N° d'ordre : 4967

THÈSE

PRÉSENTÉE À

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET D'INFORMATIQUE

Par **Jonathan Ouoba**

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : INFORMATIQUE

Communications multi-niveaux sécurisées dans une flotte de terminaux mobiles

---

Soutenue le : 11 décembre 2013

Après avis des rapporteurs :

Julien Bourgeois	Professeur
Keith Mayes	Professeur

Devant la commission d'examen composée de :

Julien Bourgeois	Professeur	Rapporteur
Serge Chaumette	Professeur	Directeur de thèse
Olivier Ly	Maître de Conférences	Examinateur
Keith Mayes	Professeur	Rapporteur
Tuomo Tuikka	Directeur de Recherche	Examinateur

– 2013 –

Résumé : Les matériels mobiles actuels, et les téléphones mobiles en particulier, sont équipés de différentes technologies sans fil qui augmentent et diversifient leurs capacités de communication. L'utilisation combinée et efficace de ces technologies offre des possibilités variées et accrues en termes de services et d'applications. Néanmoins elle requiert la réalisation d'analyses fines en matières de sécurité et de choix du mode de communication à utiliser en fonction de critères dépendant du contexte : coût énergétique, coût financier, préférences des entités impliquées, préservation de la vie privée, etc.
Cette problématique est apparue comme une question clé au sein du projet Smart Urban Spaces dans le cadre duquel s'inscrit cette thèse. Notre contribution à ce projet est la création d'applications collaboratives qui utilisent de façon appropriée la gamme des technologies sans fil disponibles sur les matériels considérés. En d'autres termes, on cherche à utiliser les moyens de transmission les plus appropriés (au sens des critères indiqués plus haut) que deux ou plusieurs équipements mobiles peuvent utiliser pour réaliser leurs échanges, qui plus est, sans que cela ne nécessite de connaître leurs positions respectives. La transparence de la localisation des cibles devient ainsi une règle.
On peut synthétiser la question centrale que nous avons choisie d'étudier de la manière suivante : comment faire communiquer un ensemble de terminaux mobiles (des téléphones portables en particulier) de façon sécurisée en utilisant la technologie la plus adaptée en fonction du contexte ? Notre objectif est de proposer une réponse à cette question en définissant une plate-forme multi-niveaux prenant en compte les différentes technologies disponibles sur les équipements considérés. Il s'agit en particulier d'identifier l'ensemble des éléments à prendre en compte dans la conception de la plate-forme, de les modéliser, de développer des applications de référence et de valider la pertinence des solutions proposées par des tests, ainsi que des évaluations qualitatives et quantitatives.

Abstract : Current mobile devices, and mobile phones in particular, are equipped with different wireless technologies that increase and diversify their communication capabilities. The combined and effective use of these technologies offers various opportunities in terms of services and applications. However, it requires detailed analysis in terms of security and choice of the communication mean to use according to context-dependent criteria : energy costs, financial costs, preferences of the involved entities, privacy issues, etc.
This problem has emerged as a key issue in the Smart Urban Spaces project in which this thesis was carried out. Our contribution to this project is the creation of collaborative applications adequately using the available wireless technologies on the considered equipments. In other words, we try to use the most appropriate communication mean (according to the criteria listed above) that two or more mobile devices can use to perform exchanges (without considering their respective positions). Then, the transparency of targets localization becomes a rule.
We can synthesize the central question that we have chosen to study in the following manner : how to allow a set of mobile terminals (mobile phones in particular) to securely communicate using the most appropriate technology depending on the context ? Our goal is to answer this question by defining a multilevel platform taking into account the different technologies available on the considered equipments. It is necessaty to identify the elements to consider in the design of the platform, to model them, to develop reference applications and to validate the relevance of the proposed solutions with qualitative and quantitative evaluations.

Remerciements

Je tiens tout d'abord à remercier les membres du jury :

- Julien Bourgeois pour avoir accepté de présider ce jury et dont la relecture minutieuse ainsi que les conseils en tant que rapporteur ont été particulièrement utiles
- Keith Mayes dont les commentaires et les propositions m'ont permis d'améliorer la qualité et la cohérence du manuscrit tout en identifiant de nouvelles perspectives pour mes travaux
- Tuomo Tuikka avec qui j'ai eu des discussions très enrichissantes concernant mon manuscrit et qui m'accueille dans son équipe de recherche
- Olivier Ly qui avait déjà été relecteur de mon mémoire de master et dont les remarques m'ont permis d'envisager de nouvelles orientations pour mes travaux

Je souhaite également remercier tout particulièrement Serge Chaumette qui m'a donné l'opportunité de réaliser ces travaux de thèse. Sa disponibilité, ses conseils, ses idées et son attention m'ont fourni le cadre indispensable à la réussite de ce projet. Je n'oublierai jamais les (bons) moments que nous avons passés dans le montage et la conduite du projet Smart Urban Spaces.

Je pense aussi aux membres de la CVT (anciens et nouveaux) avec qui j'ai eu l'occasion de travailler au quotidien. Merci de m'avoir accepté avec mon caractère si particulier. Je peux le dire sans hésiter, la CVT est le meilleur endroit du LaBRI où effectuer des travaux de thèse.

Mes pensées vont tout naturellement vers mes amis de l'AB Bègles. Leur affection, leurs attentions et leurs encouragements m'ont porté durant ces années. Je ne peux tous les citer, mais je pense à chacun d'entre eux et en particulier à Serge et Rosy, Célestin et Rosalie, Michel et Monique ainsi qu'à leurs familles respectives.

Je termine en remerciant ma famille. Que dire ? Sans chacune de ces personnes, je ne serais tout simplement pas allé au bout de ce projet. Toujours présente dans les moments de doute et de découragement, elle m'a soutenu de façon admirable. Mon père qui est un modèle et grâce à qui j'ai eu le goût de la thèse, ma mère qui a toujours su trouver les mots pour m'encourager quelles que soient les circonstances, ma sœur et mon frère qui m'ont supporté tout en étant attentifs à mes besoins. Ma tante Flore, Serge et Betty, Tonton Joseph et sa famille, les Passi, Papy et Mamie Bassoka. Des noms et des personnes qui représentent tant de choses pour moi. Je pense à de nombreuses autres personnes et ces personnes savent combien elles comptent pour moi. Un seul mot exprime toute la reconnaissance que j'ai : merci. Il y a tant de choses que je ne peux exprimer, j'ai tout simplement la plus belle famille qui puisse exister.

Table des matières

Introduction

Les services mobiles permettent à des équipements eux-mêmes mobiles, et plus particulièrement aux *smartphones*, d'accéder à des ressources numériques de différentes natures. Ces équipements, en raison de leur utilisation en situation de mobilité, sont dotés d'une ou plusieurs technologies sans fil afin de pouvoir communiquer avec leur environnement. Les technologies sans fil dont il est question ici ont des portées qui vont de quelques dizaines de centimètres à plusieurs kilomètres (définissant ainsi une forme de hiérarchie entre les technologies).
La question d'une utilisation combinée et efficace de ces technologies se pose dans le cadre du développement de services mobiles innovants à destination des citoyens des zones urbaines. En effet, les collectivités locales ont vocation à proposer des services visant à faciliter le quotidien de leurs citoyens ; le téléphone étant l'équipement mobile le plus répandu, il est naturel d'utiliser ses capacités technologiques afin de proposer de tels services.
En prenant en compte ces considérations, nous avons choisi, dans les travaux que nous avons menés, de proposer une plate-forme multi-niveaux (en référence à la hiérarchie définie par la portée des technologies sans fil disponibles) pour téléphones mobiles. Cette plate-forme a pour objectif de permettre à un ensemble de terminaux mobiles de communiquer entre eux de façon sécurisée en utilisant la technologie sans fil la plus adaptée en fonction du contexte et suivant les contraintes définies par le système. Ces contraintes concernent tout particulièrement la minimisation des différents coûts (en termes financiers ou de consommation en énergie) résultant des communications effectuées.
Ce document comporte quatre chapitres qui décrivent les différents éléments théoriques et pratiques que nous avons considérés dans la spécification, le développement et l'évaluation du système multi-niveaux proposé ainsi qu'une conclusion qui présente les perspectives liées à nos travaux.

Chapitre 1. Le projet Smart Urban Spaces et les services mobiles
Les travaux que nous avons effectués se sont déroulés au sein du projet Européen Smart Urban Spaces qui avait pour objectif de définir de nouveaux services numériques (pour téléphones mobiles) basés sur les technologies mobiles les plus récentes. Il nous est donc apparu pertinent, après avoir défini plus précisément les services mobiles auxquels nous nous intéressons et leur évolution en fonction des développements technologiques, de présenter en détails le projet SUS ainsi que nos contributions en termes d'implémentation et de déploiement.

Chapitre 2. Les MANets et les premiers éléments théoriques de nos travaux
Les MANets (Mobile Ad hoc Networks) constituent l'environnement cible de la plate-forme

multi-niveaux dans lequel les téléphones mobiles doivent communiquer. Les MANets sont constitués d'un ensemble de dispositifs mobiles (appelés nœuds) capables de communiquer les uns avec les autres via des technologies sans fil et sans infrastructure préexistante. Il nous a donc semblé important de présenter les éléments principaux de caractérisation des MANets et en particulier : la bande passante limitée et variable des technologies sans fil utilisées, les contraintes énergétiques des dispositifs mobiles et la difficulté à mettre en place une sécurisation physique des communications. Après avoir choisi de considérer l'approche opportuniste (communications en mode *peer-to-peer* entre nœuds au gré de leurs rencontres) à partir de l'analyse que nous avons menée des principaux axes de recherche dans le domaine des MANets, nous avons proposé une approche et une modélisation du problème dans laquelle chaque nœud de la plate-forme multi-niveaux possède des caractéristiques qui lui sont propres (capacités technologiques par exemple). L'ensemble des ces caractéristiques définit ce que nous appelons le profil du nœud.

Chapitre 3. La plate-forme multi-niveaux
L'objet de notre plate-forme est le partage d'informations et plus précisément le fait d'offrir les moyens à chaque entité de rechercher des informations en fonction de ses besoins ou de partager ses propres informations. Nous avons donc proposé et validé des solutions pour les cinq opérations principales que nous avons identifiées dans notre contexte pour la plate-forme multi-niveaux, à savoir : la publication de profil (pour permettre à un nœud de publier son profil dans son voisinage) ; la spécification d'un ensemble de cibles (pour permettre à un nœud de déterminer les entités susceptibles de répondre à ses besoins) ; le choix de la technologie la plus adaptée pour communiquer entre deux nœuds ; l'échange d'informations privées en cas de rencontre physique entre deux nœuds ainsi que la sécurisation des communications et le contrôle de l'anonymat. Ces choix ont conduit à définir une architecture générale qui supporte le fonctionnement de la plate-forme multi-niveaux.

Chapitre 4. Implémentation d'un prototype
A partir des éléments proposés pour l'architecture multi-niveaux, nous avons implémenté une application mobile (pour téléphone) à déployer sur chaque nœud du système et qui utilise le NFC, le Bluetooth, le Wi-Fi direct et le GSM comme technologies sans fil. Cette application, développée pour Android (système d'exploitation pour terminaux mobiles), a fait l'objet de tests, notamment concernant l'opération de publication de profil et les aspects liés à la consommation énergétique, qui ont permis de montrer l'intérêt de la plate-forme multi-niveaux dans un environnement réaliste.

Première partie

Cadre des travaux et premières réalisations

Chapitre 1

Contexte opérationnel

Sommaire

Les travaux que nous présentons se sont déroulés au sein du projet européen Smart Urban Spaces (SUS) [web30]. Ce projet avait pour objectif de proposer un ensemble de services pour téléphones portables basés sur les technologies les plus actuelles dont ces équipements sont dotés et ce dans le but d'améliorer la vie quotidienne des citoyens des villes européennes impliquées. SUS avait également pour ambition de susciter la création d'un réseau de villes "numériques" (e-cities) interconnectées qui utilisent les mêmes standards technologiques pour l'ensemble des services qu'elles mettent à la disposition de leurs citoyens respectifs. Le développement, le déploiement et l'évaluation de services, qui peuvent être appelés *services mobiles* en raison du caractère mobile des équipements sur lesquels ils s'exécutent, est au cœur des préoccupations des partenaires de SUS. Par conséquent, avant de présenter plus en détails le consortium SUS et ses réalisations, il est pertinent de s'intéresser à la définition des services mobiles ainsi qu'à leur évolution liée aux nouveaux équipements mobiles disponibles.

1.1 Services mobiles

1.1.1 Présentation et enjeux

Les services mobiles fournissent le cadre à partir duquel il est possible d'avoir accès à des ressources en utilisant des équipements dits *mobiles* et leurs capacités. Le terme *mobiles*, dans ce cas, fait référence à des équipements qui peuvent circuler/se déplacer dans l'espace en fonction du temps (être à un point A à un instant t_n donné puis se déplacer à un point B à l'instant t_{n+1}).

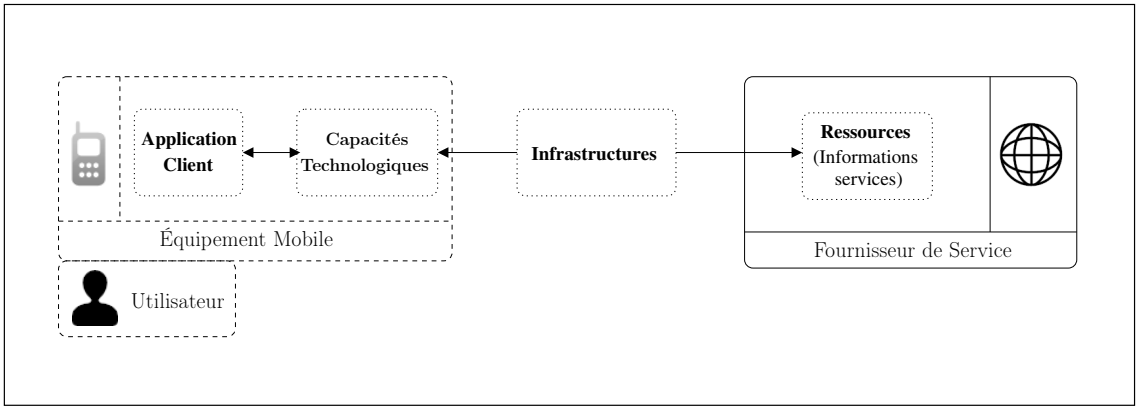


FIGURE 1.1 – Environnement de déploiement des services mobiles.

Le schéma de la figure 1.1 présente la conception que nous avons de l'ensemble des éléments nécessaires à la mise à disposition de services mobiles. Ce schéma nous conduit à définir les éléments suivants :

- les **ressources** qui représentent les informations à mettre à la disposition des utilisateurs des services. Ces informations, qui ne sont pas directement ou nécessairement disponibles (stockées) sur les terminaux mobiles considérés, doivent pouvoir être accessibles (par ces terminaux) à travers les infrastructures appropriées (voir ci-dessous).
- les **capacités technologiques** (ou techniques) qui représentent les technologies dont sont équipés les terminaux et qui les rendent capables, même en déplacement, d'avoir accès aux informations dont ils ont besoin. Dans le contexte de services mobiles, ces moyens sont principalement des technologies de communication sans fil.
- l'**application client** qui représente le logiciel, déployé sur l'équipement mobile, permettant d'exploiter les capacités technologiques disponibles pour accéder aux ressources.
- les **fournisseurs de services** qui représentent les entités qui rendent des ressources accessibles en utilisant les capacités technologiques des terminaux mobiles considérés. Les fournisseurs de services peuvent également être les entités qui diffusent (i.e. rendent disponible pour les terminaux mobiles des utilisateurs) le service mobile associé aux ressources.
- les **infrastructures** qui représentent les éléments matériels permettant d'établir le lien de communication (en cas de nécessité) entre les ressources disponibles (proposées par les fournisseurs de services) et les équipements mobiles des utilisateurs.

En d'autres termes, les services mobiles permettent l'utilisation, en situation de mobilité, des capacités technologiques des appareils mobiles (via une application client) pour accéder à un ensemble de ressources spécifiques qui dépendent du type de service proposé. L'implémentation des services mobiles repose donc essentiellement sur la prise en compte des capacités technologiques et des caractéristiques des appareils mobiles considérés. Ce point de vue est d'ailleurs confirmé par la définition que donne l'OCDE [1] des services mobiles, définition où l'accent est mis sur les capacités de communication des équipements. Pour l'OCDE, les services mobiles sont des services de radiocommunications entre navires, aéronefs, véhicules routiers et stations de terminaux portables pour une utilisation en déplacement ou entre ces stations et des points fixes sur la terre [web25].

Afin de procéder à une analyse plus précise, nous limitons le domaine d'étude des services mobiles au cas des téléphones mobiles. Cela se justifie par le fait que le téléphone mobile est devenu l'équipement mobile par excellence en raison de sa pénétration au sein de la population. En effet, selon les statistiques de l'Observatoire Européen de l'Industrie Mobile [37], en 2011 le taux de pénétration du téléphone mobile était de 128% en Europe avec plus de 654 millions d'abonnements individuels. De plus (pour Mobile Statistics [web29]) au premier trimestre 2012, le nombre d'applications mobiles disponibles à destination des smartphones, qui sont les téléphones mobiles les plus évolués en termes technologiques, ne cesse d'augmenter et atteint environ 500 000 unités sur le Google Play Store et plus de 650 000 unités sur l'App Store avec les plates-formes les plus populaires que sont respectivement Android et iOS. Il est à noter que les applications mobiles pour smartphones représentent un type particulier de services mobiles comme cela sera expliqué plus loin. Le choix d'étudier particulièrement les services mobiles dédiés aux téléphones mobiles est donc pertinent.

Au regard de tout ce qui précède, l'étude des services mobiles orientée vers les téléphones portables passe par l'analyse des technologies dont ils font usage pour accéder aux ressources disponibles. Les progrès technologiques, essentiellement dans le domaine de la miniaturisation électronique, ont permis de doter les téléphones portables de fonctionnalités toujours plus évoluées. Ainsi, la transition s'est faite en une vingtaine d'années entre les premiers combinés mobiles commerciaux du début des années 90 avec lesquels il était uniquement possible d'effectuer des appels vocaux et les tous derniers smartphones à écrans tactiles proposant, par exemple, des services de reconnaissance vocale. Ces innovations ont pour objectif d'accroître les possibilités d'interactions des téléphones avec leur environnement. En ciblant plus principalement les smartphones les plus récents et en considérant que les fonctions de base sont assurées, les dernières évolutions des capacités technologiques des téléphones mobiles nous ont conduit à les distinguer selon deux critères, à savoir, leurs interfaces réseaux et leurs capteurs [2]. Concernant les interfaces réseaux, elles représentent les moyens qui rendent l'appareil capable d'entrer en contact avec des entités extérieures, notamment à travers les technologies de communication sans fil. Les capteurs, quant à eux, concernent les outils qui permettent à l'équipement d'avoir connaissance du milieu qui l'entoure ; il s'agit entre autres de l'appareil photo/caméra, du gyroscope ou encore de l'accéléromètre. Le tableau 1.1 présente l'exemple des spécifications du Galaxy S3 [web15] selon les deux catégories retenues.

1. Organisation de Coopération et de Développement Économiques - http ://www.oecd.org/

2. Les fonctions de base qui ont elles aussi bénéficié des progrès techniques correspondent aux éléments d'affichage, de saisie et de puissance de calcul de l'équipement considéré.

Interfaces réseaux	**Capteurs**
- GSM (Global System for Mobile Communications) - GPRS (General Packet Radio Service) - EDGE (Enhanced Data rates for GSM Evolution) - HSPA (High Speed Packet Access) - UMTS (Universal Mobile Telecommunications System) - LTE (Long Term Evolution) - NFC (Near Field Communication) - Bluetooth - Wi-Fi	- Accéléromètre - Caméra (analyse faciale) - Détecteur de proximité - GPS - Gyroscope - Microphone (analyse vocale)

TABLE 1.1 – Spécifications techniques du Galaxy S3.

De par leur nature, les capteurs constituent principalement des outils permettant aux applications de prendre en compte le contexte d'utilisation des téléphones. En effet, les capteurs sont des pourvoyeurs d'informations diverses. Par exemple, la reconnaissance vocale à l'aide du microphone permet à un utilisateur de transformer un message oral en données textuelles, données qui pourront par la suite être utilisées par un service mobile. Nous choisissons, pour catégoriser les services mobiles en fonction des capacités technologiques des téléphones mobiles utilisés, de mettre l'accent sur les interfaces réseaux.

Dans la partie *interfaces réseaux* du tableau 1.1, les six premiers éléments mentionnés (GSM, GPRS, EDGE, HSPA, UMTS et LTE) sont des technologies qui permettent de se connecter à des réseaux d'opérateurs de téléphonie mobile pour pouvoir émettre des appels vocaux, expédier des messages textuels ou encore, dans certains cas, accéder à Internet. Sous réserve d'être situé dans la zone couverte par les infrastructures de l'opérateur mobile concerné ou de ses partenaires, un téléphone portable peut théoriquement, par le moyen de ces technologies, utiliser les services offerts quelle que soit sa position géographique. Ces interfaces réseaux fournissent des solutions de communication globales dans le sens où ce sont des opérations qui peuvent être initiées à partir d'un endroit quelconque et être à destination de n'importe quel autre endroit. Quant aux trois autres interfaces (NFC, Bluetooth et Wi-Fi), ce sont des technologies de radiocommunication dont la portée varie, en théorie, entre une dizaine de centimètres environ pour le NFC et plusieurs centaines de mètres pour le Wi-Fi. Ces trois interfaces fournissent donc des solutions de communication que nous appelons locales en raison de leurs portées limitées. En généralisant, les interfaces réseaux peuvent donc être réparties en deux groupes ce qui conduit à définir deux catégories de services mobiles :

– les **services mobiles locaux** qui font usage de technologies de communication de portée locale. L'échange d'images via Bluetooth et la synchronisation en Wi-Fi du contenu d'un téléphone portable et d'un ordinateur sont des exemples de services locaux. Ces services permettent d'accéder à des ressources qui se situent dans un espace appelé **espace local**.
– les **services mobiles globaux** qui font usage de technologies de communication de portée globale. L'envoi/réception de SMS et la consultation de courriers électroniques à travers le réseau d'un opérateur mobile sont, par exemple, des services de type global. Ces services permettent d'accéder à des ressources qui se situent dans un

espace appelé **espace global**.

Certains services mobiles peuvent à la fois faire usage de technologies de portée locale et de technologies de portée globale. Dans ce cas de figure, ces services sont considérés comme des services mobiles globaux du fait que la portée des technologies dites globales englobe celle des technologies dites locales (qui peut le plus peut le moins). La figure 1.2 résume le fonctionnement des deux types de services mobiles. *Téléphone Mobile 1* embarque deux applications clients à savoir *Application Locale* et *Application Globale* tandis que deux fournisseurs de services proposent des ressources. Pour accéder aux ressources proposées, *Téléphone Mobile 1* lance une requête en utilisant les technologies dont il équipé. En fonction du type de service et de l'endroit où le mobile est localisé, cette requête est reçue par le fournisseur qui la traite afin d'effectuer les opérations demandées. Dans l'exemple décrit par la figure 1.2, lorsque que *Téléphone Mobile 1* se situe au *point A*, il peut accéder aux ressources de *Fournisseur de Service 1* et de *Fournisseur de Service 2* en utilisant respectivement *Application Locale* et *Application Globale*. Par contre lorsqu'il se déplace au *point B* ce sont uniquement les ressources de *Fournisseur de Service 2* qui lui sont accessibles à travers *Application Globale*. *Point B* se situe dans une zone où les portées limitées des technologies dont se sert *Application Locale* ne permettent pas d'avoir accès à l'*Espace local*. L'accès aux ressources proposées dépend donc du type de service et de la position géographique du téléphone portable qui initie les opérations. Il serait par exemple impossible à deux téléphones se situant à 500 mètres l'un de l'autre d'échanger des images par Bluetooth, en revanche ils pourraient interagir par l'intermédiaire de SMS.

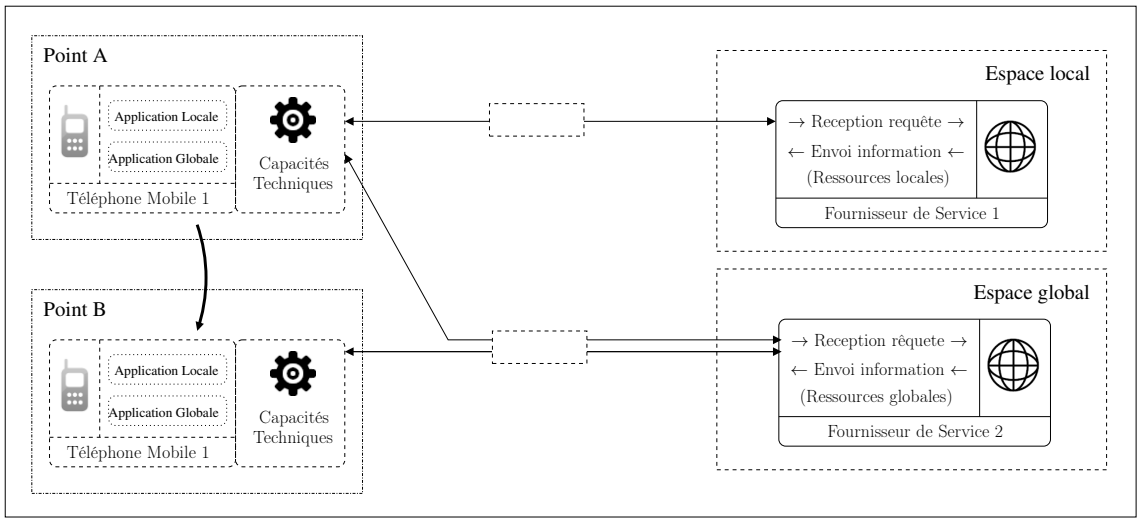


Figure 1.2 – Exemple de fonctionnement des services mobiles.

Un autre point important de caractérisation des services mobiles est l'application mobile. Elle constitue une des formes les plus répandues d'application client pour accéder à des ressources proposées par un fournisseur de service. Une application mobile, dans notre contexte, est un programme (dédié) exécuté sur les téléphones mobiles qui rend possible des communications avec un fournisseur de service. Le système d'exploitation dont est équipé le téléphone ainsi que le modèle précis définissent les contraintes à considérer lors de la conception de l'application. De plus, une application mobile est développée à l'aide

	Plateforme	**Système d'exploitation**
Amazon	Appstore	Android
Apple	App Store	iOS
Google	Play Store	Android
Microsoft	Marketplace	Windows Mobile
Nokia	Nokia Store	Meego, Symbian
RIM	BlackBerry App World	BlackBerry OS
Samsung	Samsung Apps	Android, Bada

TABLE 1.2 – Diffusion des applications mobiles.

d'outils de programmation spécifiques à chaque système d'exploitation ciblé. Ces outils de programmation fournissent un ensemble d'APIs (Application Programming Interfaces) pour manipuler les ressources internes du téléphone et les données issues des différents capteurs. Les applications mobiles qui peuvent être gratuites ou payantes sont de catégories variées allant des outils de localisation à des utilitaires de consultation de courriers électroniques en passant par des services d'informations météorologiques. Le circuit de diffusion privilégié des applications mobiles passe par des boutiques dématérialisées appelées *Stores* à partir desquelles il est possible, en se connectant à Internet, de télécharger et d'installer des programmes compatibles avec l'environnement technique du mobile cible. Le modèle a été initié par Apple qui a créé son *Store* sous le nom d'*App Store* en 2008. Aujourd'hui, de nombreux acteurs du milieu des technologies de l'information et de la communication ont investi pour proposer des plates-formes de diffusion d'applications mobiles. Le tableau 1.2 donne un aperçu des principales plates-formes de diffusion disponibles.

En l'espace de 20 ans, l'industrie qui s'est développée autour des services mobiles a atteint une taille plus grande que celle de l'industrie pharmaceutique [37]. Le développement de l'industrie des services mobiles se prolonge, avec le déploiement de nouvelles technologies de communication comme la LTE (Long Term Evolution) [96], pour proposer des services toujours plus innovants. Dans ce contexte, l'enjeu principal autour des services mobiles réside dans la manière dont les utilisateurs s'approprieront ces services. En effet, certains d'entre eux peuvent présenter de l'intérêt sans pour autant être totalement adaptés à l'environnement socio-économique des utilisateurs. De nombreuses initiatives d'autorités publiques ont vu le jour pour tenter d'offrir un ensemble de services visant à améliorer, à l'aide des technologies les plus modernes, la vie quotidienne des citoyens. Le concept de *smart cities*, villes intelligentes en français, a ainsi émergé.

1.1.2 *Smart cities*

Le terme *smart cities* fait référence aux villes qui ont décidé d'investir dans les technologies de l'information et de la communication dans le but de proposer des services innovants (en collaboration avec des fournisseurs de services) qui sont à même de faciliter la vie quotidienne de leurs citoyens. Il est à noter que la description des *smart cities* peut également prendre en compte les aspects économiques, environnementaux, de développement durable et de gouvernance [90]. Toutefois, dans notre contexte, nous limitons le cadre de définition aux considérations technologiques. Les termes *digital cities* et *intelligent cities* sont également utilisés. Au sein des *smart cities*, les infrastructures de communication servent à

améliorer le fonctionnement des systèmes intégrés à l'environnement urbain des citoyens. Ces systèmes concernent les domaines du transport, de l'éducation, du commerce, de la culture ou de l'administration. Du fait que les infrastructures de communication utilisées ont généralement une portée qui est au moins à l'échelle de la ville, les services déployés dans ce cadre sont généralement de type global (comme nous l'avons défini section 1.1 page 6). La figure 1.3 présente des exemples d'interactions entre citoyens et fournisseurs de services dans les différents domaines mentionnés.

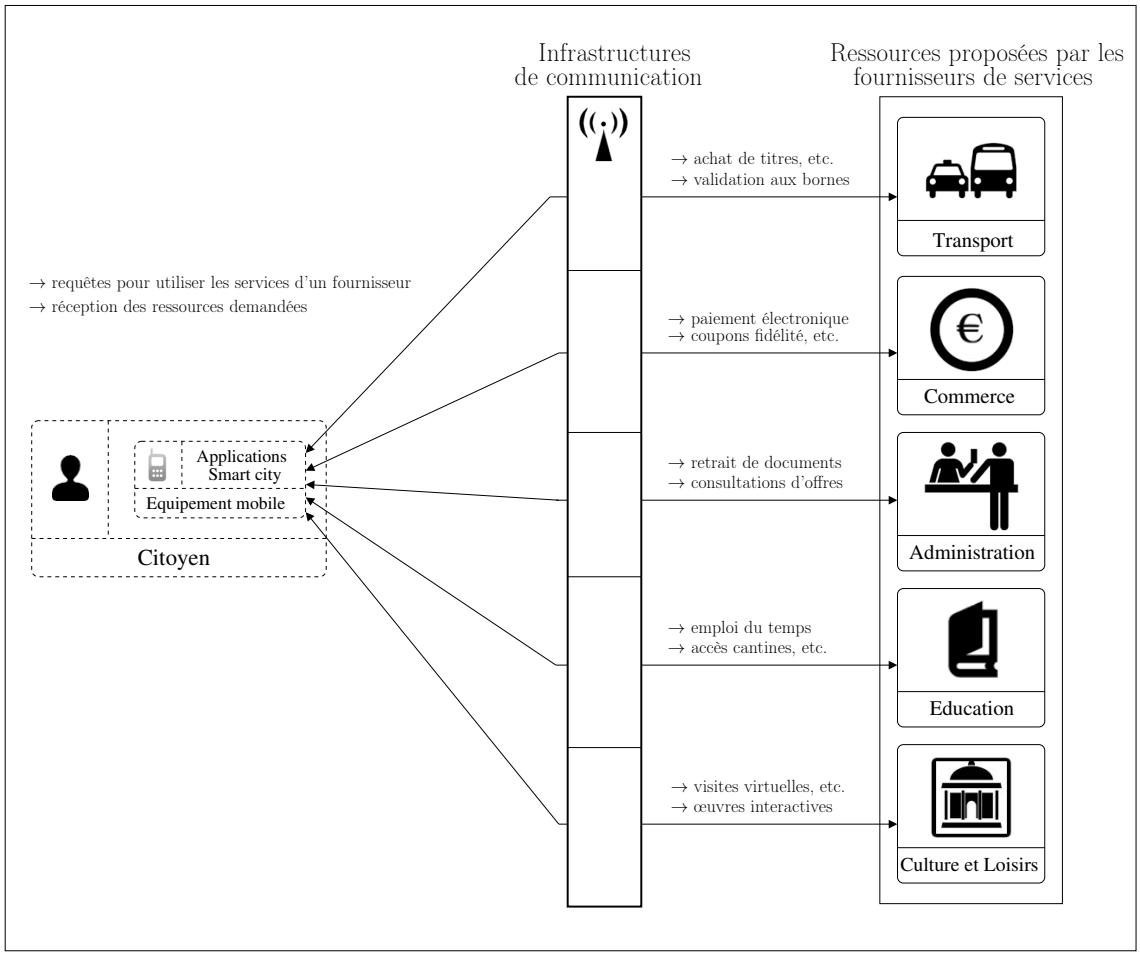


Figure 1.3 – Exemple d'interactions dans une smart city.

Dans une *smart city*, un citoyen pourrait utiliser un équipement mobile pour accéder à la cantine de son lieu de travail ou à la piscine municipale. Il pourrait également utiliser le même équipement mobile pour payer des titres de transport en commun tout en visualisant les horaires de passage actualisés en temps réel. Les services offerts par les *smart cities* ne sont pas exclusivement orientés vers les services mobiles, mais la mobilité étant un élément essentiel du paysage urbain, les terminaux mobiles et plus particulièrement les téléphones mobiles (ainsi que leurs propriétaires) sont au cœur de l'architecture qui est généralement mise en place (figure 1.3). A ce titre, plusieurs projets ont été initiés afin d'utiliser les technologies les plus récentes en matière de téléphonie mobile pour créer des espaces urbains

dits intelligents s'articulant autour d'un ensemble de services mobiles. Ces services mobiles ont pour objectif de simplifier les interactions (de la vie quotidienne) qui s'opèrent de façon régulière dans l'environnement urbain des citoyens. Les exemples suivants présentent un échantillon représentatif de projets qui ont été engagés dans quelques villes européennes.

1.1.2.1 Nice, France

Le projet **Cityzi** [web8][web9] a été lancé au mois de mai 2010 dans la ville de **Nice** en France. Ce projet a pour objectif de proposer un ensemble de services mobiles, autour de la technologie NFC (Near Field Communication), afin de permettre aux citoyens de réaliser de façon simple et à l'aide de leurs téléphones portables les opérations de la vie quotidienne [100]. Le slogan publicitaire du projet est d'ailleurs "Cityzi vous simplifie la ville". Les origines du projet se trouvent dans la création en 2008 du Forum des services mobiles sans contact [web13] par le gouvernement français pour promouvoir l'utilisation de la technologie NFC. Par la suite, certains opérateurs de télécommunication ont constitué l'Association Française du Sans Contact Mobile [web1] (AFSCM) qui a permis de regrouper les acteurs indispensables au déploiement de services mobiles compatibles avec la technologie NFC. Ces initiatives ont conduit au lancement de Cityzi. Au niveau pratique, la technologie NFC est une technologie sans fil qui autorise des communications de très courte portée (10 centimètres environ) entre deux équipements compatibles. Les opérateurs mobiles agréés proposent une gamme de portables NFC avec lesquels il est possible d'avoir accès, à travers une application mobile dédiée, aux ressources proposées dans le cadre de l'initiative Cityzi. Cette application mobile sert de point d'entrée pour souscrire aux différents ressources disponibles. A Nice, Cityzi rassemble des partenaires du milieu des télécommunications, des transports, de la banque, de l'industrie et du commerce, dans le but de présenter des solutions prenant en compte les aspects les plus importants du quotidien des citoyens. Ainsi, l'offre de services comprend des applications mobiles pour le transport urbain, le paiement, la gestion des avantages fidélité. Les utilisateurs peuvent, s'ils le souhaitent, acheter des titres de transport et les valider sur les bornes prévues à cet effet à l'aide de leurs téléphones portables ou encore régler des achats chez les commerçants équipés de lecteurs NFC.

FIGURE 1.4 – Signalétique pour les tags NFC labellisés Cityzi.
source : http://www.cityzi.fr/

Des tags NFC avec la signalétique Cityzi (figure 1.4) sont également disséminés dans l'espace urbain de Nice. Les tags sont généralement de petites pièces en matière plastique qui portent des circuits électroniques qui contiennent des données. Les téléphones mobiles compatibles, en étant approchés des tags, peuvent lire les données qui y sont inscrites. Dans la plupart des cas, les tags contiennent des informations qui permettent d'indiquer au téléphone mobile considéré une ou plusieurs actions à déclencher. Le système de tags permet, par exemple, d'offrir un service d'informations pratiques où il suffit d'approcher le téléphone du tag approprié pour lancer l'affichage de propositions d'emplois et de stages ou lancer une recherche sur Internet pour obtenir davantage de détails concernant une œuvre exposée dans un musée. Les actions susceptibles d'être déclenchées par les tags dépendent des capacités technologiques du téléphone mobile qui les lit. La ville de Strasbourg a rejoint le projet en octobre 2011 et des communautés urbaines comme Caen ou Bordeaux proposent actuellement quelques services labellisés Cityzi. Fin juin 2012, plus d'un million d'abonnés utilisaient des téléphones mobiles compatibles Cityzi. De façon pratique, les téléphones mobiles compatibles Cityzi sont des appareils (équipés de la technologie NFC) sur lesquels les opérateurs mobiles partenaires de l'initiative Cityzi ont pré-installé (ou permettent l'installation) d'applications mobiles spécifiques (achat de titres de transport, paiement, etc.)

1.1.2.2 Caen, France

En plus de services labellisés Cityzi, la ville de **Caen** a mis en place, avec la collaboration de quelques partenaires, un ensemble d'outils mobiles à l'intention de ses habitants [web5]. Les services disponibles se basent essentiellement sur les technologies NFC et QR codes disponibles sur certains téléphones portables. Les QR (Quick Response) codes sont des types de codes barres bi-dimensionnels graphiquement représentés sous forme d'un ensemble de carrés noirs sur fond blanc encodant des données. Concrètement, un appareil compatible capture une image du QR code qui lui est présenté grâce à son appareil photo numérique pour ensuite l'analyser, extraire l'information codée et réaliser l'opération correspondant aux données décodées. Tout comme avec la technologie NFC et les tags, les actions qui sont déclenchées par les QR codes dépendent des capacités du téléphone mobile qui les lit.

Caen est une ville pionnière dans l'utilisation de certaines technologies mobiles et plus particulièrement du NFC. En effet, en 2005 Caen a été la première ville au monde à proposer l'emploi de téléphones NFC pour effectuer des paiements électroniques. Plus tard en 2006, le projet "Payez Mobile" qui a réuni six grandes banques et quatre opérateurs de téléphonie mobile a permis de mettre en place un système pilote pour régler des achats avec un téléphone portable dans plus de 160 commerces de la ville. Ces initiatives ont été rendues possibles grâce au pôle de compétitivité TES (Transactions Électroniques Sécurisées) labellisé en 2005, qui regroupe une centaine d'acteurs majeurs dans le domaine du paiement électronique [web27], et qui a fait de Caen une sorte de laboratoire à ciel ouvert. Aujourd'hui, en tant que *smart city* technologique, Caen propose à ses habitants et aux touristes de passage des services pour le transport, le tourisme, le sport, et la culture.

Concernant le transport, tous les arrêts de bus et de tram de la ville sont dotés de tags NFC et de QR codes qui permettent aux usagers d'être informés en temps réel sur les temps d'attente et sur l'état du réseau (figure 1.5). Les touristes, de leur côté, peuvent

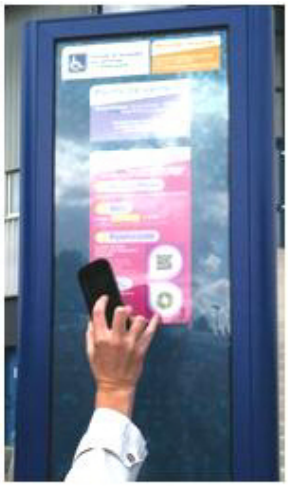


FIGURE 1.5 – Informations en temps réel aux arrêts de bus.
source : http://www.caen.fr/Economie/nfc/applications.asp

parcourir des sites équipés de tags NFC et de QR codes qui leur fournissent des liens vers des informations audio et vidéo complémentaires sur les endroits visités. Le circuit touristique "Guillaume le Conquérant" qui conduit les visiteurs à découvrir des monuments représentatifs d'une partie de l'histoire de la ville en est un exemple.

Des solutions de billettique sont également proposées avec le service M-Stadium qui permet de payer et de faire valider, à l'aide de smartphones équipés de la technologie NFC, des billets d'entrée aux compétitions sportives se déroulant au stade d'Ornano de Caen. En janvier 2011, à l'instar de huit autres villes françaises, Caen a reçu le label "Territoire leader du mobile sans contact" de la part du ministère français de l'industrie, de l'énergie et de l'économie numérique [web4]. Ce label vise à promouvoir le développement de services mobiles compatibles NFC au sein des communautés urbaines.

1.1.2.3 Oulu, Finlande

Certains pays scandinaves ont également lancé des projets de services mobiles citoyens. L'un des exemples les plus intéressants est celui de la ville d'**Oulu** qui constitue une sorte de vitrine en Finlande concernant les *smart cities* [web7]. Oulu a d'ailleurs été la seule ville européenne nommée en janvier 2012 dans le top 7 des villes les plus "intelligentes" du monde lors de la conférence annuelle du PTC[3]. Ce top 7 rassemble les villes qui ont les modèles les plus pertinents de développement, d'innovation, de résolution des problèmes urbains et de promotion de la culture basés sur l'investissement dans les technologies de l'information et de la communication.

Un des services les plus remarquables que les infrastructures de la ville d'Oulu (en partenariat avec l'université d'Oulu et le VTT Technical Research Centre of Finland) fournissent aux citoyens et aux visiteurs est l'accès libre et gratuit à Internet par un réseau appelé panOulu [web26] auquel il est possible de se connecter via Wi-Fi ou Bluetooth. Environ 1270 points d'accès Wi-Fi et 30 points d'accès Bluetooth répartis dans toute

3. Pacific Telecommunications Council - http ://www.ptc.org/

la ville (figure 1.6) permettent à la population d'accéder à Internet avec des téléphones mobiles ou des ordinateurs portables correctement équipés [72]. En Wi-Fi, il est possible de se connecter pratiquement quel que soit l'endroit de la ville où l'on se trouve. Le réseau panOulu facilite la consultation, en situation de mobilité, des ressources que la municipalité met à la disposition des citoyens sur son site web. Il permet également à des fournisseurs de services ne dépendant pas des autorités municipales de proposer des systèmes dont le fonctionnement repose sur l'utilisation des infrastructures de communication déployées. C'est le cas du système RunWithUs[35] qui vise à encourager la pratique du jogging. RunWithUs est une sorte de réseau social accessible via un téléphone mobile qui donne des conseils sur des parcours de course en fonction des conditions météorologiques, qui permet de réunir un groupe de personnes avec la même condition physique, qui compare les performances de coureurs sur le même parcours et qui se sert des points d'accès Wi-Fi visités pour donner les positions approximatives des utilisateurs qui l'autorisent. L'ensemble de ces initiatives est coordonné dans le programme UBI (UrBan Interactions) qui est supervisé par l'université d'Oulu [web31][73]. Oulu offre également des services d'information comme Caen et Nice à travers un système de tags NFC déployés dans les lieux les plus fréquentés afin de fournir des renseignements utiles comme les horaires de passage des bus.

Figure 1.6 – Points d'accès au réseau panOulu dans la ville d'Oulu.
source : http://www.infotech.oulu.fi/Annual/2010/mteam.html

Au niveau des investissements pour l'avenir, la ville d'Oulu fait partie des fondateurs du CIE (Center for Internet Excellence) situé dans les locaux de l'université d'Oulu. Le CIE a pour objectif de promouvoir la recherche et le développement dans le secteur des technologies mobiles tout en faisant de l'espace urbain une zone d'expérimentation pour des services novateurs proposés aux citoyens de la ville [web6].

1.1.2.4 Valence, Espagne

L'Espagne a également conçu des plans pour favoriser l'essor des *smart cities*. Financé par le ministère espagnol de la Science et de l'innovation, le projet Mobitrans [web21] qui

vise à mettre la technologie au service du développement d'une mobilité urbaine qualifiée de durable fait partie de ces plans. Mobitrans rassemble des partenaires de l'industrie des technologies de la communication, des laboratoires de recherche ainsi que des autorités publiques locales. La ville de **Valence** a participé à ce projet dans le but d'offrir à ses habitants des services mobiles évolués dans le domaine du transport public et privé. Dans la pratique, Mobitrans met à la disposition des usagers un système d'information qui intègre tous les moyens de transport disponibles dans l'agglomération et incite à l'éco-responsabilité : les utilisateurs sont informés, à la demande, de toutes les possibilités pour effectuer un trajet entre deux endroits de la zone urbaine en prenant en compte des critères comme le coût, la durée ou le confort. Un accent particulier est mis sur les transports en commun qui sont privilégiés en cas de disponibilité. De plus, les options de parcours sont mises à jour en temps réel en fonction des incidents qui surviennent. L'impact en émission de CO_2 de chaque trajet proposé est également notifié aux usagers afin d'encourager les comportements urbains respectueux de l'environnement. A partir de son téléphone portable et en situation de mobilité, un citoyen peut donc planifier un voyage en fonction de ses préférences et de ses obligations. Le système lui indiquera différentes combinaisons de transports publics à envisager pour atteindre sa destination, ou alors le parcours à emprunter (en fonction du trafic) si le trajet devait être effectué en véhicule privé.

En dehors du transport, d'autres secteurs font l'objet d'initiatives pour améliorer le quotidien des Valenciens. Au niveau de la santé, un système d'alertes mobiles fonctionne pour avertir les habitants lors de la survenue de risques sanitaires particuliers [web11]. Tout citoyen peut s'inscrire sur le site web de la mairie pour recevoir des informations par SMS en cas de taux élevé de pollen dans l'air ou de prévisions de températures particulièrement hautes. Concernant les actions à plus long terme, le conseil municipal de Valence a apporté son soutien au plan "Smart City VLC" [web28]. Ce projet, qui est conduit par les responsables du Parc Technologique et de l'université de Valence, a pour ambition de mettre en place une plate-forme pour explorer les avantages offerts par les nouvelles technologies de l'information afin d'accroître la compétitivité de l'économie locale et la qualité du cadre de vie à travers des services orientés vers le développement durable. Les services étudiés sont pensés dans l'objectif de réduire la consommation en énergie fossile et l'émission de CO_2 comme cela est le cas du système de location de véhicules que la ville souhaite déployer pour les touristes. Ce système de location, accessible via téléphone mobile, propose des voitures électriques équipées de tablettes tactiles présentant les points d'intérêt de la ville.

1.1.2.5 Conclusion

L'échantillon des projets engagés démontre le caractère dynamique des actions qui sont entreprises autour du concept de *smart cities*. A travers toute l'Europe, des initiatives nationales ont été lancées et encouragées par les gouvernements. L'utilisation de technologies émergentes comme le NFC ouvre, en effet, des perspectives remarquables en matière de services de proximité dédiés aux citoyens. Cependant, à l'origine, il existait très peu de collaborations entre pays afin de partager les retours d'expérience sur les différents déploiement de services qui avaient été réalisés. L'intégration européenne étant devenue une réalité plus tangible, les instances du continent ont multiplié les efforts pour remédier à ce problème. Des programmes intra-européens, comme ITEA2 [web17], ont permis à de grandes entreprises technologiques, à des universités, à des laboratoires de recherche,

à des PME et à des structures municipales d'établir des coopérations en matière de recherche et développement. Les efforts des autorités européennes se sont traduits par le lancement de nombreux projets collaboratifs dans plusieurs domaines des technologies de l'information et de la communication. Le programme ITEA2 qui est spécialisé dans les SiSS (Software-intensive Systems and Services) donne lieu aujourd'hui plus de 40 projets de type collaboratif dans le domaine des systèmes et services logiciels pour les villes européennes [29]. Ainsi, des coopérations qui visent à transformer les zones urbaines en *smart cities* par le moyen de services mobiles, tout en essayant d'établir des standards européens, ont aussi vu le jour. Le projet Smart Urban Spaces, qui a été labellisé par le programme ITEA2, fait partie de cet ensemble de coopérations.

1.2 Le projet *Smart Urban Spaces*

1.2.1 Présentation et fonctionnement

Le projet *Smart Urban Spaces*, SUS en abrégé, a rassemblé au sein d'un consortium européen des partenaires issus de 3 pays européens à savoir l'Espagne, la Finlande et la France. SUS visait, à travers le cadre défini par le programme ITEA2, à promouvoir une coopération entre instituts de recherche, entreprises du domaine des technologies de l'information et de la communication et structures municipales afin de proposer des services numériques (e-services) pour téléphones mobiles à l'intention des citoyens des villes européennes impliquées. Le projet a débuté en juillet 2009 et s'est achevé en décembre 2012 pour l'ensemble de partenaires à l'exception du LaBRI [4] (représentant l'Université de Bordeaux par l'intermédiaire du thème MUSE) qui a continué à travailler sur le projet jusqu'à la fin du mois de juin 2013. L'originalité de cette initiative réside non seulement dans le fait que les applications proposées sont basées sur les technologies mobiles les plus récentes comme le NFC mais aussi dans la conception de ces applications qui met l'accent sur l'interopérabilité entre les services mobiles proposés. La notion d'interopérabilité dans le sens adopté par le projet SUS, qui sera expliquée plus en détails dans la partie 1.2.2 de ce document, englobe les éléments liés à l'adaptation d'un service à son contexte d'exécution urbain ainsi que ceux liés à la possibilité pour un citoyen d'utiliser de façon transparente des services mobiles de villes différentes. Cette attention particulière portée à la notion d'interopérabilité devait conduire au développement de services mobiles qui sont non seulement adaptés à l'environnement courant des citoyens des villes partenaires du projet mais qui utilisent aussi des standards technologiques compatibles. Les villes qui intégreront cet ensemble de services dans leur offre à leurs citoyens vont constituer un réseau de villes "numériques" (e-cities) virtuellement connectées les unes aux autres dans le but de poser les premiers jalons en terme de standards européens pour *smart cities*.

En d'autres termes, le projet SUS devait contribuer à la création de standards pour des services mobiles en zone urbaine, définir les moyens de diffusion de ces services et évaluer les solutions proposées, par le déploiement de prototypes dans les villes partenaires. Tous les aspects de préservation de la vie privée et de gestion appropriée de l'identité dans le contexte urbain devaient naturellement être considérés afin de respecter les réglementations européennes. Il s'agissait également, à travers SUS, de fournir des briques technologiques

4. Laboratoire Bordelais de Recherche en Informatique - http ://www.labri.fr/

	Villes	**Entreprises**	**Instituts de recherche**
Espagne	- Bilbao - Gijón - La Pobla de Vallbona - Melissia - Paterna - Valence	- AICIA - Avanzis S.L. - CBT Communicación - Creativ IT - Palma Tools - Telvent ARCE - Visual Tools S.A.	- ESI Tecnalia
Finlande	- Forum Virium Helsinki - Oulu	- Bonwal - Fara Oy - ToP Tunniste Oy - While on the move	- VTT Technical Research Centre Of Finland
France	- Caen - Saint-Lô	- Applicam S.A. - CEV Groupe Chèque Déjeuner - Gemalto Frane - Intelligéré - NXP Semiconductors France - Thales	- Université de Bordeaux - Université de Caen

TABLE 1.3 – Partenaires du projet Smart Urban Spaces.

de base et des cadres de conception nécessaires au développement de futurs services dans différents domaines essentiels aux espaces urbains. A titre d'exemple, certains des domaines ciblés dans ce projet qui peuvent faire l'objet de propositions de services pour améliorer la vie quotidienne des citoyens sont les suivants :

- la billettique mobile (particulièrement dans le domaine du transport ou de la gestion d'évènements) pour acheter et utiliser des tickets avec un téléphone portable ;
- les smart-posters dotés de tags NFC et de QR codes pour accéder à des informations ou lancer des opérations spécifiques avec un téléphone portable ;
- le e-tourisme pour améliorer l'interactivité des visites de musées ou d'autres sites culturels en proposant des compléments d'informations sous forme multimédia, consultables avec un téléphone portable.

La réalisation des objectifs mentionnés nécessite une collaboration entre acteurs du monde académique, de la recherche scientifique, de l'industrie, du milieu des prestataires de services et du domaine de la gestion des zones urbaines. Le consortium SUS a donc regroupé 32 partenaires provenant de ces différents milieux. Le tableau 1.3 donne un aperçu de la répartition des différents membres du consortium en fonction de leur statut et de leur pays d'origine. L'entreprise qui a coordonné l'ensemble des activités du projet est Gemalto France. Les activités de *Smart Urban Spaces* se sont articulées autour de 8 groupes de travail interdépendants, appelés Work Packages (WP), dans lesquels chaque partenaire a apporté des contributions à hauteur de ses compétences. Les WP, avec chacun un objectif spécifique, ont permis de scinder le travail à effectuer en tâches moins complexes et de suivre les différentes phases d'exécution du projet. Les huit WP ont été définis de la façon

suivante :

- le **WP 1 (Services for Cities)** a pour objet d'identifier et de décrire en détails un ensemble de services à développer autour des technologies mobiles les plus récentes et qui présente un intérêt commun pour les citoyens des villes représentées.
- le **WP 2 (Pilots)** doit préparer l'environnement technologique et humain pour que les propositions de services qui ont donné lieu au développement de prototypes puissent être testées dans les villes qui le souhaitent et pour que les résultats de ces expérimentations soient analysés. Il est à noter que lorsque nous parlons de déploiements de pilotes, il s'agit non seulement de la mise à disposition des utilisateurs du service mobile considéré (sous forme d'application mobile) mais aussi de la mise en place du système d'accès au ressources liées (installation des infrastructures nécessaires).
- le **WP 3 (Ecosystem)** a pour mission d'étudier le contexte légal, social et économique au niveau national (Espagne, Finlande et France) et européen afin qu'il puisse être pris en compte dans toutes les étapes de conception et de mise en œuvre des services à déployer.
- le **WP 4 (Technology developments)** a pour rôle de proposer des outils de développement et à implémenter les briques technologiques de base en fonction des besoins tout en définissant une architecture générale pour la diffusion des services mobiles au sein des villes.
- le **WP 5 (End-User Framework)** doit mettre en place les méthodes et les modules technologiques indispensables (dans le respect de la législation en vigueur) à la gestion des identités et à la sécurisation des données privées des utilisateurs de services pour lesquels il est nécessaire de fournir des informations personnelles.
- le **WP 6 (Standardization)** a pour but de conduire, en partant de l'analyse du déploiement des pilotes (utilisant les technologies du WP4), à l'amélioration de standards existants ou éventuellement à la proposition de nouveaux standards technologiques.
- le **WP 7 (Exploitation and Dissemination)** est dédié à l'exploitation par les structures industrielles et urbaines ainsi qu'à la diffusion (présentations publiques, publications de conférences scientifiques, articles de journaux, etc.) des solutions et résultats issus du projet.
- le **WP 8 (Project Management)** organise le suivi et l'administration du projet à travers les structures de gestion que sont le PMB (Project Management Board) qui définit l'orientation générale du projet en référence aux objectifs assignés, le PCC (Project Consortium Committee) qui s'occupe de la plannification et du contrôle des activités de chaque groupe de travail en coordination avec les différents responsables de WP, et le CC (City Council) qui rassemble les villes partenaires et qui délivre les recommandations utiles au développement de services répondant aux besoins spécifiques des espaces urbains.

La figure 1.7 montre les relations qui existent entre les différents Work Packages. Le WP2 obtient des informations techniques et légales provenant des WP1, WP3, WP4 et WP5 afin de procéder à la préparation des pilotes à déployer. Le WP2 peut également fournir des résultats de déploiement au WP4 afin que les modules technologiques puissent être affinés en fonction des besoins. Il est à noter que le WP2 a un rôle majeur en raison du fait que le projet est centré sur le développement de prototypes et le déploiement de

pilotes. Le WP3, lui aussi, reçoit des retours d'information des pilotes du WP2 afin qu'ils puissent être analysés suivant le contexte socio-économique. Les WP4 et WP5 interagissent en échangeant les outils qu'ils peuvent partager pour produire les modules technologiques (prenant en compte l'environnement défini au WP3) requis pour le développement des prototypes décrits dans le WP1. Quant au WP7, il utilise les résultats technologiques des WP2, WP4, WP5 et WP6 dans la phase d'exploitation et de dissémination. Toutes ces relations entre Work Packages sont établies dans l'espace du WP8 qui gère l'ensemble du projet.

L'Université de Bordeaux a apporté des contributions aux WP1, WP2, WP4, WP5 et au WP7. En effet, le LaBRI possède une expertise dans la modélisation et le développement d'applications collaboratives sécurisées dans un milieu à forte mobilité. La possibilité d'adapter, d'étendre et d'intégrer ces modèles aux outils technologiques à fournir dans les WP2, WP4, et WP5 a fait partie des éléments explorés. De plus, en raison du caractère innovant des technologies employées au sein du consortium SUS, les modèles conçus et implémentés sous forme de services mobiles soulèvent des problématiques de recherches intéressantes (gestion distribuée des identités, sécurisation des communications en mode *peer-to-peer*, etc.).

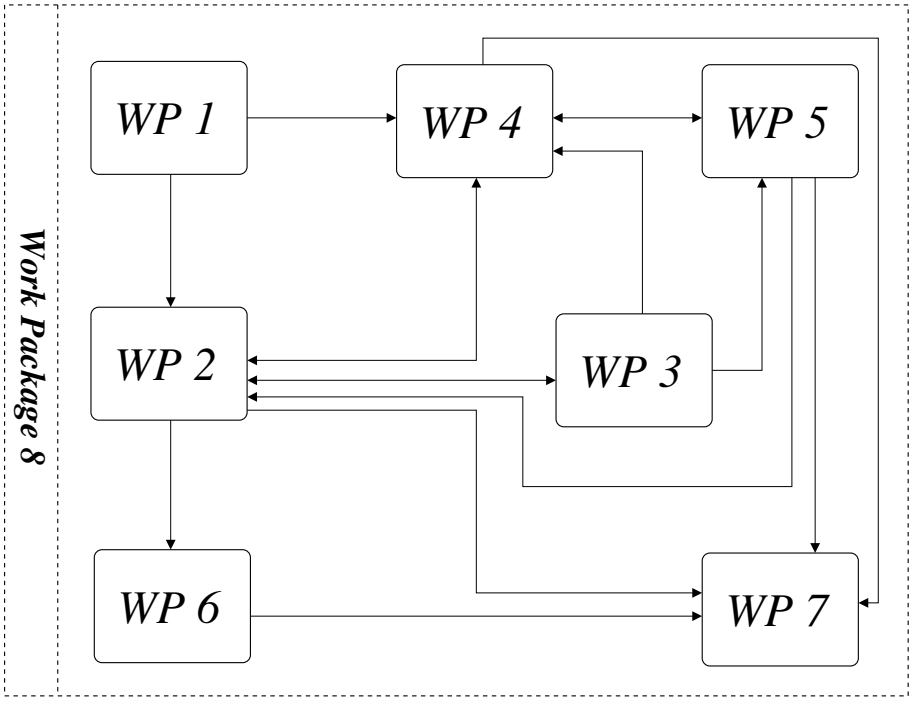


FIGURE 1.7 – Relations entre les Work Packages.

Au niveau des réalisations en matière de services, 49 scénarios de pilotes et les applications associées ont été envisagés. 21 d'entre eux ont fait l'objet de tests dans certaines villes tandis que les autres sont soit en cours de déploiement soit toujours en phase d'étude. Ces pilotes avaient pour but d'explorer dans un contexte réaliste avec des expériences menées sur le terrain les possibilités de services pour *smart cities*. La carte de la figure 1.8 donne un aperçu des différents domaines qui ont été ciblés dans la cadre du consortium et

quelques exemples de propositions qui ont conduit à l'implémentation d'applications mobiles testées suivant des scénarios de pilotes. La figure 1.9 détaille l'architecture générale

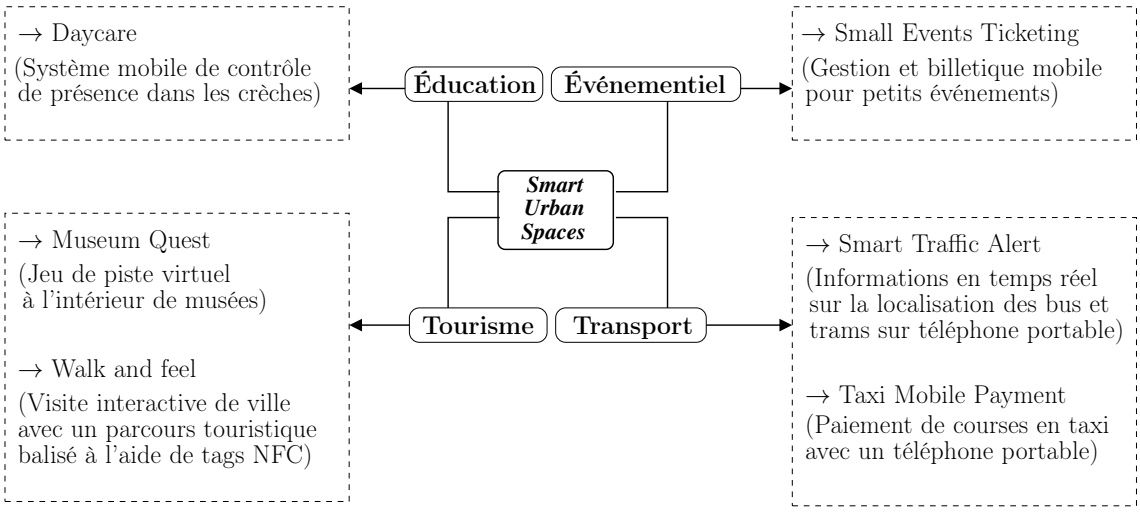


Figure 1.8 – Aperçu de la carte des services proposés.

du système conçu pour la diffusion des services. L'architecture présentée comprend toutes les entités indispensables au fonctionnement de la plate-forme SUS. Ces entités ont des rôles qui peuvent décrits comme suit :

- le **Citoyen** qui est l'utilisateur des applications offertes par le moyen des services mobiles disponibles depuis son téléphone portable.
- les **Services Providers** sont les entités qui rendent disponibles les services mobiles liés aux ressources qu'ils proposent aux utilisateurs de la plateforme.
- la **SUS-Administration Platform** ou SUS-AP qui sert de lien entre le Citoyen et les autres entités que sont le CSS (voir ci-dessous) et les Services Providers.
- le **Central Secure Storage** ou CSS qui a en charge le stockage sécurisé des données personnelles fournies par les utilisateurs et qui pourraient être utiles aux Services Providers.

