités du standard IEEE 802.15.4. La particularité de notre solution est la prise en compte de la nature des signaux mesurés par les capteurs. Ces signaux sont caractérisés par une fréquence d'échantillonnage relativement élevée et un besoin de synchronisation pour une reproduction fidèle du mouvement au niveau du modèle biomécanique. Comme le montrent les Figure 52 et Figure 53, notre protocole permet de minimiser les erreurs de transmission qui peuvent être très fréquente si une simple méthode d'accès au canal avec contention était utilisée. Ces erreurs se propageraient alors au modèle biomécanique, ce qui influencerait négativement la reproduction du mouvement et donc la prise de décision.

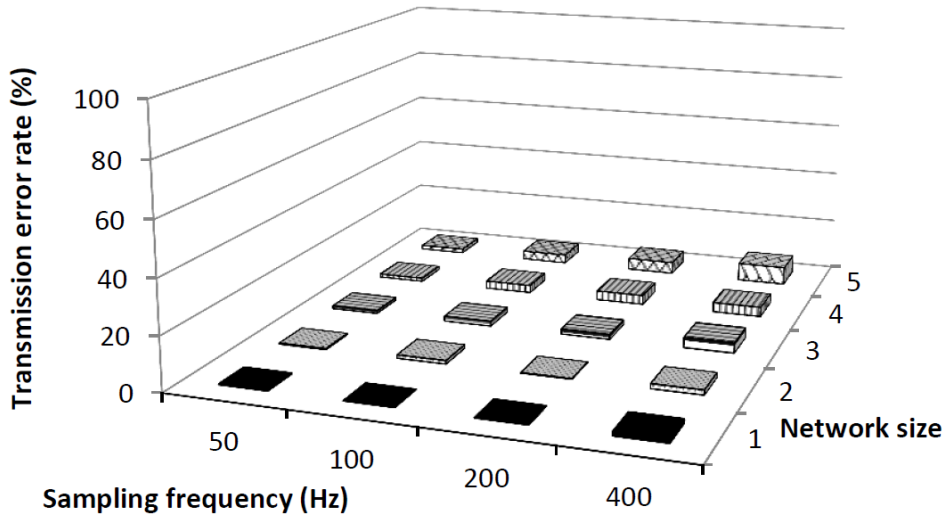


Figure 52 Taux d'erreurs de transmission : notre protocole

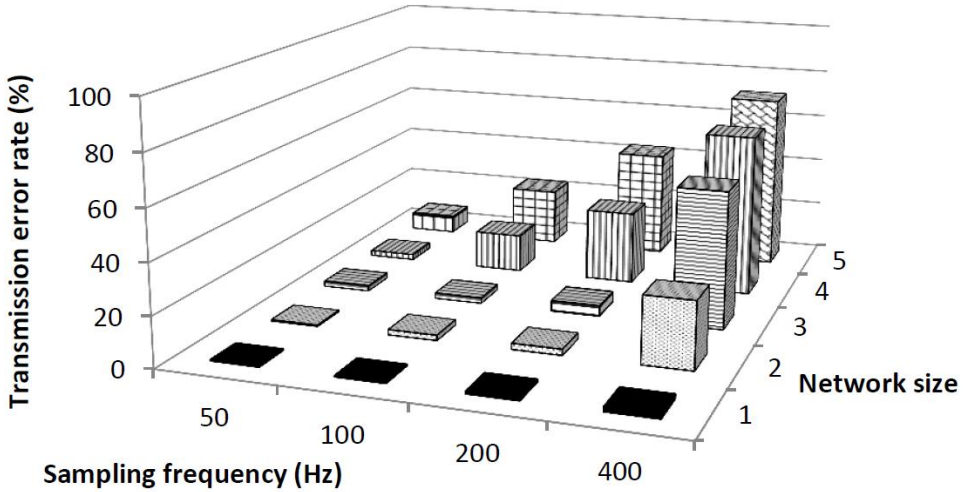


Figure 53 Taux d'erreurs de transmission : protocole basique de TinyOS

4.3 SIRENE : SupervIsion aéRiEnne coordoNnée et sEcurisée

Le projet SIRENE était soutenu au début par le laboratoire HEUDIASYC (2008-2010). Puis il a été soutenu par ANR-CARNOT entre 2010 et 2012. J'ai participé au projet dès son lancement en 2008, et je suis actuellement coordinateur du projet avec Pedro Castillo (équipe ASER du laboratoire Heudiasyc). Dans le cadre de ce projet j'ai coencadré les stages de master de M. Bassam Tayba et Melle. Asma Guesmi et un post-doc, M. José Alfredo Guerrero.

Ce projet a pour objectif de développer une architecture de supervision aérienne d'espaces géographiques larges [25]. Cette architecture est basée sur un ensemble de drones (type avions et hélicoptères sans pilotes) organisé en formation synchronisée horizontale qui parcourt une zone déterminée pour relever des informations comme la détection d'incendies, la recherche d'individus, etc. Ces informations sont transmises à une plate-forme de supervision et de prévention afin de déclencher les actions nécessaires (appel des pompiers, agents de sécurité, etc.). La tâche de supervision de tels espaces n'est pas réalisable à l'aide d'un seul drone et cela à cause de l'importance de l'espace à surveiller.

La Figure 54 illustre les composants de base de notre architecture de communication. L'architecture est composée d'un ensemble de drones pouvant communiquer entre eux et avec une station de base. Chaque drone est équipé : d'un GPS, d'interface de communication (Digi connect Wi-ME), d'unité de traitement (Rabit RCM3400), d'une centrale inertielle ainsi que d'une caméra vidéo (cf. Figure 55).

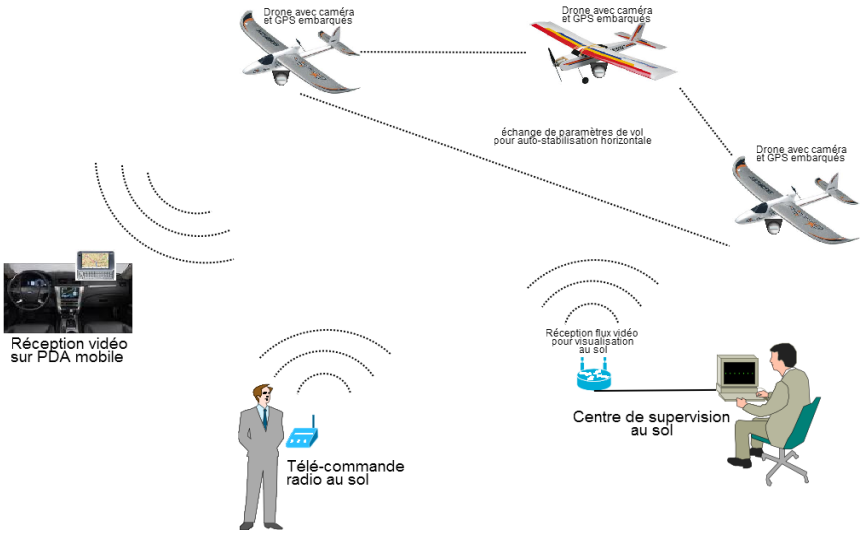


Figure 54 Architecture de communication Inter-drones

Les drones communiquent entre eux en envoyant des informations sur leur cinétique (position GPS, vitesse, accélération, direction, …) ainsi que des informations relatives à leur mission (vidéo, grandeurs physiques mesurées, etc.).

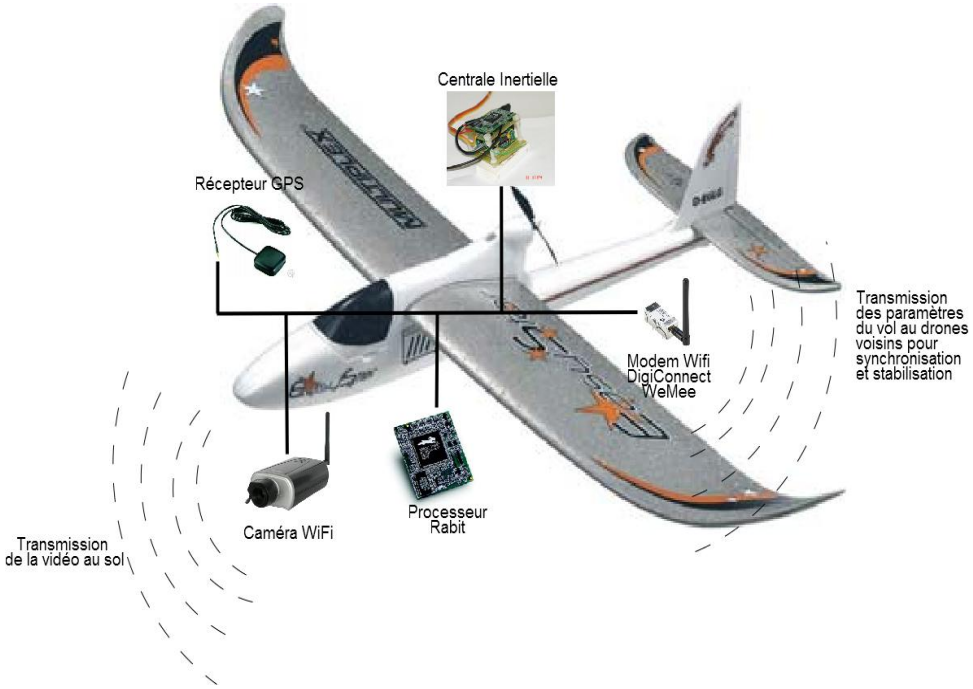


Figure 55 Composants d'un drone

Etant donné la nature sensible des communications inter-drones et de leurs missions, il est nécessaire de sécuriser ces communications. Par ailleurs, la robustesse devient un élément essentiel de l'architecture de communication pour assurer une continuité du vol en formation

malgré le disfonctionnement éventuel d'un ou de plusieurs drones. Les pannes dans un tel système peuvent intervenir à deux niveaux : au niveau des équipements ou des transmissions. Dans un premier temps, nous nous sommes intéressés au deuxième type de défaillances. En effet, les transmissions sans fil sont sujettes à des pertes de paquets fréquentes (collisions, obstacles, mobilité et changement de topologie, etc.). Afin d'élaborer une architecture de communication robuste à tout niveau, il est donc nécessaire d'analyser l'impact du choix des protocoles de communication au niveau de toutes les couches protocolaires. Dans ce contexte, nous avons réalisé une étude de l'impact des protocoles d'accès au canal radio sur la qualité de la loi de commende des drones [24]. Nous avons considéré une loi de commande simple qui est la convergence vers une valeur moyenne. Comme l'illustre la Figure 56, le protocole TDMA permet une convergence plus rapide avec moins d'oscillations. En effet, TDMA souffre moins des collisions et est plus approprié aux communications temps réel.

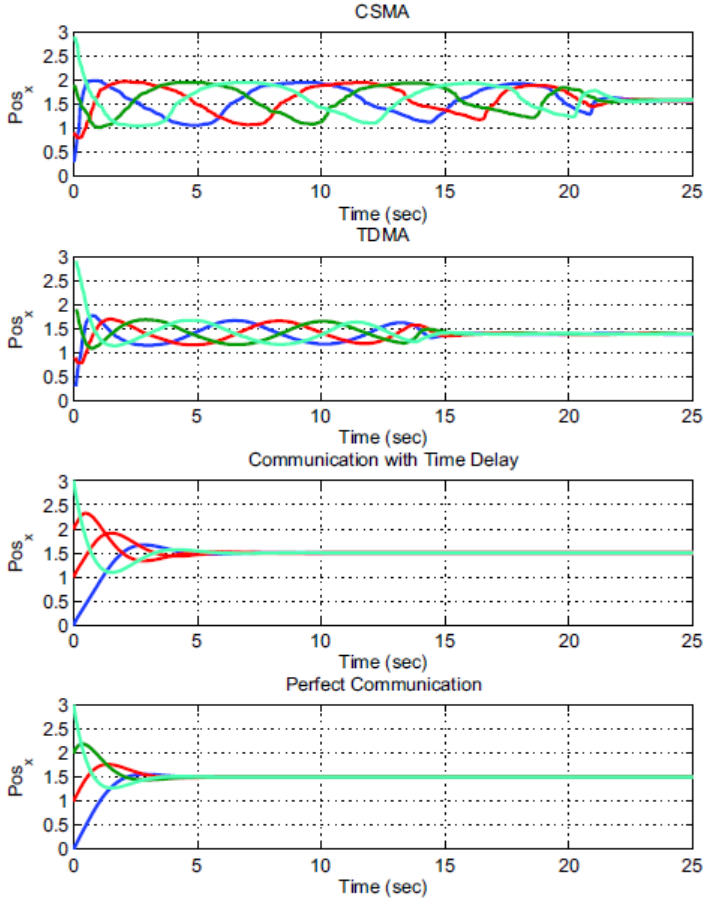


Figure 56 Comparaison de la convergence de plusieurs algorithmes MAC

Dans le cadre de ce projet, nous allons continuer à caractériser l'impact des protocoles de communication à différentes échelles sur la loi de commande inter-drones. Cette analyse nous permettra par la suite de proposer une architecture de communication inter-drones robuste et sécurisée, avec éventuellement de nouveaux protocoles de communication plus appropriés.

4.4 Conclusion

Dans ce chapitre, nous avons présenté quelques projets de recherche partenariale en cours. Ces projets pluridisciplinaires portent sur des domaines aussi variés que la santé, l'agriculture et la commande de drones en vol en formation horizontale. A l'aide de nos partenaires respectifs (INRA, BMBI, équipe ASER) nous avons pu explorer de nouveaux domaines et proposer des solutions technologiques à des problèmes difficiles. Notre plateforme de réseaux de capteurs pour l'agriculture est aujourd'hui opérationnelle et prête à être utilisée chez notre partenaire (INRA) pour l'expérimentation en recherche agronomique en général et l'étude de la variabilité hydrique du sol à court terme. Par ailleurs, la plateforme de réseaux de capteurs pour la rééducation fonctionnelle est opérationnelle et peut être utilisée pour alimenter un modèle biomécanique pour la reproduction du mouvement et l'aide à la décision en rééducation fonctionnelle. Notre projet autour de la communication d'une flotte de drones est en progression. Les premiers résultats de simulations nous aideront à faire les bons choix quant aux protocoles de communication à utiliser ou à concevoir.

