Service-based Networking for M2M Communications

Guillaume Habault

▶ **To cite this version:**

Guillaume Habault. Service-based Networking for M2M Communications. Networking and Internet Architecture [cs.NI]. Télécom Bretagne; Université de Rennes 1, 2015. English. NNT : . tel-01262731

HAL Id: tel-01262731
https://hal.science/tel-01262731

Submitted on 27 Jan 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

THÈSE / Télécom Bretagne
sous le sceau de l'Université européenne de Bretagne

pour obtenir le grade de Docteur de Télécom Bretagne
En accréditation conjointe avec l'Ecole Doctorale Matisse
Mention : Informatique

présentée par
Guillaume Habault

préparée dans le département Réseaux, Sécurité et Multimédia
Laboratoire Irisa

Service-based Networking for Machine-to-Machine (M2M) Communications

Thèse soutenue le 15 janvier 2015
Devant le jury composé de :

Hossam Afifi
Professeur, Télécom SudParis / président

Naoaki Yamanaka
Professeur, Université de Keio – Japon / rapporteur

Farouk Kamoun
Professeur, Sesame - Tunisie / rapporteur

Nicolas Montavont
Maître de conférences, Télécom Bretagne / examinateur

Laurent Toutain
Maître de conférences (HDR), Télécom Bretagne / examinateur

Jean-Marie Bonnin
Professeur, Télécom Bretagne / directeur de thèse

Philippe Bertin
Ingénieur Sénior & Docteur en Informatique, Orange Labs – Cesson Sévigné / invité

N° d'ordre : 2015telb0328

Sous le sceau de l'Université européenne de Bretagne

Télécom Bretagne

En accréditation conjointe avec l'Ecole Doctorale Matisse

Ecole Doctorale – MATISSE

Service-based Networking applied to Machine-to-Machine Communications

---

Thèse de Doctorat

Mention : Informatique

Présentée par **Guillaume Habault**

Département : Réseaux, Sécurité et Multimédia (RSM)

Laboratoire : IRISA

Directeur de thèse : Jean-Marie Bonnin

Soutenue le 15 Janvier 2014

Jury :

M. Naoaki Yamanaka, Professeur, Université de Keio (Rapporteur)
M. Farouk Kamoun, Professeur, SESAME (Rapporteur)
M. Hossam Afifi, Professeur, Télécom SudParis (Examinateur)
M. Nicolas Montavont, Maître de conférences, Télécom Bretagne (Examinateur)
M. Jean-Marie Bonnin, Professeur, Télécom Bretagne (Directeur de thèse)
M. Laurent Toutain, Maître de conférences, Télécom Bretagne (Encadrant de thèse)
M. Philippe Bertin, Ingénieur Sénior & Docteur en Informatique, Orange Labs (Invité)

TELECOM
Bretagne

Dedication

To my parents for their limitless support.

Acknowledgments

This work would not have been possible without the invaluable help of the many people I had the privilege to encounter during this thesis.

First, I would like to thank Orange Labs which provided the financial support to accomplish this thesis. I am also thankful for the encouragement, understanding and valuable discussions of Dr. Philippe Bertin.

I would like to thank my thesis director, Professor Jean-Marie Bonnin and my supervisor, Dr. Laurent Toutain for giving me the possibility to discover academic environment both in research and teaching, for giving me the opportunity to realize this work, as well as for providing help and valuable contributions.

I am especially thankful to Dr. Nicolas Montavont for his help and guidance on the Wi-Fi study chapter, as well as for his valuable advice during the redaction of this thesis dissertation.

I wish to thank Professor Naoaki Yamanaka, Professor Farouk Kamoun and Professor Hossam Afifi for accepting to be part of this Ph.D jury and for their effort in reviewing this dissertation.

I wish also to thank my colleagues from the RSM department at Télécom Bretagne, with whom I have spent the last years working on many projects, preparing lab works, discussing, debating and yet playing.

I owe a lot to my family and friends for their patience, love and unlimited support. Finally, I especially thanks Mary-Claire for her help in proof-reading my manuscript and Camille for her endless starry support.

Abstract

The network ecosystem has tremendously changed in the past years and is becoming more complex as devices, available services and access technologies are continuously evolving. Devices currently at stake in this ecosystem can be divided into two categories: user devices, which usage depend on the user willingness and requirements, and constrained self or remote -operated devices, which usually have resource constraints and which usage happen at regular intervals. As usage is different, needs in terms of delay, bandwidth and coverage are also different. The number of access technologies has then spread to cover these needs and with the generalization of Internet Protocol (IP) over these different technologies, Internet coverage is constantly expanding. All these access technologies offer different characteristics but none of them manage to fulfill all the needs and requirements of this multitude of existing devices. As a result, in most parts of the world there are multiple ways to access a given network.

Devices could benefit from this diversity of access technologies, and associated services, to select their accesses based on their needs and service availability. The purpose of this thesis is to propose a mechanism to inform any device from a Complex Heterogeneous Environment on available services within each access technology. The information retrieve will help these devices in their decision and selection of the most appropriate Access Network (AN). Our Lightweight Service Announcement (LSA) mechanism is simple, re-uses existing network discovery messages and is based on an ontology. Therefore, it allows any device to automatically detect and interpret the service availability of each discovered AN in order to perform a service-based AN selection. Finally, this service announcement mechanism could be associated with other protocols in order to enable user devices with multiple interfaces to always select and connect to the best possible access network at any given time and in any given location. The framework resulting from this association will ensure session survivability for each application.

We studied the impact of the LSA mechanism in a scenario of M2M data retrieval using existing Wi-Fi deployment. This scenario is fully described before presenting its credibility based on M2M traffic characterization and simulations. Afterward, different Wi-Fi environments are characterized using an Android tool which also help us collect empirical data. These data are used to instantiate mathematical models of the studied scenario. Markov chains have been used to model this Wi-Fi M2M scenario and help us evaluate the impact and validity of our proposal depending on different parameters such as the Access Point density, the frequency of service announcement and the success rate of data retrieval. We managed to show that our proposal could enhance the network environment in numerous ways, but it would require additional work.

Résumé

L'environnement réseau dans lequel évoluent les utilisateurs et leurs appareils a beaucoup changé depuis quelques années. En effet, celui-ci se complexifie à mesure que les appareils, les services et les technologies d'accès évoluent. Il existe deux types d'appareils dans cet environnement : les appareils qui dépendent de la volonté et des besoins de leurs utilisateurs et les objets connectés qui ont des ressources limitées et qui émettent périodiquement des données. Comme les utilisations de ces appareils sont différentes, leurs besoins en terme de bande passante et de délais le sont aussi. Cependant, aucune technologie d'accès ne pouvant répondre à l'ensemble de ces besoins ainsi qu'à la multitude d'appareils en jeu, le nombre de technologies d'accès s'est vu décuplé. Par ailleurs, avec la généralisation du protocole IP au sein de ces différentes technologies, la couverture de l'Internet s'étend continuellement. Par conséquent, dans la majorité du monde, il y a plusieurs manières d'accéder à un réseau.

Les utilisateurs pourraient profiter de cette abondance de réseaux d'accès, et des services associés, en sélectionnant le réseau d'accès le plus adapté à ses besoins. L'objectif de cette thèse est de proposer un mécanisme qui permettrait d'annoncer les différents services disponibles sur chaque technologie d'accès et vers tout type d'appareil. Notre mécanisme, Lightweight Service Announcement (LSA), est simple car se base sur des tags ; réutilise les messages de découverte des réseaux d'accès ; et fonctionne avec une ontologie pour organiser les différents services. Ainsi, il permet de détecter et interpréter automatiquement la disponibilité d'un service sur l'ensemble des réseaux d'accès découvert. Par conséquent, ce mécanisme aide les appareils dans leur choix du réseau d'accès le plus approprié pour un service donné. Qui plus est, ce mécanisme d'annonce de service peut Ãłtre associé avec d'autres protocoles. Cette association permet aux appareils qui peuvent utiliser plusieurs technologies d'accès, de toujours sélectionner et de se connecter au meilleur des réseaux d'accès et à tout moment. Le résultat de cette association assure la continuité de n'importe quelle session de communication.

Nous avons étudié l'impact de notre mécanisme LSA avec un scénario de récupération de données collectées par des objets mobiles. Ce scénario novateur de réutilisation des points d'accès Wi-Fi domestiques est décrit en détails avant d'en étudier sa faisabilité. Différents environnement Wi-Fi ont été caractérisés à l'aide d'un outil Android. Les données récoltées ont permit d'initialiser une chaine de Markov complexe représentant notre scénario. Cette étude mathématique nous as permit d'évaluer l'impact et la validité de notre mécanisme selon différents paramètres dont : la densité des points d'accès, la fréquence des annonces et le taux de succès de la récupération des données. Nous avons ainsi pu démontrer que notre proposition permet d'améliorer les temps de connexion.

TELECOM
Bretagne

Contents

List of Figures

List of Tables

LIST OF TABLES

1 Introduction

1.1 Motivation and Objectives

Over the past twenty years, the arrival of new attractive applications designed to appeal to a wide variety of different devices has dramatically increased the amount of network data traffic. As shown in [22] and [26], the increase is exponential. In addition, these growth tendencies are expected to appear in wireless networks as measured and forecast in [27]. Consequently, the demand for bandwidth required to unload this traffic is also increasing. As a result, access technologies have evolved and expanded to meet these increasing demands. As a consequence, devices have currently access to more than one Access Network (AN) via various access technologies. The generalization of Internet Protocol (IP) over these different technologies, which extends Internet coverage, also participates in the rise of traffic exchange in this ecosystem.

Today's devices currently include interfaces for multiple technologies which enables them to benefit from the aforementioned access diversity in any situation. However, even though these devices have the necessary capabilities to fully take advantage of the wide variety of access options available, i.e. being able to use all or a subset of interfaces simultaneously, we observe a lack of mechanisms to efficiently do so. Instead, devices currently use only one interface at a time and all their data flows are transported on this one interface. However, this behavior does not guarantee that the connected interface will be best suited to each traffic flow, as individual requirements may differ. Furthermore, this model of using one active interface for several applications, increases the complexity of the protocols being used because it requires to adapt traffic flows to the corresponding AN. This model becomes even more problematic with the arrival of constrained devices, which are different from current devices in terms of traffic produced and devices capabilities. Therefore, these devices need a new model not centered on Internet in order to conserve a maximum of energy and resources.

In this thesis, we propose contributions which aim to help any device – constrained and not-constrained – benefit from the diversity of ANs. Our approach is two-fold. First, devices should be able to distinguish ANs capable of transporting a given traffic flow from the other ANs. For this, devices need to discover the service availability of each AN and compare it with the requirements of a given application. Second, in the case of devices with multiple interfaces, the network service discovery mechanism has to be the same across all available access technologies. This way, devices can compare all the network services available on each AN as well as their characteristics, thus enabling them to assign the application's traffic flow to the proper interface. Finally, both network service discovery and assigning mechanisms have to be simple, automatic and transparent as these actions may be performed repeatedly and in order to increase the application range for this type of solution.

1.2 Thesis Overview and Contributions

In this thesis, we study current network environments and the multitude of elements they consist of in order to propose a simple solution for advertising Access Network (AN) capabilities to any device that needs to connect to these networks. This solution could be used to help these devices take full advantage of the diversity of services, providers and access technologies available by facilitating their selection.

A Lightweight Service Announcement Mechanism

In order to allow a service-based Access Network (AN) selection, AN service availability needed to be uniformly announced to any surrounding devices. Several protocols and architectures exist but none of them provided a generic method to simply collect network service information. After studying the different network discovery mechanisms, we defined a simple and lightweight mechanism to announce network services availability as presented in [56]. The Lightweight Service Announcement (LSA) mechanism is based on an ontology, which enables any device to automatically detect and interpret the services supported by a provider and the associated AN, at the moment they discover the network itself. This mechanism offers different advantages as devices can then filter, without human intervention, ANs according to their needs and select the one that best suits them among the subset of access supporting a desired service. This mechanism has a limited impact as it re-uses existing network messages, offers new service deployment opportunities and is entirely backward compatible.

A Service-based Always Best Connected Framework for User Devices

In order to take full advantage of Access Network (AN) diversity, user devices – with few resource limitations and multiple interfaces – could use the Lightweight Service Announcement (LSA) mechanism to determine the best provider for each data traffic flow in order to distribute data flow simultaneously onto different interfaces. With this in mind, we have defined a framework based on the LSA mechanism, a decision algorithm, a protocol providing Internet Protocol (IP) address agility, and a routing protocol [57]. This framework should enable user devices to always select the best possible AN at any given time and in any given location. Additionally, the dynamic flow distribution should enable devices to maintain session continuity as long as an AN that supports the desired service is available. All these framework's properties should enhance usage of current services.

Mathematical Model of Wi-Fi Devices Behavior

In order to further study the Lightweight Service Announcement (LSA) mechanism and in particular to determine its impact, we modeled the behavior of a Wireless Fidelity (Wi-Fi) device moving through an urban area. Our models can help estimate the time necessary to discover a Wi-Fi network (or in a LSA-capable scenario, to detect a service) as well as the associated success rates. These models are based on Markov chains which are instantiated using empirical data. These data obtained during measurement campaigns also allow us to characterize Wi-Fi deployment and to study the significance of Access Points (APs) distribution for the detection results, i.e. discovery/detection time and success rate. One of these models would in particular help define the optimal distribution of APs to select, in order to announce a service seamlessly in a given area.

1.3 Outline

The thesis is composed of three chapters. First, we describe the various heterogeneous environments that users and devices gravitate towards currently. The diversity present in these environments raises some challenges and we focus in particular on the possibility of selecting an Access Network (AN) based on the services it may support. Then, we list the existing solutions, their limitations and express our desire to make it possible for any device to select the network best suited to its needs no matter what the access technology may be.

Afterwards, we present our proposal, the Lightweight Service Announcement (LSA) mechanism, to enable service-based AN selection for all devices regardless of the access technology. This proposal allows Service Providers (SPs) to advertise supported services via their Point of Attachments (PoAs) of the corresponding network to sur-

roundings devices. To achieve this, and in order to automate both the announcement and the selection, services are organized in a standardized and hierarchical way to ensure that all entities have the same representation. This additional network information helps devices select the most appropriate network for all their applications. This mechanism may be used in parallel with other existing protocols, enabling user devices not only to select the appropriate AN for each service, but also to always be connected to the best possible AN for each service. Therefore, in a scenario where providers compete with each others, the LSA mechanism is supposed to enhance existing services and define several new opportunities.

Finally, we present a test case scenario used to study the effectiveness of the LSA mechanism. This scenario consists of re-using residential IEEE 802.11 Access Points (APs) in order to collect data generated by Wi-Fi constrained devices without having to deploy a new infrastructure. Simulations have been performed to validate this scenario and the behavior of mobile Wi-Fi devices has been modeled using Markov chains. These mathematical models, instantiated using empirical data gathered in real-world experiments, enable us to study both the time needed and the success rate to detect an appropriate AN. The impact of the announcement frequency, the AN density and distribution, as well as the amount of data to be collected with specific parameters can be evaluated using these models. With the LSA mechanism, even with a small number of APs or long intervals between service announcements, our models show that it is still possible to collect the data from mobile constrained devices with minimal impact on traditional Wi-Fi nodes. This study also helps us unveil some limitations of the current connection model (one complex connection to transport all possible traffic flows). We propose some solutions that, assisted by the LSA mechanism, might greatly improve this model.

2 Heterogeneous Access Network, Devices and Services

In the past years, the user's demands, needs and requirements in terms of network connections have evolved hand-in-hand with devices, services and access technologies. However, in today's network environment, there is not a single access technology that satisfies all user requirements. Depending on the penetration of these access technologies, devices have multiple ways to access Internet and its associated services such as web, video-streaming, etc. Moreover, services which are no longer linked solely to an Internet connection and their associated Service Providers (SPs) are beginning to appear in this ecosystem. This means that devices have access to multiple services – not just Internet services – via different access technologies and that the Access Network (AN) must be selected accordingly as studied in [32]. While devices might take advantage of heterogeneous accesses, they mainly use one access at a time. This means that all traffic flows are transported using a single access even though they could distribute their traffic over multiple paths. As a consequence, the network landscape with its multiple possibilities is more complex than what it used to be. Moreover, devices require more protocols in order to transport all possible types of services regardless of the technology used, which leads to more complex connections establishment. In addition, this Internet-based connection model is not adapted for the massive arrival of constrained and less human operated devices. These new devices have highly specific requirements for simple and low resource-, time- and energy-consuming mechanisms. However, all these devices could benefit from the diversity of access technologies offered by a Complex Heterogeneous Environment (CHE).

Before proposing any solutions to exploit this type of environment diversity, we described all of the elements that make up such a complex environment. This inventory will help us identify the requirements that need to be addressed in order to select the most appropriate access for each service. However, due to the multitude of possibilities, criteria and characteristics, enabling any device to determine the best service/access combination is a rather complicated task and additional mechanisms will be required.

In this chapter, the first section presents the current network environment status with its multitude of devices, services and diversity of access technologies. In Section 2.2, we describe the emergence of constrained devices in this environment, their impact on current access technology and their specific requirements. We then focus in Section 2.3 on existing network and service discovery mechanisms that could help devices from complex network environments select an Access Network (AN) based on service availability. However, we show that these existing solutions have limitations and cannot fully handle the diversity of the ecosystem with all the technologies, devices and services at stake. Finally, we conclude the chapter by presenting a service-based connection model that is supposed to enable any device to select ANs based on service availability.

2.1 Complex Heterogeneous Environment

2.1.1 Multitude of User Devices

User devices evolved with the diversification of user needs and with the evolution of the technology. The oldest type of user devices are wired devices – the first commercialized communication network was a wired network –, which are not meant to move as they are limited to the range of the wire. Most wired devices are not battery-operated devices, and the fact that they are not mobile – due to wire-range constraints – means that they tend to be equipped with heavier and more powerful hardware capacities than other devices. These increased capacities make it possible to use any type of application from the most resource-demanding, such as high quality video streaming or video gaming, to the least resource-demanding, such as social networking. Capabilities also define how many applications can be simultaneously run on wired devices. Although, wired devices are not supposed to be mobile, we noticed that they are equipped with a wireless interface to take advantage of any wireless networks present – as a backup interface, in case of wired network failure, or to provide a connection if no wired connection is available.
Some users move constantly between locations – e.g. home and work – and therefore, need to be connected at each location they stay at. However, it is not possible to constantly move static wired devices – even if they have both wired and wireless interfaces – between locations due to their weight and the absence of a battery. The presence of multiple interfaces associated with the increasingly nomadic behavior of users had led to the emergence of nomadic user devices such as laptops. These devices are not mobile, as they are not designed to be used while the user is moving, but they can be used in moving locations such as vehicles.

In opposition to wired and nomadic user devices, mobile user devices have been designed to offer connectivity while moving. This is also why these devices only possess wireless interfaces. In order to offer a better mobile experience, these devices are smaller than most wired user devices and they are battery-operated. However, they

do not have the same capabilities in terms of hardware, compared to wired devices, and battery life. The latter also prevents them from running the most resource-demanding applications, as this would quickly drain their batteries. Even though, all wireless devices offer mobility, they have different levels of mobility. Some are used within buildings, some are nomadic and others are mobile. Each wireless interface included on these devices enables them to connect to different networks corresponding to different mobility ranges. However, having multiple interfaces on battery-operated devices is a thorny issue as ideally they need to be able to use them in an optimal way so as to limit the energy consumption while providing best possible user experience.

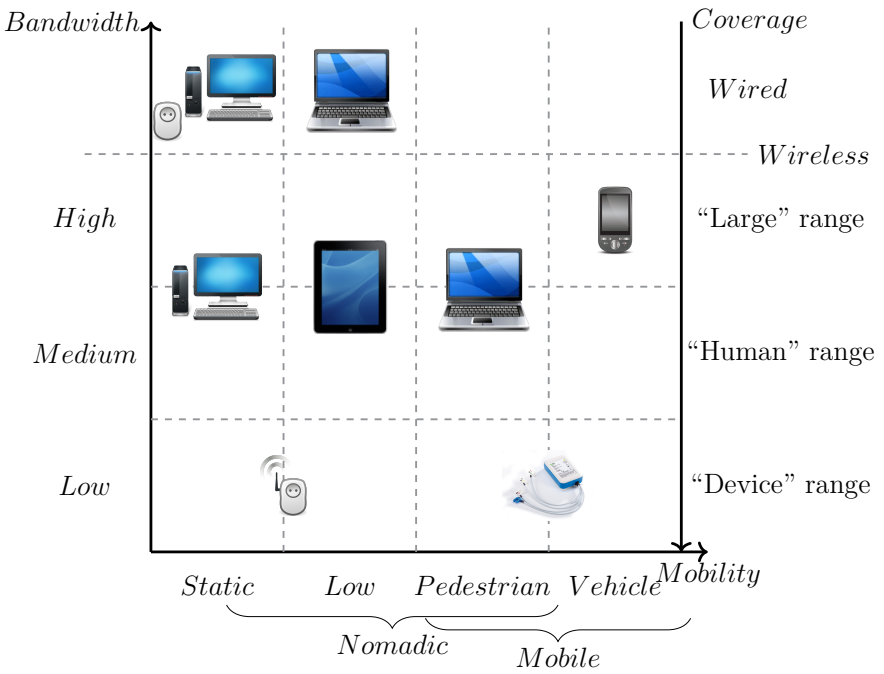


Figure 2.1: Diversity of device

With these devices being used for an increasing number of applications, the number of connected user devices is continuously growing. As a result, a multitude of devices – static, nomadic and mobile – with different characteristics coexist in the network environment. This diversity is illustrated in Figure 2.1 where each axis represents a user requirement. All these devices have one or several interfaces to connect to different ANs and satisfy different users needs for mobility, coverage and bandwidth. However, they all only use one interface at a time. The current challenge is therefore to make the simultaneous use of different interfaces possible and manage them in an optimal way as shown in [108], [96] and [36].

2.1.2 Variety of Services

Internet – a network of networks – enables billions of devices worldwide to interconnect. In the past twenty years, the use of Internet for commercial traffic has made it expand faster. Internet hides the specificity of all link layers to create a uniform network for applications. With the popularization of IP, Internet offers devices from different access technologies to exchange information with each other. Different types of communications have arisen from these interconnections, which can be divided into two groups: real-time communications, which include Human-to-Human (H2H) communication, and non real-time communications.

Real-time communication ranges from instant messaging, to telephony, to gaming, to video calls and supposes that both communicating nodes are connected. The traffic resulting from this type of communications is not generated at regular intervals as it depends on users willingness, and has a burst-like nature with a generated traffic volume that depends on the application. However, this type of communication requires both low latency and packet-loss to reproduce the characteristics of a face-to-face communication. As a consequence, and in order to ensure Quality of Experience (QoE) and Quality of Service (QoS), special attention has to be paid to the accesses and protocols used to transport this type of communication. The combination of protocols and accesses should ensure that delays and loss are kept to a minimum while offering a bandwidth as high as possible.

On the other hand, in non real-time communications, end-users do not need to be connected to receive the information sent. This type of communications, which includes Human-to-Machine (H2M) communications, has fewer constraints than real-time communications. In fact, even if the nature of this traffic is burst-like, the need for a high level of QoS is less seeing as the information will be stored. Just like real-time communications, the traffic volume generated by this type of communications depends on the application used – watching a video will generate higher data volume than checking emails. As a result, less attention needs to be paid to transport the corresponding traffic. These communications have been made famous with email, discussion forums and many more services offered on the World Wide Web (WWW).

Indeed, the WWW is the most well known service that Internet offers, relying on non real-time communications, and giving access to a large set of information, resources and applications. By extension, a large set of services – and even near-to-real-time ones with the appropriate protocols – can be accessed via this set of interlinked hypertext documents. Several other services have popped up from the increasing use of the WWW (such as online shopping and file sharing) that may have other constraints such as security.
Internet networks, with the appropriate protocols and mechanisms, provide access for all types of services. Devices with access to Internet can perform non real-time

communications such as web browsing, e-mail, file transfer or video streaming. But they can also have access to real-time communications such as instant messaging, telephony, video conferences or telepresence. Each has different needs in terms of bandwidth, latency and packet loss in order to provide QoS and QoE. Therefore, depending on the access used, some traffic flows may have to be adapted in order to be transported. According to the latest Ericsson report [33] and Cisco forecast [27], the amount of data generated with these services, and transiting on the network, is continuously increasing. This trend will continue to increase and, as concerns user devices, the number of available services is also increasing in order to keep up with user demands.

2.1.3 Diversity of Access Networks

As suggested previously, there are several types of access technology in the current network environment for devices to connect to. These technologies coexists as none of them have managed to establish themselves as a reference for all of the various uses, applications and user requirements. As a result, in almost any location there are multiple ways to access a given network. In addition, each technology can be used for different user requirements as illustrated in Figure 2.2.

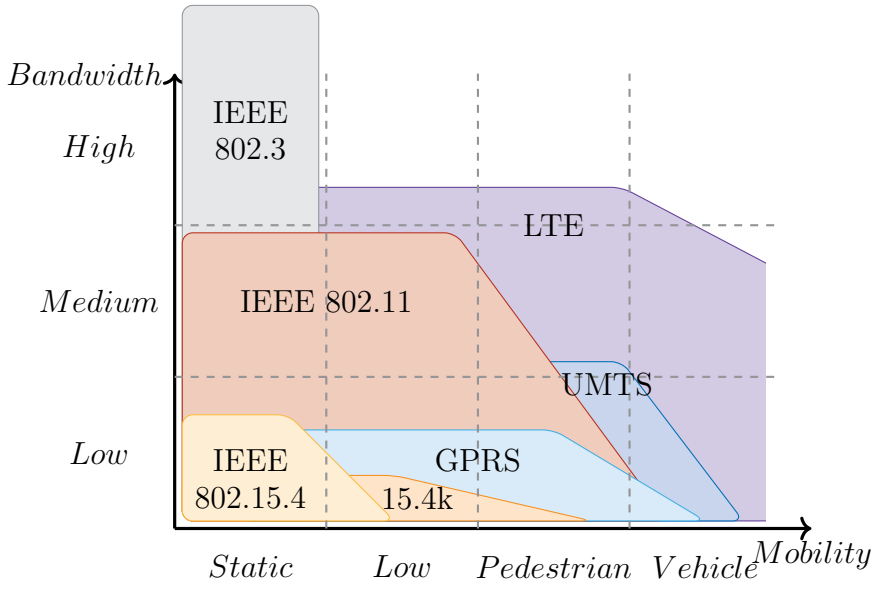


Figure 2.2: Diversity Access Networks

Devices have access to different infrastructure-based wireless technology in urban areas. In these areas, technology should offer mobility support as users may be highly mobile. The most well known wireless access technology to do so is cellular technology, which was first released both to support voice services for Mobile Station (MS) and to offer very large coverage range. Cellular technologies evolved over

the past years to support new services such as data communications and improve network characteristics. The latest cellular technology that has been deployed is Long Term Evolution (LTE) – a cellular network with a full-IP core network and commercially known as 4G – which provides data-rates up to $300Mbps$. The advanced version of LTE is supposed to reach data-rates up to $1Gbps$. Cellular devices do not have to choose among available Cellular Operators as this access technology is subscription-based – except for dual SIM device – but additional cost or volume limits may be applied for data communications with these technologies.

IEEE 802.11 [66], commercially known as Wi-Fi, is a set of standards defining wireless communications for Wireless Local Area Network (WLAN) (first released in 1997). It operates within the open Industrial Scientific and Medical (ISM) $2.4GHz$ frequency band. The unlicensed nature of this frequency makes it possible for anybody to use it to broadcast information. As a result, this communication medium is subject to interference from other ISM systems and the medium itself cannot be improved. However, evolution notably in the form of modulation and the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) method used to share this medium, has allowed to make the most of this medium and has enabled the latest version to reach a maximum theoretical data rate of $600Mbps$. The unpredictable and environment-dependent nature, associated with the high probability of interference of the medium, makes it unreliable for long distance communications (contrary to cellular technology). In addition, when we take into account the limited transmitting power, we find that IEEE 802.11 technology provides a coverage range of up to hundred meters. This coverage range can be improved by setting up several Wi-Fi APs, which makes it possible to use this infrastructure-based wireless technology in urban areas. In a wireless network, switching from one network Point of Attachment (PoA) to another within the same wireless technology, is called a *handover* and performing this switch between different technologies is called a *vertical handover*. A seamless presence of APs allows mobile devices to connect to different APs while moving inside an urban area – just like cellular system but with more frequent attachments. However, current modulation and antenna technologies, which are evolving alongside $5GHz$ band availability, will enable IEEE 802.11 to cover a $5km$ coverage range with gigabit data rate. Moreover, its deployment simplicity makes it a popular technology and consequently the number of available Wi-Fi APs is continuously growing. As a result, in some areas, the IEEE 802.11 access is almost ubiquitous. If Wi-Fi devices could benefit from such a high presence of APs, the density would enable them to be constantly connected [10].

Furthermore, with the arrival of constrained devices, low-consumption and low-rate ANs are available in urban areas. IEEE 802.15.4, as of its fifth amendment, describes an infrastructure-based Low Rate Wireless Personal Area Network (LR WPAN) with IEEE 802.15.4k [68]. This amendment has been released to define alternate mechanisms and provide "large"-range coverage access technology with low energy-consumption but low available data rate.

Devices could also access various networks in smaller areas, such as in buildings. Large-range coverage technologies such as cellular and LR WPAN can also provide an access in these areas. However, due to its deployment simplicity, fair bandwidth, no volume limitation and license-free nature, Wi-Fi technology is often preferred as a wireless technology in these areas because it allows devices to be mobile within their "human"-coverage range.

Another highly used access technology in these areas is wired technology. Even though several wired Local Area Network (LAN) technologies exist, IEEE 802.3 [70], which was standardized in 1985 and is commonly known as Ethernet, is largely dominant. Along with the upgrade of this standard, the wire used to establish communications has evolved from coaxial to fiber-optic technology. Moreover, the emergence of full duplex wires results in collision-free technology. Despite not being mobile, wired technologies offer therefore very good bandwidth capabilities, especially with the popularization of fiber-optic technologies. The available data rate of IEEE 802.3 has also grown considerably with the evolution of topology and protocols used to support these communications and reaches a data rate of up to $100Gbps$.

Finally, devices also have access to various ad hoc technologies. These technologies are infrastructure-free and communications take place between nearby stations.

Bluetooth [14] is a wireless technology standard developed to replace data cables. This means that devices can be interconnected by setting up an ad hoc Wireless Personal Area Network (WPAN) to transport both voice and data communications. It allows users to exchange data within a very short distance using the open $2.4GHz$ ISM band. Bluetooth has evolved over the years but, just like any radio technology, the available range and data rate depend largely on propagation conditions, antennas, power transmissions and interference. However, signal fading and attenuation due to the intrinsic nature of the environment are less problematic for this technology, thanks to its short-range application. However, the latest version of Bluetooth should provide devices with a data rate of up to $24Mbps$ and, depending on the environment, a coverage range from $1m$ to hundreds meters.

Another example of ad hoc access technology is IEEE 802.15.4 [67], which is a standard for LR WPAN released in 2003. This technology is primarily designed for Wireless Sensor Network (WSN) and aims to provide low energy-consumption transmissions for short-range communication. Just like IEEE 802.11 it uses the CSMA/CA method to share the medium and operates on an unlicensed frequency band, such as the $2.4GHz$ ISM band. Contrary to IEEE 802.11, the "device"-range coverage of this standard enables it to limit the unpredictable nature of the shared medium even though probability for interference is higher due to the open nature of the used bands. The IEEE 802.15.4 standard is designed to provide a communication range of up-to $10m$ and reach a data rate of up to $250Kbps$. An IP-based wireless network can be set up based on IEEE 802.15.4 using 6 Low Power Wireless Personal Area Network (6LoWPAN), enabling this "low-resource" network to simply interconnect to any other IP-based network.

These networks made of neighbor stations offer several possibilities as they can be linked to other access networks if one node of the network is acting as a bridge. This makes them particularly likely to have access to Internet and its services.

2.1.4 Versatile Connections

The network environment has changed over the past years and it is becoming more complex. As illustrated in Figure 2.3, a multitude of devices continue to spread across the different network areas, adapting and differentiating themselves to correspond to different user requirements such as mobility, coverage and bandwidth. Users run a variety of different applications on these devices, all of which have different needs in terms of delay, loss and data rate. User devices also have access to a diverse range of access technologies with varying performances. This means that user devices have multiple options for transporting one communication flow and devices need to be able to determine which options to use. This type of environment with a plethora of user devices using several types of services and surrounded by different ANs can be described as a Complex Heterogeneous Environment (CHE).