L'un des points essentiels de cette architecture est l'apparition du concept de SUS-AP. La SUS-AP répond au besoin de fournir un lien entre les utilisateurs et les services mobiles qu'ils peuvent utiliser dans l'espace urbain. C'est la plate-forme de diffusion des services mobiles. La SUS-AP est l'entité qui offre à l'utilisateur final un point d'entrée unique, à partir de son terminal mobile, pour les différents services disponibles au sein d'une ville. En d'autres termes, la SUS-AP agit comme un agrégateur de services et son objectif principal consiste à faciliter les échanges entre les citoyens et les fournisseurs de services. Elle est au cœur du système. Les citoyens peuvent, par exemple par le biais de l'interface qu'elle propose, s'abonner facilement à un service de transport ou télécharger une application mobile de billettique. Les différents fournisseurs utilisent la plate-forme pour publier les informations concernant le type de ressource qu'ils offrent. Généralement, pour accéder aux ressources proposées par un fournisseur de services, l'utilisateur doit communiquer des données personnelles permettant de l'identifier. Des données identiques peuvent être requises pour des fournisseurs différents et il est donc souhaitable d'éviter à l'utilisateur une saisie répétée des mêmes informations. A ce titre, la SUS-AP prend également en charge la

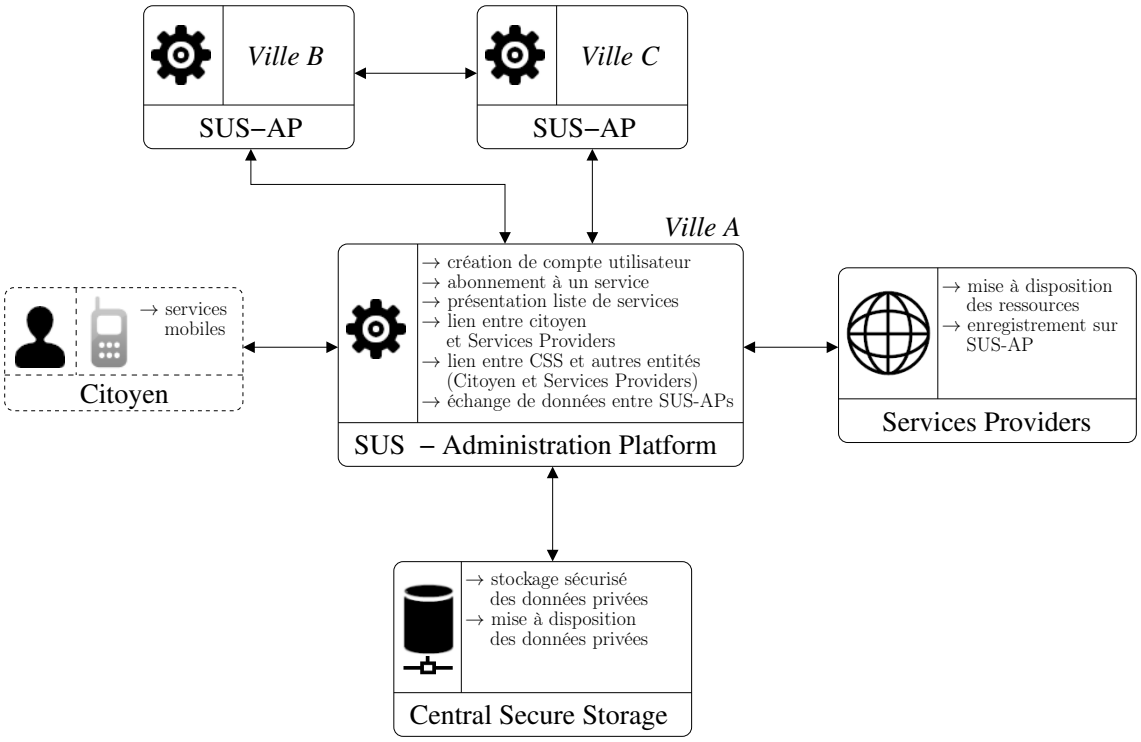


FIGURE 1.9 – Architecture de la plate-forme Smart Urban Spaces.

centralisation de ces données personnelles des utilisateurs et leur transmission lorsque cela est nécessaire. La SUS-AP gère d'un côté les comptes des utilisateurs (création, édition, etc.) dont les données sont sécurisées dans le CSS et de l'autre la communication aux prestataires des informations personnelles requises pour l'utilisation de leurs services.
La SUS-AP peut être considérée comme une plate-forme proposant un ensemble de ressources que les autorités locales d'une ville mettent à la disposition de leurs citoyens à travers un portail dédié. En pratique pour l'utilisateur, la SUS-AP prend la forme d'une application mobile dont l'interface permet d'avoir un point central qui gère de manière efficace et sécurisée ses interactions avec toutes les entités extérieures.
Pour terminer la définition du concept de SUS-AP, il est à noter qu'une SUS-AP est dédiée à une ville et ce en raison des spécificités liées à l'environnement de chaque zone urbaine. De plus, la construction d'un réseau de *smart cities* étant un des objectifs majeurs du projet SUS, les SUS-AP des différentes villes doivent être interconnectées afin de rendre possible les échanges de profils d'utilisateurs et faciliter leur accès à des services non localisés dans leur zone urbaine d'origine.

En plus des réalisations concernant les services, la notion d'interopérabilité a également été étudiée de façon spécifique. A partir de l'architecture générale, un cadre particulier dénommé *Interoperability Framework* a été défini pour proposer des outils d'évaluation de cette notion d'interopérabilité dans l'espace des *smart cities*.

1.2.2 Cadre de mise en place et d'évaluation de l'interopérabilité

Il est à noter que nous proposons des notions d'interopérabilité différentes de celles qui sont généralement développées. La particularité de cette approche est présentée dans notre définition de l'*Interoperability Framework* dans la suite de cette section.

L'*Interoperability Framework* a pour objectif de fournir des outils de compréhension et d'analyse du concept d'interopérabilité, de façon générale dans les *smart cities* et plus particulièrement pour le projet SUS. Il s'agit d'explorer les notions que peuvent recouvrir ce concept d'interopérabilité dans le but de proposer des règles de conception, de déploiement et de fonctionnement d'un système de diffusion de services mobiles pour espaces urbains interconnectés.

L'interopérabilité est généralement définie comme étant la capacité que possède deux ou plusieurs composants logiciels à interagir entre eux en dépit de leurs différences en matière d'interface et de plate-forme d'exécution [109]. Cette définition qui privilégie les aspects techniques semble trop restrictive dans notre contexte. En effet, dans le cadre des *smart cities*, il est indispensable de prendre en compte tout l'environnement dans lequel les services mobiles sont déployés. Par conséquent, notre conception de l'interopérabilité passe par la prise en compte des entités qui sont impliquées dans les opérations effectuées au sein de la plate-forme SUS. Afin d'avoir une vue globale de tout l'environnement, les types suivants d'entités sont considérés :

- l'**Utilisateur** qui est le citoyen utilisant les services proposés avec son téléphone portable ;
- le **Téléphone Mobile** qui est l'outil d'interaction de l'utilisateur avec l'environnement extérieur physique ou virtuel ;
- l'**Infrastructure** qui représente (dans le contexte du projet SUS) l'ensemble des équipements compatibles NFC comme les lecteurs NFC ou les tags NFC avec lesquels le téléphone mobile peut entrer en contact ;
- le **Service** qui prend généralement la forme d'une application mobile s'exécutant sur un téléphone mobile et qui est le moyen qu'un citoyen utilise (en s'appuyant si nécessaire sur une infrastructure) pour réaliser des opérations en zone urbaine ;
- la **SUS-AP** qui est la plate-forme telle que décrite dans la section 1.2.1 ;
- la **Ville** qui est la zone géographique pour laquelle une SUS-AP est déployée ;
- le **Pays** ;

L'étude de l'interopérabilité a pour objectif de déterminer les capacités que doivent posséder les différentes entités du système pour pouvoir interagir entre elles. Dans ce sens, l'identification des entités permet de définir un premier outil de l'*Interoperability Framework*, à savoir la matrice d'interopérabilité représentée dans le tableau 1.4. Cette matrice, à travers ses cellules, modélise les différents niveaux d'interopérablité qui sont à considérer (la signification des couleurs des cellules sera expliquée dans la suite). En d'autres termes, chaque cellule représente le lien d'interopérabilité qui peut être étudié entre deux types d'entités. Par exemple, la cellule Service-Infrastructure doit être interprétée de la façon suivante : quelles sont les conditions à remplir pour que Service soit "interopérable" avec Infrastructure ? La matrice d'interopérabilité permet donc d'avoir une vision plus claire des différentes relations possibles entre entités. En plus de cette visibilité sur les relations entre entités, la matrice conduit à prendre en considération l'idée de hiérarchisation associée à la notion d'interopérabilité. En effet, il est aisé de remarquer qu'une ville est soumise aux

	Utilisateur	Mobile	Infrastructure	Service	SUS-AP	Ville	Pays
Utilisateur							
Mobile							
Infrastructure							
Service							
SUS-AP							
Ville							
Pays							

TABLE 1.4 – Matrice d'interopérabilité.

Les cellules en rouge du tableau font référence aux cas d'interopéabilité hiérarchique tandis que les cellules vertes ont rapport à l'interopérabilité fonctionnelle. Les cellules noires marquent les relations qui n'ont pas de signification, en pratique, dans le cadre de notre analyse. Par exemple, dans notre contexte, la relation Ville-Ville n'a pas réellement de sens, l'intérêt résidant plutôt dans l'analyse des interactions entre deux SUS-AP que déploient deux villes différentes. Les cellules blanches, quant à elles, identifient à la fois les cas pour lesquels la relation hiérarchique n'est pas directe (cf . figure 1.10) et les cas pour lesquels il n'existe ni hiérarchie ni relation fonctionnelle.

lois du pays dans lequel elle se trouve, ce qui a nécessairement de l'influence sur l'analyse de l'interopérabilité qui peut être menée. Les contraintes entre pays ont un impact sur les contraintes entre villes même si ces dernières peuvent avoir leurs propres contraintes supplémentaires (lois spécifiques par exemple). Cette idée de hiérarchisation marque la dépendance qu'un type d'entité affiche par rapport à un autre type d'entité. La figure 1.10 montre la hiérarchie qui existe entre les types d'entités identifiés. Le schéma introduit deux nouveaux concepts : l'interopérabilité hiérarchique et l'interopérabilité fonctionnelle. L'interopérabilité hiérarchique concerne les cas où une entité dite de niveau "supérieur" impose ses règles à une entité dite de niveau "inférieur". Dans ces cas de figure, pour assurer le fonctionnement du système l'entité "inférieure" doit au préalable se conformer à certaines exigences que peut imposer l'entité "supérieure" (exemple de la relation Ville-Pays). Au contraire, l'interopérabilité fonctionnelle s'applique aux situations avec deux types d'entités qui occupent le même niveau dans la hiérarchie. Dans ce genre de situation, la question de l'interopérabilité entre ces deux entités peut être résolue en utilisant les composants d'un élément de niveau supérieur. Par exemple, deux services peuvent interagir l'un avec l'autre par le moyen d'une interface fournie par une SUS-AP. Il est à noter que l'Infrastructure ne fait pas partie de la hiérarchie définie figure 1.10 car c'est un élément transversal qui peut être utilisé par les autres entités dans la réalisation de leurs fonctions respectives ; par exemple, un service d'information peut exploiter un ensemble de tags NFC déployés dans une ville afin de proposer l'affichage de renseignements appropriés sur l'écran des équipements mobiles des utilisateurs.

Les premiers concepts définis donnent une vision plus structurée des relations qui sont possibles entre entités de l'environnement SUS. Il est ensuite nécessaire d'analyser chaque instance de relation suivant les dimensions - cf. ci-dessous - pertinentes dans notre contexte, tout en prenant également en compte l'interopérabilité hiérarchique et l'interopérabilité fonctionnelle, telles que décrites ci-dessus. La nature et les catégories des services proposés dans le cadre du projet SUS permettent d'affirmer que les dimensions techniques, légales et sociétales sont pertinentes pour étudier les problèmes d'interopérabilité soulevés. En

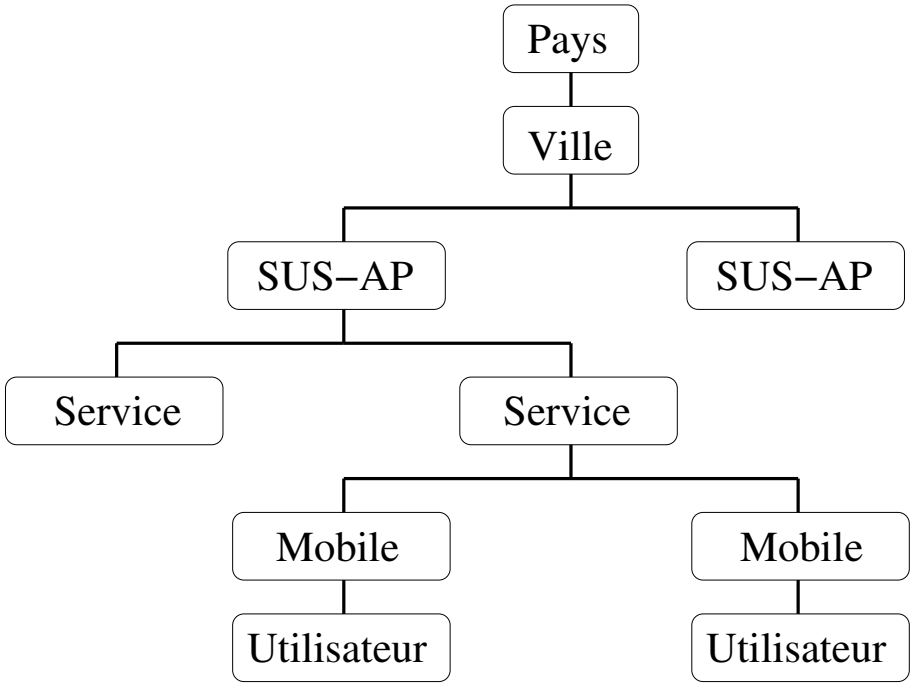


Figure 1.10 – Hiérarchie des entités.

outre, de par la nature des membres du consortium (dont certains sont des partenaires industriels) la prise en considération de la dimension commerciale est indispensable. Les quatre axes suivants d'analyse, tels que présentés figure 1.11, ont donc été privilégiés :

- la dimension **Commerciale** pour les aspects liés au *business model* (modèle d'affaire) concernant les activités dont il est question ;
- la dimension **Technique** pour l'évaluation des technologies disponibles et des standards de communication tant au niveau matériel que logiciel ;
- la dimension **Légale** pour la prise en compte des lois et des réglementations qui peuvent avoir un impact sur le comportement des entités ;
- la dimension **Sociétale** pour l'analyse des aspects culturels, de personnalisation et d'utilisation des services proposés.

Pour chaque cellule de la matrice d'interopérabilité, il s'agit donc d'examiner les quatre dimensions afin de déterminer les conditions d'interopérabilité entre deux entités. Chaque cellule de la matrice a ainsi donné lieu à la création d'un formulaire. Tous les formulaires ont une structure composée de cinq blocs : un bloc général avec des sections (question à laquelle il faut répondre - qui doit remplir ce formulaire - pré-requis) qui visent à comprendre le contexte, un bloc dédié à la dimension technique, un bloc pour la dimension légale, un bloc pour la dimension commerciale et enfin un dernier bloc consacré à la dimension sociétale. Les blocs relatifs aux dimensions d'analyse contiennent chacun un ensemble de questions jugées essentielles pour appréhender la notion d'interopérabilité entre les deux entités considérées. L'ensemble des questions a été construit en collaboration avec les membres du consortium SUS en fonction de leurs compétences et il a été régulièrement enrichi à partir des retours d'expériences obtenus à travers le déploiement de pilotes. Le tableau 1.5 présente le modèle qui a été établi pour le formulaire Service→Pays.

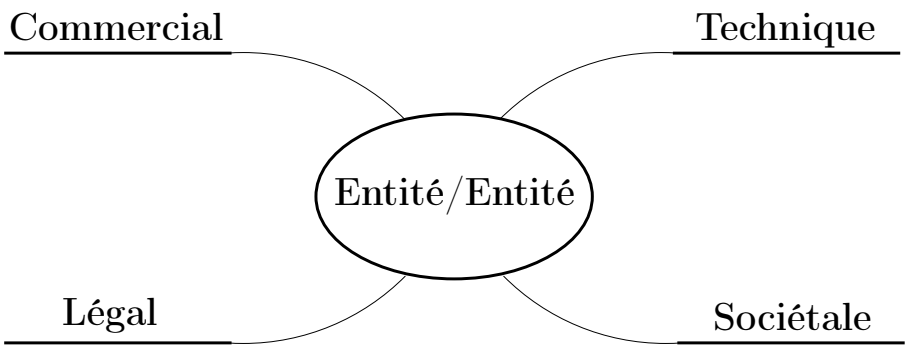


FIGURE 1.11 – Dimensions d'analyse de l'interopérabilité.

Pour une utilisation effective, il s'agit d'instancier les formulaires (le formulaire Service→Pays devient par exemple le formulaire Museum Quest→France) et de répondre à toutes les questions. Les questions ont trois réponses possibles à savoir "oui", "non" et "peut-être". Une valeur est attribuée à chaque réponse selon les critères suivants : 0 point pour une réponse "non" à une question de nature positive, 0 point pour une réponse "oui" à une question de nature négative, 1 point pour une réponse "peut-être", 2 points pour une réponse "oui" à une question positive et 2 points pour une réponse "non" à une question négative. Les questions de nature positive sont des interrogations liées aux aspects favorables à l'interopérabilité alors que les questions de nature négative concernent les aspects défavorables. Dans le formulaire Service→Ville, "Can the Service be localized if required ?" est une question positive et "Might the Service be subject to acceptation arguments in my Country ?" une question négative. La somme des points obtenus permet de calculer un pourcentag pour chaque dimension d'analyse par rapport à un maximum qui correspond à 2 fois le nombre de questions de la section considérée. Dans le tableau 1.5, si les réponses aux trois questions de la catégorie "Usability/Social" (dimension sociétale) sont respectivement "oui", "oui" et "peut-être", le pourcentage est donc de $(0 + 2 + 1)/6$ soit 50%. Les pourcentages des quatre dimensions définissent ainsi le "degré d'interopérabilité" atteint pour la cellule considérée. C'est à l'utilisateur des formulaires de choisir les valeurs minimales, pour les pourcentages des quatre dimensions, en dessous desquelles le niveau d'interopérabilité n'est pas satisfaisant. Dans le cadre de notre étude, nous fixons arbitrairement à 50% cette valeur de référence.

En plus des calculs de pourcentage et pour illustrer graphiquement l'ensemble des résultats, un diagramme de Kiviat est utilisé. Ce diagramme a plusieurs axes qui permettent de représenter une information qui dépend de plusieurs variables. Dans notre cas, le diagramme a quatre axes gradués de 0 à 100 qui se rapportent aux quatre dimensions d'analyse. La représentation graphique ainsi définie facilite les comparaisons entre différents niveaux d'interopérabilité ou entre différentes instances de formulaires. De façon concrète, le formulaire du tableau 1.6, les résultats d'analyse du tableau 1.7 et le diagramme de la figure 1.12 donnent un exemple pratique de l'application du processus d'évaluation de l'interopérabilité Daycare→Finland. Le Daycare est un service mobile de contrôle de présence dans les crèches qui a été développé dans le cadre de SUS par WhileOnTheMove [5] et qui est déployé dans certaines villes finlandaises.

5. Société finlandaise de développement de services mobiles - http ://whileonthemove.com

Service ⟶ Country

Question to answer :
What are the necessary conditions so that a given service can be used in my Country ?
Who should fill this form :
This form must be filled by a representative of a Country who is considering using a pre-existing Service, with the help of the Service provider.
Prerequisite(s) :

Technical issues
- ◦ Can the Service be localized if required ?
  → Example : language, metrics, cultural references, etc.
- ◦ Can the Service fit with the available hardware/software infrastructure available in my Country ?
  → Example : is an electronic signature national system required and if yes does the Service have one ? Open interfaces of legacy systems, etc.
- ◦ Is the Service technology standard based ?

Legal issues
- ◦ Does the Service obey the specific regulations of my Country ?
  → Example : free speech related regulations, right to forget, security and privacy, etc.
- ◦ Does the Service use and provide (if applicable) open public data in the way regulations and contract require ?

Business issues
- ◦ Will the benefit(s) gained by deploying the service be concrete ?
  → Example :
  - better flow in the national public transportations
  - better relationships between the citizens and theirs representatives
  - better sales for national museums and national museums shops
- ◦ Is the cost/benefit ratio positive ?
  → Example : is the help to find a parking space at national airports resulting from the service, worth the required monthly subscription rate ?
- ◦ Is it possible to use the same solution in many cities to save costs of public investment ?

Usability/Social questions
- ◦ Might the Service be subject to acceptation arguments in my Country ?
  → Example : would a service that connects to a public network of surveillance cameras be accepted by the population ?
- ◦ Can the Service be localized if required (note that this is also a technical issue) ?
- ◦ Does the Service make any country specific cultural reference ?

Table 1.5 – Exemple de formulaire.

Daycare ⟶ Finland	
Prerequisite(s) : the country has rules and legislations for open data, privacy and security, and open interfaces of public information systems	
Questions	**Answers**
Technical issues	
◦ Can the Service be localized if required ?	Yes(2)
◦ Can the Service fit with the available hardware/software infrastructure available in my Country ?	Yes(2)
◦ Is the Service technology standard based ?	Yes(2)
Legal issues	
◦ Does the Service obey the specific regulations of my Country ?	Yes(2)
◦ Does the Service use and provide (if applicable) open public data in way regulations and contract require ?	Maybe(1)
Business issues	
◦ Will the benefit(s) gained by deploying the service be concrete ?	Yes(2)
◦ Is the cost/benefit ratio positive ?	Yes(2)
◦ Is it possible to use the same solution in many cities to save costs of public investment ?	Yes(2)
Usability/Social questions	
◦ Might the Service be subject to acceptation arguments in my Country ?	Maybe(1)
◦ Can the Service be localized if required (also a technical issue) ?	Yes(2)
◦ Does the Service make any country specific cultural reference ?	Yes(0)

TABLE 1.6 – Réponses au formulaire Daycare→Finland.

	Service to Country (%)	**Reference values** (%)
Technical	100	50
Legal	75	50
Business	100	50
Usability	50	50

TABLE 1.7 – Résultats d'analyse du formulaire Daycare→Finland.

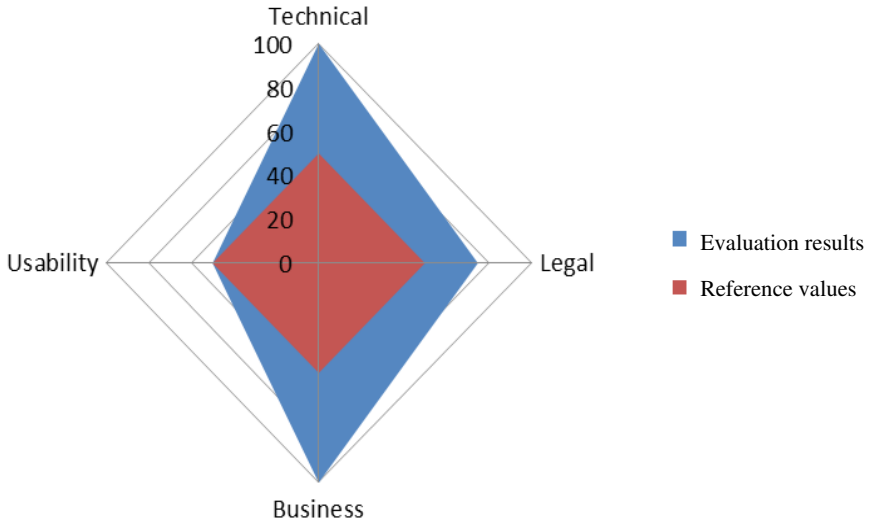


Figure 1.12 – Représentation graphique des résultats d'analyse du formulaire Daycare→Finland.

En conclusion, l'*Interoperability Framework* est une première approche développée au sein du consortium SUS dans le but de spécifier des méthodes d'appréciation et de comparaison des différents niveaux d'interopérabilité que l'on retrouve au sein des *smart cities*. En fonction du contexte, la matrice d'interopérabilité associée aux formulaires appropriés fournit les indications essentielles quant aux rapports qui existent ou peuvent exister entre deux entités. L'interopérabilité au sein de la plate-forme se comprend donc à travers l'analyse comparée des interactions entre les différentes entités prises deux à deux.

1.2.3 Conception et développement d'applications

Dans le cadre de sa participation au projet SUS, l'équipe MUSE du LaBRI a contribué (en collaboration avec ses partenaires) à concevoir, développer et tester des prototypes de services mobiles qui se présentent pour l'utilisateur final sous forme d'applications mobiles. D'un point de vue pratique, les applications mobiles ainsi implémentées ont non seulement permis de fournir des briques technologiques de base à intégrer à d'autres services mobiles mais aussi de donner des indications utiles pour la diffusion de services dans l'espace urbain. Les principales applications développées et qui seront présentées plus en détails dans la suite sont les suivantes : *Profile Providing*, *Collecting Documents*, *Small Event Ticketing* et *Museum Quest*. *Profile Providing* et *Collecting Documents* sont de la catégorie des briques technologiques tandis que les deux autres ont fait l'objet de pilotes (déployés dans quelques villes dont Caen).

Il est noter que l'une des technologies principales utilisée dans les prototypes que nous avons mis en œuvre et que nous allons présenter est la technologie NFC. Les descriptions qui sont faites de cette technologie, dans chacun des cas nous semblent suffisantes pour la compréhension du fonctionnement des applications développées. Toutefois, une description plus complète de la technologie NFC est proposée à la section 4.1.1 de ce document.

1.2.3.1 *Profile Providing*

Profile Providing est un système qui offre la possibilité à un utilisateur de communiquer à une entité extérieure, de façon sécurisée, des données personnelles stockées sur un téléphone portable. Un cas d'utilisation possible est décrit figure 1.13. Dans l'exemple présenté, l'utilisateur se sert de son téléphone mobile pour remplir le formulaire d'un site web. Pour réaliser cette opération, le téléphone est mis en contact avec un lecteur relié à l'ordinateur sur lequel le formulaire est affiché. Dans la pratique, le prototype développé permet

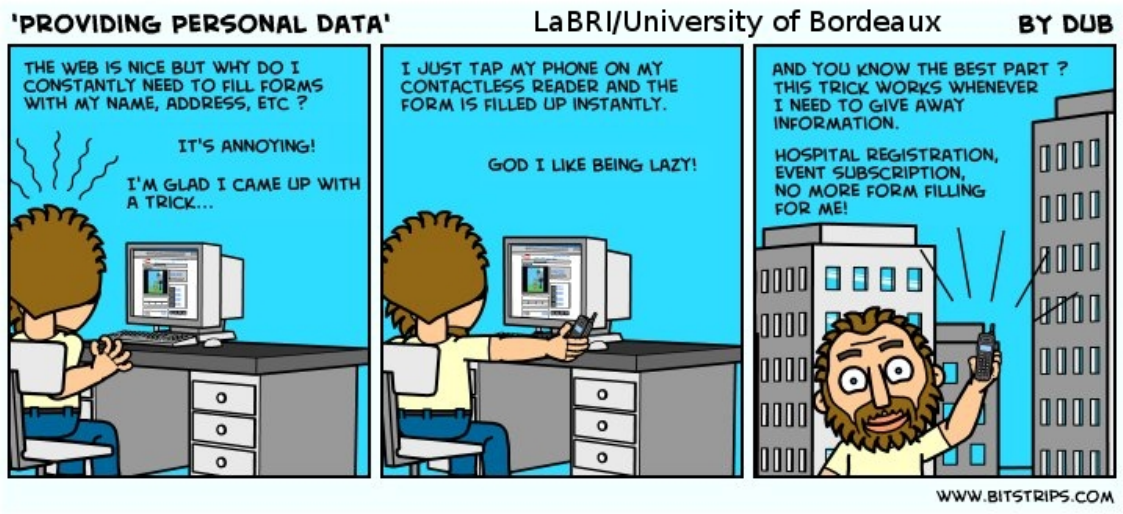


FIGURE 1.13 – Scénario d'utilisation pour Profile Providing.

de s'identifier automatiquement sur les sites web de messageries et de réseaux sociaux en utilisant un téléphone et un lecteur équipés de la technologie NFC. Dans l'architecture présentée figure 1.14, les données personnelles sont contenues dans un élément sécurisé du téléphone portable. Les données personnelles doivent donc au préalable être enregistrées dans l'élément sécurisé du téléphone. Il est à noter que l'élément sécurisé est une puce intégrée au téléphone et connectée à un circuit NFC et qui est capable de communiquer avec un lecteur sans contact équipé lui aussi de la technologie NFC. Lorsqu'une page avec un formulaire à remplir est affichée dans le navigateur, l'utilisateur approche son téléphone du lecteur NFC relié au port USB de l'ordinateur. Le lecteur, qui interagit avec le navigateur, communique à l'élément sécurisé la demande d'informations nécessaires au remplissage du formulaire. Si l'utilisateur valide l'opération, ses données personnelles sont transmises par NFC au lecteur qui les transfère ensuite via USB au navigateur pour que le formulaire puisse être rempli. La sécurité du système réside dans le fait que les données sensibles sont stockées dans un élément sécurisé et l'échange des données entre le téléphone et le lecteur, sous réserve de validation par l'utilisateur, se fait par NFC qui est une technologie sans fil de très courte portée (environ 10 cm).

Pour réaliser le prototype, nous nous sommes servis d'un Nokia 6212 Classic [web24] et d'un lecteur Prox-PU de Gemalto [web16]. Le Nokia 6212 est un téléphone portable doté d'une puce sécurisée, appelée *Secure Element* (SE), capable de communiquer par NFC avec des entités extérieures. Le Prox-PU est quant à lui un lecteur de cartes à puce capable de communiquer via NFC avec le SE du Nokia 6212. Afin de rendre possibles

les différentes opérations que le système exige, une application mobile en Java Mobile Edition (Java ME) qui s'exécute sur le téléphone mobile ainsi qu'un programme Java Card, aussi appelé applet et qui est chargé sur le SE ont été développés. L'application mobile permet d'enregistrer les informations personnelles en gérant les interactions avec le SE intégré au téléphone alors que l'applet Java Card propose un module pour répondre aux requêtes (enregistrement, récupération de données) que reçoit le SE. Il est nécessaire de préciser que Java ME [web19] est une plate-forme de développement basée sur le langage de programmation Java et destinée aux équipements aux ressources limitées (du type téléphone portable), tandis que la technologie Java Card [web18] qui est un sous-ensemble de Java fournit un ensemble d'APIs permettant d'utiliser les fonctionnalités de stockage, de communication et de cryptographie des SE compatibles. Du côté de l'ordinateur, le navigateur utilisé pour le prototype est une instance de Firefox à laquelle est greffée une extension qui inclut un programme Java pour gérer les communications du lecteur Prox-PU avec la puce sécurisée du Nokia 6212. Plus globalement, l'extension comprend des outils pour reconnaître la page web visitée et analyser le formulaire qui y figure afin de déterminer les requêtes d'information à transmettre à la puce du téléphone mobile. Il est à noter que de façon générale les échanges entre un SE et un lecteur fonctionnent en mode client/serveur en utilisant des commandes APDU (Application Protocol Data Units) selon le protocole défini dans la norme ISO 7816-4 [47]. La puce reçoit des requêtes de la part d'un lecteur sous forme de commandes APDU et elle y répond. Dans notre cas de figure ce sont à la fois l'application mobile du téléphone et le programme Java de l'extension Firefox (par l'intermédiaire du lecteur Prox-PU) qui transmettent des commandes APDU à destination du SE.

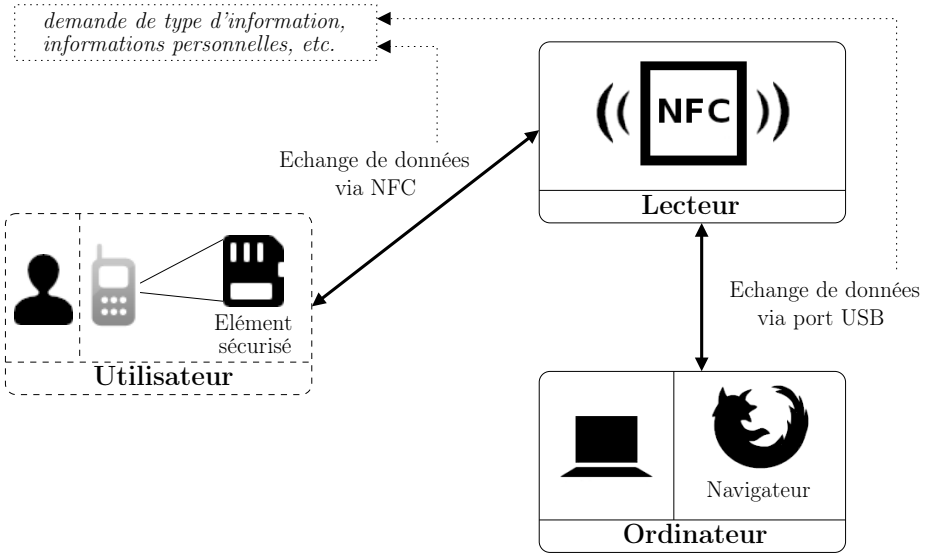


Figure 1.14 – Architecture du prototype Profile Providing.

Le déroulement des opérations s'effectue donc comme suit, si on suppose que les données personnelles d'identification sont déjà enregistrées dans le téléphone : l'utilisateur accède d'abord à une page web contenant un formulaire qu'il souhaite remplir automatiquement ; l'extension Firefox est alors activée ce qui met le lecteur Prox-PU en attente

d'une connexion avec un équipement NFC compatible ; l'utilisateur approche son téléphone Nokia 6212 Classic du lecteur et la puce reçoit une requête APDU qui spécifie les informations à fournir ; l'utilisateur valide l'opération ; la puce renvoie les informations personnelles demandées vers le lecteur ; l'extension récupère les données et s'en sert pour remplir le formulaire ; le navigateur ouvre alors automatiquement la page web correspondante. Le système actuel fonctionne par exemple sur des sites tels que Facebook et Google Mail.

1.2.3.2 *Collecting Documents*

Collecting Documents est un système qui permet de faciliter le téléchargement de documents électroniques (audio, vidéo, etc.) sur un téléphone portable. Dans le cas d'utilisation présenté figure 1.15, l'utilisateur se sert de son téléphone mobile pour récupérer des documents administratifs ou touristiques au format électronique. Dans l'exemple présenté, l'opération de téléchargement est déclenchée par un simple passage du téléphone sur un lecteur sans contact. Dans la pratique, le prototype développé consiste en une application

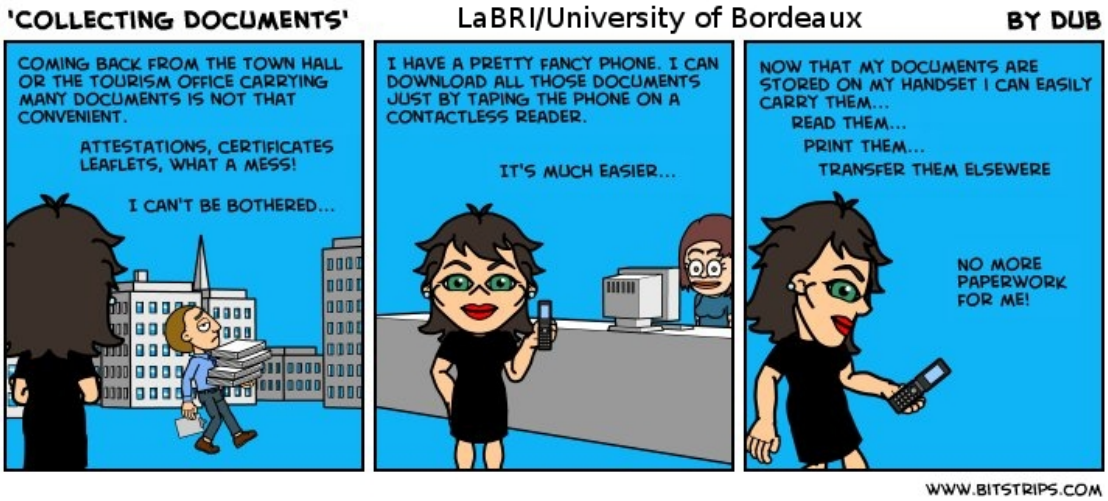


FIGURE 1.15 – Scénario d'utilisation pour Collecting Documents.

mobile qui permet de télécharger un fichier audio sur un téléphone portable en l'approchant simplement d'un tag NFC. Le fichier audio à télécharger est stocké sur un ordinateur qui est équipé de la technologie Bluetooth.

Dans l'architecture décrite figure 1.16, l'utilisateur se sert de son téléphone mobile pour récupérer une adresse Bluetooth de connexion inscrite dans la mémoire d'un tag NFC. L'adresse de connexion doit donc au préalable avoir été enregistrée dans le tag. Cette adresse est ensuite utilisée par le téléphone pour se connecter à l'ordinateur sur lequel figure des documents et transmettre une requête de téléchargement. Le document demandé est alors envoyé au téléphone par le moyen d'une application installée sur l'ordinateur considéré. Il est à noter que Bluetooth est un protocole de communication [36] par ondes radio défini par la norme IEEE 802.15 et qui a une portée pouvant atteindre 100 mètres. Chaque matériel compatible possède une adresse MAC (Media Access Control) Bluetooth

unique. Cette adresse est le plus souvent notée sur 48 bits en hexadécimal avec une séparation de chaque octet par deux points. *00:00:3A:69:E4:17* est un exemple d'adresse MAC Bluetooth. Les connexions entre équipements dotés de la technologie Bluetooth s'effectuent en mode client/serveur. L'équipement qui joue le rôle du serveur définit ce que l'on appelle un service qui spécifie les opérations que les clients sont autorisés à effectuer. Pour accéder au service, les clients utilisent une adresse de connexion qui est composée de l'adresse MAC Bluetooth du serveur et d'un code unique appelé UUID (Universally Unique IDentifier). Ce code qui sert à identifier de façon unique le service Bluetooth proposé prend généralement une forme hexadécimale sur 128 bits. Il est par exemple possible d'avoir l'UUID suivant : *710E8400-A29B-71D4-B716-347775440011*. Il est également utile de préciser que lorsqu'un client se connecte à un service, un canal de communication bi-directionnel (via Bluetooth) est alors ouvert entre eux ce qui permet un échange de données dans les 2 sens. Dans l'exemple de notre architecture, l'application qui s'exécute sur l'ordinateur définit un service Bluetooth qui permet à des clients potentiels de télécharger un fichier audio. C'est l'adresse de ce service qui est inscrite dans le tag NFC.

Dans l'implémentation du prototype, nous nous sommes servis d'un Nokia 6212 Classic et d'un tag NFC Topaz [87]. Le Nokia 6212 est non seulement équipé de la technologie NFC intégrant le mode lecture/écriture (mode qui permet en particulier de lire le contenu d'un tag) mais aussi de la technologie Bluetooth. Le tag NFC Topaz, quant à lui, possède des capacités de stockage d'information de taille au moins égale à celle d'une adresse Bluetooth de connexion à un service. La gestion des procédures de lecture du tag, de récupération de l'adresse de connexion, de connexion au service Bluetooth et de réception du fichier audio est confiée à une application mobile Java ME qui s'exécute sur le téléphone de l'utilisateur. En effet, la plate-forme Java ME comprend un ensemble d'APIs qui permettent à la fois d'utiliser les fonctionnalités de la techonolgie NFC et celles de la technologie Bluetooth. Du côté de l'ordinateur, un programme Java permet de recevoir les requêtes via Bluetooth et d'envoyer au client le fichier audio qu'il souhaite télécharger. Le langage de programmation Java fournit également un ensemble d'APIs qui permettent à une application de gérer la partie serveur des connexions Bluetooth (création de service, réception de requêtes, réponses aux requêtes et échange de données à travers un canal de communication).

Les différentes étapes dans le fonctionnement du prototype sont donc les suivantes, si l'on suppose que l'adresse Bluetooth de connexion est déjà enregistrée dans le tag NFC : l'utilisateur souhaite télécharger un fichier audio et approche son téléphone du tag NFC qui est situé près de l'ordinateur ; les informations de connexion que contient le tag sont transférées à l'application mobile du téléphone ; l'application mobile utilise ces informations pour se connecter au serveur Bluetooth hébergeur (le programme Java de l'ordinateur) et lui transmettre une requête ; ce programme Java traite la requête et envoie le fichier audio à travers le canal de communication qui relie alors le téléphone et l'ordinateur ; le téléphone mobile reçoit le fichier pour le mettre à disposition de l'utilisateur.

1.2.3.3 *Small Event Ticketing*

Small Event Ticketing est un système qui propose une solution de billettique mobile pour les petits événements. L'approche proposée vise à réduire autant que possible les coûts de déploiement (sur le lieu de l'événement et pour l'émission des billets) et s'appuie sur l'hypothèse que les utilisateurs possèdent un téléphone NFC. Dans notre contexte, nous

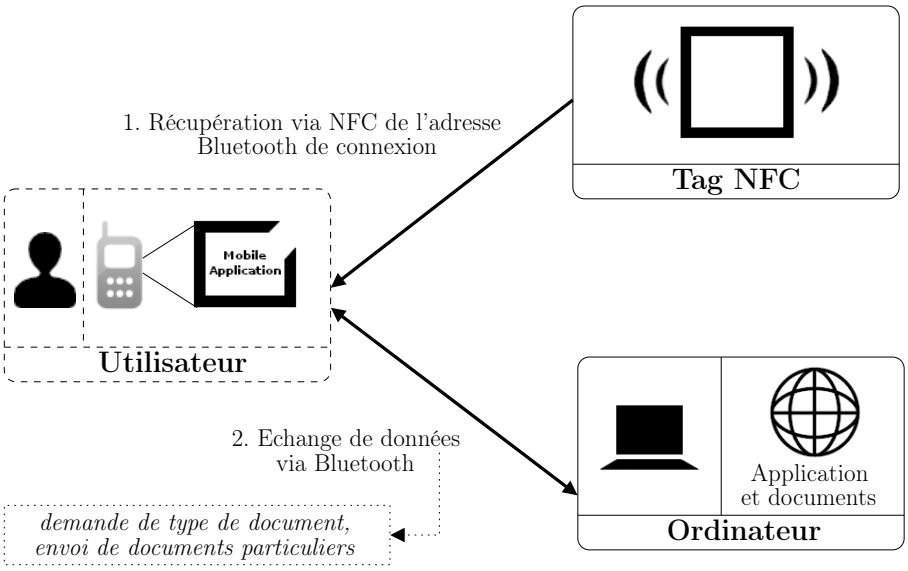


FIGURE 1.16 – Architecture du prototype de Collecting Documents.

considérons que les petits événements sont des événements avec un nombre relativement bas de participants (moins de 500 personnes) et dont les organisateurs ont des moyens financiers limités, c'est à dire qu'ils ne peuvent pas s'offrir les services d'une entreprise de gestion de billetterie.

De façon générale un système de billettique fonctionne selon quatre grandes étapes présentées figure 1.17 et qui sont les suivantes : l'utilisateur sélectionne l'événement par lequel il est intéressé ; dans le cas où cela est nécessaire, il recherche des informations complémentaires sur l'événement auquel il souhaite assister avant de confirmer son choix ; lorsque les renseignements nécessaires sont fournis l'organisme chargé de la gestion de la billetterie émet le ticket électronique et l'envoie à l'utilisateur ; le jour de l'événement l'utilisateur présente le billet électronique qu'il a acquis pour valider son accès au spectacle. Dans le cas du *Small Event Ticketing*, toutes les opérations de sélection, d'émission et de validation des billets électroniques (ou e-tickets) s'effectuent à l'aide d'un téléphone mobile. La figure 1.18 décrit un cas d'utilisation dans lequel un utilisateur qui souhaite assister à un concert se procure des places avec son téléphone mobile avant d'envoyer certains des billets émis à des amis. Le jour du concert, l'utilisateur se sert également de son téléphone portable pour présenter le e-ticket qui lui permet d'accéder à la salle de spectacle.

Dans la pratique, le prototype développé est composé de trois entités comme le montre l'architecture de la figure 1.19. Ces entités sont les suivantes : une application mobile pour le téléphone portable de l'utilisateur (ou application client) ; une application mobile pour effectuer le contrôle des e-tickets (ou application de validation) pour le téléphone portable du "validateur" ; un portail pour publier la liste des événements. Le prototype se focalise plus particulièrement sur les processus d'émission et de validation des e-tickets et ne prend donc pas en compte l'ensemble du scénario de la figure 1.18. Dans le processus d'émission des tickets, les interactions concernent l'application client et le portail de la structure qui émet les e-tickets tandis que dans le processus de validation les échanges ont lieu entre l'application client et l'application de validation. Le portail se présente sous la forme d'un

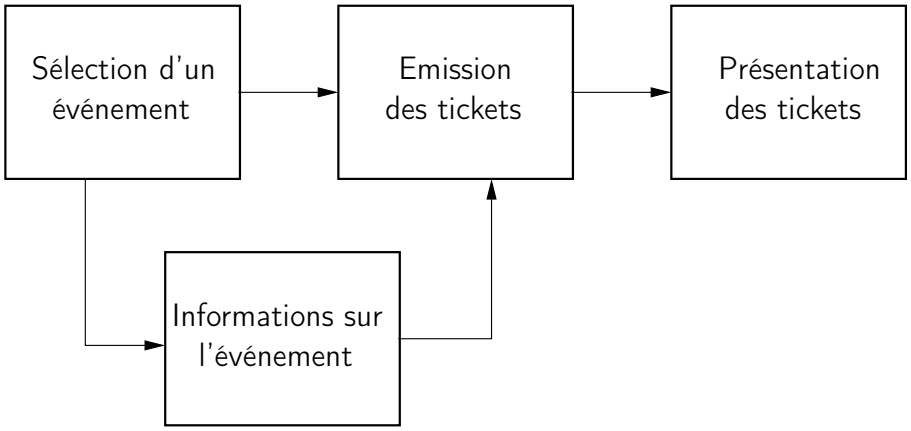


Figure 1.17 – Etapes d'un processus de billetique.

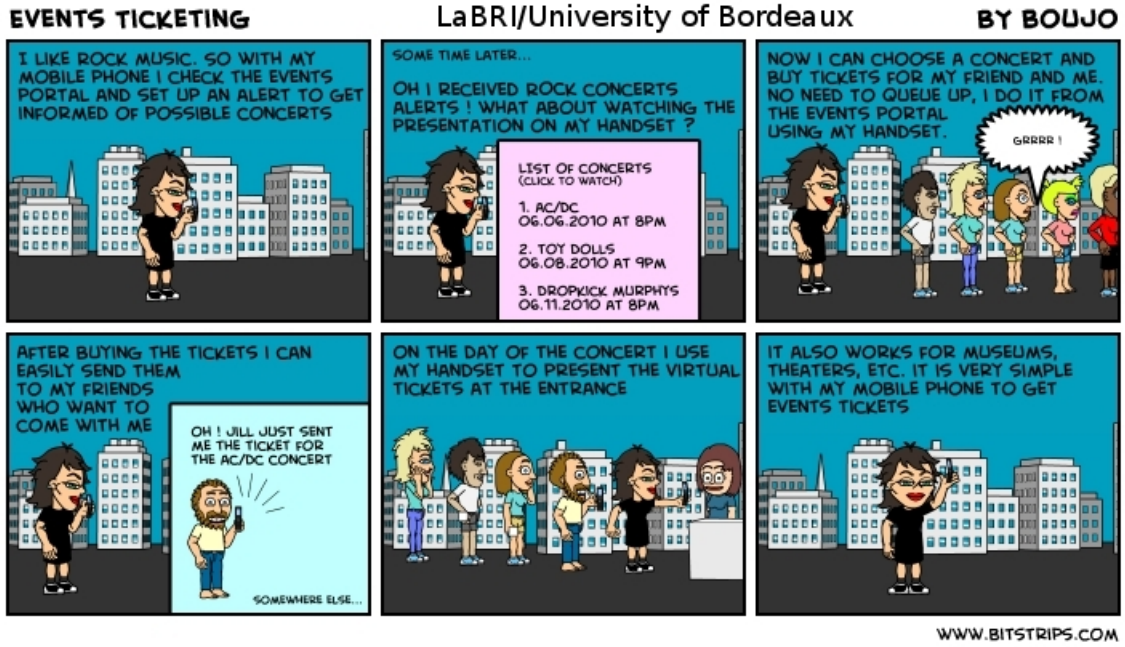


Figure 1.18 – Scénario d'utilisation pour le Small Event Ticketing.

site web qui affiche la liste des événements pour lesquels il est possible de se procurer des billets. Lorsque l'utilisateur fournit les informations nécessaires (nom, adresse mail, etc.), le portail est alors chargé de produire et de rendre disponible les e-tickets définis en fournissant un lien de téléchargement sur Internet. Les e-tickets sont signés avec une clé publique (l'application de validation possédant la clé privée correspondant) afin que leur intégrité puisse être vérifiée au moment de la validation. A chaque événement correspond une paire clé publique/clé privée spécifique. Il est à noter que le e-ticket est un fichier XML avec un numéro unique (correspondant au numéro du e-ticket) qui comprend l'identifiant de l'événement ainsi que les informations à vérifier au moment de la validation. L'application client, quant à elle, permet non seulement de se connecter au portail afin de parcourir la

liste des événements existants, de choisir les événements pour lesquels l'utilisateur souhaite obtenir des billets mais aussi de télécharger et de stocker dans la mémoire du téléphone les e-tickets acquis auprès de l'émetteur. L'application client permet également de sélectionner et de transférer, via NFC, des e-tickets stockés sur le téléphone vers le téléphone validateur afin de procéder à leur contrôle. Concernant l'application de validation, elle permet au téléphone du validateur de recevoir des e-tickets par NFC, de contrôler leur intégrité en utilisant la clé privé correspondant à l'événement et de donner des indications pour autoriser ou non l'accès au spectacle en fonction du résultat de la validation. Pour éviter qu'un e-ticket soit présenté plusieurs fois pour le même événement, l'application de validation garde la trace des billets déjà validés en enregistrant leur identifiant unique.

Un point important à noter est le fait que l'opération de validation des tickets, à l'entrée de l'événement considéré, s'effectue en mode *offline*. Cela signifie qu'aucune connexion à un serveur distant n'est nécessaire. En d'autres termes, toutes les interactions se font en local entre le téléphone du client et le téléphone du validateur (le ticket étant stocké dans la mémoire du téléphone du client).

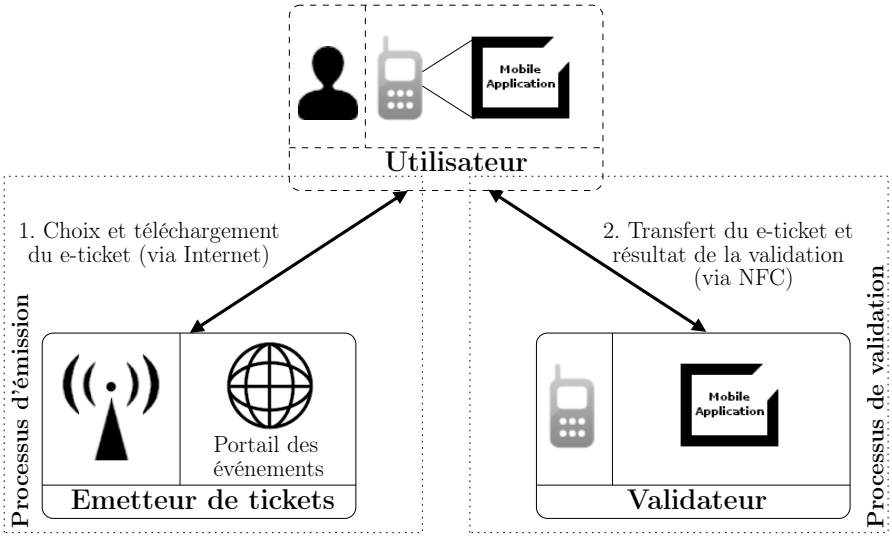
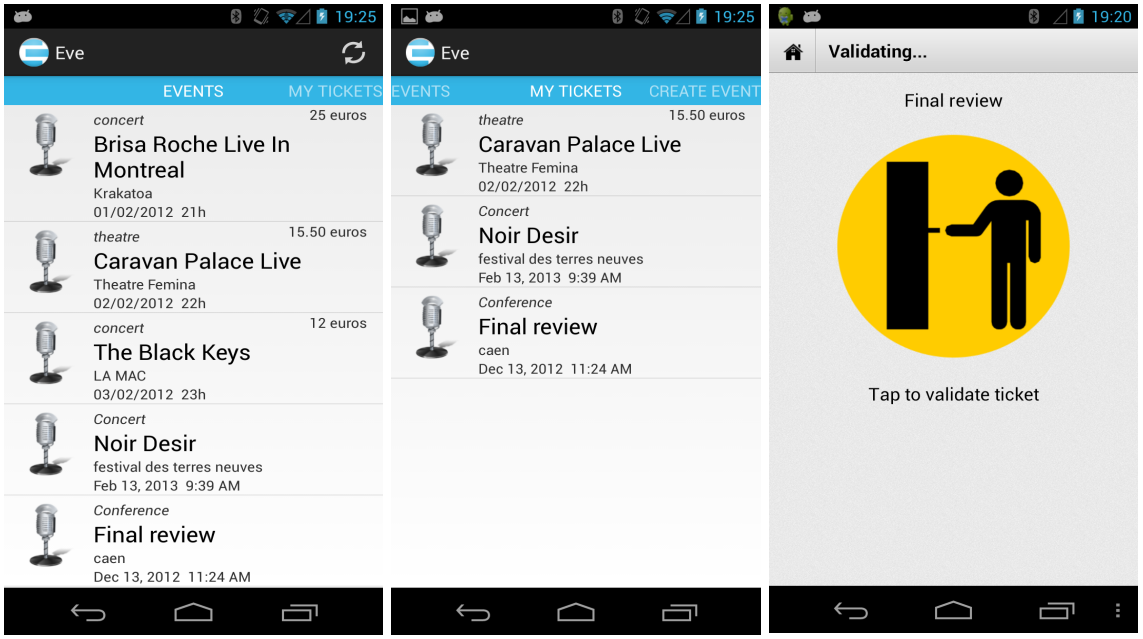


FIGURE 1.19 – Architecture du prototype de Small Event Ticketing.

Au niveau de l'implémentation, le système nécessite des téléphones prenant en charge le mode peer-to-peer de la technologie NFC. Ce mode rend possible des communications directes entre deux téléphones compatibles. Nous nous sommes servis de Samsung Nexus S [web22][web23] qui embarquent une version du système d'exploitation Android. Android est une plate-forme mobile [web2] développée par Google qui met un ensemble de couches logicielles à la disposition des fabricants de téléphones mobiles et des développeurs. Ces couches logicielles permettent de gérer les fonctionnalités de base des téléphones portables (connexion à un réseau GSM, appel, envoi de SMS, etc.) et de concevoir des applications qui leur sont dédiées. La plate-forme mobile de Google (à partir de la version 2.3.4) fournit un environnement de développement qui inclut des APIs pour développer des applications mobiles prenant en charge le mode peer-to-peer de la technologie NFC (cf. section 4.1.1 page 130). La plate-forme Android fournit aussi des modules pour gérer une connexion à Internet (pour par exemple intégrer un site web dans une application mobile) de même

que pour signer et vérifier l'intégrité d'un fichier XML à l'aide d'une paire clé publique/clé privée. Les applications mobiles de l'utilisateur et du validateur ont été réalisées avec les outils de développement du système Android. La figure 1.20 montre quelques images des applications du prototype dont le fonctionnement comprend les étapes suivantes : l'utilisateur parcourt la liste des événements (image de gauche figure 1.20) en se connectant au portail avec l'application client ; il choisit l'événement qui l'intéresse et transmet au portail les renseignements nécessaires à l'établissement du e-ticket ; le portail émet alors le e-ticket et fournit le lien de téléchargement à l'application client ; le e-ticket est téléchargé via Internet et stocké dans la mémoire du téléphone de l'utilisateur ; à l'entrée de l'événement, l'utilisateur sélectionne le e-ticket à présenter (image du milieu figure 1.20) et rapproche son téléphone de celui du validateur ; le e-ticket est automatiquement transféré par NFC sur le téléphone mobile du validateur et l'application de validation (image de droite figure 1.20) procède à sa vérification ; l'autorisation est accordée (ou pas) par l'application de validation et l'utilisateur peut alors avoir accès (ou pas) au spectacle.



Application Client **Application Client: Liste des tickets** **Application de Validation**

Figure 1.20 – Captures d'écran du prototype du Small Event Ticketing.

Ce prototype a fait l'objet de tests et des pilotes ont été déployés. L'un des pilotes a concerné la gestion de l'accès au dîner de gala d'une conférence en informatique organisée par l'Université Bordeaux 1. Lors de ce dîner, certains des participants avaient téléchargés le e-ticket correspondant à l'événement sur des téléphones mobiles mis à leur disposition et une personne à l'entrée de la salle effectuait le contrôle muni d'un téléphone équipé de l'application de validation. Une évaluation du prototype a également été menée en prenant en compte les critères de sécurité, de vitesse de validation et de simplicité d'utilisation de l'application. Pour les trois critères considérés, les points suivants ont été relevés :

– au niveau de la sécurité qui s'appuie essentiellement sur la signature des e-tickets, les propriétés de la technologie NFC (communications d'une portée d'environ 10

centimètres), l'enregistrement des e-tickets présentés pour la validation et la confiance que doit inspirer la personne responsable du téléphone validateur, il a été possible de conclure qu'un niveau raisonnable dans un contexte de petits événements était atteint

- pour la vitesse de validation des e-tickets par l'application mobile, qui est un point crucial pour éviter de trop longues files d'attente aux entrées, elle s'effectue en moyenne en 400 millisecondes ce qui est satisfaisant par rapport aux normes en vigueur (selon l'autorité des transports de Londres, la vitesse de validation d'un système de billetique qui utilise les téléphones mobiles ne doit pas excéder 500 millisecondes [web12])
- concernant l'interface de l'application client, l'utilisation du "usability scale" de John Brooke [14] (questionnaire en 10 points qui permet d'attribuer une note sur 100 à un système dont l'interface utilisateur doit être évaluée) sur un échantillon de 15 personnes a permis de montrer le potentiel de ce système dématérialisé de billetterie avec un score moyen de 77% (selon les normes admises [6] un score supérieur ou égal à 75% constitue un bon résultat dans l'évaluation de l'interface utilisateur).

Sur la base du *Small Event Ticketing*, un "modèle" pour la gestion de la billetterie des petits événements a émergé au sein du projet SUS. En effet, dans le cadre de projets orientés vers les *smart cities*, le portail des événements décrit dans le prototype peut prendre la forme d'une plate-forme développée, déployée et administrée par les autorités municipales dans chaque ville du réseau SUS. Les organisateurs d'événements pourront souscrire à la plate-forme (afin de publier des informations sur leur activité et permettre aux utilisateurs de se procurer des e-billets) et les villes signeront avec eux les accords nécessaires à la formalisation de la collaboration. La plate-forme pourra également être utilisée dans le cas où une ville souhaiterait mettre à la disposition de ses habitants des billets gratuits pour une activité culturelle. Ce modèle permettra de mettre en place des partenariats qui prennent en compte les intérêts (réduction des coûts, facilité de déploiement, etc.) des différentes parties prenantes. Les organisateurs de petits événements seront alors en mesure de proposer un système de billettique mobile malgré les moyens financiers limités dont ils disposent.

1.2.3.4 *Museum Quest*

Museum Quest est une application mobile qui permet à un utilisateur muni d'un téléphone mobile NFC de participer à une quête culturelle dans un musée donné. La quête prend la forme d'une suite de questions auxquelles il s'agit de répondre afin de progresser dans le jeu. Les questions et les réponses correspondant portent principalement sur l'art et la culture. Un des objectifs est d'améliorer le caractère ludique des visites de musées, en particulier pour les jeunes. Le concept d'une quête culturelle associée à l'utilisation des technologies mobiles les plus récentes est un outil adapté pour attirer le public et plus particulièrement les jeunes dans les musées. Le scénario de la figure 1.21 décrit un cas d'utilisation dans lequel un utilisateur s'inscrit pour participer à une quête. A l'intérieur du musée, le participant lance l'application mobile qui affiche sur l'écran du téléphone portable les questions auxquelles il doit répondre. En cas de difficulté pour fournir une réponse, il approche le téléphone d'un tag NFC afin d'obtenir un indice concernant la question posée. L'utilisateur se sert également de l'application mobile pour contacter des

personnes qui peuvent l'aider à répondre à certaines questions de la quête.

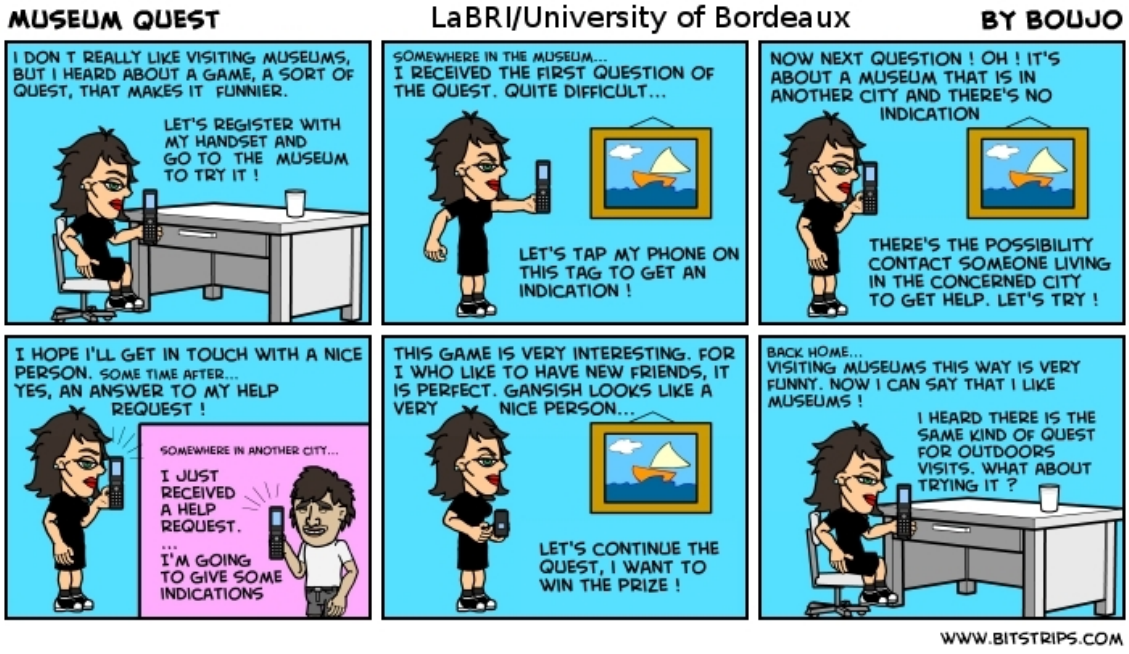


Figure 1.21 – Scénario d'utilisation pour la Museum Quest.