Grâce à ces projets pluridisciplinaires, nous avons fait émerger au sein de notre laboratoire une nouvelle activité originale autour des réseaux de capteurs et de leurs applications. Par ailleurs, nous avons mené autour de ces projets une recherche à la fois scientifique et intégrative portant sur l'optimisation, la sécurité et la résilience de ces réseaux à fortes contraintes de ressources. En outre, ces projets ont drainé des ressources qui ont permis d'animer une équipe composée de plusieurs doctorants, stagiaires, et post-doc sur des thèmes connexes et variés : gestion de clés dans les réseaux de capteurs, routage multi-chemins et résilience, économie de l'énergie, communication inter-drones et impact sur la loi de commande, interface de communication entre un réseau de capteurs et un collecteur mobile, etc.

Chapitre 5 : Sécurité de l'Internet des objets : vers une approche cognitive et systémique

L'évolution de nos axes de recherche est principalement motivée par la prise en compte de nouvelles évolutions technologiques et de leur usage pour lesquels nous proposerons des solutions algorithmiques de sécurité, supportant la mobilité, tout en optimisant les ressources.

Une évolution majeure qui s'inscrit dans la continuité des développements récents des technologies de l'information et de la communication et des systèmes embarqués, est *« l'internet des objets (IdO)»*. Cette évolution sera accompagnée d'une évolution de l'écosystème technologique environnant dans toute sa complexité. En effet, comme illustré par la Figure 57, le réseau mondial Internet a évolué ces dernières décennies d'un réseau de calculateurs à un réseau d'ordinateurs personnels, puis vers un réseau qui intègre tout dispositif communiquant : les tags RFID, les réseaux de capteurs et actionneurs, les réseaux véhiculaires, etc.

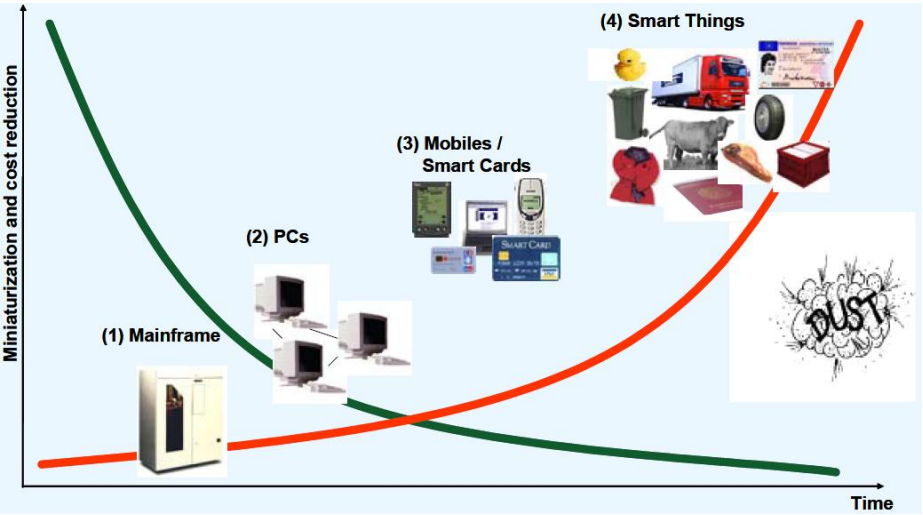


Figure 57 Evolution de notre environnement technologique. Fleisch et al. [30]

L'internet des objets suscitera des questions, qui concerneront directement la sécurité des biens et des personnes. Par exemple, certaines applications peuvent être étroitement liées à des infrastructures stratégiques telles que la fourniture d'eau et d'électricité, la surveillance de ponts et bâtiments, tandis que d'autres géreront des informations liées à la vie privée des personnes comme leurs déplacements et états de santé. Ainsi, la confiance en l'IdO et son acceptation sont conditionnées par la mise en place de mesures adéquates de protection des données personnelles et de la vie privée : deux droits fondamentaux de l'UE [32].
Le développement des TIC a montré par le passé que la sécurité est parfois négligée durant la phase de conception, et que son intégration par la suite entraîne des difficultés et des coûts et peut réduire considérablement la qualité des systèmes. Il est donc primordial que la

conception initiale des éléments de l'IdO intègre le respect de la vie privée et la sécurité ainsi que l'ensemble des exigences des utilisateurs [32].
En effet, l'Internet des objets doit être conçu pour un usage facile masquant la complexité technologique sous-jacente, et une manipulation en toute quiétude empêchant les menaces et risques potentiels. Dans l'IdO, tout objet est potentiellement connecté à Internet et capable de communiquer avec d'autres objets. Ceci engendre de nouveaux risques liés notamment à la confidentialité, l'authenticité et l'intégrité des données échangées entre les objets. Des solutions cryptographiques existent pour assurer ces services de sécurité. Cependant, ces solutions ne seraient-elles pas inefficaces voire inapplicables à des objets ayant de fortes contraintes de ressources ? Par ailleurs, ces solutions cryptographiques s'appuient sur des protocoles de distribution et de gestion de clés : un sous-système sensible et déjà difficile à concevoir et à configurer pour les systèmes actuels. Des solutions de gestion de clés à base de pré-distribution de clés pourraient accommoder les contraintes de ressources des objets. Néanmoins, des questions se posent sur la scalabilité de telles approches à un IdO comportant potentiellement des milliards d'objets. Un challenge difficile serait de concevoir des protocoles de gestion de clés à la fois scalables, robustes et résilients.
L'omniprésence des objets, leur fragilité intrinsèque, leur mobilité et leur hétérogénéité sont de nouveaux challenges. Quels modèles de confiance conviendraient à cet écosystème complexe et fragile ? Comment gérer l'hétérogénéité technologique des objets couplée à une hétérogénéité des besoins des applications et des usagers en termes de services de sécurité ? Ces questions deviennent encore plus pertinentes quand on sait que ces besoins peuvent évoluer dans le temps selon le contexte. Parmi ces besoins des usagers, on peut citer le respect de la vie privée, ou « privacy », qui doit être protégée pour éviter l'identification et la localisation non autorisée. Comment s'assurer que les objets de la sphère privée, *dotés de capacités à percevoir et à agir,* respectent scrupuleusement ces exigences ? Dans ce contexte, plus les objets acquièrent de l'autonomie*,* plus les problèmes liés à la vie privée s'accentuent.
Par ailleurs, la traçabilité des actions des objets, ainsi devenus autonomes, doit être soigneusement considérée. En effet, la forte intégration de l'IdO au monde physique accroît le contrôle sur ce monde, mais le rend vulnérable aux actions potentiellement risquées des objets qui le contrôlent. Ainsi, émerge la question de gestion des crédentités dans l'IdO. Une gestion qui permet à la fois d'instaurer des politiques de sécurité claires, adaptatives selon le contexte et d'établir les responsabilités des faits et des actions sur l'environnement physique des objets.
La taille de l'IdO est un autre challenge pour la sécurité. En effet, comment garantir l'authentification individuelle de plusieurs milliards d'objets hétérogènes, utilisant des technologies de communication hétérogènes, et à travers des domaines administratifs multiples ? [31]. Par ailleurs, l'IdO défiera les systèmes de bases de données distribuées classiques, en considérant un nombre pharamineux d'objets qui traitent des données dans un espace informationnel global. Ceci soulève des questions sur la sécurité des transactions traversant des millions d'objets, qui mettent à jours continuellement leurs données, à travers des politiques de sécurité diverses et variées [31].

Dans ce chapitre, nous analyserons les enjeux, les vulnérabilités et les menaces potentielles qui entourent l'internet des objets. Puis nous présenterons certaines évolutions prospectives de la sécurité de l'internet des objets dans lesquelles s'inscriront les perspectives de nos travaux.

5.1 L'internet des objets : enjeux, applications et architecture

5.1.1 Définition

Le CERP-IoT « Cluster des projets européens de recherche sur l'Internet des objets » définit l'Internet des objets comme : « une infrastructure dynamique d'un réseau global. Ce réseau global a des capacités d'auto-configuration basée sur des standards et des protocoles de communication interopérables. Dans ce réseau, les objets physiques et virtuels ont des identités, des attributs physiques, des personnalités virtuelles et des interfaces intelligentes, et ils sont intégrés au réseau d'une façon transparente » [29].
Cette vision de l'Internet des objets introduira une nouvelle dimension aux technologies de l'information et de la communication : en plus des deux dimensions temporelle et spatiale qui permettent aux personnes de se connecter de n'importe où à n'importe quel moment, nous aurons une nouvelle dimension « *objet* » qui leur permettra de se connecter à n'importe quel objet (cf. Figure 58).

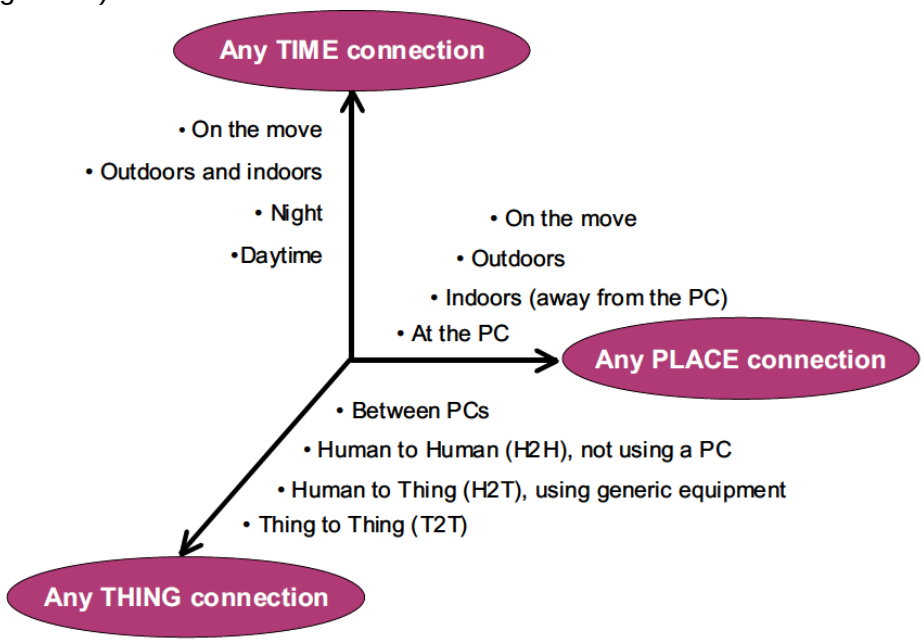


Figure 58 Une nouvelle dimension pour l'IdO (Source ITU 2005 [27])

5.1.2 Applications

L'IdO couvrira un large éventail d'applications (comme illustré par la Figure 59) et touchera quasiment à tous les domaines que nous affrontons au quotidien. Ceci permettra l'émergence d'espaces intelligents autour d'une informatique omniprésente. Parmi ces espaces intelligents, on peut citer :

- Les villes : l'IdO permettra une meilleure gestion des réseaux divers qui alimentent nos villes (eaux, électricité, gaz, etc.) en permettant un contrôle continu en temps réel et précis. Des capteurs peuvent être utilisés pour améliorer la gestion des parkings et du trafic urbain et diminuer les embouteillages et les émissions en CO2.
- L'énergie : la gestion des grilles électriques se verra améliorée grâce à la télémétrie, permettant une gestion en temps réel de l'infrastructure de distribution de l'énergie. Cette interconnexion à large échelle facilitera la maintenance et le contrôle de la consommation et la détection des fraudes.

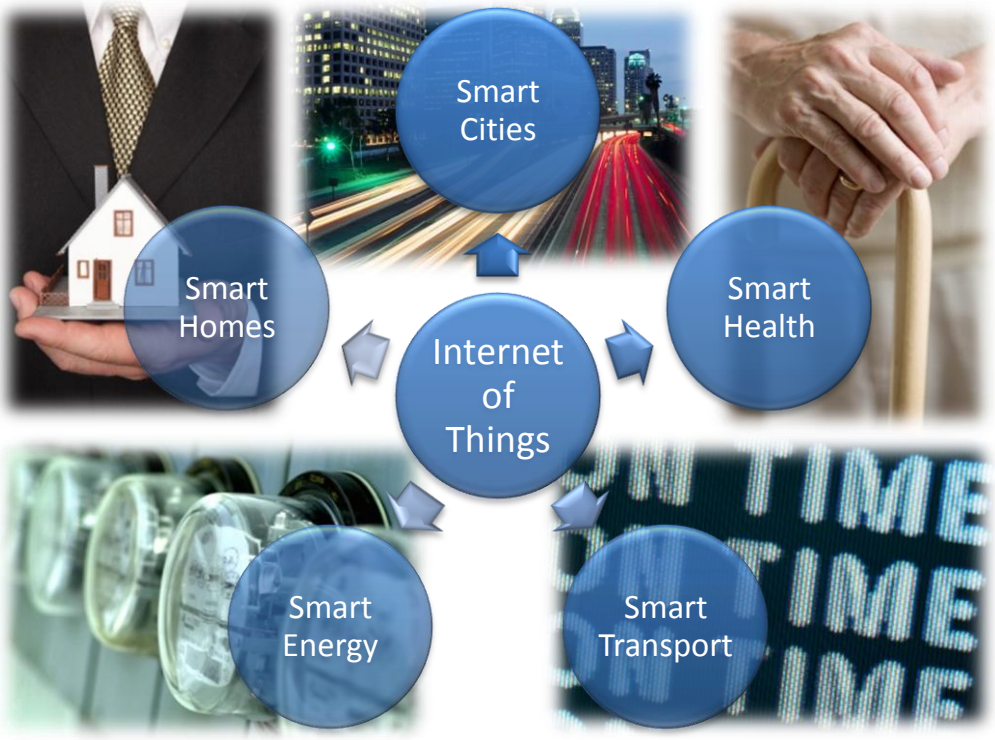


Figure 59 L'Internet des objets et la création d'espaces intelligents

- Le transport : dans ce domaine l'IdO appuiera les efforts actuels autour des véhicules intelligents au service de la sécurité routière et l'aide à la conduite. Cela portera sur la communication inter-véhicule et entre véhicules et infrastructure routière. L'IdO constituera ainsi un prolongement naturel des « systèmes de transport intelligents » et leurs apports en termes de sécurité routière, confort, efficacité de la gestion du trafic et économie du temps et de l'énergie.
- La santé : dans le domaine de la santé, l'IdO permettra le déploiement de réseaux personnels pour le contrôle et le suivi des signes cliniques, notamment pour des personnes âgées. Ceci permettra ainsi de faciliter la télésurveillance des patients à domiciles, et apporter des solutions pour l'autonomie des personnes à mobilité réduite.
- L'industrie : dans l'industrie l'IdO permettra un suivi total des produits, de la chaîne de production, jusqu'à la chaîne logistique et de distribution en supervisant les conditions d'approvisionnement. Cette traçabilité de bout en bout facilitera la lutte contre la contrefaçon, la fraude et les crimes économiques transfrontaliers.
- L'agriculture : dans ce domaine, des réseaux de capteurs interconnectés à l'IdO peuvent être utilisés pour la supervision de l'environnement des cultures. Ceci permettra une meilleure aide à la décision en agriculture, notamment pour optimiser l'eau d'irrigation, l'usage des intrants, et la planification de travaux agricoles. Ces réseaux peuvent être aussi utilisés pour lutter contre la pollution de l'air, du sol et des eaux et améliorer la qualité de l'environnement en général.