There are multiple ways for user devices to connect to a given network – via different access technologies – which result in them being "multihomed". According to Fekete et al. [37], multihoming refers to having multiple paths to reach a certain entity. Multihoming was first used by large companies to ensure reliability by having more than one Internet Service Providers (ISPs) serving their IP network [83]. However, current multihoming refers to the property that a device or a site can be connected to more than one ANs [72]. This asset offers the possibility of using any given AN for a desired service regardless of the type of technology used. IETF in [24] is especially studying the insertion of multihoming and the resulting issues for Home Networks (HNs), which supposes that multihoming will be more and more common in future network environments. From now on, we refer to any device inside a multihomed network (one interface multiple providers) or any device with several interfaces (multiple interfaces, each of them with one or several providers) as multihomed device. However, current user devices do not take advantage of their multihomed assets, whereas they could benefit from such CHE by using their interfaces simultaneously for different services. Instead, devices use one interface at a time and all the data flows are transported exclusively on this active interface. However, the network the device is connected to might not be the most appropriate for all of the services being used. In fact, services vary in nature and require different levels of QoS to ensure the best possible QoE. Therefore, rather than adapting services or adding protocols to transport all types of services on one type of access technology – i.e. having connection versatility –, user devices could benefit from assigning data flows to the most appropriate interface and access technology depending on specific requirements.

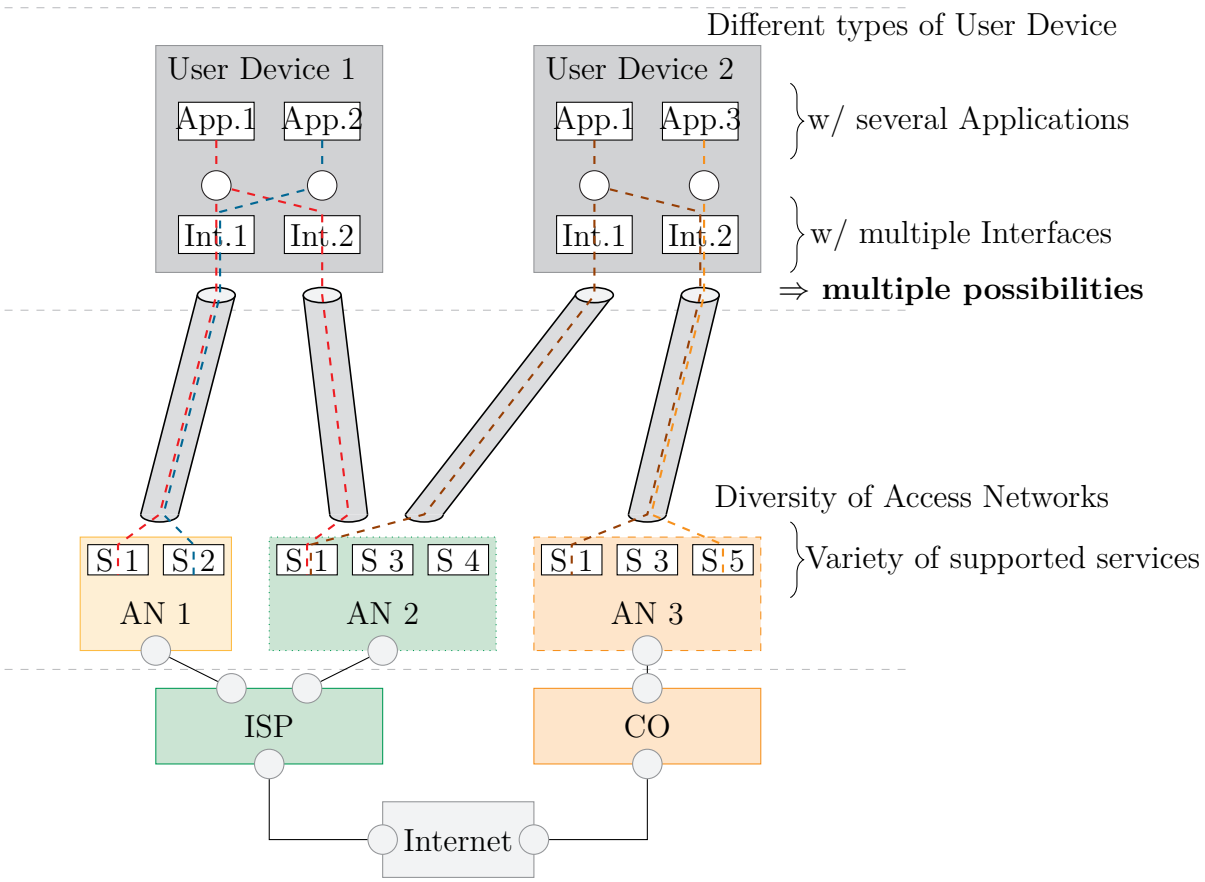


Figure 2.3: Illustration of a Multiple- User Devices, Interfaces, Services and Access Environment

The current connection model, centered on Internet, builds off of several protocols within user devices which enables them to transport as many traffic flows as possible on the same access. This model, due to its complexity, requires more and more device resources and increases the time needed to effectively start data traffic. This versatility is not a problem for user devices as they already have sufficient resource capabilities. However, this model for its resource consumption drains battery life which may be an issue for battery-operated user devices. For instance, [107] shows that the use of TCP increases the battery consumption compared with the use of UDP. Moreover, this model is (unfortunately) not adapted to the emergence of constrained and self- or remote-operated devices.

2.2 The Arrival of the Internet of Things

All available content on Internet is human made. Based on this assertion, experts began to discuss the possibility of using devices to produce information that would keep us informed about our everyday environments. From these discussions emerged the concept of Internet of Things (IoT) [6]. This concept consists of a set of smart "things" that are able to connect to Internet and feed other devices with their collected information. As long as these things can be uniquely identified and provide some empirical data on our environment, anything can be a "thing". These objects can monitor everything and users can collect raw data on their status to perform analyses and, when possible, manage their environment. Many types of news services can be imagined with the arrival of these "things" as the information they collect would enable people to know the exact status of the monitored environment. For instance it could have applications for waste, loss and cost reduction in numerous fields such as logistics and energy. Finally, it could also have useful applications for environment management as an individual would be able to control and manipulate objects and therefore, adapt them in order to be in a specific state.

The Machine-to-Machine (M2M) paradigm is part of the IoT concept. This technology paradigm is built around the principle of interconnecting machines with the least possible human intervention. This concept stipulates that machines be embedded with several "things" and then aggregate their data for direct local analysis or send corresponding data to another machine for more global analysis. These data can then be used to representing the monitored state as a more global and meaningful piece of information – e.g. representing the cost of the lighting used in a room.

With the wide variety of possibilities offered by the IoT, it is estimated that billions of IoT objects be connected to actual networks within a 10 year span [76]. However, for interaction to be possible in this all-IP world, IoT objects must all have a unique IP address. Due to the limited address space of IPv4, it is anticipated that IPv6 will be used to address this large number of objects. Even though solutions exist to bypass the IPv4 address shortage, we will consider in the rest of this dissertation that future networks will use the IPv6 addressing scheme. In fact, the standardization of IoT is steering towards IPv6 based solutions such as 6LoWPAN. It is therefore highly probable that IPv6 will be used in all future networks. This will prevent any problem that might occur as a result of using an addressing scheme that will no longer be sufficient as well as prevent the increase of network complexity.

2.2.1 IoT Specification

Although, technologies are always evolving to offer – and therefore, to support – more services for users, the exponential growth associated with arrival of the IoT is

impacting current network architectures that have not been designed for so many devices or for supporting these new types of traffic flows. Indeed, the mostly low-volume per endpoint, event-driven, scheduled or periodic, energy-, resource-, and cost-efficient nature of the M2M traffic is in stark contrast to the high-volume per endpoint, burst-like nature of the H2M communications and even more to the H2H communications. Pötsch et al. [95] already demonstrate that even what would be considered "light" M2M traffic can increased the delay on best effort H2M traffic in LTE cellular networks due to the massive number of nodes involved.

Moreover, elements of the IoT have a different purpose, compared to classical user devices – wired or wireless –, as they are built to be connected to Internet and continuously provide information on the environment in which they evolve. They are then expected to last much longer than current devices, which is the reason why these objects are usually restricted in terms of capabilities and are designed to use as little energy as possible. For that matter, they have only one main low-consumption interface to transmit their data and are generally deployed to accomplish a single goal. That is also why there are often more "intelligent" devices, which are technologically superior to these "things", use to gather, aggregate and relay data from a set of things to the appropriate destination.

2.2.2 IoT Requirements

The IoT model contrasts sharply with the current more versatile model. IoT devices have highly specific requirements and need to conserve resources and energy in order to accomplish their tasks on a continuous basis. The generated traffic volume for IoT devices is consistently the same and is either scheduled or sent at regular intervals, but which requires these devices to continuously repeat the connection process. These objects therefore need to have a simple but fast, energy- and resource-efficient connection mechanism. Moreover, they require lower bandwidth availability for the traffic they generate as compared to traffic volumes generated by user devices. However, these specific devices need to connect to access technologies that are designed to support this massive number of low but recurrent traffic flows, either via an appropriate low-rate AN or via a gateway device that will connect to common ANs.

Despite the diversity of ANs present in today's network environment, new network infrastructure are being deployed, such as SigFox [40], in order to face the emergence of IoT. However, this is not the only solution for transporting the associated traffic. Some existing infrastructure are not overloaded and could be re-used, this way avoiding new deployment. In any case, and even more if several providers tend to deploy dedicated infrastructure, IoT devices would need to be able to select the most adapted AN inside this complex environment. To summarize, IoT needs a simplified connection process based on a mechanism that would help determine the most appropriate AN to transport the corresponding traffic for a specific purpose.

If each purpose is generalized as a service, this solution could also help any device select the most appropriate AN – and therefore, the corresponding interface for devices with multiple interface – for each service.

The question we must ask is how will any device – user or IoT – from a CHE be able to determine the best service/interface (if there are several)/AN combination? We can hypothesize that a service-based selection could compare the characteristics required for a given service with the characteristics of available ANs in terms of physical parameters and supported services. This comparison has to be simple in order to be used by constrained devices. Moreover, it has to be automated, so that devices are able to perform this selection repeatedly and at any moment especially for mobile devices as they face an ever-changing environment. However, in order for this selection method to function, devices need to retrieve additional information from available ANs.

2.3 Existing Network and Service Discovery Mechanisms

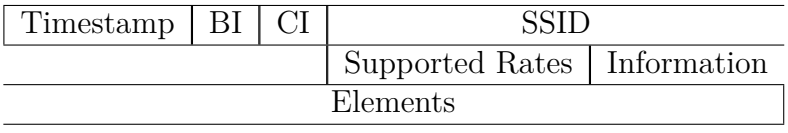
2.3.1 Network Discovery Mechanisms

Before studying the possible solutions for device to retrieve additional information on available ANs, it is important to list the mechanisms of each technology enabling devices to discover a network and retrieve basic information on these networks.

2.3.1.1 IEEE 802.11 - Beacon

As mentioned in Section 2.1, IEEE 802.11 [66] is a set of standards defining local wireless communications. A beacon frame is a management message enabling APs to advertise their presence to surrounding devices within the wireless environment. It helps devices discover Wi-Fi networks and retrieve basic information on them. These messages are sent at regular intervals but the information they contain can also be obtain in response to a Probe Request (PReq) message.

Figure 2.4: Representation of IEEE 802.11 Beacon Frame



A beacon frame contains fixed parameters such as the timestamp, the Beacon Interval (BI), the Capability Information (CI), a Service Set Identification (SSID) and the Supported Rates. It also contain an optional field containing as much Information Elements (IEs) as the beacon frame size allows. Some examples of IE are:

- **Parameter Sets**: indicating information on specific signaling methods (frequency hopping or direct sequence spread spectrum, etc.);
- **Traffic Indication Map**: indicating the buffered frames for sleeping stations;
- **Vendor-Specific information**: providing information on the vendor.

Even though these IEs are defined and set, they are usually ignored such as the Vendor-specific IE, as they are not standardized and so might not provide useful information for ranking and selecting Wi-Fi networks.

IEEE 802.11 compliant devices discover available ANs via received Beacon frames. The more beacons that are received, the more ANs that are present in the Wi-Fi area. Information and parameters of Beacon frames along with the Received Signal Strength Information (RSSI) are currently what enable devices to rank the discovered Wi-Fi networks.

2.3.1.2 IEEE 802.15.4 - Beacon-enabled mode

IEEE 802.15.4 defined two modes for accessing the channel: a synchronized mode based on the use of beacons sent at regular intervals, like in IEEE 802.11, and a contention-based mode [88]. In the former mode, all the coordinators of a LR WPAN send synchronization frames at regular intervals – which includes a beacon frame – to their associated devices. In the latter mode, beacons are not used for synchronization but are still used for discovery and association. Actually, the beacon-enabled mode is equivalent to the passive scanning in IEEE 802.11 and the contention-based mode to the active scanning of IEEE 802.11. Therefore, in the non-synchronized mode, devices looking for a coordinator send out broadcast requests and wait for an answer which will include the information on the beacon frame.

Figure 2.5: Representation of IEEE 802.15.4 Beacon Frame

Beacon Order			Superframe Order		Final CAP
Slot	BLE	Res	PAN C	AP	GTS Fields
Pending Add. Fields			Payload		

Beacon frames in IEEE 802.15.4 enable devices to discover and pair to IEEE 802.15.4 coordinators as well as provide other information. There are no optional fields available in this beacon frame, which makes it harder to implement any extension.

2.3.1.3 Neighbor Discovery Protocol - Router Advertisement

Neighbor Discovery Protocol (NDP) [92] is an IPv6-based layer 3 protocol responsible for address auto-configuration and the discovery of other devices on an IPv6 link.

It is composed of five packet types: Router Advertisement (RA), Router Solicitation (RS), Neighbor Advertisement (NA), Neighbor Solicitation (NS) and Redirect. RA, as shown in Figure 2.6, allows routers to advertise their presence along with link information. Among these parameters, an RA message may contain the list of available prefixes on the current network. This Prefix Information option enables devices to configure a unique IP address for each prefix. Other information can be added in this Options field however, nodes must ignore options they do not recognize (by default) and continue processing the message. RA messages are sent by routers at regular intervals but can also be sent in response to an RS message.

Figure 2.6: Router Advertisement Message Format

Type	Code			Checksum
Cur Hop Limit	M	O	Reserved	Router Lifetime
Reachable Time				
Retrans Timer				
Options				

Devices discover available ANs connected to the network via the Prefix Information. In the case of a wired network, each Customer Edge Router (CER) advertises its prefix on its link, which is then relayed by internal routers to the network. The more prefixes there are in the Prefix list, the more ANs are connected to the corresponding network. Devices have as many IP addresses as prefixes. Deciding which address a device should use depends on the prefix of the destination address. If the device does not have an address with the corresponding prefix, everything is performed with default address and routing mechanism. Otherwise, its corresponding IP address is used.

Each network technology has its own discovery mechanism. Almost all of them have planned optional fields in order to extend the information provide by their messages sent at regular intervals and advertising the presence of an AN. However as they are optional fields, these information, if they are not standardized, are often ignored.

2.3.2 Network Information Advertisement Mechanisms

As previously mentioned, devices need additional information about ANs in order to refine selection of the most suitable access. This information needs to be generic so that devices can compare available ANs regardless of the technology used. Therefore, a unified method must be used to inform devices about the ANs capabilities. Presented below are several solutions that have already been defined to provide a unified information advertisement mechanism.

2.3.2.1 IEEE 802.21

IEEE 802.21 [69] also known as Media Independent Handover (MIH) is a standard defined to provide methods and procedures that facilitate handover between heterogeneous ANs – vertical handovers. In order to easily perform handovers devices are enabled to monitor events, execute commands and gather information from other MIH-capable nodes.

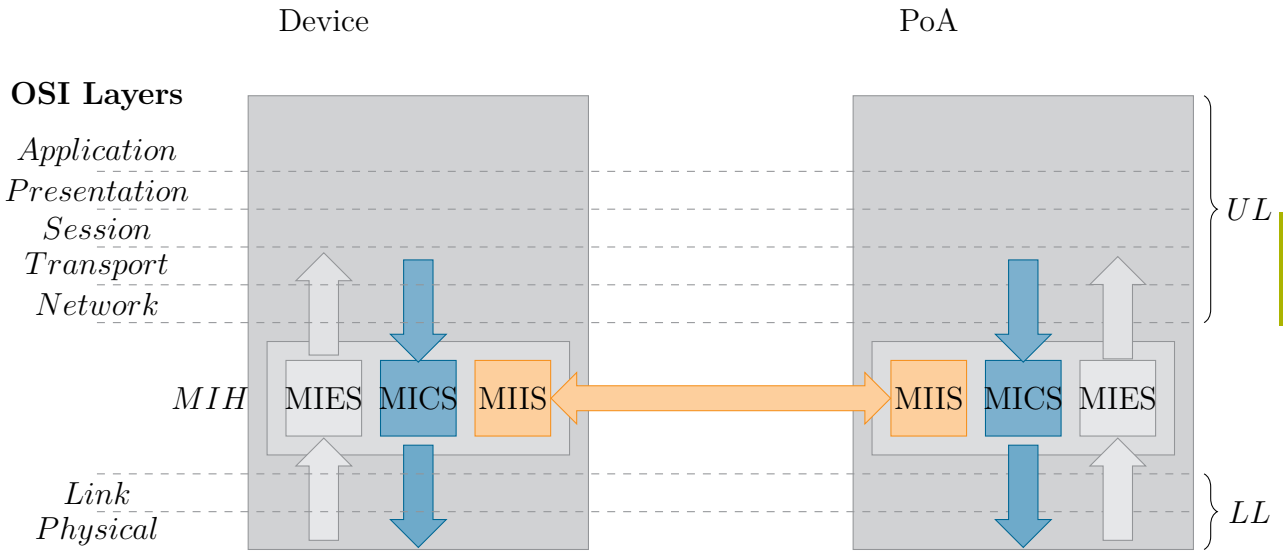


Figure 2.7: Representation of IEEE 802.21 Service Functions

To accomplish these tasks, IEEE 802.21 is broken down into three parts as shown in Figure 2.7:

- **Media Independent Event Service (MIES)**: A service giving information to the Upper Layers (ULs) about layer 2 events such as low power level signals, lost connections, etc. Some events may lead the decision engine to engage handover.
- **Media Independent Command Service (MICS)**: A service that provides the tools for the device to send commands to the Lower Layers (LLs) in order to execute corresponding actions such as scanning for new networks, connecting to a new AN, etc.
- **Media Independent Information Service (MIIS)**: A service enabling devices to retrieve information on the availability of surroundings networks and their parameters. In particular, it enables nodes to gather unified information on different heterogeneous networks without having to query information on all of them. In fact, a Point of Attachment (PoA) can collect and store information

on other surrounding networks and provide them on demand. MIIS messages are exchanged using the SPARQL query method (below layer 3 and therefore, prior to the connection process with ANs) making it so that MIH-nodes do not need to connect to an AN in order to retrieve its information.

Especially, with the information retrieved from different MIH-capable PoAs from several ANs, MIH helps devices determine the best target network and realize a handover toward this network. More specifically, it facilitates the information discovery on network and event management to engage handovers if necessary. However, MIH defines nothing on the policies used to handle handover. It provides the means for a device to connect to the most appropriate network based on both the information gathered and policies defined by users. Finally, based on the usual link characteristic and information collected using MIIS messages, deciding which target network is the most suitable has to be done by the device's decision engine.

The MIIS element might be used to exchange information between devices and PoAs in order to help select a network as suggested in [3]. Information within MIIS is separated in *Information Element* that can be represented by two methods. The first one is a Binary Representation based on Type-Length-Value (TLV) elements and associated with a query method. MIIS information is structured in containers, MIH standard has defined three main containers as shown in Table 2.1. With this representation, it is clear that a PoA stores not only its network's information, and also capabilities, but information of surrounding PoAs and associated ANs.

Table 2.1: List of Possible Container in MIH

Name of Container	Description
Point of Attachment Container:	containing information that depicts a PoA, i.e. a list of Information Element of the PoA.
Access Network Container:	containing information that depicts an AN, i.e. a list of Point of Attachment Container.
List of neighboring Access Network Containers:	containing information that depicts a list of heterogeneous neighboring access networks for a given geographical location, i.e. a list of Access Network Container.

The second representation is based on Resource Description Framework (RDF) associated with the SPARQL query method. RDF data model allows to describe statements about resource in the form of subject-predicate-object expressions. Information Elements can be written in a document using this representation and

organized according to the aforementioned containers. It enables devices to query each other in order to determine capabilities of each queried node.

MIIS enables MIH-capable nodes to discover all available PoAs from an area, by querying only one PoA of this area. Devices could retrieve information on their environments in a succession of query messages, for example they might start with the list of available ANs of the area and then query information on one or several inner containers.

2.3.2.2 IEEE 802.11u

IEEE 802.11u [65] is an amendment of the IEEE 802.11 Wireless Network Standard. It provides features for improving the interworking with external networks. Among other improvements, it allows a better network discovery and selection. In order to accomplish these tasks, IEEE 802.11u provides information about the network prior to association. In this amendment, a terminal collects information on networks via messages exchanged with specific Station (STA) such as AP. The information gathered during this phase is then used to perform the selection of the best possible network.

This amendment provides a Layer 2 frame that can transport network services advertisement messages, called Generic Advertisement Service (GAS). As its name suggest, these messages are generic and enable any AN to advertise its network services information over an IEEE 802.11 network. This network service discovery is done prior to the association with the corresponding AP. However, in order for a STA to determine whether an AP is GAS-capable, it has to listen to Wi-Fi messages (beacon or Probe Response (PRes)). In fact, legacy Wi-Fi messages might now contain *Interworking Elements*. *Interworking Elements* are defined by IEEE 802.11u and are used to inform devices on the capability of an AP to advertise network services information, possibly from external networks. They are encoded as a TLV element and provide additional information such as the type of AN, the Venue Information, etc.

The protocol used in IEEE 802.11u to query information about a network is Access Network Query Protocol (ANQP). Although the specification of the network service information is out of scope of IEEE 802.11u, this standard is expected to enable Wi-Fi nodes to query APs on different types of network information such as EAP method supported for authentication, IP address type availability, roaming partners accessible, etc. Moreover, queried APs are taking care of relaying queries to the correct destination, if they concern external networks, as well as delivering corresponding replies to the node. With this method, devices retrieve information on their environment in a succession of query messages performed on Wi-Fi networks.

For instance, as mentioned previously, the data traffic on cellular networks is increasing, therefore Cellular Operators (COs) might need to offload data traffic on other available networks such as Wi-Fi [12]. With IEEE 802.11u, COs can advertise an offloading service on a subset of APs using *Interworking Elements*. Devices will query corresponding APs in order to determine this service's requirements and discover that it requires a specific cellular authentication in order to function. If the device satisfies all the requirements, it would be able to use the corresponding APs to transport its traffic instead of the cellular network.

2.3.3 Existing M2M architecture

As mentioned in Section 2.2, IoT objects owing to their low-resource capabilities cannot used too demanding protocols such as IEEE 802.21 and IEEE 802.11u. There is therefore a need to simplify as much as possible the environment discovery for these objects. The European Telecommunications Standards Institute (ETSI) has defined an architecture to manage M2M communications [34] that is agnostic of the network technology used. After noticing that the number of different custom integration of M2M architectures was increasing, the ETSI raise the need for a uniform and standardized architecture to be use for any M2M communication. This architecture will allow to re-use available functions and applications of similar scenarios and to facilitate the implementation of new ones. This standardization is expected to stimulate the emergence of new applications and the use of M2M devices over other ANs than cellular networks.

The ETSI unveiled 6 features that this architecture should provide:

1. **Network agnostic message layer:** "Black-boxing" limitations and issues of physical layers in order for devices to only focus on message destination;

2. **Support synchronous and asynchronous communication:** enabling users to define real-time and non real-time communications;

3. **Subscribe / Notify model:** being able to poll data from M2M devices only if needed;

4. **Uniform data storage model:** storing data in a standardized way to facilitate the usage of collected data from other devices;

5. **Uniform language independent API:** allowing to develop M2M applications in any language;

6. **Distributed security framework:** providing a secure architecture as core components are shared.

Based on these features, the ETSI designed an architecture that helps transport M2M communications over any type of network technology. This architecture shadowed all the network and link issues as regards to M2M applications.

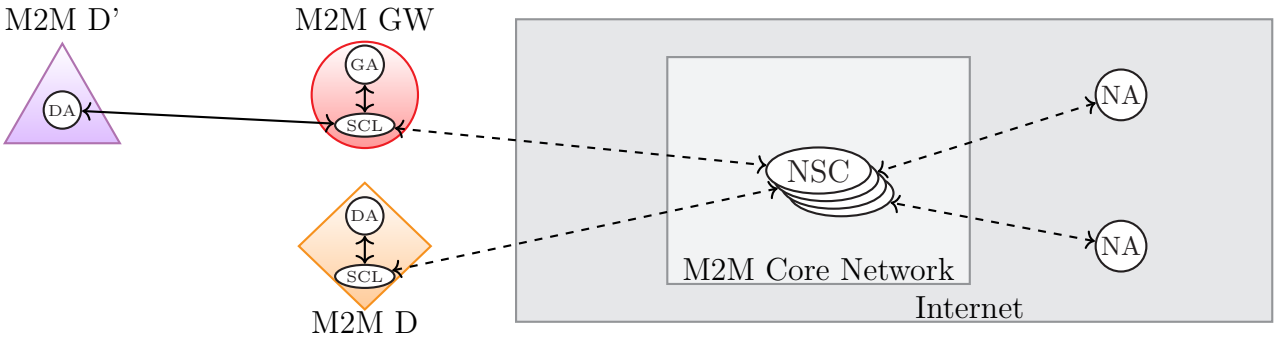


Figure 2.8: Representation of ETSI M2M Architecture

The ETSI architecture is composed of three entities [16] as shown in Figure 2.8:

1. **M2M Network Service Capabilities (NSC):** Inside the M2M Core Network, this component might be seen as a big "router". Indeed, it routes messages to the corresponding destination, it manages profiles in order to ensure permission access (who can do what) and it handles storage. It is planned to be implemented over a cluster of servers. The Service Capabilities (SC) offered by the NSC are accessible by any other Service Capabilities Layer (SCL) connected to it;

2. **M2M Gateway (GW):** a component interfacing M2M devices environment with ANs. Several M2M applications can be running simultaneously and independently on this gateway. Additionally, other M2M devices can use this gateway to relay their collected data to the appropriate destination. For instance, a device with energy constraint (such as device D' on Figure 2.8) could use low energy consumption network to connect to an M2M-GW, which will then transfer its data;

3. **M2M Application:** the application itself as designed by developers. They can be embedded into an M2M gateway (GA) or into any M2M device (DA). Devices with enough resources can directly access the M2M NSC with their own SCL. M2M applications can also be embedded within networks (NA) mainly to use web server. These applications access information from external or embedded "objects".

Communications between these entities are based on Representational State Transfer (REST) [39] architectural style. According to REST mechanism, everything can be done by manipulating and exchanging documents, as proved by the everyday use

of the WWW. In other words, every action can be performed by reading, updating or removing a "document". REST mechanism features four commands to perform these manipulation, *a*) GET, *b*) POST, *c*) PUT, and *d*) DELETE. Finally, the ETSI architecture re-uses standard management framework from fixed and mobile networks.

ETSI M2M architecture is a very interesting architecture providing a common way to interconnect M2M devices over different types of access technologies. However, this architecture is only designed to support M2M devices and M2M communications.

2.3.4 Limitations of Current Technologies

As presented in this section, solutions exist to advertise additional network information on the available ANs. However, these solutions address only one type of access technologies or one type of devices, from the existing diversity as presented in the beginning of this chapter. The distinctive features of these solutions restrain from extending them to any node and any access technology. For instance, the ETSI architecture is dedicated to M2M applications and extending it to any application would require that all applications can be converted to a file manipulation mechanism, which is not the case. On the other hand, IEEE 802.11u standard enables APs to advertise the network service availability of any AN, but this solution is limited to Wi-Fi devices. However, not all devices have a Wi-Fi interface.

Nevertheless, these solutions have interesting features. First, both advertisement solutions allow devices to exchange messages below the network layer, which gives devices the opportunity to retrieve network information before deciding which one to use. Then, both IEEE 802.11u and IEEE 802.21 use TLV information element associated to a request/reply mechanism. According to Andrei et al. [3], when using a TLV representation, MIH offers better performance (faster handover decision and less processing power required) than with RDF representation. However, another implementation [105] shows that the parsing performance when using TLV representation in MIH message may vary depending on the TLV composition – i.e. number of containers. In any case, TLV appears to be preferred as used in many other protocols.

MIIS seems to be the most adapted solution to uniformly exchange network information regardless of the access technology used. Moreover, within devices with multiple interfaces, MIH can fasten APs discovery and can reduce delay and packet loss when engaging handovers as studied in [111] and [80]. Furthermore, associated with the appropriate framework, traffic flows may be adapted to match the target network's capabilities as shown in [25]. Gehlen et al. [44] even shows that MIH could help design an architecture which enable vehicle to always be best connected to a specific gateway. Thus, MIH, and in particular MIIS, appears to be a good candidate to allow devices to retrieve extra network information and engage handovers if necessary.

However, all these results were obtained by simulation or in experimental environment using few ANs. Or with a large number of ANs (i.e. in dense area), the amount of information to be included in each MIIS message might be more important than what have been currently studied. In that case, the retrieval of network information will either be performed in several exchanged messages or within one overloaded message. For such dense area, we assume that the discovery time or processing time will be higher than what currently obtained. In fact, MIIS allows PoAs to aggregate information on surrounding ANs. This way nodes can retrieve ANs information of an area by querying one PoA of this area. Results from [19] show that an average of fifteen different APs are available at any location in a downtown area. In such area, a mobile device using MIIS to query PoAs about network service information, will then receive and have to parse information on at least fifteen ANs, for each different position. It is then clear that the amount of information to aggregate, store and provide by PoA will quickly be large in a CHE, and might generate a scalability issue.

Corujo et al. in [28] present the performance and impact of their implementation of IEEE 802.21 for Network-Based mobility experiment in a handover scenario with PMIPv6. The end of this article focuses on experimental results obtained using an architecture composed of a Mobile Terminal (MT), an Information Server (IS), a Mobility Decision Engine (MDE) (both inside the operator core network) and two ANs. These results show that the MDE and the MT are respectively involved in 44% and 13% of the exchanged signaling data (MIH messages), an expected difference as they demonstrated a network-based decision. However, 42% of the data exchanged to perform a handover belongs to the network information's retrieval. According to their conclusion, this percentage is mainly due to the RDF schema size used in the reply. However, this experiment has only been performed using two ANs. It therefore emphasizes that for denser areas, the size of the reply will be even more important which will significantly increase the amount of exchanged data. Moreover, in this experiment, the signaling involving the MT represents 22% of the total transmission time. Therefore, in a device-based scenario, this time will certainly be higher. Then, this article shows that, even though MIH is an efficient solution to retrieve network information and engage handovers, in denser area, it might significantly increase the amount of both data and message exchanged. As a result, MIH might also make the decision and selection process of a target network more time and resource consuming. These results also suggest that constrained devices might not be able to use this solution as the amount of data to parse and the total transmission time will be increased [105]. Therefore, in order to be more widely used, MIH should be optimized.

To the best of our knowledge, no solution has yet been defined to enable any device in a CHE to automatically and efficiently select an AN based on additional information. There is therefore a need for a light solution to discover network capabilities, which would help select the appropriate AN.

2.4 Towards a Service-based Connection

In this chapter, we have described the evolution of network environments. They have distinctively changed over the past years and the number of devices within them is growing exponentially. Devices can be divided into two categories: user devices, which generate high-volume traffic mostly depending on user desire, and constrained devices, which mainly generate low-volume traffic automatically and for scheduled events or at regular intervals. Access technologies available in these networks have also evolved in order to take account of user requirements in terms of bandwidth, mobility and coverage. Moreover, new access technology appears to take care of the massive arrival of IoT devices. As a result, devices are surrounded by several ANs, each of them having advantages and limitations. Therefore, devices need to determine and select the most appropriate AN among this diversity for each application. These enhancements of the network environment make it more complex than what it used to be, but devices in particular could benefit from this diversity.

The "Always Best Connected (ABC)" concept, first proposed by Gustafsson and Jonsson [55], aims to ensure device with built-in cellular capabilities to always be connected to the best PoA available regardless of the access technology – the wide coverage range of the cellular network ensuring to at least have one available network to connect to. This concept enhances cellular technology and should increase user experience by allowing devices to seamlessly switch, if there are any, to a better network – Broadband or WLAN – and adapt application flows accordingly. However, in order to be ABC-capable, several key components are required among which *a*) *Access Selection*, to define parameters and process to select the best network; *b*) *Mobility Management*, to allow session continuity and session transfer; *c*) *Content Adaptation*, to enable applications to adapt to networks capabilities. Despite all the advantages this concept would offer, it requires several modifications on current network environments. In addition, these components play a role at different communication layers, which makes it even more difficult to be fully implemented. As a consequence, all the requirements needed by this ABC concept currently prevent it from being widely used. Moreover, rather than having devices using their multiple interfaces simultaneously, they currently used only one at a time. In addition, the current network selection is based on the physical characteristics of available networks.