Comme le montre l'architecture présentée figure 1.22, le prototype de l'application mobile comporte pour le moment deux processus : le processus de réponse aux questions et le processus de récupération des indices. Dans le processus de réponse aux questions, l'application mobile propose une interface utilisateur qui facilite les interactions qui ont lieu pendant la quête. Cette interface comprend les éléments d'affichage des questions et des indices correspondant ainsi que ceux de saisie des réponses. Il est à noter que l'application embarque l'ensemble des questions, des réponses et des indices. Ce choix signifie qu'il n'est pas nécessaire d'accéder à un serveur distant durant le jeu et donc, toutes les opérations se déroulent en "local" c'est à dire au sein de l'application. Ce mode de fonctionnement *offline* permet à l'application d'avoir une bonne réactivité quant au contenu à afficher et à traiter en fonction des actions de l'utilisateur. Il est également utile de préciser que les questions de la quête sont de type QCM (Question à Choix Multiples) avec une seule réponse correcte et les indices prennent la forme de contenus multimédia (image, audio ou vidéo). Dans le processus de récupération des indices, lorsque le téléphone mobile est approché d'un tag NFC l'application mobile lit le code qui y est inscrit. Ce code sert à sélectionner, parmi les éléments multimédia disponibles dans l'application, l'indice à présenter en fonction de la question. L'utilisation de la technologie NFC (technologie sans fil de très courte portée) oblige les participants à se trouver physiquement près des œuvres exposées afin d'obtenir des indices au sujet des questions difficiles qui leur sont soumises durant le jeu. On les incite ainsi à une observation plus attentive des œuvres concernées.

Concernant l'implémentation, l'application mobile a été développée en ciblant les Samsung Nexus S équipés de la version 2.3.4 du système Android. La plate-forme Android fournit des APIs qui permettent de lire le contenu d'un tag NFC. Elle propose aussi un ensemble d'outils de développement pour concevoir des interfaces graphiques adaptées aux

téléphones mobiles les plus récents (gestion des écrans tactiles, saisie de texte, affichage d'images, lecture de vidéos).

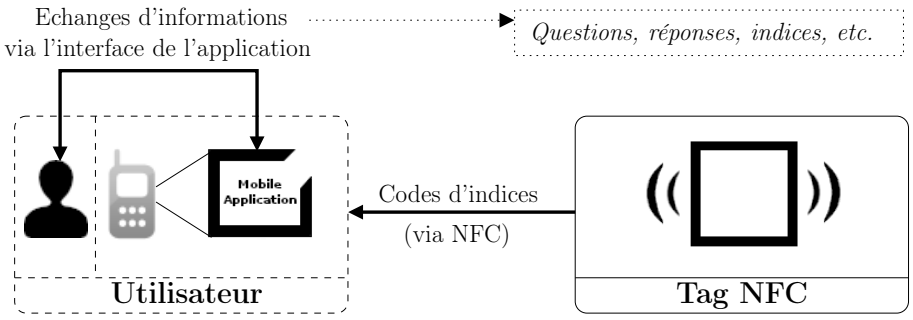


FIGURE 1.22 – Architecture du prototype de Museum Quest.

Les différentes étapes dans le fonctionnement du prototype peuvent donc être résumées de la façon suivante : l'utilisateur se rend au musée et lance l'application mobile sur son téléphone portable ; une première question qui concerne une ou plusieurs œuvres exposées s'affiche sur l'écran du téléphone (figure 1.23) ; si l'utilisateur connaît la réponse il la donne alors via l'interface graphique de l'application ; si au contraire l'utilisateur a besoin d'indications il se rend à l'endroit où se trouve le tag NFC qui correspond à la question posée pour récupérer un indice (l'utilisateur approche son téléphone du tag et le code de l'indice est transféré à l'application qui présente les indications sous forme d'image, de son ou de vidéo) ; lorsqu'une réponse correcte est entrée l'utilisateur progresse dans la quête en passant à la question suivante. Le processus se répète ainsi jusqu'à la fin du jeu ou jusqu'à ce que l'utilisateur y mette un terme.

FIGURE 1.23 – Capture d'écran du prototype de Museum Quest.

Museum Quest a fait l'objet d'un déploiement au sein du Musée de Normandie à Caen pour une quête consacrée à Guillaume le Conquérant. Des extensions du prototype actuel sont en phase de conception afin d'y inclure un module qui permettrait à un utilisateur de demander de l'aide à d'autres participants (comme cela a été présenté dans le scénario de la figure 1.21). Il serait alors possible pour des joueurs se situant au même endroit ou dans des musées différents d'échanger des messages pour s'entraider au cours de la quête.

Chapitre 2

Contexte théorique

Sommaire

Les matériels mobiles existant et les téléphones mobiles en particulier, peuvent être équipés de différentes technologies sans fil qui augmentent et diversifient leurs capacités de communication. La figure 2.24 montre un téléphone mobile capable d'utiliser une gamme de moyens de communication comprenant non seulement des technologies de très courte portée du type NFC mais aussi des technologies de plus longue portée comme le Wi-Fi ou la 3G. L'utilisation combinée et efficace de ces technologies, tout en offrant des possibilités variées et accrues en termes de services et d'applications, requiert la réalisation d'analyses fines en matière de sécurité et de choix du mode de communication à utiliser en fonction de critères dépendant du contexte (coût énergétique, coût financier, préférences des entités

impliquées, préservation de la vie privée, etc). L'accent, dans la manière de communiquer, est donc mis sur les moyens de transmission les plus appropriés que deux ou plusieurs équipements mobiles ont la possibilité d'utiliser lors de leurs échanges. Les critères considérés définissent ainsi une approche dans laquelle la distance de communication n'intervient plus vu des utilisateurs et des services considérés, elle est masquée durant les échanges. La localisation des cibles est alors elle aussi transparente. Dans cet environnement où toutes les entités sont, en permanence, en mouvement en raison de leur nature mobile, une des questions qui se pose et que nous avons choisie d'étudier est la suivante : comment permettre à un ensemble de terminaux mobiles, et à des téléphones portables en particulier, de communiquer, de façon sécurisée, en utilisant la technologie la plus adaptée en fonction du contexte ? Notre objectif est de proposer une réponse à cette question en définissant une plate-forme multi-niveaux [1], prenant en compte les différentes technologies disponibles sur les terminaux et permettant un échange sécurisé de messages. Il s'agit de définir l'ensemble des éléments, théoriques et pratiques, à prendre en compte dans la conception de la plate-forme, de modéliser ces éléments, de développer des applications de référence et de valider la pertinence des solutions proposées par des tests, des évaluations qualitatives et quantitatives.

Avant de présenter une modélisation du problème et la première approche envisagée pour le résoudre, il est nécessaire d'examiner la définition, les spécificités et les problèmes liés aux MANets (Mobile Ad hoc Networks) qui constituent l'environnement cible de la plate-forme multi-niveaux que nous proposons.

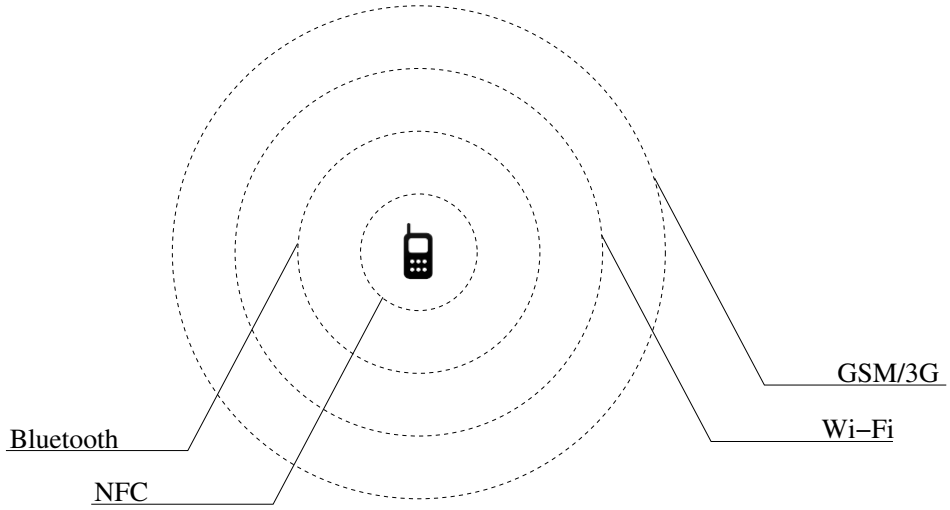


FIGURE 2.24 – Exemple de technologies de communication d'un téléphone mobile.

1. Le choix du terme *multi-niveaux* sera expliqué plus loin.

2.1 MANets

2.1.1 Présentation générale

Les MANets sont constitués d'un ensemble de dispositifs mobiles (ou nœuds) qui sont en mesure de communiquer spontanément les uns avec les autres par le moyen de technologies sans fil et sans aucune infrastructure préexistante. Les configurations pour initier des communications entre les différents dispositifs mobiles se font à la volée et de façon totalement décentralisée. Chaque dispositif mobile considéré dans un MANet peut directement communiquer avec le ou les nœuds qui sont situés dans la zone de transmission radio couverte par la technologie utilisée. L'exemple de la figure 2.25 présente les différentes possibilités de communication directe offertes à des nœuds en fonction de leurs positions et de leurs zones de transmission radio. Nous avons les situations suivantes :

- le nœud 2 se trouve à portée du nœud 1, ce dernier peut lui envoyer un message mais l'inverse n'est pas vrai ;
- les nœuds 3 et 4 se trouvent à portée l'un de l'autre et peuvent donc échanger des messages ;
- le nœud 5 est isolé et ne peut communiquer avec aucun autre nœud du réseau.

Un autre élément caractéristique des MANets est leur appartenance à la famille des réseaux dynamiques qui sont des réseaux au sein desquels la topologie (i.e. l'architecture du réseau en fonction de la position des différents nœuds) change très fréquemment. En effet, les

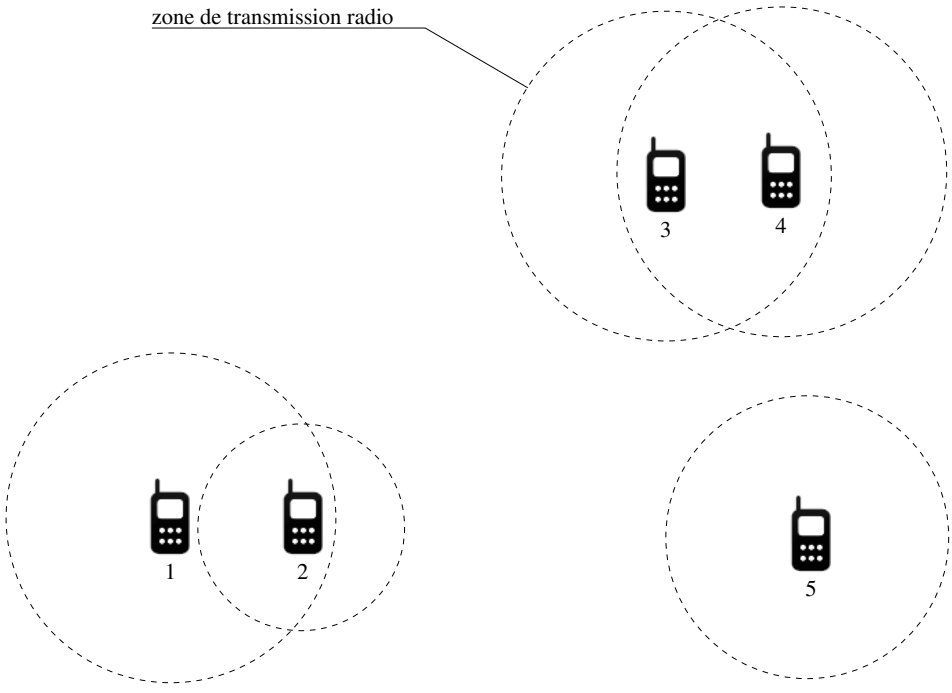


Figure 2.25 – Possibilités de communications au sein d'un MANet.

appareils au sein d'un MANet, en raison de leur caractère mobile, peuvent se déplacer, apparaître et disparaître, ce qui conduit à des modifications de la topologie du réseau. La figure 2.26 décrit le caractère dynamique d'un exemple de configuration de MANet :

– à l'instant t le nœud 4 est capable de communiquer avec le nœud 3 ;
– à l'instant t' le nœud 4 s'est déplacé et il ne peut plus communiquer avec le nœud 3 mais il est en revanche capable de communiquer avec les nœuds 5 et 6.

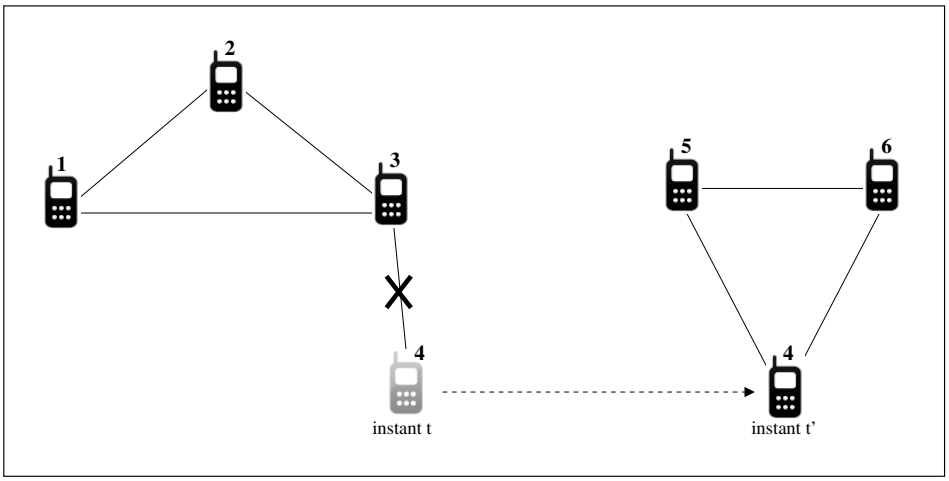


FIGURE 2.26 – Nœuds dans un MANet.

D'après la RFC 2501, *Mobile Ad hoc Networking (MANET) : Routing Protocol Performance Issues and Evaluation Considerations* [26], quatre éléments principaux doivent être retenus dans la caractérisation des MANets. Ces éléments, décrits dans les sections qui suivent, nous permettent également de définir les points à prendre en compte dans le développement et le déploiement des applications qui ont vocation à être exécutées dans le cadre de MANets.

2.1.1.1 Topologie dynamique

La nature mobile des nœuds qui composent les MANets conduit au fait que la topologie du réseau évolue de façon (plus ou moins) fréquente et imprévisible. En d'autres termes, la topologie du réseau est instable et varie donc au cours du temps. Il est nécessaire de prendre en compte cet aspect qui signifie de façon concrète qu'il est pratiquement impossible de garantir que deux nœuds du réseau pourront toujours communiquer directement l'un avec l'autre (même si des communications ont déjà eu lieu entre eux). Les informations qu'un nœud peut posséder concernant son voisinage doivent être régulièrement mises à jour pour (tenter de) demeurer pertinentes.

2.1.1.2 Bande passante limitée et variable

Les liaisons sans fil sont soumises aux interférences que peuvent provoquer par exemple les accès multiples, le *fading* ou le bruit, ce qui réduit le plus souvent leurs capacités en matière de transmission radio. En raison de ces interférences, les débits réels que peuvent atteindre les communications à l'aide de technologies sans fil sont la plupart du temps inférieurs aux taux maximum théoriques. Plus la densité de nœuds est élevée au sein du réseau, plus le risque d'interférence est élevé. Il est donc nécessaire de s'assurer, lorsque cela est possible, de l'acheminement des messages transmis et de prévoir, si possible, des

moyens alternatifs de communication ou des retransmissions dans le cas où des erreurs surviennent.

2.1.1.3 Contraintes énergétiques

Du fait de leur mobilité, les dispositifs qui composent les MANets sont alimentés dans la plupart des cas au moyen de batteries. Par conséquent, les capacités énergétiques des nœuds du réseau sont limitées et économiser l'énergie est un élément primordial. Il est donc nécessaire de prendre en compte ce facteur dans la conception de systèmes exploitant les capacités des MANets. Dans la mesure du possible, les échanges entre les nœuds doivent être minimisés, la duplication d'envoi de messages doit être évitée et l'utilisation des moyens de communication les moins gourmands en ressources énergétiques doit être privilégiée.

2.1.1.4 Sécurité physique limitée

Les communications dans les MANets sont basées sur les transmissions radio. La nature des transmissions radio, même lorsqu'un message a pour destinataire un nœud particulier, ne permet pas d'éviter l'écoute passive. Il est pratiquement impossible d'appliquer une sécurité physique (comme dans le cas de réseaux filaires par exemple) pour empêcher que les ondes radio émises ne soient interceptées. Il est donc nécessaire de prévoir pour les données transmises, dans le cas où les informations échangées entre les nœuds sont sensibles et n'ont pas vocation à être publiques, des mécanismes de sécurisation du type chiffrement et signature. Les clés de chiffrement et les identités associées peuvent être stockées dans des éléments sécurisés ; cette solution est généralement considérée comme étant efficace dans ce type de contexte. Toutefois, les mécanismes de chiffrement et de signature permettent d'envisager d'autres types d'attaques comme le rejeu où une information chiffrée et/ou signée est interceptée au moment de son émission et retransmise plus tard au destinataire initial afin de le tromper. Un autre point à noter concerne les possibilités d'attaques par déni de service. Toutefois, les aspects de décentralisation, de configuration à la volée et de flexibilité (changement de topologie, partage de charge entre entités, etc.) des MANets les rendent plus robustes que les réseaux dits classiques. En effet, au sein des MANets les échanges ne dépendent pas d'un point central qui pourrait être attaqué ou être défaillant empêchant ainsi le fonctionnement du réseau.

2.1.1.5 Bilan

La mise en œuvre des communications au sein des MANets repose donc principalement sur deux éléments à savoir les propriétés des dispositifs mobiles et les caractéristiques des technologies sans fil dont ils peuvent être équipés. Il est donc important d'étudier ces éléments en fonction des quatre points (topologie dynamique, bande passante limitée, contraintes énergétiques et sécurité physique limitée) qui ont été précédemment mentionnés pour concevoir un système adapté.

2.1.2 Quelques axes majeurs de recherche dans le domaine des MANets

2.1.2.1 Le routage

Le routage consiste à acheminer un message, d'un point à un autre dans un réseau, à travers un chemin ou une succession de nœuds à emprunter. Dans l'exemple figure 2.27, le message m est acheminé du nœud 1 vers le nœud 8. Pour définir ce chemin de routage, chaque nœud doit maintenir ce que l'on appelle une table de routage qui permet de déterminer à chaque étape du parcours le nœud vers lequel le message à délivrer doit être relayé afin d'atteindre sa destination finale. Le routage permet de réaliser des communications multi-sauts par opposition aux communications dites "directes" où un nœud contacte directement l'entité à laquelle il souhaite adresser un message. Dans le cadre des MANets, la mobilité des nœuds nécessite la mise en place de systèmes de routage particuliers. A cet effet, de nombreux protocoles, qui sont répartis en trois groupes principaux ont été développés. Les trois classes de protocoles de routages dans les MANets sont les suivantes :

- les **protocoles de routage réactifs** dans lesquels lorsqu'un nœud souhaite communiquer avec un autre nœud du réseau, il doit émettre au préalable une requête de type RREQ (Route Request) pour déterminer le chemin que le message doit emprunter jusqu'à destination. Les informations de routage pour acheminer un message sont en quelque sorte déterminées "à la demande" si elles ne figurent pas déjà dans la table de routage du nœud considéré. De façon concrète, la requête RREQ est envoyée aux voisins du nœud initiateur et elle est retransmise de proche en proche jusqu'à atteindre la cible ce qui permet de déterminer le chemin. Le tableau 2.8 donne quelques exemples de protocoles de routage réactifs appliqués aux MANets ainsi que certaines de leurs caractéristiques.
  Il est à noter que le principal inconvénient de ce mode de routage est le délai nécessaire, induit par le processus de découverte des chemins "à la demande", pour initier l'émission d'un message [39]. Ce délai peut être plus ou moins long en fonction de la densité de nœuds dans le réseau et de la localisation de la cible.
- les **protocoles de routage proactifs** dans lesquels tous les nœuds tentent de maintenir dans leur table de routage respective des informations à jour concernant les chemins à destination de chaque nœud du réseau. Cela est réalisé par un échange permanent entre nœuds des informations de routage dont ils disposent. Ce processus permet à chaque nœud de constamment connaître la route pour atteindre une cible particulière. Le tableau 2.9 donne quelques exemples de protocoles de routage proactifs.
  Toutefois, le principal problème des protocoles de routage proactifs se situe dans le nombre élevé de messages qu'il est nécessaire d'échanger pour maintenir à jour les tables de routage des différents nœuds [79]. Cela peut conduire à un surcoût non négligeable, en terme de consommation d'énergie et de bande passante par exemple, pour l'ensemble du système.
- les **protocoles de routage hybrides** qui combinent les propriétés des protocoles de routage réactifs et proactifs. Dans ces protocoles, le réseau est divisé en zones à l'intérieur desquelles le routage est réalisé de façon proactive et les communications entre nœuds situés dans des zones différentes se fait à l'aide de mécanismes de routage réactifs.
  L'un des exemples les plus connus est le protocole Zone Routing Protocol (ZRP)

défini par Haas et al. et soumis à l'IETF [2] en 2002 [40]. Dans le protocole ZRP, les zones sont définies par rapport aux nœuds. Chaque nœud est au centre d'une zone de rayon n où n correspond au nombre de sauts maximum nécessaire pour atteindre une entité de la zone. Au sein de chaque zone, les informations de routage sont déterminées à partir d'un protocole de routage proactif (protocole IARP [42]). Ainsi, chaque nœud peut accéder aux entités de sa zone grâce à des tables de routage maintenues de façon proactive. Lorsqu'un nœud doit atteindre une entité située en dehors de sa zone, il envoie un message de type RREQ aux nœuds frontières (nœuds en bordure de zone). Ces derniers inondent le reste du réseau afin de déterminer le chemin le plus adapté pour atteindre le nœud de destination. Le chemin interzones est ainsi déterminé de façon réactive (protocole IERP [41]).
Comme dans la plupart des protocoles hybrides, le principal problème du protocole ZRP réside dans le choix de la taille des zones. En effet, si la taille des zones n'est pas configurée de manière optimale, les performances de la procédure de détermination des routes d'acheminement des messages seront affectées [8].

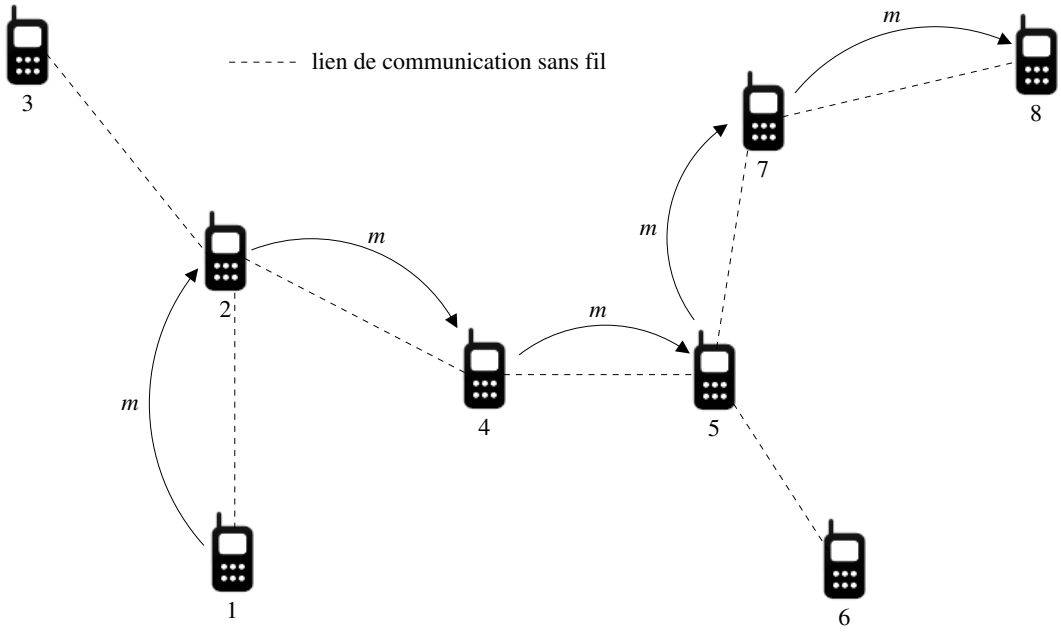


Figure 2.27 – Acheminement d'un message dans un réseau.

Il est important de noter que des facteurs tels que la densité ou la mobilité des nœuds dans le réseau ont un impact sur les performances des protocoles de routage. En effet, comme le montrent Sarkar et Lol dans leur étude [92], ces facteurs ont un effet significatif, en termes de débit réseau et de délai d'acheminement des paquets, sur la plupart des systèmes de routage que nous avons présentés. Par exemple, pour les protocoles OLSR et AODV en particulier, plus la densité de nœuds est grande plus les retards dans la transmission des messages peuvent être élevés. De plus, comme cela est décrit par Nordstrom et al. dans [69], les performances atteintes avec ces différents protocoles varient en fonction des scénarios

2. Internet Engineering Task Force - www.ietf.org/

d'exécution choisis. Elles changent en fonction du type de trafic observé ou en fonction du modèle de déplacement des nœuds. Par exemple, dans des réseaux de petite taille (où le nombre de nœuds est inférieur à 10), selon les expériences réalisées dans [69] et dans un scénario dans lequel la source et la destination d'un message se déplacent toutes les deux pendant les échanges (scénario du *end node swap*), le protocole OLSR obtient de meilleurs résultats que le protocole AODV en matière de débit réseau atteint dans l'acheminement des paquets. Au contraire, dans le cas de figure où un nœud se déplace au sein du réseau et tente d'accéder à une passerelle dont la mobilité est réduite (scénario du *roaming node*), le protocole AODV réalise de meilleures performances que le protocole OLSR.
De façon générale, il est très complexe de prévoir le fonctionnement de protocoles de routage [5] et donc de valider certaines de leurs propriétés au sein de réseaux dans lesquels l'évolution de la topologie n'est pas ou est difficilement prévisible (comme c'est le cas des MANets).

2.1.2.2 La diffusion de messages

La diffusion consiste à transmettre un message à l'ensemble des nœuds du réseau. La méthode classique utilisée au sein des MANets est l'inondation ou *Simple Flooding* [70] qui revient pour chaque nœud, à la réception du message à diffuser, à le retransmettre à tous ses voisins. Le message est ainsi propagé à l'ensemble des nœuds. L'inondation est d'ailleurs utilisée dans certains protocoles de routage afin de transmettre les paquets de type RREQ. Toutefois, l'utilisation de l'inondation comme protocole de diffusion entraîne des surcoûts en termes de messages échangés. Par exemple, à la réception d'un message, un nœud peut être amené à le retransmettre à l'émetteur bien que ce dernier possède déjà l'information. De plus, ce processus de retransmission des messages peut entraîner une boucle infinie dans le protocole de diffusion ; cela peut conduire au phénomène connu sous le nom de *broadcast storm* [68].
Afin d'éviter les problèmes liés au *Simple Flooding*, la stratégie la plus répandue consiste à définir des critères pour choisir les nœuds qui ont la charge de retransmettre les messages à diffuser. Plusieurs méthodes qui peuvent être classées dans les catégories suivantes ont été proposées :

- les méthodes de type *probability-based* [110][2][66] qui utilisent des heuristiques simples. De façon concrète, ces méthodes sont basées sur la prise en compte de paramètres dont les valeurs définissent, suivant des seuils fixés au préalable (souvent déterminés de façon probabiliste), si un message doit être retransmis ou non par un nœud. Les paramètres considérés peuvent être, entre autres, le nombre de paquets transmis avec succès par un nœud ou encore le nombre de doublons reçus par un nœud pour un paquet donné. Il est à noter, en raison de leur caractère heuristique, que le principal problème de ces méthodes se situe dans la définition du seuil optimal à partir duquel les critères de retransmission d'un message doivent être modifiés. Le tableau 2.10 présente des exemples de méthodes qui utilisent l'approche *probability-based*.
- les méthodes de type *area-based* [110][2][66] qui nécessitent l'utilisation d'informations spatiales. Selon le principe général de l'approche *area-based*, un nœud est amené à transférer ou non un message reçu en fonction de sa position ou de la distance qui le sépare des autres entités du réseau. De par leur nature, ces méthodes sont entièrement dépendantes d'une appréciation correcte de la distance qui sépare les nœuds ou

Protocole	**Caractéristiques**
ABR, Associativity-Based Routing [103]	- lorsqu'un nœud reçoit une requête RREQ qui lui est destinée (c'est à dire qu'un autre nœud du réseau souhaite lui transmettre un message), il répond en proposant le chemin le plus stable possible pour l'atteindre en fonction des *associativity ticks* qui existent entre noeuds ; les *associativity ticks* correspondent à la mesure de la stabilité des liens entre les nœuds, en d'autres termes plus deux nœuds ont été voisins sur une longue période plus leur *associativity tick* est élevé
AODV, Ad-hoc On-Demand Distance Vector routing [83]	- quand un nœud reçoit un paquet RREQ, s'il n'est pas la cible du message à envoyer il enregistre l'adresse de l'émetteur avant de le retransmettre, dans le cas contraire il renvoie un message de type RREP à l'émetteur ; lorsqu'un nœud reçoit un paquet RREP si ce dernier ne correspond pas à une requête RREQ qu'il a initiée il le retransmet, dans le cas contraire il envoie le message à expédier à travers le nœud émetteur du paquet RREP, le message est ainsi acheminé jusqu'à destination en suivant le trajet inverse de celui du paquet RREP - ce protocole est décrit dans la RFC 3561 [82]
DSR, Dynamic Source Routing [52]	- après avoir déterminé une route vers une cible du réseau par l'envoi d'une requête RREQ, le nœud émetteur inscrit dans l'en-tête du message à acheminer le chemin complet à emprunter jusqu'à destination avant de l'expédier ; lorsqu'un lien est découvert indisponible durant le parcours, le nœud au niveau duquel le paquet se situe est chargé de déterminer un nouveau chemin à inscrire dans l'en-tête du message afin que ce dernier puisse être acheminé - ce protocole est décrit dans la RFC 4728 [51]

Table 2.8 – Exemples de protocoles de routage réactifs.

Protocole	**Caractéristiques**
FSR, Fisheye State Routing [80]	- les fréquences de mises à jour des informations des tables de routage dépendent de la distance (en nombre de sauts) qui sépare les nœuds ; plus le nombre de sauts qui existent entre une entité et le nœud considéré est élevé, moins la fréquence de mise à jour des informations concernant le chemin pour l'atteindre sera élevée.
OLSR, Optimize Link State Routing [49]	- des nœuds spéciaux appelés MultiPoint Relays (MPRs) sont chargés de retransmettre les messages que l'on souhaite diffuser à tous les nœuds du réseau ; dans le processus de maintenance des tables de routage seuls ces MPRs sont autorisés à transmettre les informations de routage disponibles et qu'ils ont reçues des autres nœuds. - ce protocole est décrit dans la RFC 3626 [25].
TBRPF, Topology Dissemination Based on Reverse-Path Forwarding routing [9]	- une adaptation de l'algorithme de Dijkstra est utilisée pour déterminer le chemin le plus court (en nombre de sauts) entre deux nœuds ; chaque nœud met ainsi à jour périodiquement sa table de routage avec les plus courts chemins vers les nœuds du réseau qu'il peut atteindre ; chaque nœud partage également avec ses voisins les informations pertinentes dont il dispose dans sa table de routage. - ce protocole est décrit plus en détails dans la RFC 3684 [71].
B.A.T.M.A.N., Better Approach To Mobile Ad hoc Networking [67]	- chaque nœud envoie de façon périodique à l'ensemble de ses voisins des messages (avec chacun un numéro de séquence unique) de type OGM (originator message) ; lorsqu'un nœud reçoit un message OGM il le retransmet à l'ensemble de ses voisins ; dans le processus de sélection du chemin à emprunter par un message le nœud émetteur choisit le nœud voisin, pour le premier saut, à partir duquel il a reçu le plus grand nombre d'OGM provenant de la destination à atteindre ; le processus se répète de proche en proche jusqu'à atteindre la cible.

TABLE 2.9 – Exemples de protocoles de routage proactifs.

Méthode	Caractéristiques
Counter Based [68]	- un intervalle de temps appelé RAD (Random Assessment Delay) est considéré au niveau de chaque nœud pour le processus de retransmission (à la réception d'un message à diffuser) ; lorsqu'un nœud reçoit le doublon d'un message à diffuser durant l'intervalle RAD pris en compte, il incrémente un compteur ; si à la fin de la période RAD considérée le compteur a atteint un certain seuil (défini au préalable), la retransmission du message est annulée
Gossiping [68]	- la diffusion suit un principe simple selon lequel un nœud retransmet un message à ses voisins selon une certaine probabilité p, en d'autres termes sur 100 messages reçus un nœud en retransmet $100 \times p$; cette probabilité de retransmission est fixée au préalable, ou évolue en fonction du contexte d'application de la méthode de diffusion ; lorsque la probabilité prise en compte dans le processus de retransmission est égale à 1, la méthode Gossiping est équivalente au *Simple Flooding*

Table 2.10 – Exemples de méthodes de type *probability-based*.

de la précision de la localisation des nœuds. Ce sont des paramètres qui sont difficiles à évaluer dans les MANets. Le tableau 2.11 présente des exemples de méthodes qui utilisent l'approche *area-based*.

– les méthodes de type *neighbor knowledge-based* [110][2][66] qui s'appuient sur les informations que chaque nœud du réseau peut recueillir concernant son voisinage (à un ou plusieurs sauts). A travers les informations recueillies, chaque nœud a une connaissance plus précise de la topologie locale et peut ainsi prendre des décisions quant au transfert des messages à diffuser (comme le présente le tableau 2.12 avec des exemples de méthodes qui utilisent l'approche *neighbor knowledge-based*.). Généralement, les informations de voisinage sont collectées en recevant des paquets de type *Hello* que les nœuds envoient de façon périodique pour signifier leur présence. Il est à noter que les méthodes de type *neighbor knowledge-based* sont sensibles à la forte mobilité des nœuds. En effet, plus les nœuds se déplacent au sein du réseau, plus il est difficile de maintenir les informations de voisinage à jour afin d'avoir une politique adaptée de retransmission des messages.

2.1.2.3 La sécurité des communications

Au sein d'un réseau, la sécurisation des communications permet, entre autres, de protéger les informations et les ressources qui n'ont pas vocation à être publiques, c'est à dire qui ne doivent pas être accessibles à l'ensemble des nœuds. Les exigences suivantes doivent être satisfaites :

– **la confidentialité** qui garantit que seuls les destinataires d'un message peuvent en

Méthode	**Caractéristiques**
DAD, Distance Adaptive Dissemination [24]	- le principe de cette méthode consiste à utiliser la mesure de la force du signal radio reçu pour évaluer la distance entre un émetteur et un récepteur ; chaque nœud définit un seuil S_{tresh} qui correspond au niveau pour lequel il existe k de ses voisins lui ayant envoyé des messages avec une force de signal inférieure à S_{tresh} (le nombre k étant choisi au préalable) ; un nœud procède à une retransmission uniquement si le message à diffuser est reçu via une transmission radio dont la force du signal est inférieure au seuil S_{tresh} défini (le seuil étant choisi pour retransmettre les messages reçus avec une force de signal relativement faible)
OFP, Optimized Flooding Protocol [77]	- il est ici supposé que chaque nœud connaît sa position géographique ce qui lui permet d'évaluer les distances qui le séparent des autres nœuds et chaque message diffusé contient la position de son émetteur ; dans le processus de diffusion, un nœud retransmet un message dans son voisinage uniquement si la distance qui le sépare de son voisin le plus proche est plus grande qu'un seuil Th déterminé au préalable (pour ainsi atteindre les zones relativement éloignées)

TABLE 2.11 – Exemples de méthodes de type *area-based*.

Méthode	**Caractéristiques**
MPR, Multipoint Relays [86]	- chaque nœud connaît une approximation de la liste de ses voisins à 1-saut et à 2-sauts ; en utilisant ces deux listes chaque nœud peut déterminer le ou les voisins à 1-saut qui peuvent servir de relais pour atteindre le plus de nœuds possibles au sein du voisinage à 2-sauts et les en informer ; lorsqu'un nœud reçoit un message à diffuser il ne le retransmet que s'il a été au préalable désigné comme *nœud-relais*
Flooding with Self Prunning [55]	- chaque nœud connaît une approximation de la liste de ses voisins à 1-saut ; lorsqu'un nœud retransmet un paquet à diffuser il inclut dans l'en-tête du message la liste de tous ses voisins à 1-saut dont il a connaissance ; à la réception d'un message à diffuser si la liste de voisins à 1-saut du nœud récepteur contient des nœuds qui ne figurent pas dans la liste de l'émetteur alors le message est retransmis

TABLE 2.12 – Exemples de méthodes de type *neighbor knowledge-based*.

déchiffrer le contenu ; la confidentialité est généralement assurée par le moyen d'outils cryptographiques qui permettent de chiffrer le contenu d'un message afin de le rendre accessible uniquement aux nœuds qui possèdent la ou les clés associées [102] ;
- **l'authentification** qui permet de garantir qu'un nœud malveillant n'a pas la possibilité de se faire passer pour un autre nœud pendant une communication ;
- **l'intégrité** qui permet de garantir que le contenu d'un message n'a pas été modifié par un nœud malveillant ou de façon accidentelle durant son acheminement ; l'intégrité peut être vérifiée en utilisant une fonction de hachage qui permet d'obtenir une *empreinte* de chaque message [102], cette empreinte (éventuellement chiffrée) est ajoutée au message avant son expédition afin que le destinataire puisse effectuer le contrôle d'intégrité ;
- **la non-répudiation** qui interdit à un nœud de nier l'émission d'un message donné ; la non-répudiation peut être assurée à travers une signature numérique (à l'aide d'une clé secrète et propre au nœud considéré) apposée par l'émetteur avant toute émission (le destinataire possédant la clé publique correspondante pour contrôler la signature) [102].

Les caractéristiques des MANets rendent relativement plus difficile la prise en compte de ces exigences. En effet, leur caractère décentralisé conduit à considérer une approche collaborative afin de ne pas dépendre d'une entité unique. De plus, la mobilité et le fait que des nœuds puissent entrer et sortir du réseau de façon dynamique empêchent d'avoir une vision globale de la topologie. Ce manque de vision globale amène à utiliser des solutions de sécurité où seules les interactions locales doivent être considérées.

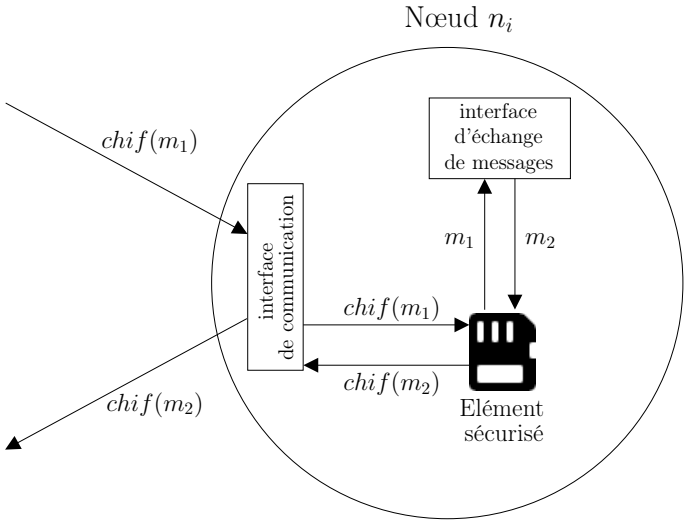


FIGURE 2.28 – Nœud équipé d'un élément sécurisé.

L'une des options privilégiée pour traiter les problèmes de sécurité des communications au sein des MANets consiste à doter chaque nœud du réseau d'un équipement matériel appelé *Secure Element* [3]. Les *Secure Elements* sont des modules (considérés comme) inviolables qui possèdent des capacités cryptographiques et qui offrent un espace de stockage

sécurisé. Dans la plupart des cas, un *Secure Element* est à la fois capable de chiffrer et de déchiffrer des données, de signer un message et de contrôler une signature numérique, ainsi que de vérifier l'intégrité d'une information. Dans l'exemple figure 2.28, le nœud n_i à l'aide de l'élément sécurisé dont il est équipé déchiffre le message $chif(m_1)$ reçu et chiffre le message m_2 à envoyer, ce qui est un moyen de réaliser des communications sécurisées. Un des équipements le plus représentatifs des *Secure Elements* est la carte à puce qui est constituée de circuits intégrés capables de réaliser des calculs et dont le standard est défini par la norme ISO 7816 [48]. Une approche raisonnable, pour gérer la sécurisation des communications au sein des MANets (dans lesquels les nœuds sont généralement considérés comme non sûrs), consiste à utiliser des *Secure Elements* pouvant contenir des outils cryptographiques (clés de chiffrement et/ou de déchiffrement, outils de signature, etc.). De nombreux travaux existent dans le domaine. Les exemples suivants en présentent quelques uns parmi ceux que nous considérons comme les plus significatifs :

- la solution proposée Atallah et Chaumette dans [4] vise à sécuriser les échanges entre nœuds au sein d'un MANet en utilisant une infrastructure distribuée de gestion des identités reposant sur des cartes à puce. Chaque nœud embarque une carte à puce sur laquelle figure une clé publique globale PK_{CA} (commune à tous les nœuds), une clé publique unique PK_i signée avec la clé privée globale SK_{CA} correspondant à PK_{CA} et une clé privée SK_i correspondant PK_i. Un outil qui permet la génération d'identités est également installé sur chaque carte à puce afin de permettre à chaque nœud de générer lui-même une identité liée à la paire de clés uniques PK_i et SK_i. Il est à noter que l'identité ainsi définie est stockée dans la carte à puce du nœud considéré. La création d'identité, qui respecte les critères d'unicité et de permanence (non modifiable une fois générée) en raison de son lien avec la paire de clés uniques (PK_i et SK_i) et du caractère inviolable de la carte à puce, est effectuée au moment de la phase d'initialisation des nœuds.
  Dans le fonctionnement du système, avant d'initier des communications confidentielles, les nœuds doivent au préalable échanger leurs identités respectives. L'échange s'effectue, pour chaque nœud, en envoyant sa clé publique unique PK_i signée par SK_{CA} ainsi que son identité chiffrée avec SK_i aux entités concernées. Deux nœuds qui ont procédé à l'échange de leurs identités respectives peuvent alors communiquer de façon sécurisée en procédant à la signature (avec la clé privée de l'émetteur) et au chiffrement (avec la clé publique du destinataire) des messages avant de les expédier. La robustesse de la solution proposée réside dans le fait que seules des informations à caractère publique (ou dont la divulgation ne pose pas de problème de sécurité à l'infrastructure de gestion des identités) transitent sur le réseau de façon non chiffrée ou sont accessibles sans contrôle.
- la plate-forme présentée par Xu et Čapkundans [112] a pour objectif de permettre une initialisation distribuée et sûre des éléments nécessaires aux communications sécurisées au sein des MANets. Dans le système proposé, des nœuds spéciaux appelés *initiators* (qui appartiennent initialement au réseau MANet considéré) sont équipés de modules matériels inviolables (*Secure Element*) et sont chargés d'admettre, au sein du réseau considéré, les nœuds extérieurs qui remplissent des critères définis (selon les notions introduites dans le papier et qui sont liées à l'objet du réseau à constituer). La solution suppose qu'il existe un canal privé de communication (de bande passante limitée) entre deux nœuds qui se retrouvent à portée l'un de l'autre.

Tout d'abord les *initiators* doivent être configurés. Chaque *initiator* I_i, en utilisant le module inviolable dont il est doté, définit une paire de clés d'autorité unique à savoir (PK_i, SK_i). Cette paire de clés asymétriques sert à certifier ou à contrôler la validité des éléments relatifs à l'identité des nœuds du réseau. Tous les *initiators* sont supposés connaître l'ensemble des PK_i avec $i = 1 \dots l$ (l étant le nombre d'*initiators*). Les *initiators* définissent également, chacun, une paire de clés asymétriques dont la clé publique est certifiée par le SK_i correspondant. Cette paire de clés permet aux *initiators*, quand cela est nécessaire, d'agir comme de simples nœuds (et non pas comme des *initiators*) lors d'échanges à engager. Ensuite, lorsqu'un nœud n qui remplit les critères d'intégration au réseau se retrouve à portée de communication d'un *initiator* I_i, le canal privé qui est constitué sert à échanger des informations de configuration. En effet, si n désire adhérer au réseau, I_i lui attribue un identifiant unique qu'il lui envoie, certifie la clé publique (en utilisant SK_i) d'une paire de clés asymétriques associée à n et lui transmet également l'ensemble des PK_i dont il a connaissance. A partir de cet instant, le nœud n appartient au réseau. Enfin, deux nœuds qui ont au préalable été admis au sein du réseau peuvent initier des communications sécurisées en échangeant leurs clés publiques certifiées. Le contrôle de la certification d'une clé publique reçue est effectué au moyen des PK_i dont le nœud considéré dispose.

2.1.2.4 La gestion de l'énergie

Comme nous l'avons vu dans la description générale des MANets, les nœuds qui composent le réseau sont soumis à des contraintes énergétiques fortes. La consommation énergétique est liée aux communications qui peuvent se produire entre les différents nœuds [38]. Par conséquent pour préserver l'énergie dont chaque nœud dispose, il est nécessaire de réduire, autant que possible, le nombre de messages échangés pour l'accomplissement des tâches visées.

Le modèle de consommation énergétique d'un nœud, en prenant uniquement en compte les aspects communication, peut être décrit plus finement de la façon suivante [30][31][114] :

- trois états sont possibles (figure 2.29), à savoir l'état *émetteur* dans lequel le nœud transmet des messages, l'état *récepteur* dans lequel le nœud reçoit des messages et l'état *en attente* dans lequel le nœud est inactif en ce qui concerne l'émission ou la réception de messages. Ces trois états identifient les modes dans lesquels peut se trouver un nœud pour effectuer des opérations d'émission, de réception ou de contrôle du médium de communication (contrôle de la connectivité ou rejet de paquets qui ne sont pas destinés au nœud considéré par exemple). A chacun de ces trois états correspond un niveau particulier de consommation énergétique.
- l'énergie consommée par un nœud suivant les différents modes de communication est calculée à l'aide de l'équation linéaire $E = m \times taille + b$ [3]. Les variables *taille*, m et b correspondent respectivement à la taille du message contenant l'information, au coût énergétique par unité de message suivant les différents états possibles d'un nœud et au coût énergétique fixe lié à chaque état possible d'un nœud. De plus, il est généralement admis que $E_a < E_r < E_e$ où E_a représente l'énergie consommée

3. Dans l'état *en attente*, il est considéré qu'il n'y a pas de message transmis/reçu au niveau applicatif.

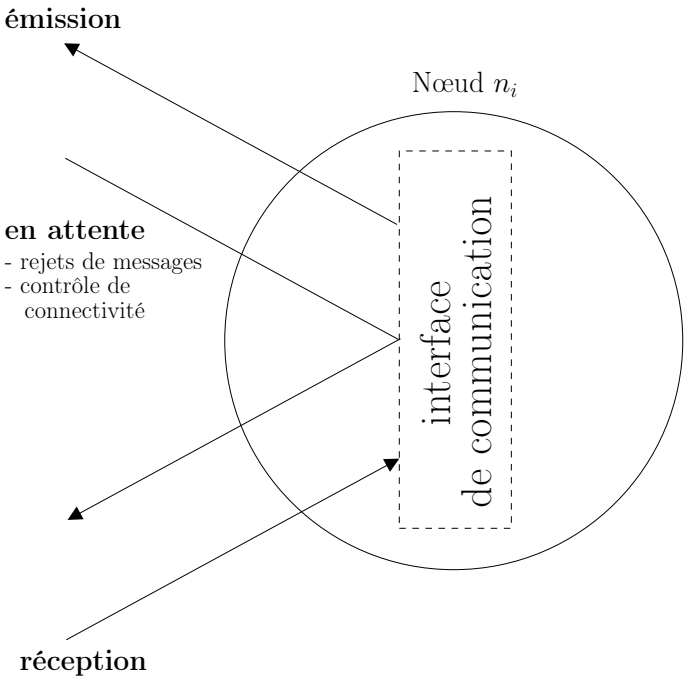


FIGURE 2.29 – États possibles d'un nœud.

dans l'état *attente*, E_r représente l'énergie consommée dans l'état *récepteur* et E_e représente l'énergie consommée dans l'état *émetteur*.

Le modèle de consommation énergétique présenté ci-dessus est utilisé pour appliquer, évaluer ou comparer des politiques de gestion de l'énergie au sein des MANets comme c'est le cas pour les travaux décrits dans [18].

La réduction de la consommation d'énergie passe en particulier par la limitation du nombre de messages échangés au sein du réseau. Il existe, par exemple, des techniques qui visent à éviter la duplication de messages ou à en diminuer légèrement le nombre quitte à perdre un peu de la qualité du service rendu. Ces deux approches, qui nous paraissent pertinentes dans la cadre de la gestion de l'énergie dans les MANets, prennent en compte les éléments suivants :

– dans le cas de la réduction du nombre de duplications de messages, il s'agit d'éviter à un nœud de recevoir/envoyer le même message un nombre trop important de fois. Si l'on considère le problème du point de vue de l'émetteur, la réduction de la duplication permet d'éviter à un nœud d'envoyer un message à une entité du réseau qui l'a déjà reçu, l'opération d'émission étant la plus coûteuse du point de vue énergétique. Les opérations de routage et de diffusion de messages, avec leurs protocoles associés, que nous avons présentés dans la section 2.1.2.1 prennent en compte cet aspect car ce sont des processus qui génèrent (dans la plupart des cas) un nombre conséquent d'échanges de messages. Toutefois, des algorithmes de routage et de diffusion de messages spécialement orientés vers la gestion de l'énergie et dits *energy-efficient* (qui limitent la consommation énergétique) ont été développés. C'est le cas du protocole EOLSR [61] qui est une extension du protocole de routage OLSR (présenté dans le tableau 2.9 page 52) et qui vise à réduire le nombre de transmissions nécessaires pour

atteindre tous les nœuds du réseau dans le processus de recherche de chemins. C'est également le cas du protocole LEAR [111] qui est basé sur le protocole de routage DSR (présenté dans le tableau 2.8 page 51).

– dans le cas de la légère diminution de la qualité du service rendu, il s'agit de définir des stratégies qui permettent à un nœud de décider sous quelles conditions il peut s'abstenir d'émettre certains messages à l'attention de ses voisins. Il est utile de rappeler que les échanges entre nœuds au sein du réseau ont naturellement pour objectif de contribuer à l'accomplissement d'une tâche particulière et, dans ce cadre, les messages non émis ne doivent pas empêcher la réalisation de cette tâche d'une façon qui demeure satisfaisante. En d'autres termes, le concept consiste à accepter une dégradation mineure de la qualité de service au sein d'un réseau dans le but de limiter la consommation énergétique des nœuds (par la réduction du nombre de messages échangés).
  Pour prendre un exemple concret, supposons que le fonctionnement des opérations au sein d'un réseau nécessite que chaque nœud envoie des informations contextuelles le concernant (sa position géographique par exemple) à l'ensemble de ses voisins. Dans le plus simple des cas, la méthode utilisée consiste pour le nœud considéré, à chaque fois qu'un changement de contexte est observé, à transmettre l'information à ses voisins. Or, si un nœud donné du réseau doit émettre des messages à ses voisins en suivant le rythme des modifications des informations contextuelles qu'il peut observer, cela peut induire une consommation énergétique élevée. En effet, les entités qui constituent les MANets sont mobiles ce qui rend le réseau dynamique et donc les changements de contexte de chaque nœud particulièrement fréquents. Une stratégie de réduction de la consommation énergétique pourrait consister à autoriser un nœud à relever ses informations contextuelles à intervalles de temps réguliers et à les transmettre uniquement dans le cas où de nouvelles données (qui apportent un information différente de celles déjà émises) sont disponibles. Une autre stratégie pourrait consister à classifier les informations contextuelles suivant leur pertinence pour les voisins du nœud considéré et à ne transmettre que les données jugées utiles ou appropriées. Les travaux présentés par Föll et al. dans [32] illustrent ces techniques appliquées au développement de protocoles efficaces du point de vue énergétique pour la mise à jour du contexte d'utilisateurs mobiles (localisation, activités effectuées, etc.). Dans ces travaux, les méthodes utilisées permettent d'atteindre un taux de réduction de plus de 80% des messages initialement échangés (dans le cas de la méthode simple où tous les changements de contexte d'un nœud sont retransmis à tous ses voisins) avec une dégradation mineure de la qualité des informations de contexte dont chaque nœud a connaissance. Les travaux de Musolesi et al. dans [65] montrent également qu'il est possible, dans un cadre d'optimisation du processus de collecte et de diffusion des données issues des capteurs des téléphones mobiles, de réduire le trafic des messages échangés de 60% (par rapport à la méthode naïve) tout en préservant un niveau élevé de pertinence des données transmises (environ 80% des données sont utiles par rapport à la masse de l'ensemble des données échangées).
  De façon générale, la légère diminution de la qualité du service rendu afin de préserver les ressources énergétiques des nœuds au sein d'un réseau repose sur deux éléments principaux. Ces deux éléments, qui doivent être étudiés avec attention, sont

la définition des critères à prendre en compte dans la décision d'émission d'un message par un nœud et le contrôle de la qualité de service atteinte afin d'assurer un fonctionnement du système qui satisfasse les besoins des nœuds tout en réduisant le traffic.

2.1.2.5 L'approche opportuniste

La mobilité des nœuds au sein des MANets peut, dans certaines situations, conduire au partitionnement du réseau. En effet, il peut arriver que deux nœuds en mouvement ne puissent plus communiquer directement l'un avec l'autre en raison des limites de la zone de couverture des technologies sans fil dont ils sont équipés, tout en restant à portée de communication d'un groupe différents (pour chacun d'eux) d'autres nœuds du réseau. Dans ces cas, les protocoles classiques de routage et de diffusion de messages sont difficiles à mettre en œuvre entre deux nœuds qui n'appartiendraient pas à la même fraction du réseau du fait que l'application de ces protocoles requiert l'existence d'un chemin entre les nœuds considérés. Une solution pour résoudre ce problème est de considérer l'approche dite *opportuniste* ou DTN (*Delay Tolerant Network*) [81]. Le principe général de cette approche est d'utiliser la mobilité des composantes du réseau et de supposer que des nœuds peuvent se déplacer entre deux sous-réseaux non connectés pour faire transiter les messages et ainsi leur permettre d'atteindre, de proche en proche, leur destination. Cette méthode est connue sous le nom de *store-and-forward* et les nœuds dont la mobilité sert à transmettre des messages sont appelés les *data mules*. L'approche opportuniste suscite beaucoup d'intérêt et un groupe de recherche de l'IETF, le *Delay-Tolerant Networking Research Group* (DTNRG), a d'ailleurs été créé dans le but de concevoir des protocoles (présentés dans la RFC 4838 [17]) répondant aux spécificités des DTNs [10].
La figure 2.30 illustre comment un message peut être transmis dans un réseau partitionné en utilisant la méthode *store-and-forward*. Dans l'exemple présenté, le réseau est divisé en deux parties. Le nœud 1 doit transmettre un message m_i à destination du nœud 6. A l'instant t_{n-1}, le nœud 1 se trouve à portée du nœud 4, qui est une *data mule*, et il lui transfère le message m_i. Le nœud 4 stocke le message m_i puis se déplace au sein du réseau pour se retrouver, à l'instant t_n ($t_n > t_{n-1}$), à proximité du nœud 6. Le message m_i est alors transmis par le nœud 4 au nœud 6. Le message m_i a ainsi pu être acheminé entre les nœuds 1 et 6 malgré le partitionnement du réseau.
Les principales caractéristiques de l'approche *opportuniste* sont les suivantes :

- les délais de transmission sont généralement longs en raison du processus d'acheminement des messages [10][60]. En effet, le processus nécessite que les nœuds se déplacent sur des périodes qui sont plus ou moins longues et, dans certains cas, le passage par plusieurs *data mules* peut être nécessaire pour faire transiter un message entre la source et la destination.
- il est pratiquement impossible de fournir des garanties quant à l'acheminement des messages vers une destination donnée [10][60]. En effet, si une *data mule* ne rencontre jamais le destinataire ou un relais dans le processus d'acheminement, le message ne pourra pas être transmis. La mobilité (imprévisible) au sein d'un réseau qui peut même être parfois partitionné ne permet pas de certifier que les rencontres entre nœuds (nécessaires au transfert des messages) vont s'effectuer. Un message peut ainsi circuler dans le réseau sans jamais pouvoir être remis à son destinataire.

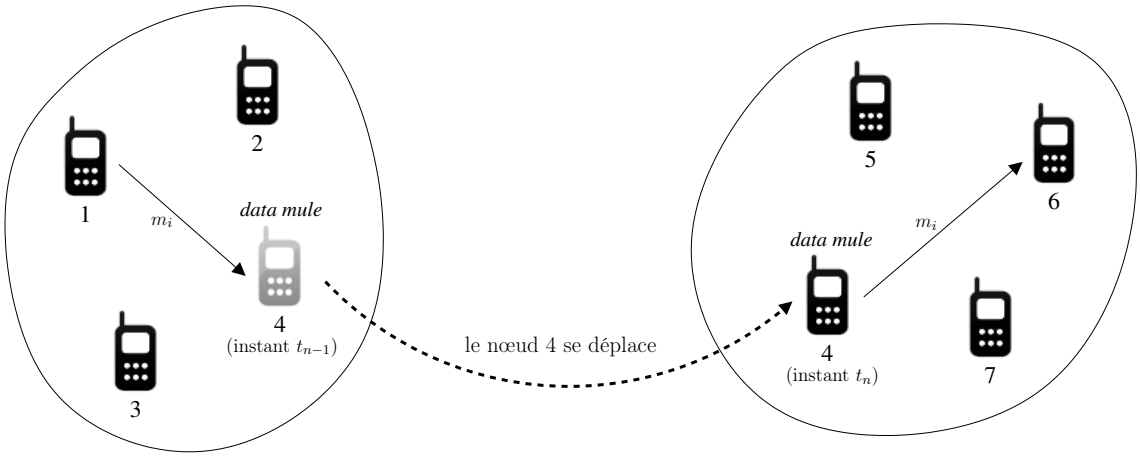


FIGURE 2.30 – Exemple d'acheminement de message dans l'approche opportuniste.

La démarche classique dans l'approche opportuniste consiste à permettre à chaque nœud de jouer le rôle de *data mule* [106]. Ainsi, chaque nœud transmet les messages qu'il transporte aux autres nœuds rencontrés au cours de ses déplacements. Cette démarche pose des problèmes en terme d'encombrement du réseau et de capacité de stockage [54]. En effet, le fait que chaque nœud transmette les messages dont il a connaissance au hasard des rencontres qu'il effectue peut générer un niveau élevé (en fonction de la taille du réseau) d'échanges d'informations entre nœuds. Ainsi, si chaque nœud est dans l'obligation de conserver tous les messages qu'il reçoit lors de ses différentes rencontres (avant éventuellement de les transmettre à leurs destinataires respectifs), les limites de capacité de stockage de l'équipement mobile considéré peuvent être rapidement atteintes. Des travaux ont été menés dans le but de développer des techniques opportunistes de transmission de données qui permettent de réduire l'impact des problèmes mentionnés. Les deux principes généralement utilisés, dans la recherche de solutions (opportunistes) plus efficaces, sont les suivants [60] :

- le principe du transfert de messages axé sur la destination à atteindre. Il s'applique dans le cas où un message est destiné à un (ou plusieurs) nœud(s) spécifiques. Les différentes interactions (opportunistes) entre nœuds doivent donc permettre au message d'atteindre la ou les destinations considérées. En d'autres termes, en fonction des informations recueillies au niveau des entités rencontrées (nœuds avec lesquels des échanges ont déjà eu lieu ou zones déjà visitées par exemple), un nœud peut décider à qui transmettre (ou ne pas transmettre) un message pour espérer atteindre la ou les destinations cibles.
- le principe de la diffusion de l'information axée sur le contenu proposé. Selon ce principe, les contenus sont échangés entre les nœuds suivant les différentes sollicitations reçues. En d'autres termes, suivant ses intérêts et ses préférences, un nœud envoie des requêtes aux autres nœuds qu'il rencontre lors de ses déplacements afin d'obtenir les informations recherchées.

Comme nous l'avons déjà noté, l'approche opportuniste n'offre aucune garantie quant à l'acheminement d'un message entre un émetteur et un destinataire. Par conséquent, le principe de la diffusion de l'information axée sur le contenu apparaît comme étant le plus

adapté pour fournir des solutions efficaces dans ce contexte [60]. Ce principe offre des avantages : il n'est pas nécessaire de spécifier une destination pour un contenu à partager et le choix pour un nœud de stocker et proposer un contenu peut se faire selon ses propres intérêts. Nous présentons donc, dans la suite, des exemples de techniques qui ont été proposées dans le cadre diffusion de l'information axée sur le contenu.

Dans l'exemple présenté par Bissyandé et al. dans [12], un système opportuniste de mise à jour d'applications mobiles est proposé. Chaque nœud du réseau sur lequel est installé un certain nombre d'applications mobiles diffuse régulièrement à son voisinage la liste des *patchs* de mise à jour dont il dispose. Chaque nœud possède également une table qui contient les informations reçues (nœud émetteur et version du *patch*) concernant les *patchs* disponibles. De façon périodique, chaque nœud recueille les caractéristiques des *patchs* portés par les nœuds qu'il croise et ce pendant un certain laps de temps. Les données obtenues durant la période considérée vont permettre au nœud d'enrichir le contenu de sa table d'informations afin de prendre la meilleure décision possible quant au *patch* qui peut répondre à ses besoins (en fonction de la version courante de l'application à mettre à jour). Ce *patch* est alors demandé par le nœud considéré au voisin qui le possède (sous réserve que ce dernier soit toujours présent). Les nœuds ne diffusent donc pas tous les *patchs* de mise à jour dont ils disposent (mais uniquement les détails concernant ces *patchs*), les *patchs* sont plutôt transmis aux nœuds qui en font explicitement la demande en fonction de leurs propres critères. Les évaluations conduites montrent que la sélection du meilleur *patch* disponible pour un nœud à un instant donné est fonctionnelle dans un contexte de traces réelles de mobilité humaine.

Dans le protocole présenté par Haillot et Guidec dans [43], la diffusion de l'information, réalisée de façon opportuniste, s'appuie sur la différenciation entre les contenus à transmettre. Dans le système proposé chaque nœud dispose de certaines informations à partager et souhaite en recevoir de nouvelles. Toutes les informations disponibles possèdent chacune un identifiant unique et sont accompagnées d'un ensemble de mots-clés et d'éléments descriptifs (type, éditeur, date de publication, etc). Chaque nœud se construit également un profil qui contient une description du type d'informations recherchée. Les interactions au sein du réseau se basent sur le principe suivant : chaque nœud diffuse de façon périodique à son voisinage son profil ainsi qu'un catalogue regroupant les informations dont il dispose et qui pourraient être utiles à ses voisins (en fonction des profils qu'il a au préalable reçus). Si un nœud reçoit un catalogue où figurent des informations intéressantes, il lance une requête à l'émetteur. Lorsqu'un nœud reçoit une telle requête et qu'il peut la satisfaire, il diffuse à l'ensemble de son voisinage l'information requise. Ainsi, lors des rencontres entre nœuds ce sont uniquement les informations explicitement demandées qui sont diffusées. Les résultats obtenus dans les simulations effectuées montrent que le protocole peut être utilisé dans un contexte réaliste.