5.1.3 Enjeux socioéconomiques

Les applications de l'IdO, de par leur étendue, devraient grandement contribuer à répondre aux problèmes sociétaux d'aujourd'hui: les systèmes de télésurveillance de la santé apporteront des solutions en matière de vieillissement de la population et d'autonomie des

personnes âgées. Les parcelles agricoles connectées aideront à optimiser l'usage de l'eau pour l'irrigation et des intrants pour une meilleure agro-industrie. Les véhicules connectées aideront à optimiser la gestion du trafic urbain, à diminuer la pollution et leur empreinte carbone. Les grilles électriques connectées aideront à optimiser la consommation et la distribution de l'énergie électrique, etc. Cette interconnexion des objets physiques devrait accentuer l'impact considérable, déjà produit sur notre société par les TIC, et entraîner ainsi peu à peu un véritable changement de modèles socio-économiques et culturels.
Ces exemples d'applications montrent que l'IdO peut contribuer à améliorer la qualité de vie des personnes, en créant un nouveau marché, de nouveaux emplois, des débouchés et de la croissance pour les entreprises, et un élan pour la compétitivité. Selon la GSMA [38], l'Internet des objets est une industrie qui devrait apporter aux opérateurs mobiles un revenu autour de $1200 milliards vers 2020. Le nombre d'objets connectés aux horizons de 2020 devrait atteindre les 24 milliards d'objets contre 9 milliards d'objets en 2011.

5.1.4 Architectures et standardisation

L'IdO ne doit pas être considéré comme un concept utopique. En réalité, il sera fondé sur plusieurs technologies habilitantes tels que la RFID [167], la communication en champ proche (NFC : Near Field Communication) [168], les capteurs et actionneurs sans fil, les communications machine-à-machine (M2M [164]), l'ultralarge bande ou 3/4G, IPv6 [165], 6LowPAN [54] et RPL [57], etc. qui devraient tous jouer un rôle important dans le développement de l'IdO [32]. L'IdO voit ses racines remonter aux technologies M2M (Machine-to-Machine) pour le contrôle de processus de production à distance. Cette technologie a évolué vers le concept d'Internet des Objets depuis l'apparition d'IP sur réseaux mobiles cellulaires durant les années 2000 [34].
L'ETSI préconise une évolution du paradigme M2M vers l'internet des objets. Cet organisme de normalisation propose une architecture à base de trois domaines comme illustré sur la Figure 60 : le domaine du réseau d'objets, le domaine du réseau cœur d'accès, et le domaine des applications M2M et applications clientes.

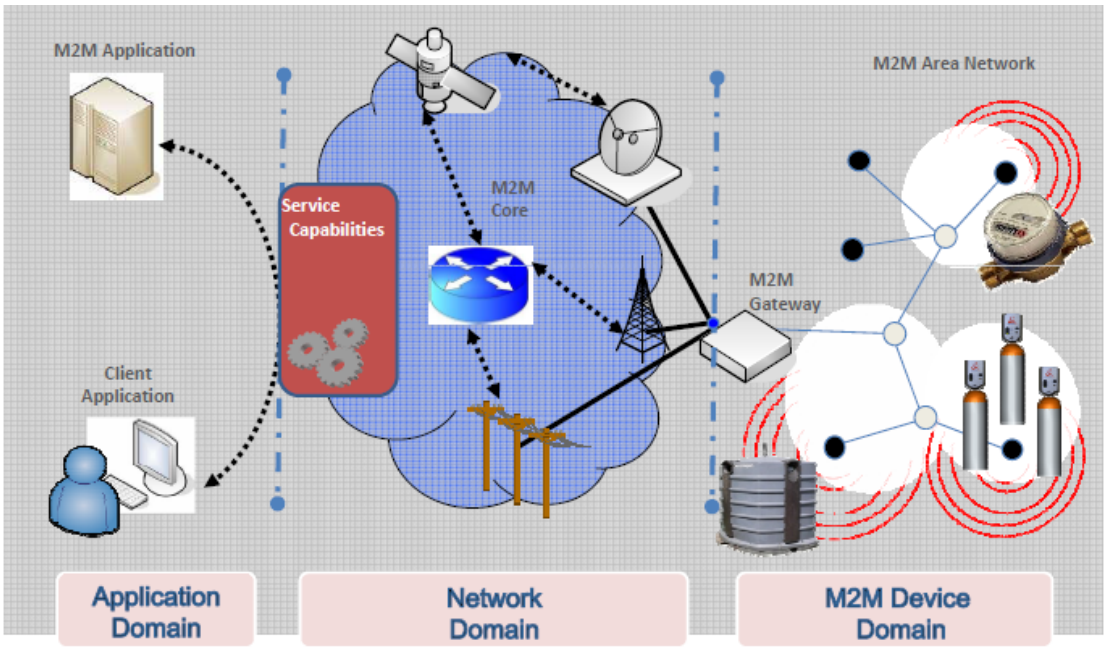


Figure 60 Architecture simple pour l'interconnexion d'objets. Source présentation ETSI à MWC 2011 [36]

Cette architecture permet une coexistence des différentes technologies actuelles et futures qui entrent dans le paysage de développement de l'Internet des objets comme l'illustre la Figure 61 :

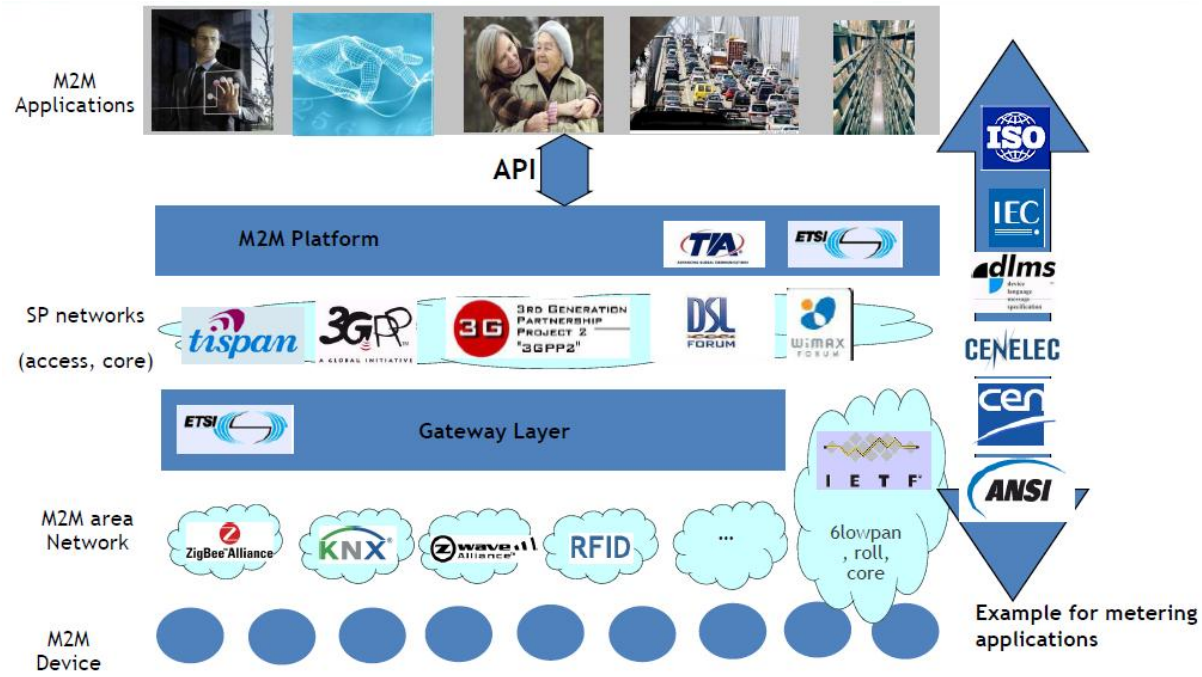


Figure 61 Paysage de standardisation M2M. Source présentation ETSI à MWC 2011 [36]

- Dans le domaine du réseau d'objets, on retrouve les différentes technologies d'interconnexion des objets (M2M [164], RFID [167], IEEE802.15.4, IETF-6LowPAN [54], IETF-RPL [57], etc.), et des passerelles vers les réseaux cœurs de transport
- Dans le domaine du réseau cœur, on retrouve les différentes technologies de réseaux de transport et d'accès comme xDSL, WiMax, WLAN, 3/4G, etc.
- et dans le domaine des applications M2M et applications clientes on retrouve les plateformes M2M, les middlewares et API des applications M2M, processus métiers exploitant l'internet des objets, etc.

5.2 L'internet des Objets : vulnérabilités et menaces

« *The National Intelligence Council (NIC)*» américain considère que les avancées technologiques combinées à une forte demande des marchés encourageraient une adoption et un déploiement à large échelle de l'IdO. Néanmoins, la plus grande crainte est que les objets du quotidien deviennent des risques potentiels d'attaque de sécurité. Pire encore, la pénétration à large échelle de l'IdO diffuserait ces menaces d'une façon beaucoup plus large que l'Internet d'aujourd'hui [39].

En effet, l'ubiquité de l'IdO amplifiera les menaces classiques de sécurité qui pèsent sur les données et les réseaux. Mais en plus, le rapprochement du monde physique et du monde virtuel à travers l'IdO ouvre la voie à de nouvelles menaces qui pèseront directement sur l'intégrité des objets eux-mêmes, les infrastructures et processus (monde physique), et la vie privée des personnes.

5.2.1 Amplification des menaces sur les données et les réseaux

L'omniprésence des objets communicants dépourvus de protection physique et de surveillance, les rendent une proie facile aux attaques matérielles et logicielles. Ces objets peuvent être volés, corrompus et contrefaits. Sans mesures particulières, les données stockées sur ces dispositifs seraient alors accessibles, y compris des données cryptographiques qui permettraient d'accéder à d'autres données sensibles ou jouer des rôles sensibles dans les systèmes complexes les hébergeant. Par ailleurs, les transmissions sans fil, sont à leur tour une proie facile à l'écoute et au dénie de service (« *jamming* » [162][163]). Il existe aujourd'hui des solutions cryptographiques pour assurer des services de confidentialité, de contrôle d'intégrité, d'authentification, de non-répudiation, etc. mais beaucoup reste à faire pour rendre ces algorithmes efficaces et performants sur des dispositifs embarqués de plus en plus miniaturisés.
Le CERP-IoT cite dans [29] quelques problématiques amplifiées par la nature des objets embarqués miniaturisés. On cite notamment : l'hétérogénéité et la mobilité des objets qui rajoutent une couche de complexité aux problèmes de sécurité.

5.2.2 Menaces sur la vie privée

Tous les pronostics envisagent le développement d'une informatique ambiante avec potentiellement des dizaines d'objets par personne y compris dans leur sphère privée et intime. Ces objets de l'espace personnel sont *géo-localisables,* peuvent communiquer avec d'autres objets à travers des réseaux spontanés, peuvent *écouter* ce que dit la personne, peuvent *filmer* la personne et/ou son environnement, et peuvent même enregistrer son rythme cardiaque, son rythme respiratoire, la température de son corps, et sa cinématique !
Des questions légitimes se posent sur le devenir de cette masse de données personnelles et parfois intimes. Sans régulation stricte, une protection accrue de la privacy, un degré élevé de contrôle des objets par les usagers, l'adoption de l'IdO serait un échec. L'ITU dans son rapport sur l'Internet des Objets [27] a pointé du doigt ces menaces potentielles. Elle conclue que la protection de la privacy ne doit pas se limiter à des solutions technologiques, mais doit comprendre des mesures juridiques, une régulation du marché et des considérations socio-éthiques comme illustré sur la Figure 62.