Therefore, devices with multiple interfaces within these CHEs do not fully benefit from the multihomed nature of their environments. As illustrated on the left side of Figure 2.9, current model – based on Internet access – is universal. These devices have several applications running, all with specific needs, but all of them are transported via the only active interface. However, some applications might be better served via another interface/AN. This versatility is making the connection process (from the discovery to the adaption of traffic flows to the corresponding interface)

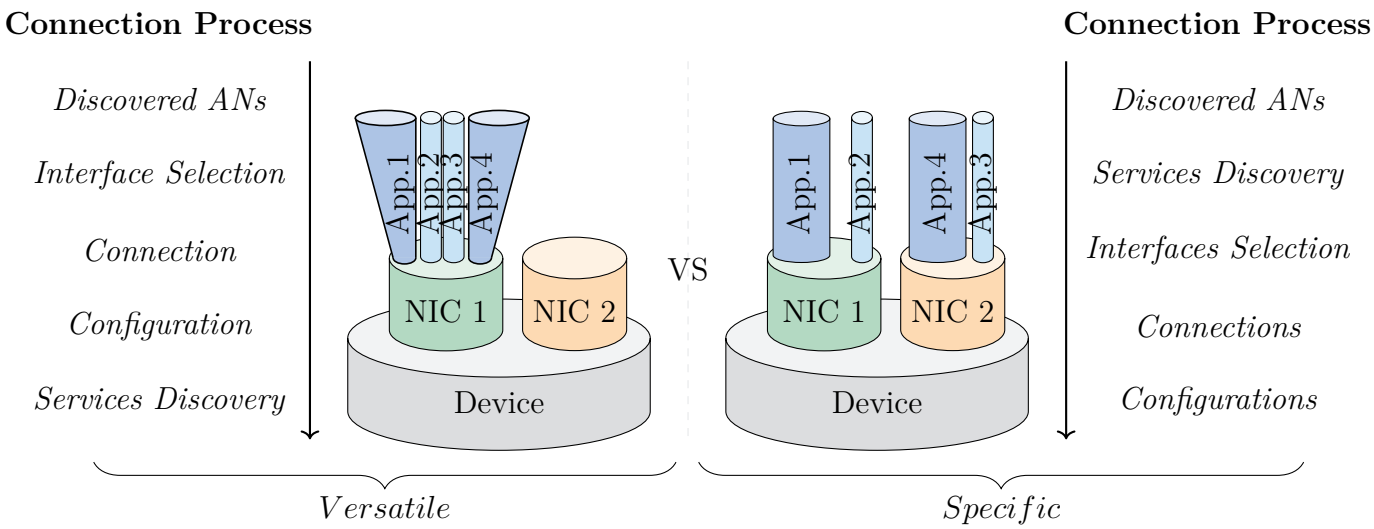


Figure 2.9: Illustration of the Connection Process & Model

more complex. In fact, several protocols are needed to address the different nature of traffic generated by all these applications, in order to enable devices to perform a "for-any-service" connection. The model used with nowadays device has a cost in terms of resource consumed and time needed to perform the connection process. Moreover, this versatility which was not an issue for resource-capable user devices, is raising concerns regarding resource-constrained devices and makes us wonder on the necessity of this versatility. In fact, IoT devices have a need for simple, low-resource, -time and -energy consuming protocols. These nodes do not have many applications to address, but they require specific connection process. Moreover, all devices from a CHE could benefit from the multihomed nature of today's network environment and be close to be ABC-capable. A more specific connection model based on service availability could be used to reach this goal. In this model the discovery of service availability would take place before the connection process. It would enable devices to perform a "per-service" connection as shown on the right side of Figure 2.9 and considered in this thesis.

This new model could be useful for any type of devices. It would first help them automatically discover and sort out ANs based on their service availability. This way, any device in a CHE will be able to limit their connections attempt only to ANs providing a dedicated network service and then, ignoring all the others not providing it. This ANs filtering will enable constrained-device to connect only on appropriate networks and help them conserve energy and resource.
This AN discovery based on service availability, will help user devices with multiple interfaces determine a per-interface service availability. These devices will therefore be able to quickly determine the appropriate application/interface combination. However, due to their multiple interfaces property, a specific service might

be available on several interfaces. Therefore, a decision engine will be required in order to provide an efficient service-based interfaces/ANs selection.
In any case, devices need to be able to detect the network service capabilities of available ANs in order to perform a service-based selection. This selection will ensure any device to always connect to an appropriate AN, and, if these devices can compare services offered by ANs, this mechanism will guarantee devices to always connect to the best available AN, i.e. be Service-based Always Best Connected (S-ABC).

It raises the question on how a device will determine the most appropriate interface/AN combination for each application. Currently, we observe that the network selection is performed manually by users based on their preferences and knowledge of a service, but this would require to be automated in order to be applied to any device involved in a CHE. In fact, an automated selection process would be preferable as *a*) the environment of mobile devices is ever-changing and users do not have a global vision of the environment; *b*) IoT devices have very few human interaction and therefore have a need for automation; and *c*) an automatic service availability detection could be completed using users preferences. To accomplish this automatic selection, a collaboration is needed between end-nodes and PoAs to determine the most appropriate network for each application based on service availability. There is therefore a need for defining a link between the available ANs and an abstract representation of a service and its characteristics. Current solutions cannot guarantee any device within a CHE to efficiently discover the available network services on any access technology. They are either technology-specific, device-specific or have a significant impact on both the amount of signaling data and the time needed to connect to a target network – from its discovery, to the connection. Therefore, a light, simple and generic solution has to be defined in order to retrieve information about service availability on surrounding ANs. This solution will therefore help any device perform a per-service selection process.

In the context of this thesis, a fine-grained knowledge of the evolution of network environment as well as the elements being part of this complex environment, help better understand the drawbacks and limitations of current deployments. It also helps identify the opportunities and challenges in order to optimize the connection model in CHEs. Chapter 3 particularly focuses on optimizing the discovery of available network services in such CHE.

3 Supporting Heterogeneous Services in a Multihomed Environment

In any given location, several access technologies coexist as none of them manage to satisfy all user requirements. As a result, devices have different way to access a given network. However, user devices do not fully benefit from this diversity of accesses as they use only one access at a time. Indeed, with the current connection model, any traffic is transported on the same interface, whereas some traffic flows would be better transported on other available access technologies. In addition, most of current access technologies are not adapted to constrained devices, which have highly specific needs. In order to take account of the arrival of these constrained devices, the current "for-all-service" connection model has to be simplified or new access technology has to be deployed. The second solution has been chosen in on-going deployment [40]. However, defining a "per-service" connection model could benefit to all devices, while avoiding to deploy new access technologies. In fact, such a connection model would allow any device to filter relevant Access Networks (ANs) based on service availability, which would lead to a better ANs selection.

In today's environment, the increasing deployment of access technologies is expanding ANs ubiquity in any given location. Therefore, multihomed devices have the opportunity to select the best AN, within an existing diversity of ANs, to connect to a given network. However, with this increasing diversity, link characteristics information is not anymore sufficient to perform an appropriate selection, as discussed in [5]. This ubiquity is also increasing the options in terms of available services, which may also have different characteristics such as cost, security or offered bandwidth. Therefore, devices need to know what are the possibilities offered by each AN and need to have the ability to compare available services during their selection process in order to determine the most appropriate AN. This new type of selection will push providers to compete with each other by offering better service characteristics. We assume that this service differentiation will also stimulate the emergence of new Service Providers (SPs) and so, increase the number of available services. These new SPs can be of many types, but in particular they can be virtual providers re-using an already deployed infrastructure, just as in the concept of Community Networks (CNs), or aggregating resources from several infrastructures in order to create a new virtual AN as studied in [32]. Moreover, with the increasing popularity of Internet of Things (IoT), we are expecting to witness the arrival of

several dedicated IoT services. However, this service differentiation supposes that devices should be able to choose an AN depending on service availability.

In this chapter, we define a mechanism allowing Point of Attachments (PoAs) to announce their network service availability to surrounding devices. This mechanism will help devices determine the most appropriate network depending on available services. This network service discovery takes place during the network discovery phase in order for devices to associate with each discovered AN the network services supported. Our proposal consists in re-using network discovery messages in which we insert a generic and standardized service announcement tag.
This light and simple service announcement mechanism can also be combined with other exiting protocols to provide a complete framework allowing user device with multiple interfaces to always be best connected for a given application. This framework is composed of our service announcement mechanism, a decision algorithm, a flow distribution mechanism and a routing protocol.

3

This chapter aims to define a generic method for PoAs to announce their available services regardless of the technology used. Section 3.1 lists the requirements needed to define an efficient service advertisement mechanism and presents our service classification resting upon an ontology. This classification and the representation of a service help create the *Service Availability Announcement* tags used in our proposal. This proposal, a Lightweight Service Announcement (LSA) mechanism, as well as the methods used to establish a tag are described in Section 3.2. Before concluding this section, we present the opportunities that this framework might offer for both devices and SPs. Section 3.3 focuses on the application of this proposal in a complete framework allowing user devices with multiple interfaces to be "always best connected" for a given application. Then, Section 3.4 concludes this chapter.

3.1 Providing Network Service Information

In a service differentiation context, nodes need to be able to discover services offered by ANs in their vicinity. Before presenting our network service discovery mechanism, we identified the requirements a service announcement mechanism should address in order to be efficient in both user and constrained device scenarios.

3.1.1 Requirements

In a Complex Heterogeneous Environment (CHE) context, devices are multihomed either because they have multiple interfaces or because they have access to multiple providers via their interface. In order to have a service-based selection of the AN, devices need be able to determine available services and capabilities of surroundings PoAs. But, this network service discovery has to be generic and standardized for

each access technology as devices might have access to several ones. It will therefore facilitate the comparison of available network services regardless of the access technology they are associated with. Moreover, this discovery has to be automated in order to limit human interaction and therefore, be as transparent as possible for users. The remaining human interaction might be for users to inform on their preferences, if there are any, as study in [54]. As a result, the first requirement is:

R1 Any PoA should be able to advertise its supported network services in a generic and standardized method.

In the previous chapter, we have shown that devices at stake in a CHE will not only be resource-capable devices. The second requirement should consider that some of the devices using a service-based discovery, may have some resource or energy limitations. It is therefore crucial to limit the volume of data exchanged for this discovery. As a consequence, constrained devices will not have to parse important volume of information.

R2 The solution must not exchange large volume of data to limit energy and resource consumption.

In dense area, devices will have to discover network service availability from many PoAs. The network service discovery has therefore to be fast in order for devices to avoid spending too much time in each network service discovery. This is even more crucial for mobile device, moving from one wireless coverage to another and thus, having to discover service availability on all discovered PoAs. As a consequence, the number of message exchanged during this network service discovery must be as low as possible. This requirement will also prevent energy-constrained device from consuming too much energy during service discovery.

R3 The service discovery has to be performed in few messages in order to minimize its impact.

Finally, this solution should enable devices to decide whether a PoA, and the associated AN, is of interest for their applications before actually connecting to the PoA. It will prevent devices from connecting to a PoA that does not provide the desired service.

R4 The service discovery has to take place prior to the connection process with PoAs.

3.1.2 Organizing Network Services

In a multihomed environment where devices used a service-based AN selection, devices need to have a link between an abstract representation of a service and the network supporting this service. Moreover, in order for the solution to be compliant with **R1**, the representation used to describe a service needs to be similar for all services and independently from the technology used to announce these services. It will allow devices to automatically interpret and understand service announcements and therefore, be autonomous for the selection of the appropriate AN.

In this context, a device may have access to specific services on different ANs. As a result, it will have to decide which AN to use based on both the service availability and AN characteristics. We assume that attributes will be used to better describe network services, such as the additional cost or the type of authentication required to used it. These network services' attributes, associated with the access technology parameters – available in the network discovery messages –, will help devices compare available network services and determine the appropriate target network. Therefore, the service representation has to consider the service attributes and the relation that can exist between services. In order to facilitate discovery and interpretation of network services, they need to be structured and also hierarchically organized. Figure 3.1 represents a non-exhaustive set of services and their relationships. In this organization, we regrouped services based on their types of application such as connectivity, monitoring, etc. – but this classification could have been done based on their domains of application such as health, energy, etc.

In computer science, a common way of structuring concepts in order to facilitate automatic interpretation by machines of these concepts is to represent these concepts with ontologies. According to Heflin et al. [61], an ontology is a formal and explicit specification of a shared conceptualization, enabling an automatic interpretation of this conceptualization by any device. In fact, devices sharing a structured knowledge can understand any information formed following this structure, which, at the end, facilitate interactions between machines. For example, Semantic Web [2] and Information architecture [47] are domains where ontologies are mainly used as it provides structured documents facilitating the sharing and re-using of data.

Ontologies have been proven useful in several other domains. In [98], the author used an ontology-based traffic model in order to facilitate and fasten the decision-making regarding direction for Autonomous Vehicles, in particular when vehicles arrive at intersections. The complexity arising from all possibilities that offer intersections is simplified to lane section decisions using this model. In [91], authors present a dynamic framework composed of a multi-criteria decision-making technique and an ontology. This framework aims to overcome the complexity arising from decisions that have to be taken based upon multiple sources and multi-criteria

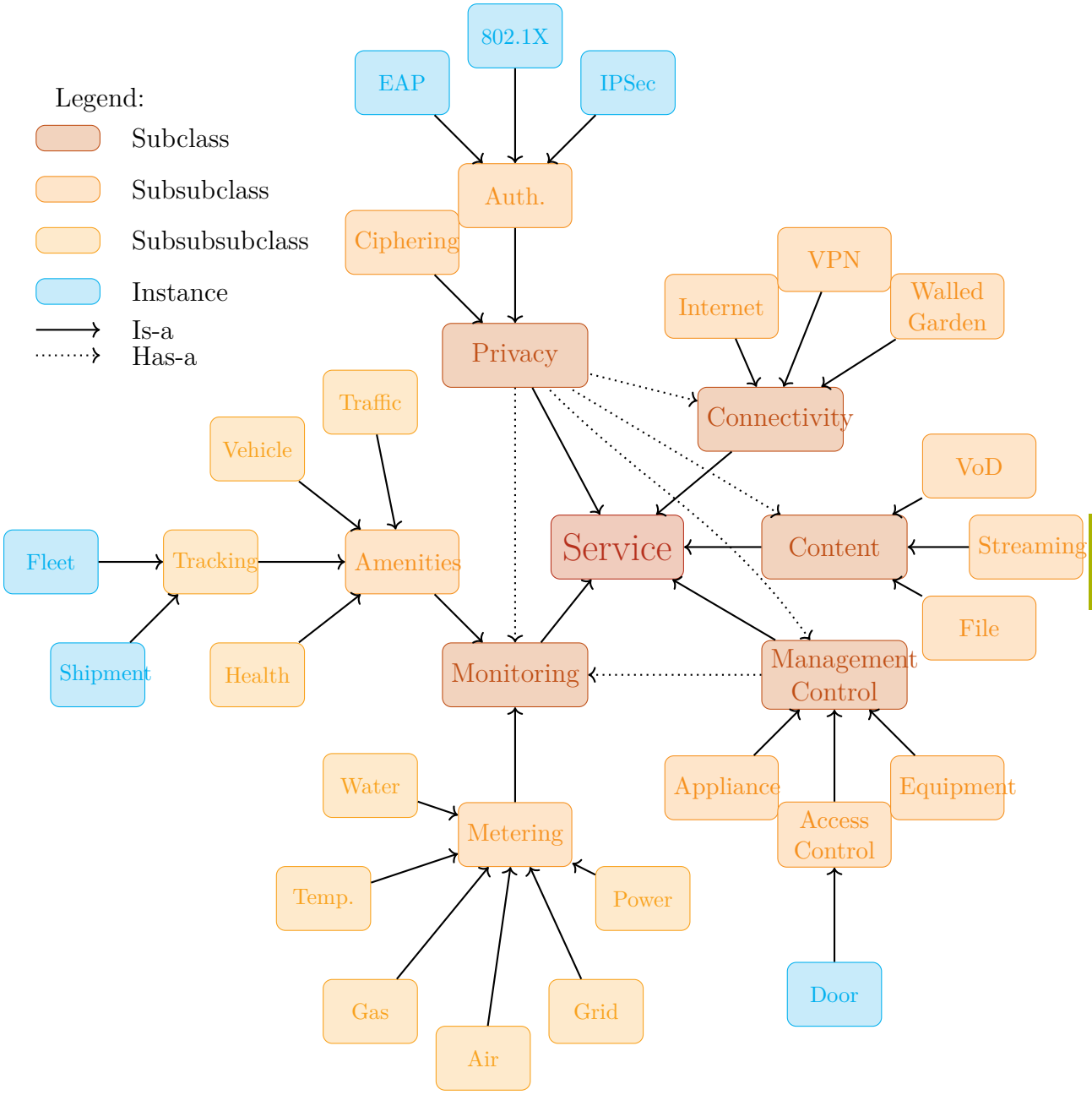


Figure 3.1: Network Service Organization [100] [1]

information. Their proposed solution improves dynamic routing-decision in a SIP-based scenario. Other research show that ontology can increase the efficiency in Web Services discovery [31] and selection [97], as well as it can help discover and match Manufacturing Grid services [60]. Therefore, in our network service discovery context, a Generic Network Service Ontology (GNSO) used with the proper decision

and selection mechanisms should make it possible for any device to select a PoA, and the associated ANs, based on their service availability.

Some languages have been developed to structure information and are therefore often used when creating ontology:

- **XML**: Markup language that defines a set of rules for encoding documents in a format that is both human and machine-readable.
- **RDF**: Metadata language that makes statements about resources (in particular Web resources), in a form of subject-predicate-object expressions.
- **Simple HTML Ontology Extensions (SHOE)**: Small set of HTML extensions designed to give web pages semantic meaning by allowing information such as class, subclass and property relationships.
- **Web Ontology Language (OWL)**: Knowledge representation language that is characterized by formal semantics and RDF/XML-based serializations.

With the spreading of web services, dedicated languages for building Semantic Web Services ontologies appeared such as Web Ontology Language-Service (OWL-S). It enables users and software agents to automatically discover, invoke, compose, and monitor Web services. Another interesting work on ontologies is the Simple Semantic Web Architecture and Protocol (SSWAP) [45], which is an architecture for the Semantic Web based on REST mechanism and OWL. This decentralized protocol enables nodes to be autonomous in the discovery and inferencing of information. Ontologies have also proven their efficiency in IP-service discovery such as in [87].

Based on our network service organization as shown in Figure 3.1, an attempt of GNSO has been created and represents a possible classification of service that could be provided on ANs. This proposed ontology is currently divided into five categories – which could also be seen as classes:

- **Monitoring:** Services enabling to collect data from monitoring devices.
- **Connectivity:** Includes services offering a connectivity to an AN. It can be connection to Internet, to a walled garden or also to a VPN.
- **Management Control:** Services enabling to manage set of devices such as home automation, sensors, etc.
- **Content:** Services enabling to get access to specific content.
- **Privacy:** Services ensuring privacy of users such as authentication, certification, etc.

3.2 The Lightweight Service Announcement Mechanism

3.2.1 Principle

Based on the requirements made in the previous section, we propose a solution, called the Lightweight Service Announcement (LSA) mechanism, which allows PoAs to announce their service availability inside existing network discovery message – Beacon, Router Advertisement (RA), etc. In Chapter 2, we have seen that most access technologies use network discovery messages to advertise their presence to surrounding devices. These messages are sent at regular intervals, therefore, and as requested by **R3**, having a network service discovery mechanism based on these messages prevent from sending extra messages for discovering service availability. These messages contain different information regarding the advertised network and almost all of them are offering optional fields that could transport additional information. Therefore, we decided to use these discovery messages to transport network services information. Such enhanced discovery messages will then enable devices to discover service availability of a network at the same time they discover the network announcing them, along with its physical characteristics. Advertising information in discovery messages have been proven possible for instance in [21]. However, adding extra-information in network discovery messages is not as simple as it may seem as it increases the message payload and therefore, the signaling traffic load on the network. Some research [52] and [53] study the possibility to add information inside the non-used bits of a beacon. They have shown that it was possible to embed custom information – e.g. coupon, discount, etc. – towards mobile stations inside beacons and without increasing the beacon size. Despite the message size restriction, network discovery messages are the perfect place to include our network service announcements. That way, network service availability will be discovered simultaneously with the PoA as requested by **R4**. Moreover, this proposal enables to re-use existing messages and necessitate few modifications for current architectures, which would facilitate its use in existing ANs. However, an optimal trade-off has to be found between the message size and the extra-information relevancy. Furthermore, for access technology that do not use network discovery messages providing an optional field, the network service discovery will have to be made via an optional request/reply mechanism defined in the LSA mechanism.

Our proposal consists in adding standardized network service information inside network discovery messages in order to enable devices to perform a “service-based” selection of the AN. Moreover, this mechanism, associated with the proper decision mechanism, could help devices sort out ANs providing a given service and connect to the AN offering the best characteristics. In addition, they will be able to perform these actions for each service at any given time and in any given location.

Our announcement mechanism is aimed to be used with any type of devices evolving within a CHE. In this proposal, we defined two entities that will interact with each other to exchange network services information:

- **Service User (SU)**: A device that needs to collect information on service availability in order to select an appropriate AN;
- **Service Announcer (SA)**: A device that announces its service capabilities to others.

Note that any device providing a network service could be a SA and not only PoAs. In addition, a device can be at the same time a SU on a network and a SA on another. For instance, a mobile equipment sharing its cellular connectivity over its Wi-Fi interface, will act as a SU on the cellular network – discovering available services on this network – and as a SA on the Wi-Fi network – announcing the services available on the associated cellular network. Furthermore, with a service differentiation hypothesis and the popularization of multihoming, we assume that new SPs will emerge and announce their supported services to surrounding devices. These new SPs could for instance re-use several existing infrastructures to create a new virtual network [32] or they could insert gateway device into existing networks to offer a specific service as stated in [24] – where the IETF Homenet Working Group is describing the evolution of Home Networks (HNs) and its modifications proposal in order to satisfy this evolution. Hereinafter, we discuss the interactions between SAs and SUs.

In this proposal, SAs include in their network discovery messages a *Service Availability Announcement Tag* describing their supported network services. This mechanism helps SUs sort out relevant networks in terms of service availability and therefore determine which networks are worth connecting to. SAs connected to several ANs can regroup the supported services of each AN inside one tag. To limit the number of messages necessary for network service discovery this *Service Availability Announcement* tag is mainly planned to be included into periodic discovery messages – Beacon, RA, etc. However, we also imagine that request messages can be used to actively demand detailed information on network services. That way, this tag can also be included in other messages such as network solicitation messages – e.g. Router Solicitation (RS), Probe Request (PReq) – if they authorize optional information. SUs can therefore use such messages to specifically request ANs providing one or several network services to all SAs in their vicinity. SAs supporting at least one of the requested network services will reply to the SU.

Each network service is represented with a unique Network Service Identifier (NSID), which is composed of a Service ID (SID) identifying the network service and a Unique Provider Identifier (UPID), as shown in Figure 3.2. In fact, in a multiple providers environment, we believe that it is essential for SUs to be able to determine

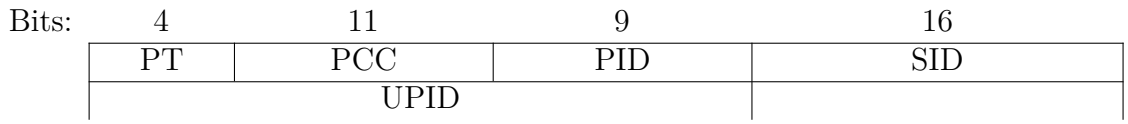


Figure 3.2: Representation of a *Network Service Identifier*

the provider deploying each discovered network service and therefore, to include a UPID in the discovery mechanism. This way, provider-dedicated nodes can ignore announcements from all providers except the one they belong to. Moreover, it will also allow providers to be able to announce their network services on other infrastructures. The UPID is divided into three fields:

- *Provider Type (PT)*: a code representing the type of provider, it can be an ISP, a specific SP, a content provider, a personal device provider, etc.
- *Provider Country Code (PCC)*: three digit code representing the country in which the service is deployed;
- a unique *Provider ID (PID)*.

In our network service representation, network services are described using attributes such as *NSID*, *Authentication*, *Cost* or *Requires*. For example, network services from the *Internet* subclass in Figure 3.1 provide an access to Internet. A SA may announce an instance of this subclass with the corresponding NSID and the following attributes: *hasValue:IPv6* and *samePropertyAs:EAP*. This SA is then informing that its Internet access supports IPv6 addressing scheme and requires an EAP-based authentication. This way, any SU receiving this announcement can determine that it needs to have credentials for the associated provider in order to have access to its Internet service. This classification enables SUs to determine whether the discovered SAs (and the AN associated) is of interest for their applications. These classes and attributes are not meant to be exhaustive and require to be further extended, but they offer a glimpse of what should the GNSO be in order for us to test the effectiveness of this mechanism.

3.2.2 Service Availability Announcement Tag

In the LSA mechanism, we propose to include a *Service Availability Announcement Tag* in optional fields of legacy network messages – RAs, Beacons, RSs, PReqs, etc. This tag, containing network service announcements, ensures that SUs discover simultaneously the service availability and the AN.

Figure 3.3: Representation of a *Service Availability Announcement Tag* as a TLV

Figure 3.3 is a TLV representation of this tag. The *Type* field indicates that this tag is a *Service Availability Announcement*. The *Length* field represents the tag size. The *Announcement Type (AT)* flag helps SUs determine which announcement type will be used. In fact, as any device must be able to use this mechanism, we defined two methods to build the *Service Information* field. These methods take account of the specificity of these devices. In the first type, the *Service Information* field contains the list of available network services' NSIDs, which is ideal for device looking for a specific service such as constrained device or for networks that do not have many services to announce. Otherwise, in the second type, this field contains the availability of the main network service categories extracted from the ontology. Upon reception of this type of announcement, SUs will be able to determine network service category availability. However, in most cases, this information will not be sufficient to select the AN based on service availability. Therefore, SUs will have to complete this information using request mechanism in order to retrieve either categories or services details from corresponding SAs, this way allowing SUs to compare available services if it is required.

3.2.2.1 NSIDs List Type

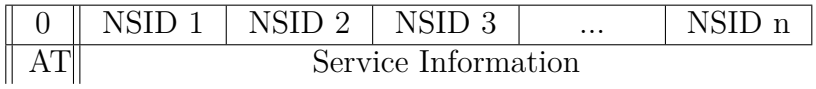


Figure 3.4: Representation of a NSIDs List *Service Information* Field

In this type of announcement, the *Service Information* field contains as much NSIDs as supported network services and the *AT* flag is set to 0 as illustrated in Figure 3.4. With this method SUs can directly determine if a SA is providing the desired service, as well as the provider offering it, as we recall that NSIDs also contain provider information.

This method avoids using additional messages as SUs directly have the list of supported network services included into network discovery messages. SUs have therefore no further action to perform for the discovery and can right away determine the target AN. This method limits then to the minimum devices energy-, time- and resource-consumption. It should therefore be preferred for announcement made to constrained devices as it will also simplify the number of actions required to perform their AN selection. However, the number of NSIDs includes in the *Service Information* field should be limited. This limitation will avoid increasing the size of messages transporting such tag and it will decrease the volume of information to be processed by SUs. The subset of NSIDs announced via the tag will then rotate to prevent from overloading discovery message as we will demonstrate later on.

3.2.2.2 Ontology Categories Type

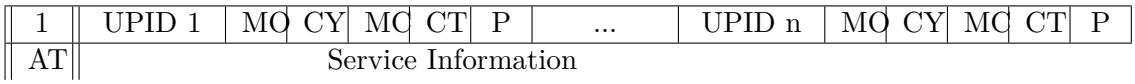


Figure 3.5: Representation of an Ontology Categories *Service Information* Field

On the other hand, if the *AT* flag is set to 1, the *Service Information* field contains as many flags as there are network service categories defined in the network service ontology. If a SA supports at least one service from a category it sets the corresponding flag to 1, otherwise it is set to 0. However, SAs may have to announce services from different providers, the *Service Information* field will then contain a list of UPID followed by the ontology categories' flags set for this provider as depicted in Figure 3.5.

This type of announcement only provides information on the categories of the available services, leaving it up to SUs to complete the network service discovery with extra messages if additional information is required. Therefore, the LSA mechanism needs to enable SUs to request details about network services supported by a SA – its entire list, a subset, a category or only one of them. If the technology used provides a solicitation message, SUs should use it to request service details from a SA. Otherwise, if the access technology used does not provide any request mechanism, SU will use a request/reply RESTful mechanism in order to retrieve details about supported services. Our choice is motivated by the simplicity that REST architecture offers. Moreover, REST architecture are based on well known standards such as URI, HTTP or XML, and it satisfies our requirements. For instance, a SU could send the following GET command in order to request details about all services from the Metering subclass of the Monitoring class, supported by surrounding SAs:

```
GET /SA/Monitoring/Metering
```

Targeted SAs will then reply by sending their current representation of the Metering subclass in the appropriate format. The previously mentioned SSWAP project based on RESTful architecture and OWL ontologies, is an example of the working association of REST mechanism and ontology. With this solution, a SU can request details about a list, a subset or one provider-specific service(s) by adding the corresponding NSID(s) in its request tag. It can also ask for a list, a subset or one specific service(s) by adding the corresponding SID(s) in its request tag. In the latter specific case, upon reception of replies, SUs will be able to determine the network service availability regardless of the provider. It is to note that access technologies that do not have network discovery mechanism, or that have network discovery messages that cannot be modified, will only be able to use the LSA mechanism to discover network service availability using REST request/reply messages.

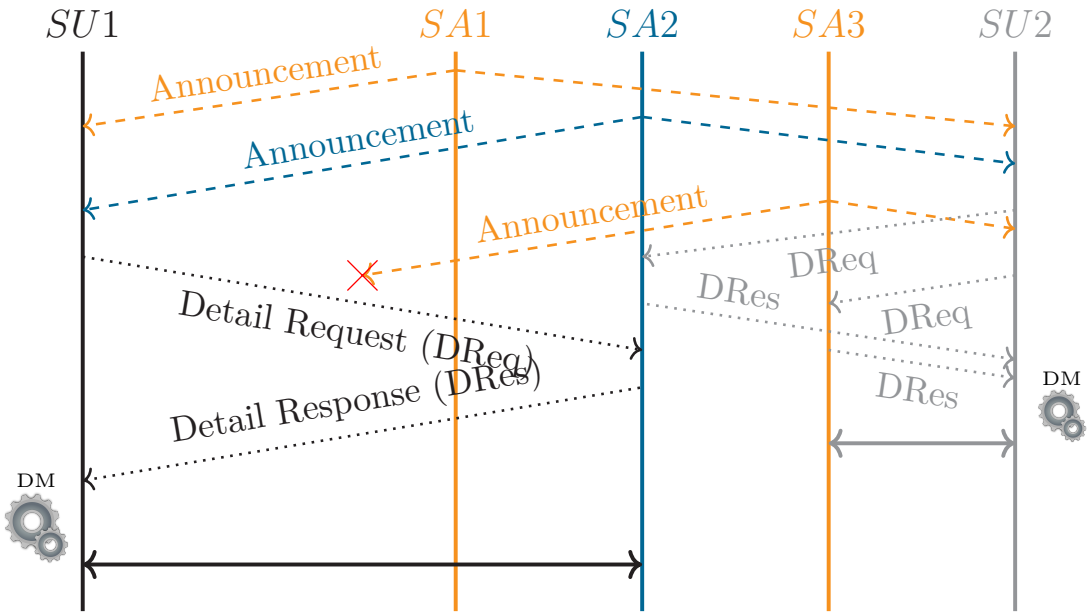


Figure 3.6: Service Discovery Sequence Chart

Figure 3.6 illustrates the interactions occurring using this announcement method in a scenario with two SUs and three SAs. This figure shows that SU1 upon reception of different announcements, ignores SA1 – even though this is the first SA it discovered – as it understands that SA1 is not providing the category of the desired service. That way SU1 does not exchange extra messages with SA1 – and so will not even try to connect to it – but instead exchange messages with SA2 that may provide the desired service. The decision engine of SU1 determines that SA2 is an appropriate AN. As a result, SU1 starts its connection process with SA2. In the same way, SU2 ignores SA1 but requests service details from both SA2 and SA3. Upon reception of their services details, and after the decision-making process, SU2 starts its connection process with SA3.

This second method is to be preferred if SAs have several network services to announce. Even tough, this method needs extra messages to complete network service discovery, the tag still enables SUs to sort SAs based on the supported network service categories. However, after requesting details, SUs have access to the entire description of a network service. This request mechanism has to be used by SUs that do not have any resource or energy constraint, and the replies enables them to perform a detailed comparison of available network services in order to select the best AN. Furthermore, category announcement enables SUs to limit the number of requests to send and the amount of details to process by requesting information only from relevant SAs. Moreover, it is unlikely that SAs will have services from numerous different providers to announce, however, if necessary and to avoid overloading any message, we also consider a rotation in the announced provider categories.

3.2.2.3 Fixed Tag Size

Regardless of the type of announcement used, the question of the tag size can be raised. In fact, in both methods, but more particularly with the "NSID list" type, the size of the tag can continuously increase and with it the size of network discovery messages. However, **R2** requests to limit the volume of exchanged data in order to limit the impact of the service discovery on both the network and on SUs. In order to be compliant with **R2**, we propose in the LSA mechanism to vary the frequency of a service's announcement depending on the importance given to it. In fact, some "critical" services, such as the ones associated with health care, need to be announced using a high frequency to ensure SUs to always discover them, whereas less critical services will not need to be announced as often. Each service will then be announced at a different frequency, defined by the provider.