Les techniques opportunistes, comme nous l'avons vu, exploitent les possibilités de communication offertes par la mobilité des nœuds. A ce titre et même si certaines garanties ne peuvent pas être fournies (notamment dans l'acheminement de messages entre deux points), ces techniques, et plus particulièrement celles privilégiant l'approche orientée contenu, apparaissent réalistes dans l'environnement caractéristique des MANets.

2.2 Modélisation du problème

2.2.1 Description du problème

Comme nous l'avons noté dans l'introduction de ce chapitre (figure 2.24 page 44), les téléphones mobiles sont équipés (pour certains d'entre eux) de plusieurs types de technologies sans fil ce qui augmente leurs capacités en terme de moyens de communication. Pour tirer parti de l'utilisation combinée de ces technologies, et proposer des services et des applications mobiles efficaces, il est nécessaire de définir une méthode, se basant sur des critères précis (par exemple la consommation énergétique, le coût financier ou encore les aspects de confidentialité), qui permette de sélectionner le type de technologie adaptée au contexte.
Dans le cadre du projet SUS [web30], les caractéristiques multi-technologiques (sans fil) des téléphones portables ont été étudiées. Par exemple, une extension de l'application Museum Quest (présentée section 1.2.3.4 page 38) qui autorise les participants de la quête à interagir entre eux, en considérant les caractéristiques multi-technologiques des équipements utilisés, a été proposée. Pour rappel, le principe de Museum Quest, qui est un jeu culturel, est de permettre aux joueurs de répondre, à l'aide d'une application mobile, à une série de questions disséminées dans un musée donné. Dans l'extension proposée, en cas de difficulté pour répondre à une question, le joueur peut choisir de contacter d'autres participants (qui peuvent être dans son voisinage immédiat ou non) dont le profil (cette notion sera définie plus loin) suggère qu'ils sont en mesure de répondre au problème posé. Ainsi, l'extension doit offrir à chaque joueur la possibilité : (i) de découvrir à la volée des participants qui peuvent lui être utiles, et (ii) de déterminer la meilleure technologie sans fil à utiliser pour les contacter (Bluetooth, Wi-Fi, GSM, 3G, etc.) La figure 2.31 montre les différentes interactions entre joueurs qui se situent dans des musées différents (site A et site B) ou entre joueurs qui se trouvent à proximité (environnement local) les uns des autres. Dans l'exemple présenté, le joueur 1, tout en essayant d'entrer en contact avec des joueurs de son site pour certaines questions, peut aussi avoir besoin de communiquer avec le joueur 2 qui se situe sur un site distant. Cette évolution possible de l'application Museum Quest illustre, de façon pratique, l'utilisation qui peut être faite des différentes technologies sans fil des téléphones portables.

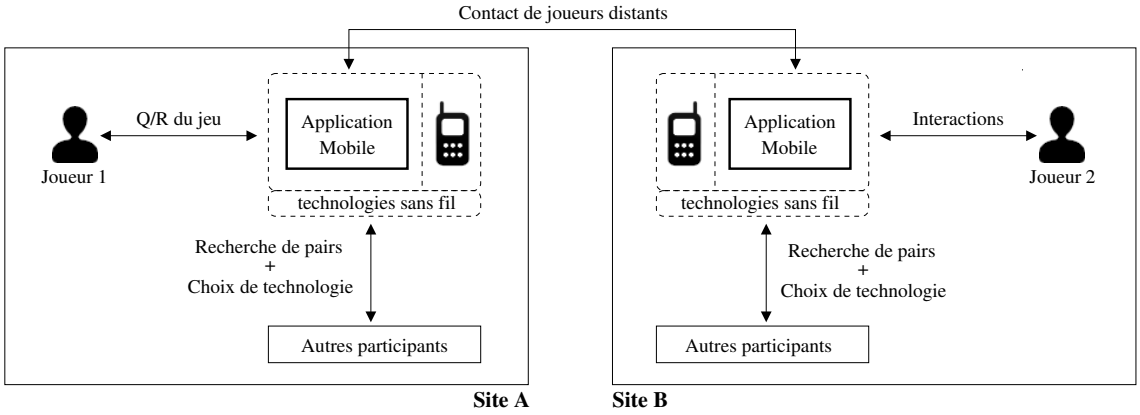


Figure 2.31 – Extension de l'application Museum Quest.

La question principale est donc de savoir comment permettre à un ensemble de téléphones portables de communiquer en utilisant la technologie la plus appropriée en fonction du contexte ? Afin de contribuer à la résolution de ce problème, notre objectif est de concevoir une plate-forme multi-niveaux qui prenne en compte les caractéristiques multi-technologiques (sans fil) d'entités mobiles dans un MANet et qui permette l'échange sécurisé (pour des aspects de confidentialité) de messages entre entités suivant le moyen de communication le plus adapté. Pour mieux appréhender les contours du problème que nous posons, il est nécessaire de le présenter sous une forme qui permette de détailler tous ses aspects. Il s'agit donc de schématiser le fonctionnement de la plate-forme en prenant en compte l'environnement caractéristique des MANets. Dans notre cas et dans le modèle à définir, les nœuds mobiles du réseau sont des téléphones portables. En fonction des éléments que nous avons pu étudier concernant les MANets, il nous semble pertinent de prendre en compte les aspects suivants dans la modélisation de notre plate-forme :

- les noeuds se déplacent au sein du réseau et la mobilité de chaque nœud est difficilement prévisible (caractère dynamique des MANets) ;
- le routage pour acheminer des messages ne sera pas une solution considérée et ce en raison des difficultés à le mettre en œuvre dans le contexte des MANets (changements fréquents dans la topologie du réseau), et les échanges entre nœuds doivent donc avoir lieu de façon directe (communications en mode *peer-to-peer*) ; l'approche opportuniste doit être privilégiée afin de proposer des solutions adaptées à l'environnement ;
- la sécurité des communications doit être mise en œuvre à l'aide d'approches cryptographiques (par exemple un ensemble de paires de clés asymétriques pour chiffrer/-déchiffrer les échanges) ;
- les échanges de messages doivent être réduits autant que possible et dans certains cas la plate-forme peut tolérer une légère dégradation de la qualité du service fourni dans le but de limiter la consommation des nœuds en énergie.

La figure 2.32 présente un exemple de plate-forme multi-niveaux. Dans cette plate-forme, l'accès à un "bus" correspond à la possibilité pour un nœud d'utiliser une technologie de communication sans fil donnée pour émettre un message. Le terme "multi-niveaux" fait référence au fait que plusieurs niveaux de communication cohabitent, chacun lié à une technologie de communication sans fil avec ses caractéristiques propres (portée, débit, etc.), et sont accessibles aux nœuds suivant les technologies dont ils sont équipés. Dans l'exemple, le système est constitué de six nœuds répartis en deux îlots. En fonction de leurs capacités, les nœuds peuvent faire usage de différents bus. Dans la situation décrite figure 2.32, n_3 est équipé de $Technologie_2$ et $Technologie_3$ tandis que n_5 est équipé de $Technologie_1$ et $Technologie_2$. Les lignes en pointillé à l'intérieur de chaque bus représentent les liens de communication directe qui peuvent être noués entre des nœuds par le moyen de la technologie mentionnée. Les nœuds n_3 et n_4 ont, par exemple, la possibilité de communiquer via $Technologie$ 3. Les ilôts regroupent des nœuds reliés entre eux au sein d'un bus de technologie de courte et moyenne portée. n_1, n_2 et n_3 forment l'$Ilot_A$ car ils peuvent communiquer entre eux via $Technologie_2$. Un autre point important du système, figure 2.32, est l'utilisation de moyens alternatifs pour accéder à un nœud quand une communication directe est impossible. n_1 utilise le canal c_1 pour atteindre l'$Ilot_B$ et le nœud n_5. Il est à noter, si nécessaire, que la figure 3.54 page 128 présente une version plus détaillée du fonctionnement de la plate-forme avec les canaux.

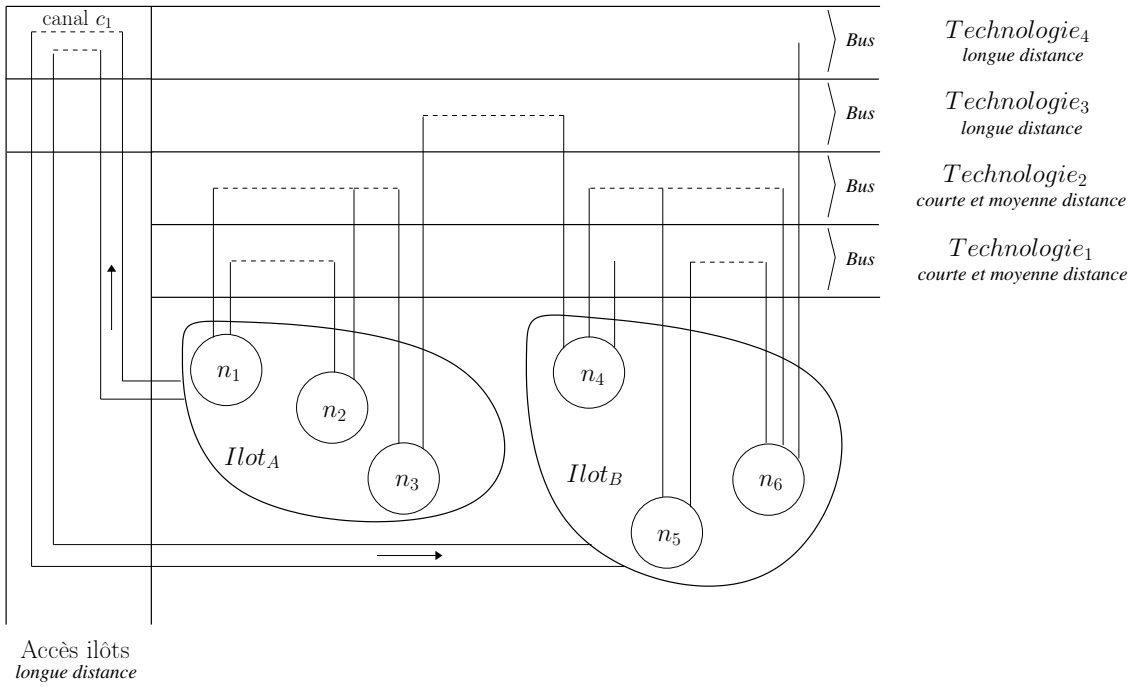


Figure 2.32 – Exemple de plateforme multi-niveaux.

2.2.2 Définitions des éléments à considérer

Nous modélisons le fonctionnement du système, qui est schématiquement représenté figure 2.33, de la façon suivante :

- Soit N l'ensemble des nœuds (terminaux mobiles) du système. N contient les nœuds n_i tels que $i = 1 \dots m$.
- Soit T l'ensemble des technologies sans fil considérées. T contient les technologies t_j telles que $j = 1 \dots u$. T_{n_i} est défini comme étant l'ensemble des technologies dont le nœud n_i est équipé. La fonction *portee* est définie sur T tandis que les fonctions *debit*, *coutE*, *coutF* sont définies sur T_{n_i} de la façon suivante : $portee(t_j)$ = portée maximale de la technologie t_j , $debit_{n_i}(t_j, t)$ = débit de la technologie t_j à un instant t donné pour le nœud n_i, $coutE_{n_i}(t_j)$ = coût énergétique de l'envoi d'un message par la technologie t_j pour le nœud n_i et $coutF_{n_i}(t_j)$ = coût financier de l'envoi d'un message par la technologie t_j pour le nœud n_i. La prise en compte de la notion de temps (instant t donné) est particulièrement significative pour le débit en raison de son caractère fluctuant. Nous choisissons de ne pas le considérer pour les autres fonctions.
  La fonction *adr* est aussi définie sur T de la façon suivante $adr_{n_i}(t_j)$ = adresse de connexion [4] qui permet aux différentes entités du système de communiquer avec n_i via la technologie t_j (si la portée le permet naturellement).
  Quatre relations binaires ($\geq^P$, $\geq^{D_{n_k,t}}$, $\geq^{E_{n_k}}$, $\geq^{F_{n_k}}$) sont également définies de la façon suivante : $\forall (t_i, t_j) \in T \times T, \geq^P (t_i, t_j) \Leftrightarrow portee(t_i) \geq portee(t_j)$, $\forall (t_i, t_j) \in$

4. Nous supposons que cette valeur ne change pas au cours du temps. C'est par exemple une adresse MAC Bluetooth.

$T_{n_k} \times T_{n_k},\ \geq^{D_{n_k,t}}\ (t_i, t_j, t) \Leftrightarrow debit_{n_k}(t_i, t) \geq debit_{n_k}(t_j, t)$ à un instant t donné, $\forall (t_i, t_j) \in T_{n_k} \times T_{n_k},\ \geq^{E_{n_k}}\ (t_i, t_j) \Leftrightarrow coutE_{n_k}(t_i) \geq coutE_{n_k}(t_j)$ et $\forall (t_i, t_j) \in T_{n_k} \times T_{n_k},\ \geq^{F_{n_k}}\ (t_i, t_j) \Leftrightarrow coutF_{n_k}(t_i) \geq coutF_{n_k}(t_j)$.
T possède deux sous-ensembles disjoints T_C et T_L qui sont respectivement l'ensemble des technologies de courte portée et l'ensemble des technologies de longue portée. T_C et T_L sont définis tels que $\forall t_i \in T_L$ et $\forall t_j \in T_C,\ \geq^P\ (t_i, t_j)$ avec $T_C \cup T_L = T$.
Un autre critère de différenciation des éléments de T est le mode de fonctionnement des technologies en terme d'acheminement d'un message. Cet acheminement peut être soit direct soit via des relais. En cas d'utilisation de technologies exploitant des relais, il est nécessaire, pour envoyer un message à un nœud particulier, de connaître à l'avance une information de connexion privée [5] - souvent une adresse - que le nœud considéré ne donne qu'aux entités qu'il juge dignes de confiance : il est en effet impossible pour un nœud, avec ces technologies, de connaître par exploration la liste de tous ses voisins d'où la nécessité d'une connaissance préalable.
Nous prenons en compte ces technologies qui nécessitent l'utilisation de relais, même si de par leur nature elles ne permettent pas des échanges strictement directs entre nœuds, en raison de leur spécificité en matière de portée (très longues distances). L'ensemble T est donc divisé, en prenant en compte ce critère, en deux sous-ensembles disjoints T_{DI} et T_{Re} qui sont respectivement l'ensemble des technologies avec lesquelles un message est acheminé directement entre l'émetteur et le récepteur et l'ensemble des technologies avec lesquelles l'utilisation d'une infrastructure relais est nécessaire dans l'acheminement d'un message.

- Soit $V_{n_i,t_j}(t)$ l'ensemble des noeuds voisins de n_i par la technologie t_j à un instant t donné (dans le cas où il est possible de déterminer les voisins). $\forall n_k \in N,\ n_k \in V_{n_i,t_j}(t)$ si et seulement si n_i peut émettre un message à destination de n_k à l'instant t en utilisant t_j. Nous choisissons de ne pas inclure un nœud dans son propre voisinage.
- Soit E un ensemble de nœuds à un instant t donné. Les nœuds de l'ensemble E sont tous équipés de la technologie t_j. Si $\forall n_i \in E, V_{n_i,t_j} = E - \{n_i\}$ à l'instant t, alors on dit que E est un îlot et on note $E = I_{t_j}(t)$. Chaque nœud n_i de l'îlot $I_{t_j}(t)$ peut donc émettre un message à destination d'un autre nœud de l'îlot par le moyen de la technologie tj. En raison du lien direct existant entre les nœuds qui le composent, $I_{t_j}(t)$ est appelé *îlot physique*.
- Une **passerelle** est un nœud n_j qui sert de relais à un nœud n_i dans le transfert d'un message qui est à destination d'entités situées dans le voisinage de n_j (suivant les technologies dont il est équipé) et auxquelles n_i ne peut (ou ne veut) pas accéder directement. Il est à noter que n_j doit appartenir au voisinage de n_i. Pa est l'ensemble des nœuds qui offrent un service de passerelle.
- Un **site distant** pour un nœud n_i est un îlot non accessible (pour l'envoi de messages) à l'aide d'une technologie t_j telle que $t_j \in T_C$.
- Un **canal** est un moyen alternatif de communication qui permet de mettre en relation deux sites distants. A travers un canal, un nœud peut donc avoir accès à d'autres entités situées sur des sites dits distants et cela sans nécessairement être équipé lui-même d'une technologie de longue portée qui lui permettrait d'accéder directement à ces sites.

5. Par exemple, cette information peut être le numéro de téléphone.

- un **abonnement** représente l'opération, pour un nœud, qui consiste à notifier un canal de son souhait d'utiliser ses services de mise en relation de sites distants.
  C contient les canaux c_k, $k = 1 \dots b$ disponibles dans le système. Un canal c_k est donc un moyen par lequel un nœud n_i peut accéder à une zone (ou site) distante (et communiquer avec l'ensemble de ses nœuds). Le nœud n_i doit avoir au préalable souscrit un abonnement auprès de c_k pour être en mesure d'utiliser ses services. En fonction des circonstances, il est à noter que lorsqu'une information est émise sur un canal donné, elle est soit diffusée à l'ensemble des noeuds concernés du site distant ciblé qui ont souscrit l'abonnement ou alors l'information est sauvegardée afin d'être mise à la disposition des nœuds abonnés du site distant ciblé (mode *push* ou mode *pull*).
- un **îlot virtuel** est un ensemble de nœuds auxquels n_i peut accéder à travers un canal particulier. Chaque nœud est donc lié à un certain nombre d'*îlots virtuels* en fonction des canaux qu'il a la possibilité d'utiliser pour atteindre des sites distants. Si n_i peut accéder à un site distant où se situe un nœud n_j à travers un canal c_k, de même n_j peut accéder au site où se situe le nœud n_i en utilisant le même canal c_k.

Cette modélisation nous permet non seulement de proposer une définition précise de la notion de **nœud** mais aussi de définir le concept de **groupe de nœuds** qui peut en découler et ce de la façon suivante :

- $\forall\ n_i \in N$, n_i se définit comme un triplet contenant un profil individuel, des capacités technologiques, un ensemble d'abonnements et une paire de clés publique/privée RSA. Nous avons donc $n_i = (profil_{n_i}, techno_{n_i}, abo_{n_i}, clePub_{n_i}, clePri_{n_i})$. $profil_{n_i}$ est le profil individuel du nœud n_i qui regroupe un ensemble d'informations relatives à ce nœud. Le profil individuel peut contenir un pseudonyme, une localisation et d'autres éléments optionnels décrivant des caractéristiques spécifiques du nœud considéré. Les attributs du profil d'un nœud peuvent être de plusieurs types. Ils peuvent être soit dynamiques et varier au cours du temps (exemple de la localisation), soit statiques. Ils peuvent également être soit certifiables (par exemple la localisation) et fournis par le système qui certifie ainsi leur valeur à un instant t donné, soit non certifiés (et fournis par le nœud lui-même). La certification éventuelle peut être réalisée en permanence ou de façon intermittente. $techno_{n_i}$ est un sous-ensemble de T regroupant les technologies de communication dont le nœud n_i est équipé, en d'autres termes $techno_{n_i} = T_{n_i}$. Quant à abo_{n_i} il s'agit d'un sous-ensemble de C contenant l'ensemble des abonnements auxquels le nœud n_i a souscrit. $clePub_{n_i}/clePri_{n_i}$ représente la paire de clés publique/privée RSA.
- nous définissons également $kernel_{n_i}$ qui sont les informations minimales (publiques) à publier (pour un nœud n_i) et à rendre visible aux autres nœuds.
  $kernel_{n_i} = (kernelprofil_{n_i}, kerneltechno_{n_i}, clePub_{n_i})$ avec $kernelprofile_{n_i}$ qui est un sous-ensemble de $profile_{n_i}$ et $kerneltechno_{n_i}$ qui comprend une partie de l'ensemble $techno_{n_i}$. Pour être plus précis, $kernelprofil_{n_i}$ correspond aux informations (des compétences particulières par exemple) que n_i juge indispensable de rendre publiques (publier) aux autres entités. Le sous-ensemble $kerneltechno_{n_i}$, quant à lui, contient toutes les technologies et leurs caractéristiques correspondantes (adresse de connexion, portée, etc.) dont n_i est équipé et dont il souhaite rendre les informations publiques. Il est à noter que c'est donc à n_i de définir la ou les technologies (généralement des technologies de l'ensemble T_{Di}) dont les informations de configuration

doivent être mentionnées dans $kernel_{n_i}$.

- nous définissons aussi des **nœuds dits spéciaux** qui possèdent des capacités particulières. Les *nœuds spéciaux* sont des nœuds qui offrent des services de passerelle et de canal aux nœuds de leurs voisinages, c'est à à dire qu'ils appartiennent aux ensembles Pa et C. De plus, les nœuds spéciaux sont liés les uns aux autres par un moyen de communication qui ne figure pas dans l'ensemble T et qui leur permet d'échanger des informations de façon sécurisée. Chaque *nœud spécial* est associé à un site qui représente une zone délimitée de l'espace des nœuds ce qui signifie en d'autres termes que le *nœud spécial* en question se déplace uniquement dans la zone correspondant au site. En raison de leurs propriétés, les *nœuds spéciaux* sont également des entités qui permettent au système de certifier la valeur de certains attributs du profil des autres nœuds (la localisation en l'occurrence). A l'image des nœuds basiques du système, les *nœuds spéciaux* possèdent chacun un profil individuel, des capacités technologiques et un ensemble d'abonnements.
- une **zone** représente un espace géographique limité dans lequel un certain nombre de nœuds peuvent se déplacer (par exemple, dans le cas de l'application Museum Quest, la zone est l'espace du musée considéré). C'est un site distant pour les nœuds qui ne s'y situent pas.
  Nous notons S l'ensemble des *nœuds spéciaux* ($S \subset N$). Un élément de S s'écrit sous la forme $n_i^{zone_r}$ avec $zone_r$ qui représente le site auquel le nœud est associé (avec $i = 1 \dots u$ et $r = 1 \dots v$).
- le concept de **groupe de nœuds** est caractérisé par la notion de profil de groupe. Un profil de groupe contient un ensemble d'attributs communs présents dans les profils des nœuds composant le groupe. Un groupe $G_{profilA}$, dans notre contexte, est un sous-ensemble de N tel que : $\forall\, n_i \in N, n_i \in G_{profilA} \Leftrightarrow profilA \subset profil_{n_i}$. $profilA$ est l'ensemble des attributs et des informations caractéristiques que partagent les nœuds du groupe. Il est à noter qu'un groupe peut être constitué d'un seul nœud. La figure 2.34 présente une vue de la notion de groupe dans l'espace des nœuds.

Le tableau 2.13 résume l'ensemble des éléments introduits pour modéliser l'environnement dans lequel la plate-forme multi-niveaux doit évoluer. Ces éléments, qui sont répartis en fonction de leurs caractéristiques, permettent de donner les premiers détails de l'approche que nous proposons pour le fonctionnement du système à développer.

2.3 Premiers éléments de l'approche proposée

Le système se compose d'un ensemble de nœuds équipés de certains types de technologies sans fil (de courte, moyenne et longue portée). L'objectif est de permettre à ces nœuds, dans la mesure du possible, d'échanger directement des messages sans que cela ne nécessite un passage par un ou plusieurs relais mis à part les cas où un abonnement est utilisé. Le mode *peer-to-peer* virtuel (vu comme du *peer-to-peer* classique par l'utilisateur final même si la mise en œuvre par la plate-forme multi-niveaux nécessite des rebons successifs), sans procédure classique de routage, est donc privilégié dans le sens où aucun chemin (succession de nœuds) par lequel un message à émettre devrait transiter n'est au préalable déterminé dans les échanges qui ont lieu. Il s'agit d'envois directs d'un nœud émetteur vers un nœud destinataire. De même, dans la situation où l'utilisation d'un abonnement est nécessaire,

-	**Ensemble N des nœuds**	**Ensemble T des technologies**	**Ensemble C des canaux**
Éléments	- n_i avec $i = 1 \dots m$	- t_j avec $j = 1 \dots u$	- c_k avec $k = 1 \dots b$
Sous-ensembles	- V_{n_i,t_j}, voisins de n_i par t_j - Pa, ensemble des nœuds passerelles - $G_{profilA}$, groupe de nœuds avec $profilA$ - S, ensemble des nœuds spéciaux	- T_C, technologies de courte portée - T_L, technologies de longue portée - $T_{n_i} = techno_{n_i}$, technologies de n_i - T_{DI}, technologies directes - T_{Re}, technologies via relais	- abo_{n_i}, ensemble des abonnements de n_i
Fonctions		- $portee(t_j)$ - $debit_{n_i}(t_j, t)$ - $coutE_{n_i}(t_j)$ - $coutF_{n_i}(t_j)$ - $adr_{n_i}(t_j)$, adresse de connexion à n_i par t_j	
Propriétés	- $profil_{n_i}$, profil de n_i - $clePub_{n_i}$, clé publique de n_i - $clePri_{n_i}$, clé privée de n_i - $kernelprofil_{n_i}$, sous-ensemble de $profil_{n_i}$		

Table 2.13 – Résumé des éléments mathématiques du modèle.

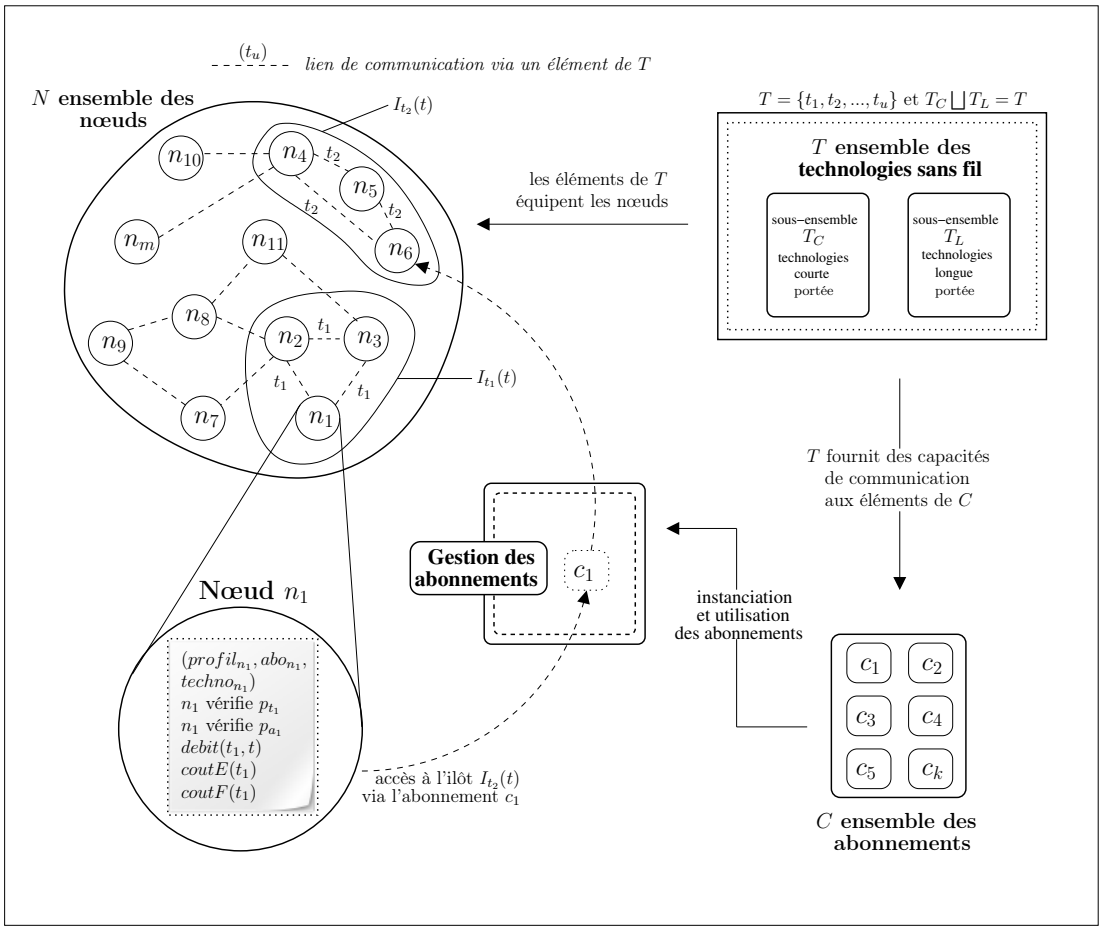


FIGURE 2.33 – Fonctionnement du système - Modélisation.

l'accès au canal qui doit relayer le message à émettre se fait également en mode direct. Dans ce cadre, le système doit non seulement être suffisamment flexible pour prendre en compte les caractéristiques spécifiques de chaque nœud (en fonction de leurs profils) mais aussi assurer la sécurité des communications. La gestion de l'aspect multi-niveaux (choix de la technologie la plus appropriée pour échanger des messages en fonction du contexte) tout en manipulant de façon appropriée les données personnelles des nœuds fait également partie des exigences auxquelles le système doit répondre.

A ce niveau, il est important de noter que le *comportement* d'un nœud est aussi étroitement caractérisé par les relations qui existent par nature ou que le système va imposer entre l'Utilisateur, l'Application et le Runtime comme le décrit la figure 2.35. Ces éléments vont être utilisés dans la suite pour modéliser et comprendre les échanges nécessaires au fonctionnement du système.

Comme nous l'avons déjà mentionné, la nature dynamique et mobile des nœuds rend particulièrement difficile la mise en œuvre, dans un environnement réaliste, de protocoles de routage avec lesquels deux entités trouvent toujours un chemin pour communiquer l'une avec l'autre. Selon notre opinion, dans le développement de systèmes pour MANets, l'accent doit donc plutôt être mis sur une approche opportuniste en veillant à ce que, selon

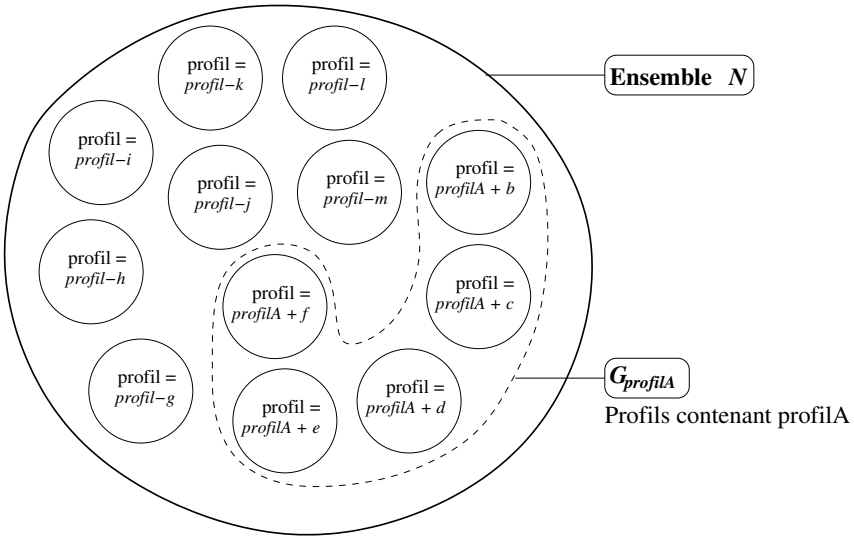


Figure 2.34 – Exemple d'un groupe dans un espace de nœuds.

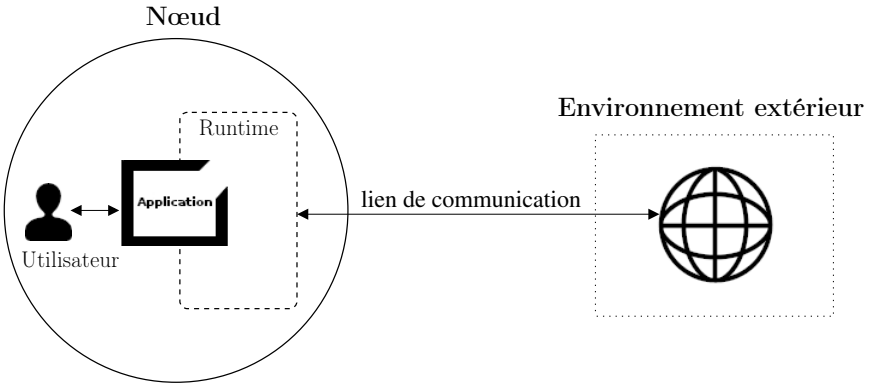


Figure 2.35 – Comportement d'un nœud dans le système.

le contexte, l'utilisation des possibilités de communication offertes à chaque noeud soit optimale (en fonction des exigences du système).
L'intérêt d'un système qui regroupe un ensemble de nœuds mobiles capables de communiquer directement (en fonction des circonstances) avec leurs voisinages respectifs réside dans le fait d'offrir les moyens à chaque entité de rechercher des informations en fonction de ses besoins et par réciprocité de partager des données utiles. Ces considérations doivent guider le choix des processus et des interactions nécessaires au fonctionnement de la plate-forme. Il est également important de préciser qu'en raison de ces considérations, le profil de chaque nœud doit être diffusé (le plus possible) afin que le système opère de façon optimale. En effet, la possibilité de lancer des recherches ou de mettre à disposition des informations est liée aux profils dont chaque nœud peut avoir connaissance. Prenons deux nœuds n_i et n_j appartenant à N. Supposons que n_i désire émettre un message à destination de nœuds ayant des caractéristiques particulières tandis que n_j souhaite partager des informations avec certains nœuds. Supposons également qu'à un moment donné, n_i et n_j se rencontrent physiquement. La distinction qui est faite entre n_i et n_j (et leurs objectifs) permet de

prendre en compte toutes les situations qui peuvent survenir. Les interactions (possibles) au sein du système peuvent alors être résumées par les étapes suivantes :

$$\begin{cases} \text{(Chaque nœud du système) - } \textit{Publier le plus possible son profil individuel} \\ \text{(Nœud } n_j\text{) - } \textit{Mettre à disposition des informations pour des profils de nœuds donnés} \\ \text{(Nœud } n_i\text{) - } \textit{Lancer une requête d'exploration de profil de groupe} \\ \text{(Nœud } n_i\text{) - } \textit{Récupérer la liste d'émetteurs de profils correspondant à la requête} \\ \text{(Nœud } n_i\text{) - } \textit{Choisir la technologie appropriée pour communiquer} \\ \text{(Nœud } n_i\text{) - } \textit{Communiquer avec le ou les nœuds souhaités} \\ \text{(Nœuds } n_i \text{ et } n_j\text{) - } \textit{Echanger (si besoin) des informations de profils en cas de rencontre} \end{cases}$$

Sur chaque ligne de l'accolade, les entités entre parenthèses sont celles qui doivent exécuter les processus correspondant. Par exemple, c'est à chaque nœud du système d'effectuer l'action *"Publier le plus possible son profil individuel"*. De façon générale, si un nœud du système souhaite entrer en contact avec un ou plusieurs correspondants dont le profil est déterminé, il doit réaliser les mêmes opérations que n_i à savoir *"Lancer une requête d'exploration de profil de groupe"*, *"Récupérer la liste d'émetteurs de profils correspondant à la requête"*, *"Choisir la technologie appropriée pour communiquer"* et *"Communiquer avec le nœud souhaité"*. De même, si un nœud possède des informations qu'il souhaite rendre disponibles pour certains autres nœuds, il lui est nécessaire de *"Mettre à disposition des informations pour des profils de nœuds donnés"* comme le fait n_j. Dans le cas où deux nœuds se rencontrent physiquement au sein du système, ils peuvent échanger des informations concernant leurs profils respectifs avec le processus *"Echanger (si besoin) des informations de profils en cas de rencontre"* comme le font n_i et n_j. En plus de ces processus, il est nécessaire mettre en place un mécanisme qui assure (autant que possible) la sécurité des communications ainsi que la préservation de l'anonymat des nœuds suivant leurs préférences.
Les différentes étapes d'interaction qui sont considérées entre les nœuds nous permettent d'identifier les processus qui entrent en jeu dans le fonctionnement général du système. Ces processus sont les suivants :

- **la publication de profils** afin de permettre à un nœud de publier son profil dans son voisinage (en utilisant les technologies dont il est équipé) et dans d'autres zones non accessibles directement (en utilisant des nœuds relais) ;
- **la spécification d'un ensemble de cibles** afin de permettre à un nœud de déterminer, parmi les profils disponibles (reçus, accessibles dans le voisinage ou accessibles à travers des nœuds relais), les entités susceptibles de répondre à ses besoins ;
- **le choix de technologie** afin de permettre à un nœud de sélectionner, en fonction du contexte et des préférences des entités impliquées, le moyen le plus adapté pour communiquer avec un autre nœud du système ;
- **l'échange de profils** afin de permettre à deux nœuds, mis physiquement en contact l'un avec l'autre, d'échanger de façon sécurisée des données privées les concernant ;
- **la sécurisation des communications et le contrôle de l'anonymat** afin d'assurer que les informations transmises, lorsque cela est nécessaire, ne peuvent être déchiffrées que par les destinataires sans que cela ne nécessite la divulgation (non autorisée) de données privées.

La figure 2.36 donne un aperçu des étapes à considérer dans la mise en œuvre des processus identifiés. Dans l'exemple présenté, le nœud n_1 publie son profil et initie une recherche de profils parmi ses voisins. Les voisins sont divisés en trois catégories qui ne sont pas disjointes : le groupe de voisins accessibles via la technologie t_1, le groupe de voisins accessibles via la technologie t_2 et le groupe de voisins accessibles via la technologie t_3. Les nœuds relais n_9 et n_{10} (disponibles au moment où les opérations sont effectuées), équipés avec des technologies de communication de plus longue portée, sont utilisés pour transférer les messages aux entités auxquelles n_1 n'a pas directement accès. La recherche de profils est également menée dans l'ensemble des profils déjà reçus par le nœud n_1. En plus des opérations de publication et de recherche de profils, le nœud n_1 échange des données privées avec le nœud n_2 (qu'il rencontre physiquement).

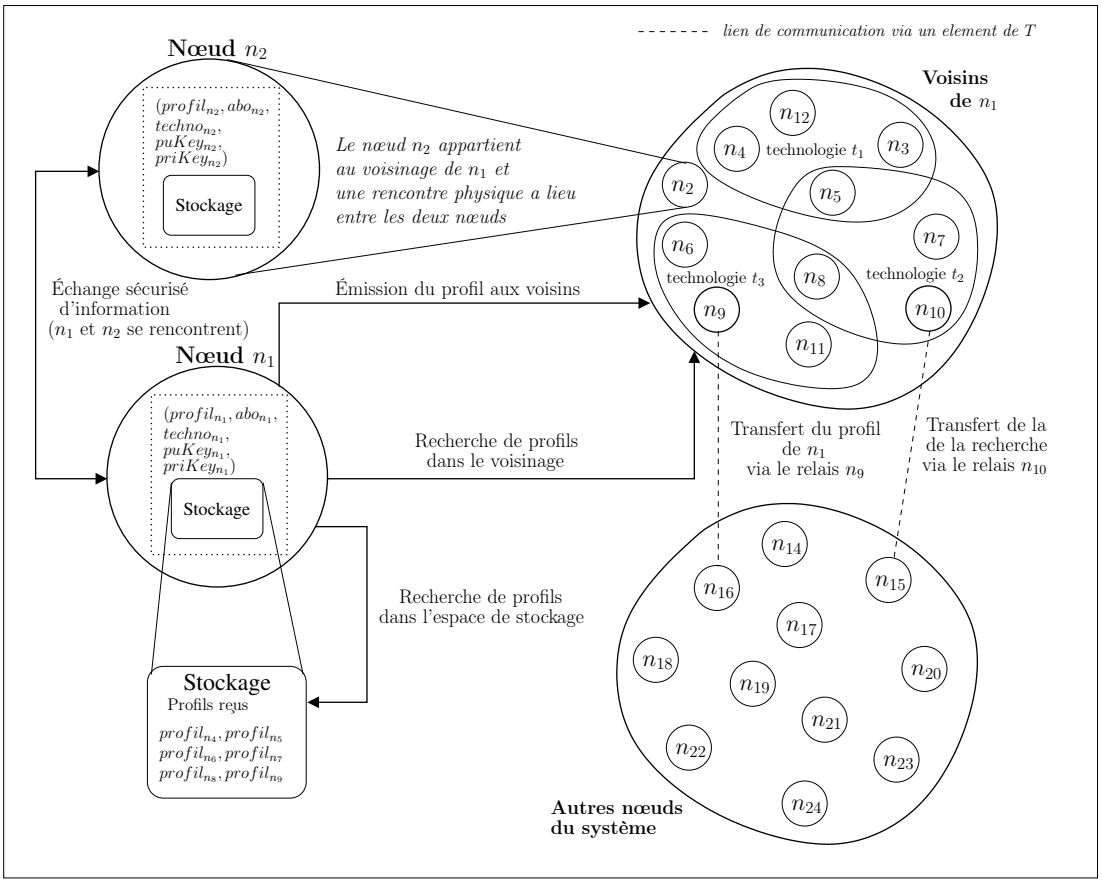


Figure 2.36 – Opérations au sein de la plate-forme.

2.4 Positionnement de l'approche

Le modèle de plate-forme multi-niveaux que nous voulons développer soulève de nombreuses questions de recherche. Ces questions ont souvent été explorées mais, à notre avis, selon un point de vue différent. Nous avons identifié certaines d'entre elles, en particulier celles qui nous paraissent pertinentes dans notre contexte d'étude. Il s'agit notamment

des aspects de sélection d'un canal de communication et de distribution de contenu dans les MANets. Il nous est apparu nécessaire, au delà de l'identification des problématiques pertinentes, de positionner notre approche par rapport à certains projets existants. Nous développons ces éléments dans la suite.

2.4.1 Sélection de réseau

Le domaine de la sélection de réseau vise à développer des méthodes qui permettent à un nœud désirant effectuer des communications de se connecter au réseau le plus approprié en fonction du contexte. Les méthodes développées se basent sur des fonctions de coût qui permettent de déterminer le réseau offrant le coût d'accès le moins élevé en fonction des paramètres à considérer. Une fonction de coût, dans ce cadre, est une fonction qui permet de calculer le coût d'accès (au sens énergétique et financier par exemple) à un réseau donné (en considérant les caractéristiques propres au réseau). Généralement, le réseau retenu par un nœud est celui dont la valeur de la fonction de coût est la moins élevée.
Wang, Serrador et Correia (dans leurs travaux respectifs) présentent des stratégies de sélection de réseau sur la base de fonctions d'utilité normalisées (fonctions de coût) qui tiennent compte de paramètres tels que la bande passante, la consommation énergétique et le coût financier [108][95]. D'autres méthodes de sélection de réseau, avec un modèle de spécification de la politique de choix toujours basé sur des fonctions de coût, mettent davantage l'accent sur des questions spécifiques telles que les exigences de l'utilisateur comme dans [104] (travaux de Ormond et al.) et [97] (travaux de Shen et Zeng). Certains auteurs identifient aussi la décision de *handover* (changement de réseau) comme un problème à résoudre avec la méthode dite *fuzzy* MADM (Multiple Attribute Decision-Making) et proposent une solution basée sur la méthode SAW (Simple Additive Weighting) comme dans les travaux [113] (Zhang) et [7] (Bari et Leung). Le *fuzzy* MADM est une méthode de modélisation pour des systèmes à évaluer suivant des critères multiples pour lesquels les préférences des utilisateurs (être humains) doivent être prises en compte. La méthode SAW permet de définir l'importance (ou le poids) de chaque critère à considérer dans un problème *fuzzy* MADM afin de procéder à l'évaluation des systèmes à comparer.
Tout en prenant en compte les éléments les plus essentiels à considérer, c'est à dire les paramètres à intégrer dans le calcul des fonctions de coûts, ces solutions ne tiennent pas compte de l'aspect multi-niveaux tel que nous le développons dans notre plate-forme. Classiquement, dans les approches existantes il s'agit de choisir le réseau le plus adapté étant donné une technologie (par exemple choix du *SSID* le plus approprié avec la technologie Wi-Fi). Certes, il existe des systèmes, tels que ceux proposés par Issarny et al. [16][19], qui prennent en compte l'aspect multi-technologies des équipements. Toutefois, ces systèmes se focalisent sur l'accès à un service particulier (les *Service Discovery Protocols* dans les exemples cités). Dans notre plate-forme multi-niveaux, nous supposons que tous les nœuds ont le même rôle : tous offrent des "services" et recherchent des "services" dans le réseau. De plus, à travers les technologies que nous choisissons d'utiliser, les "négociations" entre nœuds pour déterminer la technologie la plus adaptée aux échanges se font en mode direct (*peer-to-peer*) et non via une infrastructure. Dans notre cas, il s'agit de sélectionner, en fonction des contraintes du système (caractéristiques des technologies, réduction des coûts, etc.), la technologie intra-îlot la plus appropriée, parmi celles disponibles, qui permette d'effectuer des communications en mode *peer-to-peer*.

2.4.2 Distribution de contenu

Le problème majeur de la distribution de contenu au sein d'un réseau consiste à déterminer les méthodes à mettre en œuvre afin qu'une information donnée puisse atteindre les entités qui seraient susceptibles d'en avoir besoin. Elle revêt un caractère particulièrement complexe, au sein des MANets, en raison de la mobilité des nœuds et du fait que l'évolution du réseau est difficilement prévisible.
Divers travaux présentent des solutions qui mettent l'accent sur une approche coopérative entre nœuds comme c'est le cas de la plate-forme proposée par Ma et Jamalipour dans [57]. Des protocoles spécifiques ont été conçus pour permettre des communications entre nœuds basées sur le contenu à transmettre ; Haillot et Guidec présentent un protocole de ce type dans [43]. Ces protocoles utilisent la mobilité et la connectivité de certains nœuds pour faire transiter des informations entre îlots (zones non reliées entre elles par un canal de communication) du réseau. Les exemples mentionnés ci-dessus fournissent des informations utiles et pertinentes pour développer et déployer des systèmes de distribution de contenu (avec une approche opportuniste) dans de tels réseaux. Cependant, l'aspect multi-niveaux, qui tient compte des différentes technologies (de plus ou moins longue portée) disponibles sur un nœud donné, n'est pas considéré. Nous pensons qu'il s'agit d'une question importante à traiter et nous voulons proposer une solution adaptée à ce contexte particulier.
D'autres approches, présentées par Lindgren et al. dans [56] ainsi que Spyropoulos et al. dans [101], offrent des solutions à base de routage dans le cadre de MANets où les nœuds sont connectés entre eux par intermittence. Ces solutions utilisent des traces de mobilité recueillies et des estimations du comportement futur des nœuds du réseau afin de proposer un schéma de distribution de contenu (en fonction des rencontres anticipées entre nœuds) assurant ainsi une diffusion efficace. Notre approche, au sein de ce type de réseaux très dynamiques consiste plutôt à réduire le niveau des garanties proposées, ces garanties devant en revanche être assurées quelle que soit l'évolution du réseau. Les simulations et les traces de mobilité ne représentent que certaines instances d'exécution et ne peuvent donc pas être utilisées pour prouver des résultats systématiques comme nous cherchons à le faire. Nous choisissons de ne pas les utiliser.

2.4.3 Quelques projets existants

Nous présentons quelques projets qui nous paraissent représentatifs des systèmes développés afin de rendre possibles des communications entre nœuds mobiles d'un réseau. La présentation de ces projets nous permet de positionner davantage notre approche et la plate-forme que nous concevons par rapport à certains choix de développement.
Le projet Musubi [28], développé par le Stanford Mobile and Social Computing Research Group, est, à notre avis, à mentionner. Musubi est une plate-forme de gestion des échanges entre nœuds mobiles au sein d'un réseau social distribué qui met l'accent sur le respect de la vie privée. Le principe central de Musubi réside dans le fait que les données personnelles ne sont pas stockées sur un serveur central mais uniquement sur les équipements mobiles (des smartphones généralement) des utilisateurs. De plus, seuls les nœuds qui interagissent entre eux peuvent avoir accès aux informations échangées car toutes les communications sont chiffrées. Cependant, l'approche que nous proposons diffère sur le point du mode de communication. En effet, avec Musubi il n'est pas possible d'émettre des messages directement de nœud à nœud en raison du fait qu'ils ne possèdent pas d'adresse IP publique, au

contraire une infrastructure est mise en place pour acheminer les messages (chiffrés) entre correspondants.
Un autre projet intéressant est le développement de Junction [45] qui est un protocole de communication pour applications mobiles fonctionnant en mode *peer-to-peer* sans utilisation d'une infrastructure pré-existante. Un exemple d'utilisation de Junction se trouve dans les jeux mobiles multi-joueurs. Plus précisément, un utilisateur lance un jeu sur son équipement mobile (qui intègre le protocole Junction) et peut ensuite, à l'aide d'une technologie sans fil (NFC ou Bluetooth), contacter d'autres joueurs afin d'initier une partie multi-joueurs. Les communications ne nécessitent pas de serveur central unique et permanent pour ce type d'applications fonctionnant en mode multi-utilisateurs. Le principe réside dans le fait qu'un nœud (généralement l'initiateur de la demande de fonctionnement en mode multi-joueur) fait office de *switchboard* afin de gérer l'échange de messages entre participants et que tous les nœuds embarquent l'application mobile considérée. L'approche que nous proposons pour notre plate-forme diffère principalement sur l'aspect multi-niveaux. En effet, Junction n'intègre pas une architecture multi-niveaux qui permettrait de sélectionner automatiquement, parmi les technologies disponibles, le meilleur canal de communication direct (au sens de la réduction des coûts énergétiques et financiers par exemple) entre deux nœuds qui souhaitent échanger des informations.
Il nous semble enfin pertinent de mentionner le projet MobiClique [85]. MobiClique utilise une approche opportuniste afin de développer un réseau social mobile dont les échanges entre utilisateurs s'effectuent par le moyen des technologies Bluetooth et/ou Wi-Fi (via leurs équipements mobiles respectifs). Chaque nœud est donc doté d'un profil (issu d'un réseau social classique existant) qui contient les informations personnelles à rendre publiques. Les opérations s'effectuent de façon périodique et en trois étapes à savoir la découverte du voisinage, l'identification des nœuds présents et les échanges de données avec les destinataires choisis. Ces échanges de données de façon opportuniste combinés à la mobilité des nœuds constituent la base de la plate-forme MobiClique. Les informations sont transmises entre nœuds suivant les rencontres effectuées et en fonction des besoins exprimés dans les profils. Par exemple, lorsque deux nœuds sont à portée l'un de l'autre (via Bluetooth ou Wi-Fi), s'ils ont déjà été en contact dans le passé (on peut supposer que les deux nœuds sont "amis" au sens réseau social du terme) et si leurs profils respectifs ont été modifiés alors les échanges nécessaires sont effectués pour procéder aux mises à jour. Cependant, il est à noter que MobiClique nécessite que l'équipement mobile d'un utilisateur donné se connecte occasionnellement à un serveur central (via une connexion Internet) pour une synchronisation entre son profil et les données du réseau social classique dont le profil est issu. Un autre point important est le fait que MobiClique n'intègre pas d'approche multi-niveaux dans les communications entre nœuds. De plus, dans sa version initiale, la plate-forme n'intègre pas de mécanisme de sécurisation des communications. Ces éléments montrent les différences qui existent entre notre approche et celle proposée par le projet MobiClique.
Le tableau 2.14 permet de faire une synthèse des différences entre les projets représentatifs que nous avons présentés et l'approche que nous proposons. La comparaison porte sur les points suivants qui nous semblent essentiels :

- la prise en compte de l'aspect multi-niveaux ;
- les communications entre nœuds en mode *peer-to-peer* ;
- la gestion de la sécurisation des échanges entre nœuds ;

Systèmes \ **Critères**	Multi-niveaux	*Peer-to-Peer*	Sécurité	Décentralisation
Musubi			×	×
Junction		×		×
MobiClique		×		
Notre approche	×	×	×	×

Table 2.14 – Résumé du positionnement par rapport à des projets existants.

– le caractère totalement décentralisé (sans besoin d'un serveur central pour stocker des données).

Cette synthèse relève le caractère pertinent de notre proposition de plate-forme multi-niveaux pour communications sécurisées en mode *peer-to-peer* au sein de MANets.

Deuxième partie

Conception du système multi-niveaux

Chapitre 3

Plate-forme multi-niveaux

Sommaire

3.1 Approche proposée

Dans l'approche introduite dans le chapitre précédent, nous avons identifié les opérations principales qui doivent être mises en œuvre pour développer notre plate-forme. Pour rappel, ces opérations sont les suivantes :

- la publication de profils ;
- la spécification d'un ensemble de cibles ;
- le choix d'une technologie de communication ;
- l'échange de profils ;
- la sécurisation des communications et le contrôle de l'anonymat.

Il s'agit donc maintenant, en fonction du contexte propre aux MANets et du cadre fixé (définitions et positionnement du système à développer), de proposer une approche complète permettant le fonctionnement de notre plate-forme multi-niveaux. Les cinq sections suivantes présentent le détail des processus à mettre en œuvre, selon notre conception du système, pour chaque opération identifiée.

3.1.1 Publier un profil

La finalité de ce processus est que chaque nœud ait son profil publié et porté à la connaissance du plus grand nombre possible de nœuds du système. La démarche classique qui consiste en une inondation du réseau (l'inondation est un algorithme de diffusion dans lequel chaque message entrant est retransmis, sans aucune exception, à l'ensemble du voisinage) est écartée. En effet, nous supposons que les nœuds qui composent le système ont des ressources limitées en termes d'énergie (ce sont des appareils mobiles électroniques) ce qui nous amène à éviter, autant que possible, l'envoi dupliqué de messages, lequel aurait par ailleurs l'inconvénient de risquer de saturer la bande radio concernée.

3.1.1.1 Approche intuitive

Une première approche intuitive, pour profiter de l'aspect multi-niveaux, consiste à demander à chaque nœud de retransmettre (si cela s'avère possible) un profil avec une technologie de portée supérieure à celle avec laquelle il l'a reçu. Ceci permet à un nœud de voir son profil publié dans des zones auxquelles il n'a pas accès directement. La figure 3.37 présente un exemple de processus de publication de profil qui intègre cette première approche et qui prend en compte le fait que les nœuds sont équipés de plusieurs types de

technologies de communication, de courte et de longue portée. Nous rappelons que nous sommes en mode point à point. Soit l'ensemble de nœuds $N = \{n_1, n_2, n_3, n_4, n_5, n_6\}$ avec :

- $n_1 = (profil_{n_1}, techno_{n_1} = \{t_1\}, abo_{n_1})$
- $n_2 = (profil_{n_2}, techno_{n_2} = \{t_1, t_2\}, abo_{n_2})$
- $n_3 = (profil_{n_3}, techno_{n_3} = \{t_2, t_3\}, abo_{n_3})$
- $n_4 = (profil_{n_4}, techno_{n_4} = \{t_2, t_3\}, abo_{n_4})$
- $n_5 = (profil_{n_5}, techno_{n_5} = \{t_1, t_2\}, abo_{n_5})$
- $n_6 = (profil_{n_6}, techno_{n_6} = \{t_1\}, abo_{n_6})$
- $t_1, t_2 \in T_C$ et $\geq^P (t_1, t_2)$
- $t_3 \in T_L$

Supposons que le nœud n_1, uniquement équipé de la technologie t_1 doit publier son profil et atteindre le nœud n_6 avec lequel il n'est pas capable de communiquer directement. n_1 établit d'abord la liste de ses voisins suivant la technologie t_1 (V_{n_1,t_1}), tout en récupérant les informations (disponibles) sur les technologies dont chacun est équipé. Il parcourt ensuite cette liste pour déterminer s'il existe un nœud possédant une technologie dont la portée est supérieure à celle de t_1 et capable de prolonger la publication du profil. Dans notre exemple il existe un tel nœud n_2 qui est alors sélectionné. n_1 émet donc un message à destination de l'ensemble de ses voisins, via t_1, contenant $profil_{n_1}$ et V_{n_1,t_1} ainsi qu'un marqueur particulier à l'attention de n_2 lui demandant de retransmettre les informations de son profil à un niveau supérieur. n_2 reçoit, via t_1, $profil_{n_1}$, V_{n_1,t_1} et l'information selon laquelle il doit faire passer l'information concernant le profil de n_1 à un niveau supérieur (par la technologie t_2). Après avoir fait une comparaison entre V_{n_1,t_1} et V_{n_2,t_2} (pour éviter l'émission répétée d'un même message à destination d'un nœud), n_2 envoie $profil_{n_1}$ et V_{n_2,t_2} à ses voisins (n'ayant pas déjà reçu $profil_{n_1}$) suivant la technologie t_2 tout en spécifiant au nœud n_3 (choisi au préalable en fonction de ses capacités technologiques) de faire passer l'information à un autre niveau. n_3 transfère l'information à son voisinage (donc à n_4) en utilisant t_3. Dans le cas du nœud n_4, ce dernier ne possède pas de technologie de plus grande portée que celle avec laquelle l'information de profil est reçue (t_3), il ne peut donc pas transférer les données à un niveau supérieur. Le message est alors retransmis, après les comparaisons nécessaires entre V_{n_3,t_3} et V_{n_4,t_2} pour éviter les duplications de messages, via la technologie de plus grande portée. Dans l'exemple donné, t_2 est le moyen de retransmission utilisé par n_4. Le processus se répète ainsi, de proche en proche, jusqu'à ce que n_6 reçoive un message contenant $profil_{n_1}$ de la part de n_5 via t_1.

3.1.1.2 Proposition d'une approche générale

De façon plus générale, la publication de profil par un nœud suit les étapes présentées dans la figure 3.39. La première approche décrite dans la section précédente ne prend pas en compte le fait que l'intersection non vide des voisinages de deux nœuds distincts à un instant t donné peut avoir une influence sur le choix du moyen de transmission d'un profil. En effet, lorsque deux nœuds ont un ou plusieurs nœuds en commun dans leurs voisinages respectifs, il faut définir une stratégie coordonnée (en fonction des technologies disponibles) pour choisir l'entité qui doit transmettre ou retransmettre un profil. Il est donc nécessaire d'améliorer cette approche pour que les interactions locales de nœud à nœud permettent d'assurer une diffusion optimale.
Dans la suite de la description des opérations, seules les technologies qui appartiennent à

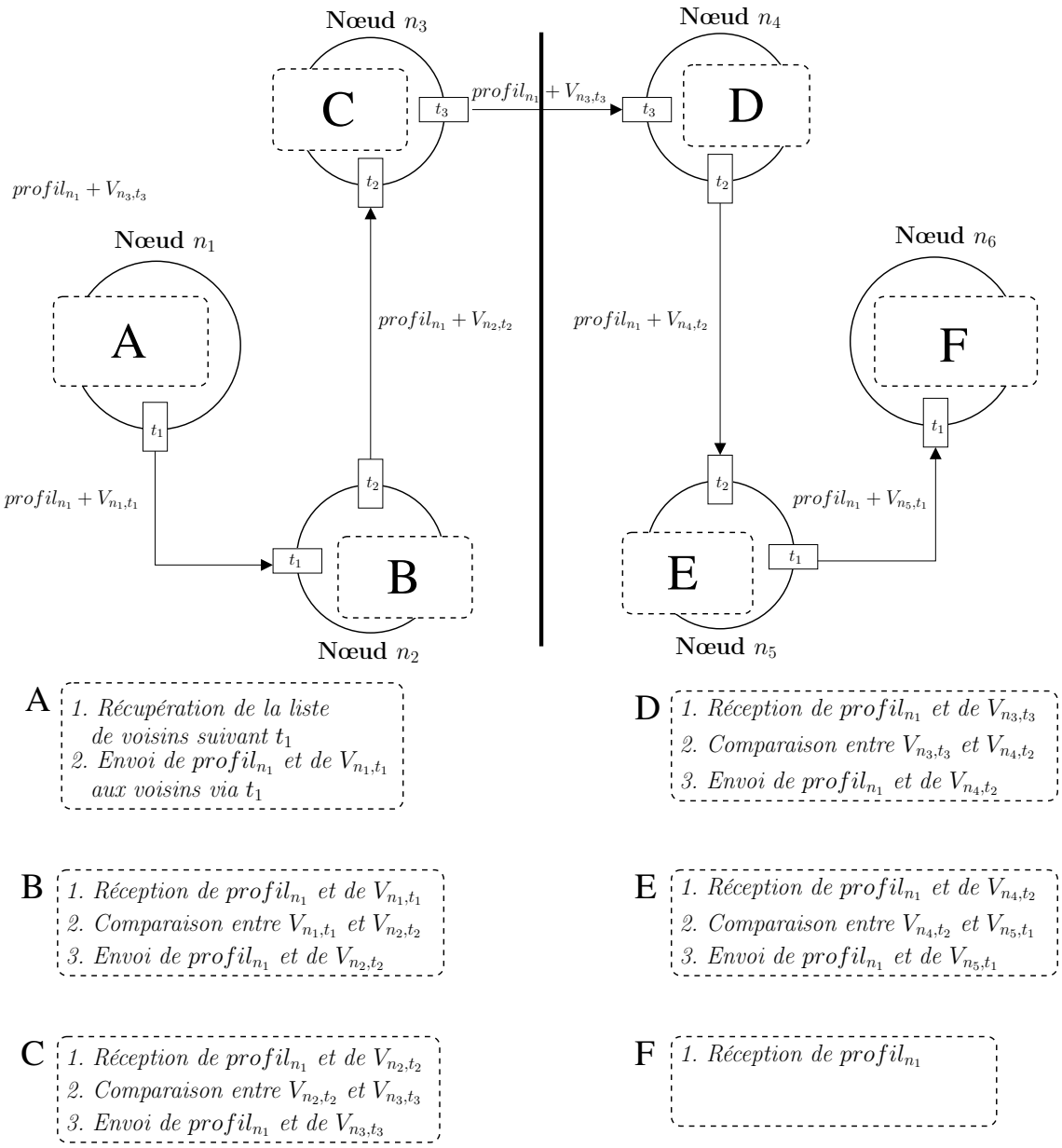


FIGURE 3.37 – Exemple de mécanisme de publication de profil.

l'ensemble T_{DI} sont considérées (lors de la mention d'éléments de l'ensemble T) en raison des besoins en terme de connaissance du voisinage que nécessite la publication d'un profil par un nœud. En effet, un nœud qui publie son profil doit être en mesure de s'adresser directement aux entités accessibles dans son voisinage sans que cela ne requiert une connaissance préalable d'informations privées ; la connaissance d'une telle information suppose qu'un échange préalable de profil a déjà eu lieu et le problème serait donc sans objet. Il est également à noter que lorsque la mention de la publication du profil d'un nœud n_i est faite (dans toutes les descriptions), il s'agit de la partie $kernel_{n_i}$ de ce profil (i.e. les informations minimales publiques concernant le nœud n_i).