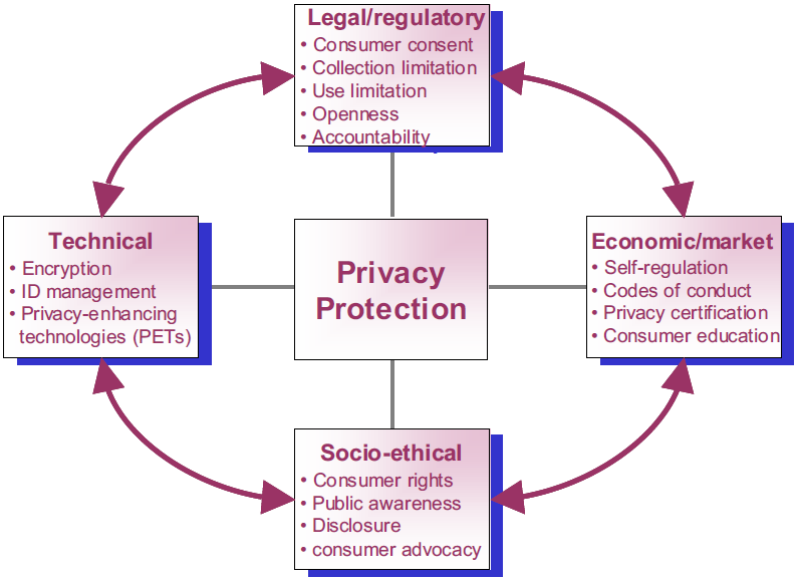


Figure 62 Les différentes facettes de protection de la privacy. Source ITU [27]

5.2.3 Menaces sur les systèmes et l'environnement physique des objets

L'IdO fera partie intégrante du monde physique et des systèmes complexes. En conséquence, un disfonctionnement quelconque, un déni de service, ou un comportement byzantin des objets n'entravera plus uniquement l'intégrité du monde virtuel (composé de données et d'informations), mais directement les processus sous leur contrôle en causant des dommages collatéraux importants. De ce point de vue, l'IdO pourrait constituer un véhicule privilégié pour les *hackers* amateurs de sensations fortes et la menace terroriste !
Par exemple, dans [36], il est rapporté qu'en 2010 le ver StuxNet avait infecté des dizaines de milliers de stations Siemens SCADA. Ces systèmes étaient utilisés en majorité dans des entreprises de services et de fabrication et même des stations nucléaires ! StuxNet avait montré alors qu'il était relativement simple de causer des dommages catastrophiques à un réseau de contrôle industriel. En 2009 [35], une équipe de recherche d'IOActive avait démontré l'existence de failles de sécurité dans des dispositifs utilisés dans des « smart grids » pour le contrôle de distribution de l'énergie. Cette faille permettait à un *hacker* potentiel de diffuser un code malicieux et de couper l'alimentation en électricité des foyers.
Les menaces sur les infrastructures et l'environnement physique des objets sont bien réelles, et nécessitent des mesures préventives pour les contrarier et des solutions curatives pour les confiner et empêcher leur propagation le cas échéant.

5.3 Sécurité de l'Internet des Objets : challenges et perspectives

5.3.1 Dimensions de la sécurité de l'IdO

L'IdO est une *technologie* caractérisée par une forte ubiquité dans le *monde physique* et une omniprésence autour de ses *usagers***.** Les diverses applications potentielles de l'IdO, l'hétérogénéité de ses technologies habilitantes et sa forte dimension humaine et socioéconomique rendent sa sécurité un sujet difficile et complexe. En plus des problèmes de *sécurité des technologies* qui le constitueront, l'IdO accentue les problèmes de *sécurité des personnes* qui l'utiliseront, et fait émerger de nouveaux problèmes liés à la sécurité des *systèmes* sous son contrôle. Comme nous l'illustrons sur la Figure 63, la *sécurité et la privacy* dans l'IdO peut être abordée de trois angles complémentaires qui reflètent ses dimensions *technologique, humaine et systémique*.
La protection de la technologie concerne en premier lieu la sécurité des données, des communications et des infrastructures réseaux. Cette protection est nécessaire pour contrarier les attaques classiques et futures sur l'intégrité, l'authenticité et la confidentialité des données, ainsi que les attaques sur les infrastructures réseaux et leurs fonctionnalités. La protection des personnes concernera la protection de la vie privée des usagers (*« privacy »*) qui nécessite, en plus des solutions technologiques, une régulation appropriée qui établit les responsabilités en cas de litiges. La protection des systèmes interconnectés et hébergeant les objets de l'IdO, concernera la protection des objets eux-mêmes livrés à ces systèmes et les processus qu'ils contrôleront.

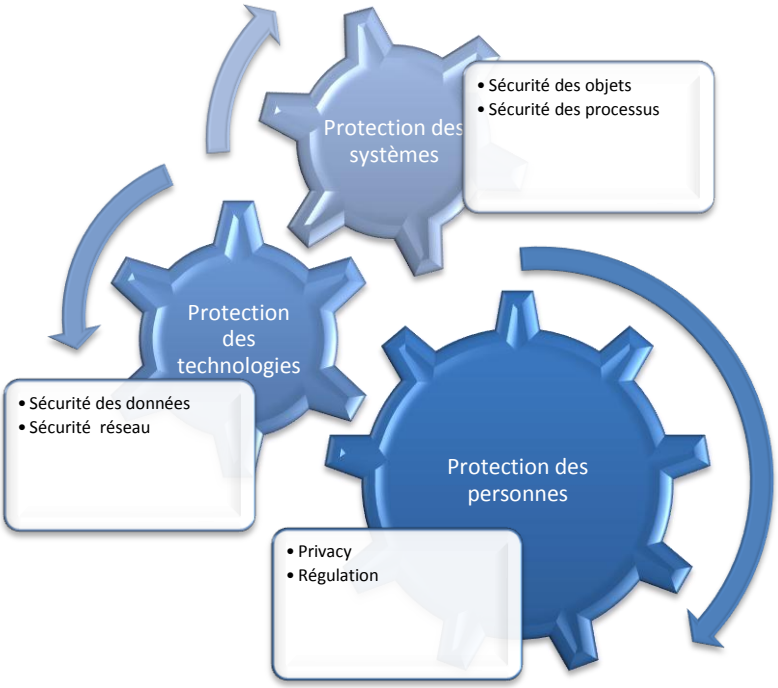


Figure 63 Sécurité et Privacy de l'Internet des Objets

5.3.2 Plan d'action à court, moyen et long termes

Après analyse des travaux existants et les besoins de l'IdO en termes de sécurité, nous concluons que les développements potentiels se dérouleront autour de trois axes à court, moyen et long termes :

- une sécurité efficace pour une informatique embarquée miniaturisée,
- une sécurité adaptative de l'informatique mobile omniprésente, et
- une sécurité de l'internet des objets selon une approche cognitive et systémique.

Ces trois axes répondront aux besoins évolutifs de l'IdO en termes de sécurité et accompagneront son évolution vers *plus d'autonomie* des objets. Dans la Figure 64, nous illustrons ces trois chantiers et synthétisons les verrous scientifiques et technologiques derrière chacun de ces axes.

Dans les sections suivantes nous donnons un aperçu de ces verrous en nous appuyant sur nos travaux antérieurs et en nous positionnant par rapport aux travaux en cours. Nous présenterons, en outre, des perspectives à la lumière des besoins potentiels du futur IdO.

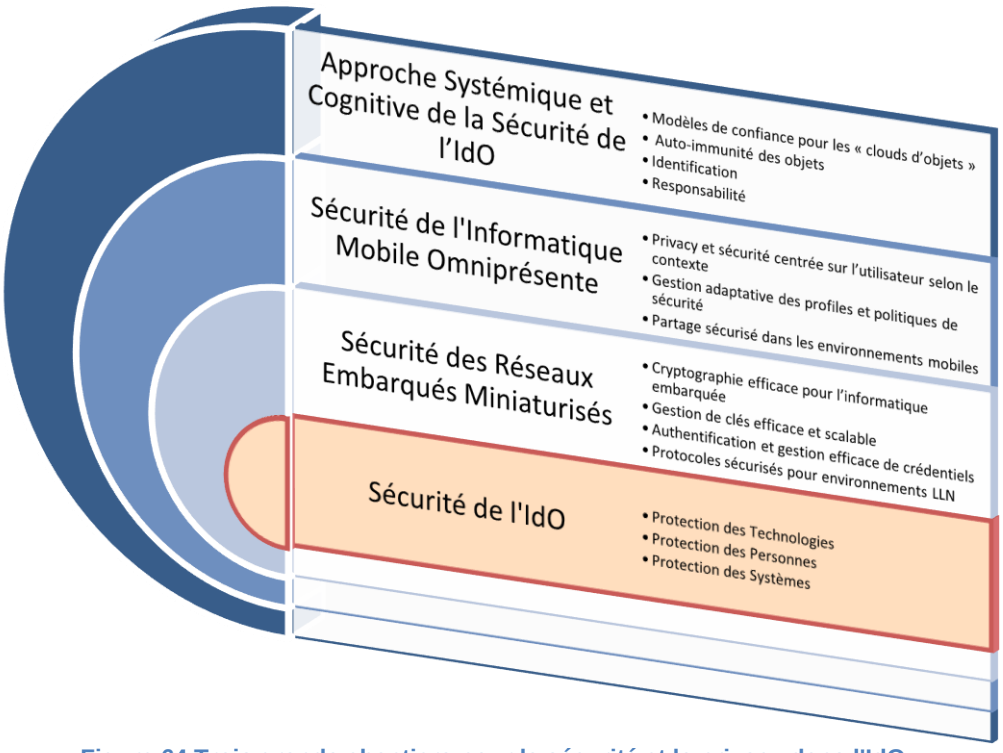


Figure 64 Trois grands chantiers pour la sécurité et la privacy dans l'IdO

5.3.3 Sécurité des réseaux embarqués miniaturisés

Durant ces dernières années, le besoin de développer des systèmes cryptographiques performants, efficaces et peu coûteux en termes de ressources (énergie, mémoire, bande passante) fut déjà ressenti. L'avènement de l'IdO avec l'interconnexion d'un nombre potentiellement très élevé d'objets omniprésents, accentue le problème de rareté des ressources en y ajoutant une problématique d'adaptation au facteur d'échelle. Parmi les challenges et verrous scientifiques et technologiques, les problèmes suivants occuperont une place importante dans les travaux à venir à court et long termes :

5.3.3.1 Cryptographie efficace pour l'informatique embarquée miniaturisée

Un besoin immédiat est le développement de mécanismes de sécurité efficace pour l'informatique embarquée miniaturisée. Les développements actuels des réseaux de capteurs, actionneurs, de la technologie RFID et de l'informatique mobile montrent les limites des dispositifs qui constitueront l'IdO en termes de ressources et capacités. Tim Polk et Sean Turner (IETF Security area editors) évoquent, dans [41], la nécessité de vérifier l'applicabilité de la cryptographie moderne dans le contexte de l'IdO. En effet, les limitations de ressources et capacités des objets embarqués miniaturisés rend difficile l'utilisation des algorithmes cryptographiques actuels en raison de leur consommation en termes de calcul et mémoire [43][44].

Nous croyons que l'émergence d'une cryptographie robuste et peu coûteuse en termes de ressources combinée à des avancées technologiques d'auto-récupération de l'énergie (« energy harvesting »), permettraient de surmonter ces difficultés à moyen terme. En effet, plusieurs travaux de recherche ont montré que la cryptographie à base de courbes elliptiques [42] offrait un niveau de robustesse de la sécurité semblable à la cryptographie asymétrique classique avec l'avantage d'être peu coûteuse en termes de ressources (mémoire, calcul, bande passante). Par ailleurs, des développements récents ont démontré

la possibilité de récupérer de l'énergie (« energy harvesting »), sous certaines conditions, de l'environnement des objets communicants. En effet, plusieurs sources d'énergie peuvent être exploitées pour augmenter l'autonomie des objets en termes d'énergie, tels que : le mouvement et les vibrations [45].

5.3.3.2 Gestion de clés efficace et scalable pour l'Internet des Objets

Durant ces dernières années, nous avons abordé le sujet de gestion de clés pour les réseaux de capteurs à fortes contraintes de ressources. L'inadéquation de la cryptographie asymétrique nous a poussés vers l'exploration de techniques à base de clés symétriques et en particulier la pré-distribution de clés. Nous pensons qu'il faudra remettre en cause ce choix dans le contexte de l'Internet des objets. En effet, comme le notent Tim Polk et Sean Turner dans [41], l'IdO fait émerger la question d'échelle avec force en ce qui concerne la gestion de clés. Si l'on rajoute à cela, la maniabilité de la technologie par des utilisateurs non-experts, les approches de gestion de clés à base de pré-déploiement de clés ne seraient applicables qu'à une échelle réduite et limitée à des usagers expérimentés.

Nous croyons que la situation devrait évoluer dans le contexte de l'IdO vers des méthodes de gestion de clés basée sur une cryptographie peu coûteuse, ne nécessitant pas une intervention humaine. Ainsi, la cryptographie à base de courbes elliptiques [42], entre autres, devrait jouer un rôle important dans les systèmes de gestion de clés.

Par ailleurs, l'ubiquité des objets de l'IdO et la difficulté de leur procurer une protection physique et/ou une surveillance permanente, les exposent au risque de compromission physique par des intrus. Ceci peut avoir un impact important si les intrus réussissent à récupérer les clés cryptographiques qui seraient dans la mémoire des objets corrompus et à les utiliser pour mener des attaques diverses sur le réseau et les autres objets. Afin de réduire les conséquences de cette vulnérabilité due à l'intégration des objets de l'IdO au monde physique, il serait nécessaire que la gestion de clés soit *résiliente,* en d'autres mots *tolérante* à la compromission des objets.

Deng et al. [46] définissent deux propriétés qui doivent être vérifiées dans la conception d'un système *résilient* de gestion de clés : (i) la propriété d'*opacité* : un adversaire ne devrait pas avoir la capacité de déduire d'autre clés utilisées dans le réseau en compromettant un nombre réduit d'objets. (ii) la propriété d'*inoculation* : un adversaire ne devrait pas pouvoir introduire un objet non légitime dans le réseau en compromettant un nombre réduit d'objets. Nous pensons que ce type de propriétés devrait en effet être pris en compte dans la conception d'une gestion de clés *résiliente* pour l'IdO.

Sur un autre volet, nous croyons que la communication de groupe est l'un des paradigmes de communication qui sera largement utilisé dans l'IdO. En effet, c'est un des scénarios de communication envisagés dans les architectures M2M [47][48], où plusieurs machines s'adressent à un serveur ou un serveur s'adresse à plusieurs machines. Par ailleurs, l'ubiquité des objets, favorisera le concept de réseaux privés de groupe d'objets (VPN d'objets). Dans ce contexte, nous croyons que nos travaux de thèse sur la communication de groupe sécurisée [49] avec une approche adaptative pour les réseaux dynamiques [161][160][159][158][157][156] nous permettent de concevoir des solutions adaptées à la gestion de clés pour les communications de groupe dans l'IdO.

5.3.3.3 Authentification et gestion efficace de crédentités

L'Internet des objets, par sa taille et les rôles importants que joueront les objets dans leur environnement, rend l'authentification des objets et la gestion des crédentités, un enjeu important et un challenge difficile. En plus des problèmes de *scalabilité*, la relation, parfois

complexe, des objets aux utilisateurs rendent la gestion des crédentités difficile [41]. L'hétérogénéité des techniques d'identification des utilisateurs et des objets est un autre verrou technologique qui nécessite une investigation particulière.