As a consequence, a service could be announced in each network discovery message or in every n messages, depending on its delay tolerance. This frequency of announcements will impact the *Service Information* field as the list of NSIDs or the ontology category availability might be different for each network discovery message. In both case, the *Service Information* field of the announcement tag will be modified dynamically by the SA. Therefore, in the first type of announcement, the list will have a base of highly critical NSIDs to which other NSIDs will be attached. In the second type of announcement, the ontology categories associated to a provider offering an highly critical service will be the base of the announcement, and ontology categories of other providers will be appended depending on frequency associated to them. In order to avoid any misleading in the announcements only SAs and providers can modify the tag. For example, in a Wi-Fi scenario, users can rename the SSID of their residential Wi-Fi APs, which prevents providers from offering wide range services using these accesses to all their customers (devices not having anymore the mean to detect the provider an AP belongs to). Our service announcement mechanism will enable providers to always announce services, even if the SSID of an AP is different from the provider default one. Moreover, SU will always be able to determine the service availability as it will not be possible for users to modify service announcements.

This "announcement hopping" enables SAs to have more services advertised while bypassing the tag size issue as there will be a shifting in the announced services. Moreover, as SAs handle dynamic announcements, they will also be able to vary the announcement frequency depending on the situation. For example, a SA having too many SUs to serve for one service, will be able to vary the frequency of the associated service announcement, if possible, to force arriving SUs to find an other SA. Furthermore, considering that SAs can vary announcement intervals intelligently, this variation will also enable SAs to balance traffic load among other SAs of its vicinity.

3.2.3 LSA Properties and Advantages

The LSA mechanism makes it possible to announce network service availability to any surrounding SU and retrieve services' details within few messages. Re-using existing network discovery messages limits the impact of this new mechanism on both devices and ANs, which should favor its adoption. One of the biggest issue with growing diversity of ANs, is for a device to be unable to determine the appropriate AN to connect to. This inability to determine the appropriate ANs, which is emphasized when devices have multiple interfaces, may also lead devices to connect to ANs not providing the expected service. This situation will then require to perform other attempts until finding a suitable AN. The information collected with the LSA mechanism helps SUs filter relevant SAs, and associated ANs, in order to determine the appropriate network to use for a given application. Therefore, devices can no longer connect to an AN not providing what it needs for its applications, allowing them to conserve time and energy for other tasks. With our proposal, SU may also sort SA based on the provider announcing network services. This property will for instance allow provider to deploy dedicated devices pre-assigned with specific IP address, as providers will now be sure that these devices will only connect to ANs providing the expected network service. Therefore, the time and resource required to retrieve an IP address will be suppressed from the connection process leading to have simplified process for some dedicated accesses.

The LSA mechanism is based on an ontology classifying network services with their attributes and relationships. This ontology is used to build the *Service Availability Announcement Tag* included in network discovery messages and allows any SU to automatically interpret and understand network service announcements. Moreover, adding a new service in the announcement is fairly simple as it just requires to add it into the ontology instance managed by a SA. The LSA mechanism rests on two types of announcement, the first one preferred for announcement made to constrained devices, as it limits their energy and resource consumption; the other one is more adapted for announcement made to other devices and enables SUs to precisely compare available network services in order to select the appropriate SA. This network service discovery mechanism can therefore be used with any type of devices. Its low volume and low number of exchanged messages properties should fasten the discovery of service availability and then the selection of the appropriate SA.
The frequency at which a service is announced depends on the importance given to it. This "announcement hopping" ensures to have a fixed tag size and therefore, to not overload messages in which this tag is included. As a result, this mechanism also prevents from overloading the AN with signaling messages.

This dynamic service announcement provides the opportunity to leverage existing network infrastructures and generate additional revenues sources by renting announcements and access to others. In fact, we believe that some SPs might have an interest of not deploying their own infrastructures for providing a given network service and would rather re-use existing one to announce their services. For instance, an event planner may want to provide specific services during its events, but is likely to avoid deploying a network infrastructure for them as these events are temporary. Our solution would enable this planner to re-use existing infrastructures to announce its services and collect the associated data traffic. This planner, seen as a SP, after determining the area in which its announcements are required, can "rent" accesses from different and already present ISPs. Rented ISPs will then provide slots for announcing these new services inside the announcements of their participating PoAs, as well as a "restricted" access towards the event planner domain. Therefore, this proposal can help deploy several types of services by re-using the multitude of already existing infrastructures. This access-renting scenario is ideal for deploying temporary network services and could notably be used to monitor a race, a festival, etc. However, its usage will strongly depend on the "renting" price and fairness offered by the different providers.

The proposed announcement mechanism also offers the possibility to announce any type of services on a network even if not owning the corresponding AN and without renting announcements. For example, a content provider could provide an access to its specific content using a device, which will be placed inside a given network. With our solution, this device will be able to understand received announcements from ISPs, and use one in order to reach its provider domain. Simultaneously, it will be able to announce its own services in this network. The LSA mechanism is facilitating any SP to announce their network services on infrastructures that are already deployed using specific devices. Therefore, our mechanism can increase the "catalog" of available services in an existing network.

More generally, the LSA mechanism enables devices to sort PoAs based on service availability. Therefore, devices using this mechanism are separating out the environment depending on their needs. This closely resembles the method described in [32] as our mechanism enables SUs searching for a specific network service to simplify their vision of a CHE. Figure 3.7 illustrates this service-based separation. In this illustration, there are two ISPs, each of them having several SAs, which announce the network services provided by their ISP. An other SP is renting announcements and accesses on some SAs of this area to announce its network service. The LSA mechanism enables SU to sort out relevant SAs depending on the desired service. As a result, it allows providers to "create" Service-based Virtual Access Network (SVAN). In this example, there are three SVANs corresponding to the availability of one or a set of network services. As a consequence, and depending on the desired service, the SU vision of the environment is virtually modified but above all simplified.

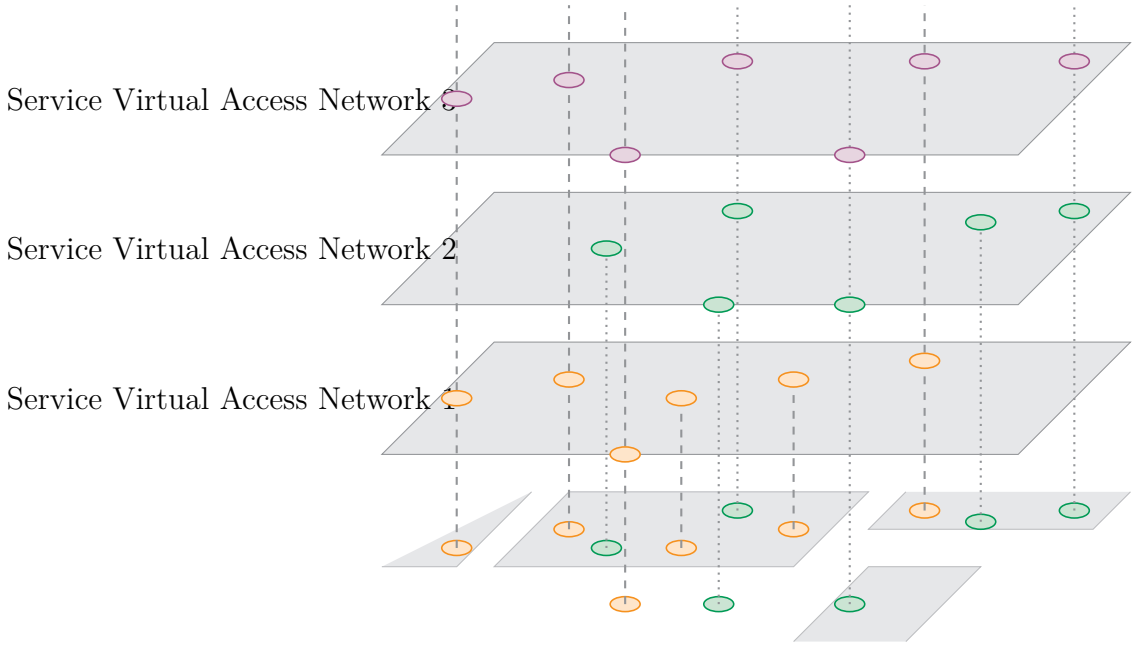


Figure 3.7: Illustration of Service Virtual Access Networks

A SVAN may be fixed (such as network services announced by an ISP) or it can be dynamic and depend on renting policies of SPs.

For example, an Energy provider could offer to its customers, devices to monitor and manage the energy consumption of their buildings. This energy monitoring solution can be based on a set of devices metering and controlling the energy consumption of the building, the Metering Devices (MDs). This Energy provider, with the LSA mechanism, can announce services inside targeted networks without having to set up its solution and all its MDs on site. In fact, one device will announce this energy monitoring service, and will act as the gateway between the Energy provider domain and the MDs. It will use Internet connectivity of the building, discover via the corresponding announcements, to receive commands from and send the collected data to the Energy provider domain. The MDs will be pre-configured to search for the Energy provider specific service, announced by the gateway. The collected data could be locally analyzed by the gateway and represented in a more meaningful information, and/or analyzed by the Energy provider for a more global interpretation.

Finally, even though the possibilities offered by the LSA mechanism are limitless, devices that do not base their network selection on service availability can simply ignore this tag as it is optional – i.e. this mechanism is entirely backward compatible.

3.3 A Complete Framework for Multihomed User Device

In this section, we present a complete framework designed to help user device with multiple interfaces dynamically manage their connections. By associating the LSA mechanism with a decision algorithm, a flow distribution protocol and a routing mechanism, we show that a user device could fully benefit from all the possibilities offered by a CHE.

3.3.1 Problem Statement and Possible Use Case

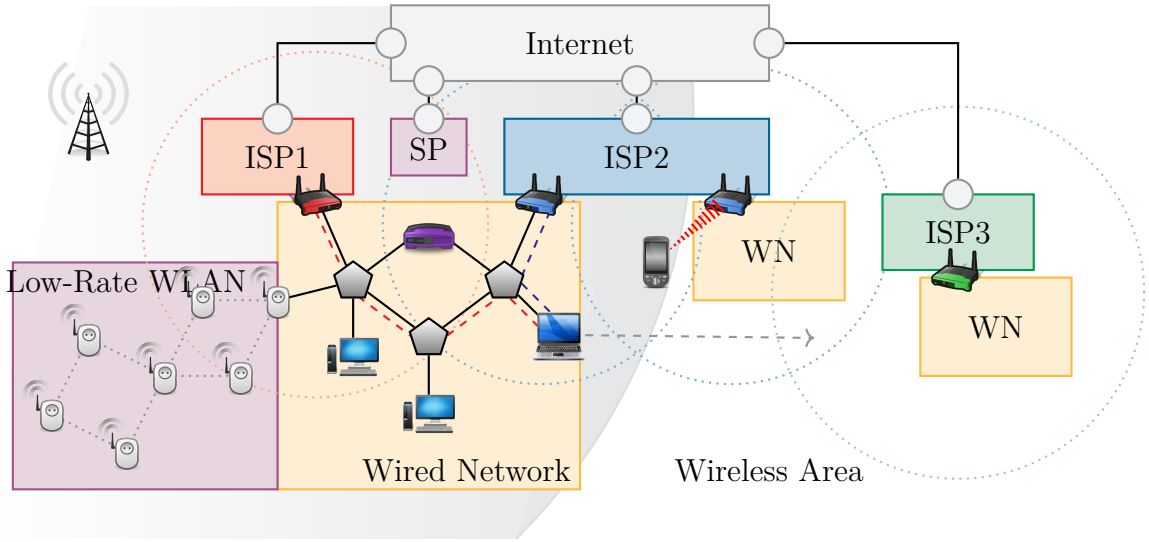


Figure 3.8: Multiple Interfaces User Device Use Case Illustration

User device with multiple interfaces could take advantage of the increasing diversity of available ANs. Figure 3.8 illustrates a possible multihomed scenario where the LSA mechanism associated with proper mechanisms could help user devices with multiple interfaces have a better management of their data flows. In this use case, a SU, represented in Figure 3.8 by a laptop, is connected to a wired network which have access to two SAs, the first one SA1 belonging to ISP1 and the second one SA2 belonging to ISP2. Each SA announces its network services, which might be different, and the SU has two on-going data flows – depicted as blue and red dashed lines on the figure – that need to be routed to the SA announcing the corresponding service, i.e. SA1 and SA2 respectively. The SU is then moving from the wired area to a wireless area and is willing to continue its on-going traffic flows. In the wireless area, the SU receives announcements from newly discovered SAs. These announcements show that the new SAs support the network services required by both type of on-going data flows. The SU should therefore be able to re-assign them on the appropriate wireless interfaces and continue its sessions. In order to accomplish such

a scenario several mechanisms are required as explained below.

The LSA mechanism helps SUs retrieve ANs information – i.e. network service availability – in addition to their physical characteristics, which enables SUs to compare available network services. With the appropriate mechanisms, this comparison would ensure SUs to always select and connect to the best possible SA, and the associated AN, for each application and regardless of the access technology used. Therefore, in addition to the LSA mechanism, proper decision algorithms, flow distribution and routing mechanisms are required, in order to enable devices to perform a per-service AN selection and connection. These mechanism will then help devices be ABC for a given service, at any given time and in any given location – or what we called Service-based Always Best Connected (S-ABC) in Chapter 2. In the following section, we propose a complete framework to guarantee SU to be S-ABC and enabling them to:

1. Retrieve network service information;
2. Determine the best AN for a specific traffic flow regardless of the technology used;
3. Dynamically assign flows to the selected interface;
4. Have their traffic flows routed accordingly in multihomed wired networks.

Content adaptation is not considered in this framework as we assume that the LSA mechanism allows SU to select network that could transport traffic flow as is. Furthermore, this framework is not adapted to IoT devices as it requires additional components and resources. That is the reason why this section focuses on resource-capable devices with multiple interfaces.

3.3.2 Framework Design

This framework is divided into three chronological phases: *Information-gathering*, *Network-Selection* and *Routing*. First, in the *Information-gathering phase*, SUs have to determine network service availability for each discovered ANs in order to include the gathered information into their AN selection process. This phase will be handled by our LSA proposal and will not be further discussed as it as been presented in the previous section. After having collected all the required information, SUs have to select the ANs that will be used for each application. This second phase is called the *Network-selection phase* and requires a decision engine and a flow distribution mechanism. The two first phases are continuously repeated, even if the SU is already connected, in order to ensure to be always best connected in any given location and for each application flow. The last phase to fulfill our objective, called the *Routing phase*, allows routing protocols of multihomed wired network to route packet flows to the proper SA in order to avoid any unjustified packet loss. The *Network-selection phase* and *Routing phase* will now be detailed.

3.3.2.1 Network-Selection Phase

After the *Information-gathering phase*, SUs have received all the required information on available ANs (in terms of network services and physical capabilities) in order to determine for each running application which AN will be used. Before starting the selection process, SUs have then to associate these information with corresponding interfaces, or more precisely with corresponding IP addresses. In fact, due to the multihomed nature of the environment, devices might have several IP addresses per interface. Therefore, SUs have one or several network services associated with one or several IP addresses. The network selection then comes down to the selection of an IP address – and of the associated interface – for each application. During this phase, devices require to *a*) store the information gathered per IP address; *b*) select the most appropriate IP address for each application; and *c*) assign the corresponding traffic flow to the IP address, and if necessary dynamically.

Network services are described with different attributes that will be taken into consideration during the decision-making, along with the physical characteristics of the network announcing them. In addition, SU, that can be mobile, could detect a better network service/AN characteristics on another interface, and this at any given time. In such scenario, SUs will constantly have to compare network service/AN combination in order to determine the best one for a given service. The decision-making is therefore a dynamic multiple-source and multiple-criteria problem, which can be taking care of using the Multi-Attribute Decision Making (MADM) technique [115]. This method has already proven its efficiency in network selection among a set of available alternatives during wireless handover in [103]. Ismail et al. propose a comparison of different MADM methods in [71] and conclude that the choice of the best method depends on the parameter – bandwidth, delay, loss – that needs to be highlighted. Therefore, we decided that our framework will rely upon this technique, and its optimization, to realize the decision-making.

However, this technique will only help devices determine the target network and does not provide any solution to assign – or re-assign – flows on the appropriate interface – IP address. Different solutions exist to maintain traffic flow while assigning it to a different interface and solve either multihoming, mobility or both such as discussed in [46]. These solutions can be divided into two groups: the network-centric or network-assisted solutions among which we found Mobile IP (MIP)v6 [94] and its extensions [4], Location Independent Network Architecture for IPv6 (LIN6) [106] and its extensions [84]; versus the host-centric solutions among which we found Site Multihoming by IPv6 Intermediation (Shim6), Host Identity Protocol (HIP) and Stream Control Transmission Protocol (SCTP). We have not considered network-assisted solutions for this framework, as we want to limit its impact on infrastructures that have been already deployed. And that is the reason why we will focus on host-centric solution in the following.

SCTP [104] is a transport protocol with a multihoming features which enables nodes to connect concurrently to several interfaces, giving these nodes the possibility to balance their traffic flows on any of the connected interfaces. This protocol, along with enabling devices to realize vertical handovers, decreases the delay and jitter usually occurring when performing them, as shown in [15]. It can also be enhanced to avoid the slow start phase on newly used link as mentioned in [79]. With this enhancement, this protocol ensures devices to have a steady traffic rate even when changing the type of access technology. However, SCTP will only be efficient for applications using it as their transport protocol, which limits its potential usage. In fact, in order to be widely use and benefit from such improvements, enhanced-SCTP will have to be embedded in all devices, and current applications will require to be modified to function with it. Unfortunately, we were looking for a solution that would need as few modifications as possible on both devices and applications.

The other host-centric solutions mentioned propose to separate the end-point identifier and locator role of IP addresses. In fact, an IP address can be divided into two parts: a prefix and a host identifier. It is therefore not surprising that these addresses are used to both identify and locate nodes. IP addresses are used as locator at the network layer, their prefixes enabling devices to determine the location of the node in the network. And simultaneously, the complete address, prefix and host identifier, are used by upper-layer to uniquely identify a node. If these two functions are separated, nodes will be able to change their location without having to change their identifier. As a result, nodes will be able to switch from different IP addresses at lower-layer without breaking the connection at upper-layer.

HIP [89] is a shim protocol acting below the transport layer. Based on this separation concept, it introduces a Host Identity (HI) used, as its name supposed, to identify the node, the IP address being therefore only used as a locator. HIP provides mobility supports as well as multihoming, and with proper signaling mechanism, it enables devices to fasten handovers as stated in [102]. This protocol offers high secure methods as HIs are cryptographic key and HIP messages are signed. However, using HIs implies to be able to associate each HI to the corresponding locator – i.e. an IP address. In fact, with such protocol, applications will be using HIs to identify a device but will not have the means to "reach" it as the HI is not a locator. An association table and a HIs resolution is therefore needed to be able to use this protocol, as shown during technical experiments in [62]. Even though, HIP provides multihoming and mobility supports for all transport protocols, it also supposes that all applications and devices should be modified in order to use HIs.

Shim6 [93] is an other layer 3 shim approach and protocol providing locator agility below transport protocols. It enables multihoming for IPv6 site with fail-over and load-sharing properties by setting up states with each peer hosts. It allows com-

munications to continue when a site, that has multiple connections, experience an outage on one of its connections or discover new possible connections. It separates the identifier and locator role of an IPv6 address in the upper-layers to ensure to be able to change the IPv6 address at the network layer without breaking on-going connections. The identifier is an IPv6 address chosen among a set of IP addresses composed of all the IP addresses available when starting the application. This identifier stay unchanged until the application stops even if the IPv6 address used as locator is changed. Shim6 enables devices to preserve established sessions by keeping a set of available IPv6 addresses, and therefore can be used in both multihoming and mobility scenario, as studied in [29]. Just like SCTP, Shim6 can be enhanced to provide better delay and jitter performance during handovers as proposed in [30]. Applications can benefit from this protocol without requiring any modification, as they still use an IP address. Only devices need to be modified in order to support Shim6 [43].

In this way, Shim6 is the protocol requiring less modifications on both devices and applications, and so Shim6 is the ideal protocol to complete the *Network-selection phase* of our framework. Information on each SA gathered previously will be associated with each locator pair. Shim6 would therefore be able to distinguish available locator pair and generate set of addresses for each network service. In that case, Shim6-capable SU will be able to use a different IP address, if there are any, should the original one experience failure or if a better one is found, without breaking the session. It ensures devices to select the appropriate locator pair for each application and network service. In addition, Shim6 offers the possibility to switch IP addresses regardless of the access technology used below them. It also helps maintain the connectivity when SUs discover and/or select a new AN.

Effectiveness and advantages of Shim6 has already been proven in [11] or [90] and can be easily deployed as it does not require modifications as regard of applications or network infrastructures. It should be enhanced with specific MADM decision algorithms to perform optimal selection when facing multiple criteria decision, such as the one described and tested in [18]. Finally, Shim6 is completely backward compatible as Shim6 nodes can communicate with classical IPv6 nodes, however multihoming support will not anymore be ensured.

3.3.2.2 Routing phase

As soon as SUs have selected the IP address to be used for an application in the *Network-selection phase*, it can start sending the corresponding traffic using this address. With this framework, devices are supposed to use one or several IP addresses simultaneously and more particularly regardless of the access technology used. However, most PoAs, implement “Ingress Filtering” [9] to avoid some attacks. Therefore, they are not supposed to forward traffic if the source IP address of the

corresponding packets does not belong to the PoA addressing scheme, i.e. address using a different prefix. This situation is likely to occur in a multihomed context as devices have multiple IP addresses, and in particular, inside "not actively managed" wired network, as mentioned in [24]. In these type of networks, packets are principally routed to the closer CER based on their destination IP address. However, if the closer CER has not delegated the prefix of the source IP address of an incoming traffic, associated packets will simply be dropped. In order to avoid such unjustified packet loss in a multihomed scenario, which may result in subsequent delay in packet transmission or even in the impossibility to establish the communication, our framework needs to deal with this specific issue.

This situation will mainly occur in wired network as devices do not need to pair with a specific CER before sending their traffic, contrary to wireless network. In order for wired SUs to be able to dynamically toggle from one available IP addresses of their wired interfaces to another, routing protocols need to be able to determine the shortest route to the appropriate SA for each packet. Several solutions exist such as tunneling the traffic [58] [35], modifying packets header [110], modifying internal routers [8] or modifying the network architecture [77]. However, they add non-negligible complexity to the network. Gallet de Santerre et al. in [41] takes into consideration packet source address when default-route is involved in the site routing decision. Their proposed solution, called SDSA, also modify internal routers but only used two routing tables contrary to [8]. This simple mechanism prevent the ingress filtering issue from occurring, while being easily set up in any routing protocol and without increasing the routing complexity.

3.3.3 Enhancement of Existing Services

Our proposed framework composed of the LSA mechanism, Shim6 enhanced with MADM technique and SDSA solution, enables multihomed user devices to automatically determine and connect to the most suitable AN. The selection depends on the needs of each used application and if possible, session continuity can be maintained even if devices used different AN along the session. The LSA mechanism enables devices to retrieve network service details and so, to sort out relevant AN. The other aforementioned protocols offer devices the possibility to fully take advantage of all surrounding networks and their capabilities for each application separately. In particular, this framework can re-define usage of some current services.
This framework can first be useful for resource-capable devices as it will help them maintain their sessions for each network service, depending on their penetration rate and with the best available AN. The decision algorithm and flow distribution mechanisms ensure that these devices will only break sessions when there are no more ANs supporting the expected service. Therefore, if a network service is provided with an almost ubiquitous penetration, applications using this network service will then fully benefit from such a framework. In that way, this framework can help resource-

capable devices take the best of available ANs in several scenarios. For example, we can imagine that a health monitoring service could be announced on several ANs, leading user of such service to always be monitored even if an AN is not available. This framework could also help network infrastructure have a better management of their infrastructure. In fact, we can forecast that with this framework cellular operator could plan to offload some of the cellular traffic on another AN. These networks can therefore advertise that they *a*) support the transport of this specific type of traffic, and *b*) require prior authentication on the cellular network. This way, users having access to a specific service with their cellular subscription, using this framework, would be capable to detect other networks in their vicinity – probably on other interfaces – that can offload the corresponding traffic. The user device will automatically understand that it has first to authenticate on the cellular network, but that it can retrieve the corresponding traffic from another network with the obtained credentials.
Several other network service are conceivable with this framework that might enhance usage of current services in multihomed environment.

3.4 Chapter Outcome

The Lightweight Service Announcement (LSA) mechanism is evolutionary technology-wise and enables any device to uniformly announce their support for specific network services to surrounding devices. Devices receiving these announcements could therefore select the best possible AN based on the discovered network service availability and regardless of the technology used.

The LSA mechanism is based on a *Service Availability Announcement* tag, which is mainly inserted in network discovery messages. The tag size is limited to prevent from increasing the payload of network discovery messages and so, overloading the network with signaling messages. This mechanism enables devices to receive the network service availability at the same time they discover the associated networks, which offers several advantages in addition to perform a service-based selection.
First, it enables devices to sort ANs based on their network service availability and ignore any AN that are not adapted for a given application. Therefore, this mechanism allows to virtually simplify the network environment based on network service availability. This way, it prevents devices from attempting to connect to an AN not providing the desired service and it helps them focus only on relevant one. This virtual separation can further be narrowed down based on providers offering the available network services. This way, it ensures that provider-dedicated devices ignore any announcement but the one from their providers. In addition to filtering ANs, the LSA mechanism enables devices to specify their selection not only on the physical characteristics but also based on their needs and depending on network services information. It allows to further limit the interactions to only potential ANs and therefore, provide a more efficient and faster selection process.

The tag of this mechanism is based on an ontology and can be built for two type of devices: constrained devices, which need low-resource, -time and -energy consumption mechanisms; and user devices, resource-capable and without specific constraints. This tag technique, associated with simple request/reply messages – either by re-using legacy messages or based on REST mechanism – enable to adapt and use this mechanism on any access technology. In particular, this request/reply mechanism helps devices have more detailed information on available network services in order to compare them for different ANs. As mentioned previously, the LSA mechanism allows devices to sort ANs, it ensures to minimize the amount of exchanged messages in order to retrieve network service availability by limiting the requests to only relevant networks.

The LSA mechanism can also be associated with existing protocols in order to define a complete framework for user devices to always select and connect to the best possible AN and to ensure, when possible, connections survivability. The LSA mechanism and its advantages opens new horizons for business applications. It can enhance the usage of current services while facilitating the emergence of new Service Providers (SPs) and the deployment of new services. For instance, it allows SPs to announce and provide their services by re-using infrastructures that are already deployed. In such scenario, SPs will provide a nearly-ubiquitous service connectivity among different types of network to users. Therefore, each Point of Attachment can be used for different usages, they might have their main legacy usage – for instance providing an Internet access to their customers – and at the same time, offer a "restricted" access for other usages/providers.

However, despite all the possibilities that the LSA mechanism and the associated framework offer, their adoption will strongly depend on the fairness between providers. In fact, these solutions suppose that all providers "correctly" announced their supported network services and that they provide a restricted access for others in order to ensure seamless and ubiquitous service access.
For all that, possibilities in terms of services are limitless as announcements can be performed on different types of networks. We can imagine several services such as:

- Health monitoring, temporary re-using residential Wi-Fi APs to cover specific area in order to follow the health state of patients;
- Controlling Home Appliance, providing a full set of devices to monitor and manage home electrical consumption. Monitoring devices will have their own networks within the HN. And they will use the Internet access to send monitored data;
- M2M monitoring, re-using residential Wi-Fi APs to collect data generated by M2M nodes.

This last example has been intensively studied in particular to determine the impact of announcement frequencies and APs density over the time needed to discover a service. This study, based on real-world data, is the object of the next chapter and helps determine the validity of our proposal.

3

4

Modeling the Case for Single Interface Node

The number of devices connecting to current network systems is increasing as device features and application-ranges improve. This trend will only increase due to the massive arrival of Internet of Things (IoT) objects, which have their own distinctive features such as hardware limitations and energy constraints. These objects differ from today's standard devices not only because of their limited features, but also because of the type of traffic they produce (from very low to high volume and at regular intervals or trigger by an event). But, because current access technologies are not designed to support such high number of constrained-devices, dedicated architectures have therefore to be rolled out to transport such traffic. Nonetheless, M2M devices could also benefit from the plethora of existing ANs, instead of adding even more complexity to the environment. However, as mentioned in the Chapter 2, existing access technologies, and more precisely connection process, require to be adapted in order to simplify access modes.

In Chapter 3, we described a network service announcement mechanism Lightweight Service Announcement (LSA), which enhances the information provided by network discovery messages. This mechanism can be applied to different scenarios in order to simplify the detection of available network services and therefore Access Network (AN) selection.

In this chapter, we will prove the effectiveness of the LSA mechanism in single-interface device applications. To do this, we will study the impact of LSA mechanism by deploying specific services in an existing Wi-Fi environment. The Access Points (APs) within this environment, in addition to providing usual Internet access, were also used to collect traffic generated by moving IoT objects. This study is primarily based on two Markov chains used to model such scenario and instantiated using empirical data. The aim of these mathematical models is to highlight how both the Wi-Fi environment and the service announcement impact the amount of time necessary to detect a specific network service and the ability of IoT objects to successfully transmit data.

This chapter is organized as follows. In Section 4.1, we give a detailed explanation of the IoT data traffic retrieval scenario. The following section focuses on confirming the credibility of this scenario by simulating the impact on legacy Wi-Fi users when re-using Wi-Fi APs for collecting IoT data traffic. In Section 4.3, we characterize Wi-Fi deployments based on real-world measurements collected during several war-driving campaigns. These characterizations are then used in Section 4.4 to instantiate the Markov chain models and thus determine the validity of this scenario in terms of both detection time and detection probability for a specific service. Before concluding this chapter, we present and discuss the results obtained in our mathematical study in Section 4.5.

4.1 Reusing APs to Collect New Services Traffic

A new concept, which has been gaining popularity in the recent years, is the sharing of Wi-Fi connectivity among the members of a given group – CNs. The CNs are built around the notion of a Virtual Wireless ISP (VW-ISP) with a dedicated, and recognized Wi-Fi SSID that is announced by every participating AP in addition to the user-defined one. The ISP behind this CN provides credentials (typically user name and password, but can also be based on certificates, etc.) to its clients, which allows them to connect to the VW-ISP. It is important to note that this type of service is different from "free-for-all", open Wi-Fi networks. For example, all major ISPs in France offer to their customers the possibility to participate to ISP-wide CNs [19], which given the significant high-speed Internet penetration rate, provides an almost ubiquitous access. FON[1] offers the same kind of service in several countries such as the UK or Japan.

In this scenario, we introduce the role of a company that will deploy IoT objects in an given area to collect data on their environment. We consider that these objects are mobile and need to connect to an AN to transfer their monitored data. We can imagine that this IoT company does not possess any network architecture in the area where its objects will be deployed. This would therefore imply that the company must either deploy a network architecture in the area or rent "access" to existing APs to have a service which will function much like that of a CN.

We can assume that several ISP Wi-Fi networks are available in the area in question. In this scenario, we propose to re-use this existing Wi-Fi architecture for transporting IoT communications such as M2M data traffic. The company will then rent the access offered by all or some of the APs within the area in order to collect the data traffic from its IoT objects. APs participating in this service will announce it along with their own services via the LSA mechanism. Conversely, IoT objects will look for announcements that provide this service to connect to the associated AP.

[1] http://corp.fon.com/

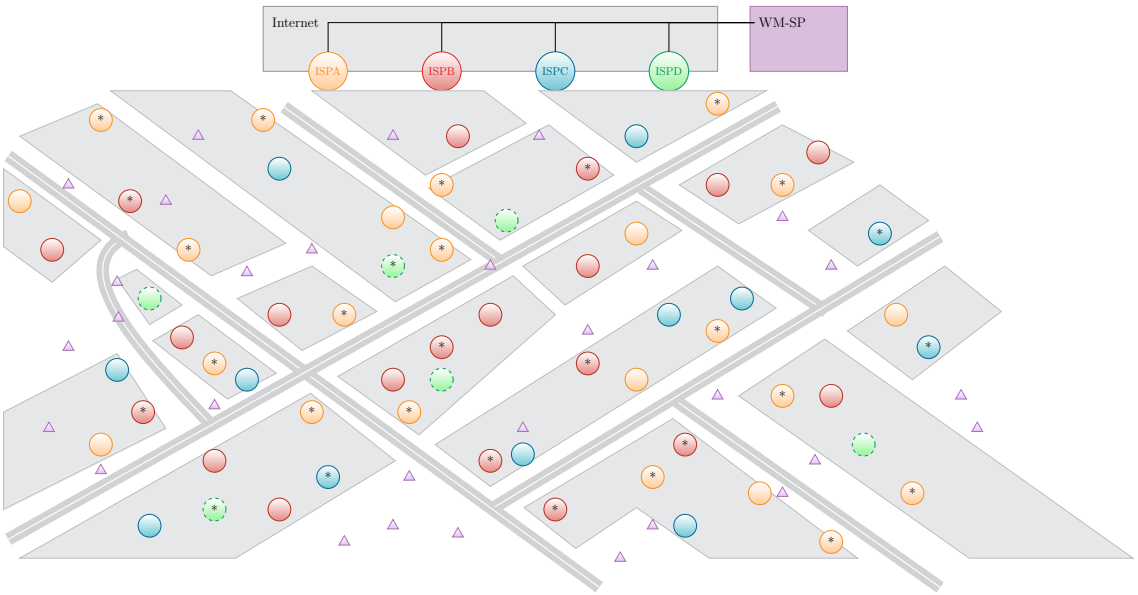


Figure 4.1: Representation of the WM-SP scenario

After the connection process, these objects will be able to transmit their data. Participating APs will then securely forward this traffic data to the company domain, for instance via a tunneling mechanism. This type of data transfer must be defined by the company with the ISPs. This scenario is illustrated in Figure 4.1 with circles representing APs positions – each color corresponds to a different Wi-Fi ISP – and triangles representing the IoT objects deployed by the company. APs announcing this data collecting service are marked with a black star.