Quelques définitions complémentaires. En supposant, pour un nœud n_i donné, que T_{n_i} contient les technologies de la forme t_a, $a = 1, \ldots, b$ (avec b entier), nous proposons les définitions suivantes :

- $V_{n_i}(t)$ est l'ensemble des voisins de n_i à un instant t donné et il est possible de noter $V_{n_i}(t) = \bigcup_{a=1}^{b} V_{n_i,t_a}(t)$
- P_{n_i} contient l'ensemble des identifiants des profils que n_i a reçus
- T_{n_i,n_k} est l'ensemble des technologies par lesquelles un nœud n_k est voisin de n_i
- $VT_{n_i}(t)$ est l'ensemble des couples de la forme (n_k, T_{n_i,n_k}) avec $n_k \in V_{n_i}(t)$ et $T_{n_i,n_k} \subset T_{n_i}$.

Description de l'approche générale de publication. Dans un premier temps nous donnons une approche formalisée de la publication de profil. Cette formalisation complexe est reprise point par point dans les sections suivantes. Le processus de la figure 3.39 va maintenant être détaillé en mettant l'accent sur les échanges qui doivent avoir lieu afin que chaque entité puisse effectivement *"Publier le plus possible son profil individuel"*. Soit n_i le nœud qui doit publier le plus possible son profil et n_j un nœud qui reçoit le profil de n_i. Pour chaque nœud $n_k \in V_{n_i}(t)$, tout en envoyant T_{n_i} et $VT_{n_i}(t)$, le nœud n_i réalise une requête pour obtenir T_{n_k}, $VT_{n_k}(t)$ ainsi que P_{n_k} (figure 3.40). Pour chaque nœud $n_l \in V_{n_i}(t)$ qui a répondu à la requête de n_i et tel que l'identifiant de n_i n'appartient pas à P_{n_l} les étapes suivantes (figure 3.41) sont observées :

- cas 1 : transmission par rebond (figure 3.38). Si n_i et n_l ont au moins un voisin en commun, c'est à dire que $V_{n_i}(t) \cap V_{n_l}(t) \neq \varnothing$, alors pour chaque nœud $n_m \in V_{n_i}(t) \cap V_{n_l}(t)$ il existe deux couples (n_m, T_{n_i,n_m}) et (n_m, T_{n_l,n_m}) qui appartiennent respectivement à $VT_{n_i}(t)$ et à $VT_{n_l}(t)$ (en d'autres termes, le nœud n_m est accessible par n_i et n_l respectivement via les technologies des ensembles T_{n_i,n_m} et T_{n_l,n_m}).
  [si $\geq^P (maxT_{n_l,n_m}, maxT_{n_i,n_m})$ (i.e. $portee(maxT_{n_l,n_m}) \geq portee(maxT_{n_i,n_m})$) (suivant un facteur f qui sera déterminé et expliqué dans la section 3.3 page 114, en d'autres termes $portee(maxT_{n_l,n_m}) \geq f.portee(maxT_{n_i,n_m})$)] $\wedge$ [si n_l est considéré comme plus efficace pour transmettre un profil] alors n_i envoie son profil à n_l et lui demande de le retransmettre à n_m (si et seulement si cette retransmission vers n_m n'a pas déjà été demandée par n_i à un autre nœud) via la technologie $maxT_{n_l,n_m}$; dans ce cas de figure il faut également que $\geq^P (maxT_{n_i,n_l}, maxT_{n_i,n_m})$ (nous supposons qu'en situation de mobilité, plus la portée d'une technologie est grande plus la probabilité d'atteindre une cible en l'utilisant est élevée).

- cas 2 : transmission directe à un *nœud isolé*. Si le nœud n_p est un *nœud isolé* (car il n'a qu'un seul voisin, le nœud n_i dans ce cas précis), c'est à dire que $n_p \notin V_{n_i}(t) \cap V_{n_l}(t)$ $(\forall n_l \in V_{n_i}(t))$, alors n_i envoie son profil à n_p via la technologie $t_c = maxT_{n_i,n_p}$ (nous supposons toujours qu'en situation de mobilité, plus la portée d'une technologie est grande plus la probabilité d'atteindre une cible en l'utilisant est élevée).

- cas 3 : cas par défaut. Si après la prise en compte des deux étapes précédentes, un nœud n_l (voisin de n_i) n'a pas été considéré pour recevoir le profil publié, alors n_i

envoie son profil à n_l via la technologie $maxT_{n_i,n_l}$

Lorsque le nœud n_j reçoit le profil de n_i, les étapes suivantes sont également observées :

- si $n_i \notin V_{n_j}(t)$ alors la poursuite de la publication du profil de n_i par le nœud n_j (au sein de l'ensemble $V_{n_j}(t)$) est effectuée suivant les capacités techniques, en fonction de son voisinage et en fonction de la nature du profil (par exemple son caractère rare qui en fait un profil particulièrement recherché) concerné.
- si $n_i \in V_{n_j}(t)$ alors n_j retransmet le profil de n_i (si et seulement si la retransmission a été demandée) aux nœuds indiqués qui appartiennent à $V_{n_i}(t) \cap V_{n_j}(t)$. La poursuite de la diffusion, par le nœud n_j, du profil de n_i dans l'ensemble $V_{n_j}(t) - (V_{n_i}(t) \cap V_{n_j}(t))$ dépend du contexte (capacités et voisinage de n_j) et de la nature du profil du nœud n_i (par exemple son caractère rare).

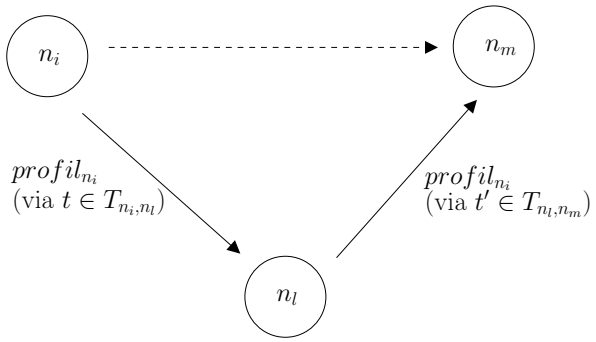


FIGURE 3.38 – Transmission du profil de n_i par rebond.

Le processus de diffusion de profils doit également intégrer la notion d'abonnement. En effet, lorsqu'un noeud possède un abonnement il doit l'utiliser pour diffuser son profil. En d'autres termes, pour tout c_q appartenant à abo_{n_i}, le nœud n_i doit publier son profil sur le canal c_q afin de le rendre disponible sur le site distant associé.

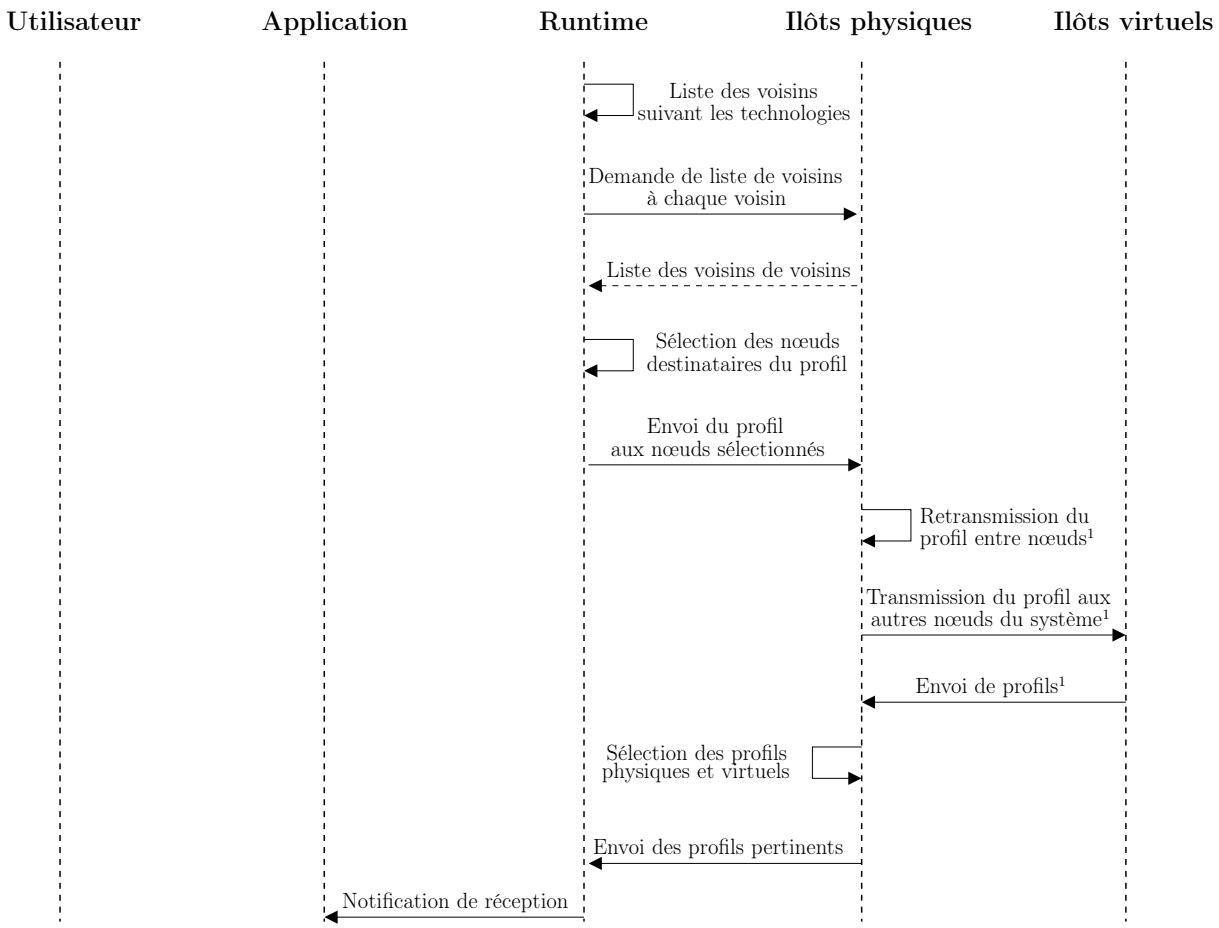
3.1.1.3 Précisions sur l'approche générale

Quelques éléments doivent être précisés dans le déroulement du processus de diffusion de profils. Ils sont présentés dans la suite. Nous supposons toujours que n_i est le nœud qui doit publier le plus possible son profil et que n_j est un nœud qui reçoit le profil de n_i.

Requête de voisinage. Cette étape permet au nœud n_i de recueillir les informations disponibles concernant les voisins avec lesquels il est nécessaire d'interagir dans le but de *"Publier le plus possible son profil individuel"*.

Le nœud n_i doit d'abord déterminer la liste de ses voisins, à l'instant t donné, suivant les différentes technologies dont il est équipé. Afin d'établir cette liste, n_i initie une recherche de voisinage (en fonction des spécificités de chaque technologie) qui lui permet de recevoir des informations élémentaires (identifiants et technologies disponibles) des nœuds voisins capables de répondre. Afin de limiter par la suite les échanges au sein du réseau, ce sont uniquement les s_e (s_e étant un seuil arbitraire à spécifier) premiers nœuds distincts (un même nœud pourrait répondre à travers plusieurs technologies) ayant répondus à la demande de voisinage qui sont considérés et qui constituent l'ensemble $V_{n_i}(t)$.

Ensuite, pour récupérer les informations de voisinage, le nœud n_i parcourt la liste de ses



1. Ce sont uniquement certains nœuds, en fonction du contexte, qui procèdent à ces opérations

Figure 3.39 – Publier son profil le plus possible.

voisins (ensemble $V_{n_i}(t)$) et initie une requête par voisin identifié. De façon arbitraire, chaque requête est émise suivant la première technologie avec laquelle le nœud destinataire a transmis les informations élémentaires le concernant (lors de la recherche de voisinage). Ainsi, même si un nœud est voisin de n_i par plusieurs technologies de communication, il suffit à n_i de recueillir le détail du voisinage du nœud considéré à travers une seule requête transmise suivant une seule technologie. Il n'est donc pas nécessaire d'effectuer des requêtes d'information de voisinage suivant toutes les technologies dont un nœud peut être équipé. De plus, l'attente de réponse à une requête a une durée limitée dans le temps (à spécifier en fonction du contexte). La requête (figure 3.40) permet au nœud n_i de recevoir les informations au sujet des profils reçus par ses voisins (P_{n_k}) et sur les capacités technologiques de ses voisins (T_{n_k}) sur les capacités technologiques des voisins de ses voisins ($VT_{n_k}(t)$). Enfin, il est à noter que les nœuds isolés ne peuvent être déterminés que lorsque n_i a parcouru l'ensemble des éléments de $V_{n_i}(t)$ pour effectuer des requêtes d'information concernant leurs voisinages respectifs. Les nœuds qui n'ont pas répondu à la requête de voisinage sont ignorés dans la suite du processus de diffusion du profil de n_i et ne sont donc pas pris en compte dans la caractérisation des nœuds isolés. En pratique, cela signifie que c'est

l'ensemble $V_{n_i}(t)$ privé des nœuds qui n'ont pas répondu à la requête d'information de voisinage qui est considéré pour réaliser les différentes étapes du processus de publication de profil suivant les catégories de voisins (figure 3.41).

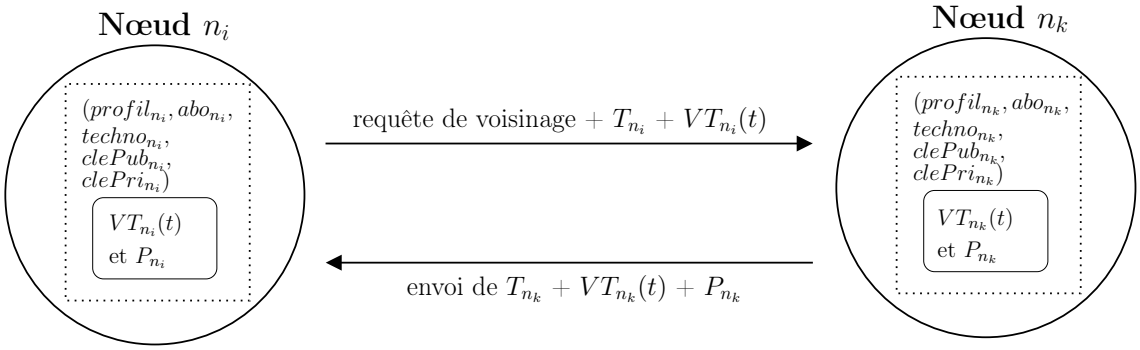


FIGURE 3.40 – Échange des informations de voisinage entre deux nœuds.

Retransmission de profil avec demande préalable. Supposons que le nœud n_j reçoive le profil de n_i. Il est alors demandé au nœud n_j de retransmettre ce profil à un autre nœud n_k qui appartient à l'ensemble $V_{n_i}(t) \cap V_{n_j}(t)$ et ce, via la technologie $maxT_{n_j,n_k}$. Cette demande de retransmission est effectuée car [$\geq^P$ $(maxT_{n_j,n_k}, maxT_{n_i,n_k})$] $\wedge$ [n_j est considéré comme étant plus efficace que n_i pour transmettre le profil à publier]. Pour évaluer l'efficacité d'émission d'un profil dans ce contexte et en fonction des informations disponibles, nous définissons, sur $N \times T$, un ensemble de fonctions Fe_{n_b} dite fonctions d'efficacité de transmission de profil à un nœud n_b ($n_b \in N$) de la façon suivante :

- $Fe_{n_b}(n_a, t_c) = \delta_{[n_a,t_c]} + \gamma_{[n_a,t_c]} + \rho_{[n_a,t_c]} + \sigma_{[n_a,n_b]}$

Les paramètres de ces fonctions sont quant à eux définis de la façon suivante :

- $\delta_{[n_a,t_c]}$ représente le pourcentage de nœuds à l'instant t, parmi l'ensemble des voisins de n_a, qui ne sont pas dotés de la technologie t_c (on obtient ainsi une plus grande disponibilité de la technologie). $\delta_{[n_a,t_c]} = 1 - \frac{V_{n_a,t_c}(t)}{V_{n_a}(t)}$.
- $\gamma_{[n_a,t_c]}$ représente le pourcentage de communications effectuées, sur l'ensemble des communications par le nœud n_a, via la technologie t_c.
- $\rho_{[n_a,t_c]}$ représente le pourcentage de tentatives réussies, sur l'ensemble des tentatives effectuées, d'émission de messages en utilisant la technologie t_c.
- $\sigma_{[n_a,n_b]}$ traduit le fait que n_a a déjà transmis (avec succès) ou non un message à destination de n_b par le moyen de la technologie t_c. $\sigma_{[n_a,n_b]}$ prend la valeur 1 si un message a déjà été transmis et 0 dans le cas contraire

Les fonctions de type Fe_{n_b} (avec $n_b \in N$) permettent de faire une évaluation comparative, selon les choix de paramètres que nous avons effectués et que nous considérons pertinents dans notre contexte, de l'efficacité attendue dans la transmission d'un profil. En effet, à travers la fonction Fe_{n_b} nous appliquons la méthode WSN (Weighted Sum Model) selon laquelle plus la somme des valeurs des paramètres est élevée plus la solution (dans l'évaluation de la caractéristique liée aux paramètres) qui prend en compte ces valeurs de paramètres est optimale [105]. Nous considérons la cas particulier où tous les paramètres choisis (avec le même intervalle de valeur compris entre 0 et 1) ont le même poids et donc la même importance dans le calcul. Dans l'exemple considéré, il est donc demandé (par n_i)

au nœud n_j de retransmettre le profil de n_i parce que $\geq^P (maxT_{n_j,n_k}, maxT_{n_i,n_k})$ et que $Fe_{n_k}(n_j, maxT_{n_j,n_k}) \geq Fe_{n_k}(n_i, maxT_{n_i,n_k})$. Il est à noter que les données concernant δ, γ, ρ et σ qui sont les paramètres des fonctions Fe_{n_k}, doivent être transmises lors de la requête de voisinage entre les nœuds impliqués.

Retransmission de profil sans demande préalable. Il s'agit de la situation où le nœud n_j reçoit le profil de n_i alors que certains nœuds de son voisinage ne l'ont pas reçu. Le nœud n_j peut décider de retransmettre ce profil en fonction de ses capacités et suivant l'intérêt qui peut être porté à la nature du profil en question (comme il sera expliqué dans la suite). Dans notre contexte, deux conditions doivent être remplies pour que n_j choisisse de continuer la publication du profil de n_i parmi ses voisins qui ne l'ont pas encore reçu :

- la première condition est liée aux caractéristiques du nœud n_j. Il faut que le nœud n_j ait spécifié dans ses préférences qu'il est disposé à effectuer des opérations de retransmission (sans demande préalable) si ses capacités techniques le lui permettent. De plus, il est indispensable que n_j soit en période d'inactivité (pas de communications en cours par exemple) pour que l'éventuelle retransmission de profil ne perturbe pas le déroulement des opérations qui lui sont propres. Le nœud n_j doit également préciser dans ses préférences le nombre de retransmissions (sans demande préalable) autorisées et le nombre maximum de nœuds à cibler pour chaque retransmission.
- le seconde condition est liée aux caractéristiques du profil de n_i. Le profil considéré doit être rare pour qu'il y ait un intérêt à poursuivre sa publication même si elle n'a pas été expressément demandée par l'émetteur. La rareté est évaluée en fonction des caractéristiques contenues dans le profil et elle dépend donc des attributs qui y sont présents. Pour évaluer l'éventuelle rareté des caractéristiques de n_i, le nœud n_j analyse le contenu du profil de n_i en fonction de tous les autres profils qu'il a déjà reçus ou dont il a eu connaissance. Dans le cas où au moins un des attributs du profil analysé se retrouve dans une proportion inférieure à β (β exprimé en pourcentage est un paramètre à spécifier) dans les autres profils connus, alors il peut être considéré comme rare. De plus, afin de limiter les retransmissions, chaque profil de nœud est doté d'un compteur initialisé à une valeur c_e (c_e est un entier à spécifier). Ce compteur est décrémenté à chaque fois qu'un processus de retransmission (sans demande préalable) est initié par un nœud récepteur du profil. Une retransmission (sans demande préalable) n'est plus possible lorsque le compteur du profil considéré atteint la valeur 0 (c'est une sorte de TTL).

La vérification des deux conditions précédentes permet au nœud n_j de déterminer s'il est possible de poursuivre la publication du profil de n_i. Dans le cas où la poursuite de la publication de profil est à envisager, elle s'effectue d'une façon similaire à celle que le nœud n_j utilise pour publier son propre profil tout en respectant les contraintes liées au nombre maximum de nœuds à cibler. Il est utile de rappeler que les échanges d'informations, entre les différents nœuds, s'effectuent en mode point à point

Prise en compte des abonnements. La prise en compte des abonnements signifie que le processus de publication de profil par le nœud n_i doit être prolongé en utilisant les abonnements disponibles. En d'autres termes, durant le processus de publication de profil, n_i doit publier son profil sur tous les canaux c_k appartenant à abo_{n_i} et par lesquels ces

informations n'ont pas déjà transité. Ainsi, le profil de n_i sera sauvegardé et rendu disponible (pour les nœuds abonnés) sur tous les sites distants correspondant aux différents canaux utilisés pour prolonger la publication du profil. Ce sont les nœuds du site distant considéré, lorsque cela est nécessaire (et sous réserve qu'ils ont souscrit à l'abonnement adéquat), qui émettent une requête vers le canal afin d'accéder au profil comme cela sera expliqué dans la section suivante.

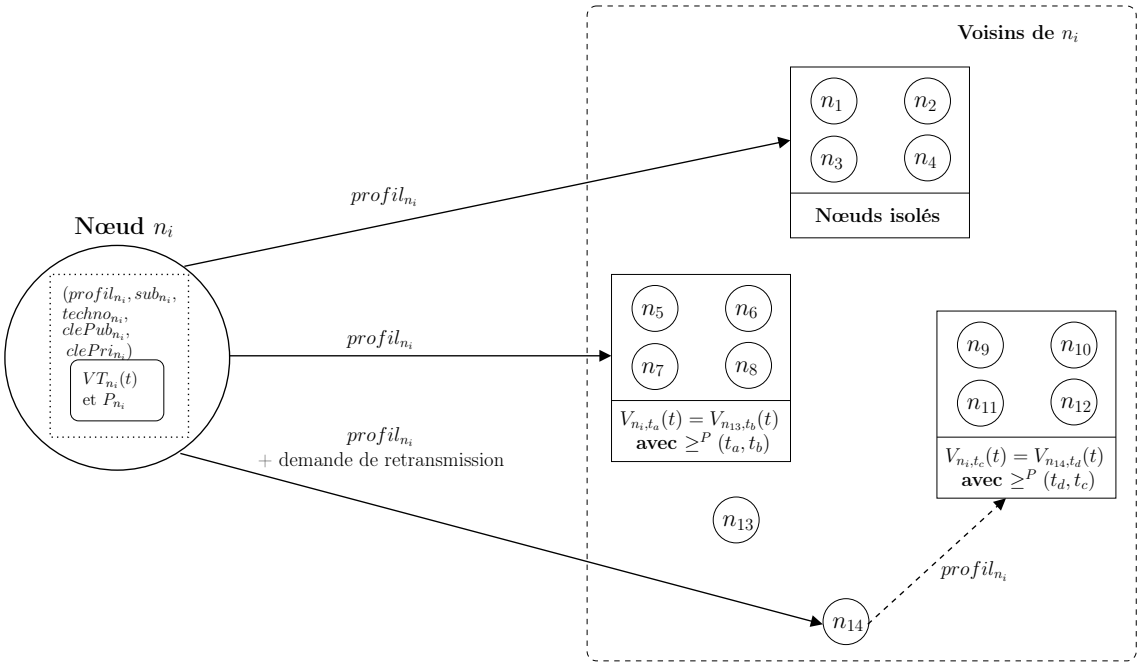


FIGURE 3.41 – Émission du profil de n_i suivant les cas possibles.

3.1.2 Spécifier un ensemble de cibles

La spécification d'un ensemble de cibles, dans notre contexte, permet de décrire un ensemble de nœuds qui sont ciblés pour une opération particulière. Cette spécification se base sur une description de profil de groupe qui permet de préciser des éléments qui doivent être contenus dans tous les profils des nœuds constituant le groupe. De façon concrète, la spécification d'un ensemble de cibles est réalisée au moyen d'une requête d'exploration dont l'argument principal est le profil du groupe à constituer. Par exemple si une entité souhaite entrer en relation avec un nœud en connaissant son pseudonyme, si celui-ci est spécifié dans son profil, elle doit initier une requête d'exploration avec le pseudonyme comme argument. La spécification de groupe est donc un préalable pour tenter de communiquer avec un ensemble de nœuds ayant une caractéristique particulière contenue dans leur profil. La requête d'exploration de profil a donc pour paramètre le profil ($profilA$) du groupe à constituer mais elle peut également contenir un argument nommé *déjà-vu*. Lors du lancement de la requête, cet attribut permet de déterminer si les nœuds du groupe à constituer doivent être connus de l'initiateur (*déjà-vu* = *vrai*) ou non (*déjà-vu* = *faux*). Cela permet, par exemple, de définir un groupe de cibles avec lesquelles l'initiateur a eu des contacts au préalable. Dans le cadre de la spécification de cibles, chaque nœud a non seulement la

possibilité de définir, à travers les préférences liées à son profil, les informations à travers lesquelles il peut être connu et reconnu dans le système mais aussi des nœuds, en décrivant leurs profils, par lesquels il ne souhaite pas être contacté.
La figure 3.42 présente la démarche qui est utilisée afin de procéder à la spécification d'un ensemble de cibles. Le nœud considéré spécifie le type d'information recherchée et les caractéristiques à privilégier dans cette recherche. Ces données permettent de déterminer le profil du groupe qui doit être utilisé comme paramètre de la requête d'exploration initiée parmi tous les profils de nœuds accessibles. Les profils accessibles sont constitués des profils reçus par le nœud, des profils reçus par les voisins du nœud et des profils disponibles à travers les abonnements auxquels le nœud a souscrit. Ce sont les profils de nœuds qui correspondent aux critères recherchés, parmi les profils accessibles, qui constituent l'ensemble des résultats de la requête. Cette liste de profils de nœuds établit l'ensemble des cibles que le nœud initiateur de la requête peut essayer de contacter pour (éventuellement) obtenir l'information dont il a besoin. Cette démarche de spécification de cibles est constituée de plusieurs étapes que nous allons détailler dans la suite.

3.1.2.1 Paramètres supplémentaires à considérer dans la requête

En plus des paramètres que nous avons déjà mentionnés pour la requête d'exploration, à savoir le profil du groupe à constituer et le drapeau *déjà-vu*, il nous semble utile de prendre en compte certains aspects opérationnels. Ces aspects sont liés au fait qu'il est nécessaire d'équilibrer la charge entre nœuds. En effet, en raison des caractéristiques, en matière de consommation énergétique, des nœuds composant les MANets, il faut éviter (autant que possible) que les mêmes nœuds soient trop souvent sollicités pour répondre aux besoins d'autres entités. Nous proposons donc de prendre en compte les éléments suivants qui nous paraissent pertinents pour effectuer une requête d'exploration efficace dans ce contexte :

- les nœuds ayant contribué, de façon fréquente, à répondre aux besoins des autres entités doivent être exclus, dans la mesure du possible, des résultats de la requête. De façon pratique, les nœuds qui sont contributeurs fréquents ne sont pas pris en compte s'il existe d'autres nœuds répondant aux critères de la requête. Le seuil à partir duquel il est possible de classer un nœud parmi les grands contributeurs est déterminé par un entier s_c (à définir). Si le nombre de fois où le nœud considéré a répondu aux besoins d'autres entités est supérieur à s_c alors il est classé comme faisant partie de la catégorie des grands contributeurs.
- les nœuds considérés comme isolés, par rapport à l'émetteur de la requête, doivent être privilégiés. Il est à noter que les nœuds isolés sont les nœuds qui ont uniquement pour voisin l'initiateur de la requête d'exploration. En effet, il est raisonnable de supposer qu'un nœud isolé aura répondu à moins de sollicitations qu'un nœud ayant un voisinage plus fourni. De façon pratique, lorsque le résultat de la requête peut concerner des nœuds isolés, ce sont en priorité ces nœuds qui sont considérés.
- les nœuds dont le profil est considéré comme rare doivent être exclus, dans la mesure du possible, des éventuels résultats. On en réserve l'usage aux requêtes qu'ils sont les seuls à pouvoir traiter (et pour lesquelles ils sont peut-être déjà extrêmement sollicités). De façon pratique et dans le cadre d'une requête bien entendu non liée à un profil supposé rare, les nœuds au profil rare ne sont pas pris en compte s'il existe d'autres nœuds pouvant répondre aux critères de la requête.

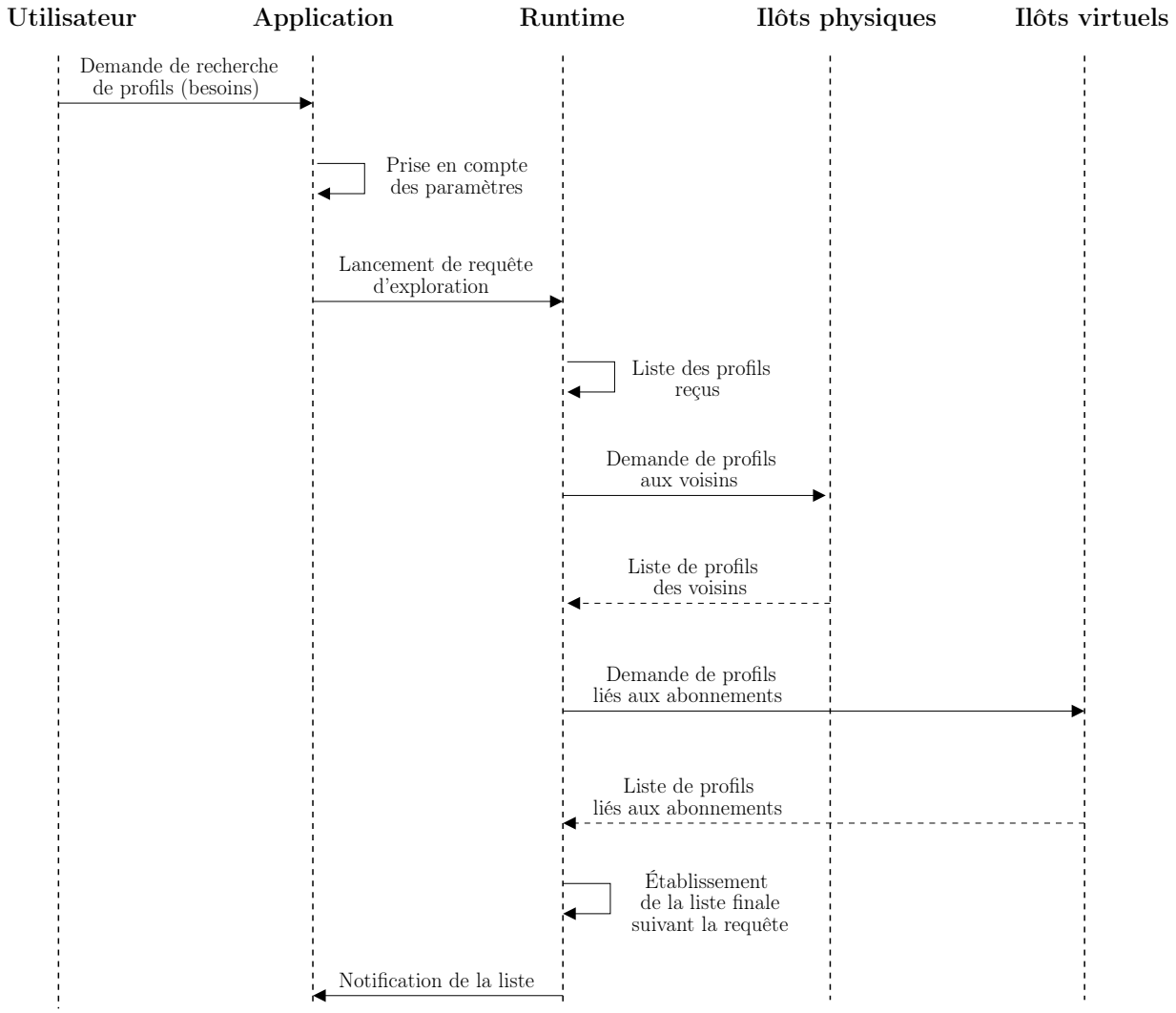


FIGURE 3.42 – Spécifier un ensemble de cibles.

3.1.2.2 Recherche de profils compatibles

Il s'agit, à ce niveau, de définir l'ensemble des profils qui pourraient correspondre aux critères de la requête d'exploration qui a été émise (nous appellerons $L_{potentiels}$ cet ensemble). Il existe trois types de profils parmi lesquels la recherche de profils peut s'effectuer. Pour chacune de ces catégories, une comparaison est effectuée entre le contenu du profil de groupe ($profilA$) de la requête et les caractéristiques des profils accessibles. S'il s'avère que le profil d'un nœud n_j correspond aux besoins spécifié dans $profilA$ et qu'il n'y a aucune incompatibilité entre le profil de l'initiateur de la requête d'exploration et le profil de n_j alors n_j est retenu comme potentiel élément de l'ensemble de la spécification de cibles. Concernant l'incompatibilité, il est par exemple possible que le nœud n_j ne souhaite pas être contacté par des nœuds du type de celui de l'émetteur de la requête. De façon concrète, les trois différents types de profils qu'il est possible de cibler dans une recherche et qui sont présentés figure 3.43 sont les suivants :

(i) les profils reçus par l'émetteur. Ce sont les profils que le nœud initiateur de la requête d'exploration a reçus de la part de ses voisins. Ces profils sont sauvegardés dans l'espace de stockage que le nœud possède comme dans l'exemple donné figure 3.43 avec le nœud n_1 et ils sont donc accessibles directement.

(ii) les profils reçus par les voisins de l'émetteur. Ce sont les profils qui sont sauvegardés dans l'espace de stockage des voisins de l'émetteur. De façon pratique, suivant ses préférences et ses capacités technologiques courantes, le nœud diffuse une requête de demande de profils (spécifiant le type de profils recherché) dans son voisinage. Les nœuds récepteurs de la requête qui ont la capacité de répondre et dont les préférences le permettent renvoient alors les profils correspondant aux critères de la requête d'exploration. Les profils considérés comme rares ou appartenant à des nœuds grands contributeurs sont signalés. Il est à noter que pour limiter les opérations dans le temps, la durée d'attente de réponse à une requête de demande de profils dans le voisinage est fixée. Cette durée d'attente est donnée par τ, τ étant une valeur arbitraire à spécifier. Seuls les profils reçus pendant la durée τ sont considérés.

(iii) les profils sauvegardés à travers les abonnements auxquels l'émetteur a souscrit. Ce sont les profils que le nœud peut récupérer à travers l'ensemble des canaux auxquels il est abonné. Dans l'exemple décrit figure 3.43, le nœud n_1 récupère les profils disponibles dans les canaux c_1 et c_2. De façon pratique, le nœud émet un message à l'attention de c_k (canal auquel il est abonné) de la même façon que celle utilisée pour transmettre un message à destination du site distant associé à c_k. Le contenu du message précise qu'il s'agit d'une requête de profils ainsi que le type de profils recherché et en retour le nœud considéré reçoit les profils correspondants (le cas échéant marqués comme rares ou appartenant à de grands contributeurs). L'opération se répète pour tous les canaux auxquels le nœud est abonné et une liste de profils est ainsi établie. De cette liste sont retirés les profils non compatibles (comme cela a été expliqué plus haut) avec le profil du nœud émetteur.

Le lancement d'une requête d'exploration déclenche donc l'analyse de ces trois catégories de profils et la constitution d'un ensemble de profils potentiellement compatibles. Ensuite, les doublons de profils sont éliminés avant de prendre en compte la valeur de l'argument *déjà-vu* de la requête d'exploration. Dans le cas où *déjà-vu* est égal à *vrai*, les profils de nœuds avec lesquels l'émetteur n'a jamais eu de contact sont alors exclus de l'ensemble des profils.

3.1.2.3 Établissement de la liste définitive de cibles

A partir de la liste déterminée lors de l'étape de recherche de profils compatibles, il faut établir une liste définitive de cibles. Nous appellerons L_{cibles} l'ensemble des profils de nœuds retenus dans la liste définitive. Pour cela, il est nécessaire de prendre en compte les paramètres supplémentaires que nous avons précédemment définis tout en s'assurant que les nœuds de cette liste peuvent être contactés par l'émetteur de la requête d'exploration. Soit n_i le nœud émetteur de la requête d'exploration. Lors de la recherche de profils parmi ses voisins, n_i récupère également la liste des voisins de ses voisins. Cette opération permet à n_i, à l'instant t, de définir l'ensemble $V_{n_i}(t)$ de ses voisins ainsi que l'ensemble $N^t_{n_i,isoles}$ des nœuds isolés, c'est à dire les nœuds dont il est le seul voisin à l'instant t. L'ensemble $N_{n_i,actifs}$, qui regroupe les nœuds ayant répondu au moins r_e (r_e étant un entier spécifié

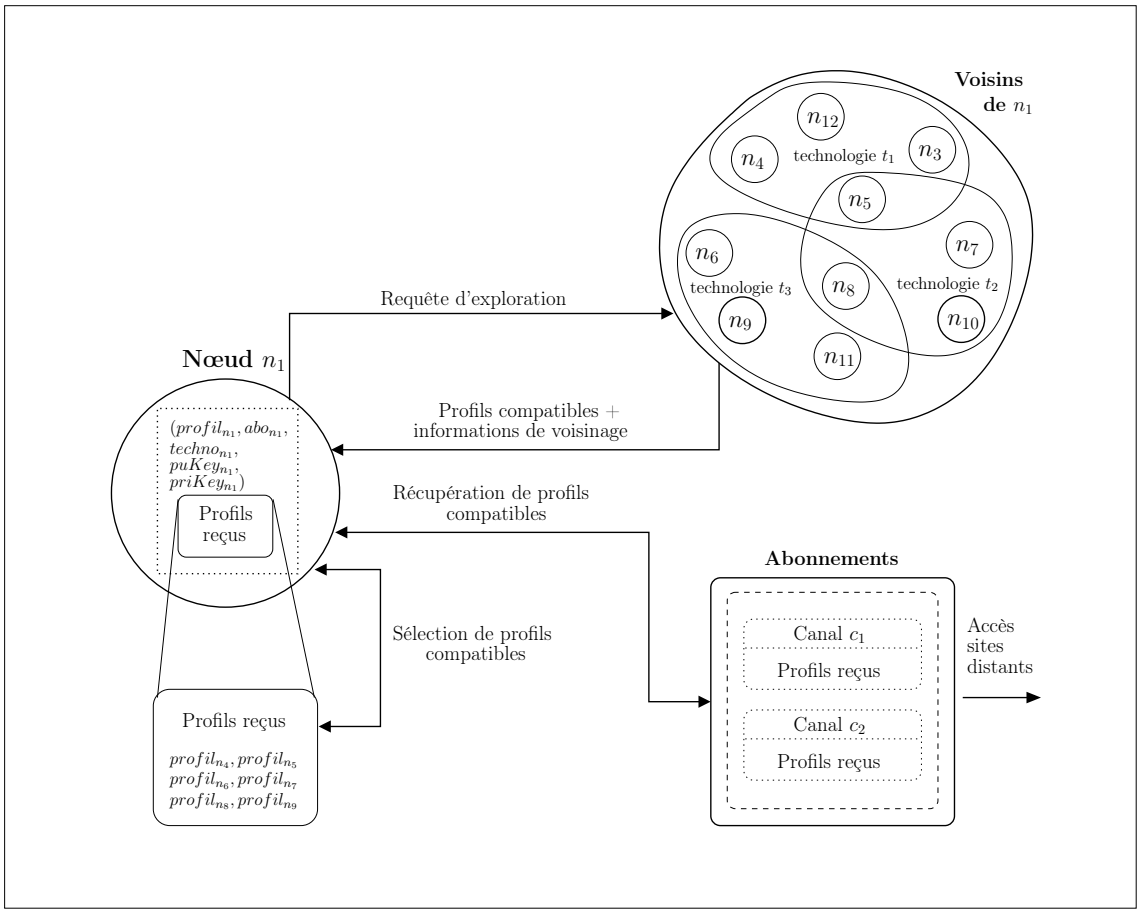


FIGURE 3.43 – Recherche de profils compatibles.

pour caractériser les grands contributeurs) fois à un besoin de n_i et les nœuds marqués comme étant de grands contributeurs par les entités qui ont envoyés leurs profils (voisins ou canal d'abonnement) à n_i, est également défini. L'ensemble $N_{n_i,rares}$ quant à lui regroupe les nœuds dont le profil est considéré comme rare par n_i et les nœuds marqués comme ayant un profil rare par les entités (voisins ou canal d'abonnement) qui les ont transmises à n_i. Nous définissons également l'ensemble $N_{n_i,distants}$ comme étant l'ensemble des nœuds qui peuvent être contactés par n_i à travers les canaux accessibles (c'est à dire via les abonnements auxquels le nœud a souscrit) ; cette liste est établie lors de l'étape de recherche de profils sauvegardés à travers les abonnements auxquels n_i a souscrit. On suppose que $N_{potentiels}$ correspond à l'ensemble des nœuds dont le profil appartient à $L_{potentiels}$ et N_{cibles} correspond à l'ensemble des nœuds dont le profil appartient à L_{cibles}. Nous spécifions les éléments de l'ensemble L_{cibles} de la manière suivante :

- On calcule $N_1 = N_{potentiels} \cap (V_{n_i}(t) \cup N_{n_i,distants})$ (on ne garde que les nœuds accessibles)
- On calcule N_2 comme suit. Si $N_1 \setminus N_{n_i,actifs} \neq \varnothing$ alors $N_2 = N_1 \setminus N_{n_i,actifs}$ sinon $N_2 = N_1$ (on retire les nœuds actifs, s'il n'y a pas que des nœuds de ce type, de l'ensemble N_2)

- On calcule maintenant N_3 comme suit.. Si $N_2 \backslash N_{n_i,rare} \neq \varnothing$ alors $N_3 = N_2 \backslash N_{n_i,rares}$ sinon $N_3 = N_2$ (on retire les nœuds au profil rare, s'il n'y a pas que des nœuds de ce type, de l'ensemble N_3)
- Si $N_3 \cap N^t_{n_i,isoles} \neq \varnothing$ alors $N_{cibles} = N_3 \cap N^t_{n_i,isoles}$ sinon $N_{cibles} = N_3$ (on retire les nœuds isolés, s'il n'y a pas que des nœuds de ce type, de l'ensemble N_{cibles})

L_{cibles} est constitué des profils de nœuds appartenant à l'ensemble N_{cibles}. En d'autres termes, L_{cibles} est l'ensemble des profils de nœuds accessibles et correspondant à la spécification de groupe que n_i peut tenter de contacter afin de trouver une réponse à ses besoins, tout en écartant si possibles, les nœuds rares ou potentiellement surchargés. Les étapes qui permettent de spécifier les éléments de l'ensemble L_{cibles} suivent l'ordre présenté ci-dessus car nous considérons qu'il est nécessaire de réduire, autant que possible (et en priorité), la charge des nœuds actifs. L'ensemble L_{cibles} est donc le résultat de la spécification de cibles.

3.1.2.4 Cas particulier d'un unique nœud destinataire

Ce cas particulier illustre la situation où un nœud n_i désire entrer en contact avec un nœud n_j qu'il a par exemple au préalable déjà physiquement rencontré sans tenir compte des caractéristiques particulières de son profil. Il n'y a donc pas de requête d'exploration liée à une définition de profil de groupe, mais c'est le nœud n_i qui choisit de façon arbitraire l'entité avec laquelle communiquer. Deux conditions doivent être remplies afin de rendre possible cette opération :

- il faut s'assurer que le profil de n_j fait partie des profils reçus par n_i et que ce profil contient les informations nécessaires à une demande de contact par n_i.
- il faut vérifier à l'aide d'une procédure particulière que le nœud n_j est accessible à l'instant t où la demande de contact est effectuée par le nœud n_i.

Concernant la première condition, le fait de posséder le profil du nœud n_j permet au nœud n_i de connaître les caractéristiques et les préférences de n_j en termes de mode de communication. Le profil de n_j doit contenir les technologies de communication par lesquelles ce nœud peut être contacté, les adresses de connexion correspondant à ces technologies ainsi que les éventuels abonnements auxquels n_j a souscrit.
Pour la deuxième condition, une procédure de *ping* est mise en place. Elle consiste à vérifier qu'à l'instant t, le nœud n_i est capable d'utiliser au moins une technologie de communication ou un abonnement pour entrer en contact avec le nœud n_j. Il s'agit donc de contrôler qu'il existe une technologie t_q appartenant à $techno_{n_j}$ ou un abonnement c_k appartenant à abo_{n_i} qui permet de contacter n_j. De façon pratique, le nœud n_i parcourt l'ensemble des technologies de communication mentionnées dans le profil de n_j et pour chacune d'elle il tente de se connecter (sans envoyer de message) en utilisant l'adresse de connexion correspondante. Si la connexion est possible, l'opération de vérification est arrêtée ; dans le cas contraire l'opération se poursuit jusqu'à ce que toutes les technologies (du profil de n_j) aient fait l'objet d'une tentative de connexion. Lorsque cela est nécessaire, c'est à dire dans le cas où les tentatives de connexion directes n'ont pas abouti, n_i émet une requête à travers ses différents abonnements pour déterminer s'il existe un canal de abo_{n_i} qui permet de contacter n_j. Il est noter que les différents canaux répondent à la requête suivant les informations dont ils disposent et qui proviennent des opérations de publication de profil de n_j.

Dans le cas particulier que nous avons décrit, le problème se résume donc à contrôler que le nœud choisi par l'émetteur remplit les conditions nécessaires pour être contacté. En conséquence, s'il existe au moins une technologie de communication ou un abonnement par lequel le nœud cible est accessible (à l'instant t de la demande de contact) alors $N_{cibles} = \{n_j\}$, sinon $N_{cibles} = \varnothing$.

3.1.3 Choisir une technologie

Le problème à résoudre à ce niveau est le suivant : quelle technologie t_j doit utiliser un nœud n_i à un instant t donné pour émettre un message à destination d'une autre entité du système en prenant en compte les préférences (en termes de technologies à utiliser pour communiquer) contenues dans le profil de l'émetteur et du destinataire ? Il s'agit donc, en partant des résultats de la spécification d'un ensemble de cibles, de définir la procédure qui permet à un nœud n_i de sélectionner la technologie la plus appropriée (en fonction du contexte) pour contacter l'entité qui peut répondre à ses besoins ou à laquelle une information doit être transmise. Dans le cadre de notre étude nous retenons deux critères principaux dans le choix de cette technologie :

- la minimisation des coûts (au niveau énergétique et financier) et la maximisation des performances. Ces points intègrent les spécificités et les préférences, en termes de moyens de communication disponibles, des nœuds impliqués (émetteur et récepteur). De façon concrète, il s'agit par exemple de choisir une technologie t_j de façon à s'assurer que la combinaison de $coutE(t_j)$ et $coutF(t_j)$ soit minimale et $debit(t_j, t)$ maximum pour les nœuds impliqués (comme cela sera expliqué plus loin).
- l'historique des communications déjà effectuées. Il peut s'avérer pertinent, dans certains cas, d'effectuer un choix technologique, pour émettre un message, en fonction des données recueillies au préalable. En clair, il s'agit de tenter de contacter une entité du système uniquement à travers des technologies avec lesquelles des communications ont déjà eu lieu.

Pour les deux principaux critères que nous avons retenus, des contraintes et des paramètres supplémentaires sont à prendre en compte dans le choix de la technologie pour émettre un message à partir d'un nœud n_i donné vers un nœud n_j donné. Les différentes contraintes du système sont de deux ordres : les contraintes liées au profil du nœud émetteur et les contraintes liées à l'entité vers laquelle un message doit être émis. Ces différents éléments à prendre en compte permettent à la fois de définir l'ensemble T' (sous-ensemble de T, ensemble des technologies du système) dans lequel le choix de technologie doit être effectué ainsi que l'importance (poids) qui doit être accordée aux différents paramètres de coût et de performance.

Dans son profil un nœud peut définir ses préférences en matières de consommation énergétique et de coût financier pour l'émission ainsi que pour la réception de messages. Supposons par exemple que dans les calculs de minimisation des coûts, $poidsE$ et $poidsF$ correspondent respectivement à l'importance attribuée aux paramètres $coutE$ et $coutF$. Dans le cas où la consommation énergétique est particulièrement sensible et doit donc être limitée, la valeur de $poidsE$ sera élevée et inversement la valeur de $poidsF$ sera basse. Au contraire, dans la situation où l'aspect financier a un caractère crucial, la valeur de $poidsF$ sera élevée. On peut également considérer qu'en dessous d'un certain niveau d'énergie, un nœud peut préférer l'utilisation d'une certaine technologie (même si elle très coûteuse au

niveau financier), ou alors que, pendant un laps de temps défini, un nœud privilégie un type de technologie en particulier (même très coûteuse au niveau de la consommation en énergie). L'affectation des valeurs à $poidsE$, $poidsF$ et aux autres poids possibles s'effectue en fonction des contraintes liées au profil du nœud considéré (en mode émission ou réception). Il s'agit des *priorités en termes de coûts et de débit* et des *préférences en termes de mode de réception*.
Un autre point important est la définition de l'ensemble T' (ensemble dans lequel le choix de technologie doit être effectué). L'historique d'émission des messages, ainsi que les capacités et les limitations technologiques des nœuds impliqués permettent de déterminer les éléments de l'ensemble T'. En ce qui concerne l'historique d'émission, il s'agit, pour un émetteur, de conserver une trace des technologies utilisées pour contacter un nœud donné. Dans le cas où ce critère est retenu dans le choix de la technologie, l'ensemble T' est constitué des technologies avec lesquelles des échanges ont déjà été effectués avec le nœud destinataire. Dans le cas des capacités et des limitations technologiques, il s'agit de considérer les technologies dont sont équipés les nœuds. Dans un échange direct, l'émetteur et le récepteur doivent avoir au moins une technologie de communication en commun.

En partant de la spécifications de cibles, la figure 3.44 présente les étapes que nous mettons en œuvre pour effectuer le choix d'une technologie pour un nœud donné. Tout d'abord, il est nécessaire de prendre en compte les préférences du nœud. Cette prise en compte consiste à spécifier les priorités en terme de minimisation des coûts et de maximisation des performances ainsi que tous les autres éléments (que nous détaillons dans les sections suivantes) qui peuvent avoir une influence sur la manière dont le choix de technologie est effectué. Ensuite, en utilisant les résultats de la spécification de cibles, deux possibilités sont offertes au nœud. Soit il décide de contacter un nœud particulier, soit il laisse le système déterminer la meilleure cible en fonction des différentes contraintes qui existent. Dans le premier cas, il est nécessaire de procéder à la sélection de la meilleure technologie pour atteindre la cible particulière. Cette sélection s'effectue en procédant à des calculs qui permettent de concilier les préférences des deux nœuds impliqués. Dans le second cas, l'objectif est de déterminer, en fonction des informations disponibles, la cible la plus appropriée. Cette sélection de cible s'effectue par des calculs qui permettent de choisir le nœud cible qui possède les caractéristiques correspondant (dans la mesure du possible) aux préférences de l'émetteur. Lorsque la sélection est possible, dans l'un ou l'autre des cas, le message est alors envoyé avec la technologie choisie au nœud désigné. Enfin, avant de reprendre la procédure de choix d'une technologie lorsqu'une nouvelle spécification de cibles est effectuée, le système doit prendre en compte les événements qui surviennent dans son environnement au sens large et qui pourraient avoir un impact sur les préférences du nœud émetteur. Les quatre sections suivantes développent les étapes principales nécessaires au choix de la technologie.

3.1.3.1 Spécifications des préférences

Pour chaque nœud n_i une fonction C_{n_i}, de coûts et de performance est définie de la façon suivante :

- $C_{n_i}(t_j) = poidsE_{n_i}.coutE_{n_i}(t_j) + poidsF_{n_i}.coutF_{n_i}(t_j) + \frac{poidsD_{n_i}}{debit_{n_i}(t_j,t)}, t_j \in techno_{n_i}$
  avec $poidsE_{n_i} + poidsF_{n_i} + poidsD_{n_i} = 1$

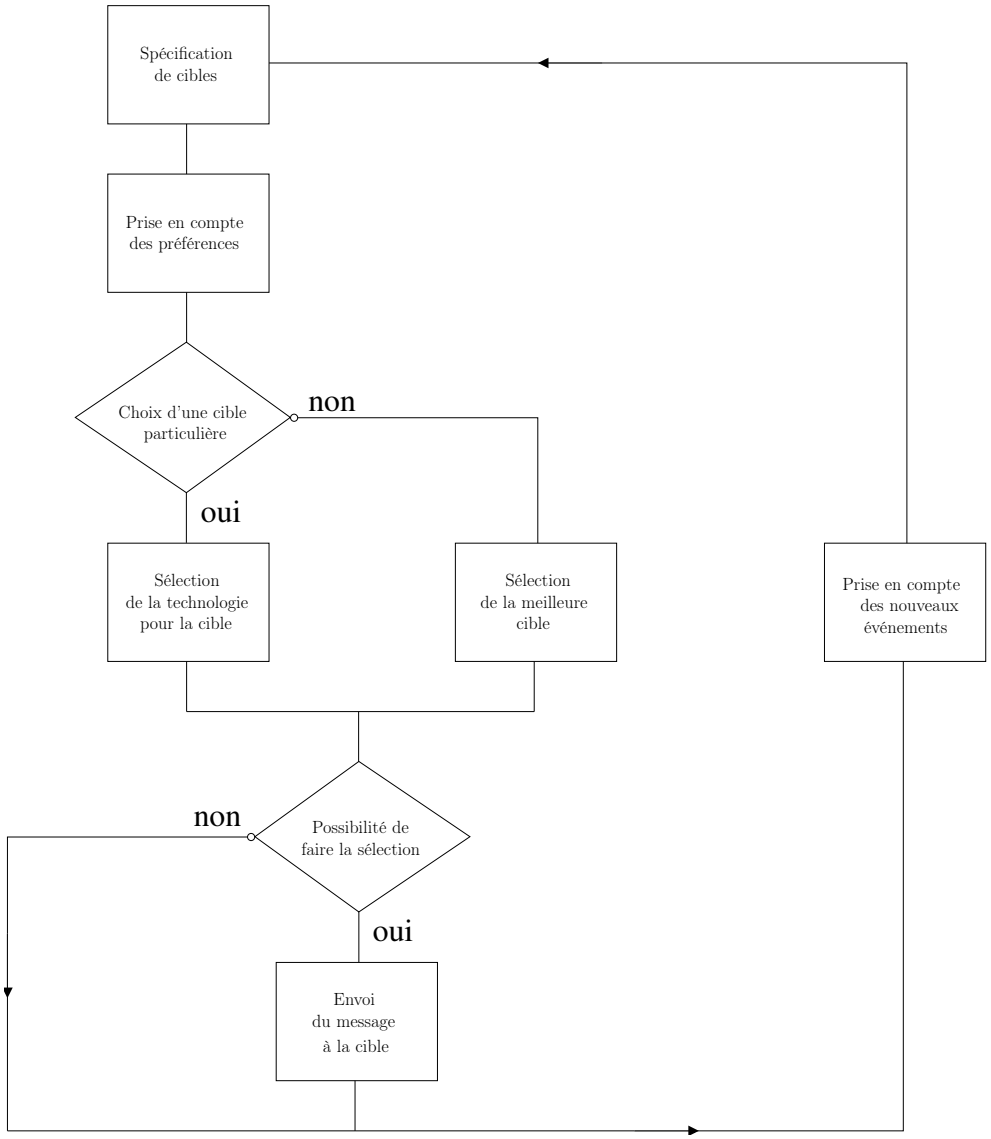


FIGURE 3.44 – Étapes dans le choix d'une technologie.

$poidsE_{n_i}$, $poidsF_{n_i}$ et $poidsD_{n_i}$ représentent respectivement les poids des paramètres $coutE_{n_i}$, $coutE_{n_i}$ et $poidsD_{n_i}$. La fonction C_{n_i} permet de déterminer, pour le nœud n_i, la technologie qui permet de minimiser les coûts et de maximiser les performances. Pour cela, on calcule $\min C_{n_i}$. Il est possible de généraliser la définition de la fonction C_{n_i}, pour le nœud n_i, afin de prendre en compte des paramètres qui n'ont pas encore été définis dans le modèle ou qui pourraient faire partie des caractéristiques à ajouter dans le but de l'améliorer le modèle :

– $C_{n_i}(t_j) = \sum_{k=1}^{a}(poids_{[n_i,k]}.coutMin_{[n_i,k]}(t_j)) + \sum_{l=1}^{b}(\frac{poids_{[n_i,l]}}{coutMax_{[n_i,l]}(t_j)}), t_j \in techno_{n_i}$
avec $\sum_{k=1}^{a} poids_{[n_i,k]} + \sum_{l=1}^{b} poids_{[n_i,l]} = 1$

où $coutMin_{[n_i,k]}$ représente les critères à minimiser tels que $coutE$ et $coutF$ tandis que $coutMax_{[n_i,l]}$ représente les critères à maximiser tel que $debit$. Leurs poids respectifs sont

$poids_{[n_i,k]}$ et $poids_{[n_i,l]}$. Afin de rendre les calculs de C_{n_i} cohérents, il est nécessaire que les valeurs de $coutMin_{[n_i,k]}$ et de $coutMax_{[n_i,l]}$ soient des valeurs normalisées car elles ne sont pas nécessairement définies avec la même unité de mesure (par exemple le débit et le coût financier n'ont pas la même unité de mesure). Cette normalisation s'opère de la façon suivante :

- $coutMin_{[n_i,k]}(t_j) = \frac{coutMinBrut_{[n_i,k]}(t_j)}{\max coutMinBrut_k(t_j)}$, avec $coutMinBrut_{[n_i,k]}(t_j)$ qui est la valeur brute du paramètre avec l'unité de mesure usuelle et $\max coutMinBrut_k(t_j)$ qui la valeur maximale que le paramètre peut atteindre pour la technologie t_j.

Pour effectuer le calcul de $\min C_{n_i}$, il est également nécessaire de définir les valeurs de $poids_{[n_i,k]}$ et $poids_{[n_i,l]}$ en fonction des préférences du nœud considéré. Pour définir ces valeurs, nous proposons plusieurs options :

- l'option **verte** dans laquelle 0,5 est affecté à $poidsE_{n_i}$ et les 0,5 restant sont répartis également entre les autres poids. Cette option privilégie les situations où la consommation énergétique doit être limitée.
- l'option **économe** dans laquelle 0,5 est affecté à $poidsF_{n_i}$ et les 0,5 restant sont répartis également entre les autres poids. Cette option privilégie les situations où les coûts financiers doivent être réduits.
- l'option **efficace** dans laquelle 0,5 est affecté à $debit_{n_i}$ et les 0,5 restant sont répartis également entre les autres poids. Cette option privilégie les situations où l'efficacité des communications (en termes de délais de transmission) est l'élément le plus important.
- l'option **personnelle** dans laquelle le nœud définit lui-même les valeurs à affecter aux poids des différents paramètres.

Chaque nœud n_i doit donc spécifier, dans ses préférences, l'option choisie pour gérer les différents calculs relatifs à sa fonction C_{n_i}. Il est à noter que nous déclinons la fonction C_{n_i} en deux versions : une version $C_{[n_i,e]}$ dans laquelle les paramètres sont définis en prenant en compte le mode émetteur pour le nœud considéré et une version $C_{[n_i,r]}$ qui prend en compte le mode récepteur. Cette déclinaison permet d'effectuer les calculs (de coûts et de performance) suivant le rôle (émetteur ou récepteur) du nœud considéré.

L'utilisation de l'historique des communications effectuées, quant à lui, se base sur une trace de la technologie utilisée pour communiquer avec une autre entité du réseau. Il est alors possible de classer les technologies suivant le nombre de fois où elles ont permis des échanges avec une cible particulière. Plus ce nombre est élevé pour une technologie donnée, plus il est probable que cette technologie peut être à nouveau envisagée pour communiquer avec la cible considérée.

En résumé, concernant le choix de technologie, chaque nœud n_i doit spécifier ses préférences en fournissant les informations suivantes :

- les options retenues (verte, économe, efficace ou personnelle) afin de déterminer les poids des paramètres dans les calculs liés aux fonctions $C_{[n_i,e]}$ et $C_{[n_i,r]}$;
- le critère à utiliser pour procéder au choix de technologie lorsque le nœud souhaite envoyer un message (mode émission) et lorsque le nœud est une cible potentielle (mode réception). Dans les deux cas, soit le nœud préfère minimiser les coûts et maximiser les performances soit il préfère privilégier l'historique des communications.

3.1.3.2 Sélection d'une technologie

Le passage par cette étape signifie que le nœud n_i qui veut émettre un message a désigné une cible particulière n_q à laquelle il souhaite s'adresser. Nous détaillons dans la suite la sélection d'une technologie suivant les deux critères possibles présentés dans la section précédente.

Utilisation de l'historique des communications. Le nœud n_i procède au classement des technologies (dont il est équipé et dont il souhaite éventuellement se servir) qui ont déjà permis de contacter le nœud n_q. Plus une technologie a déjà été utilisée plus elle possède une position élevée dans le classement. Ainsi, l'opération de sélection se déroule en partant du haut du classement et en choisissant la première technologie disponible et toujours active au niveau de n_q. Si plusieurs technologies ont le même classement (même nombre d'émissions réalisées vers n_q), elles sont départagées en utilisant le paramètre (en mode émission) que le nœud n_i privilégie le plus [1] en fonction de l'option choisie (verte, économe, efficace ou personnelle). En d'autres termes, en cas d'égalité, si le paramètre privilégié est à minimiser ($coutMin_{[n_i,k]}$) alors plus sa valeur est basse plus le classement de la technologie est élevé, par contre si le paramètre est à maximiser ($coutMax_{[n_i,l]}$) alors plus sa valeur est élevée plus le classement de la technologie est élevé. Il existe l'éventualité dans laquelle le nœud n_q, en fonction des préférences spécifiées dans son profil, ne souhaite pas recevoir de message émis suivant le critère de l'historique des communications. Dans ce cas, le nœud n_i doit changer de critère à utiliser dans le choix de la technologie ou changer de cible à atteindre. Le changement de critère ou le changement de cible est également nécessaire lorsque l'ensemble des technologies qui ont fait l'objet du classement par n_i ne sont plus ni disponibles ou actives pour n_q.