5.3.3.4 Protocoles sécurisés pour les environnements dynamiques à énergie et connectivité faibles

Une des technologies préconisée à l'IETF pour l'interconnexion des réseaux de l'Internet des objets est IPv6 [50]. Un des avantages majeurs est l'exploitation de l'immense capacité d'adressage de 128bits d'IPv6 [51] ce qui répondrait aux besoins d'adressage à très large échelle d'un IdO qui comporterait potentiellement plusieurs dizaines de milliards d'objets. Cependant, les ressources limitées des objets, notamment en termes d'énergie, et l'environnement de connectivité intermittente (*LLN : Low power Lossy Networks »)* rendent difficile l'implémentation de cette technologie. Une des voies explorées aujourd'hui pour la communication dans les environnements LLN à énergie et connectivité faibles est l'adaptation d'IPv6 à ces environnements à travers une série de protocoles comme 6LowPAN [54] et RPL [57].

« IPv6 over Low power Personal Area Networks » (6LowPAN) est un groupe de travail à l'IETF qui est chargé d'adapter la technologie IPv6 aux réseaux personnels à énergie et connectivité faibles LLN [52]. Parmi les résultats de ce groupe de travail, la technologie 6LowPAN (IPv6 pour PAN) [54] et son adaptation au standard IEEE802.15.4 [55][56] largement utilisé dans les réseaux personnels (PAN) et préconisé pour faire partie intégrante, entre autres technologies, de l'IdO.

« Routing Over Low power Lossy Networks » (ROLL) est un autre groupe de travail à l'IETF dont le rôle est de traiter la problématique du routage dans les réseaux LLN [53]. Après une étude des protocoles de routage existants (OSPF, ISIS, AODV, OLSR), le groupe de travail a conclu à leur inadéquation aux réseaux LLN. De ce fait, ROLL propose un nouveau protocole pour ces environnements spécifiques appelé RPL : IPv6 Routing protocol for Low power and Lossy Networks [57].

Les contraintes de ressources des environnements LLN dans lesquels évolueront les objets de l'IdO nécessitent de nouvelles solutions adaptées pour la sécurité des échanges et pour contrarier les menaces potentielles. Les deux groupes à l'IETF 6LowPAN et ROLL s'intéressent de près à ces problèmes de sécurité et travaillent sur l'élaboration d'un *« framework »* spécifique pour la sécurité dans les environnements LLN [58].

Par ailleurs, dans les réseaux dynamiques, les connexions ne sont pas permanentes, mais utilisent les opportunités qui se présentent. Cela recouvre les réseaux mobiles tels que les réseaux de drones ou de véhicules, mais aussi les réseaux pair-à-pair et les réseaux de capteurs/actionneurs. La dynamique pose de nouveaux challenges dans le développement des protocoles de communication sécurisés. Il s'agit d'une thématique émergente pour laquelle nous ne connaissons pas de solution autre qu'au cas par cas. Nous nous intéresserons au développement d'algorithmes de communication (unicast, multicast, broadcast), de solutions permettant de sécuriser ces réseaux et d'y établir un environnement de confiance, propice au développement de nouvelles applications.

5.3.4 Sécurité de l'informatique mobile omniprésente

L'évolution d'Internet vers un IdO se fera grâce à l'intégration à des systèmes complexes des objets communicants, localisables, mobiles et dotés de facultés les rendant de plus en plus autonomes. Cette informatique omniprésente fera émerger des questions légitimes sur la

privacy des usagers, et sur la variabilité et la diversité des exigences des usagers et des applications en termes de services de sécurité. Ceci nécessite des solutions de sécurité centrées sur les utilisateurs, adaptatives avec une prise en compte du contexte. La diversité des besoins et des exigences en termes de sécurité et privacy pourrait être abordée à travers une gestion adaptative des politiques et des profils de sécurité qui tient compte du contexte ambiant. La protection de la privacy aura son empreinte sur le traitement des données qui devrait désormais tenir compte de cette dimension selon le contexte.

5.3.4.1 Privacy et sécurité centrée sur l'utilisateur selon le contexte

Les capacités perceptives et actionnelles des objets, et les possibilités de géo-localisation suscitent de nombreuses craintes autour de l'anonymat (privacy) des usagers. Sans mesures particulières, des objets pourraient divulguer des informations sensibles autour de la vie privée des personnes.

Nous croyons que l'IdO devrait permettre une prise en compte du contexte de l'utilisateur en permettant un contrôle de granularité fine sur l'informatique ambiante afin de respecter scrupuleusement les convenances et exigences des usagers en termes de protection de la privacy. Par ailleurs, des méthodes doivent être développées pour permettre aux objets d'apporter un traitement des données garantissant la privacy [31]. Les techniques d'anonymisation des données existent aujourd'hui mais nécessitent des équipements dotés de capacités de calcul, de mémoire et de bande passante importantes [29]. Les limitations de ressources des objets et de leurs réseaux les rendent difficilement exploitables. De nouveaux développements de techniques d'anonymisation peu coûteuses en termes de ressources sont nécessaires. La notion de réseaux privés virtuels aura une place importante dans le paysage des techniques de sécurité et privacy de l'IdO. Néanmoins, des adaptations des protocoles sous-jacents, le plus souvent gourmands en termes de ressources, seront nécessaires. Le cas échéant, et pour les applications les plus sensibles, d'anciennes techniques d'établissement de périmètres de sécurité pour restreindre et contrôler les objets de l'IdO peuvent être adaptées [41].

5.3.4.2 Gestion adaptative des profils et politiques de sécurité

L'hétérogénéité qui caractérise déjà les TIC aujourd'hui, sera de vigueur et même amplifiée dans le future IdO. On s'attend au développement d'un écosystème technologique caractérisé par l'hétérogénéité des objets eux-mêmes, des technologies utilisées pour leur interaction, et des contextes d'usage. L'informatique ambiante qui en découle sera fortement imprégnée par les préférences des usagers, le plus souvent hétérogènes.

L'hétérogénéité technologique des objets en interaction, nécessite le développement d'une approche adaptative de la sécurité, une approche capable de tenir compte des capacités hétérogènes des objets en termes de ressources, et des niveaux de sécurité exigés par le contexte [60]. L'hétérogénéité des contextes d'usage et des domaines administratifs exigera une gestion adaptative des politiques de sécurité. Cette gestion adaptative devrait permettre aux objets, parfois mobiles, d'interagir avec leur environnement, et d'évoluer dans différents contextes, en toute sécurité. La notion de profils de sécurité pourrait être utilisée pour représenter les exigences de sécurité et privacy en tenant compte des contextes d'usage, des préférences des utilisateurs, et des capacités des objets et technologies, dans leur hétérogénéité. Encore une fois, une gestion adaptative de ces profils serait nécessaire pour permettre une interaction sécurisée des usagers et des objets dans des environnements évolutifs hétérogènes.

5.3.4.3 Partage sécurisé dans les environnements mobiles

L'omniprésence des réseaux d'objets communicants facilitera le partage des fichiers, des données personnelles, et même des ressources (« *cloud d'objets* »). Cette omniprésence conjuguée à une forte dynamique et une mobilité continue des objets communicants ne fera qu'amplifier ce partage et émerger un nouveau vecteur de partage à travers le « *nomadisme* » (un partage tolérant aux délais). Nous croyons que ce partage, véhiculé par la mobilité et le nomadisme, constituera une proie privilégiée aux attaques de sécurité. Des attaques qui sont à leur tour amplifiées et facilitées par l'ubiquité des objets communicants qui constituent des passerelles potentielles vers des réseaux et des données privées. Une des perspectives de nos travaux est d'accompagner cette évolution en proposant des solutions efficaces pour un partage serein et sécurisé. Nous prendrons en considération l'omniprésence des réseaux d'objets communicants et leur mobilité (transfert de contexte de sécurité) pour concevoir des systèmes, de partage pair-à-pair, qui soient sécurisés, efficaces et équitables.

5.3.5 Approche cognitive et systémique de la sécurité de l'IdO

L'Internet des objets permettra aux objets de notre environnement de devenir des participants actifs partageant l'information avec d'autres objets du réseau. Ces objets seront capables de reconnaître des événements et des changements dans leur environnement et pourront capter et réagir d'une façon assez autonome sans intervention humaine [33]. En effet, l'informatique évolue d'un réseau de calculateurs qui traitent des données, vers des réseaux de plus en plus *« intelligents »* dotés de capacités de captage, de perception et reconnaissance, d'action et réaction, et continuera à évoluer vers plus d'*autonomie.*

L'intégration des objets dans la commande de systèmes complexes et le monde physique, rend la sécurité de l'IdO très difficile à appréhender d'une façon analytique. Nous croyons qu'une approche systémique de la sécurité [61] est plus appropriée pour l'IdO. Une approche systémique qui permettra de tenir compte de la complexité intrinsèque des systèmes qu'interconnectent l'IdO.

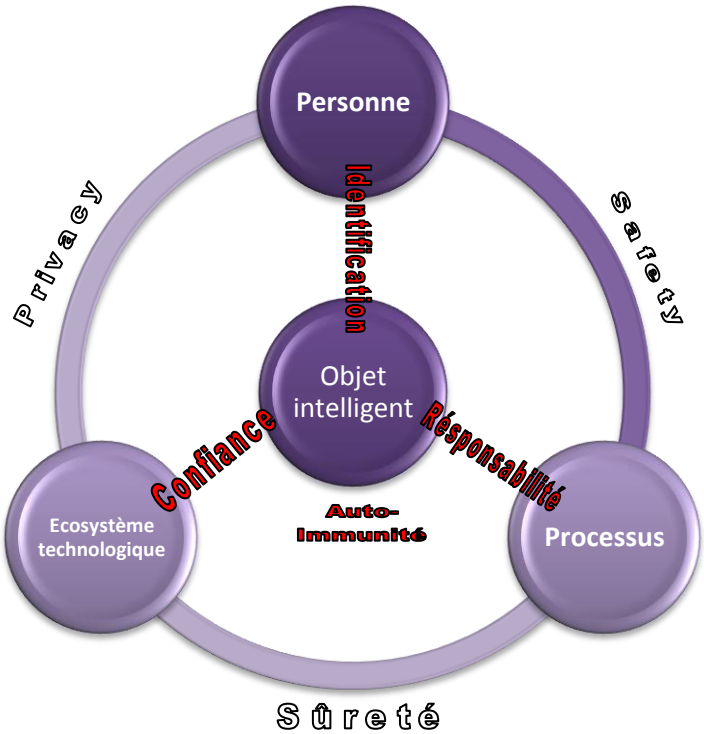


Figure 65 Vers une approche systémique de la sécurité dans l'IdO

En effet, l'Internet des objets est un système complexe dans lequel interagissent des *personnes* avec un *écosystème technologique* à base d'*objets intelligents* à travers des *processus* complexes. Les interactions de ces quatre composantes de l'IdO (personnes, objets intelligents, écosystème technologiques, processus) font émerger une dimension systémique à la sécurité de l'IdO. Sur la Figure 65, nous illustrons les différentes interactions entre les composantes de l'IdO et les tensions qu'elles créent sur la sécurité.
L'interaction des personnes avec l'écosystème technologique requiert la protection de leur *privacy*. De même, leur interaction avec les processus qui commandent les systèmes nécessite la garantie de leur *safety.* L'exécution des processus doit garantir leur *sûreté de fonctionnement* et vérifier la réalisation des objectifs pour lesquels ils sont conçus.
L'objet intelligent qui est au cœur de l'IdO crée ses propres tensions sur la sécurité de l'IdO, ce qui nécessite une attention particulière. En effet, nous croyons que l'évolution vers plus d'autonomie de ces objets accentuera les enjeux de la sécurité des technologies et des processus et de la privacy des personnes. Comme nous l'illustrons sur la Figure 66, au même titre que l'autonomie des objets à percevoir et à agir sur l'environnement, la sécurité de l'IdO devrait évoluer vers plus d'autonomie perceptive et actionnelle en se basant sur une approche cognitive [62] et systémique [61].

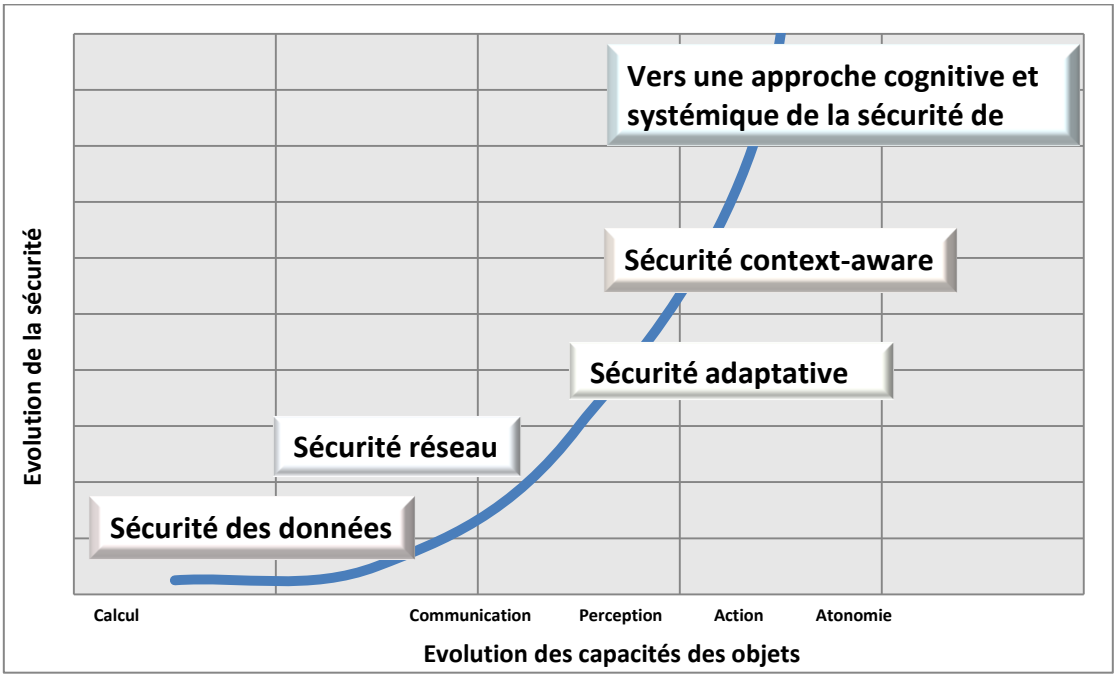


Figure 66 Vers une sécurité cognitive et systémique de l'IdO

Dans ce qui suit, nous présenterons ces verrous autour des tensions sur la sécurité de l'IdO créées par les objets intelligents dans leur interaction avec les personnes, l'écosystème technologique et les processus. Ces tensions (*confiance, responsabilité, identification et auto-immunité*) seront caractérisées par une dimension *cognitive et systémique* induite par l'*autonomie* grandissante des objets (cf. Figure 66).