It is probable that the company will have to rent access to different ISPs in order to provide seamless and ubiquitous access to its mobile objects. The APs used in this scenario are actually equipment used in the homes of private individuals for their own Internet access and might belong to different providers. However, Internet providers cannot ensure uniform coverage, as illustrated in 4.1, as the presence of an ISP depends largely on the location of their customers. Each participating AP provides a legacy Wi-Fi network, giving Internet access to users with the appropriate credentials, and at the same time, offers “restricted” access for the company’s IoT objects.

This scenario raises the question of how IoT data traffic could impact legacy customer data traffic. This will be addressed in the following section.

4.2 Impact on Legacy Wi-Fi Users

Before studying the impact of the LSA mechanism, it is crucial to determine whether or not this scenario will be effective in practical applications, for example, whether or not Wi-Fi APs can collect IoT data traffic without impacting traditional H2M or H2H communications. This is essential especially in light of the Pötsch et al. [95] study which showed that high volumes of M2M nodes, despite low-volume traffic, negatively impact the performance of even best-effort traffic on LTE networks.

4.2.1 Characterizing traffic load

So many different types of applications are possible with the IoT, especially in fields such as logistics, health, etc. Due to the diverse range of applications, characterizing the traffic generated by IoT objects is very difficult. In order to model this type of traffic, our research focused on M2M traffic characterization and related studies in the literature.

In [100], Shafiq et al. traced traffic on 2G and 3G networks, providing data on the traffic generated by smartphones and M2M devices. They were able to categorize and quantify different types of M2M traffic. As predicted, they noticed that the traffic volume produced by M2M devices is much lower than the traffic produced by smartphones. Moreover, they observed that the presence and volume of M2M traffic could vary significantly from one category to another. However, as [95] stated, the authors observed that the growing number of M2M nodes would quickly become an issue for these networks. In addition, this study confirmed that M2M devices, act as "content producers" with uplink traffic volumes higher than downlink traffic volumes. This is in stark contrast with smartphone – H2H or H2M – traffic. Their study also sheds light on the contrasting relationship between session duration and the inter-arrival of traffic, showing that the longer the session, the fewer session arrivals occur. Finally, these traces show that most M2M devices are confined to a specific area, i.e. they are less mobile than cellular devices.

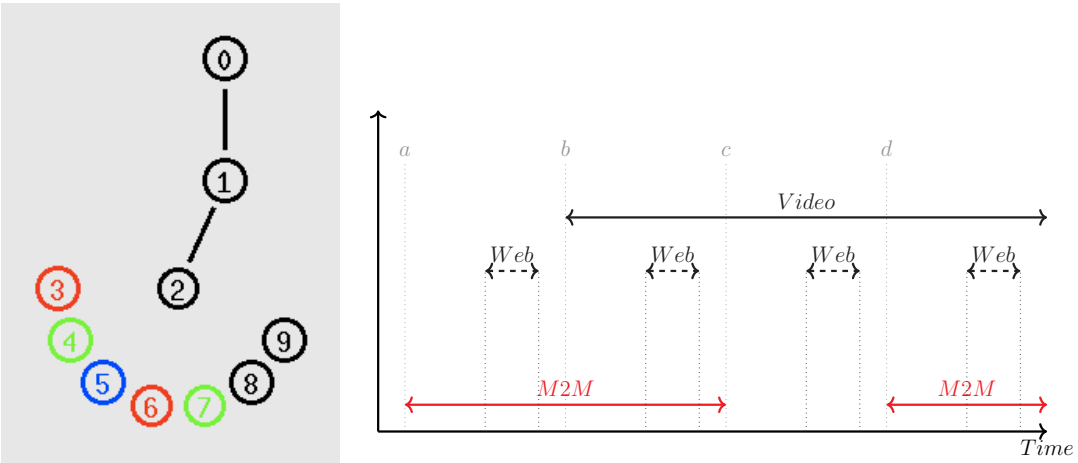
IoT applications can be separated into two main categories: "event-driven" applications and "scheduled" applications [86]. In the first category, objects generate traffic when an expected phenomenon occurs, whereas in the second category, traffic is produced at regular intervals. The "event-driven" category could explain the irregular and intermittent nature of some M2M traffic described in [100]. However, we can use the measurement analysis performed by Shafiq et al. to conclude that the characteristics of M2M traffic strongly depends on application and that it can vary significantly from one application to another. For example, a health monitoring system will generate much more data volume, and at more frequent intervals, than a room temperature monitoring system. However, modeling the irregular nature of an M2M traffic is not simple, as shown in [86].

For our purposes, we chose to focus our M2M traffic modeling on "scheduled" applications. In [49] experiments were performed to monitor the health statistics of elderly people. They used Electrocardiogram (ECG) sensors to track participants' heart rates. These sensors generate $12kB$ packets at a rate of $4.8kbps$. Pötsch et al. [95] used a similar model in their simulations with nodes generating a $6kB$ sized packet every 60 seconds.

Although this traffic volume is not representative of all possible M2M traffic, we considered a similar traffic volume of $6kB$ every 10 seconds for our simulations. This mid-range traffic volume was implemented in Network Simulator (NS2) and enables us to determine its impact on regular Wi-Fi H2H and H2M traffic.

Three scenarios have been simulated in NS2:

1. 1 AP, 1 H2H station generating traffic equivalent to video streaming (bulk transfer) and 1 H2M station generating traffic equivalent to web browsing (file transfer);
2. Scenario 1, in which we add 5 M2M devices generating traffic at regular intervals;
3. Scenario 1, in which we add 20 M2M devices generating traffic at regular intervals.



(a) Topology

(b) Phase Representation

Figure 4.2: Simulation Model

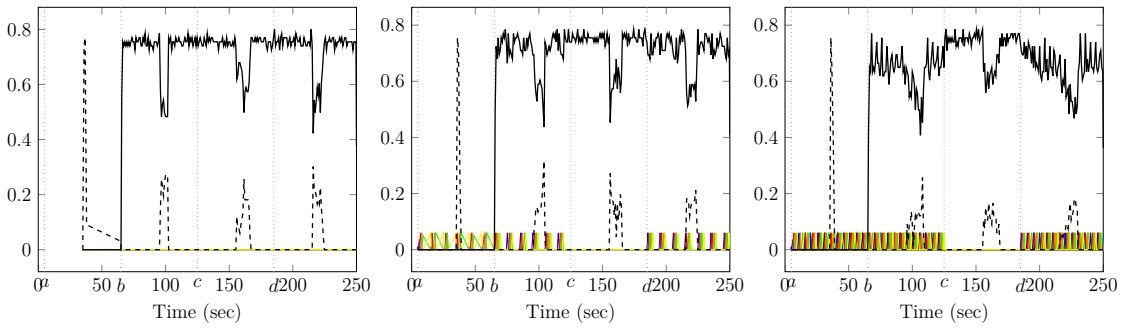
Fig. 4.2a illustrates the topology of the second scenario. The colored nodes (from node 3 to 7) are M2M nodes that upload traffic to node 0 via the AP (node 2).

The black mobile nodes, i.e. nodes 8 and 9 in the figure, represent individual Wi-Fi users. Node 8 is continuously downloading data from node 0. This traffic, modeled as a Transmission Control Protocol (TCP) bulk transfer, is comparable to the traffic produced by video streaming especially in terms of network load. Node 9 downloads data from node 0 at regular intervals. Traffic received by node 9 is equivalent to a recurring web page update. The latter was modeled as the transfer of $175kB$ – this is the average kB per page value obtained via Google Web Metrics [48].

The number of nodes involved in our simulation may seem low compared to the influence study carried out in [95]. However, we believe that in our Wi-Fi M2M traffic retrieval scenario, the number of nodes will not be as high as in a cellular scenario. First, LSA enables APs to dynamically vary service announcements, which will, as mentioned in Chapter 3, allow them to lower the frequency of an announcement if the number of nodes being served reaches a certain threshold. This prevents APs from being overloaded with M2M traffic. Furthermore, in a Wi-Fi network, we observed that home APs can manage a maximum of 20 simultaneous connections. However, Blinn et al. in [13] showed that on average a Wi-Fi HotSpot only has 7 simultaneous connections. We can therefore assume that the number of nodes simultaneously connected to a home AP should be less than 20 simultaneous connections, to ensure better performance.

We have divided each simulation into four phases, a, b, c and d, as shown in Figure 4.2b. The file transfer traffic appears in the middle of each phase while the bulk transfer traffic is only present in the last three phases (b, c and d). There is no M2M traffic in *phase c*. Separating the phases in this way enables us to study the impact of M2M traffic on ongoing and upcoming legacy traffic. The three scenarios – no M2M nodes, a small number of M2M nodes and several M2M nodes – can be compared to clearly estimate the impact of M2M traffic over usual traffic.

4.2.2 Simulation Results



(a) without M2M traffic (b) with 5 M2M traffic (c) with 20 M2M traffic

Figure 4.3: Sent and Received Throughput (Mbps)

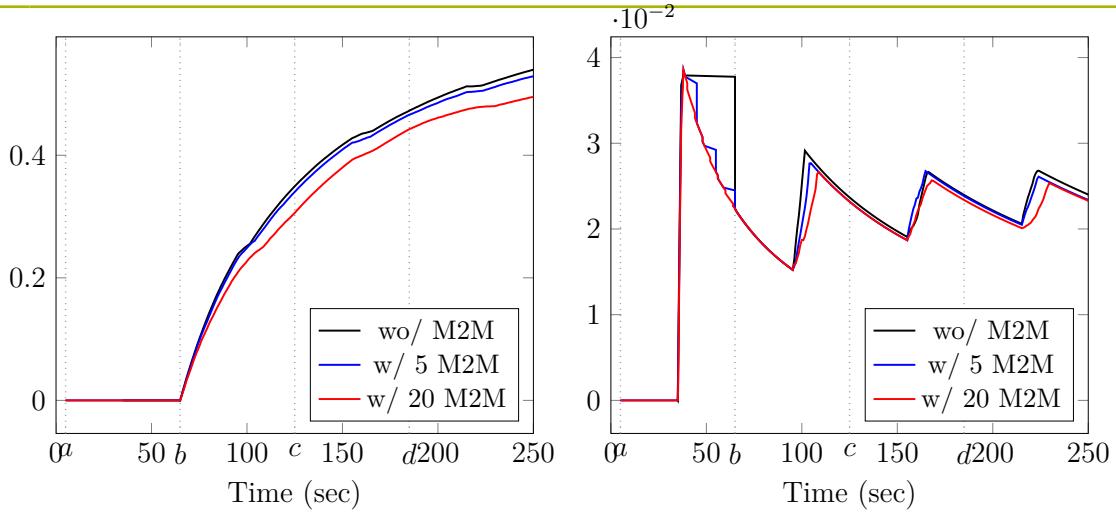
Figures 4.3 present the measured throughput for these three aforementioned scenarios. By comparing *phase a* in these figures, we show that the established M2M communications have apparently no impact on an incoming file transfer. However, the other phases show that the established bulk transfer has a greater impact on the available throughput for the file transfer traffic. In fact in the scenario 2, the available throughput in phases b, c and d is half that of the one obtained in *phase a*. However, in scenario 3, this available throughput is three times less than the one obtained in *phase a*. Table 4.1 presents the different download times that were recorded to retrieve $175kB$ of data via node 9 in each phase of each scenario. The download times for *phase a* of each scenario are very similar both with and without M2M traffic. However, this download time increases significantly in the event of sustained bulk transfer (an increase of 6.5 seconds on average). The additional 5 M2M nodes makes no difference in the time necessary for file transfer as the average transfer duration in scenarios 1 and 2 are almost the same $\sim 6.8sec$. On the contrary, bulk transfer and the additional 20 M2M nodes has a much greater impact on the time needed to download data from node 0, adding an average of 3.5 seconds.

We can conclude from these figures that the impact of M2M traffic on file transfer is negligible compared to the impact of the bulk transfer in terms of available throughput and download time. However, the combination of bulk transfer and the additional 20 M2M nodes does have an impact on file transfer traffic.

Table 4.1: File Transfer Downloading Time Comparison

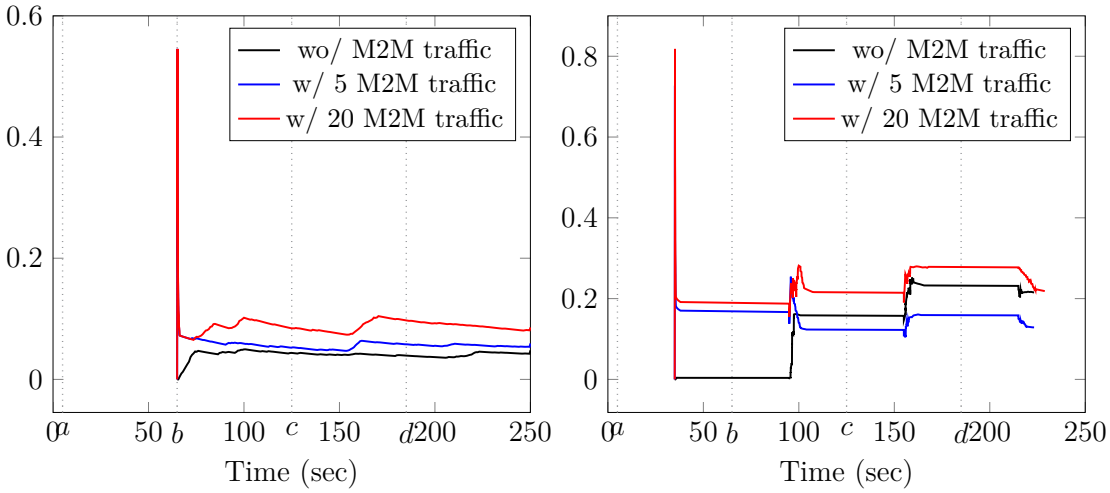
	wo/ M2M	w/ 5 M2M Nodes	w/ 20 M2M Nodes	Average per Phase
Phase a	2.99	1.97	2.19	2.38
Phase b	5.97	8.45	12.36	8.93
Phase c	10.27	8.81	12.96	10.68
Phase d	8.13	8.02	13.71	9.95
Average	6.84	6.81	10.30	7.98

Figures 4.4 compare the cumulative average throughput of legacy traffic both with and without M2M traffic. Figure 4.4a shows that the impact of M2M traffic on available throughput is negligible for bulk transfer (with a throughput loss of $0.05Mbps$ on average). Figure 4.4b confirms that, when used in combination, it is not M2M traffic (which has only minimal impact) but rather bulk transfer that significantly affects the available throughput for file transfers. These figures also indicate that surpassing 20 M2M nodes could increase the impact on available throughput. These results can be explained by the fact that legacy transfers (file transfers and bulk transfer) operate on the downlink whereas M2M traffic operates on the uplink.



(a) Bulk Transfer (∼ video stream) (b) File Transfer (∼ web page transfer)

Figure 4.4: Comparison of Cumulative Average Throughput with and without M2M traffic



(a) Bulk Transfer (∼ video stream) (b) File Transfer (∼ web page transfer)

Figure 4.5: Comparison of Cumulative Average Packet Loss with and without M2M traffic

In the same way, Figure 4.5 compares the cumulative average packet loss of both file and bulk traffic, with and without M2M nodes. Note that the packet loss value is only updated when packets are received, this is why Figure 4.5b plateaus between two file transfers. Even though the amount of M2M traffic increases packet loss for legacy traffic, this rise is still negligible compared to the packet loss resulting from TCP slow start. It should also be noted that device caches slow start thresholds for each IP-destination, as mentioned in [99]. That is the reason why slow starts for the second, third and forth file transfers are not as significant as the first one.

Regardless, packet loss for legacy traffic due to M2M traffic is negligible.

4.2.3 Discussion

Using deployed Wi-Fi APs to collect the data generated by M2M traffic have minimal impact on traditional H2M and H2H traffic in terms of transfer duration, available throughput and packet loss. However, this impact increases with the number of nodes. As mentioned previously, Wi-Fi networks provide a relatively higher number of APs compared to other wireless networks. This density would allow providers to spread devices to be served across the different available APs. As a result, M2M nodes could be dynamically allocated to different APs, this way ensuring a limited impact on APs and legacy customers.

In conclusion, if all APs in our scenario react based on the announcement of available services, data from M2M communications can be retrieved by APs while minimizing their impact on traditional H2M and H2H communications.

4.3 Characterizing Wi-Fi Environments

The IoT scenario described in Section 4.1 relies on the LSA mechanism to announce service availability. However, this scenario is very difficult to test as it would require having access to and modifying APs from different providers or or re-creating a sufficiently wide-spanned Wi-Fi environment with several APs. So, in order to validate the service announcement mechanism, we modeled the behavior of M2M Wi-Fi devices in a Wi-Fi environment. However, our models needed to be instantiated with values. We then decided to collect empirical values on real Wi-Fi deployments, so as to provide more relevant information on the use of LSA for our IoT scenario.

4.3.1 Methodology

Wi2Me [20] is an Android-based research application that has been developed to build Wi-Fi APs maps and automate Wi-Fi connections to CNs. This tool also evaluates CNs availability and performance. In scanning only mode, the Wi2Me application periodically scans the different channels and stores the results. Then, in addition to its original aim, Wi2Me can determine the Wi-Fi network density. In connection mode, it uses active probing to discover Wi-Fi networks and then connects to the AP with the highest signal level. When the devices are connected to an AP, the application is no longer scanning the channels unless triggered by an external event – RSSI loss, etc. And if the scanning results in finding a better network, it will attempt to connect to it. Once the device is connected, Wi2Me starts uploading files to a server, just like an M2M device does with its collected data.

Wi2Me enables an Android device to store all occurring events along with their timestamps. In particular, it stores the entire scanning event performed by the device along with all Wi-Fi SSID detected. Wi2Me also enables devices to automatically connect to specific SSIDs. Each connection is initiated with a *CONNECTION_START* event and terminated with a *DISCONNECTED* event. However, in some cases errors may cause connections to timeout before they are fully established. In this case, the *TIMEOUT* or *FAILED* status is given. Sometimes the specific error event may not even be reported. However, when a device is in the processes of connecting, it will not perform a scan unless forced to do so due to external event. This event monitoring enables researchers to *a*) approximately determine time during which a device is covered by an AP (the shorter the scan interval, the better the approximation); *b*) precisely determine the connection duration and the inter-connection duration, as well as the duration of all the steps required during the connection process (Association, Obtaining a IP Address, etc.); and *c*) to determine the percentage of failed and timeout connections.

This Android application enables researchers to characterize Wi-Fi environments. Wi2Me has been specifically used during three measurement campaigns, one being part of this thesis. For each campaign, an individual with a Wi2Me-equipped Android smartphone walked at a steady pace around specific areas.

4.3.1.1 City Center (CC) and Residential Area (RA) Measurement Campaigns

Wi2Me has been extensively used in [19] where volunteers have walked through the streets of Rennes (France) to characterize Wi-Fi environment in the city center. This application has also been used in [49] where a volunteer walked through the streets and footpaths of a residential area in order to determine if the Wi-Fi environment could help retrieve the health-monitoring data from a given subject. Both measurement campaigns used Wi2Me in connection mode. In the following sections, the results from these studies will be referred as the City Center (CC) and the Residential Area (RA) measurement campaigns.

Table 4.2: Wi2Me Data Overview for CC & RA Measurement Campaigns

	Traveled		Average Duration		Number of		
Campaign	Distance (km)	Duration (min)	Connected (sec)	Disconnected (sec)	Discovered APs	Connected APs	Scan
CC	34	NA	25.57	9.9	7280	625	12310
RA	4.6	74	44.7	53.9	45	NA	NA

Table 4.2 shows some metrics retrieved during these measurement campaigns. The values obtained in these studied campaigns show the differences in the Wi-Fi environments. Measurements showed that devices were connected to individual APs during an average of 25.57*sec* in the city center against an average connection duration of 44.7*sec* in the residential area. This difference can be explained by the difference in the studied environments. In the residential area there is less of shadowing effect because there are fewer objects and buildings obstructing signal emissions, which increases AP coverage ranges. In the city center, the average time between two connections was 9.9*sec* compared to 53.9*sec* in the RA campaign. Once again, this difference can be imputed to the differences between the two environments. Devices connected to 625 distinct APs in the CC campaign compared to 45 in the RA campaign. The number of deployed APs in the residential area is then much lower than in a city center, which implies that the probability that a device is not covered at all in certain areas, is higher.

4.3.1.2 Specific Path (SP) Measurement Campaign

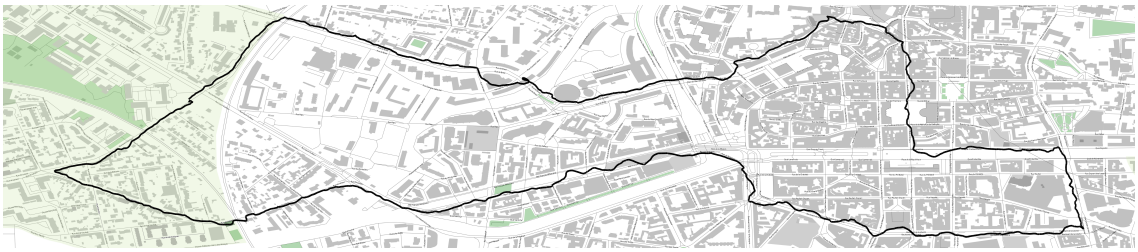


Figure 4.6: Studied path

The previous measurement campaigns were carried out with Wi2Me connection mode and do not provide complete scanning traces of the environment – as scanning stops when the device is connected. Such a trace could help us characterize the coverage (range and duration) of the environment. For this thesis, we used Wi2Me to study the Wi-Fi density and effective upload duration on a specific path inside the city of Rennes as shown in Fig. 4.6. One individual equipped with two smartphones, both running Wi2Me, walked along this path. The first smartphone, a Samsung Galaxy S3, was configured to connect to the CN "Free Wi-Fi" over all other detected APs and upload as much data as possible. The second smartphone, a Google Nexus S, was set up only to perform scanning – every second. This way, we were able to obtain a detailed mapping of the Wi-Fi density for this path at the time we roamed it and could determine the effective upload duration time along with the average volume of data to be sent.

Table 4.3: Wi2Me Data Overview for SP Measurement Campaign

	Traveled		Average Duration		Number of		
Device	Distance (km)	Duration (min)	Connected (sec)	Disconnected (sec)	Discovered APs	Connected APs	Scan
SGS3	6.5	113	24.1	5.9	498	124	339
GNS	6.5	113	N	N	4236	N	2876

Table 4.3 shows some metrics retrieved during this campaign. The connecting device measurements show that the average connection duration and disconnection duration were similar to the CC measurement campaign. This was as expected since these campaigns were performed in the same city. In the following sections, we explain how we used the measurements obtained with this campaign to study the Wi-Fi environment.

4

4.3.2 Characterizing the Environment

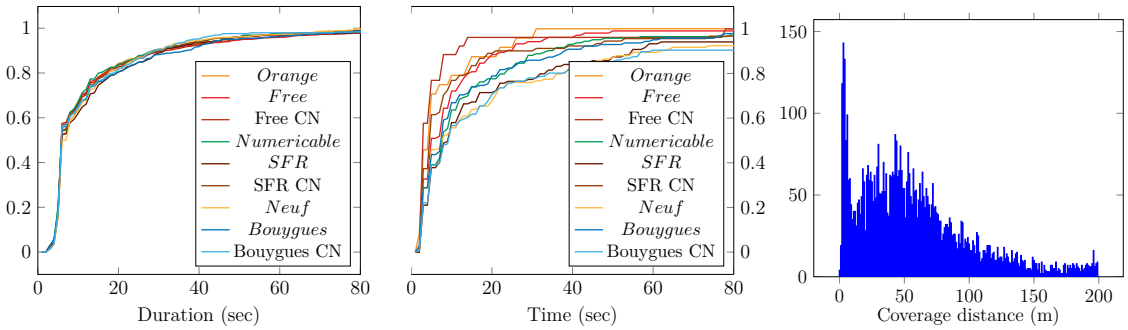
The characterization of the Wi-Fi environment was performed in two steps; the first one uses the values retrieved by the scanning only device to study the coverage statistics. The second step uses the values from the connecting device to study the connection parameters.

Table 4.4: SP Scanning - Distribution and Coverage Duration (sec)

	Number of discovered SSIDs	Percentage	Coverage Duration per AP			No Coverage Duration per AP		
			Min	Avr	Max	Min	Avr	Max
Orange	838	19.78%	2	12.597	156	1	6.75	30
Free	269	6.35%	2	13.357	209	2	9.490	84
Free CN	834	19.69%	2	13.347	215	2	6.615	77
Numericable	253	5.97%	2	12.251	149	1	15.070	196
SFR	188	4.44%	2	13.806	190	2	21.160	201
SFR CN	632	14.92%	2	12.499	195	1	12.846	175
Neuf	147	3.47%	2	12.505	88	1	22.481	225
Bouygues Telecom	219	5.17%	2	13.332	114	1	15.190	217
BT CN	126	2.97%	2	12.271	108	1	25.449	214
Average per ISP			2	12.885	158.222	1.333	15.006	157.667
Others	730	17.23%						
Overall	4236	100%	2	12.881	215	1	1	1
Minimal subset	94	2.22%	2	29.182	178	2	2	2

4.3.2.1 Coverage Characterization

As previously presented in Table 4.3, the scanning only device found 4236 different SSIDs. As shown in Table 4.4, these SSIDs belonged to 6 different ISPs among which three of them also provided a CN. Contrary to CN SSIDs, the SSID of residential Wi-Fi accesses can be modified by users. This is probably one of the reasons why there is a significant difference between the number of discovered SSIDs from one ISP and the number of discovered CN SSIDs from the same ISP. SSIDs for which the ISP could not be identified have been regrouped in the *Other* category.



(a) Covered Duration (b) Uncovered Duration (c) Distance Coverage

Figure 4.7: SP Scanning - Distance and Duration Coverage CDFs

Figure 4.7 presents the APs coverage statistics for each ISP of the SP measurement campaign. In these figures, we can see that the coverage durations per ISP are similar, 50% of APs provide Wi-Fi coverage lasting less or equal to 5.7 seconds. Table 4.4 also shows that each ISP provides an average of 12.9 seconds of coverage time.

However, the distribution of the duration without coverage is different for each provider as shown in 4.7b. This last figure and Table 4.4 depicts the penetration rate of each provider which determines a provider's capability to cover a device along the studied path. In addition, coverage duration strongly depend on the position and distance of the APs relatively from the path. Figure 4.7c represents the coverage distance distribution for all the discovered APs in the SP campaign. It illustrates that among all the discovered APs, 60% of them have a coverage range $\leq 50m$ and only 10% have a coverage range higher than $100m$. This measurement shows that the majority of discovered APs are located relatively close to the studied path, which explains why they all have a very similar coverage duration distribution. It also shows that the differences of uncovered duration distribution are due to the percentage of APs present along the studied path.

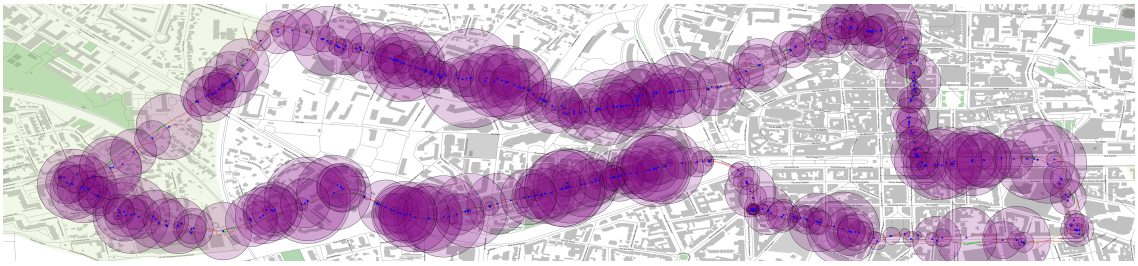


Figure 4.8: SP Scanning - Illustration of the Coverage Range

Figure 4.8 illustrates the coverage range of the discovered APs with a RSSI $\geq -90dB$. Blue points represent their weighted position and purple circles represent the range in which the corresponding AP has been detected. This last figure shows that with this subset of APs, regardless of AP provider, a device could be uniformly covered along the studied path. However, this figure raises the question of how many APs are required to uniformly cover a specific area. For instance, in our campaign are the 4236 APs necessary to cover the studied path? The answer is no, because APs coverage ranges often overlap, as illustrated in Figure 4.8. The presence of each ISP during the first 500 seconds of the trial is depicted in Figure 4.9. This figure also illustrates the overlapping of the ISP presence in the studied environment. As a consequence, a minimal subset of APs needed to cover a specific area can be determined.

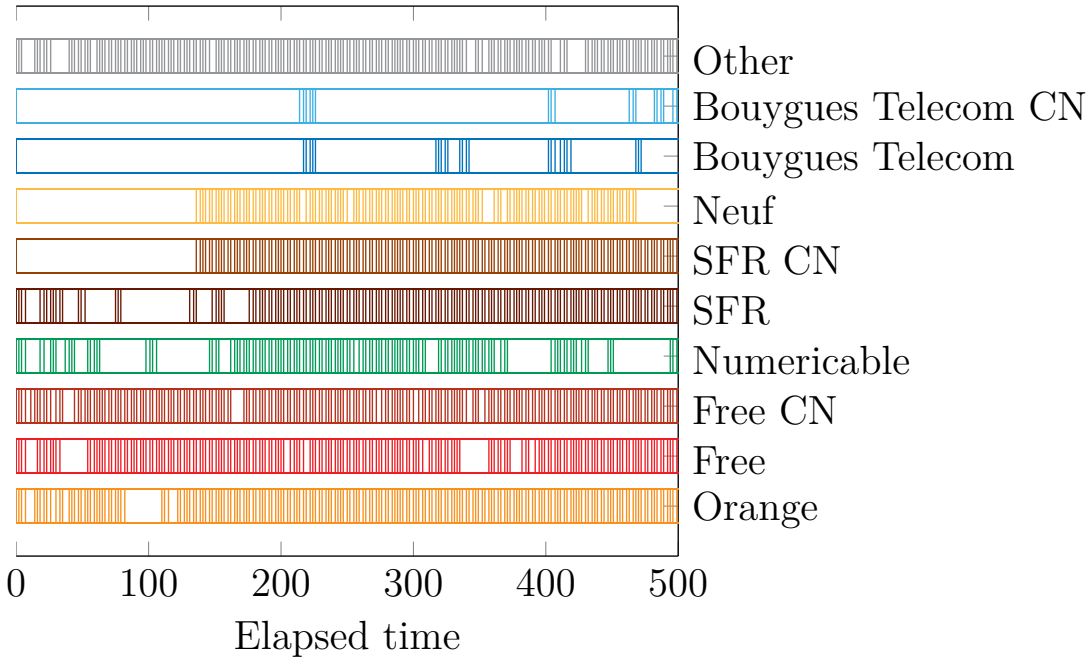


Figure 4.9: SP Scanning - Presence of each ISP along the Studied Path

We then studied the presence of each AP more specifically in order to determine this minimal subset. To do so, we selected APs from our measurements that would cover the whole path and provide the longest coverage. As a result, we were able to establish that along our set path the minimal subset is composed of 94 distinct APs. This minimal subset ensures coverage at 98%, as illustrated in Figure 4.10. It also enables devices along this path to be covered by an AP during an average of $\sim$ 30 seconds and not be without coverage by any AP for more than 2 seconds, as presented in Table 4.4.