Minimisation des coûts et maximisation des performances. Il s'agit de calculer la fonction $C_{[n_i,e]}$ pour le nœud n_i et la fonction $C_{[n_q,r]}$ pour le nœud n_q. Nous utiliserons dans la suite les définitions suivantes :

- **coût minimum d'émission**. On définit $\mu_{[n_i,e]} = \min C_{[n_i,e]}$, le minimum de la fonction de coût en émission du nœud n_i.
- **coût minimum de réception**. On définit $\mu_{[n_q,r]} = \min C_{[n_q,r]}$, le minimum de la fonction de coût en réception du nœud n_q.
- On définit les fonctions $C^{-1}_{[n_i,e]}$ et $C^{-1}_{[n_q,r]}$ réciproques respectivement de $C_{[n_i,e]}$ et de $C_{[n_q,r]}$ qui, à partir d'une valeur de coût, retournent la ou les technologies qui permettent de réaliser ce coût.
- **technologie optimale en émission**. On définit $\tau_{[n_i,e]} = C^{-1}_{[n_i,e]}(\mu_{[n_i,e]})$, la ou les technologies qui permettent de réaliser la valeur minimale de la fonction de coût $C_{[n_i,e]}$.
- **technologie optimale en réception**. On définit $\tau_{[n_q,r]} = C^{-1}_{[n_q,r]}(\mu_{[n_q,r]})$, la ou les technologies qui permettent de réaliser la valeur minimale de la fonction de coût $C_{[n_q,r]}$

Nous analysons alors le critère de minimisation des coûts et de maximisation des performances dans les deux cas de figure suivants :

1. On n'utilise pas l'ensemble de la fonction de coût.

(i) si $\tau_{[n_i,e]} = \tau_{[n_q,r]}$, on choisit alors la technologie $t_{choix} = \tau_{[n_i,e]} = \tau_{[n_q,r]}$ pour émettre le message

(ii) si $\tau_{[n_i,e]} \neq \tau_{[n_q,r]}$, il faut alors déterminer la technologie optimale pour permettre à n_i et n_q de communiquer. En d'autres termes, il s'agit de choisir la technologie t_{choix} avec laquelle les coûts seront les plus faibles en fonction des préférences (liées aux fonctions de coûts) des nœuds impliqués dans l'échange à effectuer. Pour cela nous utilisons une adaptation de la méthode des moindres carrés [13] à travers deux nouvelles fonctions $O_{[n_i,n_q,e]}$ et $O_{[n_i,n_q,r]}$ (et leurs fonctions réciproques respectives $O^{-1}_{[n_i,n_q,e]}$ et $O^{-1}_{[n_i,n_q,r]}$) que nous définissons ici.
$O_{[n_i,n_q,e]}(t_j) = (C_{[n_i,e]}(t_j) - \mu_{[n_i,e]})^2 + poids_r (C_{[n_q,r]}(t_j) - \mu_{[n_q,r]})^2$ avec $t_j \in techno_{n_i} \cap techno_{n_q}$ et $poids_r > 1$; on définit également $\theta_{[n_i,n_q,e]} = \min O_{[n_i,n_q,e]}$, le minimum de la fonction $O_{[n_i,n_q,e]}$ sur les technologies considérées.
$O_{[n_i,n_q,r]}(t_j) = poids_e (C_{[n_i,e]}(t_j) - \mu_{[n_i,e]})^2 + (C_{[n_q,r]}(t_j) - \mu_{[n_q,r]})^2$ avec $t_j \in techno_{n_i} \cap techno_{n_q}$ et $poids_e > 1$; on définit également $\theta_{[n_i,n_q,r]} = \min O_{[n_i,n_q,r]}$, le minimum de la fonction $O_{[n_i,n_q,r]}$ sur les technologies considérées.
Le minimum de chacune de ces fonctions ($\theta_{[n_i,n_q,e]}$ et $\theta_{[n_i,n_q,r]}$) permet de déterminer la meilleure option quant au choix de t_{choix} pour les nœuds impliqués (n_i et n_q). La différence entre les fonctions $O_{[n_i,n_q,e]}(t_j)$ et $O_{[n_i,n_q,r]}(t_j)$ se situe dans le fait que la première privilégie une solution minimale plus proche de l'optimal du nœud récepteur n_q tandis que la deuxième privilégie une solution minimale plus proche de l'optimal du nœud émetteur n_i. En pratique, lorsque c'est le nœud n_i qui recherche une information auprès du nœud n_q, les préférences de n_q sont plus particulièrement considérées (afin de minimiser au mieux ses coûts comme il n'est pas l'initiateur de l'échange) et alors $t_{choix} = O^{-1}_{[n_i,n_q,e]}(\theta_{[n_i,n_q,e]})$. Dans le cas contraire, ce sont les préférences de n_i qui sont plus particulièrement prises en compte et $t_{choix} = O^{-1}_{[n_i,n_q,r]}(\theta_{[n_i,n_q,r]})$. Les valeurs des poids des termes, dans chacune des fonctions, sont donc choisies en conséquence. Dans la fonction $O_{[n_i,n_q,e]}(t_j)$ le terme contenant $\mu_{[n_i,e]}$ a un poids égal à 1 et le terme contenant $\mu_{[n_q,r]}$ a un poids $poids_r > 1$ alors que dans la fonction $O_{[n_i,n_q,r]}(t_j)$ le terme contenant $\mu_{[n_i,e]}$ a un poids $poids_e > 1$ et le terme contenant $\mu_{[n_q,r]}$ a un poids égal à 1. Le choix de la valeur des poids $poids_r$ et $poids_e$ est fait en fonction de l'importance à accorder au terme associé (par rapport à l'autre terme de la fonction). Plus cette valeur est élevée plus le terme prend de l'importance dans la fonction considérée.

3.1.3.3 Sélection d'une cible

Le passage par cette étape signifie que le nœud qui veut émettre un message n'a pas désigné de cible particulière à laquelle s'adresser. Parmi les éléments de l'ensemble qui résulte de la spécification des cibles, une cible particulière doit donc être sélectionnée afin d'expédier le message. Il s'agit alors, suivant les deux critères possibles, de déterminer comment s'effectue la sélection de cette cible ainsi que la méthode à utiliser pour le choix de la technologie à utiliser pour atteindre la cible sélectionnée. Soient n_i le nœud émetteur et S_{n_i} l'ensemble résultant de la spécification de cibles.

Historique des communications. Le nœud n_i procède au classement des éléments de

S_{n_i} suivant le nombre de fois où des communications ont déjà été établies avec ces entités. Le nœud n_k appartenant à S_{n_i} et avec lequel n_i a le plus souvent eu des échanges est alors choisi. Si plusieurs nœuds de S_{n_i} ont autant d'échanges avec S_{n_i}, ils sont départagés en comparant le nombre total d'émissions des technologies de communication disponibles. n_i détermine la technologie la plus souvent utilisée pour effectuer des échanges avec chacun des nœuds à départager et le nœud avec lequel le plus grand nombre d'échanges ont été effectués (dans la technologie déterminée) est sélectionné. Dans le cas où plusieurs nœuds se trouvent à nouveau à égalité, un nœud est choisi au hasard parmi ceux-ci. Ainsi, un nœud est finalement sélectionné pour servir de destinataire au message que n_i souhaite émettre. Dans la suite, pour déterminer la technologie que doit utiliser n_i pour communiquer avec le destinataire désigné, la procédure mise en œuvre est celle qui est décrite pour la sélection de technologie suivant le critère de l'historique des communications (section 3.1.3.2). Ceci est parfois fait partiellement au cours du choix de la cible (juste au-dessus) dans le cas où il est nécessaire de départager plusieurs nœuds.

Minimisation des coûts et maximisation des performances. Le nœud n_i classe les éléments de S_{n_i} suivant la valeur moyenne de leurs fonctions de coûts en mode récepteur. Soit n_q un élément de S_{n_i} et $mC_{n_q,r}$ la valeur moyenne de sa fonction de coûts en mode récepteur ; nous avons :

- $mC_{n_q,r} = \frac{1}{Card(T_{n_i})} \sum_{t_s \in T_{n_i}} C_{[n_q,r]}(t_s)$

Le nœud n_k choisi est celui pour lequel cette moyenne est minimale. Le nœud n_k est alors considéré comme étant la cible pour l'émission du message à envoyer. Par ce moyen un nœud est automatiquement sélectionné pour servir de destinataire du message que doit émettre n_i. Dans l'étape suivante, pour déterminer la technologie que doit utiliser n_i pour communiquer avec le destinataire désigné, la procédure utilisée est celle qui est décrite pour la sélection de technologie suivant le critère de la minimisation des coûts et de la maximisation des performances (section 3.1.3.2).

3.1.3.4 Ajustement des paramètres

Cette étape permet à un nœud n_i donné de modifier ses préférences quant à l'envoi ou à la réception de messages lorsque des événements survenus dans son environnement propre ou extérieur peuvent avoir un impact sur la manière dont il effectue ses opérations. Le nœud a ainsi la possibilité de changer de critère quant au choix de technologie en mode émetteur et récepteur et de changer l'option retenue pour déterminer les poids des paramètres dans les fonctions $C_{[n_i,e]}$ et $C_{[n_i,r]}$.
Les événements qui ont un impact sur les opérations que peut effectuer un nœud sont de deux types et sont liés aux critères de choix d'une technologie :

- **les événements impactant l'historique des communications.** Il s'agit par exemple de la prise de connaissance de l'existence d'un nœud jusqu'alors inconnu et pour lequel la notion d'historique ne peut donc pas être appliquée. Il s'agit également des réceptions de messages qui conduisent à déterminer que le nombre d'échanges effectués avec certains nœuds représente une proportion trop faible pour en tirer des conclusions. Dans ces cas de figure, l'historique ne peut plus être utilisée et on bascule sur le mode fonction de coûts.

Mode \ ***Critères***	Historique	Coûts et performances
Manuel	- sélection par le nœud du critère qu'il souhaite utiliser dans le choix de technologie	- sélection par le nœud du paramètre qu'il désire privilégier (et donc préserver) dans le calcul des coûts et des performances
Automatique	- changement automatique de critère pour utiliser la minimisation des coûts et la maximisation des performances dans le choix de technologie	- changement automatique en privilégiant les paramètres (dans le calcul des coûts et des performances) qui ont fait l'objet de la notification d'événements

Table 3.15 – Possibilités d'ajustement des paramètres suivant les critères choisis.

– **les événements liés à la minimisation des coûts et à la maximisation des performances.** Les événements de cette catégorie peuvent changer l'importance qu'accorde le nœud considéré à un ou plusieurs paramètres des fonctions de minimisation des coûts et de maximisation des performances (les fonctions $C_{[n_i,e]}$ et $C_{[n_i,r]}$ pour le nœud n_i). Il s'agit d'abord des situations où le niveau de certains coûts atteint un maximum ou un minimum (selon un certain seuil spécifié) sans pouvoir retrouver un niveau satisfaisant pour le nœud. C'est par exemple le cas lorsque le niveau de la batterie du nœud devient faible ou encore lorsque les dépenses financières liées aux communications effectuées atteignent un seuil à ne pas dépasser. Il s'agit également des situations où le niveau d'un paramètre atteint une valeur remarquable pendant un certains laps de temps. C'est par exemple le cas lorsque le débit d'une technologie a un niveau très élevé pendant un certain temps ou encore lorsque l'utilisation d'une technologie n'engendre pas de coûts financiers à certaines heures. Ces événements sont portés à la connaissance du nœud considéré sous forme d'alertes.

Après avoir identifié la nature des événements qui peuvent entraîner un ajustement de paramètres, il est nécessaire de s'intéresser à la manière dont les modifications des préférences d'un nœud doit d'effectuer. Pour cela deux options sont possibles :

– **Manuellement.** Dans ce cas, lorsque le nœud considéré est notifié d'un ou plusieurs événements, il ajuste ses paramètres en choisissant lui-même de faire les changements qui lui semblent pertinents en fonction du contexte et de ses besoins.
– **Automatiquement.** Dans ce cas, les événements qui interviennent déclenchent automatiquement une modification des préférences du nœud considéré afin de prendre en compte les nouvelles caractéristiques.

Ces deux possibilités sont résumées dans le tableau 3.15 Il est important de noter que chaque nœud doit avoir spécifié dans son profil les préférences en matière d'ajustement des paramètres, c'est à dire préciser si les modifications doivent s'effectuer de façon manuelle ou de façon automatique suivant les différents types possibles d'événements.

3.1.4 Échanger des profils

Il s'agit de proposer une méthode qui permet à deux nœuds (n_i et n_j) qui se rencontrent physiquement, c'est à dire qui se retrouvent physiquement en contact l'un avec l'autre, d'échanger de façon simple et sécurisée des informations concernant leurs profils respectifs. L'échange de profils dans ce cadre se différencie de la publication de profils par le fait que cet échange concerne uniquement deux nœuds dont la proximité physique va être exploitée afin de transmettre des informations à caractère privé. Contrairement à la publication de profils où les informations diffusées sont publiques ($kernel_{n_k}$ pour un nœud n_k donné), les données dont il est question dans cette opération d'échange sont des données "sensibles" (adresse de connexion d'une technologie de l'ensemble T_{Re} par exemple) que les nœuds considérés choisissent librement de transmettre à des entités de confiance. Dans la suite, une méthode pour réaliser ces opérations d'échange entre deux nœuds n_i et n_j physiquement proches l'un de l'autre va être décrite [2].

3.1.4.1 Méthode d'échange de profils entre deux nœuds

La figure 3.45 décrit le processus que nous proposons de mettre en place pour réaliser cet échange de profils entre deux nœuds n_i et n_j. Il est à noter que lorsque le profil d'un nœud est mentionné pour la description des opération d'échange, il s'agit des informations privées (informations personnelles, adresses de connexion à une technologie donnée, etc.) à transmettre.
Tout d'abord le nœud n_i, qui souhaite initier l'échange, utilise un canal privé (unidirectionnel) qui repose sur la proximité des deux nœuds impliqués pour transmettre sa clé publique ($clePub_{n_i}$) et des informations de connexion ($config_{ni}$) pour permettre à n_j de lui répondre. Le nœud cible n_j, à la réception des données envoyées par n_i, transmet les informations de son profil qu'il souhaite partager (dans le cas où il valide l'échange) ainsi que sa clé publique ($clePub_{n_j}$) après les avoir chiffrées avec la clé publique de n_i incluse dans les données reçues. Ces informations sont transmises en utilisant les informations de connexion fournies par n_i. En retour, n_i envoie les informations de son profil après les avoir chiffrées avec la clé publique du destinataire en utilisant la même technologie que n_j. Ainsi, les deux nœuds considérés peuvent échanger de façon sécurisée des informations concernant leurs profils respectifs.

3.1.4.2 Caractéristiques de la méthode d'échange de profils

Certains éléments concernant cette méthode d'échange de profils doivent être précisés afin de comprendre le contexte dans lequel les différentes opérations sont effectuées. Ces éléments sont les suivants :

- la technologie à utiliser, pour constituer le canal privé par lequel l'échange est initié, doit être une technologie de communication dont les caractéristiques sont liées à la proximité physique entre les nœuds impliqués. Le canal doit permettre de déclencher un échange rapide (généralement unidirectionnel) et automatique d'une quantité limitée de données sans que cela ne nécessite au préalable la connaissance d'une adresse de connexion. Ces caractéristiques permettent d'initier simplement et rapidement l'échange de profils. Un exemple de technologie de ce type est le NFC (Near

2. Typiquement en utilisant la technologie NFC - cf. plus loin -

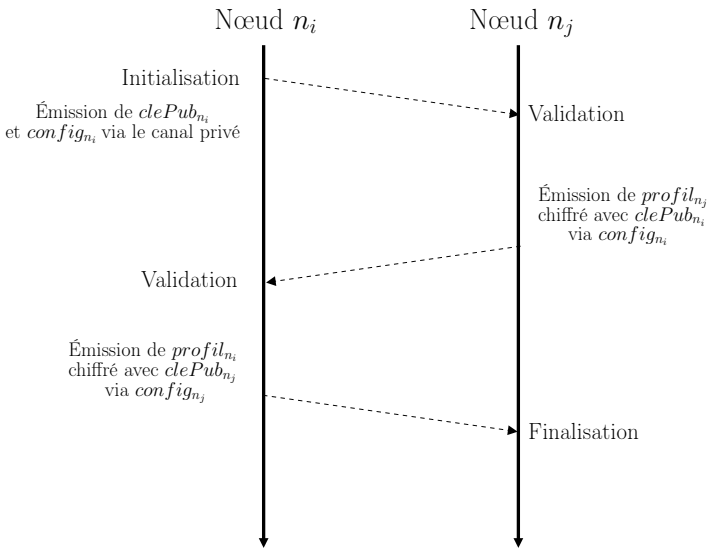


Figure 3.45 – Échange de profils lors d'une rencontre physique entre deux nœuds.

Field Communication) qui est une technologie sans fil avec une portée d'environ 10 cm [44]. Le fait que le canal privé soit limité (c'est le cas avec la technologie NFC) en terme de volume d'information à transmettre implique l'utilisation d'une autre technologie de communication pour échanger les données concernant les profils. Ce besoin d'une technologie alternative explique le fait que le premier nœud impliqué dans les opérations, après l'initialisation, fournisse une adresse de connexion (à son correspondant) suivant une technologie de communication plus classique.

- il est nécessaire de s'assurer de la confiance associée aux opérations effectuées au cours de l'échange. Dans la phase d'initialisation, le fait que les nœuds se "voient" physiquement (en raison de leur proximité) leur permet de se faire confiance. Cette confiance permet aux nœuds n_i et n_j (figure 3.45), chacun à leur tour, de valider l'émission ou la réception des informations à échanger.
- les informations à transmettre ont un caractère privé et elles sont donc chiffrées avant toute émission contrairement à ce qui se passe lors de la publication de profils où les données publiées transitent en "clair". En effet, c'est parce que les données transmises par cette méthode sont considérées comme sensibles et n'ont donc pas vocation à être rendues publiques que l'utilisation du canal privé et la validation des échanges sont nécessaires.

3.1.5 Sécuriser les communications et contrôler l'anonymat

Après avoir déterminé la meilleure technologie t_k à utiliser (en fonction des préférences des parties concernées), un nœud peut émettre des messages en se connectant à la cible à atteindre via $adr(t_k)$. Dans certains cas, les informations à échanger peuvent être sensibles et ne doivent pas être accessibles à d'autres entités. Dans d'autres cas, les nœuds impliqués dans des échanges peuvent ne pas souhaiter que leur identité soit révélée. En se basant sur la paire de clés dont chaque nœud dispose, il s'agit donc de mettre en œuvre des mécanismes pour à la fois assurer la sécurité des communications effectuées et pour préserver l'anonymat

des nœuds en fonction du contexte. Nous supposons que chaque nœud est doté d'un module cryptographique qui permet d'effectuer, de façon sûre, des opérations de chiffrement et de déchiffrement, des opérations de signature et des opérations de calcul d'empreintes de données en appliquant des fonctions de hachage.

3.1.5.1 Sécurité des communications

La sécurité des communications a pour objectif de garantir, en cas de besoin, que la confidentialité, l'intégrité et la non-répudiation sont assurées lors des échanges de messages entre nœuds. Les mécanismes (classiques) utilisés se basent sur la paire de clés (clé publique et clé privée) des nœuds concernés par l'échange qui nécessite de prendre des mesures de sécurité. Les objectifs de confidentialité, d'intégrité et de non-répudiation sont atteints en permettant à chaque nœud de chiffrer et de signer un message avant son émission. Les deux possibilités sont les suivantes :

(i) le message m auquel on s'intéresse est le premier message sensible échangé entre n_i et n_j. En plus du message m, on intègre au paquet émis un ensemble d'informations à caractère indispensable ou optionnel. La figure 3.46 présente le contenu du paquet que le nœud n_i envoie au nœud n_j. Le paquet comprend tout d'abord des données relatives au nœud n_i à savoir l'identité que n_i souhaite partager (Id_{n_i}) et l'empreinte de sa clé publique ($E(clePub_{n_i})$). Id_{n_i} représente le nom sous lequel n_i souhaite être connu par ses correspondants. L'empreinte de la clé publique de n_i, qui est obtenue en appliquant une fonction de hachage, permet d'identifier plus rapidement le nœud n_i comme émetteur du message m : dans les situations où il est nécessaire de s'assurer que la clé publique de l'émetteur correspond à une clé particulière, il suffit alors de comparer les empreintes des deux clés (il est à noter que ce point n'est pas directement lié à la sécurité des communications). Le paquet comprend ensuite une information relative à n_j à savoir l'empreinte de sa clé publique ($E(clePub_{n_j})$) (ce qui permet au destinataire de se reconnaître en tant que tel). Le paquet contient également des informations liées au message transmis. Il s'agit du numéro de séquence du message ($NumSeq$) qui permet d'éviter qu'un message identique soit traité plusieurs fois par le nœud destinataire (à la réception d'un message le nœud considéré contrôle le numéro de séquence). Un compteur (pour faire office de numéro de séquence) est affecté à chaque nœud avec lequel n_i peut communiquer. Ce numéro de séquence est incrémenté à chaque émission d'un paquet vers le nœud considéré. Enfin, lorsque le destinataire n'a pas au préalable reçu certaines informations concernant le profil de l'émetteur (notamment sa clé publique), ces informations ($profil_{n_i}$) sont intégrées au paquet à émettre afin de faciliter les éventuels futurs échanges entre n_i et n_j. Le paquet comprend aussi $E(E(clePub_{n_i}) + profil_{n_i})$ [3] qui est l'empreinte des informations relatives à n_i et qui permet d'en vérifier l'intégrité ; à la réception, il suffit de comparer cette empreinte avec le résultat de la fonction de hachage appliquée à la somme de l'empreinte de la clé publique de n_i et du profil de n_i pour déterminer si les données sont valides.
Il est à noter que l'ensemble des informations mentionnées sont chiffrées par n_i en

3. Insistons sur le fait que l'empreinte $E(clePub_{n_i})$ est considérée comme une information permettant de faire la distinction entre le nœud n_i et les autres nœuds comme nous le verrons dans la partie anonymat.

utilisant la clé publique de n_j ($clePub_{n_j}$) afin d'assurer leur confidentialité et empêcher, à partir d'une écoute passive, de faire de façon simple le lien entre un message et son émetteur et/ou son destinataire. Avant d'être chiffrées, certaines informations sont signées avec la clé privée de n_i afin de garantir leur provenance. Il s'agit de l'identité de n_i, du numéro de séquence, de la clé publique de n_j et du message m. A la réception du paquet transmis par n_i, n_j déchiffre le contenu du paquet à l'aide de sa clé privée $clePri_{n_j}$. n_j procède alors aux différentes vérifications d'intégrité avec les différentes empreintes reçues. Il vérifie que les données concernant l'émetteur sont valides en comparant le résultat d'une fonction de hachage appliquée aux informations relatives à n_i (clé publique et profil) et l'empreinte reçue. n_j peut alors savoir quelle clé publique est à utiliser pour vérifier la signature de la partie signée du paquet. Lorsque la signature est vérifiée, le nœud n_j contrôle également la validité du numéro de séquence pour s'assurer qu'un message comportant le même numéro n'a pas déjà été traité et il s'assure également d'être véritablement le destinataire du message à travers l'empreinte de sa clé publique.

Paquet $n_i \rightarrow n_j$

$$\{\{Id_{n_i}, NumSeq, E(clePub_{n_j}), m\}Sign_{clePri_{n_i}} + E(clePub_{n_i}) + profil_{ni} + E(E(clePub_{n_i}) + profil_{n_i})\}Chif_{clePub_{n_j}}$$

Figure 3.46 – Paquet transmis en mode sécurisé entre n_i et n_j pour un premier échange.

(ii) n_i et n_j ont déjà échangé des messages sensibles par le passé. Chaque nœud possède donc les informations de profil de l'autre (notamment sa clé publique). Dans cette situation, le contenu du paquet transmis par n_i est légèrement différent du paquet transmis dans le premier cas (premier message sensible échangé entre n_i et n_j). Le paquet ne contient plus les informations de profil du nœud n_i. La figure 3.47 montre la structure de ce type de paquet. A la réception, après déchiffrement, le nœud n_j peut contrôler l'intégrité de l'empreinte de la clé publique de n_i (en utilisant $E(E(clePub_{n_i}))$). Après ce contrôle d'intégrité, les vérifications de la signature, du numéro de séquence et de la destination du message sont effectuées, comme dans le premier cas.

Paquet $n_i \rightarrow n_j$

$$\{\{Id_{n_i}, NumSeq, E(clePub_{n_j}), m\}Sign_{clePri_{n_i}} + E(clePub_{n_i}) + E(E(clePub_{n_i}))\}Chif_{clePub_{n_j}}$$

Figure 3.47 – Paquet transmis en mode sécurisé entre n_i et n_j lors d'échanges répétés.

Le choix est laissé à la discrétion du nœud émetteur, en fonction des informations à transmettre et en fonction du contexte, d'utiliser ou non le mode sécurisé lors d'un échange.

Lorsque le mode sécurisé n'est pas utilisé, il est impossible pour le destinataire d'un message de vérifier son origine dans la mesure où l'émetteur n'a pas signé les informations transmises. Dans ce cas, l'empreinte de la clé publique du destinataire ne doit également pas apparaître dans le paquet transmis afin d'éviter que le lien puisse être établi, par une entité extérieure à l'échange, entre le contenu du message et sa cible (sans le consentement du destinataire). En revanche, suivant le contexte et en fonction des préférences de n_i, l'identité sous laquelle l'émetteur souhaite être connu, à savoir Id_{n_i}, peut être incluse dans le paquet. Dans ce cadre, le contenu du paquet transmis en mode non sécurisé, tel que représenté figure 3.48, comprend donc le message m, éventuellement Id_{n_i}, l'empreinte de la clé publique de n_i ($E(clePub_{n_i})$) et l'empreinte de l'ensemble des informations ($E(M = ensembledumessage)$) qui permet de vérifier l'intégrité des données transmises. Dans le cas où cet envoi représente le premier échange entre n_i et n_j (n_j n'a donc pas connaissance du profil de n_i), n_i inclut $profil_{n_i}$ dans le paquet à transmettre.
Il est à noter que les paquets transmis en mode non sécurisé ne doivent pas être considérés comme contenant des informations dont la validité est certaine dans la mesure où il est impossible d'avoir des garanties quant à leur émetteur. De plus, si un paquet transmis en mode non sécurisé appelle une réponse de la part du destinataire, cette réponse doit être envoyée en mode sécurisé afin d'éviter des tentatives d'usurpation d'identité liées aux clés publiques. En effet, un nœud pourrait inclure dans un paquet expédié en mode non sécurisé une empreinte de clé publique différente de la sienne en attendant que le destinataire lui réponde en pensant communiquer avec un autre nœud. Le fait, pour le destinataire, de répondre en mode sécurisé permet d'empêcher l'initiateur de l'échange, si sa clé publique ne correspond pas à celle dont l'empreinte figure dans le premier paquet émis (en mode non sécurisé), d'avoir accès au contenu du message.

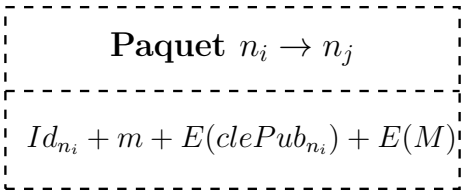


FIGURE 3.48 – Paquet transmis en mode non sécurisé entre n_i et n_j.

3.1.5.2 Contrôle de l'anonymat

En raison des caractéristiques des MANets, il est difficile de garantir certaines propriétés, notamment celles liées à l'authentification des nœuds. En effet, au sein des MANets, les nœuds entrent en contact les uns avec les autres sans infrastructure préexistante et la topologie du réseau est modifiée en permanence. Dans ce contexte, les procédures d'authentification qui nécessitent l'intervention d'entités extérieures sont compliquées à mettre en œuvre [1]. Il est cependant possible d'envisager d'autres types d'opérations. Supposons par exemple que deux nœuds échangent leurs identités avant de communiquer. Comme nous l'avons déjà noté, il est difficile d'avoir une garantie sur la validité (pas d'authentification) des identités échangées. Par contre, il serait réaliste de proposer un système qui permettrait aux deux nœuds, s'ils se rencontrent à plusieurs reprises, de se reconnaître mutuellement. En réalité, il s'agit d'imiter le comportement des personnes dans la vie réelle. Les gens

peuvent parler à d'autres personnes qu'ils rencontrent dans une foule, sans être sûrs de leur identité, et reconnaître ces personnes, plus tard, lorsqu'ils les rencontrent à nouveau. Afin de proposer un système réaliste et adapté aux MANets concernant l'anonymat, le fait de calquer le comportement des nœuds sur celui des personnes de la vie réelle nous conduit à considérer l'aspect que nous venons d'évoquer de reconnaissance mutuelle entre entités. Il est donc nécessaire qu'un nœud n_i impliqué dans des échanges avec d'autres nœuds puisse choisir la manière dont son identité est présentée aux destinataires de ses messages. En d'autres termes, il s'agit pour un nœud n_i de lui permettre de choisir l'identité (Id_{ni}) à travers laquelle il souhaite être connu par ses correspondants, de changer cette identité lorsqu'il le désire et d'être reconnu (si cela est pertinent) même en cas de changement de Id_{ni}. L'identité dont il est question à ce niveau est le nom par lequel le nœud souhaite être désigné. Plusieurs éléments doivent être considérés dans ce contexte :

- lors de l'envoi d'un paquet, le nœud émetteur n_i choisit l'identité Id_{ni} qu'il souhaite inclure dans les informations transmises. Cette possibilité permet à n_i de se présenter sous différents noms en fonction du contexte. n_i peut également décider de ne mentionner aucune identité dans les paquets transmis afin de conserver un anonymat complet vis à vis de ses correspondants.
- le contenu d'un paquet émis comprend toujours l'empreinte de la clé publique ($E(cle Pub_{n_i})$) de l'émetteur et ce, même dans le cas où aucune identité n'est incluse. En effet, il est nécessaire de pouvoir faire la distinction entre les nœuds pendant les échanges sans se baser sur l'identité qui est, comme nous l'avons vu, un élément changeant. La clé publique est une information qui ne révèle rien de l'identité d'un nœud. Le fait d'inclure son empreinte permet au récepteur du paquet de faire simplement et rapidement le lien entre le nœud émetteur et sa clé publique. Ainsi, il est toujours possible pour un nœud récepteur d'un paquet de reconnaître son émetteur sans pour autant que sa véritable identité ne soit révélée (sans son consentement).

La figure 3.49 présente un exemple où un nœud n_i change son identité entre deux envois de paquets au même nœud n_j. Le nœud n_i envoie d'abord le paquet P_1 contenant le message m_1 et dans lequel il se présente sous l'identité A. Le nœud n_i envoie ensuite le paquet P_2 contenant le message m_2 et dans lequel il se présente sous l'identité B. Entre l'émission de P_1 et de P_2, n_i change l'identité Id_{n_i} sous laquelle il souhaite être connu. Toutefois, le nœud récepteur n_j associe les deux messages m_1 et m_2 au même émetteur (sans pour autant connaître son identité réelle) parce que les deux paquets reçus comprennent l'empreinte de la clé publique de n_i. Le nœud n_i contrôle alors son anonymat tout en étant reconnu par ses correspondants et notamment n_j dans l'exemple présenté.

3.2 Architecture du système

L'architecture du système déployé sur chaque nœud n_i se compose de différents modules liés aux opérations supportées. La figure 3.50 page 113 présente les relations qui existent entre les modules au cours de la réalisation des tâches qu'un nœud met en œuvre. Ces modules ont les caractéristiques suivantes :

- **Profil.** Le module *Profil* contient deux parties, à savoir la partie *Préférences* et la partie *Données personnelles*. Le rôle de ce module est de recueillir et sauvegarder

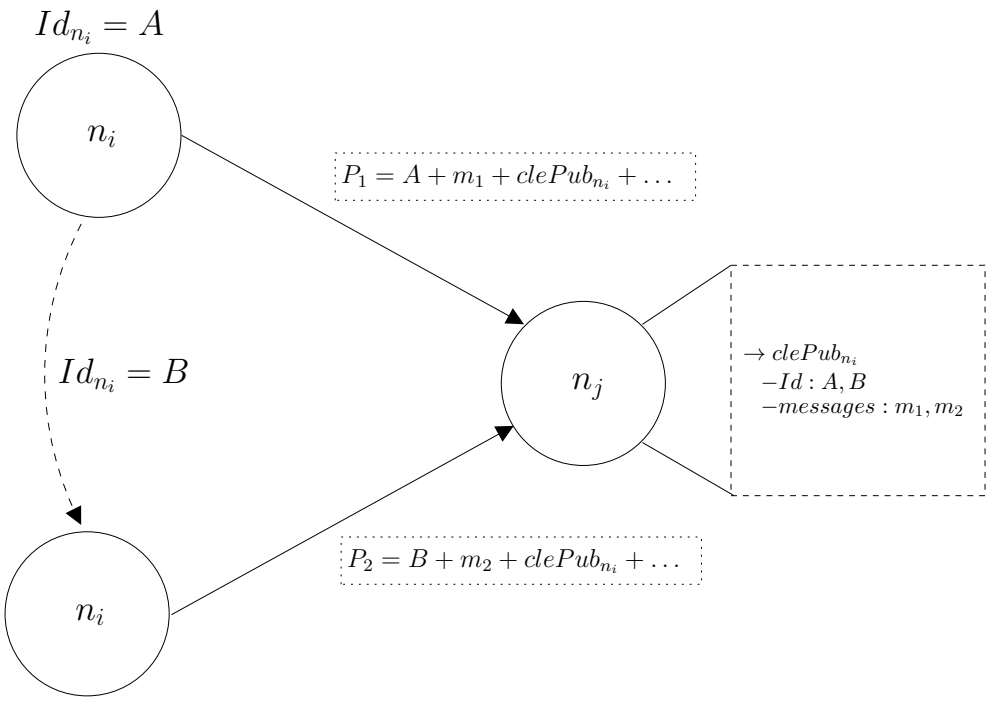


FIGURE 3.49 – Changement d'identité d'un nœud et émission de paquets.

les informations concernant le nœud qui l'embarque afin de les transmettre aux modules dont le fonctionnement en requiert la connaissance. Les informations du nœud transmises par le module *Profil* concernent notamment les préférences en matière de mode de communication, les clés de déchiffrement et de signature, les données à inclure dans le profil à publier et les données personnelles à échanger lors de rencontres physiques.

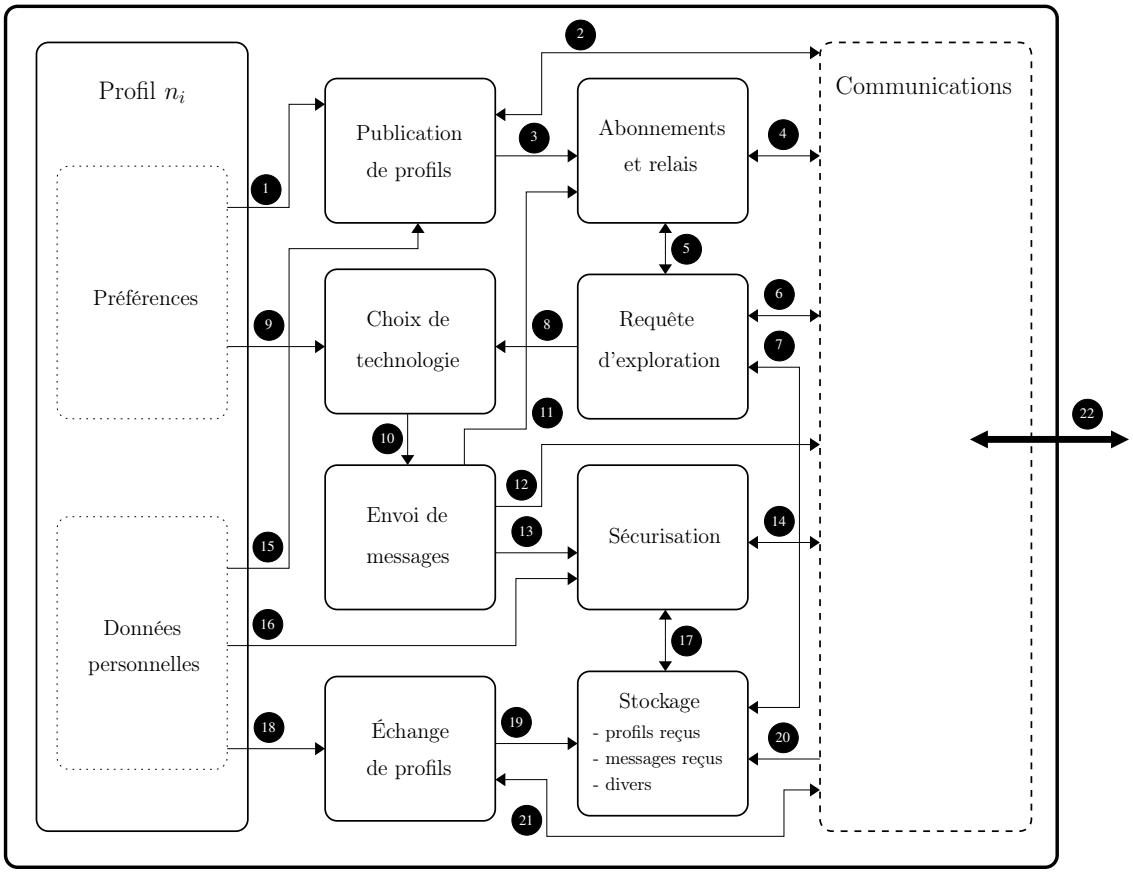
- **Publication de profils.** Le module *Publication de profils* est chargé d'appliquer l'algorithme de publication de profils afin que le profil du nœud considéré soit publié le plus largement possible dans ses différents voisinages. Tout d'abord, ce module reçoit les informations de profil en provenance du module *Profil*. Ensuite, le module *Communications* effectue une requête de voisinage (pour connaître l'ensemble des voisins). Enfin, après que les calculs nécessaires pour définir la manière dont les opérations doivent être menées (cf. section 3.1.1.2 page 83) aient été effectués, le profil est transmis au module *Abonnements et relais* et au module *Communications* afin d'être publié respectivement auprès des abonnements souscrits et des voisins.
- **Abonnements et relais.** Le module *Abonnements et relais* utilise le module *Communications* pour mettre en œuvre les échanges de messages à effectuer via les abonnements et les relais (lors de la publication de profils) ainsi que la mise à disposition de profils de nœuds situés sur des sites distants. A ce titre, le module *Abonnements et relais* reçoit des données de profil à publier de la part du module *Publication de profils* et des messages de la part du module *Envoi de messages*.
- **Requête d'exploration.** Le module *Requête d'exploration* a pour fonction de déterminer l'ensemble de profils correspondant à une requête d'exploration parmi ceux

qui sont accessibles au nœud considéré. A partir de la requête d'exploration initiée, le module *Requête d'exploration* effectue les comparaisons de profils nécessaires afin de déterminer l'ensemble des nœuds compatibles avec le besoin exprimé. Ces comparaisons concernent les profils de nœuds stockés par le module *Stockage*, les profils stockés par les voisins et les profils liés aux abonnements (accessibles via le module *Abonnements et relais*). Les comparaisons entre le besoin exprimé et les caractéristiques inscrites dans les profils disponibles se font par le biais d'une méthode utilisant le concept de *text similarity* (qui permet d'évaluer la similarité de textes). Le résultat produit par le module *Requête d'exploration*, à savoir un ensemble de cibles potentielles, est alors transmis au module *Choix de technologie*.

- **Choix de technologie.** Le module *Choix de technologie* est chargé, en partant d'un ensemble de cibles potentielles (module *Requête d'exploration*) et des préférences en matière d'émission de message (partie *Préférences* du module *Profil*), de déterminer la technologie la plus adaptée pour expédier un message suivant la procédure mise en place pour la plate-forme multi-niveaux. Lorsque la technologie à utiliser pour envoyer le message est déterminée, le module *Envoi de messages* est alors notifié afin de réaliser effectivement l'envoi du message.
- **Envoi de messages.** Le module *Envoi de messages* permet de transmettre les messages à envoyer à travers le module *Communications*. En pratique, le module *Envoi de messages* reçoit une notification du module *Choix de technologie* concernant la technologie de communication à utiliser et le message est alors transmis au module correspondant en fonction du mode d'émission privilégié. Il existe deux modes d'émission, à savoir le mode via abonnement/relais et le mode direct. Dans le cas du mode via abonnement/relais, le message est transféré au module *Abonnements et relais* pour être expédié. Dans le cas du mode direct, le message est immédiatement pris en charge par le module *Communications*. Il est à noter que dans les deux cas, le message peut être expédié à travers un paquet sécurisé (suivant les besoins) et donc transiter au préalable par le module *Sécurisation*.
- **Sécurisation.** Le module *Sécurisation* met en œuvre l'envoi de messages en mode sécurisé. A la réception d'un message à sécuriser, le module *Sécurisation* utilise la clé publique du destinataire pour chiffrer le paquet et la clé privée de l'émetteur pour signer le paquet. La clé publique du destinataire est fournie par le module *Stockage* tandis que la clé privée de l'émetteur provient de la partie *Données personnelles* du module *Profil*. Le module *Sécurisation* prend également en charge le déchiffrement et le contrôle de signature des paquets sécurisés reçus à travers le module *Communications*. Pour ce faire, le module se sert de la clé privée du nœud courant (partie *Données personnelles* du module *Profil*) et de la clé publique de l'émetteur (module *Stockage*). Après déchiffrement et contrôle de signature, les messages contenus dans les paquets reçus sont transférés au module *Stockage* afin d'être sauvegardés.
- **Échange de profils.** Le module *Échange de profils* est chargé de l'application de la procédure d'échange de profils lors d'une rencontre physique entre deux nœuds. Par conséquent, il permet à la fois d'initier un échange de profil et de recevoir une requête d'échange de profils. Le module récupère les données personnelles de profil du nœud local (partie *Données personnelles* du module *Profil*) et lorsque l'échange est validé, il transmet et reçoit les informations requises à travers le module *Communications*. Les informations de profil reçues sont ensuite transférées au module *Stockage* pour

être sauvegardées.

- **Stockage.** Le module *Stockage* sert à sauvegarder toutes les informations utiles reçues par le nœud à travers le module *Communications*. Il s'agit notamment des profils des voisins et des messages en provenance des différents nœuds connus. Ces informations sont ensuite rendues disponibles aux modules dont le fonctionnement en nécessite la connaissance.
- **Communications.** Le module *Communications* prend en charge toutes les communications que le nœud considéré effectue avec son environnement. En d'autres termes, il permet aux modules qui ont besoin d'interagir avec l'extérieur d'utiliser les technologies de communication disponibles. Le module *Communications* prend donc en compte toutes les spécificités des technologies de communication dont le nœud considéré est équipé afin de pouvoir les utiliser en fonction du contexte et des besoins. Dans la pratique, le module *Communications* réalise de manière autonome les contacts nécessaires aux échanges via les abonnements et les relais, les requêtes de voisinage, la publication de profil, l'émission des requêtes d'exploration, l'envoi/-réception de messages (en mode sécurisé ou non) et de profils du voisinage ainsi que l'envoi/réception de données personnelles dans le cas de l'échange de profils.



Flèche	Description	Flèche	Description
1	- Prise en compte des préférences du nœud n_i	12	- Transfert des messages à expédier en mode non sécurisé
2	- Requête de voisinage - Publication du profil de n_i dans le voisinage	13	- Transfert des messages à sécuriser
3	- Demande de publication du profil de n_i via les abonnements	14	- Transfert des messages à émettre et des messages reçus en mode sécurisé
4	- Envoi de messages et publication du profil de n_i via les abonnements et/ou les relais	15	- Transmission des données à publier
5	- Recherche de profils via les abonnements	16	- Données pour déchiffrement et signature
6	- Recherche de profils dans le voisinage	17	- Données pour chiffrement et contrôle de signature
7	- Exploration des profils reçus	18	- Données personnelles à transmettre
8	- Résultats de l'exploration de profils	19	- Transfert des données personnelles de profils reçus
9	- Prise en compte des préférences du nœud n_i	20	- Transfert des profils reçus
10	- Résultats du choix de technologie	21	- Échange des données personnelles de profil
11	- Transfert des messages à expédier via les abonnements et/ou les relais	22	- Intéractions avec l'environnement extérieur (envois/réceptions de messages, profils, etc.)

Figure 3.50 – Liens entre les différents modules de l'architecture.

3.3 Validation du système

Après avoir donné le détail de l'approche que nous proposons pour la plate-forme multi-niveaux ainsi que son architecture, il s'agit d'en évaluer la validité. En effet, il est nécessaire de vérifier que les actions clés prévues dans les processus présentés permettent d'atteindre les objectifs visés. Cette vérification permettra de procéder par la suite à une implémentation effective du système.
Nous sommes cependant confrontés à un problème clé. Notre plate-forme fonctionne au sein de MANets dans lesquels l'approche opportuniste est privilégiée. Par conséquent, il est difficile de donner certaines garanties quand à l'acheminement d'un message qui doit transiter entre plusieurs nœuds avant d'être délivré. Par exemple, nous ne pouvons pas garantir que tous les nœuds (sur un site donné) pourront recevoir tous les profils publiés. En revanche, nous pouvons certifier, en fonction du contexte, qu'un profil est toujours publié le plus possible dans le voisinage du nœud considéré. En d'autres termes, il s'agit de montrer que lors d'une publication de profil, les informations transmises le sont de façon optimale dans le voisinage considéré. Il nous apparaît également utile de vérifier la validité du cœur des opérations réalisées dans le cadre de la spécification d'un ensemble de cibles : il est indispensable de montrer qu'une méthode de comparaison entre les besoins qu'un nœud exprime à travers une requête d'exploration et les caractéristiques des profils disponibles peut être mise en œuvre. Enfin, il est nécessaire de s'assurer que la sécurisation des communications et le contrôle de l'anonymat sont assurés dans les opérations d'échanges de messages et d'échanges des données privées des profils entre deux nœuds qui se rencontrent physiquement.
Les trois éléments suivants ont donc été retenus comme étant primordiaux pour garantir la validité du système :

- la publication des profils ;
- la spécification des cibles ;
- la sécurité des communications et le contrôle de l'anonymat.

Nous les étudions dans la suite.

3.3.1 Publication des profils

Rappelons que pour procéder à la publication de son profil, un nœud donné n_i effectue, pour connaître son voisinage, une requête via les technologies dont il équipé et qui permettent un mode de communication direct. Deux possibilités sont alors offertes, en plus du cas par défaut (cf. section 3.1.1.2 page 83), au nœud initiateur de la publication de profil pour chaque voisin n_j identifié :

(i) cas de transmission directe à un nœud isolé. n_j est un nœud isolé (c'est à dire qu'il n'a pas d'autre voisin que n_i) ou alors il est voisin d'un ou plusieurs nœuds (eux-mêmes voisins de n_i) par des technologies dont les portées ne sont pas suffisamment supérieures à la portée de la technologie avec laquelle il est voisin de n_i (cf. section 3.1.1.2 page 83). Dans ce cas, le nœud n_i envoie directement son profil au voisin identifié.

(ii) cas de transmission par rebond. n_j est voisin d'un autre nœud n_k (lui-même voisin de n_i) par une technologie dont la portée est supérieure par un facteur donné (comme nous allons le justifier plus loin) à la portée de la technologie avec laquelle il est voisin

de n_i, comme indiqué section 3.1.1.2 page 83. Il est également supposé que la portée de la technologie avec laquelle n_k est voisin de n_i est supérieure à la portée de la technologie avec laquelle n_j est voisin de n_i. Dans ce cas, le nœud qui procède à la publication utilise le relais n_k pour transmettre son profil à n_j. L'intuition derrière cette procédure est que la probabilité d'atteindre la cible est plus élevée que dans le cas d'un envoi direct.

Il s'agit donc de déterminer la valeur du facteur qui va permettre de faire le choix entre les deux procédures ci-dessus. Pour cela, nous allons tout d'abord calculer la probabilité qu'un nœud sorte de la zone de couverture d'une technologie donnée. Nous allons ensuite évaluer la probabilité de réussite du transfert d'un message entre trois nœuds (transmission par un nœud relais). Enfin, nous allons comparer les résultats obtenus afin d'identifier les situations où l'utilisation d'un relais pour transmettre un message est plus pertinente qu'une transmission directe.

3.3.1.1 Calcul de probabilité de sortie d'un nœud d'une zone définie

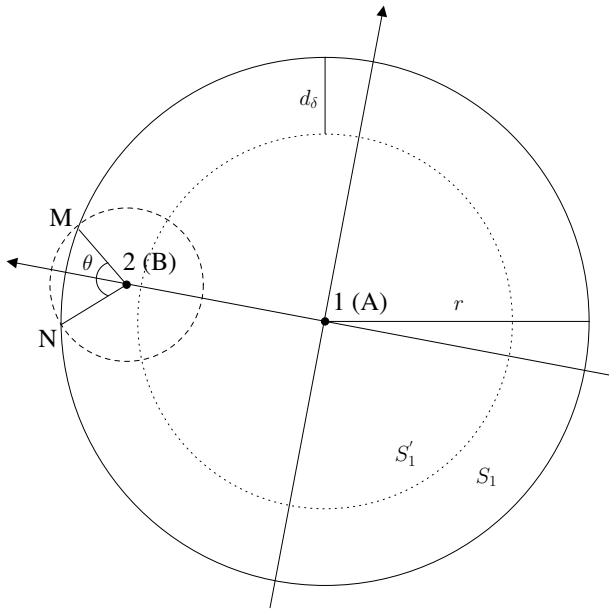


Figure 3.51 – Possibilités de sortie d'un nœud d'une zone de couverture.

Nous avons deux nœuds, à savoir 1 et 2, dans un espace donné comme le montre la figure 3.51. Nous supposons que le nœud 1 est équipé d'une technologie de communication sans fil t_1 dont la zone de portée est représentée par le cercle de rayon r (et dont l'aire est notée S_1). Nous faisons également l'hypothèse que le nœud 2 se déplace à une vitesse v qui lui permet de parcourir une distance d_δ par unité de temps (avec $d_\delta < r$). Le petit cercle (représenté par des tirets) est un cercle dont le centre est le point où se situe le nœud 2 et dont le rayon est d_δ. Ce cercle représente les possibilités de déplacement du nœud 2 en une unité de temps. Nous définissons, au sein de la zone de couverture de 1 par la technologie t_1, une zone à risque qui est constituée par l'espace compris entre le périmètre du cercle définissant la portée de t_1 et le périmètre du cercle en pointillé (dont l'aire est notée $S_1^{'}$).

La différence de rayon entre les deux cercles est égale à d_δ. Cette zone à risque est une zone à partir de laquelle le nœud 2 peut (potentiellement) en une unité de temps se retrouver hors de portée de la technologie t_1 du nœud 1 (en se déplaçant donc d'une distance d_δ).
Soient Q l'événement "le nœud 2 est à portée du nœud 1 et se situe dans la zone à risque de la technologie t_1 pour ce nœud" et R l'événement "le nœud 2 sort de la zone de couverture de 1 par t_1 quand il est dans la zone à risque". La probabilité que le nœud 2 sorte de la zone de couverture de la technologie t_1 (dont le nœud 1 est équipé) est égale à $p(Q \cap R)$. Il est donc nécessaire de calculer la probabilité $p(Q)$ de survenue de l'événement Q et la probabilité $p(R)$ de survenue de l'événement R. De façon évidente il est possible d'établir les égalités suivantes :

- $p(Q) = 1 - \frac{S_1^{'}}{S_1}$ avec $S_1 = \pi r^2$ et $S_1^{'} = \pi(r - d_\delta)^2$
  $\Rightarrow p(Q) = 1 - \frac{\pi(r-d_\delta)^2}{\pi r^2} = \frac{2rd_\delta - d_\delta^2}{r^2}$

Nous définissons ensuite un repère orthonormal (figure 3.51) centré en A (point où se situe le nœud 1) et dont l'axe des abscisses est représenté par la droite (AB), B étant le point où se situe le nœud 2. L'axe des abscisses est orienté dans le sens A vers B. Nous supposons que le point B se situe dans la zone à risque. Les coordonnées des points A et B sont : $A(0,0)$ et $B(x,0)$ avec $x \in [r - d_\delta, r]$. Pour déterminer $p(R)$, il est nécessaire de calculer la valeur moyenne (θ_m) de l'angle θ suivant toutes les valeurs possibles de l'abscisse du point B ($x \in [r - d_\delta, r]$), θ étant la portion angulaire qui représente les cas dans lesquels le nœud considéré peut sortir de la zone de couverture.
Nous pouvons tout d'abord déterminer les coordonnées des points M et N qui sont les points situés à l'intersection du cercle représentant la zone de couverture de la technologie t_1 et du cercle de rayon d_δ. Soient respectivement (x_m, y_m) et (x_n, y_n) les coordonnées des points M et N. Si nous prenons le cas du point M, à partir des informations disponibles, il est possible de faire les calculs suivants :

- $\left\{ \begin{array}{l} ||\overrightarrow{AM}|| = r \\ ||\overrightarrow{BM}|| = d_\delta \end{array} \right. \Rightarrow \left\{ \begin{array}{l} \sqrt{x_m^2 + y_m^2} = r \\ \sqrt{(x_m - x)^2 + y_m^2} = d_\delta \end{array} \right. \Rightarrow \left\{ \begin{array}{l} x_m^2 + y_m^2 = r^2 \\ (x_m - x)^2 + y_m^2 = d_\delta^2 \end{array} \right.$
  $\Rightarrow \left\{ \begin{array}{l} y_m^2 = r^2 - x_m^2 \\ y_m^2 = d_\delta^2 - (x_m - x)^2 \end{array} \right.$
- on obtient $d_\delta^2 - (x_m - x)^2 = r^2 - x_m^2$
  $\Rightarrow d_\delta^2 + 2x_m x - x^2 = r^2$
  $\Rightarrow x_m = \frac{x^2 + r^2 - d_\delta^2}{2x}$
- comme $y_m^2 = r^2 - x_m^2$
  on a $y_m = \frac{1}{2x}\sqrt{(2rx + r^2 + x^2 - d_\delta^2)(2rx - r^2 - x^2 + d_\delta^2)}$

De la même façon il est possible de déterminer les égalités suivantes pour le point N :

- $\left\{ \begin{array}{l} x_n = \frac{x^2 + r^2 - d_\delta^2}{2x} \\ y_n = -\frac{1}{2x}\sqrt{(2rx + r^2 + x^2 - d_\delta^2)(2rx - r^2 - x^2 + d_\delta^2)} \end{array} \right.$

On se sert de la relation existant entre le produit scalaire des vecteurs $||\overrightarrow{BM}||$ et $||\overrightarrow{BN}||$ et le cosinus de l'angle θ pour déterminer $\cos(\theta)$:

- on sait que $\langle\overrightarrow{BM}|\overrightarrow{BN}\rangle = ||\overrightarrow{BM}||.||\overrightarrow{BN}||.\cos(\theta)$
  nous avons $\overrightarrow{BM}(x_m - x, y_m)$ et $\overrightarrow{BN}(x_n - x, y_n)$
  nous pouvons donc établir l'égalité suivante $(x_m - x)(x_n - x) + y_m y_n = d_\delta^2 \cos(\theta)$
  $\Rightarrow (\frac{x^2+r^2-d_\delta^2}{2x} - x)(\frac{x^2+r^2-d_\delta^2}{2x} - x) - \frac{(2rx+r^2+x^2-d_\delta^2)(2rx-r^2-x^2+d_\delta^2)}{4x^2} = d_\delta^2 \cos(\theta)$
  $\Rightarrow \frac{(x^2+r^2-d_\delta^2-2x^2)(x^2+r^2-d_\delta^2-2x^2)}{4x^2} - \frac{(2rx+r^2+x^2-d_\delta^2)(2rx-r^2-x^2+d_\delta^2)}{4x^2} = d_\delta^2 \cos(\theta)$
  $\Rightarrow \frac{(x^4+r^4+d_\delta^4+2x^2d_\delta^2-2x^2r^2-2r^2d_\delta^2)-(2r^2x^2+2r^2d_\delta^2+2x^2d_\delta^2-x^4-r^4-d_\delta^4)}{4x^2} = d_\delta^2 \cos(\theta)$
  $\Rightarrow \frac{x^4-2r^2x^2+(r^2-d_\delta^2)^2}{2x^2} = d_\delta^2 \cos(\theta)$
  si on pose $X = x^2$, $a = 2r^2$, $b = (r^2 - d_\delta^2)^2$ et $c = 2d_\delta^2$
  nous avons donc $\cos(\theta) = \frac{X^2-aX+b}{cX}$
- $\theta = \arccos(\frac{X^2-aX+b}{cX})$ avec $X \in [(r - d_\delta)^2, r^2]$
  par conséquent la valeur moyenne de θ sur l'intervalle $[(r - d_\delta)^2, r^2]$ est $\theta_m = \frac{1}{2rd_\delta - d_\delta^2} \int_{(r-d_\delta)^2}^{r^2} \arccos(\frac{X^2 - aX + b}{cX}) \mathrm{d}X$

En utilisant la somme de *Riemann*, nous pouvons obtenir une valeur approchée de θ_m :

- $\theta_m = \frac{1}{n}\sum_{k=1}^{n} f((r - d_\delta)^2 + k\frac{2rd_\delta - d_\delta^2}{n})$ avec $f(x) = \arccos(\frac{x^2-ax+b}{cx}), x \in [(r - d_\delta)^2, r^2]$
  et n un entier naturel choisi (plus la valeur de n est élevée, plus le calcul est proche de la valeur exacte)

Ainsi nous pouvons déterminer, de la façon suivante, la probabilité $p(Q \cap R)$ que le nœud 2 sorte de la zone de couverture de la technologie t_1 : en raison de la nature indépendante des événements Q et R, $p(Q \cap R) = p(Q) \times p(R)$.
Or d'après les calculs précédents, nous pouvons dire que $p(R) = \frac{\theta_m}{2\pi}$ (i.e. probabilité de sortir lorsque l'on se retrouve dans la zone à risque).
Nous savons également que $p(Q) = \frac{2rd_\delta - d_\delta^2}{r^2}$.
On en conclut que $p(Q \cap R) = \frac{\theta_m(2rd_\delta - d_\delta^2)}{2\pi r^2}$

3.3.1.2 Calcul de probabilité de réussite du transfert d'un message entre trois nœuds

Considérons trois nœuds, 1, 2 et 3, dans un espace donné (figure 3.52). Nous faisons l'hypothèse que le nœud 1 est équipé des technologies de communication sans fil t_1 et t_2 dont les zones de portée sont représentées respectivement par le cercle $\mathscr{C}_1$ de rayon r_1 (dont l'aire est notée S_1) et le cercle $\mathscr{C}_2$ de rayon r_2 (et dont l'aire est notée S_2). Le nœud 3, quant à lui, est équipé d'une technologie de communication sans fil t_3 dont la zone de couverture est représentée par le cercle $\mathscr{C}_3$ de rayon r_3 (dont l'aire est notée S_3). Nous faisons également l'hypothèse que $r_1 < r_2 < r_3$ et que les nœuds 2 et 3 peuvent se déplacer à une vitesse v telle qu'ils parcourent au plus la distance d_δ en une unité de temps. Nous définissons, au sein de la zone de couverture de chaque technologie, une zone à risque qui est constituée par l'espace compris entre le périmètre du cercle définissant la portée de

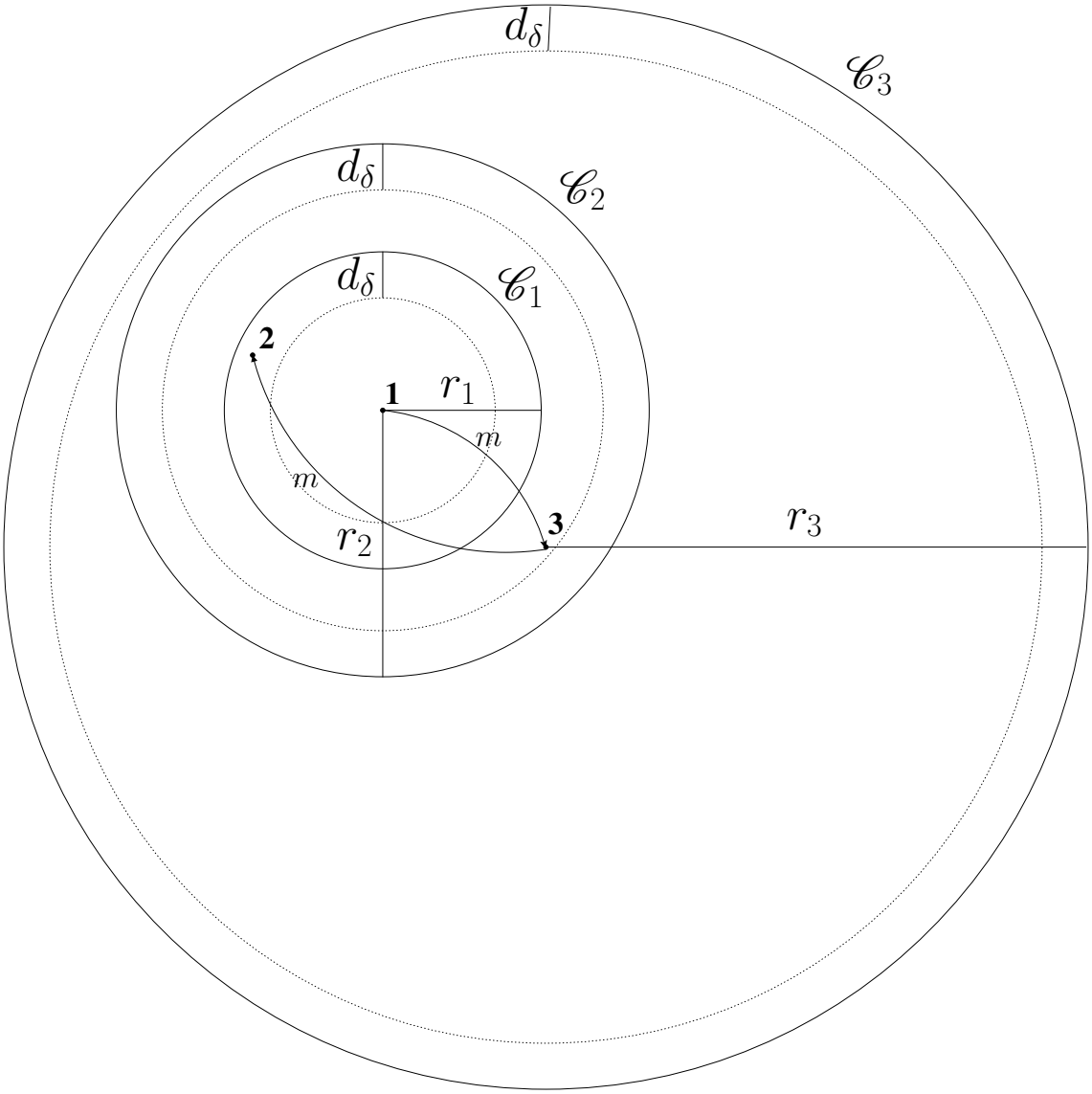


FIGURE 3.52 – Possibilités de transfert d'un message entre trois nœuds.

la technologie concernée et le périmètre du cercle en pointillés. Cette zone à risque est une zone à partir de laquelle un nœud, s'il se déplace pendant une unité de temps, peut éventuellement sortir de la zone de couverture de la technologie considérée (en fonction de la distance d_δ mentionnée ci-dessus). Les aires que représentent les cercles en pointillés sont respectivement $S_1^{'}$, $S_2^{'}$ et $S_3^{'}$ pour les cercles $\mathscr{C}_1$, $\mathscr{C}_2$ et $\mathscr{C}_3$.
A l'instant t, le nœud 2 est dans la zone $\mathscr{C}_1$ et le nœud 3 est dans la zone $\mathscr{C}_2$. L'opération à effectuer dans l'espace considéré est la suivante : le nœud 1 doit transmettre un message m (en une unité de temps) au nœud 2 en passant par le nœud 3. Il s'agit de déterminer la probabilité que les 3 nœuds considérés se trouvent dans une configuration dans laquelle le message m est effectivement transmis avec succès (en dépit des possibles déplacements des nœuds). Soient Q l'événement "le nœud 3 reste dans la zone $\mathscr{C}_2$ après une unité de

temps" et R l'événement "le nœud 2 reste dans la zone $\mathscr{C}_3$ après une unité de temps". La probabilité que nous cherchons à déterminer est la probabilité $p(Q \cap R)$. Il est donc nécessaire de calculer la probabilité $p(Q)$ de survenue de l'événement Q et la probabilité $p(R)$ de survenue de l'événement R. En prenant en compte les aires S_2, S_3, $S_2^{'}$ et $S_3^{'}$, il est possible d'établir les égalités suivantes :

- $p(Q) = \frac{S_2^{'}}{S_2}$ avec $S_2 = \pi r_2^2$ et $S_2^{'} = \pi(r_2 - d_\delta)^2$
  $\Rightarrow p(Q) = \frac{\pi(r_2 - d_\delta)^2}{\pi r_2^2} = \frac{r_2^2 - 2r_2 d_\delta + d_\delta^2}{r_2^2}$
- $p(R) = \frac{S_3^{'}}{S_3}$ avec $S_3 = \pi r_3^2$ et $S_3^{'} = \pi(r_3 - d_\delta)^2$
  $\Rightarrow p(R) = \frac{\pi(r_3 - d_\delta)^2}{\pi r_3^2} = \frac{r_3^2 - 2r_3 d_\delta + d_\delta^2}{r_3^2}$

- les événements Q et R sont indépendants
  d'où $p(Q \cap R) = p(Q) \times p(R) = (\frac{r_2^2 - 2r_2 d_\delta + d_\delta^2}{r_2^2}).(\frac{r_3^2 - 2r_3 d_\delta + d_\delta^2}{r_3^2})$

3.3.1.3 Comparaison des deux possibilités pour transmettre un message à un nœud

Dans le cas où un nœud n_i souhaite transmettre un message à un nœud n_j dans un espace donné, deux possibilités sont offertes à n_i. Le nœud émetteur (n_i) peut soit envoyer directement le message à la cible (via une technologie de communication t_1) ou soit utiliser un nœud relais n_k qui est équipé d'une technologie de communication de plus grande portée t_3 pour retransmettre le message au nœud n_j. Lors de l'utilisation du relais, le nœud n_i transmet le message au nœud n_k via une technologie de communication t_2. Notons que le nœud n_i est équipé des technologies t_1 et t_2, le nœud n_j est équipé des technologies t_1 et t_3, tandis que le nœud n_k est équipé des technologies t_2 et t_3.
En considérant les deux calculs de probabilité que nous avons effectués, il est possible de déterminer quelle est la méthode la plus appropriée pour transmettre le message en fonction du contexte. En effet, si la probabilité de sortie du nœud n_j de la zone de portée de la technologie t_1 est plus grande que la probabilité pour le nœud n_k de se retrouver dans une zone qui lui permet de retransmettre le message alors la méthode du nœud relais doit être privilégiée. Inversement, si la probabilité de sortie du nœud n_j de la zone de portée de la technologie t_1 est inférieure à la probabilité pour le nœud n_k de se retrouver dans une zone qui lui permet de retransmettre le message alors le message doit être transmis directement au nœud n_j.
Ainsi lorsque le nœud n_i doit déterminer le meilleur moyen pour transmettre le message au nœud n_j, après avoir vérifié la condition sur les portées de t_1, t_2 et t_3, il procède aux calculs des deux valeurs de probabilité des sections précédentes (en utilisant les informations disponibles sur les portées des différentes technologies). En fonction des résultats obtenus, le choix du moyen de transmission peut alors être effectué.
Afin de donner un aperçu de l'évolution des probabilités, dans les deux modes de transmission, nous les représentons pour un cas donné sur un graphique [4] (figure 3.53). Nous

4. Toutes les valeurs de distance s'expriment en mètres.

supposons que r_1 est fixé et nous lui donnons la valeur 15. La portée r_2 est définie comme étant un multiple de r_1 en fonction d'un paramètre α qui varie entre 1 et 5. De même, la portée r_3 est définie comme étant un multiple de r_2 en fonction d'un paramètre β qui varie entre 1 et 5. Nous supposons également que la valeur de d_δ, qui est la distance que peut parcourir un nœud en une unité de temps, est fixée à 1,4 en prenant la seconde comme unité de temps. Cette valeur correspond à la vitesse moyenne (1,4m/s) à laquelle les êtres humains marchent en l'absence de contraintes extérieures [64]. En utilisant les formules de calcul de probabilité que nous avons déterminées pour les deux modes de transmission, nous obtenons le graphique de la figure 3.53. Il représente la différence de probabilité (de réussite de la transmission du message) entre le mode relais et le mode direct. On remarque que l'utilisation du mode relais devient pertinente lorsque α est supérieur ou égal à 1,5 et β supérieur ou égal à 2, c'est à dire que la portée de t_3 est trois fois supérieure à celle de t_1 (cf. graphique). Nous pouvons donc dire que 3 est la valeur du facteur (présenté page 114 en introduction de la section) qui permet de faire le choix entre les deux possibilités d'envoi d'un message (envoi direct ou via le mode relais).