5.3.5.1 Modèles de confiance pour les « clouds d'objets »

Selon le CERP-IoT, les communications dans l'IdO auront plutôt une nature transactionnelle sur des nuages d'objets. Cette vision est créditée par l'évolution des capacités de stockage avec plus de miniaturisation, et une évolution constante des capacités de calcul à moindre coût (loi de Moore). Ceci aura pour conséquence, la disponibilité locale de l'information dans

le nuage d'objets à proximité. Cette évolution va pousser les objets à jouer un rôle de plus en plus important dans l'infrastructure réseau [29].
Nous croyons, effectivement, que le développement de l'IdO à large échelle engendrera des évolutions majeures des modèles économiques qui gouverneront l'internet des objets. Une de ces évolutions potentielles serait *l'intégration des objets dans le processus de transport des flux de l'IdO,* une fonction jusque-là réservée à des opérateurs bien établis*.* En effet, nous assisterons à une *banalisation* des objets communicants, et à une omniprésence des réseaux domestiques et personnels qui viendraient s'ajouter aux réseaux d'entreprise. La multiplication de ces réseaux (*clients*) omniprésents créerait des infrastructures de communication à part entière, avec des capacités de calcul, de stockage et de bande passante grandissantes. Ainsi, il serait bénéfique d'intégrer ces infrastructures clientes dans le processus de transport des flux de l'internet des objets. Ce qui encourage cette évolution est le succès qu'a connu une évolution similaire dans des réseaux de transport plus classiques : nous pensons en particulier aux réseaux électriques où de grands opérateurs mettent en location des infrastructures de leurs clients (panneaux solaires, éoliennes) pour participer au processus de production d'électricité. Une autre « success story » similaire est le covoiturage, où les clients du réseau de transport urbain, participe au processus de transport publique avec leur propre moyen de transport.
Partant de cette hypothèse, de nouveaux modèles économiques verront le jour, mais aussi de nouvelles menaces d'attaques, d'intrusion, et de piraterie se développeront comme ce fut le cas après chaque évolution technologique majeure.
Une des perspectives de nos travaux est d'accompagner cette évolution. Nous proposerons des modèles de confiance qui permettraient une évolution sereine vers un tel modèle *« oligarchique »* de l'infrastructure de transport de l'internet des objets à base de micro-opérateurs. Nos travaux autour des modèles de confiance dans les MANET nous serviront de base pour affronter ces nouveaux challenges. Nous considérerons en particulier des verrous qui émergent de la nature de l'Internet des objets et qui auront un impact important sur la conception de ces modèles de confiance : *scalabilité à un nombre très élevé d'objets et des domaines administratifs les accueillant, environnement à énergie et connectivité faibles (LLN), et hétérogénéité technologique des objets et des réseaux.*

5.3.5.2 Auto-immunité des objets

Les objets de l'IdO ont tendance à acquérir plus d'autonomie à travers leurs capacités d'action et de perception. Néanmoins, ils souffrent d'une vulnérabilité intrinsèque vu l'absence de protection physique de ces objets. En conséquence, il devient nécessaire de développer des mécanismes procurant aux objets une *auto-immunité* contre les codes malicieux. Dans ce contexte, Rachel Greenstadt de Harvard University et Jacob Beal du MIT préconisent, dans [59], l'utilisation de la *virtualisation* et le *« trusted computing»* à travers une *TPM (Trusted Platform Module)* pour la protection des objets.
Vu les contraintes de ressources et de coût, il est prématuré d'envisager une généralisation de ces mécanismes de virtualisation et de « trusted computing » à toutes sortes d'objets quelles que soient leurs capacités et leur coût. Il est néanmoins important de concevoir des mécanismes d'auto-immunisation des objets contre les attaques, et leur confinement en cas d'infection par un code malicieux pour limiter les *dommages collatéraux* et la propagation des attaques*.*

5.3.5.3 Identification

Nous croyons que l'identification robuste et scalable jouera un rôle déterminant dans la sécurité de l'IdO. En effet, elle permettrait de compenser la vulnérabilité des objets livrés sans protection à un environnement potentiellement hostile. Cette absence de protection physique encouragera alors les attaques à base de compromission physique des objets pour accéder aux données cryptographiques sensibles qui ouvrent la voie à des attaques par escalade de privilèges.

R. Greenstadt et J. Beal [59] proposent l'utilisation d'une imprégnation des objets puis une identification biométrique continue pour la protection des objets. Cette identification biométrique peut être diverse et variée comme les empreintes, l'image de la rétine, la fréquence de la voix, le mouvement, la reconnaissance du visage, etc. L'objectif est de permettre une reconnaissance assez naturelle du propriétaire de l'objet et ainsi éviter un tas de failles et d'attaques de sécurité par de tierces parties non légitimes à manipuler les objets.

5.3.5.4 Responsabilité

L'autonomie des objets à capter, percevoir, agir et réagir dans le cadre d'un écosystème technologique complexe suscite la question d'établissement de *responsabilités* (« liability enforcement »). On écarte bien évidemment la connotation pénale et humaine de cette notion, mais l'implication des objets dans des processus de commande nous sensibilise à cette question d'un point de vue systémique. Il est donc important que les objets autonomes de l'IdO puissent revenir à l'Homme lorsque qu'il s'agit d'actions importantes en liaison avec la sécurité [59]. Toute la difficulté de la question réside bien évidemment dans la caractérisation de ce qui est *dangereux* pour un processus, la *perception objective de la menace* et la *conception mesurée de la réponse* [59].

5.4 Conclusion

Dans ce chapitre, nous avons présenté des perspectives de nos travaux motivés par l'évolution de l'Internet vers un Internet des objets. Nous avons montré que cette nouvelle technologie de rupture à enjeux socioéconomiques importants suscitera ses propres challenges de sécurité et de « privacy ». Afin d'apporter des réponses à ces problèmes de sécurité de l'Internet des objets, nous avons présenté un plan d'action à court, moyen et long termes. Ces trois phases porteront respectivement sur *la sécurité efficace pour une informatique embarquée miniaturisée, la sécurité et privacy de l'informatique mobile omniprésente, et une approche cognitive et systémique de la sécurité de l'IdO.* Nous avons présenté les verrous scientifiques et technologiques qui se présentent pour chacun de ces paliers avec un positionnement par rapport aux travaux existants. Nous avons par ailleurs, présenté des perspectives d'évolution de ces verrous et montré comment on pouvait s'appuyer sur nos travaux récents pour affronter ces nouveaux challenges difficiles et complexes.

Chapitre 6 : Conclusion générale

Dans nos travaux, nous nous sommes intéressés à la maîtrise de l'interaction des systèmes en termes de robustesse. Nous avons développé des solutions algorithmiques aptes à satisfaire les besoins des utilisateurs en termes de performance et de robustesse tout en leur permettant de faire abstraction de la complexité sous-jacente. Depuis la fin de ma thèse en 2005, nous avons amorcé une nouvelle activité au sein de notre laboratoire HEUDIASYC. Cette activité s'articule autour de deux axes de recherche qui se situent à deux limites de la connaissance contemporaine sur la sécurité des systèmes : *la sécurité collaborative des systèmes en interaction et la sécurité des systèmes à fortes contraintes de ressources*. Cette activité s'inscrit pleinement dans les axes de notre laboratoire, et tout en particulier dans le cadre du *LABEX MS2T « Maîtrise de Systèmes de Systèmes Technologiques »*. En effet, un des axes majeurs du *LABEX MS2T* est l'interaction et la coopération entre systèmes. Une interaction qui doit être robuste au sens large du terme, et sécurisée tout en particulier. Nous avons proposé des solutions efficaces pour une interaction robuste et sécurisée entre des systèmes hétérogènes. Nous avons considéré en particulier les systèmes à fortes contraintes de ressources comme les réseaux de capteurs sans fil, et les systèmes sujets à des attaques de sécurité internes de plus en plus sophistiquées. Plusieurs de ces attaques sont asymptotiques aux comportements légitimes des processus des systèmes en interaction, ce qui rend leur diagnostic très difficile. Nous avons démontré à travers nos travaux que l'interaction robuste et sécurisée entre ces systèmes atypiques est possible. Elle est possible grâce à une nouvelle appréhension de la sécurité basée sur la collaboration de processus de confiance, et la prévention à base de mécanismes proactifs de tolérance aux dysfonctionnements.

L'évolution de nos axes de recherche est principalement motivée par la prise en compte de nouvelles évolutions technologiques et de leur usage pour lesquels nous proposerons des solutions algorithmiques de sécurité tout en optimisant les coûts inhérents. Une évolution majeure qui s'inscrit dans la continuité des développements récents des technologies de l'information et de la communication et des systèmes embarqués, est *« l'internet des objets »*. Cette technologie de rupture sera accompagnée d'une évolution des usages et de l'écosystème technologique dans toute sa complexité.

Dans ce rapport, nous avons montré que cette nouvelle technologie à enjeux socioéconomiques importants suscitera ses propres challenges de sécurité et de « privacy ». Afin d'apporter des réponses à ces problèmes de sécurité de l'Internet des objets, nous avons présenté une évolution de la thématique sur trois axes. Ces trois axes porteront sur *la sécurité efficace pour une informatique embarquée miniaturisée, la sécurité et privacy de l'informatique mobile omniprésente, et une approche cognitive et systémique de la sécurité de l'internet des objets.* Nous avons présenté les verrous scientifiques et technologiques qui se présentent pour chacun de ces paliers avec un positionnement par rapport aux travaux existants. Nous avons présenté des perspectives d'évolution de ces verrous et montré comment on pouvait s'appuyer sur nos travaux récents pour affronter ces nouveaux challenges difficiles et complexes. Nous avons montré, par ailleurs, que l'évolution des objets vers plus d'autonomie accentuera les enjeux de la sécurité et de la privacy. Au même titre que l'autonomie des objets à percevoir et à agir sur l'environnement, la sécurité de l'Internet des Objets devrait évoluer vers plus d'autonomie perceptive et actionnelle en se basant sur une approche cognitive et systémique centrée sur les objets intelligents.

Chapitre 7 : Bibliographie

[1] Mawloud Omar, Yacine Challal, Abdelmadjid Bouabdallah, “Certification-based trust models in mobile ad hoc networks: A survey and taxonomy”, Journal of Network and Computer Applications (Elsevier), Volume 35, Issue 1, January 2012, Pages 268-286.

[2] M. Omar, Y. Challal, A. Bouabdallah, “Reliable and fully distributed trust model for mobile ad hoc networks”, Computers and Security (Elsevier), vol. 28, num. 3-4, pp. 199-214, 2009.

[3] M. Omar, Y. Challal, A. Bouabdallah, “NetTRUST: mixed networks trust infrastructure based on threshold cryptography”, IEEE- SecureCom / SECOVAL Workshop, 2007.

[4] M. Omar, Y. Challal, A. Bouabdallah, « ICARM : Infrastructure de Confiance pour les Architectures de Réseaux Mixtes », SAR-SSI’07.

[5] Sinan Hattahet, " Worms propagation and detection in Peer-to-Peer networks“, Thèse de doctorat, (Avril 2011)

[6] S. Hatahet, A. Bouabdallah, Y. Challal, “A New Worm Propagation Threat in BitTorrent : Modeling and Analysis”, Telecommunication Systems (Springer), Vol. 45, N° 2-3, pp. 95-109, 2010.

[7] S. Hatahet, Y. Challal, A. Bouabdallah, “BitTorrent Worm Sensor Network : P2P Worms Detection and Containment”, IEEE Euromicro International Conference on Parallel, Distributed, and network based Processing, Weimar, Germany, February, 2009.

[8] A. Babakhouya, Y. Challal, A. Bouabdallah, S. Gharout; “S-DV: a new approach to Secure Distance Vector routing protocols”, IEEE-SecureCom’06 (SECOVAL Workshop), 2006.

[9] Ouadjaout, A., M. Bagaa, A. Bachir, Y. Challal, N. Lasla, L. Khelladi, “Information Security in Wireless Sensor Networks” in Encyclopedia on Ad Hoc and Ubiquitous Computing, pp. 427-472, World Scientific, 2009.

[10] Bechkit, W. and Bouabdallah, A. and Challal, Y. “Enhancing resilience of probabilistic key pre-distribution schemes for WSNs through hash chaining”, ACM-CCS, pp. 642—644, 2010

[11] Bechkit, W. and Challal, Y. and Bouabdallah, A. and Bencheikh, A. “An efficient and highly resilient key management scheme for wireless sensor networks” IEEE-LCN, pp. 220-223, 2010.

[12] Bechkit, W. and Bouabdallah, A. and Challal, Y. “A New Highly Scalable Key Pre-distribution Scheme for WSN”, INFOCOM 2012, Student Track.

[13] Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah, “A New Scalable Key Pre-distribution Scheme for WSN », In Proceedings of IEEE ICCCN, Berlin, Germany, 2012.

[14] Jennifer D. Key. Some applications of magma in designs and codes: Oval designs, hermitian unitals and generalized reed-muller codes. *J. Symb. Comput.*, 31(1/2):37–53, 2001.

[15] Maala, B. and Challal, Y. and Bouabdallah, A. “HERO: Hierarchcal key management protocol for heterogeneous wireless sensor networks “, IFIP WSAN 2008, vol. 264/2008, pp. 125-136, ed.: Springer Boston, 2008

[16] Maala, B. and Challal, Y. and Bettahar, H. and Bouabdallah, A. “Node Capture Attack Impact on Key Management Schemes For Heterogeneous Wireless Sensor Networks”, Global Information Infrastructure Symposium, ed.: IEEE, June, 2009.