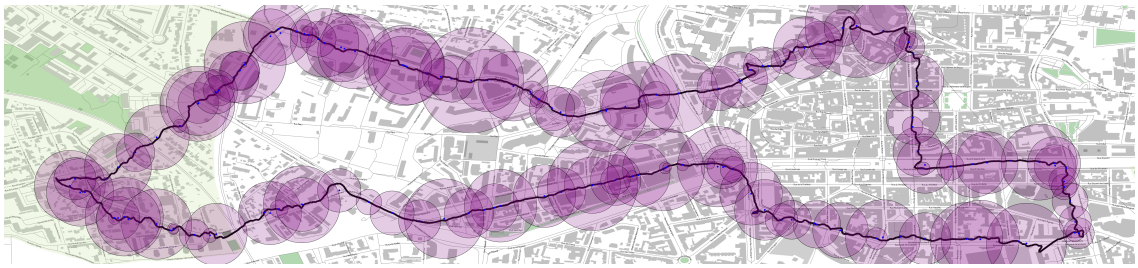


Figure 4.10: SP Scanning - Illustration of the Coverage with Minimal Subset of APs

4.3.2.2 Connection Characterization

In addition to scanning, we used a second smartphone connecting to one of the three available CNs: “Free Wi-Fi”. This device helped us characterize the time necessary to connect to an AP and determine the time left to upload data. It also enabled us to study the possibility of devices to connect to a service that would be announced by a subset of all the APs along a path. The measurements obtained by this device are similar to those of the devices used in the CC measurement campaign [19] mentioned previously. As we had access to some of these measurements, we will compare our values with those from the CC campaign in this section.

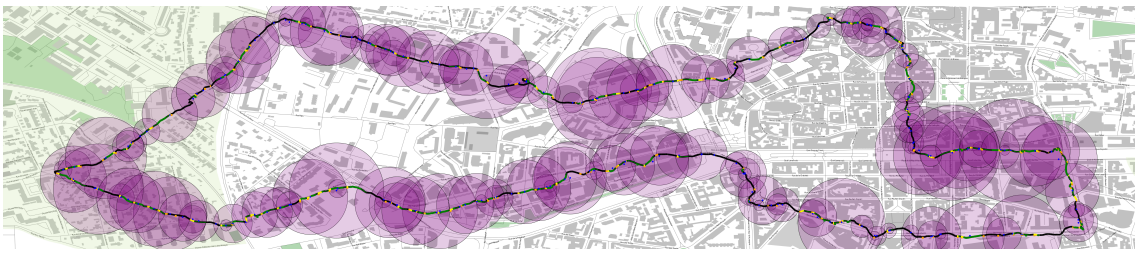


Figure 4.11: SP Connection - Illustration of the APs Coverage and Performed Connections

Figure 4.11 illustrates the coverage of the subset of APs with which the device has attempted a connection. This figure, along with a zoom of it in Figure 4.12, illustrates the time spent in each stage of the connection process, i.e. orange depicts the association with the AP, yellow depicts the IP address retrieval, the thin green line depicts the connection with the AP and the thick green line depicts the data uploading process.

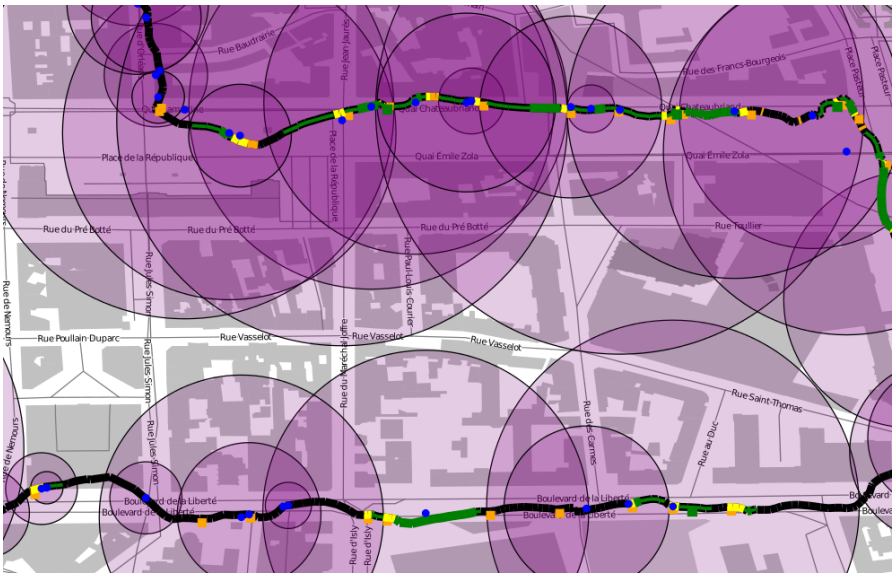


Figure 4.12: SP Connection - Zoom of the Connection Stages Illustration

Table 4.5: Wi2Me Connection Stages Duration Comparison during SP & CC Measurement Campaigns

Average Duration to	CC	SP
Start connection process	0.929	1.392
Accomplish Association	0.860	1.394
Obtain IP Address	3.865	4.852
Start Uploading	NA	2.008
until Upload stopped	NA	12.508

Table 4.5 summarizes the average duration of the connection and upload stages for both CC and SP measurement campaigns. The durations obtained in both campaigns differ but this is probably due to the number of connections carried out in each campaign. For example, Wi2Me connected to 625 distinct APs during the CC campaign compared to only 124 distinct APs in our measurement campaign. Despite these differences, these values show that the device has to wait 40% of the average connected time before being able to start uploading data.

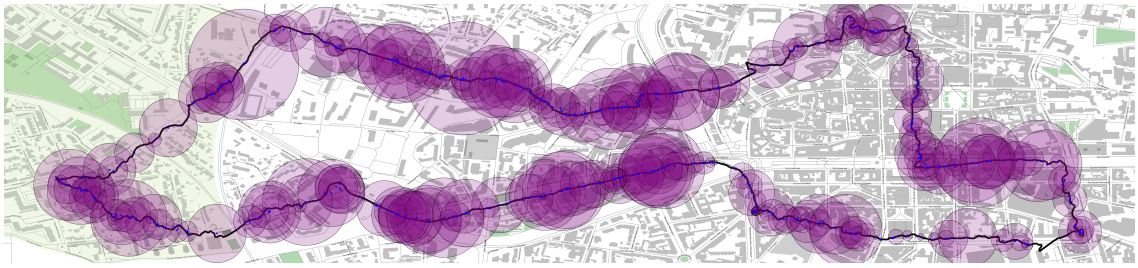


Figure 4.13: Connecting Device - Coverage of Discovered "Free WiFi" APs

The data collected in our campaign shows that the penetration of the Free Wi-Fi CN ensures that the connecting device remains connected during an average of 24 seconds and waits an average of 6 seconds for an AP to connect to, as shown in Table 4.6 and illustrated in Figure 4.13.

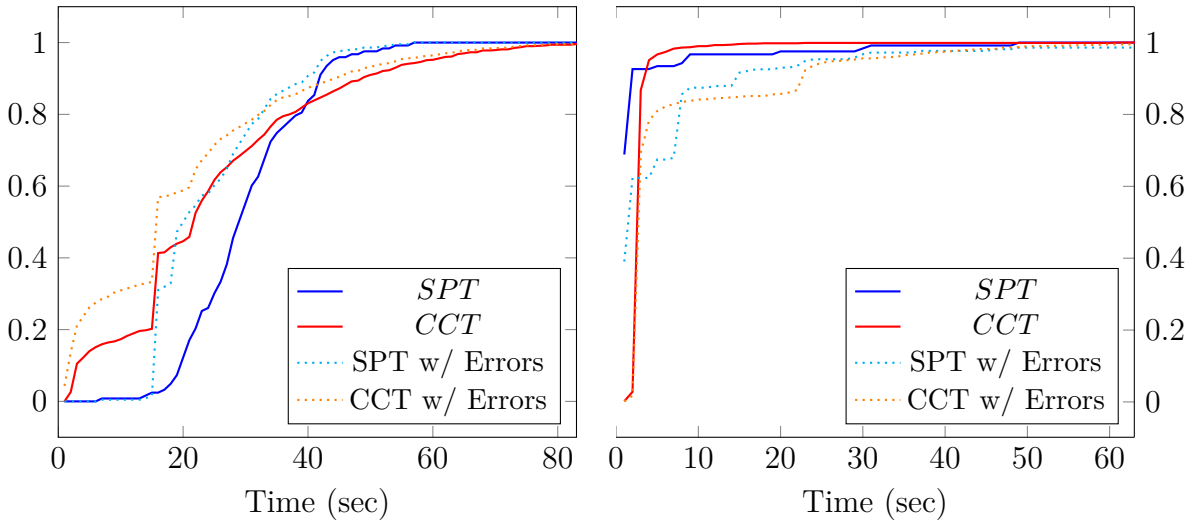
Table 4.6: Wi2Me Detail Data Comparison of SP & CC Measurement Campaigns

	Number of Connections	Connected Time		Inter-Connection Time	
		wo/ Errors	w/ Errors	wo/ Errors	w/ Errors
SP	124	29.945	24.112	2.161	5.949
CC	625	24.782	19.990	2.711	6.893

If we set these average values against the values measured during the CC measurement campaign, as shown in Table 4.6, we can see that devices in the CC campaign were connected to an AP an average of 20*sec*, while the average time between two connections – *Inter-Connection Time* – was reported at 7 seconds. Once again, the differences in each campaign explain these variations in results. For example, measurements from the CC campaign were obtained on several paths of the city and with connections performed on different CNs, whereas measurements from the SP campaign were performed on only one specific path in the same city and where the device connected to only one CN. It is therefore not surprising that this path obtained better results than over a whole area.

In fact, if we look at Figure 4.14, we notice that the studied path offers a more suitable environment. This figure presents the CDFs of the measured *Connected Time* and *Inter-Connection Time* in each campaign. The dotted lines in Figure 4.14 represent the connection (resp. inter-connection) times of all the connections made during the campaign – i.e. including errors. The solid lines represent the CDFs of the connection times of only the connections that terminated with a *DISCONNECTED* event.

The connection timeout value for Wi2Me is set at 15 seconds. As a result, if the device does not receive any packet during that time, a *TIMEOUT* event is trig-



(a) Connected Time

(b) Inter-Connection Time

Figure 4.14: Wi2Me Connections CDFs Comparison for SP & CC Measurement Campaigns

gered in Wi2Me, forcing the device to start looking for a new AP. During the CC campaign, we can notice by looking at the red curve of Figure 4.14a that almost 20% of connections lasted around fifteen seconds and 20% lasted less than fifteen seconds. All connections that terminated with a *Disconnected* event, received at least one packet before triggering the *TIMEOUT* event. On the contrary, in the SP measurement campaign all connections that exceeded the timeout value ended up triggering the *TIMEOUT* event and were counted as errors. Thus, almost 60% of the CC measurement campaign connections lasted around 15 seconds, against 30% for the SP one, which also explains the difference in average connected time.

4.3.3 Discussion

The Wi2Me application collects empirical measurements regarding specific Wi-Fi deployments. It has notably been used in two measurement campaigns where devices carried out connections to subset of APs. These campaigns showed the differences in terms of connection and inter-connection times that can exist between two Wi-Fi deployments. However, these campaigns did not provide characterization on the Wi-Fi coverage of these environments. We then performed another measurement campaign in order to characterize a specific Wi-Fi environment in terms of coverage, connection and uploading. This campaign helped us test the scenario presented in 4.1 as measurements were obtained on a device attempting to connect to one of the CNs. These measurements illustrate then the behavior of a device looking for a specific subset of APs in an area with high Wi-Fi AP density in order to transfer its data.

As a result, our measurement campaign enables us to study the ability of a device to transfer data via a subset of APs. In fact, our connecting device uploaded a total of 61.3MB of data via a total of 158 connections. The device therefore uploaded an average of 388kB per connection which is 64 times more than the 6kB packet in our simulated M2M traffic model from Section 4.2. Each uploading session lasted on average 12.5 seconds. Table 4.5 presents the duration of each stage in the Wi-Fi connection process. It shows that the device has to wait on average 9.646 seconds before being able to start uploading data. Thus, a device moving within a Wi-Fi area spent almost half of its coverage time establishing the connection with the AP. We can assess from these results that our scenario is valid even if the average effective time for uploading data represents only half of the average connected time.

However, the total transmitted data could be improved if the connection process was shorter. For instance, the measured values show that the retrieval of an IP address represents 50% of connection process time. Therefore, the connection process could be speeded up by pre-assigning an M2M device with an IP address. This solution would make our scenario more efficient as devices benefiting from the services offered by a subset of APs would have more time to upload their data.

Our measurements also enable us to conclude that our scenario could be deploy with a minimal subset of APs. In our studied environment, the minimal subset was composed of 94 APs which only represented 2.22% out of the 4236 discovered APs. However, depending on the number of M2M nodes to be served, this subset of APs may not be sufficient to collect all the data. A high number of M2M nodes would probably require more than the minimal subset of APs to cover the area. So, the number of APs necessary to cover an area not only depends on the size of the area but also on the number of devices to be served in this area.

Moreover, the timeout value for these devices has to be chosen properly. Our measurements show that this timeout value could decrease the ability for a device to upload its data. Indeed, when devices wait for the timeout value to end before starting a new connection they are moving and may miss out on a more suitable AP for sending their data. Furthermore, Figure 4.12 shows that the device used was sometimes reported as connected without being able to upload its data, see the top left of the figure. We do not have the information on what happened as a result of this behavior. But it may be linked to the timeout value and is worth being investigated in order to improve the number of packets uploaded.

This measurement campaign showed that current Wi-Fi architectures can be used for the retrieval of M2M data. However, our scenario and its efficiency could be improved.

4.4 Modeling this Scenario with Markov Chains

We used two Markov chains to model the IoT scenario. This enabled us to determine the impact of the LSA mechanism and, in doing so, validate this scenario.

4.4.1 Model principle

We considered the scenario described in Section 4.1 to model the behavior of M2M Wi-Fi devices. In this scenario, M2M devices monitored certain physical characteristics in the area where they were deployed. They could, for instance, monitor the activity and/or the position of a pet, or the health status of the person holding the device. It is crucial to emphasize that both examples can be used with this solution despite having different levels of importance. This implies that the retrieval of data generated by M2M devices for certain applications will be more critical than others.

In all possible scenarios, we supposed that these devices would be moving within a predefined area and therefore alternate between having Wi-Fi coverage and not being covered by any APs. When a device has Wi-Fi coverage, it receives beacons. If a beacon contains an announcement of the desired service, the device connects to the corresponding AP and starts uploading its data. It then repeats this process for as long as possible. However, a device may not be able to send its data even if it has Wi-Fi coverage as the corresponding AP may not support the desired service, or the device may be sleeping when receiving the beacons.

The goal of this model is to study *a*) the impact of the announcement interval on the time it takes to detect the expected services; *b*) the influence of the Wi-Fi AP density on the performance of the solution; *c*) and the time needed to send the collected data to the AP.

This scenario can be modeled with Markov chains, which provide both the time necessary as well as the probability of successfully detecting the desired service.

4.4.2 Continuous-Time Markov Chain

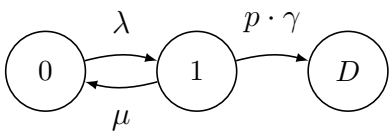


Figure 4.15: Continuous-Time Markov Chain Model for a Monitoring Service

The aforementioned scenario can be simply represented by a three states Continuous-Time Markov Chain (CTMC) as shown in Figure 4.15:

- State 0: the device has no Wi-Fi coverage;
- State 1: the device has Wi-Fi coverage but has not received a beacon with the desired announcement;
- State D: the device has Wi-Fi coverage and has received a beacon with the desired announcement.

In this CTMC, we consider that a device at state 0 (no coverage) leaves this state after a delay following an exponential law at a rate λ. While transitioning from covered to uncovered region is done at a rate μ. Hence, the average time with Wi-Fi coverage is $1/\mu$ and the average time without Wi-Fi coverage is $1/\lambda$. In order to make the problem mathematically tractable, we consider that beacons are received following a Poisson's law at a rate γ. And we denote with p the probability that the device is not idle.

4.4.2.1 Solution

The scenario we studied is a CTMC with a fixed number of states. Therefore, the generator matrix, Q, can be obtained in closed form:

$$Q = \begin{pmatrix} -\lambda & \lambda & 0 \\ \mu & -\mu - p \cdot \gamma & p \cdot \gamma \\ 0 & 0 & 0 \end{pmatrix} \tag{4.1}$$

Let $\pi_t(i)$ represent the probability of a device being in state i, while P_t represents the transition state matrix. If we note $\Pi_t = (\pi_t(0), \pi_t(1), \pi_t(D))$ then

$$\Pi_t = \Pi_0 \cdot P_t = \Pi_0 \cdot \mathrm{e}^{Q \cdot t} \tag{4.2}$$

This model makes it possible to determine the time needed to receive a given announcement within a specific Wi-Fi AP density. We are interested in determining the time necessary to arrive at state D, i.e. to detect the desired service. After resolving the equation (4.2), $\pi_t(D)$ can be reduced to the following expression :

$$\pi_t(D) = 1 - K_1 \mathrm{e}^{-\frac{At}{2}} - K_2 \mathrm{e}^{-\frac{Bt}{2}} \tag{4.3}$$

with

$$K_1 = \frac{1}{2} - \frac{\mu^2 + p\gamma(\mu - \lambda) + \lambda^2}{2(\mu + \lambda)R}, K_2 = \frac{1}{2} + \frac{(\lambda + \mu)^2 + p\gamma(\mu - \lambda)}{2(\mu + \lambda)R}$$

$$A = \mu + p\gamma + \lambda + R$$

$$B = \mu + p\gamma + \lambda - R$$

$$R = \sqrt{\mu^2 + 2\mu\lambda + 2\mu p\gamma + (p\gamma)^2 - 2\lambda p\gamma + \lambda^2}$$

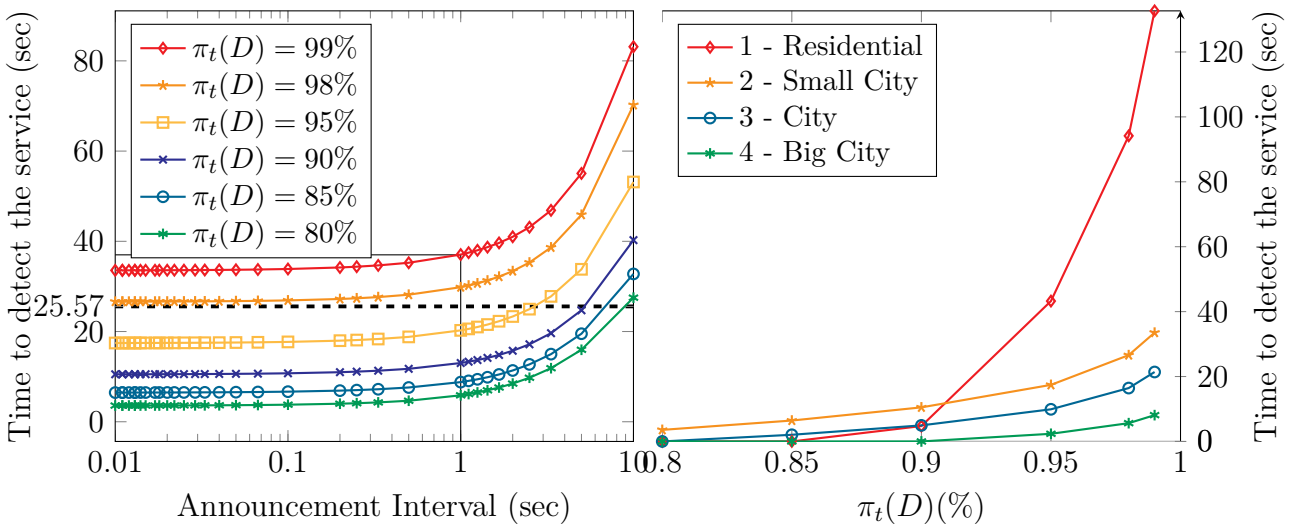
Values for λ and μ must be determined in order to instantiate this model and to study their influence on the amount of time needed to detect the service. They can be determined using the average time a device has or does not have Wi-Fi coverage in a given environment. The Wi-Fi coverage in this environment is expressed as $\rho = \frac{\lambda}{\lambda+\mu}$. Even though, the CC and RA measurement campaigns do not provide the average coverage parameters, they give a good approximation of the average time with Wi-Fi coverage (based on the average amount of time they were connected) as well as an approximation of the average amount of time without Wi-Fi coverage (based on the amount of time between connections). It should be noted that these approximations are slightly misleading as devices spend more time within coverage areas than their connection time shows. These measurements can be used to determine values for λ and μ, as presented in Table 4.7, and to instantiate the CTMC of Figure 4.15. Furthermore, the values for λ and μ, used in case studies 3 and 4, were estimated based on basic cross-multiplication. As a result, we are able to study the impact of better Wi-Fi environments (i.e. environments with a higher percentage of Wi-Fi coverage) on the performance of our scenario. All these values (measured and estimated) are summarized in Table 4.7.

Table 4.7: Measured and Estimated Values for λ and μ

	Case	λ	μ	$\rho = \lambda/\mu$	Coverage
Measured					
	1 - Residential	0.018	0.022	0.82	45%
	2 - City	0.1	0.04	2.50	72%
Estimated					
	3 - City	0.14	0.035	4	80%
	4 - City	0.28	0.03	9.33	90%

4.4.2.2 Results

The rate at which a service is announced within a beacon depends on the importance given to it. First, we studied the influence of the announcement interval over the time needed to detect the desired service. To do so, fixed values were used for the probability $\pi_t(D)$ as well as for λ and μ. In the following results, values from the second study (Table 4.7) were used. We also considered that the device is never idle – $p = 1$. $1/\gamma$ represents the announcement interval and t is the time needed to detect the desired service (i.e. reaching state D on Figure 4.15). The influence of γ (on the abscissa) on the time t (on the ordinate) has been plotted as shown in Figure 4.16a. Each curve represents different values of $\pi_t(D)$ (the probability that the time to detect the service is less than t).



(a) CTMC - Announcement Interval Impact

(b) CTMC - Wi-Fi Density Impact

Figure 4.16: Influence of Announcement Interval and Wi-Fi AP Density over the Time to Receive an Announcement

For instance, the point marked with solid black lines in this figure shows that there is a probability of 99% that the device will receive the expected announcement in under than 37 seconds for a service announced every second.

Then, we studied the influence of Wi-Fi AP density over the amount of time needed to discover the service as shown in Figure 4.16b. We fixed the value of γ to have one announcement every second and observed the influence of different values for λ and μ, i.e. the average time with and without Wi-Fi coverage, on the time t to detect the desired service.

4.4.2.3 Discussion

This model provides us with preliminary results on the performance of the application of LSA mechanism. We can conclude from Figure 4.16a that the time needed to receive the desired announcement grows exponentially for announcement intervals greater than $1sec$. And as expected, the higher the success rate, the longer the delay. Figure 4.16b shows that the time needed to detect the service is lower in denser areas. But surprisingly, case study 1 (the residential area) presents better or equivalent results than case studies 2 and 3 (city center) with success rates below 90%. The number of available APs in the residential environment is fourteen times lower than in the city center. So, it was reasonable to think that the city center environment would provide better results than the residential area. But this did not take into account that the average connected time is twice as much in this environment than in the city center.

However, for success rates above 90%, the results for the residential area become drastically worse. This should be taken into consideration as the time without Wi-Fi coverage in rural areas is too high to ensure a constant, high probability of successful service detection. Thus, depending on the desired success rate, studies on the available Wi-Fi AP density must be performed before deploying services based on a service announcement mechanism.

Even though, this first model shows interesting trends, it also shows some surprising results. For example, Figure 4.16a supposes that for low announcement intervals and different success rates, the time needed to detect the service converges towards different limits. Whereas we could expect that they converge to the same limit. Indeed, with low announcement intervals, service announcements will always be in the beacon, which implies that devices will always see them, especially if the device is never idle. Moreover, Figure 4.16b shows that the time without Wi-Fi coverage only impacts detection in residential areas for success rates over 90% and for announcement intervals of 1 second. With an average of 53.9 seconds without Wi-Fi coverage, we would expect that the results for this environment would worsen even for success rates below 90%.

Several hypotheses have been made that do not reflect reality which may explain these surprising results. First, we assumed that the times spent "with" and "without" Wi-Fi coverage followed an exponential law, which remained to be proven. Then, we stated that beacons were received following a Poisson law, which in reality is not the case. So, in order to have results closer to reality, we defined a more precise Markov chain model to also be instantiated using empirical data.

4.4.3 Discrete-Time Markov Chain Model

A Discrete-Time Markov Chain (DTMC) model was used to model the behavior of M2M Wi-Fi devices in an LSA-capable environment. In this new model, time is divided into time slots T_s. Figure 4.17 represents this new DTMC.

In Figure 4.17, n_l states represent the states in which devices have no Wi-Fi coverage, thus $n_l * T_s$ represents the time spent without coverage. The other states represent the time spent with Wi-Fi coverage. In these (n, m) states, a device in a dashed state (first column) may revert to a non-covered state. In this model, the announcement interval is given by $n * T_s$. Devices receive announcements in one of the dotted states – $(1, x)$ states. If the desired service is present, the device goes into the detection state D, and will start the connection process with the corresponding AP. Otherwise, it will wait for the next announcement.

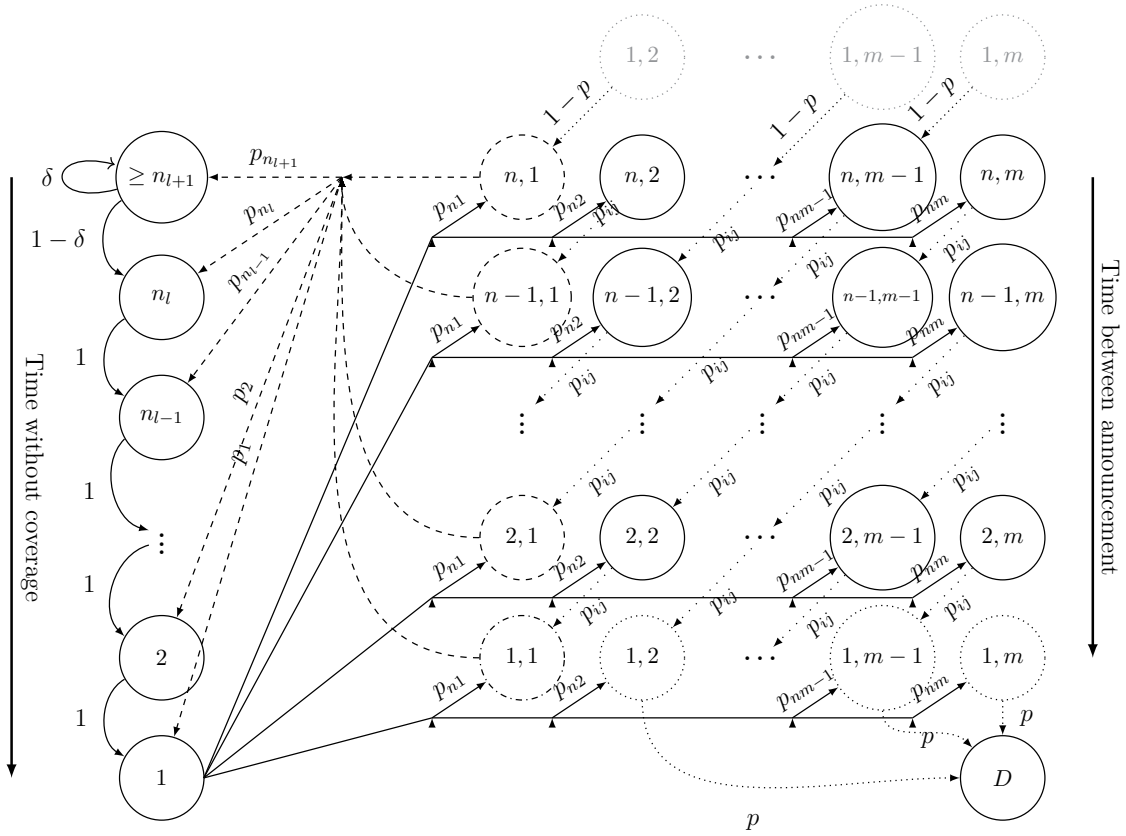


Figure 4.17: Discrete-Time Markov Chain Model

We assume that when in a Wi-Fi coverage area, devices shift from one state to another with a probability of $p_{ij} = 1$, meaning that devices stay in each covered state during one time slot T_s. Devices shift from non-covered to covered states with a probability of p_{nk}, $k \in [1, m]$. These probabilities are obtained from the measurement campaign as the probability of remaining in a Wi-Fi coverage area for $k * T_s$ seconds when leaving a non-covered area. While p_l, $l \in [1, n_l]$ are the transition probabilities of shifting to an uncovered state. They are also obtained using empirical measurements as the probability of not being covered by any APs for $l * T_s$ seconds when leaving a covered area. To obtain these transition probabilities, we used the distribution of duration with and without coverage for the service, measured during our campaign and represented in Figure 4.7. We have then separated these distributions in T_s intervals, which gave us the probability to stay in a covered [resp. uncovered] area during each time slot.

Once again, p is the probability that devices will not be idle. Thus, the probability of shifting from dotted states to the detection state is p, otherwise the devices will have to wait for the next announcement.

4.4.3.1 Solution

We use P to identify the transitioned matrix of this DTMC and V the column vector corresponding to the initial state – i.e. being in the n_{l+1} state. These matrices can be obtained in closed form:

$$\begin{pmatrix}
\delta & 1-\delta & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
 & \vdots & & \vdots & & \vdots & & & & \vdots & & & & & \vdots & & & \vdots & & & \vdots & & & & & \vdots & & & \\
0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & p_{n1} & p_{n1} & \cdots & p_{n1} & p_{n1} & p_{n2} & p_{n2} & \cdots & p_{n2} & p_{n2} & \cdots & p_{nm-1} & p_{nm-1} & \cdots & p_{nm-1} & p_{nm-1} & p_{nm} & p_{nm} & \cdots & p_{nm} & p_{nm} & 0 \\
p_{n_{l+1}} & p_{n_l} & p_{n_{l-1}} & \cdots & p_3 & p_2 & p_1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
p_{n_{l+1}} & p_{n_l} & p_{n_{l-1}} & \cdots & p_3 & p_2 & p_1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
 & \vdots & & \vdots & & \vdots & & & & \vdots & & & & & \vdots & & & \vdots & & & \vdots & & & & & \vdots & & & \\
p_{n_{l+1}} & p_{n_l} & p_{n_{l-1}} & \cdots & p_3 & p_2 & p_1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
p_{n_{l+1}} & p_{n_l} & p_{n_{l-1}} & \cdots & p_3 & p_2 & p_1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1-p & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & p \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
 & \vdots & & \vdots & & \vdots & & & \ddots & & & & \ddots & & & \vdots & & & \vdots & & & & & \vdots & & & & \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
 & \vdots & & \vdots & & \vdots & & & & \vdots & & & & & \vdots & & & \vdots & & & \vdots & & & & & \vdots & & & \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & p \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
 & \vdots & & \vdots & & \vdots & & & & \vdots & & & & & \vdots & & & \ddots & & & \vdots & & & & & \vdots & & & \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 1 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1-p & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & p \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
 & \vdots & & \vdots & & \vdots & & & & \vdots & & & & & \vdots & & & \ddots & & & \ddots & & & & & \vdots & & & \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0
\end{pmatrix}
\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{4.4}$$

The probability of receiving the announcement – i.e. reaching state D – can be determined using the following equation:

$$\pi_t(D) = P(t \leq k \cdot T_s) = [P^k \cdot V]_D \tag{4.5}$$

This equation allows us to determine the probability $\pi_t(D)$ of reaching state D – i.e. service detection – when starting from the state n_{l+1}, in a time of t less than $T = k \cdot T_s$.

Using this DTMC, it is also possible to determine the probability that the device will leave the covered area without receiving the desired announcement (provided that it was already coming from an uncovered area before shifting to a covered area). This is the case when a device approaches a Wi-Fi area but does not fully enter in it. This is the probability of arriving in the upper left triangle of the DTMC – i.e. inside states $(2,1)$, $(n,1)$ and $(n,n-1)$. This probability can be expressed by the following equation:

$$P_{missed} = \sum_{i=1}^{n-1} \frac{1}{i} \sum_{j=1}^{i} p_{n,j} + (1-p) \tag{4.6}$$

4.4.3.2 Model Validation

Before using this model to continue our study, we wanted to verify it using our SP measurement campaign. To do so, we focused on the "Free WiFi" connectivity offered by the Free CN. This connectivity is shown as a service announced every $100ms$, i.e. for every beacon of Free CN, by all Free CN APs. The measurements gathered from the scanning device during this campaign give us the coverage parameters of Free CN along the studied path. The Free CN SSID represents 19.69% of all scanned APs – the whole distribution is presented in Table 4.4. And, based on the presence of the Free CN SSID at the different scanning positions, we estimated that this subset of APs cover approximately 94% of the studied path. This coverage can also be interpreted as the device received a beacon from this provider in 94% of the scans – i.e. the probability of a device to detect this service along the path. The connection device used during this measurement campaign attempted connections on the same subset of APs. The measured values obtained with this device enabled us to determine that the average time required to start the connection process – i.e. receive a beacon with the expected "Free WiFi" SSID – is of 1.392 seconds.

Our verification process aimed determine whether our model provided a value for the time to detect the desired service similar to the one obtained in the measurement campaign. We have then used the same parameters to instantiate our DTMC – i.e. Free CN coverage parameters (covered and uncovered distributions), a $100ms$ announcement interval and a 94% probability of finding the expected SSID. Using these parameters our model estimated that the device would have to wait at most 0.9 second to detect the "Free WiFi" SSID.