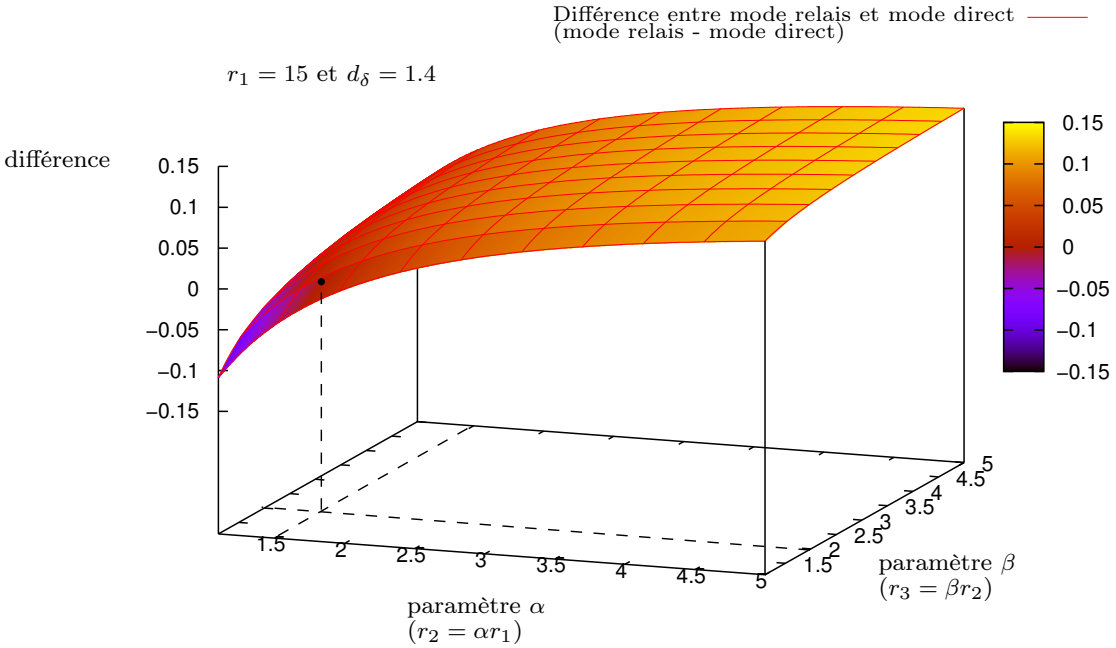


FIGURE 3.53 – Différence de probabilité de réussite suivant les deux méthodes

3.3.2 Spécification des cibles

La spécification de cibles consiste à déterminer un ensemble de nœuds qui pourraient répondre, selon le contenu de leurs profils respectifs, aux besoins exprimés par un nœud donné via une requête d'exploration. Un des points principaux de ce processus est donc la comparaison des paramètres de la requête avec le contenu des profils accessibles au nœud

initiateur de l'opération. Nous détaillons la méthode que nous proposons.

3.3.2.1 Contexte

Il s'agit de déterminer, lors de l'opération de spécification de cibles, comment comparer des éléments de profils afin d'obtenir un résultat correspondant au contenu de la requête. Il s'agit également de montrer la validité de cette comparaison dans notre contexte. Rappelons le processus mis en œuvre. Pour procéder à une spécification de cibles, le nœud initiateur émet une requête d'exploration dont l'argument principal représente les caractéristiques que doivent avoir les entités susceptibles de répondre à ses besoins. Les paramètres de cette requête peuvent concerner des caractéristiques classiques des nœuds comme un type particulier de technologie dont ils pourraient être être équipés. Ils peuvent également concerner des caractéristiques spécifiques comme des compétences (c'est à dire des capacités particulières) dans un domaine précis. Par conséquent, pour prendre en compte les requêtes basées sur des caractéristiques spécifiques, chaque nœud du système doit spécifier dans son profil les compétences qu'il souhaite mettre à la disposition des autres nœuds.
Pour le cas des caractéristiques classiques, la correspondance entre le contenu de la requête et un profil compatible est relativement simple à effectuer en raison du fait que le champs des possibilités est limité et connu. En effet, si nous reprenons l'exemple où un nœud recherche des entités équipées d'un certain type de technologie, l'ensemble dans lequel l'initiateur de la requête peut choisir l'élément dont il a besoin est fixé. La mise en œuvre de ce type de comparaison est donc triviale. Nous nous intéressons donc plus particulièrement aux requêtes d'exploration liées aux compétences spécifiques des nœuds. Dans ce cas, il n'y a pas de limite stricte dans les compétences à rechercher et dans les compétences proposées par les nœuds. Afin de montrer que la recherche de profils compatibles suivant ces critères est réaliste, nous allons tout d'abord détailler la manière dont les compétences doivent être spécifiées dans un profil et dans la requête d'exploration. Nous allons ensuite présenter la manière dont la comparaison entre l'argument principal de la requête d'exploration et les compétences spécifiées dans les profils disponibles doit être effectuée.

3.3.2.2 Spécification des compétences

La spécification des compétences concerne les requêtes d'exploration et les profils. La liberté doit être laissée aux nœuds d'utiliser les termes qu'ils souhaitent pour représenter les compétences. Toutefois, il est nécessaire de préciser la manière dont ces descriptions sont faites afin que les comparaisons entre compétences puissent être réalisées. Nous supposons que les différentes compétences sont décrites sous forme textuelle. Nous proposons donc que chaque compétence à spécifier soit détaillée à travers en ensemble de mots-clés dont le nombre doit être limité. Nous fixons à 5, de façon arbitraire, la limite pour le nombre de mots-clés à utiliser dans le détail d'une compétence. Ainsi une compétence $Comp_i$ est définie de la façon suivante : $Comp_i = \{mc_1, mc_2, \ldots, mc_k\}$ avec k un entier tel que $1 \leq k \leq 5$ et mc_k un mot-clé Le mot-clé est généralement défini comme étant un terme permettant d'effectuer une requête dans un outil de recherche. Nous proposons de plus les définitions suivantes :

- arg est l'argument principal d'une requête d'exploration ; $arg = Comp_q$ avec $Comp_q$ la compétence recherchée ;

– $Comp_{n_i}$ est défini comme l'ensemble des compétences spécifiées dans le profil du nœud n_i. $Comp_{n_i} = \{Comp_1, Comp_2, \ldots, Comp_k\}$ avec k un entier tel que $1 \leq k \leq q$ et q un entier représentant le nombre de compétences que le nœud n_i met à la disposition des autres entités.

Chaque nœud a donc la possibilité d'utiliser les termes (mots-clés), en nombre limité, qui lui paraissent les plus représentatifs des caractéristiques (compétences) à représenter.

3.3.2.3 Comparaison entre la requête d'exploration et les compétences spécifiées

Il s'agit ici de comparer les compétences recherchées (arguments de requêtes d'exploration) et les compétences proposées dans les profils de nœuds disponibles. Pour effectuer cette comparaison nous utilisons le concept de *text similarity* [62][63]. Ce concept permet d'évaluer le niveau de similarité de deux portions de textes en se basant sur des techniques de **racinisation** et de **lemmatisation**. La racinisation consiste à déterminer la racine des mots, c'est à dire à dépouiller les mots de leurs éventuels suffixes et préfixes. La lemmatisation, quant à elle, consiste à déterminer la forme canonique des mots, c'est à dire ramener les mots à l'entité la plus simple de la famille de mots à laquelle ils appartiennent. Ces techniques permettent d'harmoniser le contenu d'ensembles de termes dans le but de faciliter les comparaisons. Ainsi, en fonction du niveau de similarité atteint (suivant des critères liés au contexte), il est alors possible de conclure que deux textes sont proches (ou non) au sens sémantique du terme. Dans notre cas, il s'agit d'utiliser le concept de *text similarity* pour comparer un ensemble de mots-clés définissant un besoin (requête d'exploration) avec des ensembles de mots-clés définissant des compétences (profils de nœuds). Cette comparaison à pour objectif de déterminer la ou les compétences qui pourraient satisfaire le besoin exprimé.

Supposons que nous ayons deux éléments $Comp_i$ et $Comp_j$ représentant respectivement un argument de requête d'exploration et une compétence inscrite dans le profil d'un nœud. Nous allons détailler les étapes qui permettent d'établir si les compétences que décrivent $Comp_i$ et $Comp_j$ sont proches au niveau sémantique :

– il est d'abord nécessaire de déterminer la forme canonique des mots-clés composant les deux compétences. Cette étape est réalisée au moyen d'un dictionnaire qui contient les racines et les formes canoniques des mots usuels. Il est à noter que le nœud qui procède à l'opération de comparaison doit être équipé du dictionnaire nécessaire à cette étape de lemmatisation. Lorsqu'un mot ne figure pas dans le dictionnaire, la forme canonique considérée du mot est le mot lui-même. Ainsi nous obtenons les compétences (canoniques) $Comp_i^{'}$ et $Comp_j^{'}$ respectivement dérivées de $Comp_i$ et $Comp_j$ et qui sont constituées de mots-clés sous forme canonique. Ce sont $Comp_i^{'}$ et $Comp_j^{'}$ que nous utiliserons dans la suite.
– il est ensuite nécessaire de diminuer, dans chaque compétence, le poids des termes fréquemment utilisés. En effet certains mots-clés peuvent apparaître régulièrement dans les descriptions en raison du fait qu'ils représentent des termes génériques. Prenons par exemple deux ensembles de mots $E_1 = \{programmation, langage, C++\}$ et $E_2 = \{programmation, langage, Java\}$ que nous voulons comparer. Ces deux ensembles définissent des compétences dans des langages de programmation. En comparant simplement E_1 et E_2, il serait possible d'aboutir à la conclusion qu'ils sont

proches en raison des éléments qu'ils partagent (*programmation* et *langage*). Pourtant, les deux ensembles considérés définissent des compétences différentes, l'une concernant le langage de programmation $C++$ et l'autre concernant le langage de programmation $Java$. Il serait donc pertinent de réduire, dans la comparaison, le poids des éléments tels que *programmation* et *langage* pour ne considérer que $C++$ et $Java$ comme éléments importants.

De façon générale, pour réaliser l'opération de réduction du poids des mots-clés communs, nous utilisons l'*inverse document frequency* ou *idf* [89]. L'*idf*, qui permet d'évaluer le caractère commun ou rare d'un terme, est obtenu en divisant le nombre total de documents par le nombre de documents où apparaît le terme considéré et en calculant le logarithme de ce quotient. Plus l'*idf* d'un terme est élevée, plus ce terme doit être considéré dans des opérations de comparaisons textuelles. Dans la suite, si $mc_{i,k}$ est le mot-clé numéro k de la compétence canonique $Comp_i^{'}$, l'*idf* du mot-clé considéré est notée $idf_{i,k}$. $idf_{i,k} = \log \frac{n}{n_{i,k}}$ avec n le nombre de compétences dans tous les profils dont le nœud qui initie la requête d'exploration a connaissance et $n_{i,k}$ le nombre de compétences (parmi les profils accessibles) dans lesquels le mot-clé $mc_{i,k}$ se retrouve.

Ainsi à chaque mot-clé de $Comp_i^{'}$ et $Comp_j^{'}$ est affecté une *idf* qui correspond au poids à prendre en compte dans la suite de la comparaison. Il est à noter que plus un nœud a connaissance d'un nombre élevé de profils, plus les calculs des différents *idf* des mots-clés seront affinés. L'*idf* d'un mot-clé évolue donc en fonction des profils accessibles au nœud qui en effectue le calcul.

– il est alors possible de ranger les différents mots-clés des compétences de $Comp_i^{'}$ et $Comp_j^{'}$, suivant les valeurs de leurs *idf* respectifs, afin de les comparer deux à deux. Les mots-clés à l'*idf* le plus élevé seront les plus importants dans les descriptions des compétences. Ces valeurs des *idf* permettent ainsi de définir les compétences canoniques ordonnées $Comp_i^{''}$ et $Comp_j^{''}$, dérivées respectivement de $Comp_i^{'}$ et $Comp_j^{'}$, et qui sont des représentations de compétences dans lesquelles les différents mots-clés sont rangés de façon décroissante suivant la valeur de leurs *idf*.

On a donc $Comp_i^{''} = \{mc_{i,1}, mc_{i,2}, \ldots, mc_{i,k}\}$ avec k le nombre de mots-clés ($1 \leq k \leq 5$) et $idf_{i,p} \geq idf_{i,p+1}$ ($mc_{i,p}$ et $mc_{i,p+1}$ sont deux mots-clés de $Comp_i^{''}$, p un entier tel que $p \leq k-1$)

et $Comp_j^{''} = \{mc_{j,1}, mc_{j,2}, \ldots, mc_{j,l}\}$ avec l le nombre de mots-clés ($1 \leq l \leq 5$) et $idf_{i,q} \geq idf_{i,q+1}$ ($mc_{i,q}$ et $mc_{i,q+1}$ sont deux mots-clés de $Comp_i^{''}$, q un entier tel que $q \leq l-1$)

Chaque élément de $Comp_i^{''}$ est comparé à chaque élément de $Comp_j^{''}$ et une somme $S_{i,j}$ est calculée suivant les résultats des différentes comparaisons. L'algorithme 1 (page 124) présente la manière dont la comparaison est effectuée. Lorsque deux mots-clés sont comparés, s'ils sont identiques alors le produit de leurs *idf* respectifs est ajouté à $S_{i,j}$. Dans le cas où deux mots-clés évalués sont différents et sont de même niveau (dans l'ordre d'importance selon l'*idf*) alors le produit de leurs *idf* est retranché à $S_{i,j}$. A l'issue de toutes les comparaisons deux à deux, suivant la valeur de la somme $S_{i,j}$ et en fonction d'un seuil fixé, une conclusion peut être tirée sur la similarité de $Comp_i$ et $Comp_j$.

– il est enfin nécessaire de déterminer le seuil, pour la valeur de $S_{i,j}$, qui permet de

déterminer si $Comp_i$ et $Comp_j$ sont similaires. De façon intuitive, lorsqu'une comparaison de compétences est effectuée pour la première fois, le seuil est fixé à 0. En d'autres termes, il est raisonnable de supposer que si la somme $S_{i,j}$ est supérieure à 0, les compétences peuvent être considérées comme étant relativement similaires. En effet, le fait que la somme $S_{i,j}$ soit supérieure à 0 signifie que l'équilibre entre les éléments communs et les éléments différents des compétences comparées est favorable aux éléments communs. Ce seuil peut, dans la suite, être modifié en fonction du nœud initiateur de la requête d'exploration qui a conduit aux comparaisons de compétences. Cette modification du seuil dépend des résultats constatés lors de la comparaison. Si le nœud considère qu'une compétence présentée comme étant compatible avec un besoin exprimé ne l'est pas, le seuil est alors ajusté pour être fixé à la valeur correspondant à la somme $S_{i,j}$ de la comparaison effectuée au lieu de 0. Ainsi, au fur et à mesure des différentes évaluations de similarité entre compétences, la valeur fixée pour le seuil est affinée. L'objectif du calcul de la somme $S_{i,j}$ est donc de représenter le nombre de mots-clés communs entre $Comp_i$ et $Comp_j$ en mettant l'accent sur les termes essentiels. Plus les deux compétences comparées ont des termes de même importance (selon le le niveau de l'*idf*) identiques plus la somme $S_{i,j}$ est grande.

Algorithme 1: Comparaison de $Comp_i^{''}$ et $Comp_j^{''}$

Entrées : $Comp_i^{''} = \{mc_{i,1}, mc_{i,2}, \ldots, mc_{i,k}\}$, $Comp_j^{''} = \{mc_{j,1}, mc_{j,2}, \ldots, mc_{j,l}\}$

```
1 S_{i,j} ← 0;
2 pour p ←1 a k faire
3 |   pour q ←1 a l faire
4 |   |   si mc_{i,p} = mc_{j,q} alors
5 |   |   |   S_{i,j} ← S_{i,j} + idf_{i,p} × idf_{j,q};
6 |   |   sinon
7 |   |   |   si p = q alors
8 |   |   |   |   S_{i,j} ← S_{i,j} - idf_{i,p} × idf_{j,q};
```

3.3.2.4 Validité de la méthode

La validité de ce processus de comparaison repose sur la méthode d'évaluation mise en place. En se basant sur des éléments clés du concept de *text similarity*, à savoir la lemmatisation et l'*idf*, un indicateur évaluant la correspondance entre les descriptions de deux compétences a pu être proposé. Il est admis que l'*idf* est un indicateur performant, dans le domaine de la recherche d'informations de type textuel, pour mettre en place des méthodes de comparaison comme le montrent Robertson et Papineni dans leurs travaux respectifs [89][76]. On notera par ailleurs que la méthode proposée est évolutive en raison du fait que le niveau requis pour interpréter l'indicateur de correspondance (le seuil pour la somme $S_{i,j}$) comme étant positif est adapté aux résultats obtenus par les nœuds considérés.

3.3.3 Sécurité des échanges et contrôle de l'anonymat

La sécurité des échanges au sein du système repose sur la paire de clés (publique et privée) dont chaque nœud est doté. Cette paire de clés permet de répondre aux attentes en matière de confidentialité, d'authentification et d'intégrité durant les échanges, comme nous l'avons vu dans la partie "sécurité des communications" de ce document lors de la présentation de la plate-forme multi-niveaux. Bien évidemment, ces procédures sont dépendantes du respect du caractère secret de la clé privée. Ce secret est assuré par le fait que les opérations cryptographiques sont effectuées par un module sécurisé (ou *Secure Element*) présent sur chaque nœud et qui stocke la paire de clés considérées.
En dehors de ces considérations, il est également utile de s'intéresser aux opérations d'initialisation d'échanges de profils (entre deux nœuds qui se rencontrent physiquement) et aux opérations mises en place pour préserver l'anonymat afin de déterminer quelles garanties elles offrent.

3.3.3.1 Échanges des profils

Dans l'opération d'échange de la partie privée de profil entre deux nœuds qui se rencontrent, nous avons précisé que l'initialisation de la procédure devait s'effectuer à l'aide d'une technologie sans fil de type NFC (Near Field Communication) comme indiqué section 3.1.4 page 104. Il est à noter qu'une description plus complète du fonctionnement de cette technologie est donnée en section 4.1.1. Comme notre approche fait usage de NFC en mode *peer-to-peer*, il est nécessaire de considérer le modèle de menace associé à cette technologie lors de communications utilisant ce mode de dialogue.
Le modèle de menace comprend des attaques telles que l'écoute passive, l'attaque par relais et l'attaque de type *man-in-the-middle* [44][58]. Le principe de l'attaque par relais consiste à faire croire à deux entités qu'elles communiquent directement l'une avec l'autre alors que les données échangées sont relayées (sans être altérées) par l'attaquant. Quant à l'attaque de type *man-in-the-middle*, elle a pour but, pour un attaquant, d'intercepter des informations échangées entre deux entités afin de les modifier à son avantage (avant éventuellement de les retransmettre). Ces menaces ne sont pas sensibles dans notre contexte. En effet, des attaques de type relais ou de type *man-in-the-middle* sont particulièrement difficiles à mettre en œuvre dans un environnement réel où des opérations sont réalisées via la technologie NFC [34]. Cela est dû aux caractéristiques (très courte portée) de cette technologie qui nécessite que les deux parties réalisant une transaction se situent physiquement très proches l'une de l'autre (ce qui permet "d'authentifier physiquement" les parties impliquées).
La principale menace réside donc dans l'écoute passive. En effet, une entité malveillante pourrait effectuer une écoute passive [99] et enregistrer les données transmises lors de l'initialisation de l'échange (en l'occurrence la clé publique et les informations de connexion) à travers le canal privé qui est uni-directionnel. Les conséquences de cette attaque sont néanmoins limitées, en raison du fait que très peu de données personnelles ou non destinées à être publiques sont transmises à travers ce canal privé. Toutefois, ce problème pourrait être résolu en utilisant le protocole SNEP (Simple NDEF Exchange Protocol) [33] (qui n'est pas encore implémenté sur la plupart des équipements compatibles NFC) pour établir des communications bi-directionnelles dans l'initialisation de la procédure d'échanges de profil via le canal privé. Ce mode bi-directionnel pourrait permettre de transmettre uniquement

la clé publique dans un sens de communication et l'entité de destination répondrait en envoyant ses informations de connexion chiffrées à l'aide de la clé publique reçue pour ainsi initier la procédure d'échange.
Au vu de l'analyse ci-dessus, il apparaît que même si le système peut être amélioré (notamment en utilisant le protocole SNEP), l'opération d'échange de la partie privée de profil entre deux nœuds atteint un seuil de sécurité raisonnable.

3.3.3.2 Préservation de l'anonymat

Les éléments présentés dans cette section argumentent sur des techniques validées dans le domaine de la sécurité. Ils ne sont donc pas essentiels pour le lecteur ayant une connaissance approfondie du domaine.
La préservation de l'anonymat, dans la plate-forme multi-niveaux, repose sur les deux éléments suivants :

- chaque nœud a la possibilité de se présenter suivant l'identité qu'il souhaite faire connaître aux autres entités ;
- tous les messages (paquets) transmis contiennent l'empreinte de la clé publique de l'émetteur.

Le principal problème dans l'utilisation de l'empreinte d'une donnée est le phénomène de collision [94]. De façon pratique, une collision survient lorsque deux données différentes se voient attribuer la même empreinte par la fonction de hachage considérée. En effet, la fonction de hachage est une fonction mathématique qui permet de convertir une donnée de longueur arbitraire en une information de taille fixe (souvent de taille beaucoup plus réduite que la donnée initiale) que l'on appelle empreinte [84].
Une collision, si elle intervient, attribuerait une même empreinte à deux clés publiques distinctes et pourrait donc entraîner une confusion dans la reconnaissance, par une entité, de l'émetteur d'un message (associé à l'une des clés publiques considérées).
Toutefois, la problématique de conflit d'empreinte pour deux clés publiques différentes est limitée :

- la taille des empreintes que produisent les fonctions de hachage considérées comme les plus sûres est au moins de 256 bits [50][93]. Cette valeur offre 2^{256} possibilités d'empreintes pour les clés publiques des différents nœuds. En prenant en compte le fait que les fonctions de hachage considérées génèrent les empreintes suivant une distribution aléatoire homogène et que le nombre de nœuds ne peut raisonnablement pas atteindre 2^{256}, le risque de collision est réduit.
- en cas de collision, c'est à dire si un nœud reçoit un paquet contenant une empreinte de clé publique pouvant correspondre à deux entités, une distinction peut être faite. En effet, nous supposons que l'équipement mobile lié à chaque nœud ne change pas au cours du temps (ce qui est raisonnable si l'équipement est un téléphone mobile personnel). Dans cette situation, lorsqu'un nœud reçoit un paquet, il lui est possible de récupérer les caractéristiques (uniques) de la technologie (liée à l'équipement mobile) à travers laquelle l'émetteur a transmis le message. Ainsi, en cas de conflit, le destinataire d'un paquet peut comparer les caractéristiques (l'adresse de connexion en l'occurence) de la technologie utilisée pour l'échange avec celles qui figurent dans les profils des nœuds aux empreintes identiques et faire la distinction entre les deux entités.

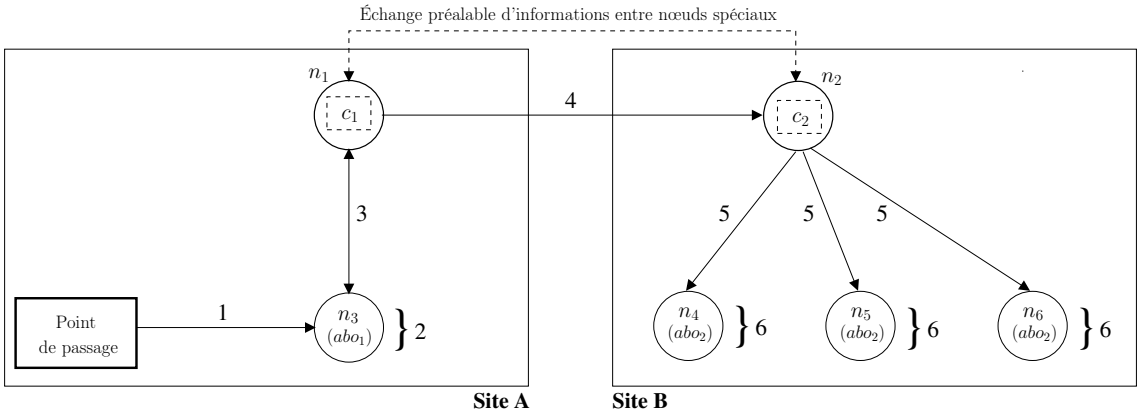
Pour ces raisons, il nous semble raisonnable d'affirmer que l'utilisation de l'empreinte des clés publiques permet au système de préservation de l'anonymat d'offrir les garanties recherchées.

3.4 Initialisation du système

Il est à noter que nous considérons ici que l'environnement dans lequel les nœuds évoluent est soumis à certaines règles qui facilitent l'initialisation des opérations au sein de la plate-forme multi-niveaux. Il est par exemple réaliste de faire l'hypothèse que dans le monde réel les nœuds sont conduits à passer par certains points de l'espace géographique dans lequel il se trouvent et que des relations ont ainsi pu être établies au préalable entre eux.
En reprenant l'exemple de l'application Museum Quest, les nœuds ont non seulement la possibilité de communiquer avec des entités qui se trouvent dans leur voisinage local mais aussi avec des entités qui se trouvent sur des sites distants. Concernant les communications effectuées en local, les nœuds utilisent simplement les capacités de découverte de voisinage des technologies dont ils sont équipés. Pour les communications distantes, l'utilisation de relais et/ou d'abonnements, dans le cas où les informations de contact direct avec les entités recherchées ne sont pas connues, est indispensable. Il est nécessaire de savoir comment les nœuds peuvent accéder aux renseignements concernant les abonnements disponibles afin de pouvoir échanger des messages avec des entités distantes pour recueillir, en particulier des informations de contact pour d'éventuelles futures communications.
Comme nous l'avons vu dans la description générale de la plate-forme proposée, les *nœuds spéciaux* offrent des services de passerelle et de canal aux nœuds présents sur un site donné. Les *nœuds spéciaux*, qui sont liés pour chacun d'entre eux à un site donné, sont dotés d'un moyen de communication particulier (ne figurant pas dans l'ensemble T, cf. section 2.2.2 page 67) leur permettant d'échanger, les uns avec les autres, des informations de contact. Dans la pratique, pour poursuivre avec l'exemple de Museum Quest, il est raisonnable de supposer que les conservateurs des différents musées considérés sont en relation les uns avec les autres (via messagerie électronique par exemple) ce qui leur permet de recueillir les informations à fournir aux *nœuds spéciaux*. Ainsi, les différents sites dans lesquels les nœuds de la plate-forme évoluent sont liés entre eux par les *nœuds spéciaux*. Pour entrer en contact avec une entité d'un site distant, un nœud doit donc utiliser comme passerelle le *nœud spécial* correspondant au site où il se situe.
Dans la suite, afin de récupérer les informations concernant les *nœuds spéciaux* (les adresses de connexion notamment) et les abonnements disponibles (pour accéder aux sites distants existant) liés à l'environnement local, on suppose qu'il existe un point de passage particulier dans chaque site. Ce point représente un endroit de l'espace local par lequel tous les nœuds présents sur un site considéré doivent obligatoirement passer. En poursuivant avec l'exemple de Museum Quest, il est possible de considérer que ce point de passage est la porte d'entrée de l'une des salles du musée dans lequel les opérations se déroulent. Ainsi, en traversant le point de passage particulier, les nœuds récupèrent les informations disponibles sur les *nœuds spéciaux* et les abonnements. Cette récupération de donnée est effectuée en interagissant avec un équipement spécifique via une technologie sans fil qui ne nécessite par la connaissance préalable d'une adresse de connexion. De façon pratique, il est raisonnable

d'envisager que les terminaux mobiles liés aux nœuds utilisent la technologie NFC pour lire le contenu d'un tag et obtenir les données recherchées. Chaque nœud peut alors avoir accès aux différents *nœuds spéciaux* de son environnement local et choisir les sites distants (à travers les abonnements) avec lesquels interagir. L'initialisation du système est alors effectuée et toutes les opérations soustendant dans notre approche peuvent être mises en œuvre.

La figure 3.54 résume le processus d'initialisation du système pour deux sites A et B. n_1 et n_2 sont des *nœuds spéciaux* qui échangent leurs informations respectives de contact à travers le canal particulier qui les lie. Quant au nœud n_3, après s'être rendu au point de passage (pour y récupérer les informations disponibles), il émet un message (après avoir au préalable effectué une demande d'abonnement au *nœud spécial* dont il a obtenu l'adresse de connexion) à destination du site distant B à travers le *nœud spécial* n_1 qui sert de canal pour accéder aux nœuds de B.



1 : Récupération d'informations sur les nœuds spéciaux et les abonnements
2 : n_3 a souscrit à l'abonnement abo_1 pour accéder au site B via le canal c_1 fourni par n_1
3 : Abonnements et envois de requêtes pour le site distant B
4 : Transfert des requêtes de n_3 au site B via le nœud spécial n_2
5 : Transfert des requêtes de n_3 aux nœuds du site B
6 : les nœuds du site B ont souscrit à l'abonnement abo_2 qui permet d'accéder aux informations du site A via le canal c_2 fourni par n_2

FIGURE 3.54 – Processus d'initialisation du système pour deux sites.

Chapitre 4

Implémentation de la plate-forme

Sommaire

Nous avons développé un prototype à partir des éléments de l'architecture multi-niveaux que nous avons proposée. Avant de présenter l'application développée ainsi que les tests qui ont été effectués, nous décrivons les technologies sans fil disponibles, la plate-forme de développement dont nous nous sommes servis et les équipements utilisés. Il est à noter que, dans notre contexte, chaque instance de l'application déployée sur un téléphone mobile (lié à un utilisateur donné) agit comme un nœud du système multi-niveaux.

4.1 Environnement de développement

4.1.1 Technologies de communication sans fil

Pour rappel, les nœuds de notre plate-forme multi-niveaux sont des téléphones mobiles. Les technologies sans fil disponibles sont donc celles qui équipent la plupart des téléphones les plus récents. Dans notre contexte, nous avons identifié quatre types de technologies.

4.1.1.1 NFC

La technologie NFC (Near Field Communication) est dérivée de la RFID (Radio Frequency Identification) [58][59]. C'est une technologie de communication sans fil dont la portée maximale est d'environ 10 centimètres, dont le débit théorique est de 100 Ko/s et dont l'utilisation n'engendre (généralement) aucun coût au sens financier du terme. L'un des plus importants promoteurs de cette technologie est l'industrie de la téléphonie mobile car la majorité des fabricants l'intègrent dans leurs nouveaux produits. Le NFC Forum, qui est un organisme de standardisation, veille à définir les spécifications techniques concernant les différents usages de cette technologie. Ce sont ces spécifications qui font référence dans l'écosystème NFC. A travers cet ensemble de spécifications, cette technologie atteint un niveau de maturité qui permet à la plupart des fabricants de l'intégrer dans leurs smartphones les plus récents.
Dans la pratique, la technologie NFC propose trois modes de fonctionnement : le mode lecture/écriture, le mode peer-to-peer (P2P) et le mode émulation de carte. Le mode lecture/écriture permet aux appareils NFC d'interagir avec des tags NFC afin d'y lire ou d'y stocker des informations. Les tags NFC sont des pièces de plastique sur lesquels figurent des circuits électroniques pouvant contenir des données. Le mode peer-to-peer (P2P) prend en charge les communications directes entre dispositifs NFC. Le mode émulation de carte, quant à lui, permet à un appareil NFC de fonctionner comme une carte à puce qui serait elle-même NFC. Les données sensibles sont stockées dans une puce appelée Secure Element (SE) qui est intégrée à l'équipement NFC considéré [88].
La technologie NFC trouve des applications principalement dans les domaines liés au contrôle d'accès, à la collecte et l'échange de données, au paiement mobile et à la billettique mobile dans le transport et l'événementiel.
En raison de ses caractéristiques, la technologie NFC offre les avantages suivants :

- la facilité d'utilisation car il suffit de rapprocher les équipements pour automatiquement initier les échanges de donnés ;
- la sécurité car la distance requise pour effectuer des communications limite les risques d'interception des données transmises ;
- la robustesse car les communications peuvent être réalisées dans des environnements variés et dans des conditions extrêmes lorsque cela est nécessaire (faible luminosité par exemple).

En raison de ses caractéristiques, la technologie NFC est utilisée, dans notre contexte, pour la récupération d'informations (mode lecture/écriture) sur les nœuds spéciaux (page 67) et les abonnements (cf. page 67) lors de l'initialisation du système et pour le déclenchement des échanges (mode peer-to-peer) des parties privées des profils de nœuds en cas de rencontre physique (cf. page 104).

4.1.1.2 Bluetooth

Bluetooth [98] est un protocole de communication par ondes radio défini, en particulier, par Ericsson, IBM, Intel, Nokia et Toshiba. L'objectif de ce protocole, qui est présenté dans la norme IEEE 802.15 [46], est de normaliser les communications sans fil de courte distance entre ordinateurs, PDA, téléphones mobiles et autres périphériques portables en réduisant, autant que possible, la consommation énergétique liée à ces communications. La portée maximale est d'environ 100 mètres, son débit théorique de 1 Mo/s et son utilisation n'engendre (généralement) aucun coût au sens financier du terme. Le SIG Bluetooth [1] est l'organisme qui définit les spécifications techniques de la technologie Bluetooth.
D'un point de vue pratique, chaque équipement doté du Bluetooth possède une adresse MAC unique. Le protocole comprend une opération de découverte de voisinage durant laquelle il est possible, pour un équipement mobile compatible, de récupérer les adresses MAC des dispositifs se trouvant à portée. Les communications se font alors en mode direct en utilisant l'adresse MAC du correspondant. Il est à noter que les communications suivent le modèle maître-esclave. En d'autres termes, le maître rend un service Bluetooth disponible sur le dispositif considéré ; les éventuels esclaves (sous réserve de connaître l'adresse MAC du maître et l'identifiant unique du service souhaité) peuvent se "connecter" au maître pour échanger des messages. Un équipement peut être à la fois maître et esclave.
En raison de ses caractéristiques, la technologie Bluetooth fait partie de l'ensemble T_{DI} (ensemble des technologies avec lesquelles un message est acheminé directement) que nous avons défini dans les éléments théoriques de nos travaux (cf. page 66). Cette technologie peut donc être utilisée dans les opérations de publication de profils ainsi que dans tout autre échange de messages entre nœuds au sein de la plate-forme multi-niveaux.

4.1.1.3 Wi-Fi direct

Wi-Fi direct, comme son nom l'indique, est dérivé du Wi-Fi qui est un protocole de communication par ondes radio pour dispositifs mobiles (ordinateurs, PDA, téléphones mobiles, etc.). Le protocole Wi-Fi est défini par la norme IEEE 802.11 et plus particulièrement par sa version 802.11n [107] (dernière version certifiée). En se basant sur le standard développé, il est possible d'identifier deux modes de fonctionnement :

- le mode infrastructure où un point d'accès joue le rôle de relais pour faire transiter les messages entre les différents équipements mobiles ;
- le mode ad hoc où les communications sont directes entre les équipements mobiles considérés.

Wi-Fi direct est une déclinaison du mode ad hoc dont la spécificité réside dans le fait que les équipements compatibles peuvent se découvrir les uns les autres lorsqu'ils sont à portée afin d'initier des échanges d'information. Au niveau des détails techniques, il est à noter que la portée moyenne de la technologie Wi-Fi est d'environ 100 mètres avec un débit théorique pouvant atteindre 600 Mbits/s et son utilisation en mode Wi-Fi direct n'engendre aucun coût de nature financière. La Wi-Fi Alliance est l'organisme chargé de définir les spécifications techniques concernant, notamment, les différents usages de la technologie Wi-Fi en général [15] et du mode Wi-Fi direct en particulier.
D'un point de vue pratique, chaque équipement doté de Wi-Fi direct possède une adresse

1. Special Interest Group Bluetooth - https ://www.bluetooth.org/en-us

MAC unique. Le protocole mis en œuvre permet à un dispositif mobile de réaliser une opération de découverte de voisinage pour déterminer les adresses MAC des dispositifs se trouvant à portée. Les communications se font alors en mode direct en utilisant l'adresse MAC du correspondant sous réserve que ce dernier accepte les échanges demandés.
De façon analogue à la technologie Bluetooth, la technologie Wi-Fi direct fait partie de l'ensemble T_{DI} décrit dans les éléments théoriques de nos travaux (cf. page 66) et peut donc être utilisée dans les opérations de publication de profils et dans tous les autres échanges de messages entre nœuds qui sont mis en œuvre sur notre plate-forme.

4.1.1.4 GSM/3G : envoi de SMS

Le GSM (Global System for Mobile communications) [91] est le standard de réseau pour la téléphonie mobile spécifié par l'ETSI (European Telecommunications Standard Institute). Le débit proposé dans un réseau mobile de type GSM peut atteindre 24 Kbits/s. Ce réseau rend possible l'échange de messages textuels, c'est à dire les SMS (Short Message Service), et la transmission de la voix pour les appels téléphoniques. Quant à la 3G (Troisième Génération) [27], elle représente l'évolution du GSM visant à fournir des débits plus élevés (plus de 2 Mbits/s). Cette évolution permet de proposer, sur les réseaux de ce type, de nouveaux services comme l'accès à Internet.
D'un point de vue pratique, chaque opérateur mobile désireux de proposer des services (appels, envois de SMS, accès à Internet) déploie son réseau GSM/3G en fonction des spécifications des normes. Ce déploiement s'effectue en disposant des antennes relais, reliées entre elles, pour couvrir les zones où on souhaite rendre les services disponibles. Les données échangées sur le réseau sont alors transmises à travers les antennes relais suivant les positions des correspondants. Du fait que les réseaux des différents opérateurs mobiles sont inter-connectés, il est possible d'entrer en contact avec un correspondant quelle que soit sa position géographique pour peu qu'elle soit couverte par l'un ou l'autre des opérateurs. Il est également à noter que pour utiliser le réseau d'un opérateur mobile, il nécessaire de posséder un abonnement qui spécifie les services accessibles et qui donne le droit de disposer d'un numéro unique. Ce numéro, qui a un caractère privé, permet l'identification du nœud considéré sur l'ensemble des réseaux GSM/3G. Concrètement, l'envoi de SMS via les réseaux GSM/3G s'opère en utilisant le numéro du correspondant afin de spécifier la destination du message (qui va transiter par les antennes relais appropriées). Il est donc au préalable nécessaire d'obtenir du destinataire du message le numéro qui l'identifie et qui est impossible à déterminer par découverte de voisinage contrairement aux technologies Bluetooth et Wi-Fi direct. Les coûts (au sens financier) liés à l'envoi et à la réception de SMS dépendent du type d'abonnement auxquel l'émetteur et le récepteur ont souscrit pour utiliser les services des réseaux GSM/3G considérés.
En raison de ses caractéristiques, la technologie liée à l'envoi de SMS à travers les réseaux GSM/3G d'un opérateur mobile fait partie de l'ensemble T_{Re} (ensemble des technologies avec lesquelles l'utilisation d'une infrastructure relai est nécessaire dans l'acheminement d'un message) décrit dans nos travaux (cf. page 66). Cette technologie ne peut donc pas être utilisée dans les opérations de publication de profils de notre plate-forme multi-niveaux. En revanche, elle peut être utilisée pour des échanges de messages entre nœuds qui se connaissent suffisamment pour détenir les informations privées nécessaires (numéro du correspondant) à ce type de communication (cf. page 104).

4.1.2 Plate-forme Android

Après avoir identifié les technologies sans fil disponibles sur les nœuds du système multi-niveaux, il est nécessaire de choisir une plate-forme mobile pour le prototype à développer. En raison de ses caractéristiques techniques et de sa popularité, notre choix s'est porté sur la plate-forme Android. Nous présentons donc cette plate-forme ainsi que l'équipement mobile compatible dont nous nous sommes servis lors du développement du prototype.

4.1.2.1 Description

Android [web2] est un système d'exploitation *open-source*, développé par Google pour les équipements mobiles tels que les téléphones portables, les smartphones et les tablettes tactiles. Ce système permet d'exploiter toutes les possibilités de connectivité des équipements mobiles sur lesquels il peut être déployé. Afin de faciliter le travail des développeurs, Google propose quelques outils parmi lesquels :

- un ensemble d'APIs (Application Programming Interface) [web3], basées sur le langage de programmation Java ;
- un plugin Eclipse [2] visant à faciliter l'utilisation de ces APIs.

En plus des éléments permettant de créer des interfaces utilisateurs, il est à noter que la plate-forme Android fournit des APIs de gestion de la technologie Bluetooth et de l'envoi/réception de SMS. Concernant les technologies NFC et Wi-Fi direct, elles sont respectivement prises en charge à partir des versions 2.3 et 4.0 du système d'exploitation. Tous ces éléments rendent pertinent le choix de la plate-forme Android. Ce choix est d'autant plus pertinent que, selon les données recueillies par Mobile Statistics, en juin 2012 56% des smartphones du marché étaient équipés d'une version du système d'exploitation Android [web20].

4.1.2.2 Configuration utilisée

Pour le développement du prototype, nous avons utilisé deux types d'équipement mobile. Il s'agit du Nexus S [web23] et du Galaxy Nexus [web14] qui sont deux smartphones proposés par Google et qui embarquent le système d'exploitation Android. Le tableau 4.16 présente quelques caractéristiques techniques de ces deux smartphones. Les deux raisons suivantes ont conduit au choix de ces deux téléphones :

- les types de technologies sans fil dont ils sont équipés correspondent aux technologies identifiées pour notre plate-forme ;
- les deux téléphones sont des appareils proposés par Google ce qui assure une compatibilité optimale des APIs Android (et de leurs éventuelles évolutions).

Le Nexus S et le Galaxy Nexus ont donc servi dans les opérations de développement, de débogage, de test, de déploiement et d'évaluation du prototype que nous avons développé sur la base des éléments définis dans les chapitres précedents.

2. Eclipse [web10] est un environnement de programmation qui permet de gérer le cycle de développement d'une application (écriture du code, débogage, test et déploiement sur la matériel considéré)

Caractéristiques \ ***Appareil***	Nexus S	Galaxy Nexus
Connectivité	NFC, Bluetooth, GSM/3G	NFC, Bluetooth, Wi-Fi direct, GSM/3G
Résolution d'écran	WVGA (800 x 480)	WXGA (1280 x 800)
Système d'exploitation initial	Android 2.3	Android 4.0

TABLE 4.16 – Quelques caractéristiques techniques du Nexus S et du Galaxy Nexus.

4.2 Application : *Multilevel Secure Messaging Application*

C'est un outil de messagerie sécurisée qui permet à un utilisateur d'entrer en contact avec des personnes se trouvant dans son environnement local (musée où il se trouve) ou distant (musée situé dans une zone géographique différente de la sienne). Cette mise en relation avec d'autres personnes a pour objectif de recevoir de l'aide, par exemple, sur une question particulière de la quête (en effectuant une requête comme nous le verrons dans la suite). Avant de décrire l'architecture et le fonctionnement de cette application que nous avons appelée MuSMA pour *Multilevel Secure Messaging Application*, nous allons présenter quelques choix de développement que nous avons effectués.

4.2.1 Choix de développement

4.2.1.1 Sécurité

En se référant à la définition de la plate-forme multi-niveaux, chaque nœud est doté d'un module lui conférant des capacités cryptographiques (chiffrement/déchiffrement et signature de données). De façon pratique, cela signifie que les téléphones mobiles utilisés dans le développement du prototype doivent être équipés d'un élément sécurisé ou *Secure Element* (contenant les clés cryptographiques nécessaires) avec lequel l'application interagira afin d'assurer la réalisation des opérations de sécurisation. Dans le but de simplifier le développement, nous avons choisi d'intégrer le module cryptographique au prototype sous forme de composant logiciel (l'interfaçage d'un *Secure Element* avec les APIs Android pouvant s'avérer complexe). Pour cela nous utilisons l'API de la plate-forme Android qui permet de générer des paires clé publique/clé privée et de procéder au chiffrement/déchiffrement/signature de données. Nous avons donc intégré la gestion des opérations suivantes dans le prototype développé :

- afin de préserver le caractère secret de la clé privée, l'accès à l'application est protégé par un mot de passe. Lors de la première utilisation, la paire clé publique/clé privée est générée par l'application pour le nœud considéré. L'utilisateur choisit un mot de passe pour procéder à un chiffrement symétrique (avec le protocole AES dans notre cas) de la clé privée. La clé privée chiffrée et la clé publique correspondant sont stockées dans le téléphone mobile.
- lors du lancement de l'application (en dehors de la première utilisation), l'utilisateur est invité à entrer son mot de passe afin de procéder au déchiffrement de la clé privée stockée dans le téléphone considéré. Un nombre aléatoire est alors généré, chiffré avec la clé publique stockée dans le téléphone. Le résultat de ce chiffrement est ensuite

déchiffré avec la clé privée obtenue à partir du mot de passe entré et il en résulte un deuxième nombre. Si les deux nombres sont identiques, l'accès à toutes les fonctionnalités de l'application est accordé. Cette opération est une adaptation des protocoles de type *challenge-response* [53] qui permettent d'authentifier un utilisateur.

Précisons que, lorsque l'application est en cours d'exécution, la clé privée est chargée dans la mémoire du téléphone (elle y est aussi chargée au moment de sa génération) afin que les opérations de déchiffrement et de signature soient possibles. Cette situation peut causer des failles de sécurité car le téléphone mobile n'est pas considéré comme un dispositif sûr (contrairement à un élément sécurisé). Pour ces raisons, il est prévu d'intégrer l'utilisation d'un élément sécurisé (pour stocker de façon plus sûre les clés de chiffrement) dans les perspectives d'évolution du prototype. Toutefois, même si ces choix de développement réduisent le niveau de sécurité attendu, il nous apparaît raisonnable de considérer, dans notre contexte, que le prototype implémenté reste représentatif de la plate-forme multi-niveaux décrite précédemment.

4.2.1.2 Profils

Par ailleurs, pour simplifier le développement du prototype, nous n'avons pas intégré de dictionnaire permettant de déterminer la forme canonique des mots (comme cela est requis pour les opérations de recherche de profils compatibles, cf. page 122). Nous supposons donc que les informations fournies dans les profils, au titre des compétences à mettre à disposition des entités de la plate-forme, sont déjà sous forme canonique.

4.2.2 Architecture

Les différents modules du prototype sont mis en œuvre par des classes (Java) développées avec les APIs Android. Nous utilisons aussi une base de données qui contient les informations à sauvegarder. Il est à noter qu'il existe sous Android plusieurs types de classes que l'on ne retrouve pas en Java :

- le type classique qui représente les classes Java classiques ;
- le type activité pour une classe qui est associée à une interface utilisateur spécifique (interface pour envoyer un courrier électronique par exemple) et qui permet à un utilisateur d'interagir avec l'application ;
- le type service pour une classe qui contient des opérations s'exécutant en arrière-plan (de l'application) sans besoin de l'intervention d'un utilisateur et pouvant nécessiter une longue durée d'exécution (requête à un serveur distant, découverte du voisinage, etc.). Une classe de type service n'est liée à aucune interface utilisateur.

La figure 4.55 présente les différents modules de l'architecture du prototype. Ces modules et leurs différents liens sont les suivants :

- **Principal.** Ce module, qui est une activité (au sens de la plate-forme Android), intègre l'interface utilisateur principale de l'application. Cette interface permet à l'utilisateur d'être notifié des informations reçues à travers le module **Réception** (voir ci-dessous), d'envoyer des messages via le module **Communication** (voir ci-dessous) et d'initier des opérations particulières (saisie/mise à jour des informations personnelles, échange de profils, recherche de profils, etc.). Cette activité intègre également

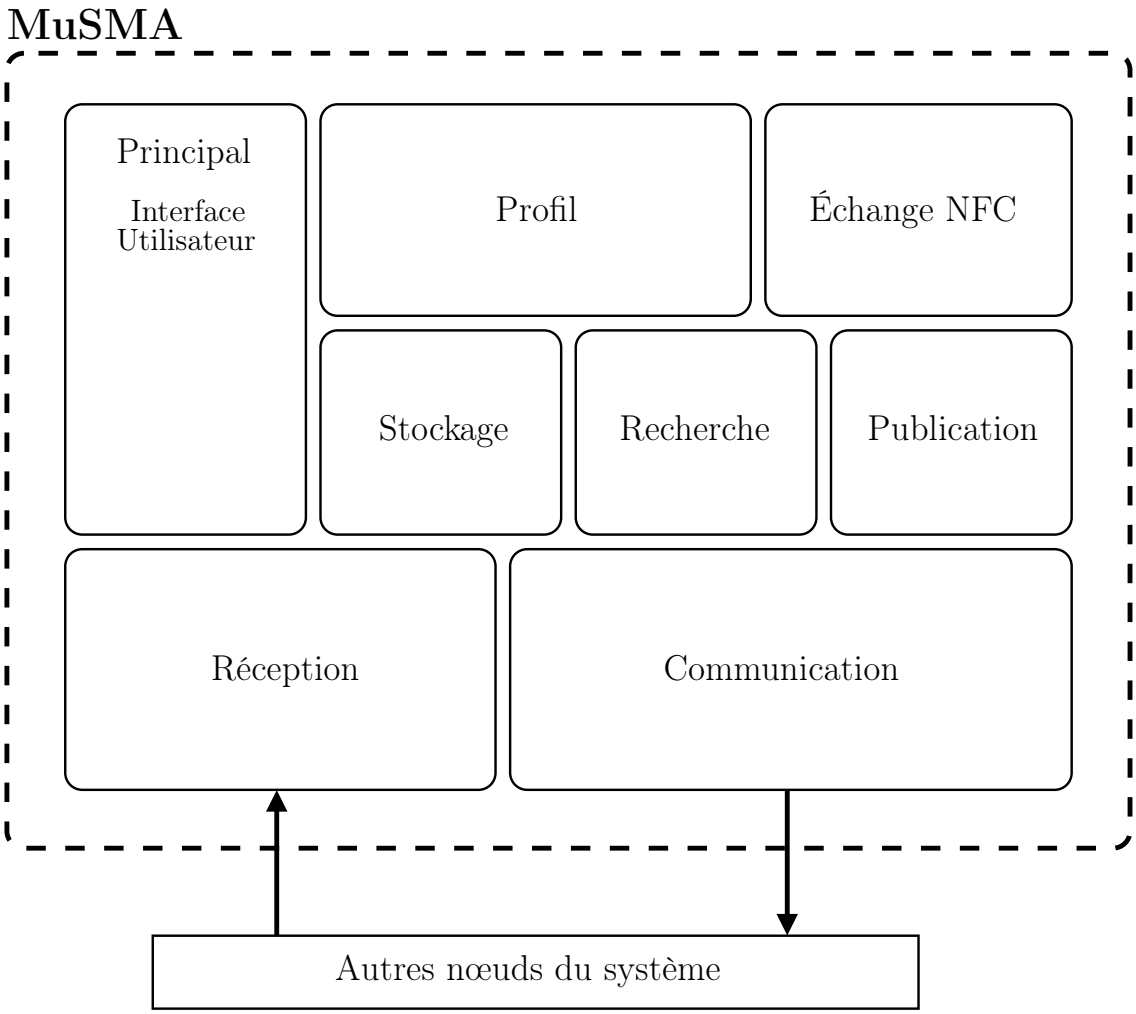


FIGURE 4.55 – Architecture de l'application MuSMA.

les éléments cryptographiques qui permettent de chiffrer et signer les messages à sécuriser avant leur expédition (données de la classe **Profil** et du module **Stockage**, voir ci-dessous).

- **Réception.** Ce module est un service (au sens de la plate-forme Android) qui gère la réception de messages suivant les différents technologies disponibles à savoir NFC, Bluetooth, Wi-Fi direct et SMS. Ces messages peuvent être des requêtes d'autres nœuds, des résultats de recherches de voisinages, des informations sur des profils échangés ou encore des profils publiés.
- **Communication.** Ce module est un service qui gère l'envoi de messages suivant les différentes technologies disponibles (NFC, Bluetooth, Wi-Fi direct et SMS). Ces messages peuvent être des requêtes à destination d'autres nœuds, des recherches de voisinage, des informations sur des profils échangés ou la publication du profil du nœud considéré.

- **Profil.** Ce module est une classe Java qui permet la gestion des informations personnelles (préférences, paire de clés de chiffrement, compétences, etc.) du nœud considéré. Lors du premier lancement de l'application, les informations personnelles qui ont été saisies sont enregistrées dans des fichiers (comme nous le verrons plus loin). **Profil** fournit également les fonctions qui permettent aux autres modules de l'architecture d'avoir accès aux informations personnelles enregistrées. Il est également possible, grâce à ce module, de mettre à jour le profil du nœud considéré.
- **Publication.** Ce module est un service qui exécute les opérations de publication de profil du nœud considéré, telles que décrites dans la présentation de l'approche proposée pour la plate-forme multi-niveaux (cf. page 83). Après avoir récupéré les informations nécessaires dans le module **Profil**, une recherche de voisinage (suivant les technologies disponibles) ainsi que l'envoi du profil aux destinataires identifiés dans le voisinage via le module **Communication** sont initiés.
- **Recherche.** Ce module est un service qui initie les opérations de recherche de profils (en local et dans le voisinage accessible) correspondant à un besoin donné que le nœud considéré spécifie (conformément à la description de l'approche multi-niveaux proposée). Ces opérations de recherche s'appuient sur le module **Stockage** (voir ci-dessous) et sur le module **Communication** (pour des requêtes dans le voisinage). Le service **Recherche**, après identification de profils compatibles et suivant les préférences du nœud considéré, procède au choix de la technologie la plus appropriée (en mettant en application les éléments correspondant de l'approche multi-niveaux proposée) pour entrer en contact avec l'entité qui pourrait le mieux répondre au besoin spécifié.
- **Échange NFC.** Ce module est un service qui est chargé de mettre en œuvre, en utilisant la technologie NFC, l'échange de la partie privée du profil du nœud courant lors d'une rencontre physique avec un autre utilisateur (tel que décrit dans la description de la plate-forme multi-niveaux, cf. page 104). Après initiation de l'échange via NFC, le module permet d'envoyer les informations choisies en utilisant le service **Communication** et d'attendre la réception des données de profil de la part du correspondant (à partir du service **Réception**). Il est à noter que les données à échanger sont récupérées à partir de la classe **Profil**.
- **Stockage.** Ce module est une base de donnée SQLite [75], intégrée à l'application et qui contient toutes les données à sauvegarder reçues à travers le module **Réception**. Les données enregistrées dans la base de données **Stockage** concernent les profils publiés par les autres nœuds et les informations reçues lorsque les opérations du module **Échange NFC** sont déclenchées. De façon pratique, **Stockage** fournit une interface qui permet aux autres modules d'obtenir des informations de profils utiles dans les opérations à initier (envoi de message chiffré, recherche de profils compatibles, etc.).

4.2.3 Fonctionnement

Nous allons maintenant décrire, de façon plus concrète, à l'aide de captures d'écran, le fonctionnement de l'application MuSMA. Nous avons retenu les scénarios d'utilisation suivants : premières utilisations de l'application ; prise en main de l'interface principale ; recherche de profils compatibles ; réponse à une requête et échange d'informations privées du profil. Chaque scénario est détaillé dans la suite.

4.2.3.1 Premier lancement de l'application

Lors de la première utilisation de l'application, un écran de configuration (écran de gauche de la figure 4.56) contenant un formulaire à remplir est affiché. L'utilisateur est invité à saisir un ensemble d'informations (conformément aux éléments décrits dans la plate-forme multi-niveaux) qui permettent de définir ses préférences et ses rapports avec les autres utilisateurs. Ces informations, dans l'ordre d'affichage, sont les suivantes :

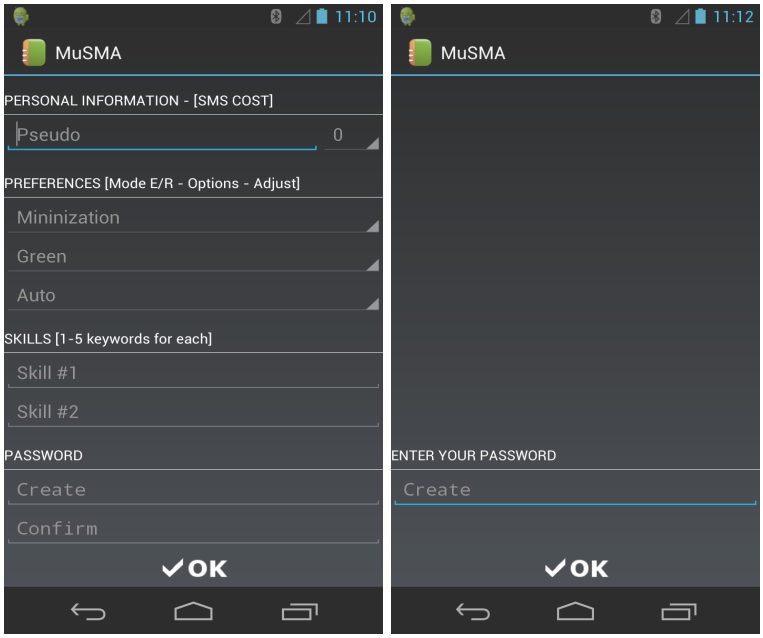
- le pseudonyme sous lequel il souhaite être connu par les autres entités ;
- le coût au sens financier de l'envoi d'un SMS pour l'utilisateur considéré ;
- le critère à utiliser (minimisation des coûts ou historique des communications) pour procéder au choix de technologie pour contacter ou être contacté par une autre entité ;
- l'option retenue (verte, économe ou efficace) pour le choix de technologie ;
- le mode d'ajustement (automatique ou manuel) des paramètres de choix de technologie pour contacter une autre entité en fonction des événements qui peuvent intervenir (niveau de la batterie particulièrement faible ou encore seuil des dépenses liées aux communications effectuées atteint) ;
- les compétences (sous forme de deux séries de 5 mots au maximum) que l'utilisateur souhaite mettre à la disposition des autres utilisateurs ;
- le mot de passe (saisi deux fois pour confirmation) qui permet de limiter l'accès à l'application.

Après la saisie des informations nécessaires, la validation du formulaire par le bouton OK entraîne la génération d'une paire clé publique/clé privée et la création de trois fichiers qui sont stockés dans l'espace dédié à l'application dans la mémoire du téléphone. Le premier fichier contient toutes les informations personnelles et les préférences fournies dans le formulaire ainsi que le numéro de téléphone (si le téléphone est relié au réseau d'un opérateur) automatiquement récupéré (à travers les APIs fournies à cet effet par la plate-forme Android). Le deuxième fichier contient la clé publique générée. Quant aux troisième fichier, il contient la clé privée chiffrée au moyen du mot de passe choisi.
Dans la suite, lorsque l'application est lancée, un écran invitant à la saisie d'un mot de passe est affiché (écran de droite de la figure 4.56). Si le mot de passe saisi est le bon, l'accès à l'interface principale de l'application est alors autorisé.