[17] Y. Challal and Ouadjaout, A. and Lasla, N. and Bagaa, M. and Hadjidj, A. “Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks”, Journal of Network and Computer Applications (Elsevier), vol. 34, pp. 1380-1397, 2011.

[18] L. Khelladi, Y. Challal, A. Bouabdallah, N. Badache ; « On Security Issues in Embedded Systems : Challenges and Solutions », Int. J. of Information and Computer Security (Inderscience), vol. 2(2), 2008.

[19] Hadjidj, A. , Bouabdallah, A. , Challal Y. “HDMRP : An Efficient Fault-Tolerant Multipath Routing Protocol for Heterogeneous Wireless Sensor Networks”, ICST-QShine 2010

[20] M. Bagaa, N. Laslaa, A. Ouadjaout, Y. Challal, “SEDAN: Securre and Efficient Data Aggregation protocol for wireless sensor Networks”, IEEE-LCN/WSN workshop, 2007.

[21] M. Bagaa, Y. Challal, A. Ouadjaout, N. Lasla, N. Badache, “Efficient data aggregation with in-network integrity control for WSN”, accepted for publication in Journal of Parallel and Distributed Computing.

[22] A. Hadjidj, A. Bouabdallah, Y. Challal “Rehabilitation supervsision using wireless sensor networks”, IEEE-WoWMoM 2011, pp. 1-3.

[23] A. Hadjidj, Y. Challal, A. Bouabdallah “Toward a High-Fidelity Wireless Sensor Network for Rehabilitation Supervision”, IEEE-LCN, pp. 462-469, 2001.

[24] J.A. Guerrero, Y. Challal and P. Castillo, “Impact of Wireless Medium Access Protocol on the Quadrotor Formation Control”, Chapter 11 of the Mini UAV Flight Formation Control, Eds. Jose Alfredo Guerrero and Rogelio Lozano, John Wiley, 2012.
[25] J.A. Guerrero, P. Castillo, Y. Challal, “Trajectory Tracking for a Group of Mini Rotorcraft Flying in Formation”, in IFAC World Congress (IFAC 2011), Milano, August 2011.
[26] Bechkit, W. and Bouabdallah, A. and Challal, Y. « Un Prototype de Réseaux de Capteurs sans Fils pour l'Agriculture et le Contrôle de l'Environnement » CFIP - Colloque Francophone sur l Ingénierie des Protocoles, Sainte Maxime France, 2011,
[27] Babakhouya, A. and Challal, Y. and Bouabdallah, A. and Gharout, S. “Securing Distance Vector Routing Protocols for Hybrid Wireless Mesh Networks”, SAR-SSI 2010
[28] International Telecommunication Union, « The Internet of Things », Report, November 2005.
[29] Cluster of European Research Projects on the Internet of Things, “Vision and Challenges for Realising the Internet of Things”, March 2010.
[30] International Telecommunication Union, “Ubiquitous Network Societies: their impact on the telecommunication industry”, ITU Workshop on Ubiquitous Network Societies, April 2005.
[31] Ovidiu Vermesan et al. “Internet of Things Strategic Research Roadmap”, Cluster of European Research Projects on the Internet of Things, 2011.
[32] Commission des Communautés Européennes, “L’Internet des Objets: un plan d’action pour l’Europe”, 2009.
[33] European Research Cluster on the Internet of Things, « Internet of Things : Pan European Research and Innovation Vision”, October 2011
[34] Lamont Wood, “Today, the Internet, tomorrow—the Internet of Things”, ComputerWorld, http://www.computerworld.com/s/article/9221614/Today_the_Internet_tomorrow_the_Internet_of_Things, November 2011
[35] Robert McMillan, « Power grid is found susceptible to cyberattack”, ComputerWorld, http://www.computerworld.com/s/article/9130178/Power_grid_is_found_susceptible_to_cyberattack, March 2009.
[36] John Brandon, “Six rising threats from cybercriminals”, ComputerWorld, http://www.computerworld.com/s/article/9216603/Six_rising_threats_from_cybercriminals, May 2011
[37] ETSI, “Machine-To-Machine Communications”, WMC, Barcelona, February 2011.
[38] GSMA http://www.gsm.org
[39] National Intelligence Council, Disruptive Civil Technologies — Six Technologies with Potential Impacts on US Interests Out to 2025—Conference Report CR 2008–07, April 2008.
[40] Christoph P. Mayer, “Security and Privacy Challenges in the Internet of Things”, Electronic Communications of the EASST, Volume 17, p.1-12, 2009.
[41] Tim Polk and Sean Turner, “Security Challenges for the Internet of Things”, Workshop on Interconnecting Smart Objects with the Internet, Prague, March 2011.
[42] Ian F. Blake, Gadiel Seroussi, Nigel P. Smart, “Advances in Elliptic Curve Cryptography”, London Mathematical Society Lecture Note Series (No. 317), April 2005.
[43] M. Passing and F. Dressler, « Experimental Performance Evaluation of Cryptographic Algorithms on Sensor Nodes », 3rd IEEE International Conference on Mobile Ad Hoc and Sensor Systems (IEEE MASS), pp 882-887, 2006.
[44] K. Jun Choi, J-I. Song, « Investigation of feasible cryptographic algorithms for wireless sensor network ». In: Proceedings of the 8th international conference on advanced communication technology (ICACT 2006). February 2006.
[45] Tom J. Kamierski (Ed.), Steve Beeby (Ed.), “Energy Harvesting Systems: Principles, Modeling and Applications”, ISBN: 1441975659, Springer, 2010.
[46] J. Deng, C. Hartung, R. Han, and S. Mishra, “A Practical Study of Transitory Master Key Establishment for Wireless Sensor Networks”, Proc First IEEE Int'l Conf Security and Privacy for Emerging Areas in Comm. Networks (SecureComm '05), Sept. 2005.
[47] 3rd Generation Partnership Project (3GPP), “Technical Specification Group Services and System Aspects; Service requirements for Machine-Type Communications (MTC)”, 3GPP TS 22.368 V11.1.0 March, 2011.
[48] 3rd Generation Partnership Project (3GPP), “Technical Specification Group Services and System Aspects; Study on Facilitating Machine to Machine Communication in 3GPP Systems”, 3GPP TR 22.868 V8.0.0, March, 2007.
[49] Yacine Challal, “Sécurité dans les communications de groupe », Thèse de doctorat, Université de Technologie de Compiègne, 2005.
[50] IP Vasseur, « The Internet of Things », Internet Area Meeting IETF 77, March 2010.

[51] Kaushik Das, “IPv6 and Wireless Sensor Networks”, http://www.ipv6.com/articles/sensors/IPv6-Sensor-Networks.htm
[52] IETF 6LowPAN Working Group: http://datatracker.ietf.org/wg/6lowpan
[53] IETF ROLL Working Group: http://datatracker.ietf.org/wg/roll/
[54] N. Kushalnagar, G. Montenegro, C. Schumacher, “IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals”, IETF RFC 4919, August 2007.
[55] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, “Transmission of IPv6 Packets over IEEE 802.15.4 Networks”, IETF RCF 4944, September 2007.
[56] J. Hui, P. Thubert, “Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks”, IETF RFC 6282, September 2011.
[57] T. Winter, P. Thubert, A. Brandt, T. Clausen, J. Hui, R. Kelsey, P. Levis, K. Pister, JP. Vasseur, “RPL: IPv6 Routing Protocol for Low power and Lossy Networks”, IETF Draft, draft-ietf-roll-rpl-19, March 2011.
[58] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, “A Security Framework for Routing over Low Power and Lossy Networks”, IETF Draft, draft-ietf-roll-security-framework-06, June 2011.
[59] Rachel Greenstadt, Jacob Beal, “Cognitive Security for Personal Devices”, MIT Computer Science and Artificial Intelligence Laboratory, Technical Report: MIT-CSAIL-TR-2008-016, March, 2008.
[60] Kang, K.-D.; Son, S.H., “Systematic Security and Timeliness Tradeoffs in Real-Time Embedded Systems”, in proc. of 12th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, pp. 183 - 189, 2006
[61] Laree Kiely and Terry Benzel, “Systemic Security Management”, IEEE Security and Privacy Magazine, Vol. 4(6), pp. 74 – 77, 2006.
[62] Rajani Muraleedharan Sreekumaridevi, “Cognitive security framework for heterogeneous sensor network using swarm intelligence”, PhD Thesis, Syracuse University NY, August 2011.
[63] Network Simulator v2: http://isi.edu/nsnam/ns/
[64] TinyOS: http://www.tinyos.net
[65] PeerSim, “A Peer-to-Peer Simulator”, http://peersim.sourcforge.net/
[66] The AVISPA Project, “Automated Validation of Internet Security Protocols and Applications”, http://avispa-project.org/.
[67] ITU-T Recommendation X509/ISO/IEC 9594-8, « Public-Key and Attribute Certificate Frameworks”. 4th edition, 2001.
[68] S. Buchegger, J.Y. Le-Boudec, “Performance analysis of the CONFIDANT protocol”. In Proceedings of 3rd ACM International Symposium, on Mobile Ad Hoc Networking and Computing, 2002.
[69] E. Ayday, F. Fekri. “A protocol for data availability in Mobile Ad-Hoc Networks in the presence of insider attacks”, Ad Hoc Networks, Volume 8, Issue 2 , Pages 181–192, March 2010.
[70] P. Michiardi, R. Molva, “CORE : a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks”, In Proceedings of 6th IFIP Communication and Multimedia Security Conference, 2002.
[71] Q. He, D. Wu, P. Khosla, “SORI : a secure and objective reputation-based incentive scheme for ad-hoc networks”, In Proceedings of IEEE WCNC'04, 2004.
[72] N. Marchanga, R. Dattab, “Collaborative techniques for intrusion detection in mobile ad hoc networks”. Ad Hoc Networks, Volume 6 Issue 4, June, 2008.
[73] H. Janzadeh, K. Fayazbakhsh, M. Dehghan, M.S. Fallah, “A secure credit-based cooperation stimulating mechanism for MANETs using hash chains”. Future Generation Computer Systems, Volume 25 Issue 8, September, 2009.
[74] C. Zouridaki, B.L. Mark, M. Hejmo, R.K. Thomas, “E-Hermes: A robust cooperative trust establishment scheme for mobile ad hoc networks”. Ad Hoc Networks, Volume 7 Issue 6, August, 2009.
[75] M. Ge, K.Y. Lam, D. Gollmann, S.L. Chung, C.C. Chang, J.B. Li. “A robust certification service for highly dynamic MANET in emergency tasks”. International Journal of Communication Systems, John Wiley and Sons, Volume 22 Issue 9, September 2009.
[76] L. Zhou, Z. Haas. “Securing Ad hoc Networks”. IEEE Network, Vol:3, Issue:6, pp.:24-30, 1999.
[77] S. Capkun, L. Buttyan, J. Hubaux. “Small Worlds in Security Systems - an Analysis of the PGP Certificate Graph. In Proceedings of New Security Paradigms Workshop (ACM), 2002.
[78] S. Capkun, L. Buttyan, J. Hubaux. “Self-organized Public Key Management for Mobile Ad hoc Networks”. IEEE Transactions on Mobile Computing, Vol:2, Issue: 1, pp:52-64, 2003.

[79] S. Raghani, D. Toshniwal, R. Joshi. “Dynamic Support for Distributed Certification Authority in Mobile Ad Hoc Networks”. In Proceedings International Conference on Hybrid Information Technology (IEEE), 2006.
[80] S. Yi, R. Kravets. “MOCA - Mobile Certificate Authority for Wireless Ad hoc Networks”. In Proceedings of the Second Annual PKI Research Workshop, 2003.
[81] J. Luo, J. Hubaux, P. Eugster. “DICTATE - Distributed Certification Authority with Probabilistic Freshness for Ad hoc Networks”. IEEE Transactions on Dependable and Secure Computing, Vol:2, Issue:4, pp:311-323, 2005.
[82] Y. Kitada, Y. Arakawa, K. Takemori, A. Watanabe, I. Sasase. “On demand distributed public key management using routing information for wirelss ad hoc networks”. IEICE Transactions on Information and Systems, Vol:J88-D-1, N°:10, pp: 1571-1583, 2005.
[83] G. Kambourakis, E. Konstantinou, A. Douma, M. Anagnostopoulos, G. Fotiadis. “Efficient Certification Path Discovery for MANET”. EURASIP Journal on Wireless Communications and Networking, Vol(2010), 2010.
[84] A. Shamir. « How to Share a Secret”, Communications of the ACM, Volume 22 Issue 11, Nov., 1979.
[85] M. Hwang, E. Lu, I.C. Lin. “A practical (t,n) threshold proxy signature scheme based on the RSA cryptosystem”. IEEE Transactions on Knowledge and Data Engineering, Volume 15 Issue 6, November, 2003.
[86] Jelena Mikovik, Sven Dietrich, David Dittrich, Peter Reiher, “Internet Denial of Service: Attack and Defense Machanisms”, Prentice Hall, ISBN: 0131475738, 2005
[87] D. Dumitriu, E. Knightly, A. Kuzmanovic, I. Stoica, and W. Zwaenepoel. “Denial-of-service resilience in peer-to-peer file sharing systems”. ACM SIGMETRICS Performance Evaluation Review, Vol: 33(1), pp.:38–49, 2005.
[88] S. Staniford, V. Paxson, and N. Weaver. “How to 0wn the internet in your spare time”. Proceedings of the 11th USENIX Security Symposium, 2002.
[89] W. Yu, C. Boyer, S. Chellappan, and D. Xuan. “Peer-to-peer system-based active worm attacks: Modeling and analysis”. IEEE International Conference on Communications, ICC, pp. 295 - 300, 2005.
[90] N. Khiat, Y. Charlinet, and N. Agoulmine. “The emerging threat of peer-to-peer worms”. In Proc. 1st EEE Workshop on Monitoring, Attack Detection and Mitigation, pages 1–3, 2006.
[91] A. Ramachandran, N. Feamster, and D. Dagon. “Revealing botnet membership using dnsbl counter-intelligence”. In USENIX 2nd Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI’06), 2006.
[92] A. Karasaridis, B. Rexroad, and D. Hoeflin. “Wide-scale botnet detection and characterization”. In USENIX Workshop on Hot Topics in Understanding Botnets (HotBots’ 07), 2007
[93] J. Morparia. “Peer-to-Peer Botnets: Analysis and Detection”. PhD thesis, San Jose State University, 2008.
[94] J. Douceur. “The sybil attack”. Proceedings of First International Workshop on Peer-to-Peer Systems, pages 251–260, 2002.
[95] J. Chan, C. Leckie, and T. Peng. “Hitlist worm detection using source ip address history”. In Proceedings of Australian Telecommunication Networks and Applications Conference, 2006.
[96] E. Koutrouli and A. Tsalgatidou. “Reputation-based trust systems for p2p applications: design issues and comparison framework”. Trust and Privacy in Digital Business, pages 152–161, 2006.
[97] S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina. “The eigentrust algorithm for reputation management in p2p networks”. In Proceedings of the 12th international conference on World Wide Web, pages 640–651. ACM, 2003.
[98] B.N. Levine, C. Shields, and N.B. Margolin. “A survey of solutions to the sybil attack”. Tech report 2006-052, University of Massachusetts Amherst, Amherst, MA, 2006.
[99] J. Kubiatowicz et al. « Oceanstore: An architecture for global-scale persistent storage”. ACM SIGARCH Computer Architecture News, 28(5):190–201, 2000
[100] B. Pretre. “Attacks on peer-to-peer networks”. Ph.D thesis, Swiss Federal Institute of Technology (ETH) Zurich, 2005.
[101] R. Dingledine, N. Mathewson, and P. Syverson. “Tor: The second-generation onion router”. In Proceedings of the 13th conference on USENIX Security Symposium-Volume 13, page 21. USENIX Association, 2004
[102] C. Buragohain, D. Agrawal, and S. Suri. “A game theoretic framework for incentives in p2p systems”. In Proceedings of the 3rd International Conference on Peer-to-Peer Computing, volume 56, 2003.