The value obtained with the model is lower than the one gathered during our measurement campaign. But, the average value for detecting the service obtained during this campaign would probably have been different if more connection attempts had been made on this path. Actually, measurements from the CC campaign are the sum of several measurement campaigns. As a consequence, the number of connections performed during this campaign is 5 times higher than what we performed in ours. We can therefore assume that with more connections the average time needed to detect the service will be closer to the value obtained during the CC measurement campaign, i.e. 0.929 second which is very close to the result obtained using our mathematical model.

The results measured during the campaigns and the one obtained using our model are similar which proves our mathematical model. The following section will present the result obtained using this model to study the credibility of our scenario. However, for more conclusive results on the validation of our model additional measurements would need to be carried out along the studied path.

4.5 DTMC Model Results

In this section, to determine the validity of our scenario, we will study the impact of using different announcement intervals and different Wi-Fi AP densities on the time necessary to detect a service as well as the probability of devices being able to send the collected data.

4.5.1 Announcement Interval Impact

In our scenario, a service is announced at a given rate depending on the importance given to it. It is thus crucial to study the influence this announcement rate has on the time needed to detect the service. By doing this we will also be able to determine the largest possible announcement interval for the parameters used to instantiate the model.

Figure 4.18 represents the time necessary to detect the desired service (on the ordinate) for the announcement interval used (on the abscissa) for given probabilities $\pi_t(D)$. The probability to detect the service – $\pi_t(D)$ – is fixed. The Markov chain has been instantiated with the Free CN parameters obtained during our measurement campaign with the scanning device. The device is considered as never idle – $p = 1$ while the announcement rate – i.e. n – varies.

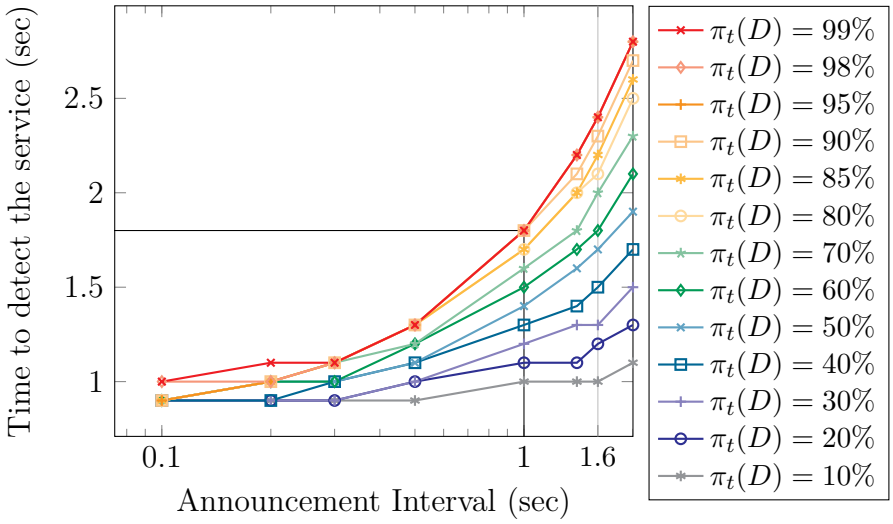


Figure 4.18: DTMC - Impact of Announcement Interval

The results obtained with this new model contrast sharply with the ones obtained with the CTMC. In fact, contrary to the results from Figure 4.16a, and as expected, the new results show that the time needed to detect the service is almost the same for different probabilities of success and with a low announcement interval. This is

closer to reality because with a very low announcement interval the announcement will be present in every beacon and is therefore more likely to be found by the device.

Besides, using the same subset of APs – i.e. Free CN –, the results obtained with the continuous Markov chain pointed out that it was impossible to deploy services with an expected success rate higher than 95% – the time necessary to detect the service being then higher than the average connected time. However, this new model shows the opposite, and in addition, it indicates that services could be deployed for any success rate, provided that the announcement interval was less than 2 seconds.

For announcement intervals of over 1 second, the time needed to detect the service started to differ significantly for different success rates. Moreover the curve slopes double for announcement intervals higher than 1.6 seconds. We assume that this time will grow exponentially for announcement intervals higher than 2 seconds, as depicted in the CTMC results.

4.5.2 Wi-Fi AP Density Impact

The preliminary study based on our first Markov chain model already stressed the importance of Wi-Fi AP density in a scenario based on the announcement of available services. The coverage parameters obtained for the different providers discovered in our measurement campaign will be used for this new model in order to study the importance of Wi-Fi AP density. Furthermore, our SP measurement campaign allows us to determine a minimal subset of APs in order to cover the studied path. The results obtained with the coverage parameters of this minimal subset will then be compared to the results obtained with the other different ISP coverage parameters.

The previous results showed that the time necessary to detect a service started to differ significantly when the announcement interval was higher than 1 second. We therefore fixed the announcement interval to 1 second in the following result and studied the impact of Wi-Fi AP density on the time needed to detect a service with different detection probabilities. Once again, we considered that the device was never idle – $p = 1$.

Figure 4.19 shows that devices needed less time to detect a service in denser areas. But it also shows that the probability to detect a service has a direct impact on the time needed to detect the service for a fixed announcement interval.

In Figure 4.20, we plotted the time necessary to detect the desired service (on the ordinate) depending on the announcement interval used (on the abscissa) for a given Wi-Fi AP density. The probability to detect the service is fixed – $\pi_t(D) = 0.9$ – and we considered that device is never idle – $p = 1$.

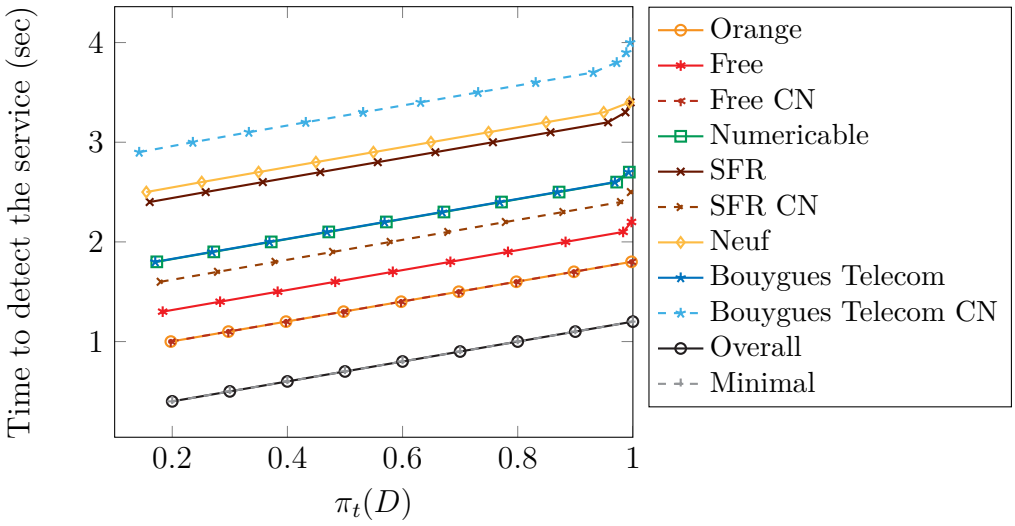


Figure 4.19: DTMC - Wi-Fi AP Density Impact for Fixed Announcement Interval

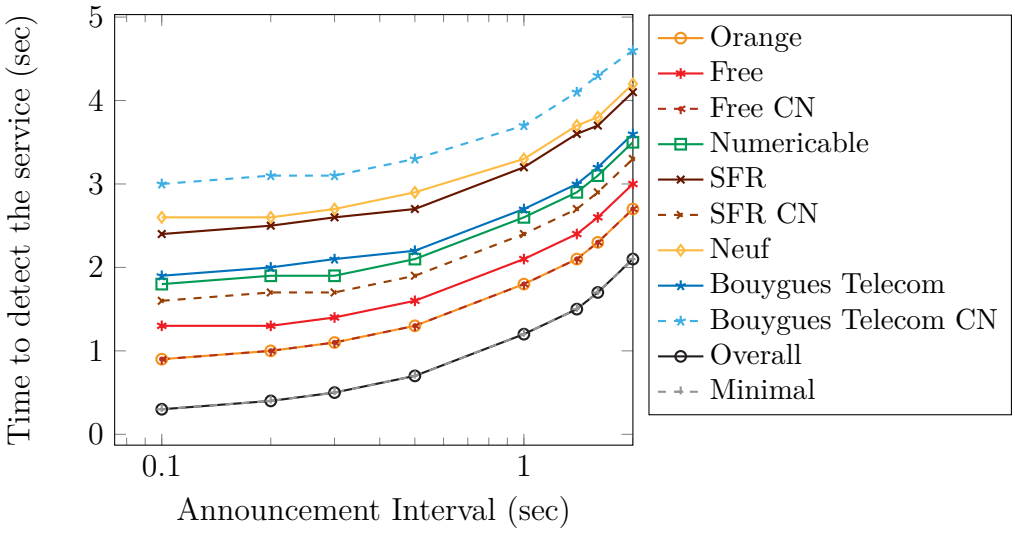


Figure 4.20: DTMC - Wi-Fi APs Density Impact for Fixed Success Rate

Once again, we noticed that the higher the Wi-Fi AP density, the lower the time needed to detect the service. However, we can see that the variations in terms of announcement intervals have a higher impact on the time necessary to detect the service than on the success rate.

These figures also show that, according to our model, the minimal subset of APs gave as good of results as the whole set of discovered APs during the SP measurement campaign. These results confirm that an optimal subset of APs can be obtained in

order to cover an area with a specific service depending on the number of devices to be served and on the available density of APs.

In addition, we noticed that the model gives similar results for Orange and Free CNs even though their coverage parameters, though similar, are not the same. These last remarks emphasize that in our model the time distribution in non-coverage areas has a greater impact on the time needed to receive an announcement than the time distribution in coverage areas.

We can therefore conclude that the most limiting parameters in our scenario are the announcement interval and the Wi-Fi AP density, or more precisely the time spent in non-coverage areas.

4.5.3 Successfully Transmit Data

The final objective in our scenario is not to be able to detect a service but for the device to successfully transmit the collected data to the appropriate destination. It is therefore crucial to determine whether or not a device can successfully transmit its data within a subset of Wi-Fi APs (which announces the desired service at a given frequency). From the Markov Chain depicted in Figure 4.17, we have determined the probability that the announcement will not be received by the device when it left the coverage area as shown in equation (4.6). Therefore, the probability that the service announced will be received upon entering a coverage area can be expressed as $P_{NM} = 1 - P_{missed}$.

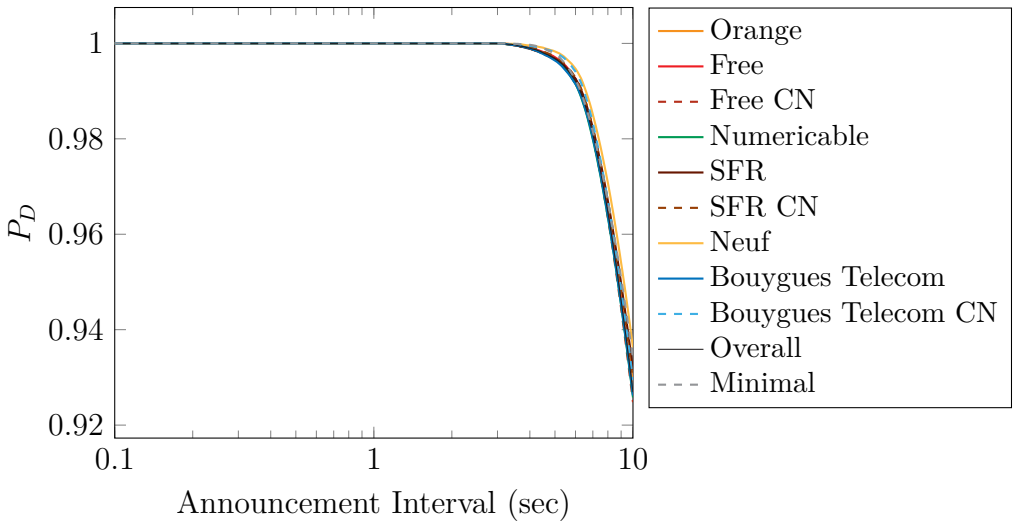


Figure 4.21: DTMC - Probability to Detect a Service when Arriving in a Covered Area

Figure 4.21 represents the probability that a device will detect the service upon entering a coverage area using different Wi-Fi coverage parameters and different announcement intervals. We consider that the device is never idle – $p = 1$.

Figure 4.21 shows that the probability of directly detecting a service upon entering a Wi-Fi coverage area is of 100% for an announcement interval less than 3 seconds and regardless of the Wi-Fi coverage parameters used. For announcement intervals of over 3 seconds the probability of detecting the service begins to decrease. In the traffic studied in Section 4.2 to characterize M2M impact, we considered that an M2M node sends a packet of $6kB$ every 10 seconds. Considering Wi-Fi node moving in an IEEE 802.11b network, we can consider that the environment contains several other nodes and therefore interference. The available throughput will therefore be around $1Mbps$ as analyzed in [63]. In this type of wireless environment, an M2M node will then require $48ms$ to send its $6kB$ of data every 10 seconds. Our model does not take into account the connection and upload processes or the probability for the connection to fail or timeout. It just gives the time needed to detect the service.

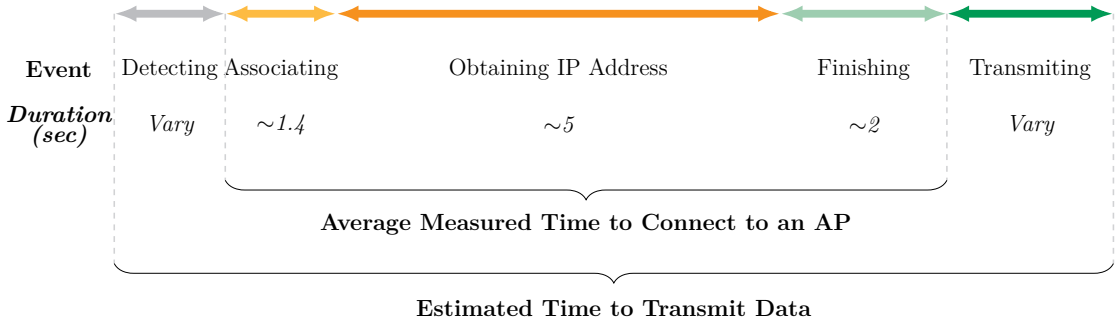


Figure 4.22: Illustration of the Time Required to Transmit Collected Data

However, we can estimate if an M2M device – as characterized in this chapter – coming from an uncovered area can successfully transmit the collected data. Figure 4.22 illustrates the estimated time to transmit this data, which is divided in three parts:

- Detection process: Time to detect an AP announcing the desired service;
- Connection process: Time to connect to this AP (from our measurement campaign);
- Transmission process: Time to transmit the data.

Let us consider a scenario where an M2M device searches for a service announced every 2 seconds in the Free CN environment. The device will have to wait the following durations to detect, connect and transmit its data:

- 2.7 seconds to detect the service at a 90% success rate (see Figure 4.18);
- 8.254 seconds (on average) before starting the upload process (see Table 4.5);
- and $48ms$ to transmit a $6kB$ packet.

The whole process last approximately 11seconds. So, in this scenario the device will only be able to upload its data using APs which provide coverage for more than 11seconds (which represent only 35% of Free CN APs based on the coverage duration distribution from Figure 4.7a).

Now, let us estimate the probability to successfully transmit this packet. We calculated the probability of a device not having connection errors during the connection process as $P_C = 0.57$. Therefore, coming from an uncovered area, the probability that an M2M device will detect a service – announced in the Free CN environment – and connect to the corresponding AP is of $P_{NM} * P_C$. This device will then be able to successfully transmit its data for less than 57% of the connection attempts – as we do not consider the probability that an error may occur during the transmission.

Therefore, based on the Free CN parameters and our estimations, this device will be able to successfully transmit the collected data with 35% of the available APs and only 57% of the connection attempts will end. So, the likelihood that for the collected data to be transmitted comes down to less than 20%.

In conclusion, the time spent during the connection process is a very limiting factor in the studied scenario. Decreasing the announcement interval increases the likelihood that a device will be able to successfully transmit its data. But reducing the time spent during the connection process – association, IP address acquisition and finishing connection process – increases even more this probability. In fact, the percentage of APs that would be worth connecting to is limited by the connection process time, in the Free CN example it represents 75% of the total time. Therefore, decreasing the connection process time increases the number of potential APs that a device could use to transmit its data and then, it would offer even more possibilities in terms of announcement interval variation.

4.5.4 Discussion

In the previous section, we proposed and evaluated a mathematical model which enabled us to study the impact of using a service announcement mechanism in an IoT traffic retrieval scenario. The results obtained using this model helped us determine which factors impact this scenario.

The first factor impacting the efficiency of this type of scenario – i.e. detection time – is the Wi-Fi AP density within which the desired service is announced. Our model showed that, in a given Wi-Fi AP density, the distribution of time spent in a non-coverage area as well as the desired detection success rate, significantly affected the minimum time needed to detect the service. The second important factor impacting detection time is the announcement interval. In fact, no matter how many APs are used to announce a service, the time necessary to detect the service increases exponentially with the rise of the announcement interval.

Moreover, contrary to the preliminary results obtained using the CTMC, the success rate does not seem to significantly impact the time needed to detect the service. Or at least, it has less impact on detection time than announcement interval and AP density. While the preliminary results suggested that using the "Free CN" density for services that require high success rates (e.g. health services) was not worth deployment. Results obtained using the DTMC model, show the opposite. Not only, could such services be deployed within the "Free CN" density but this could be done with an announcement interval higher than the beacon interval.

While our measurement campaign proved that both time spent during the connection process and the probability of a successful connection were determining factors in devices being able to successfully transmit collected data, these factors were not taken into account in our model. However, our model does help estimating the success rate of transmitting data based on both the detection success rate given and our measurement results.

This study provides some very interesting information on how this type of scenario could be improved to increase the upload success rate. As we already mentioned, the Wi-Fi AP density and the time needed before starting to upload were limiting factors for the upload success in this scenario. We have therefore come up with some solutions that might substantially improve our scenario:

- **Removing the process for retrieving an IP address:** This can be done by pre-assigning IP addresses to devices that have only one action to perform. This will eliminate the time needed to retrieve an IP address, which we recall represented 50% of the connection process time.

- **Allowing devices to store collected data and send several packets in a row:** This would enable devices to optimize connections and save energy by decreasing the number of connections. However, it will increase the need for devices to process information, so a compromise would have to be found.
- **Establishing an efficient subset of APs:** This can be done by selecting only APs which provide coverage duration for at least the time necessary to upload data (association, connection and preparation to upload). This way, devices are sure to be able to upload their data to all the APs announcing the service. Thus, the probability of successfully transmitting the data is the same as the probability of successfully starting to upload.

4.6 Chapter outcome

In this chapter, we studied the validity of a scenario using the LSA mechanism as described in Chapter 3. In this scenario, a company wants to re-use a subset of already deployed APs in order to collect the data measured by its IoT objects. However, this scenario is much more complex than it seems as it requires finding the optimal combination of *a*) the number of nodes to serve; *b*) the subset of APs used; *c*) the detection success rate required (depending on how important the service is); and *d*) the announcement interval, in order to have the best data retrieval success rate possible.

Special attention was been given to the mathematical model and the empirical data used to instantiate it. This model gives us the opportunity to study the impact of the LSA mechanism on our scenario and to identify the specific factors limiting detection time and success. However, it also shows the limitations of our model and shed light on possible improvements. The first improvement we suggest regards the verification of our mathematical model. We lacked some measurements that would have enabled us to more conclusively verify our model. It then implies that other measurement campaigns must be performed with both scanning and connecting devices. Secondly, we think that the Markov chain used here could be improved in order to take into account connection and upload states along with the probability of these processes to fail. After verification, this new version of our model should enable users to determine the time necessary to upload a given amount of data within a specific Wi-Fi environment.

The model used in this chapter allows us to verify our scenario and prove that it is possible to collect IoT traffic in existing Wi-Fi networks. We were able to show that the impact of this IoT data retrieval has a negligible effect on legacy H2H and H2M Wi-Fi traffic. Moreover, the simplicity of the LSA mechanism offers lots of flexibility for this type of scenario as a company can easily add or remove an AP from its pool of participating APs. However, this study also shows that the current connection model, designed for resource-capable devices, prevents it from fully benefiting from this solution. This is because the current connection process is time consuming for this type of scenario. Some solutions have therefore been proposed in order to increase the upload volume traffic in this scenario. These include pre-assigning IoT devices with IP addresses in order to cut down on the time spent during the connection process.

5 Conclusion and Perspectives

5.1 Thesis Outcome

Over the past years, the network environment has tremendously changed. First, the type of connected devices is constantly evolving, offering different characteristics and various access technologies – wired, wireless or cellular. The use of these devices depends on whether or not their characteristics and capabilities are compatible with user needs. In fact, each type of user devices has one strong advantage and has gradually evolved to emphasize this advantage in order to better meet the corresponding user requirement (e.g. mobility, bandwidth, etc.). In parallel, different types of access technologies have been developed and each of them addresses different uses and types of performance. Some of them provide high bandwidth, others mobility support and still others license-free technologies. The popularization of these access technologies means that in most parts of the world there are multiple ways to access a given network. Moreover, there are a wide variety of possible applications to choose from in this environment and this variety will continue to increase with the arrival of new Service Providers (SPs). However, not all applications are suited to be transported by every access technology as some of them have strict requirements in terms of packet delay and loss. As a result, applications need to be adapted according to Access Network (AN) capabilities. Be that as it may, with the proper information, devices could be able to determine the most suited AN for each application among such Complex Heterogeneous Environments (CHEs). Nevertheless, both the multiplication of interfaces and the increasing number of applications to transport increase the need to integrate additional protocols into devices. Furthermore, despite having multiple interfaces, devices do not fully benefit from the diversity of ANs and rather than using their interfaces simultaneously, they use only one at a time and have all traffic adapted to this single connection. As a consequence, the current model centered on a unique active connection (one interface for all the traffic) is slowly becoming more complex and requires devices with more and more resources.

Unfortunately, the arrival of constrained and self- or remote-operated devices, clashes with this one-for-all connection model. In fact, these devices are restricted in terms of resource and energy consumption and therefore need simple selection and connection mechanisms in order to access the appropriate network. In a multiple providers

environment, a simplified selection mechanism could also benefit to less-constrained devices as they would be able to simply sort ANs based on their capabilities and, in particular, on the services they can support. There is therefore a need to define a simple and common mechanism to detect the available network services on each AN. This mechanism will link an abstract representation of a service to the AN providing it. Therefore, enabling devices to use this mechanism to select an AN based on device needs and AN capabilities. This way any device from a CHE could benefit from the diversity of ANs and interfaces, if it has more than one. Furthermore, by associating this mechanism with appropriate decision algorithm, flow distribution and routing protocols, user devices with multiple interfaces could always select, and therefore connect to, the best possible AN for a given service. The resulting framework also enables these devices to maintain session continuity as long as there is an access providing the service, thus offering a Service-based Always Best Connected (S-ABC) capability.

In order to make a service-based selection of ANs possible, we designed a mechanism to announce AN service availability to surrounding devices, called the Lightweight Service Announcement (LSA) mechanism (see Chapter 3). This mechanism reuses existing network discovery messages to advertise service availability. The LSA mechanism is based on a Service Availability Announcement tag, which is included in legacy network discovery messages. This tag contains Service Information and is based on a service ontology to enable automatic interpretation. This tag solution allows devices to detect the available network services when discovering the corresponding network. This mechanism also ensures that services will be represented in the same way to all devices in order to automate this service-based selection. Service announcements will rotate to avoid overloading the tag and therefore, the associated network discovery message. The LSA mechanism allows SPs to announce their services on existing infrastructures even if they do not own them. To do this, they can either insert a device into the desired network, which will announce their services on the network, or rent both service announcements and a restricted access on these infrastructures. This announcing method makes it possible to leverage existing network infrastructure by both increasing the "catalog" of available services in a network and generating additional sources of revenues via access rentals. Finally, we have defined a framework based on the LSA mechanism, MADM algorithms, Shim6 and SDSA in order to ensure that user devices with multiple interfaces can be S-ABC. In a multiple providers scenario, the LSA mechanism is designed to enhance existing usage and define new opportunities.

In Chapter 4, we focused on the application of the LSA mechanism for retrieving data generated by M2M Wi-Fi device. In the studied scenario, a specific service is announced on a subset of already deployed Wi-Fi APs. These announcements inform devices that these APs offer the possibility to collect their data. Before studying the impact of the LSA mechanism on such scenario, we verified its credi-

bility by simulation. These simulations showed that the impact of retrieving M2M traffic via existing Wi-Fi APs on traditional Wi-Fi traffic flows (file download or video streaming) is minimal but proportional to the number of M2M nodes generating traffic. Nevertheless, the high density of APs in some area, associated to the LSA mechanism and its variable announcement, would enable providers to dynamically balance the M2M load on several APs and this way avoiding overloading APs. Then, we further studied the impact of the LSA mechanism on such a scenario using mathematical model. To do this, we first characterized Wi-Fi environments in terms of coverage and connection duration for each discovered Internet Service Providers (ISPs). These measurements, performed with an Android sensing tool called Wi2Me, enabled us to collect empirical data in order to illustrate our scenario. Our connection measurements enabled us to unveil that the time needed to establish a Wi-Fi connection represents 72.3% of the average Wi-Fi coverage duration, which only leaves little time for moving M2M devices to transmit their data. These measurements also showed that it is possible to find a minimal subset of APs to cover a given area and providing as good service detection results as the whole set of discovered APs. Therefore, for given areas, SPs should be able to propose a seamless service availability using an optimal set of APs. These empirical data have then been used to instantiate two Markov chains. These models enabled us to study the impact of the LSA mechanism on different points. First, it helped us study the impact of theAP density used to announced a service and showed that, the time spent without Wi-Fi coverage is a key parameter that impact the time needed to detect an announcement. Then, the success rate of detecting an announcement is linearly increasing this detection time. Finally, the announcement interval is exponentially increasing the time needed to detect a service. Therefore, an optimal trade off has to be found between *a*) the time acceptable to detect a service; *b*) the percentage of Wi-Fi non-coverage area; and *c*) the announcement interval (depending on the importance of a service); in order to have seamless service availability. However, even if using the LSA mechanism, the time needed to establish a connection is a limiting factor for the studied scenario. In order to make our solution more efficient this time has to be decreased, for instance, by pre-assigning M2M devices with IP addresses.

5.2 Future Works

In order to extend the contribution of this thesis, some points may be considered for the future work. First, the network service ontology defined in Chapter 3 could be improved. We start the work on this ontology in order to test our service announcement mechanism but it needs to be further extended. In particular, this ontology should be use with several possible scenarios in order to enhance the service representation and unveil all the necessary attributes necessary to be included. As a result, a ready to use ontology should be available for more global and intensive tests.

Regarding the Markov chain model presented in Chapter 4, other measurements campaigns are required (i.e. perform connections in other area with other Community Networks (CNs)) in order to furthermore assess the discrete-time model reliability. These studies would help determine if, for any other studied paths/areas, this model instantiated with coverage statistics, obtained using scanning devices, provides a similar detection time than the one measured using connecting devices. Moreover, this model could be extended in order to take into account connection and upload states. Currently, the model only considers the covered and uncovered states and therefore, enable us to only determine the time needed to detect a service. Although, it could also model the whole connection process – from the discovery to the end of the connection establishment – and the data upload process, including the probability to encounter errors in these states. This way the model will not only provide the time necessary to detect a service but also it will give the time necessary to complete the connection process and the effective time to upload data along with the amount of data uploaded. As a consequence, this complete model will efficiently help determine the optimal AP density and announcement interval for deploying and announcing a service over existing network infrastructures.

During this thesis, a real life experiment has been started to retrieve, using custom APs, the data generated by ECG sensor monitoring runners. This experiment has not been fully completed and the latest future work is to finish it. In order to do so, the selection of an AP based on information provide by the LSA mechanism has to be implemented in Android device. Once completed, this experiment would make it possible to compare both type of selection – classic and LSA-based – and to determine the efficiency of LSA compare to current solution in a real test-bed. The results obtained with this experiment will allow us to compare different metrics such as relevancy of the chosen AP, time necessary to detect a viable AP, time needed to connect to the corresponding AP, success rate of the performed connections and the amount of data successfully transfer to the server. Besides, the measurements obtained using LSA-capable devices during such an experiment may also be compare to the result obtained using our Markov chain instantiated with this experiment parameters in order to further more validate the model. Finally, many other scenarios – some of them presented during this thesis – could benefit from the use of the LSA mechanism. It is therefore crucial to have a functional LSA-testbed in order to test various scenarios on different access technologies.

5.3 Perspectives

The Lightweight Service Announcement (LSA) mechanism designed in this thesis aim to simplify the discovery of Access Networks (ANs) based on service availability. This mechanism is shifting the versatile model currently used and centered on Internet, toward a more specific service-based model as it enables devices to simplify their vision of the network by sorting available ANs based on their capabilities. In addition to simplifying the network service detection, the LSA mechanism offers several applications possibilities as it facilitate the arrival of new Service Providers (SPs) in current network infrastructures. It especially helps deploy IoT application using existing networks, which until now has a significant impact on ANs.

From a more general perspective, the framework presented at the end of Chapter 3 and based on the LSA mechanism could be implemented to prove its efficiency to provide S-ABC-capable device. This framework allows any user device to select the best possible IP address for a given service among all the available IP addresses. This selection should be performed dynamically and automatically in order to be used in complex intra and inter -technology scenarios. This framework should also enable devices to maintain session continuity without worrying about the IP address modifications that may occur. Several opportunities for users and providers are conceivable using this framework. However, this implementation needs to be closely studied, as it will add features in user devices that could drain even more the battery life of some devices. As soon as the LSA test-bed is completed, it might be extended with this S-ABC framework. It would then be possible to study in depth this framework and the offered opportunities. At the end, devices should be able to decide whether to use the LSA mechanism only or to use the full framework depending on the requirements of the application used. This agility will enable devices to conserve the maximum energy and resource, while ensuring that this framework could be globally used with a minimal impact.

5

Bibliography

[1] S. Abdul Salam, S. A. Mahmud, G. M. Khan, and H. S. Al-Raweshidy. "M2M communication in Smart Grids: Implementation scenarios and performance analysis". In *Wireless Communications and Networking Conference Workshops (WCNCW), 2012 IEEE*, pages 142–147, April 2012.

[2] W. Abramowicz, K. Haniewicz, M. Kaczmarek, R. Palma, and D. Zyskowski. "NFP Ontology for Discovery and Sharing Web Services in Distributed Registries". In *Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008. 22nd International Conference on*, pages 1416–1421, March 2008.

[3] V. Andrei, E. C. Popovic, O. Fratu, and S. V. Halunga. "Solution for Implementing IEEE 802.21 Media Independent Information Service". *IEEE*, 2008.

[4] A. Arcia-Moret, G. Castignani, R. Kuntz, J. Montavont, and N. Montavont. "Defining a framework for flow distribution in mobile and multihomed networks". *unknown*, 2010.

[5] J. Arkko, B. Aboba, J. Korhonen, and F. Bari. "Network Discovery and Selection Problem". RFC 5113 (Informational), January 2008.

[6] K. Ashton. "That 'Internet of Things' Thing". `http://www.rfidjournal.com/articles/view?4986`, 2009. Accessed: 2014-11-10.

[7] M. Bagnulo, A. García-Martínez, and A. Azcorra. "BGP-like TE Capabilities for SHIM6". *EUROMICRO-SEAA*, 2006.

[8] M. Bagnulo, A. García-Martínez, J. Rodríguez, and A. Azcorra. "End-site Routing Support for IPv6 Multihoming". *Comput. Commun.*, 29(7):893–899, April 2006.

[9] F. Baker and P. Savola. "Ingress Filtering for Multihomed Networks". RFC 3704 (Best Current Practice), March 2004.

[10] A. Balasubramanian, R. Mahajan, A. Venkataramani, B.N. Levine, and J. Zahorjan. "Interactive Wifi connectivity for Moving Vehicles". In *ACM SIGCOMM Computer Communication Review*, volume 38, pages 427–438. ACM, 2008.

[11] S. Barré, J. Ronan, and O. Bonaventure. "Implementation and evaluation of the Shim6 protocol in the Linux kernel ". *Computer Communications*, 34(14):1685 – 1695, 2011.

[12] M. Bennis, M. Simsek, A. Czylwik, W. Saad, S. Valentin, and M. Debbah. "When cellular meets WiFi in wireless small cell networks". *Communications Magazine, IEEE*, 51(6):44–50, June 2013.

[13] D. P. Blinn, T. Henderson, and D. Kotz. "Analysis of a Wi-Fi Hotspot Network". In *Papers Presented at the 2005 Workshop on Wireless Traffic Measurements and Modeling*, WiTMeMo '05, pages 1–6, Berkeley, CA, USA, 2005. USENIX Association.

[14] Bluetooth. "Bluetooth Basics". `http://www.bluetooth.com/Pages/Basics.aspx`. Accessed: 2014-11-10.