4.2.3.2 Prise en main de l'interface principale

Comme le montre la figure 4.57, l'interface principale de l'application est constituée de deux parties : une partie messages/profils et une partie contacts. La vue messages et profils permet d'afficher les messages en provenance d'autres utilisateurs et les informations élémentaires au sujet des profils reçus (et donc publiés par d'autres entités). La vue contacts, quant à elle, affiche la liste des contacts avec lesquels des informations privées de profil ont été échangées. De plus, l'interface principale contient un menu, accessible depuis les deux parties présentées ci-dessus, dans lequel sont incluses les entrées suivantes :

- un élément *My profile* qui permet d'afficher le résumé du profil de l'utilisateur courant (correspondant aux informations saisies dans le formulaire lors du premier lancement de l'application) ;
- un élément *New contact* qui permet d'initier (via NFC) l'opération d'échange de la partie privée du profil avec une entité rencontrée physiquement ;



Configuration initiale **Saisie du mot de passe**

Figure 4.56 – Prototype MuSMA - configuration et saisie du mot de passe.

- un élément *Publication* qui permet de lancer la procédure de publication du profil dans le voisinage de l'utilisateur courant ;
- un élément *Empty lists* qui permet de vider de leur contenu respectivement la liste des profils reçus et la liste des contacts échangés.

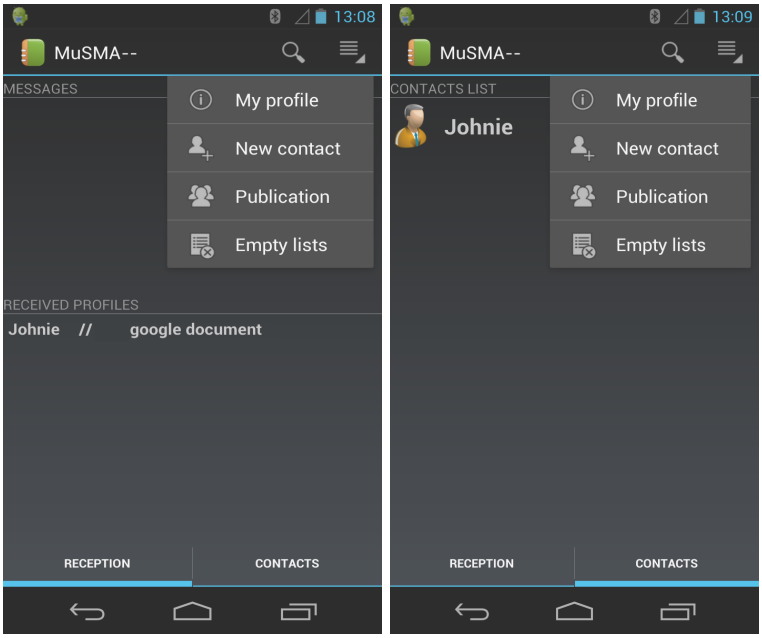
L'interface principale contient également une icône (premier élément à gauche du mot *MuSMA*– sur la figure 4.57) pour lancer une opération de recherche de profils (en local et dans le voisinage) répondant à des critères particuliers à spécifier.

4.2.3.3 Recherche de profils compatibles

La recherche de profils compatibles fonctionne en deux temps (captures d'écran présentées figure 4.58). Dans un premier temps, l'utilisateur saisit dans le champs prévu à cet effet (écran de gauche) les compétences recherchées. Après l'appui sur le bouton *Start*, la recherche est alors initiée parmi les profils reçus et parmi les entités accessibles dans le voisinage. Dans le cas où la recherche est fructueuse, les profils compatibles sont alors affichés et l'utilisateur peut choisir un correspondant auquel envoyer sa demande (écran de droite). Le choix de la technologie de communication est automatiquement effectué en fonction des préférences de chaque entité impliquée.

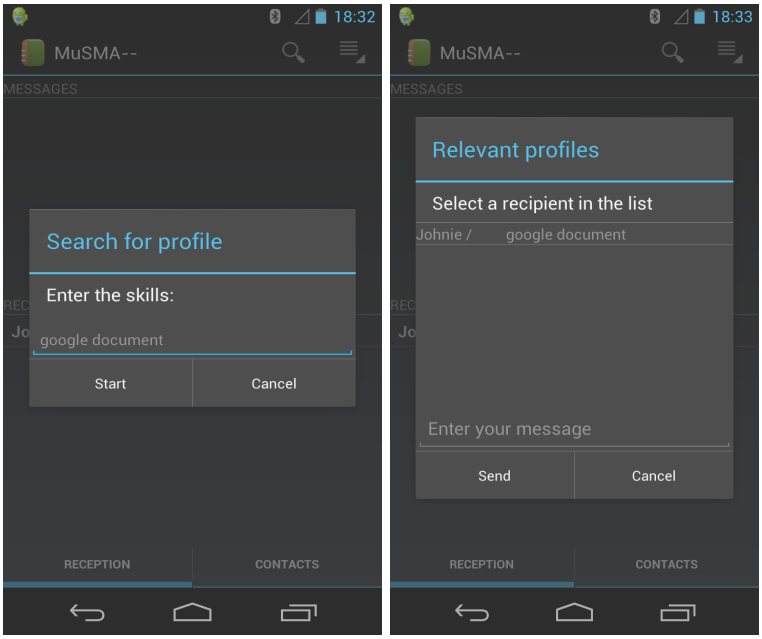
4.2.3.4 Réponse à une requête

Nous avons vu, dans la partie précédente, que les utilisateurs de l'application peuvent envoyer des requêtes (que l'on peut aussi appeler des demandes d'aide), en fonction d'un besoin spécifique, aux entités accessibles de leurs voisinages respectifs. Ces requêtes peuvent être traitées automatiquement ou remontées à l'utilisateur. C'est le deuxième scénario que



Partie message et profils **Partie contacts**

FIGURE 4.57 – Prototype MuSMA - interface principale.

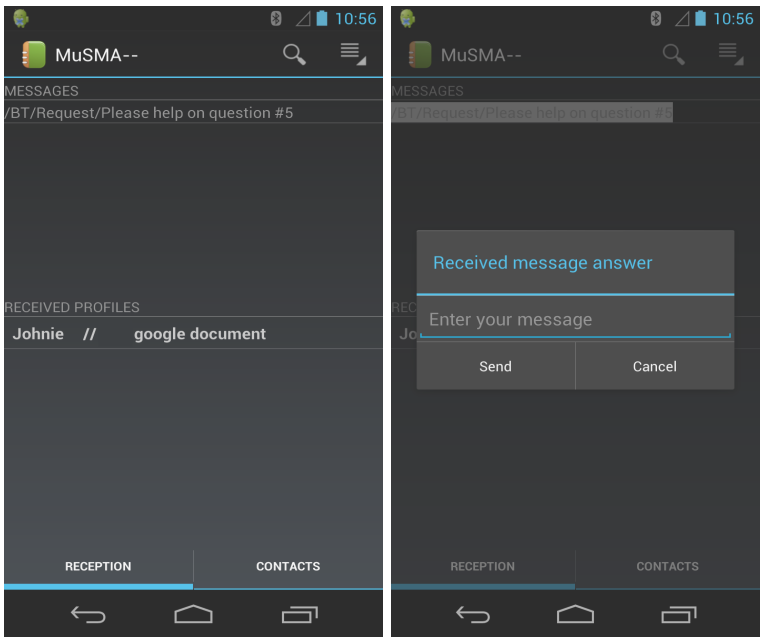


Saisie pour la recherche **Choix du destinataire**

FIGURE 4.58 – Prototype MuSMA - interface de recherche de profils.

nous présentons ici. Lors de la réception d'une telle requête, l'utilisateur de l'application considérée peut donc répondre à l'émetteur. La partie de gauche de la figure 4.59 présente un écran dans lequel une requête reçue est affichée dans la partie Messages de l'interface.

Pour répondre à la requête, l'utilisateur doit sélectionner le message dans la liste. Un champs pour saisir la réponse est alors affiché (écran de droite de la figure 4.59). Comme cela est le cas pour la recherche de profils, le choix de la technologie pour envoyer le message de réponse à la requête est automatiquement effectué en fonction des préférences des entités impliquées.



Demande d'aide **Proposition d'aide**

Figure 4.59 – Prototype MuSMA - réception d'une requête et envoi d'une réponse.

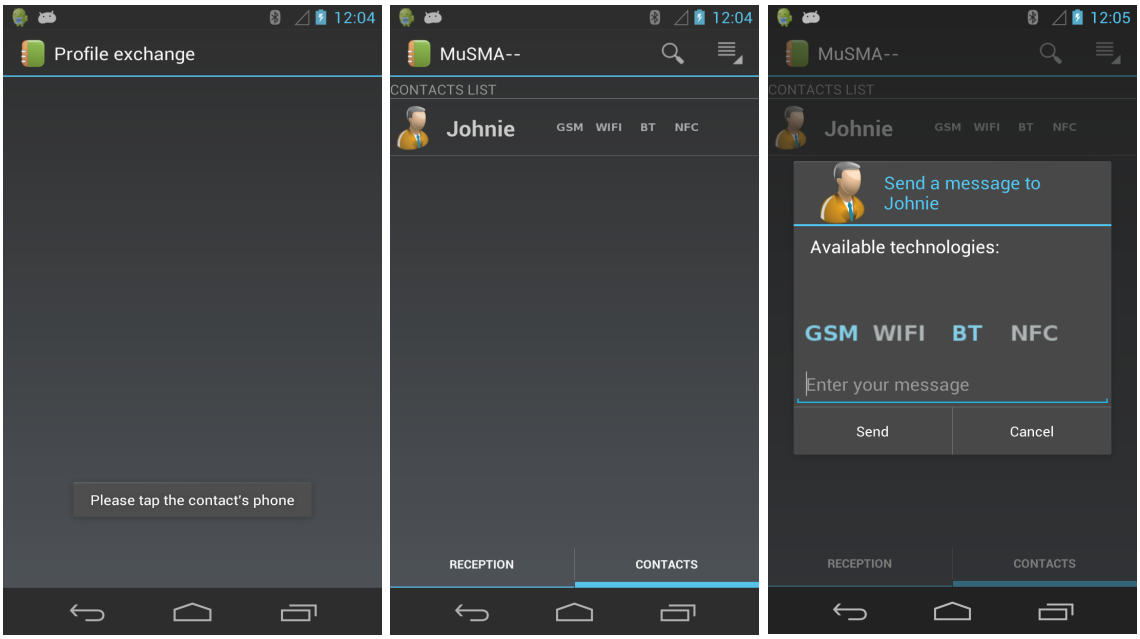
4.2.3.5 Échange d'informations du profil

Pour initier un échange d'informations privées de profil, l'utilisateur doit sélectionner l'élément *New Contact* du menu de l'interface principale. L'initialisation de l'échange s'effectue via la technologie NFC et un écran invite l'utilisateur à approcher son téléphone de celui du contact à ajouter (écran de gauche de la figure 4.60). Le contact considéré valide alors l'échange (s'il le juge pertinent) sur l'écran affiché sur son téléphone et les données privées des profils des deux protagonistes sont transmises de manière sécurisée entre les nœuds par Bluetooth. A la réception des informations transmises, les listes de contact des deux nœuds sont mises à jour en intégrant le contact ajouté comme le présente l'écran du milieu de la figure 4.60.
A partir de cet instant, chaque utilisateur concerné par l'échange peut directement entrer en contact avec son correspondant (lorsque celui-ci est accessible) à travers les technologies disponibles. L'écran du milieu de la figure 4.60 montre qu'en sélectionnant le contact à qui adresser un message une nouvelle fenêtre s'affiche. Cette fenêtre comprend non seulement un champs permettant de saisir un message à destination du contact sélectionné mais aussi des indications concernant les technologies (affichées en bleu) avec lesquelles ce contact est accessible à l'instant t donné. L'utilisateur peut choisir la technologie, parmi celles qui

Équipement \ *Technologie*	Bluetooth	Wi-Fi direct
Nexus S	10m / 0.005%	-
Galaxy Nexus	15m / 0.006%	50m / 0.009%

TABLE 4.17 – Portée et coût énergétique mesurés pour le Nexus S et le Galaxy Nexus.

sont disponibles, avec laquelle envoyer le message mais il peut aussi laisser l'application déterminer la technologie la plus appropriée suivant le contexte.



Initialisation **Insertion dans la liste de contacts** **Envoi de message au contact**

FIGURE 4.60 – Prototype MuSMA - échanges de données privées de profil.

4.3 Tests et évaluations

Les tests permettent d'analyser, en pratique, le fonctionnement de l'application et donc le fonctionnement des modules de la plate-forme multi-niveaux proposée dans un environnement réel. Pour réaliser ces évaluations, nous notons que le fonctionnement du prototype développé nécessite, notamment pour les opérations de publication de profil, la spécification du coût énergétique de l'envoi d'un message et la spécification de la portée pour les technologies Bluetooth et Wi-Fi direct. Nous avons donc effectué des tests basiques qui ont permis de déterminer ces valeurs qui sont présentées dans le tableau 4.17 où chaque cellule mentionne la portée et le pourcentage de batterie (chargée à 100%) utilisé dans l'envoi d'un message pour une technologie et un équipement donnés.

Il nous est dans un premier temps apparu pertinent de considérer l'opération de publication de profils, le niveau de consommation énergétique induit et la performance des opérations

cryptographiques. Ces points représentent, à notre avis, les éléments essentiels à évaluer afin de valider le fait que l'application est adaptée à un environnement réaliste. En effet, le fonctionnement de la plate-forme multi-niveaux repose sur le fait que les nœuds puissent largement publier leurs profils respectifs tout en maintenant un niveau de consommation énergétique (pour chaque nœud) raisonnable étant donné le contexte orienté MANets tout en prenant en compte les aspects liés à la sécurité.

4.3.1 Publication de profil

Il s'agit, à ce niveau, de vérifier que la méthode de publication du profil d'un nœud est applicable dans un environnement réaliste en fonction des technologies sans fil disponibles (à savoir Bluetooth et Wi-Fi direct). A partir des données fournies par le musée de Normandie à Caen (musée où est déployé une version de l'application *Museum Quest*, cf. section 1.2.3.4 page 38), il apparaît que la taille moyenne des salles où sont exposées les œuvres est de $50m^2$ et qu'environ 10 personnes sont présentes (en moyenne) à un instant t donné dans une même salle. Nous avons donc décidé d'effectuer des tests en faisant les deux hypothèses suivantes qui découlent de ces constatations :

- 10 nœuds se retrouvent dans une zone qui couvre un espace de 50 m^2 ;
- un des nœuds publie son profil à destination des autres nœuds.

Pendant l'opération de publication de profil de la plate-forme multi-niveaux, le nœud considéré demande la retransmission de son profil à un de ses voisins A (vers un autre de ses voisins B) si la condition suivante est remplie : A est potentiellement lié à B avec une technologie de portée au moins 3 fois supérieure à celle avec laquelle le nœud qui publie le profil est potentiellement lié à B (ce que nous avons justifié dans la partie validation de l'opération de publication de profil, cf. section 3.3.1 à la page 114). Cependant, en raison des contraintes techniques (liées aux portées des technologies sans fil disponibles sur les terminaux utilisés), nous avons choisi pour ces tests de simplifier la procédure de retransmission de profil. En effet, dans une phase de tests, on ne peut pas raisonnablement attendre que les bonnes conditions de positionnement spatial et de potentiel de communication entre nœuds (suivant les critères mentionnés ci-dessus) soient remplies pour que la retransmission ait lieu. Le scénario simplifié que nous avons donc retenu, de façon arbitraire mais pertinente par rapport à nos objectifs de validation, est le suivant :

- à un instant t donné, le nœud initiateur (1) a collecté les informations nécessaires sur son voisinage et il initie l'opération de publication de son profil ;
- à partir des informations de voisinage collectées, le nœud considéré envoie directement via Bluetooth son profil à 6 nœuds tout en demandant à l'un d'entre eux de retransmettre le profil reçu aux 3 derniers nœuds via Wi-Fi direct ;
- à l'instant t considéré (par le nœud qui publie le profil), les nœuds qui ne publient pas de profil effectuent chacun une opération d'émission ou de réception d'un message (afin de représenter une situation où les nœuds qui doivent recevoir le profil sont actifs) ;
- on notera qu'à l'instant t considéré, il est supposé que les nœuds ne bougent plus dans la zone qui est prise en compte.

Le scénario proposé permet d'effectuer des tests pour des envois directs de profils via Bluetooth et Wi-Fi direct ainsi que pour des envois de profils avec retransmission. Il est à noter que, pour chaque exécution du scénario, les nœuds seront répartis de façon aléatoire

n° nœud \ *Détails*	Technologie	Nbre de réceptions	% de réception	Moyenne
1 (émetteur)	-	-	-	-
2	Bluetooth	32	64%	74%
3	Bluetooth	41	82%	
4	Bluetooth	43	86%	
5	Bluetooth	35	70%	
6	Bluetooth	33	66%	
7	Bluetooth	38	76%	
8	Wi-Fi direct	29	58%	62%
9	Wi-Fi direct	34	68%	
10	Wi-Fi direct	30	60%	

TABLE 4.18 – Taux de réception du profil publié.

dans la zone prévue pour les tests. Le scénario est répété 50 fois et un relevé des nœuds qui ont reçu le profil est réalisé à chaque fois. Les résultats obtenus sont présentés dans le tableau 4.18.

Ce tableau indique la technologie via laquelle le nœud considéré est supposé recevoir le profil publié (colonne Technologie) ainsi que le nombre de réceptions et les pourcentages associés. Les résultats montrent en moyenne que dans 74% des cas le profil est reçu via Bluetooth et dans 62% des cas via Wi-Fi (à travers une retransmission). Les taux de non réception résultant, même s'ils paraissent relativement élevés sont à relativiser. En effet, après les analyses que nous avons effectuées, nous avons noté que dans 90% des cas où le profil n'avait pas atteint une cible, un voisin (accessible) du nœud considéré avait reçu le profil (ce qui lui permettait d'y avoir potentiellement accès en cas de besoin).
Selon les résultats obtenus pour le scénario appliqué, il nous semble raisonnable d'affirmer que l'opération de publication de profil se déroule de façon satisfaisante avec le prototype développé.

4.3.2 Consommation énergétique

Il s'agit de vérifier, de façon pratique, que le niveau de consommation énergétique supplémentaire induite par l'utilisation de notre application n'est pas trop élevé. Nous avons donc effectué des tests pour évaluer cette consommation d'énergie additionnelle. Pour ce faire, nous avons défini un profil spécifique d'utilisation de l'application qui est basé sur des données réalistes. Ces données dont de deux natures :

- selon les informations que nous avons pu recueillir auprès du musée de Normandie, la durée moyenne d'une visite est d'environ 1h ;
- la version de Museum Quest déployée dans le musée de Normandie comprend 24 questions relatives aux œuvres exposées.

Le profil d'utilisation, qui prend en compte ces deux paramètres, comprend les spécifications suivantes :

- l'application est exécutée durant 1h sur le téléphone mobile considéré ;
- l'application effectue une opération de publication de profil de l'utilisateur courant dans le voisinage ;

Équipement \ ***Consommation***	% classique	% avec MuSMA	Surcoût
Nexus S 1	24	28	16,6%
Nexus S 2	26	31	19,2%
Galaxy Nexus 1	34	40	17,6%
Galaxy Nexus 2	32	38	18,7%

Table 4.19 – Surcoût en consommation d'énergie avec le profil d'utilisation défini.

– l'application, après recherche de profils compatibles reçus, envoie 24 messages de demande d'aide, 8 via Bluetooth, 8 via Wi-Fi direct et 8 via SMS. Dans le cas où le Wi-Fi direct n'est pas disponible sur l'équipement mobile considéré, ce sont 12 messages qui sont envoyés par Bluetooth et 12 messages par SMS.

Pour réaliser les tests, nous avons tout d'abord chargé à 100% la batterie des téléphones mobiles et nous les avons utilisés de manière classique en enregistrant le niveau de consommation d'énergie chaque jour pendant une semaine. Nous avons ensuite répété la même procédure dans les mêmes conditions et avec les mêmes appareils, en exécutant cette fois l'application mobile suivant le profil d'utilisation décrit ci-dessus. Le tableau 4.19 présente les résultats que nous avons obtenus, en moyenne de pourcentage de batterie consommé sur 1 semaine, le tout sur 4 téléphones mobiles, à savoir deux Nexus S et deux Galaxy Nexus. Le surcoût semble important (18% en moyenne) et il peut être expliqué par le fait que le Bluetooth, le Wi-Fi direct et l'accès au réseau GSM doivent être en permanence activés. Néanmoins, il doit être mis en perspective par rapport à la consommation d'autres applications mobiles de référence. Par exemple, le navigateur intégré de la plate-forme Android consomme 0,35% de la batterie pour une utilisation de 30 secondes [78].

4.3.3 Performance des opérations cryptographiques

Il s'agit de réaliser des tests de performance, en terme de vitesse d'exécution de l'application, dans le cadre des opérations cryptographiques réalisées lors de l'émission de paquets en mode sécurisé (communication directe entre deux nœuds). La procédure de test mise en œuvre est la suivante :

– nous exécutons plusieurs fois la partie de l'application mobile qui consiste à sélectionner un destinataire, à signer et chiffrer un message avant de l'envoyer ainsi que la partie qui consiste à déchiffrer et à contrôler la signature à la réception d'un message (pour des raisons pratiques, nous choisissons d'utiliser la technologie Bluetooth pour les tests)
– le temps d'exécution de chaque opération effectuée plus haut est relevé ainsi que le temps nécessaire pour réaliser uniquement les opérations cryptographiques (signature, chiffrement et calcul d'empreinte)
– nous exécutons plusieurs fois sur une carte à puce insérée dans un lecteur relié à un ordinateur les opérations cryptographiques (effectuées au sein de l'application). Le temps d'exécution est à chaque fois relevé. L'exécution de ces opérations a pour objectif d'avoir des données concernant les performances d'un véritable *Secure Element*.
– en associant les résultats obtenus lors des deux séries de tests, il est possible d'évaluer

Modes \ ***Cas***	Sans SE		Avec SE	
	Crypto.	Total	Crypto.	Total
Émission	20.1 ms	22.3 ms	107.4 ms	109.6 ms
Réception	34.9 ms	37.5 ms	305.3 ms	308.1 ms

TABLE 4.20 – Évaluation de la performance des opérations cryptographiques.

les performances de l'application (en terme de vitesse d'exécution) dans le cas de l'intégration d'un véritable *Secure Element*.

Il est à noter que les paramètres pour les tests effectués sont les suivants : carte à puce JCOP 30 smart card et clés de 1024 bits. Les résultats obtenus (temps moyen) pour les différentes mesures effectuées sont présentées dans le tableau 4.20. Le surcoût lié à l'intégration d'un *Secure Element* semble important (comparé au fonctionnement du prototype implémenté). Toutefois, ce surcoût reste raisonnable dans notre contexte car il reste inférieur à 500 ms qui est la limite au-dessus de laquelle, selon certaines expérimentations [web12], l'expérience utilisateur ne serait pas adéquate.

Conclusion

L'objectif des travaux présentés dans ce document était de proposer un modèle valide pour une plate-forme multi-niveaux. Cette plate-forme devait permettre à un ensemble de terminaux mobiles de communiquer entre eux de façon sécurisée en utilisant la technologie sans fil la plus adaptée en fonction du contexte et suivant les contraintes définies par le système (minimisation des coûts des échanges en termes financiers ou de consommation en énergie).
Nous avons introduit la notion de service mobile et ses développements actuels avant de présenter le projet européen Smart Urban Spaces (SUS) qui a constitué le cadre dans lequel nos recherches ont été effectuées. Le projet SUS a permis de proposer et de déployer des services mobiles innovants, basés sur des nouvelles technologies telle que le NFC, à destination des citoyens de certaines villes européennes. Nous avons ensuite décrit les MANets (Mobile Ad hoc Networks), qui constituent l'environnement cible de notre étude, avant de proposer une modélisation du problème posé par le développement de la plate-forme multi-niveaux. Nous avons également proposé des solutions pour les opérations de publication de profil, de spécification d'un ensemble de cibles, de choix de la technologie la plus adaptée pour communiquer, d'échange d'informations privées, de sécurisation des communications et de contrôle de l'anonymat à réaliser au sein du système multi-niveaux à déployer. Nous avons enfin implémenté un prototype d'application mobile suivant l'architecture proposée et nous avons analysé son fonctionnement, à travers des tests, ce qui a permis de mettre en évidence son adéquation à un environnement réaliste.

Nos contributions principales sont les suivantes :

(i) Apports au projet Smart Urban Spaces
Nous avons pu participer à la spécification, au développement et au déploiement d'un ensemble de services mobiles utilisant la technologie NFC. Ces déploiements ont concerné, entre autres, les applications *Small Event Ticketing* et *Museum Quest*. Le projet SUS s'est vu attribué le prix *ITEA Award of Excellence, Exploitation Category*. Ce type de prix récompense les projets aux réalisations particulièrement remarquables dans le cadre du programme ITEA. De plus, l'expérience réussie dans le déploiement des services mobiles développés nous a conduit à la création de la start-up NFC-Interactive (www.nfc-interactive.fr) qui est une structure proposant des services numériques liés à la technologie NFC et aux applications mobiles associées.

(ii) Proposition d'un modèle valide pour la plate-forme multi-niveaux
Nous avons défini un modèle et une architecture pour la plate-forme multi-niveaux. Ce

modèle propose des solutions pour les opérations de publication de profil, de spécification d'un ensemble de cibles, de choix de la technologie la plus adaptée pour communiquer, d'échange d'informations privées, de sécurisation des communications et de contrôle de l'anonymat qui nous apparaissent indispensables dans le contexte visé. Nous avons montré que lors d'une publication de profil, les informations transmises sont toujours publiées le plus largement possible dans le voisinage considéré (en mode direct ou via un relais). Nous avons également montré qu'une méthode de comparaison entre les besoins qu'un nœud exprime, dans la spécification de cible, et les caractéristiques des profils disponibles peut être mise en œuvre.

(iii) Implémentation d'un prototype adapté à un environnement réaliste
Nous avons développé un prototype, sous forme d'application mobile pour le système d'exploitation Android. Ce prototype est basé sur les spécifications de l'architecture de la plate-forme multi-niveaux. Le fonctionnement de cette application mobile a été analysé afin de montrer son adaptation à un environnement réaliste. Nous avons notamment pu déterminer par expérimentation que l'opération de publication de profil se déroulait de façon satisfaisante car dans 90% des cas, un profil publié était rendu accessible aux nœuds ciblés. Nous avons également pu déterminer que le surcoût de consommation en énergie induit par l'utilisation de l'application était raisonnable en comparaison d'autres applications mobiles de référence comme, par exemple, le navigateur intégré de la plate-forme Android.

Les perspectives liées à ces travaux nous conduisent à envisager l'intégration du prototype développé à l'application *Museum Quest* afin d'analyser le fonctionnement du système de communication multi-niveaux sur une gamme plus étendue de scénarios d'utilisation. Ces tests complémentaires nous permettraient d'adapter, le cas échéant, l'architecture de la plate-forme multi-niveaux aux situations que nous n'aurions pas prises en compte dans nos travaux actuels. Il nous apparaît également pertinent d'intégrer l'utilisation effective d'un *Secure Element* (en développant les éléments d'interfaçage nécessaires avec les APIs Android) afin d'accroître le niveau de sécurité de l'ensemble du système.

Annexes

Annexe A

Contributions

En plus des solutions que nous proposons pour la plate-forme multi-niveaux qui est au cœur des chapitres 3 et 4, nous présentons dans cette partie un résumé des contributions effectuées dans le cadre de cette thèse.

A.1 Plate-forme multi-niveaux

Je rappelle que l'objectif principal de nos travaux était de proposer un système permettant à un ensemble de nœuds mobiles de communiquer de façon sécurisée en mode *peer-to-peer* (sans procédure de routage et avec une approche opportuniste) en choisissant la technologie sans fil la plus adaptée suivant des critères dépendant du contexte (coût énergétique, coût financier et préférences des entités impliquées). J'ai donc mis en œuvre un ensemble de solutions comprenant les contributions décrites ci-dessous :

- une modélisation des éléments à prendre à compte dans le fonctionnement de la plate-forme (définition des notions de nœud, d'abonnement, de passerelle, de groupe, etc.) a été réalisée ;
- la définition des opérations principales à considérer dans le développement de la plate-forme a été réalisée et les tâches à effectuer ont été décrites. Il s'agit notamment de la publication de profils, de la spécification d'un ensemble de cibles, du choix de technologie adaptée, de l'échange de profils en cas de rencontre physique entre nœuds, de la sécurisation des communication et du contrôle de l'anonymat ;
- la définition des fonctions de coûts comprenant les paramètres utiles aux calculs nécessaires, suivant la méthode des moindres carrés, pour le choix de technologie adaptée pour communiquer (entre deux nœuds) a été effectuée ;
- une validation des opérations de publication de profils (en mode direct ou via un relais suivant le contexte) a été effectué afin de prouver que les informations transmises sont toujours publiées le plus largement possible dans le voisinage considéré ;
- une méthode valide de comparaison entre les besoins exprimés par un nœud et les profils disponibles (pour procéder à la spécification d'un ensemble de cibles) a été proposée et mise en œuvre ;
- le développement d'une application mobile basée sur les spécifications de la plate-forme multi-niveaux et son évaluation dans un environnement réaliste afin de montrer que les opérations de publication de profils se déroulent de façon satisfaisante tout

en gardant un niveau raisonnable de consommation en énergie ont été réalisés.

A.2 Apports au projet Smart Urban Spaces

J'ai contribué au projet SUS à travers la spécification d'un cadre d'évaluation de l'interopérabilité pour les services mobiles sans contact (au sein des *smart cities*), le développement de briques logicielles et le déploiement d'applications mobiles utilisant la technologie NFC.
Concernant les aspects liés à l'interopérabilité, j'ai notamment contribué à déterminer les dimensions à prendre en compte (en considérant la matrice d'interopérabilité définie) et nous avons réalisé les premières versions des formulaires d'évaluation qui ont été testés sur certains services mobiles déployés. Ce cadre fait l'objet d'un article en cours de soumission en collaboration avec des collègues finlandais partenaires du projet SUS.
Les briques logicielles développées concernent les applications *Profile Providing* et *Collecting Documents*. Pour l'application *Profile Providing*, j'ai implémenté le module qui permet non seulement au navigateur Internet (Firefox dans notre cas) de recevoir des informations fournies par un téléphone mobile à travers un lecteur NFC mais aussi d'utiliser les données reçues pour remplir un formulaire de page web. Pour le *Collecting Documents*, j'ai développé la partie Serveur sur laquelle se trouve les documents à télécharger et le premier prototype de l'application mobile qui se connecte au serveur (pour récupérer les documents souhaités).
Au sujet des applications mobiles utilisant la technologie NFC, j'ai développé le premier prototype de l'application *Museum Quest* qui a servi de base à la version déployée au musée de Normandie. De plus, j'ai développé la partie Validateur et la partie Serveur de l'application *Small Event Ticketing*. J'ai également réalisé les tests concernant la vitesse de validation et l'interface utilisateur du système de billettique mobile pour petits événements.

A.3 Création de la start-up NFC-Interactive

Les déploiements que nous avons effectués durant le projet SUS, en particulier concernant les applications *Small Event Ticketing* et *Museum Quest*, nous ont conduit (Serge Chaumette, Damien Dubernet et Jonathan Ouoba) à la création de la start-up NFC-Interactive (www.nfc-interactive.fr). Cette structure propose des applications mobiles de visites de villes et de musées ainsi que des systèmes de billettique mobile qui fonctionnent en mode *offline*. A ce titre, j'ai conçu les différents modules logiciels (issus des applications mentionnées plus haut) à rendre génériques afin de proposer des applications adaptées aux besoins spécifiques des clients et j'ai également développé les premières applications pilotes de NFC-Interactive (améliorations des applications existantes) déployées sous forme de prototypes (par exemple pour la ville de Talence lors de la nuit des chercheurs).
J'ai également contribué à relever des problématiques liées à l'identification des personnes présentant des tickets à l'entrée d'événements (dans les systèmes de billettique mobile). Il s'agit notamment d'assurer que la personne qui présente le ticket (sur un téléphone mobile ou simplement un tag NFC) à valider est bien celle qui l'a acheté sans avoir besoin de recourir aux habituels contrôles de pièces d'identité. Nous souhaitons poursuivre les recherches dans ce domaine afin de proposer des applications mobiles plus sécurisées.

A.4 Résumé des principales publications

En plus des aspects présentés dans les sections précédentes, j'ai participé à des travaux qui ont fait l'objet de publications. Ces contributions concernent des articles (en tant qu'auteur principal), un brevet et des dépôts logiciels.

A.4.1 Articles

Architecture and comparison of two different user-centric NFC-enabled event ticketing approaches [21]. Cet article compare les deux approches (*offline* et *online*), en prenant en compte les aspects liés à la sécurité et à la vitesse de validation, qui peuvent être utilisées pour proposer des systèmes de billettique pour événements basés sur la technologie NFC.

Architecture and Evaluation of a User-Centric NFC-Enabled Ticketing System for Small Events [22]. Cet article présente un système de billettique mobile pour petits événements compatible avec la technologie NFC et évalue ses performances en terme de vitesse de validation et d'interface utilisateur. Ce système a servi de base au développement du système *Small Event Ticketing*.

Multilevel and Secure Services in a Fleet of Mobile Phones : The Multilevel Secured Messaging Application (MuSMA) [23]. Cet article présente les premiers éléments théoriques et une première implémentation d'application pour la plate-forme multi-niveaux que nous avons proposée dans ces travaux de thèse.

Leveraging the Cultural Model for Opportunistic Networking in sub-Saharan Africa [11]. Cet article propose un modèle pour transmettre des messages (via des équipements mobiles) entre zones géographiques isolées en utilisant une approche opportuniste à travers les déplacements de certaines catégories de population en Afrique sub-saharienne.

Many Faces of Mobile Contactless Ticketing [74]. Cet article présente (et compare) les différents modèles identifiés et utilisés dans le cadre du projet Smart Urban Spaces qui permettent de proposer des systèmes de billettique mobile en utilisant la technologie NFC.

A.4.2 Brevet

Programme d'ordinateur, ensemble d'un lecteur d'étiquette sans contact et d'une carte, terminal et système pour entrer facilement en relation avec un correspondant ou un service (System for NFC-enabled smart poster indirection) [20]. Ce brevet présente un système d'indirection permettant d'interagir de façon sécurisée avec un *smart poster* équipé de tags NFC pour lancer des services mobiles, suivant les préférences de l'utilisateur, en utilisant un téléphone mobile et en préservant la confidentialité des données personnelles (elles restent stockées dans le téléphone).

A.4.3 Dépôts logiciels

ZeKmop (déposé en 2011). Cette application mobile permet de déclencher de façon sécurisée un ensemble d'opérations (appels, envois de SMS, etc.) avec un téléphone mobile

en interagissant avec un *smart poster* équipé de tags NFC suivant les principes du brevet présenté ci-dessus.

Small Event Ticketing (en cours de dépôt). Cette application mobile propose un système de gestion de billettique mobile pour petits événements qui permet aux utilisateurs de télécharger des tickets électroniques sur leurs téléphones, la validation à l'entrée des spectacles étant réalisée à l'aide d'un autre téléphone via le mode *peer-to-peer* de la technologie NFC.

Visit Helsinki (en cours de dépôt). Cette application mobile embarque une carte d'une partie de la ville (Helsinki) sur laquelle sont indiqués des monuments à faire découvrir aux touristes ; les utilisateurs de l'application se rendent aux endroits indiqués sur la carte où ils trouvent des tags NFC avec lesquels interagir pour déclencher l'affichage d'éléments multimédia correspondant au lieu visité.

Museum Quest (en cours de dépôt). Cette application mobile propose un quiz dédié à la visite de musée ; les utilisateurs peuvent obtenir de l'aide sur les questions posées (relatives aux œvres exposées) en interagissant avec des tags NFC répartis dans le musée qui déclenchent l'affichage d'éléments multimédia.

Bibliographie

[1] N. Aboudagga, M. T. Refaei, M. Eltoweissy, L. A. Dasilva et J.-J. Quisquater : Authentication protocols for ad hoc networks : taxonomy and research issues. *In Q2SWinet 05 : Proceedings of the 1st ACM international workshop on Quality of service and security in wireless and mobile networks*, pages 96–104. ACM Press, 2005.

[2] A. Al Hanbali, M. Ibrahim, V. Simon, E. Varga et I. Carreras : A survey of message diffusion protocols in mobile ad hoc networks. *In Proceedings of the 3rd International Conference on Performance Evaluation Methodologies and Tools*, ValueTools '08, pages 82 :1–82 :16, Brussels, Belgium, 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[3] E. Atallah, P.-F. Bonnefoi, C. Burgod et D. Sauveron : Mobile Ad Hoc Network with Embedded Secure System. *In Ambient Intelligence Developments Conference*, Nice - Sophia-Antipolis, France,
septembre 2006.

[4] E. Atallah et S. Chaumette : A smart card based distributed identity management infrastructure for mobile ad hoc networks. *In WISTP*, pages 1–13, 2007.

[5] H. Bakht : Survey of routing protocols for mobile ad-hoc network. *International Journal of Information and Communication Technology Research*, 1(6), October 2011.

[6] A. Bangor, P. Kortum et J. Miller : Determining What Individual SUS Scores Mean : Adding an Adjective Rating Scale. *Journal of Usability Studies*, 4:114–123, 2009.

[7] F. Bari et V. C. M. Leung : Automated network selection in a heterogeneous wireless network environment. *Ieee Network*, pages 34–40, 2007.

[8] N. Beijar : Zone routing protocol (ZRP), 2002.

[9] B. Bellur et R. G. Ogier : A Reliable, Efficient Topology Broadcast Protocol for Dynamic Networks. *In 18th IEEE Conference on Computer Communications (IEEE INFOCOM 1999)*, volume 1, pages 178–186, New York, NY, March 1999.

[10] A. Benchi, F. Guidec et P. Launay : A Message Service for Opportunistic Computing in Disconnected MANETs. *In Proceedings of DAIS'12*, pages 118–131, Stockholm, Suède,
juin 2012.

[11] T. F. Bissyandé et J. Ouoba : Leveraging the Cultural Model for Opportunistic Networking in sub-Saharan Africa. *In Proceedings of the Fourth International IEEE EAI Conference on e-Infrastructure and e-Services for Developing Countries*, AFRICOMM 2012, pages 1–10, Yaoundé, Cameroun, novembre 2012.

[12] T. F. Bissyandé, L. Réveillère, J.-R. Falleri et Y.-D. Bromberg : Typhoon : a middleware for epidemic propagation of software updates. *In Proceedings of the Third International Workshop on Middleware for Pervasive Mobile and Embedded Computing*, M-MPAC '11, pages 1 :1–1 :7, New York, NY, USA, 2011. ACM.

[13] A. Björck : *Numerical methods for least squares problems*. SIAM, 1996.

[14] J. Brooke : SUS : A quick and dirty usability scale. *In Usability evaluation in industry*. Taylor and Francis Ltd, London, England, 1996.

[15] D. Bubley : Carrier WiFi Opportunities - Enabling offload, onload and roaming. Rapport technique, Disruptive Analysis Ltd, 2011.

[16] M. Caporuscio, D. Charlet, V. Issarny et A. Navarra : Energetic performance of service-oriented multi-radio networks : issues and perspectives. *In WOSP*, pages 42–45, 2007.

[17] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall et H. Weiss : Delay-Tolerant Networking Architecture. RFC 4838 (Informational), avril 2007.

[18] E. Chan, W. Li et D. Chen : Energy saving strategies for cooperative cache replacement in mobile ad hoc networks. *Pervasive Mob. Comput.*, 5(1):77–92, février 2009.

[19] D. Charlet, V. Issarny et R. Chibout : Energy-efficient middleware-layer multi-radio networking : An assessment in the area of service discovery. *Computer Networks*, 52(1):4–24, 2008.

[20] S. Chaumette, D. Dubernet et J. Ouoba : Programme d'ordinateur, ensemble d'un lecteur d'étiquette sans contact et d'une carte, terminal et système pour entrer facilement en relation avec un correspondant ou un service (System for NFC-enabled smart poster indirection). French Patent No. FR2961653-FR2961653-H04M1/247, 2011.

[21] S. Chaumette, D. Dubernet, J. Ouoba, E. Siira et T. Tuikka : Architecture and comparison of two different user-centric NFC-enabled event ticketing approaches. *In Proceedings of the 11th international conference and 4th international conference on Smart spaces and next generation wired/wireless networking*, NEW2AN'11/ruSMART'11, pages 165–177, Berlin, Heidelberg, 2011. Springer-Verlag.

[22] S. Chaumette, D. Dubernet, J. Ouoba, E. Siira et T. Tuikka : Architecture and Evaluation of a User-Centric NFC-Enabled Ticketing System for Small Events. *In MobiCASE*, pages 137–151, 2011.

[23] S. Chaumette et J. Ouoba : Multilevel and Secure Services in a Fleet of Mobile Phones : The Multilevel Secured Messaging Application (MuSMA). *In Proceedings of the Fourth International Conference on Mobile Computing, Applications, and Services*, MobiCASE 2012, pages 169–185. Springer, octobre 2012.

[24] X. Chen, M. Faloutsos et S. Krishnamurthy : Distance adaptive (dad) broadcasting for ad hoc networks. *In MILCOM 2002. Proceedings*, volume 2, pages 879 – 883 vol.2, oct. 2002.

[25] T. Clausen et P. Jacquet : Optimized link state routing protocol (OLSR). RFC 2501, 2003.

[26] S. Corson et J. Macker : Mobile Ad hoc Networking (MANET) : Routing Protocol Performance Issues and Evaluation Considerations. RFC 2501 (Informational), 1999.

[27] E. Dahlman, S. Parkvall, J. Skold et P. Beming : *3G Evolution, Second Edition : HSPA and LTE for Mobile Broadband*. Academic Press, 2008.

[28] B. Dodson, I. Vo, T. Purtell, A. Cannon et M. Lam : Musubi : disintermediated interactive social feeds for mobile devices. *In Proceedings of the 21st international conference on World Wide Web*, WWW '12, pages 211–220, New York, NY, USA, 2012. ACM.

[29] Eureka : Clusters annual report to hlg. Rapport technique, Eureka, 2012.

[30] L. M. Feeney : An energy consumption model for performance analysis of routing protocols for mobile ad hoc networks. *Mob. Netw. Appl.*, 6(3):239–249, 2001.

[31] L. M. Feeney et M. Nilsson : Investigating the energy consumption of a wireless network interface in an ad hoc networking environment. *In INFOCOM*, pages 1548–1557, 2001.

[32] S. Föll, K. Herrmann et K. Rothermel : Energy-efficient update protocols for mobile user context. *In AINA*, pages 120–127, 2012.

[33] N. Forum : Simple NDEF exchange protocol - SNEP 1.0. Rapport technique, NFC Forum, 2011.

[34] L. Francis, G. P. Hancke, K. Mayes et K. Markantonakis : Practical NFC Peer-to-Peer Relay Attack Using Mobile Phones. *In RFIDSec*, pages 35–49, 2010.

[35] F. Gil-Castineira, E. Costa-Montenegro, F. J. Gonzalez-Castano, C. Lopez-Bravo, T. Ojala et R. Bose : Experiences inside the Ubiquitous Oulu Smart City. *Computer*, 44:48–55, 2011.

[36] B. S. I. Group : Specification of the Bluetooth System. Rapport technique, SIG, 2010.

[37] GSMA, A. Kearney et W. Intelligence : European mobile industry observatory. Rapport technique, GSM Association, 2011.

[38] S. Guo et O. W. W. Yang : Energy-aware multicasting in wireless ad hoc networks : A survey and discussion. *Comput. Commun.*, 30(9):2129–2148, juin 2007.

[39] Z. J. Haas et M. R. Pearlman : Providing ad-hoc connectivity with reconfigurable wireless networks. *In SIGCOMM*, pages 166–177. Addison Wesley Longman, 1998.

[40] Z. J. Haas, M. R. Pearlman et P. Samar : The Zone Routing Protocol (ZRP) for Ad Hoc Networks. Rapport technique, IETF MANET Working Group, 2002.

[41] Z. J. Haas, M. R. Pearlman et P. Samar : The interzone routing protocol (IERP) for ad hoc networks, July 2002.

[42] Z. J. Haas, M. R. Pearlman et P. Samar : The intrazone routing protocol (IARP) for ad hoc networks, July 2002.

[43] J. Haillot et F. Guidec : A protocol for content-based communication in disconnected mobile ad hoc networks. *Mob. Inf. Syst.*, pages 123–154, 2010.

[44] E. Haselsteiner et K. Breitfuss : Security in near field communications (NFC). *In Proceedings of Workshop on RFID Security RFIDSec*, 2006.

[45] T.-Y. Huang, K.-K. Yap, B. Dodson, M. S. Lam et N. McKeown : Phonenet : a phone-to-phone network for group communication within an administrative domain. *In Proceedings of the second ACM SIGCOMM workshop on Networking, systems, and applications on mobile handhelds*, MobiHeld '10, pages 27–32, New York, NY, USA, 2010. ACM.

[46] IEEE 802.15.1-2002 IEEE Standard for information technology - Telecommunication and information exchange between systems - LAN/MAN - Part 15.1 : Wireless Medium Access Control (MAC) and Physical Layer (PHY) specications for Wireless Personal Area Networks(WPANs), 2002.

[47] Iso/iec : *Norme ISO/CEI 7816-4/A1 : 1997 Amendement 1 à la norme ISO/CEI 7816-4 de septembre 1995*. AFNOR, 1997.

[48] ISO/IEC : *ISO/IEC 7816-1 :1998, Identification cards - Integrated circuit(s) cards with contacts - Part 1 : Physical characteristics*. Multiple. Distributed through American National Standards Institute (ANSI), août 2007.

[49] P. Jacquet, P. Mühlethaler, T. Clausen, A. Laouiti, A. Qayyum et L. Viennot : Optimized link state routing protocol for ad hoc networks. *In Multi Topic Conference, 2001. IEEE INMIC 2001*, pages 62–68, 2001.

[50] J. Jansen : Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC. RFC 5702 (Proposed Standard), octobre 2009. Updated by RFC 6944.

[51] D. Johnson, Y. Hu et D. Maltz : The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. RFC 4728 (Experimental), 2007.

[52] D. B. Johnson et D. A. Maltz : Dynamic source routing in ad hoc wireless networks. *In MOBILE COMPUTING*, pages 153–181. Kluwer Academic Publishers, 1996.

[53] M. Just : Challenge-response protocol. *In* H. C. van Tilborg et S. Jajodia, éditeurs : *Encyclopedia of Cryptography and Security*, pages 199–199. Springer US, 2011.

[54] S. Kapadia, B. Krishnamachari et L. Zhang : Data delivery in delay tolerant networks : A survey. *In* X. Wang, éditeur : *Mobile Ad-Hoc Networks : Protocol Design*. InTech, 2011.

[55] H. Lim et C. Kim : Multicast tree construction and flooding in wireless ad hoc networks. *In Proceedings of the 3rd ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems*, MSWIM '00, pages 61–68, New York, NY, USA, 2000. ACM.

[56] A. Lindgren, A. Doria et O. Schelén : Probabilistic routing in intermittently connected networks. *SIGMOBILE Mob. Comput. Commun. Rev.*, pages 19–20, 2003.

[57] Y. Ma et A. Jamalipour : A cooperative cache-based content delivery framework for intermittently connected mobile ad hoc networks. *Trans. Wireless. Comm.*, pages 366–373, 2010.

[58] G. Madlmayr, J. Langer, C. Kantner et J. Scharinger : NFC Devices : Security and Privacy. *In Proceedings of ARES*, 2008.

[59] G. Madlmayr, J. Langer et J. Scharinger : Managing an NFC Ecosystem. *In Mobile Business 2008*, Barcelona, Spain, 2008.

[60] Y. Mahéo, N. Le Sommer, P. Launay, F. Guidec et M. Dragone : Beyond Opportunistic Networking Protocols : a Disruption-Tolerant Application Suite for Disconnected MANETs. *In Proceedings of the 4th Extreme Conference on Communication (ExtremeCom'12)*, pages 1–6, Zurich, Suisse, mars 2012. ACM.

[61] S. Mahfoudh et P. Minet : An energy efficient routing based on olsr in wireless ad hoc and sensor networks. *In Proceedings of the 22nd International Conference on Advanced Information Networking and Applications - Workshops*, AINAW '08, pages 1253–1259, Washington, DC, USA, 2008. IEEE Computer Society.

[62] D. Metzler, Y. Bernstein, W. B. Croft, A. Moffat et J. Zobel : Similarity measures for tracking information flow. *In Proceedings of the 14th ACM international conference on Information and knowledge management*, CIKM '05, pages 517–524, New York, NY, USA, 2005. ACM.

[63] D. Metzler, S. Dumais et C. Meek : Similarity measures for short segments of text. *In Proceedings of the 29th European conference on IR research*, ECIR'07, pages 16–27, Berlin, Heidelberg, 2007. Springer-Verlag.

[64] B. J. Mohler, W. B. Thompson, S. H. Creem-Regehr, H. L. J. Pick et W. H. Warren : Visual flow influences gait transition speed and preferred walking speed. *Experimental Brain Research*, pages 1432–1106, 2007.

[65] M. Musolesi, M. Piraccini, K. Fodor, A. Corradi et A. T. Campbell : Supporting energy-efficient uploading strategies for continuous sensing applications on mobile phones. *In Proceedings of the 8th international conference on Pervasive Computing*, Pervasive'10, pages 355–372, Berlin, Heidelberg, 2010. Springer-Verlag.

[66] P. Nand et S. Sharma : Analytical study of broadcast in mobile adhoc network. *International Journal of Computer Applications*, 19(8):7–12, April 2011. Published by Foundation of Computer Science.

[67] A. Neumann, C. Aichele, M. Lindner et S. Wunderlich : Better approach to mobile ad hoc networking (B.A.T.M.A.N.). Rapport technique, IETF Network Working Group, 2008.

[68] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen et J.-P. Sheu : The broadcast storm problem in a mobile ad hoc network. *In Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, MobiCom '99, pages 151–162, New York, NY, USA, 1999. ACM.

[69] E. Nordstrom, P. Gunningberg, C. Rohner et O. Wibling : A Comprehensive Comparison of MANET Routing Protocols in Simulation, Emulation and the Real World, 2006.

[70] K. Obraczka, K. Viswanath et G. Tsudik : Flooding for reliable multicast in multi-hop ad hoc networks. *Wirel. Netw.*, 7(6):627–634, novembre 2001.

[71] R. Ogier, F. Templin et M. Lewis : Topology Dissemination Based on Reverse-Path Forwarding (TBRPF). RFC 3684 (Experimental), 2004.

[72] T. Ojala et V. Kostakos : Ubi challenge : research coopetition on real-world urban computing. *In Proceedings of the 10th International Conference on Mobile and Ubiquitous Multimedia*, MUM '11, pages 205–208, New York, NY, USA, 2011. ACM.

[73] T. Ojala, J. Orajärvi, K. Puhakka, I. Heikkinen et J. Heikka : panoulu : triple helix driven municipal wireless network providing open and free internet access. *In Proceedings of the 5th International Conference on Communities and Technologies*, C & T '11, pages 118–127, New York, NY, USA, 2011. ACM.

[74] J. Ouoba et E. Siira : Many Faces of Mobile Contactless Ticketing. *In Proceedings of the Second International Conference on Smart Systems, Devices and Technologies*, SMART 2013, pages 93–98,
juin 2013.

[75] M. Owens : *The Definitive Guide to SQLite (Definitive Guide)*. Apress, Berkely, CA, USA, 2006.

[76] K. Papineni : Why inverse document frequency ? *In Proceedings of the second meeting of the North American Chapter of the Association for Computational Linguistics on Language technologies*, NAACL '01, pages 1–8, Stroudsburg, PA, USA, 2001. Association for Computational Linguistics.

[77] V. Paruchuri, A. Durresi et R. Jain : Optimized flooding protocol for ad hoc networks. *CoRR*, cs.NI/0311013, 2003.

[78] A. Pathak, Y. C. Hu et M. Zhang : Where is the energy spent inside my app ? : fine grained energy accounting on smartphones with eprof. *In Proceedings of the 7th ACM european conference on Computer Systems*, pages 29–42, New York, NY, USA, 2012. ACM.

[79] M. R. Pearlman et Z. J. Haas : Determining the optimal configuration for the zone routing protocol. *IEEE J.Sel. A. Commun.*, 17(8):1395–1414,
septembre 2006.

[80] G. Pei, M. Gerla et T.-W. Chen : Fisheye state routing in mobile ad hoc networks. *In In ICDCS Workshop on Wireless Networks and Mobile Computing*, pages 71–78, 2000.

[81] L. Pelusi, A. Passarella et M. Conti : Opportunistic networking : data forwarding in disconnected mobile ad hoc networks. *Communications Magazine, IEEE*, 44(11):134 –141, november 2006.

[82] C. Perkins, E. Belding-Royer et S. Das : Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561 (Experimental), 2003.

[83] C. E. Perkins : Ad-hoc on-demand distance vector routing. *In In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pages 90–100, 1999.

[84] M. Peyravian, A. Roginsky et A. D. Kshemkalyani : On probabilities of hash value matches. *Computers and Security*, 17(2):171–176, 1998.

[85] A.-K. Pietiläinen, E. Oliver, J. LeBrun, G. Varghese et C. Diot : Mobiclique : middleware for mobile social networking. *In Proceedings of the 2nd ACM workshop on Online social networks*, WOSN '09, pages 49–54, New York, NY, USA, 2009. ACM.

[86] A. Qayyum, L. Viennot et A. Laouiti : Multipoint relaying : An efficient technique for flooding in mobile wireless networks. Rapport technique RR-3898, INRIA, 2000.

[87] I. Research et Technology : Technical datasheet. Rapport technique, Innovision Group, 2007.

[88] M. Reveilhac et M. Pasquet : Promising secure element alternatives for nfc technology. *In 1st International Workshop on NFC*, Hagenberg, Austria, 2009.

[89] S. Robertson : Understanding inverse document frequency : On theoretical arguments for IDF. *Journal of Documentation*, 60:503–520, 2004.

[90] G. Rudolf, C. Fertner, H. Kramar, R. Kalasek, N. Pichler-Milanovic et E. Meijers : Smart cities – ranking of european medium-sized cities. Rapport technique, Vienna Centre of Regional Science, 2007.

[91] SANS-Institute : The GSM Standard (An overview of its security). Rapport technique, European Telecommunications Standard Institute (ETSI), 2001.

[92] N. I. Sarkar et W. G. Lol : A study of manet routing protocols : Joint node density, packet length and mobility. *In Proceedings of the The IEEE symposium on Computers and Communications*, ISCC '10, pages 515–520, Washington, DC, USA, 2010. IEEE Computer Society.

[93] Y. Sasaki, L. Wang et K. Aoki : Preimage Attacks on 41-Step SHA-256 and 46-Step SHA-512. *IACR Cryptology ePrint Archive*, page 479, 2009.

[94] B. Schneier : *Cryptographie appliquée*. Vuibert, Paris, France, 2001.

[95] A. Serrador et L. M. Correia : Policies for a cost function for heterogeneous networks performance evaluation. *In Proceedings of the 18th Annual IEEE International Symp. on Personal, Indoor and Mobile Radio Commun*, Athens, Greece, 2007.

[96] S. Sesia, I. Toufik et M. Baker : *LTE, The UMTS Long Term Evolution : From Theory to Practice*. Wiley Publishing, 2009.

[97] W. Shen et Q.-A. Zeng : Cost-function-based network selection strategy in integrated wireless and mobile networks. *In Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops - Volume 02*, pages 314–319, Washington, DC, USA, 2007.

[98] B. SIG : Specification of the Bluetooth System. Specification v4.0, Bluetooth SIG, juin 2010.

[99] K. H. Siitonen et M. S. Frode : Eavesdropping near field communication. *In Proceedings of the 2nd Norwegian Security Conference*, pages 57–68, 2009.

[100] F. S. SMSC : Liberty Equality Mobility - NFC mobile phones to benefit regions. Rapport technique, Forum SMSC, 2009.

[101] T. Spyropoulos, K. Psounis et C. S. Raghavendra : Efficient routing in intermittently connected mobile networks : the multiple-copy case. *IEEE/ACM Trans. Netw.*, pages 77–90, 2008.

[102] W. Stallings : *Cryptography and Network Security : Principles and Practice*. Prentice Hall Press, Upper Saddle River, NJ, USA, 5th édition, 2010.

[103] C.-K. Toh : A novel distributed routing protocol to support ad-hoc mobile computing. *In Conference Proceedings of the 1996 IEEE Fifteenth Annual International Phoenix Conference on Computers and Communications*, pages 480–486, 1996.

[104] R. Trestian, O. Ormond et G.-M. Muntean : Power-friendly access network selection strategy for heterogeneous wireless multimedia networks. *2010 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting BMSB*, pages 1–5, 2010.

[105] E. Triantaphyllou : *Multi-Criteria Decision Making Methods : A comparative Study (Applied Optimization, Volume 44) (Applied Optimization)*. Springer, 1st édition, 2000.

[106] A. Vahdat et D. Becker : Epidemic Routing for Partially-Connected Ad Hoc Networks. Rapport technique CS-200006, Department of Computer Science, Duke University, 2000.

[107] C.-Y. Wang et H.-Y. Wei : IEEE 802.11n MAC Enhancement and Performance Evaluation. *Mob. Netw. Appl.*, 14(6):760–771, décembre 2009.

[108] H. J. Wang : Policy-enabled handoffs across heterogeneous wireless networks. *In Mobile Computing Systems and Applications, Proceedings. WMCSA*, pages 51–60, 1999.

[109] P. Wegner : Interoperability. *ACM Comput. Surv.*, 28(1):285–287, mars 1996.

[110] B. Williams et T. Camp : Comparison of broadcasting techniques for mobile ad hoc networks. *In Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, MobiHoc '02, pages 194–205, New York, NY, USA, 2002. ACM.

[111] K. Woo, C. Yu, D. Lee, H. Y. Youn et B. Lee : Non-Blocking, Localized Routing Algorithm for Balanced Energy Consumption in Mobile Ad Hoc Networks. *In Proceedings of the Ninth International Symposium in Modeling, Analysis and Simulation of Computer and Telecommunication Systems*, MASCOTS '01, pages 117–124, Washington, DC, USA, 2001. IEEE Computer Society.

[112] S. Xu et S. Čapkun : Distributed and secure bootstrapping of mobile ad hoc networks : Framework and constructions. *ACM Trans. Inf. Syst. Secur.*, 12(1):2–37, octobre 2008.

[113] W. Zhang : Handover decision using fuzzy MADM in heterogeneous networks. *2004 IEEE Wireless Communications and Networking Conference IEEE Cat No04TH8733*, pages 653–658, 2004.

[114] X. Zhang, T. Kunz, L. Li et O. Yang : An energy-efficient broadcast protocol in manets : Design and evaluation. *In Proceedings of the 2010 8th Annual Communication Networks and Services Research Conference*, CNSR '10, pages 199–206, Washington, DC, USA, 2010. IEEE Computer Society.

Webographie

[web1] AFSCM Association Française du Sans Contact Mobile.
http://www.afscm.org/,
juillet 2012.

[web2] Android.
http://www.android.com/about/,
juillet 2012.

[web3] Android APIs.
http://developer.android.com/guide/components/index.html,
juin 2013.

[web4] Caen la mer choisie comme Territoire leader du Mobile Sans Contact.
http://www.caenlamer.fr/detail-a-la-une.asp?card=13637,
juillet 2012.

[web5] Caen Territoire leader du Mobile Sans Contact.
http://www.caen.fr/Economie/nfc/applications.asp,
juillet 2012.

[web6] Center for Internet Excellence.
http://www.cie.fi/home.html,
juillet 2012.

[web7] City of Oulu.
http://oulu.ouka.fi/english/,
juillet 2012.

[web8] Cityzi.
http://www.cityzi.fr/,
juillet 2012.

[web9] Cityzi.
http://www.afscm.org/en/companies/mobile-contactless-in-nice/
index.php?rubrique=3&srub=12,
juillet 2012.

[web10] Eclipse SDK.
http://www.eclipse.org/,
juin 2013.

[web11] E-Health in Valencia.
http://www.m-inclusion.eu/news/public-e-health-valencia,
juillet 2012.

[web12] Transport for London Calls for Faster NFC SIMs.
http://nfctimes.com/news/transport-london-calls-faster-nfc-sims,
juillet 2012.

[web13] Forum des services mobiles sans contact.
www.forum-smsc.org/,
juillet 2012.

[web14] Galaxy Nexus.
http://www.android.com/devices/detail/galaxy-nexus,
juin 2013.

[web15] Galaxy S III specifications.
http://www.samsung.com/us/mobile/cell-phones/SGH-I747MBBATT-specs,
juillet 2012.

[web16] Gemalto Prox-Pu Reader.
http://www.gemalto.com/products/prox_readers/index_PU.html,
juillet 2012.

[web17] ITEA2.
http://www.itea2.org/,
juillet 2012.

[web18] The Java Card Technology.
http://www.oracle.com/technetwork/java/javacard/overview/index.html,
juillet 2012.

[web19] The Java ME and Java Card Technology.
http://www.oracle.com/technetwork/java/javame/index.html,
juillet 2012.

[web20] Mobile Market Share.
http://www.mobilestatistics.com/mobile-devices/,
juin 2013.

[web21] Mobitrans.
http://inndeavalencia.com/icity/urban-innovation/best-practices/national-projects,
juillet 2012.

[web22] Nexus S noir - Open market.
http://www.samsung.com/fr/consumer/mobile-phones/smartphones/galaxy/GT-I9023FSAXEF-spec,
juillet 2012.

[web23] Nexus S.
http://www.android.com/devices/detail/nexus-s,
juillet 2012.

[web24] Nokia 6212 classic Data Sheet.
http://press.nokia.com/wp-content/uploads/mediaplugin/doc/1-nokia_6212_classic_data_sheet.pdf,
juillet 2012.

[web25] OECD glossary of statistical terms - Mobile Services.
`http://stats.oecd.org/glossary/detail.asp?ID=4973`,
juillet 2012.

[web26] Open wireless Internet access.
`http://www.panoulu.net/`,
juillet 2012.

[web27] Pôle de compétitivité Transactions Électroniques Sécurisées.
`http://www.pole-tes.com/`,
juillet 2012.

[web28] Smart City VLC.
`http://www.uv.es/uvweb/college/en/llista-de-noticies/`,
juillet 2012.

[web29] Store Statistics.
`http://www.mobilestatistics.com/mobile-statistics/`,
juillet 2012.

[web30] Smart Urban Spaces.
`http://www.smarturbanspaces.org/`,
septembre 2012.

[web31] Open Ubiquitous Oulu.
`http://www.ubioulu.fi/en/home`,
juillet 2012.

Table des figures

Liste des tableaux