[103] S. Androutsellis-Theotokis and D. Spinellis. “A survey of peer-to-peer content distribution technologies”. ACM Computing Surveys, 36(4):371, 2004.
[104] L. Zhou, L. Zhang, F. McSherry, N. Immorlica, M. Costa, and S. Chien. “A first look at peer-to-peer worms: Threats and defenses”. 4th International Workshop on Peer-to-Peer Systems, IPTPS, Ithaca NY, USA, pages 24–35, 2005.
[105] Klaus Mochalski and Hendrik Schulze. Internet study 2008/2009. Technical report, Ipoque, 2009.
[106] FBI CSI “Crime and Security Survey 2010”. FBI CSI Report, 2010.
[107] B. Cohen. Incentives build robustness in bittorrent. In Workshop on Economics of Peer-to-Peer systems, volume 6, 2003.
[108] C. E. Perkins, P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers". In Proc. of the conference on Communications, Architectures, Protocols, and Applications, pp. 234-344, August, 1994.
[109] R. Perlman, "Network Layer Protocols with Byzantine Robustness". Ph.D thesis. Department of Electrical Engineering and Computer Science, MIT, August, 1988.
[110] T. Wan, E. Kranakis, P. C. Van Oorschot, "Securing the Destination-Sequenced Distance Vector Routing Protocol (S-DSDV)". In Proceedings of the 6th International Conference on Information and Communications Security, Malaga, Spain.. LNCS vol. 3269, pp.358-374. Springer-Verlag. October, 2004.
[111] Daia F., Wub J. On constructing k-connected k-dominating set in wireless ad hoc and sensor networks. J. Parallel Distrib. Comput., Vol. 66. - pp. 947 – 958, 2006
[112] Nakayama H., Ansari N., Jamalipour A., Kato N. “Fault-resilient sensing in wireless sensor networks”. Computer Communications, Volume 30 Issue 11-12, September, 2007.
[113] Larrea M., Martîn C. et Astrain J. Coordinated Data Aggregation in Wireless Sensor Networks using the Omega Failure Detector. the 3rd ACM international workshop on Performance evaluation of wireless ad hoc, sensor and ubiquitous networks PE-WASUN '06. Terromolinos, Espagne. ACM Press, 2006. - pp. 114 - 122.
[114] L.Hu and D. Evans, "Secure aggregation for wireless networks",Workshop on Security and Assurance in Ad Hoc Networks, January 2003.
[115] M.Bagaa, N. Lasla, A. Ouadjaout and Y.Challal ; "SEDAN : Secure and Efficient protocol for Data Aggregation in wireless sensor Networks", 32nd IEEE Conference on Local Computer Networks (LCN 2007) pp. 1053-1060, Worksohop on Netwok Security, 2007.
[116] K.Wua, D. Dreefa, B. Sunb, and Y. Xiao. Secure data aggregation without persistent cryptographic operations in wireless sensor networks. Ad Hoc Networks, vol. 5, no. 1, pp. 100 - 111, 2006.
[117] Mahimkar A et Rappaport, T.S, SecureDAV : A Secure Data Aggregation and Verification Protocol for Sensor Networks, Global Telecommunications Conference, GLOBECOM, pp. 2175 - 2179 Vol.4, 2004.
[118] Jing Deng, Richard Han and Shivakant Mishra Intrusion-Tolerant Routing for Wireless Sensor Networks. Computer Communications, vol: 29, no. 2, pp.:216-230, 2006.
[119] J. Yin and S. Madria, Secrout : A secure routing protocol for sensor networks, AINA 06 : Proceedings of the 20th International Conference on Advanced Information Networking and Applications (Washington, DC, USA), vol. 1, IEEE Computer Society, 2006, pp. 393-398.
[120] S. Lee and Y. Choi, A secure alternate path routing in sensor networks, Computer Communications, Vol:30, no. 1, pp 153- 165, 2006.
[121] J. Deng, R. Han, and S. Mishra, "Defending against path-based DoS attacks in wireless sensor networks", 3rd ACM workshop on Security of Ad Hoc Sensor Networks (New York, USA), pp.89-96, 2005.
[122] S. Zhu, S. Setia, S. Jajodia, and P. Ning, “Interleaved hop-by-hop authentication against false data injection attacks in sensor networks”, ACM Transactions on Sensor Networks, vol 3, no 3, pp 14, 2007.
[123] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical En-route Filtering of Injected False Data in Sensor Networks”, IEEE INFOCOM'04, Vol. 4, pp. 2446-2457, 2004.
[124] W. Xu, K. Ma, W. Trappe, Y. Zhang. Jamming sensor networks: attack and defense strategies. IEEE.Network. Volume 20, number 3., pp 41-47, May-June 2006.
[125] A. Wood and J. Stankovic. Denial of Service in Sensor Networks. IEEE Computer, Vol(35), N°(2), pp 48-56, October 2002.
[126] D. Liu and P. Ning. Establishing pairwise keys in distributed sensor networks. In ACM CCS ’03, pages 52–61, 2003.

[127] L. Eschenauer and V.D. Gligor. A key-management scheme for distributed sensor networks. In ACM CCS '02, pages 41–47, 2002.
[128] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In IEEE Symposium on Security and Privacy, 2003.
[129] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney. A key management scheme for wireless sensor networks using deployment knowledge. In IEEE INFOCOM'04, pages 586–597, 2004.
[130] C. Castelluccia and A. Spognardi. A Robust Key Predistribution Protocol for Multi-Phase Wireless Sensor Networks. In IEEE Securecom'07, pages 351–360, 2007.
[131] Z. Yu and Y. Guan. A robust group-based key management scheme for wireless sensor networks. In Wireless Communications and Networking Conference, pages 1915–1920. IEEE, 2005.
[132] S. Zhu, S. Setia, and S. Jajodia. Leap: efficient security mechanisms for large-scale distributed sensor networks. In ACM CCS '03, pages 62–72, 2003.
[133] S. A. Camtepe and B. Yener. Combinatorial design of key distribution mechanisms for wireless sensor networks. IEEE/ACM Trans. Netw., 15:346–358, April 2007.
[134] Sushmita Ruj, Amiya Nayak, and Ivan Stojmenovic. Fully secure pairwise and triple key distribution in wireless sensor networks using combinatorial designs. In *IEEE-INFOCOM*, pages 326–330, 2011.
[135] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. Spins: Security protocols for sensor networks. Wireless Networks, 8(5):521–534, 2002.
[136] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar. Spins: security protocols for sensor netowrks. In MOBICOM, pages 189–199, 2001.
[137] National Institute of Standards and Technology. Sacure hash standard. Federal Information Processing Standards Publication, 1995.
[138] http://www.memsic.com.
[139] Ben L. Titzer, Daniel K. Lee, and Jens Palsberg. Avrora: Scalable sensor network simulation with precise timing. In IPSN, 2005.
[140] Brown, J., Du, X., Nygrad, K. : An Efficient Public-Key-based Heterogeneous Sensor Network Key Distribution Scheme. In: IEEE GLOBECOM. Washington, 2007.
[141] Levis, P., Lee, N., Welsh, M., Culler, D. : TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Application. In: ACM SenSys. Los Angeles, 2003.
[142] Du, X., Xiao, Y., Guizani, M.,Chen,H-H.: An effective key management scheme for heterogenous sensor networks. Ad Hoc Networks, Elsevier. 5(1), 24–34 ,Jan. 2007.
[143] Bencheikh, A. and Challal, Y. and Balla, A. and Bouabdallah, A., "Sécurisation du protocole Tiny Diffusion ». Sécurité des Architectures Réseaux et Systèmes d'Information, 2010.
[144] Manamohan Mysore, Moshe Golan, Eric Osterweil, Deborah Estrin , Mohammad Rahimi, «TinyDiffusion in the Extensible Sensing System at the James Reserve», UCLA, 2003.
[145] C. Intanagonwiwat, R. Govindan, D. Estrin, «Directed Diffusion: a Scalable and Robust Communication Paradigm for Sensor Networks», ACM MobiCom 2000, Boston, 2000.
[146] Barabasi A-L, Albert R. Emergence of scaling in random networks. Science, Vol. 286, pp. 509–512, 1999..
[147] W. Lou and Y. Kwon. H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks. IEEE Transactions on Vehicular Technology, 55(4):1320{1330, 2006.
[148] SDAP K. Wua, D. Dreefa, B. Sunb, Y. Xiao, Secure data aggregation without persistent cryptographic operations in wireless sensor networks, Ad Hoc Networks 5 (1) (2006) 100 – 111.
[149] SAWN L. Hu, D. Evans, Secure aggregation for wireless networks, in: Workshop on Security and Assurance in Ad Hoc Networks, 2003.
[150] RSDA H. Alzaid, E. Foo, J. Nieto, Rsda: Reputation-based secure data aggregation in wireless sensor networks, in: International Conference on Parallel and Distributed Computing, Applications and Technologies, 2008, pp. 419 – 424.
[151] SecureDAV A. Mahimkar, T. Rappaport, SecureDAV: A secure data aggregation and verification protocol for sensor networks, in: Proceedings of the IEEE Global Telecommunications Conference, 2004.
[152] CMT C. Castelluccia, E. Mykletun, G. Tsudik, E_cient aggregation of encrypted data in wireless sensor networks, in: Mobile and Ubiquitous Systems: Networking and Services, 2005, pp. 109–117.
[153] ASAP R. Bista, K.-J. Jo, J.-W. Chang, A new approach to secure aggregation of private data in wireless sensor networks, IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009. DASC '09, pp. 394 – 399.

[154] SumAGG E. Mlaih, S. Aly, Secure hop-by-hop aggregation of end-toend concealed data in wireless sensor networks, in: IEEE INFOCOM Workshops, pp. 1 – 6, 2008.
[155] V. Shnayder, M. Hempstead, B. Chen, G. W. Allen, M. Welsh, Simulating the power consumption of large-scale sensor network applications, in: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, pp. 188–200, ACM Press NY, USA, 2004.
[156] Y. Challal, S. Gharout, A. Bouabdallah, H. Bettahar "Adaptive Clustering for scalable key management in Dynamic Group Communications", Int. J. of Security & Networks (Inderscience) vol. 3(2), 2008.
[157] S. Gharout, Y. Challal, A. Bouabdallah, "Scalable Delay-constrained Multicast Group Key Management", Int. J. of Network Security, Vol. 7(2), p. 153-167, Sep. 2008.
[158] H. Ragab Hassan, A. Bouabdallah, H. Bettahar, Y. Challal; "Key Management for Content Access Control in a Hierarchy", Computer Networks (Elsevier); Vol. 51, pp. 3197-3219, 2007.
[159] Y. Challal, A. Bouabdallah, Y. Hinard; "RLH : Receiver driven Layered Hash-chaining for multicast data origin authentication", Computer Communications (Elseviers), vol. 28(7), pp.: 726-740, 2005.
[160] Y. Challal, A. Bouabdallah, H. Bettahar; "H2A: Hybrid Hash-chaining scheme for Adaptive multicast source authentication of media-streaming", Computers and Security (Elsevier), Vol. 24(1), pp. 57:68, 2005.
[161] Y. Challal, H. Bettahar, A. Bouabdallah; "SAKM: a Scalable and Adaptive Key Management Approach for Multicast Communications", ACM-SIGCOMM Computer Communications Review, Volume (34), number (2), pages: 55-70, April 2004.
[162] Y. Law, L. Van Hoesel, J. Doumen, P. Hartel, P. Havinga. Energy-Efficient Link-Layer Jamming Attacks against Three Wireless Sensor Network MAC Protocols. In Proceedings of ACM SASN, Alexandria, Virginia. November 2005.
[163] W. Xu, K. Ma, W. Trappe, Y. Zhang. Jamming sensor networks: attack and defense strategies. IEEE.Network. Volume 20, number 3. pp 41-47, May-June 2006.
[164] European Telecommunications Standards Institute (ETSI), "Machine- to- Machine communications (M2M) : Functional architecture", Draft ETSI TS 102 690 V0.10.3, 2011.
[165] S. Deering, R. Hinden, « Internet Protocol, Version 6 (IPv6) Specification », IETF RFC2460, 1998.
[166] DECAGON, http://www.decagon.com
[167] Harry Stockman, « Communication by Means of Reflected Power », Proceedings of the IRE, pp. 1196-1204, October 1948
[168] NFC Forum, http://www.nfc-forum.org