[15] L. Bokor, A. Huszak, and G. Jeney. "On SCTP multihoming performance in native IPv6 UMTS-WLAN environments". In *Testbeds and Research Infrastructures for the Development of Networks Communities and Workshops, 2009. TridentCom 2009. 5th International Conference on*, pages 1–10, April 2009.

[16] N. Buonaccorsi, C. Cicconetti, R. Mambrini, and V. Pii. "Experience on the demonstration of the ETSI M2M architecture release 1". In *Future Network Mobile Summit (FutureNetw), 2012*, pages 1–7, July 2012.

[17] C. Buratti. "Performance Analysis of IEEE 802.15.4 Beacon-Enabled Mode". *Vehicular Technology, IEEE Transactions on*, 59(4):2031–2045, May 2010.

[18] G. Castignani. *"Exploiting Network Diversity"*. PhD thesis, Telecom Bretagne, Université Européenne de Bretagne, 2012.

[19] G. Castignani, A. Blanc, A. Lampropulos, and N. Montavont. "Urban 802.11 community networks for mobile users: Current deployments and prospectives". *Mobile Networks and Applications*, 17(6):796–807, 2012.

[20] G. Castignani, A. Lampropulos, A. Blanc, and N. Montavont. "Wi2Me: A Mobile Sensing Platform for Wireless Heterogeneous Networks". In *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on*, pages 108–113, 2012.

[21] R. Chandra, J. Padhye, L. Ravindranath, and A. Wolman. "Beacon-Stuffing: Wi-Fi without Associations". In *Mobile Computing Systems and Applications, 2007. HotMobile 2007. Eighth IEEE Workshop on*, pages 53–57, March 2007.

[22] K. Cho, K. Fukuda, H. Esaki, and A. Kato. "The Impact and Implications of the Growth in Residential User-to-user Traffic". *SIGCOMM Comput. Commun. Rev.*, 36(4):207–218, August 2006.

[23] D. H. Choi, K. Kim, H. J. Kim, and S. H. Kim. "Distributed IPv6 Multihoming Support". *IEEE*, 2003.

[24] T. Chown, J. Arkko, A. Brandt, O. Troan, and J. Weil. "IPv6 Home Networking Architecture Principles". RFC 7368 (Informational), October 2014.

[25] T.-Y. Chung, Y.-M. Chen, P.-C. Mao, C.-K. Tsai, S.-W. Lai, and C.-P. Chen. "The Design and Implementation of IEEE 802.21 and Its Application on Wireless VoIP". In *Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st*, pages 1–5, May 2010.

[26] Cisco. "Cisco Visual Networking Index: Forecast and Methodology, 2013-2018". `http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html`. Accessed: 2014-11-10.

[27] Cisco. "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013-2018". `http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html`. Accessed: 2014-11-10.

[28] D. Corujo, C. Guimarães, B. Santos, and R. L. Aguiar. "Using an open-source IEEE 802.21 implementation for network-based localized mobility management". *Communications Magazine, IEEE*, 49(9):114–123, 2011.

[29] A. Dhraief and N. Montavont. "Toward Mobility and Multihoming Unification-The SHIM6 Protocol: A Case Study". In *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, pages 2840–2845, March 2008.

[30] A. Dhraief and N. Montavont. "Rehoming Decision Algorithm: Design and Empirical Evaluation". In *Computational Science and Engineering, 2009. CSE '09. International Conference on*, volume 2, pages 464–469, Aug 2009.

[31] A. Dogac, Y. Kabak, and G. B. Laleci. "Enriching ebXML registries with OWL ontologies for efficient service discovery". In *Research Issues on Data Engineering: Web Services for e-Commerce and e-Government Applications, 2004. Proceedings. 14th International Workshop on*, pages 69–76, March 2004.

[32] Q. Duan. "Automatic network service discovery and selection in virtualization-based future Internet". In *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, pages 1088–1093, Dec 2011.

[33] Ericsson. "Ericsson Mobility Report - November 2014". `http://www.ericsson.com/ericsson-mobility-report`. Accessed: 2014-11-10.

[34] ETSI. "Machine- to- Machine communications (M2M); Functional architecture". Technical report, ETSI, 2011.

[35] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis. "The Locator/ID Separation Protocol (LISP)". RFC 6830 (Experimental), January 2013.

[36] G. Fekete. *"Network Interface Management in Mobile and Multihomed Nodes"*. PhD thesis, Faculty of Information Technology of the University of Jyväskyla, 2010.

[37] G. Fekete and T. Hamalainen. "State of Host-Centric Multihoming in IP networks". *IEEE*, 2009.

[38] P. Ferguson and D. Senie. "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing". RFC 2827 (Best Current Practice), May 2000. Updated by RFC 3704.

[39] R. T. Fielding. *"Architectural Styles and the Design of Network-based Software Architectures"*. PhD thesis, University of California, Irvine, 2000.

[40] C. Fourtet and T. Bailleul. "Method for using a shared frequency resource, Method for manufacturing terminals, Terminals and telecommunication system", December 16 2011. WO Patent 2,011,154,466.

[41] E. Gallet de Santerre, S. Jammoul, and L. Toutain. "Solving the Ingress Filtering Issue in an IPv6 Multihomed Home Network". In *Networks (ICN), 2010 Ninth International Conference on*, pages 272–278, April 2010.

[42] E. Gallet de Santerre and L. Toutain. "IPv6 Ingress Filtering in a Multihoming Environment". In *INFOCOM Workshops 2009, IEEE*, pages 1–2, April 2009.

[43] A. García-Martiínez, M. Bagnulo, and I. Van Beijnum. "The Shim6 architecture for IPv6 multihoming". *Communications Magazine, IEEE*, 48(9):152–157, Sept 2010.

[44] G. Gehlen, E. Weiss, S. Lukas, C.-H. Rokitansky, and B. Walke. "Architecture of a Vehicle Communication Gateway for Media Independent Handover". *WIT*, 2006.

[45] D. Gessler, G. Schiltz, G. May, S. Avraham, C. Town, D. Grant, and R. Nelson. "SSWAP: A Simple Semantic Web Architecture and Protocol for semantic web services". *BMC Bioinformatics*, 10(1):309+, September 2009.

[46] A. Gladisch, R. Daher, and D. Tavangarian. "Survey on Mobility and Multihoming in Future Internet". *Wireless Personal Communications*, 74(1):45–81, 2014.

[47] V. K. Gondi, E. Lehtihet, and N. Agoulmine. "Ontology-Based Network Management in Seamless Roaming Architectures". In *Network Operations and Management Symposium Workshops, 2008. NOMS Workshops 2008. IEEE*, pages 60–65, April 2008.

[48] Google. "Web Metrics". `https://developers.google.com/speed/articles/web-metrics`, 2014. Accessed: 2014-08-15.

[49] F. Guidec, D. Benferhat, and P. Quinton. "Biomedical Monitoring of Non-Hospitalized Subjects using Disruption-Tolerant Wireless Sensors". In *Proceedings of MobiHealth'12*, number 61 in Springer LNICST, pages 11–19, Paris, France, November 2012.

[50] N. Gundu. "Mobility vs Multihoming". In *Seminar on Internetworking*, 2004.

[51] V. Gupta and al. "Media Independent Handover Services". Technical report, IEEE Computer Society, 2009.

[52] V. Gupta and M. K. Rohil. "Information Embedding in IEEE 802.11 Beacon Frame". *IJCA Proceedings on National Conference on Communication Technologies and its impact on Next Generation Computing 2012*, CTNGC(3):12–16, November 2012. Published by Foundation of Computer Science, New York, USA.

[53] V. Gupta and M. K. Rohil. "Bit-Stuffing in 802.11 Beacon Frame: Embedding Non-Standard Custom Information". *International Journal of Computer Applications*, 63(2):6–12, February 2013. Published by Foundation of Computer Science, New York, USA.

[54] V. Gupta and M. K. Rohil. "Modeling user preferences for vertical handover in 3G-WLAN interworking environment on top of IEEE 802.11u". In *Advance Computing Conference (IACC), 2013 IEEE 3rd International*, pages 164–169, Feb 2013.

[55] E. Gustafsson and A. Jonsson. "Always best connected". *Wireless Communications, IEEE*, 10(1):49–55, Feb 2003.

[56] G. Habault, P. Maille, L. Toutain, A Pelov, N. Montavont, and P. Bertin. "Lightweight service announcement: The case for Wi-Fi M2M service providers". In *Advanced Networks and Telecommuncations Systems (ANTS), 2013 IEEE International Conference on*, pages 1–6, Dec 2013.

[57] G. Habault, L. Toutain, N. Montavont, and P. Bertin. "Service-Based Network Selection Proposal for Complex Heterogeneous Environments". In *IEEE Globecom 2014 TCS Workshop*, Dec 2014.

[58] J. Hagino and H. Snyder. "IPv6 Multihoming Support at Site Exit Routers". RFC 3178 (Informational), October 2001.

[59] B. Hariharan, K. Sreejith, and Sangeet. "Power aware seamless emergency communication for heterogeneous wireless networks". In *Wireless and Optical*

Communications Conference (WOCC), 2012 21st Annual, pages 83–88, April 2012.

[60] Y. He, D. Wu, and T. Yu. "Research on Service Discovery and Matching Based on Ontology and Service Capabilities in Manufacturing Grid". In *Computer Science and Information Engineering, 2009 WRI World Congress on*, volume 5, pages 707–711, March 2009.

[61] J. Heflin, J. Hendler, and S. Luke. "SHOE: A Knowledge Representation Language for Internet Applications". Technical report, Dept. of Computer Science, University of Maryland at College Park., 1999.

[62] T. Henderson and A. Gurtov. "The Host Identity Protocol (HIP) Experiment Report". RFC 6538 (Informational), March 2012.

[63] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda. "Performance anomaly of 802.11b". In *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, volume 2, pages 836–843 vol.2, March 2003.

[64] F. Hussain and J. Y. Pyun. "Coordinator Discovery and Association in Beacon-Enabled IEEE 802.15.4 Network". *International Journal of Distributed Sensor Networks*, 13, 2013.

[65] IEEE 802.11. "IEEE P802.11u: Interworking with External Networks Task Group U". IEEE Computer Society, 2004.

[66] IEEE Std 802.11-2007. "IEEE Standard for Information Technology — Telecommunications and Information Exchange Between Systems — Local and Metropolitan Area Networks — Specific Requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", June 2007.

[67] IEEE Std 802.15.4-2011. "IEEE Standard for Local and Metropolitan Area Networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)".

[68] IEEE Std 802.15.4-2011. "IEEE Standard for Local and Metropolitan Area Networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), Amendment 5: Physical Layer Specifications for Low Energy, Critical Infrastructure Monitoring Networks", June 2013.

[69] IEEE Std 802.21-2008. "IEEE Standard for Local and metropolitan area networks- Part 21: Media Independent Handover", 2009.

[70] IEEE Std 802.3-2008. "IEEE Standard for Information Technology — Telecommunications and Information Exchange Between Systems — Local and Metropolitan Area Networks-Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 4: Media Access Control Parameters, Physical Layers and Management Parameters for 40 Gb/s and 100 Gb/s Operation", June 2010.

[71] A. Ismail and B.-H. Roh. "Adaptive Handovers in heterogeneous networks using fuzzy MADM". In *Mobile IT Convergence (ICMIC), 2011 International Conference on*, pages 99–104, Sept 2011.

[72] H.-J. Kim and S.-H. Hong, Y.-G.and Kim. "IPv6 multihoming for NGN". In *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*, volume 3, pages 4 pp.–2147, Feb 2006.

[73] M. Kim, T.-W. Moon, and S.-J. Cho. "A study on IEEE 802.21 MIH frameworks in heterogeneous wireless networks". In *Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on*, volume 1, pages 242–246. IEEE, 2009.

[74] L. Kleinrock and S. Lam. "Packet Switching in a Multiaccess Broadcast Channel: Performance Evaluation". *Communications, IEEE Transactions on*, 23(4):410–423, 1975.

[75] X. Lagrange. "Very Tight Coupling between LTE and Wi-Fi for Advanced Offloading Procedures". In *WCNC 2014 : IEEE Wireless Communications and Networking Conference*, 2014.

[76] G. Lawton. "Machine-to-machine Technology Gears up for Growth". *Computer*, 37(9):12–15, 2004.

[77] E. Lear. "NERD: A Not-so-novel Endpoint ID (EID) to Routing Locator (RLOC) Database". RFC 6837 (Experimental), January 2013.

[78] K. Lee, J. Lee, Y. Yi, I. Rhee, and S. Chong. "Mobile Data Offloading: How Much Can WiFi Deliver?". *Networking, IEEE/ACM Transactions on*, 21(2):536–550, 2013.

[79] K. J. Lee, S. S. Nam, and B. I. Mun. "SCTP Efficient Flow Control During Handover". *IEEE*, 2006.

[80] W.-S. Lim, D.-W. Kim, Y.-J. Suh, and J.-J. Won. "Implementation and performance study of IEEE 802.21 in integrated IEEE 802.11/802.16e networks". *Comput. Commun.*, 32(1):134–143, 2009.

[81] S. Liu, J. Bi, and Y. Wang. "A Shim6-Based Dynamic Path-Selection Mechanism for Multi-homing". In *Evolving Internet, 2009. INTERNET '09. First International Conference on*, pages 46–51, Aug 2009.

[82] S. Liu, J. Bi, and Y. Wang. "A Shim6-Based Dynamic Path-Selection Mechanism for Multi-homing". In *Evolving Internet, 2009. INTERNET '09. First International Conference on*, pages 46–51, Aug 2009.

[83] X. Liu and L. Xiao. "A survey of Multihoming Technology in Stub Networks: Current Research and Open Issues". *IEEE Network*, 2007.

[84] A. Matsumoto, K. Fujikawa, Y. Okabe, F. Teraoka, M. Kunishi, M. Ohta, and M. Ishiyama. "Multihoming Support based on Mobile Node Protocol LIN6". *SAINT*, 2003.

[85] K. Medepalli and F. A. Tobagi. "Throughput analysis of IEEE 802.11 wireless LANs using an average cycle time approach". In *Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE*, volume 5, pages 5 pp.–3011, Dec 2005.

[86] M. A. Mehaseb, Y. Gadallah, and H. El-Hennawy. "WSN Application Traffic Characterization for Integration within the Internet of Things". In *Mobile Ad-hoc and Sensor Networks (MSN), 2013 IEEE Ninth International Conference on*, pages 318–323, Dec 2013.

[87] S. Mignanti, V. Suraci, and C. Di Menna. "An Ontology-Based Multi-Protocol Service Discovery Framework". In *Mobile and Wireless Communications Summit, 2007. 16th IST*, pages 1–5, July 2007.

[88] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler. "Transmission of IPv6 Packets over IEEE 802.15.4 Networks". RFC 4944 (Standards Track), September 2007. Updated by RFC 6775.

[89] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson. "Host Identity Protocol". RFC 5201 (Experimental), April 2008.

[90] M. Mudassir Feroz and A. K. Kiani. "SHIM6 Assisted Mobility Scheme, an intelligent approach". In *Consumer Communications and Networking Conference (CCNC), 2013 IEEE*, pages 725–728, Jan 2013.

[91] S. A. Mushtaq, C. Lohr, and A Gravey. "An Integration of Semantics in Multi Criteria Decision Making for Converged Multimedia Network Management". In *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, pages 712–717, Dec 2011.

[92] T. Narten, E. Nordmark, W. Simpson, and S. Soliman. "Neighbor Discovery for IP version 6 (IPv6)". RFC 4861 (Standards Track), September 2007. Updated by RFC 7048.

[93] E. Nordmark and M. Bagnulo. "Shim6: Level 3 Multihoming Shim Protocol for IPv6". RFC 5533 (Standards Track), June 2009.

[94] C. Perkins, D. Johnson, and J. Arkko. "Mobility Support in IPv6". RFC 6275 (Standard Tracks), July 2011.

[95] T. Pötsch, S. Marwat, Y. Zaki, and C. Görg. "Influence of Future M2M Communication on the LTE System". In *proceeding of: the 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC) 2013*, April 2013.

[96] J. Puttonen, G. Fekete, T. Vaaramaki, and T. Hamalainen. "Multiple Interface Management of Multihomed Mobile Hosts in Heterogeneous Wireless Environments". In *Networks, 2009. ICN '09. Eighth International Conference on*, pages 324–331, March 2009.

[97] L. L. Qu and Y. Chen. "QoS ontology based efficient web services selection". In *Management Science and Engineering, 2009. ICMSE 2009. International Conference on*, pages 45–50, Sept 2009.

[98] R. Regele. "Using Ontology-Based Traffic Models for More Efficient Decision Making of Autonomous Vehicles". In *Autonomic and Autonomous Systems, 2008. ICAS 2008. Fourth International Conference on*, pages 94–99, March 2008.

[99] P. Sarolahti and A. Kuznetsov. "Congestion Control in Linux TCP". In *Proceedings of the FREENIX Track: 2002 USENIX Annual Technical Conference*, pages 49–62, Berkeley, CA, USA, 2002. USENIX Association.

[100] M. Z. Shafiq, L. Ji, A. X. Liu, J. Pang, and J. Wang. "Large-Scale Measurement and Characterization of Cellular Machine-to-Machine Traffic". *Networking, IEEE/ACM Transactions on*, 21(6):1960–1973, Dec 2013.

[101] Siemens. "Internet of Things: Facts and Forecasts: Billions of Things, Trillions of Dollars, 2014". `http://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/internet-of-things-facts-and-forecasts.html`. Accessed: 2014-11-10.

[102] J. Y. H. So, J. Wang, and D. Jones. "SHIP mobility management hybrid SIP-HIP scheme". In *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2005 and First ACIS International Workshop on Self-Assembling Wireless Networks. SNPD/SAWN 2005. Sixth International Conference on*, pages 226–230, May 2005.

[103] Q. Song and A. Jamalipour. A network selection mechanism for next generation networks. In *Communications, 2005. ICC 2005. 2005 IEEE International Conference on*, volume 2, pages 1418–1422 Vol. 2, May 2005.

[104] R. Stewart. "Stream Control Transmission Protocol". RFC 4960 (Standards Track), September 2007. Updated by 7053.

[105] M. Tauil, A. Dutta, Y.-H. Cheng, S. Das, D. Baker, M. Yajnik, D. Famolari, Y. Ohba, V. Fajardo, K. Taniuchi, and H. Schulzrinne. "Realization of IEEE 802.21 services and preauthentication framework". In *Testbeds and Research Infrastructures for the Development of Networks Communities and Workshops, 2009. TridentCom 2009. 5th International Conference on*, pages 1–10, April 2009.

[106] F. Teraoka, M. Ishiyama, and M. Kunishi. "LIN6: A Solution to Mobility and Multi-Homing in IPv6". Internet Draft, June 2003.

[107] S. Tozlu and M. Senel. "Battery lifetime performance of Wi-Fi enabled sensors". In *Consumer Communications and Networking Conference (CCNC), 2012 IEEE*, pages 429–433, Jan 2012.

[108] I. A. Valdovinos and J. A. P. Diaz. "TCP Extension to Send Traffic Simultaneously through Multiple Heterogeneous Network Interfaces". In *Computer Science (ENC), 2009 Mexican International Conference on*, pages 89–94, Sept 2009.

[109] P. Vidales, A. Manecke, and M. Solarski. "Metropolitan Public WiFi Access Based on Broadband Sharing". In *Computer Science (ENC), 2009 Mexican International Conference on*, pages 146–151, Sept 2009.

[110] C. Vogt. "Six/One: A Solution for Routing and Addressing in IPv6". Internet-Draft, October 2009. Expired.

[111] A. Vulpe, S. Obreja, and O. Fratu. "A study of mobility management using IEEE 802.21". In *Electronics and Telecommunications (ISETC), 2010 9th International Symposium on*, pages 205–208, Nov 2010.

[112] J. Z. Wang, F. Ali, and R. Appaneravanda. "A Web service for efficient ontology comparison". In *Web Services, 2005. ICWS 2005. Proceedings. 2005 IEEE International Conference on*, pages –844, July 2005.

[113] N. Wang and G. Pavlou. "An Efficient IP Based Approach for Multicast Routing Optimisation in Multi-homing Environments". *Crown*, 2006.

[114] Business Wire. "Fon Announces Next Generation Fonera Simpl with EAP Optimized for Mobile Devices", 2012.

[115] K. P. Yoon and C. L. Hwang. *"Multiple Attribute Decision Making: An Introduction"*. Number nos. 102-104 in Multiple Attribute Decision Making: An Introduction. SAGE Publications, 1995.

5

ANNEXES

TELECOM Bretagne

A

Résumé long

Depuis plus de vingt ans, le nombre d'appareils connectés à Internet a continuellement augmenté. Ces appareils connectés peuvent être divisés en deux catégories : ceux dont le comportement dépend de la volonté et des besoins de leurs utilisateurs. Et les objets autonome qui ont généralement des ressources limitées et qui émettent de manière périodique des données. Un rapport de Siemens [101] planifie que le nombre d'objets connectés dépassera d'ici quelques années celui des appareils des utilisateurs. Comme leurs utilisations sont différentes, leurs besoins en termes de bande passante et de délais le sont aussi. Qui plus est, l'arrivée de nouvelles applications misent au point pour fonctionner sur une grande variété d'appareils a participé à une considérable augmentation du volume de données échangées sur les réseaux filaires. Comme le présente [22] et [26], cette augmentation est exponentielle. Cette tendance est également pressentie dans les réseaux sans fil comme cela a déjà commencé à être mesuré et montré dans [27]. Par conséquent, et pour satisfaire d'une part ce besoin grandissant en bande passante, et d'autre part le nombre croissant d'appareils connectés, les technologies d'accès ont dû évoluer. Cependant, aucune d'entre elles ne pouvant répondre à l'ensemble de ces besoins, leurs nombres s'est vu décuplé. Par conséquent, dans la majorité du monde, il existe plusieurs manières de se connecter à un réseau. Les appareils ont donc actuellement à disposition plus qu'un réseau d'accès et bien souvent, via différentes technologies. La popularisation de l'Internet Protocol (IP) sur ces différentes technologies d'accès, qui au passage étend la couverture de l'Internet, participe également à l'augmentation du trafic échangé dans cet écosystème.

De nos jours, les appareils peuvent donc avoir plusieurs interfaces de communication afin d'accéder à diverses technologies d'accès. Cela leur permet de profiter, dans toutes situations, de la diversité de réseau d'accès mentionné précédemment. Ces appareils ont les capacités nécessaires pour profiter pleinement de cette grande variété d'accès, c.-à-d. utiliser plusieurs de leurs interfaces simultanément. Hors, nous observons que ceux-ci n'ont pas les mécanismes nécessaires pour le faire efficacement. Et au contraire, ces appareils n'utilisent actuellement qu'une seule de leurs interfaces et l'ensemble de leurs flux de données transitent par cette unique interface. Cependant, ce fonctionnement ne garantit pas que l'interface sur laquelle l'appareil est connecté soit la plus adaptée pour chaque flux de données, car ils peuvent avoir des besoins différents. Qui plus est, ce modèle de connexion unique, basé sur une

seule interface active pour plusieurs applications, augmente la complexité des protocoles sous-jacents. En effet, les flux de données transitant sur cette même interface nécessitent d'être adaptés au réseau d'accès utilisé. Ce modèle pose d'autant plus de problème avec l'arrivée des objets connectés. En effet, ceux-ci sont différents des appareils des utilisateurs au niveau du flux de données qu'ils produisent et de leurs capacités limitées. Par conséquent, un nouveau modèle de connexion est nécessaire, qui ne serait pas centré sur Internet, et qui permettrait de profiter pleinement de la diversité d'accès, tout en limitant la consommation de ressource et d'énergie pour des appareils restreints.

Dans cette thèse, nous proposons plusieurs contributions pour permettre à n'importe quel type d'appareil – contraint et non-contraint – de bénéficier de cette diversité de réseaux d'accès. La première contribution est de définir un mécanisme permettant aux appareils de distinguer parmi un ensemble de réseaux d'accès, ceux capables de transporter un certain type de flux de données. En effet, ce mécanisme permet aux réseaux d'accès d'annoncer leurs compatibilités à certains services ainsi que les paramètres associés. Ainsi, les appareils découvrant ceux-ci peuvent comparer les paramètres des services découverts aux besoins du flux de données à transporter, et donc choisir le réseau d'accès le plus optimal pour transporter chaque flux séparément. La deuxième contribution est de proposer un système de protocoles permettant aux appareils avec plusieurs interfaces réseaux de toujours sélectionner la meilleure interface pour un flux donné. En effet, un appareil avec plusieurs interfaces pourrait utiliser différents réseaux d'accès simultanément. Ainsi en associant notre mécanisme de découverte de services à différents protocoles de décision et de routage, il est possible de choisir une interface différente pour chaque flux à transporter et ce, en se basant sur les besoins de ceux-ci. Pour cela, le mécanisme de découverte doit être disponible et identique sur toutes les technologies d'accès. Qui plus est, les mécanismes de découverte et de décision doivent être simple, automatisé et transparent pour l'utilisateur car ces actions devront être réalisées continuellement et parfois sur des appareils avec peu de ressources et peu, voir pas, d'interactions avec l'utilisateur.

A.1 Présentation de la Thèse et des Contributions

Dans cette thèse, nous avons étudié les différents réseaux d'accès, ainsi que la multitude d'appareils pouvant se connecter à ceux-ci. L'environnement réseau dans lequel ces appareils évoluent se complexifie avec l'augmentation du nombre d'appareils en jeu et du nombre de technologie d'accès. Cette étude nous a ainsi permis de proposer une solution simple pour annoncer les capacités des réseaux d'accès, ainsi que les services associés à chacun d'eux. Cette solution permet aux appareils découvrant ces réseaux d'accès de profiter de la diversité de services, de fournisseurs et de technologie d'accès en facilitant la sélection et individualisant la connexion avec ceux-ci.

Le mécanisme Lightweight Service Announcement

Afin de permettre aux appareils de profiter de cette abondance de réseaux d'accès, et donc des services associés, nous proposons d'effectuer une sélection de ces réseaux d'accès basée sur l'accessibilité à des services. Les services disponibles sur chaque réseau d'accès seraient ainsi annoncés à tous les appareils, permettant à ceux-ci de sélectionner le réseau d'accès le plus adapté à leurs besoins. Plusieurs protocoles et architectures existent mais aucun d'eux ne proposent une méthode simple et générique pour récupérer les informations supplémentaires nécessaire pour une sélection spécialisée. Après une étude succincte des différents protocoles de découverte des technologies d'accès, nous avons définis un mécanisme permettant d'annoncer la disponibilité des services, comme présenté dans [56]. Notre mécanisme Lightweight Service Announcement (LSA) est simple et léger car il se base sur des tags et réutilise les messages de découverte des différentes technologies d'accès. Il fonctionne également sur une ontologie permettant d'organiser les différents services. Ainsi avec ce mécanisme, tous types d'appareils peuvent détecter et interpréter automatiquement la disponibilité d'un service sur l'ensemble des réseaux d'accès découvert. Ce mécanisme offre de nombreux avantages car il permet aux appareils de filtrer, sans l'intervention de l'homme, les réseaux d'accès fournissant un service donné. Il permet donc d'aider les appareils dans leur choix du réseau d'accès le plus approprié à leurs besoins. Pour au final, sélectionner, parmi ceux qui sont disponibles, celui qui fournira le service recherché et avec les meilleurs paramètres possibles. Le mécanisme LSA a un très faible impacte car il réutilise au maximum les messages des mécanismes de découverte des technologies d'accès. Qui plus est, il offre de nouvelles opportunités de déploiement de services et il est complétement rétro-compatible.

Un système Service-based Always Best Connected

Afin de profiter pleinement de la diversité des réseaux d'accès, les appareils des utilisateurs – avec peu de limitations et plusieurs interfaces – pourraient également profiter du mécanisme Lightweight Service Announcement (LSA). En effet, celui-ci pourrait leur permettre de déterminer le meilleur fournisseur d'accès pour chaque flux de données afin de distribuer ces flux simultanément sur différentes interfaces. Dans cette optique, nous avons défini un système basé sur notre mécanisme, un algorithme de décision, un protocole permettant de manipuler aisément les adresses IP et un protocole de routage [57]. Ce système permet aux appareils avec plusieurs interfaces de toujours sélectionner à n'importe quel endroit et à tout moment, le meilleur réseau d'accès disponible et donc assure qu'ils seront toujours connectés au meilleur d'entre eux. Qui plus est, cette distribution dynamique des flux de données sur différentes interfaces et de manière simultanée, permet d'assurer la continuité de n'importe quelle session de communication aussi longtemps qu'un réseau d'accès supportant le service en question est disponible. Ce système devrait nettement améliorer l'expérience utilisateur avec les appareils et les services actuels, tout en

permettant d'en développer de nouveaux.

Modèle mathématique du comportement d'appareils Wi-Fi

Afin d'aller plus loin dans l'étude de notre mécanisme Lightweight Service Announcement (LSA) et en particulier pour déterminer l'impact de son utilisation, nous avons modélisé le comportement d'appareil Wi-Fi se déplaçant dans une zone urbaine. Ce modèle permet d'estimer le temps nécessaire, ainsi que le taux de succès, pour découvrir un réseau Wi-Fi. Il permet également dans le cas de l'utilisation de notre mécanisme, d'estimer le temps nécessaire pour détecter la disponibilité d'un service sur un de ces réseaux sans fil et le taux de succès pour y accéder. Différents environnement Wi-Fi ont été caractérisés à l'aide d'un outil Android. Les données ainsi récoltées, nous ont permis d'initialiser les chaînes de Markov sur lesquelles repose ce modèle. Les données collectés durant nos campagnes de mesures, nous ont également permit d'étudier l'importance de la distribution des points d'accès pour la découverte de ce type de réseau/service (c.-à-d. temps de détection/découverte et taux de succès). Ce modèle pourrait notamment permettre de définir la distribution optimale de point d'accès pour annoncer de façon homogène un service dans une zone définie.

A

A.2 Plan

Cette thèse est composée de trois chapitres. Tout d'abord, nous présentons la variété et l'hétérogénéité des environnements réseaux dans lesquelles les appareils évoluent actuellement. La diversité présente dans ces environnements complexes soulève de nombreux défis. Dans cette thèse, nous nous intéressons tout particulièrement sur la possibilité de sélectionner un réseau d'accès en fonction des services qu'il peut fournir. Pour cela, nous étudions les solutions existantes pour répondre à ce défi, leurs avantages et leurs limitations. Cette thèse a pour but de rendre possible la sélection du réseau d'accès le plus approprié au besoin d'un appareil sans se soucier de la technologie d'accès utilisée.

Ensuite, nous présentons notre solution, le mécanisme Lightweight Service Announcement (LSA), rendant possible une sélection basée sur l'accessibilité d'un service pour tous types d'appareils et sans se soucier de la technologie d'accès. Ce mécanisme permet aux fournisseurs d'accès et de services, d'annoncer la disponibilité de services, ainsi que leurs paramètres, sur un réseau d'accès via différents points d'attachements. Pour cela, et afin d'automatiser l'annonce de service et la sélection du réseau d'accès, les services sont organisés de manière standardisé et hiérarchique à l'aide d'une ontologie. Ainsi tous les équipements en jeu dans cette sélection utilisent la même représentation. Les annonces de services, ainsi représentés de manière standardisée, facilitent l'interprétation de leurs disponibilités et donc l'automatisation de la sélection du réseau d'accès le plus approprié. Qui plus est,

ce mécanisme peut être utilisé avec d'autres protocoles, afin de permettre aux appareils des utilisateurs, en plus de sélectionner le réseau d'accès le plus approprié, de toujours être connecté au meilleur d'entre eux et sur n'importe quelles interfaces. Ainsi, dans un scénario de compétition entre différents fournisseurs de services, notre mécanisme devrait permettre d'améliorer l'utilisation de réseaux existants et de voir se déployer de nouvelle opportunités.

Pour finir, nous présentons un scénario de test utilisé pour étudier l'efficacité de notre mécanisme LSA. Ce scénario novateur consiste à réutiliser les points d'accès Wi-Fi résidentiel pour collecter les données générées par des objets mobile. En effet, les réseaux résidentiels, étant peu utilisés en journée, pourraient permettre la récupération de données sans avoir à déployer de nouvelles infrastructures. Des simulations ont été établies pour valider ce scénario et sa faisabilité. Le comportement de ces appareils Wi-Fi mobiles a été modélisé en utilisant des chaînes de Markov. Ces modèles mathématiques, initialisés par des données empiriques, nous ont permis d'étudier le temps ainsi que le taux de succès nécessaire pour détecter la disponibilité d'un service sur un réseau d'accès dans différentes configurations. Avec ces modèles, nous avons pu évaluer l'impact de la fréquence d'annonce des services, l'importance de la densité des réseaux d'accès et de la distribution des points d'accès, ainsi que le volume de données collectées. Cela permet notamment de déterminer pour une certaine distribution, la fréquence d'annonce optimale afin de collecter un maximum de données. Nous avons pu conclure que même avec un petit nombre de point d'accès et une fréquence d'annonce élevée, notre mécanisme permettait de collecter les données de plusieurs objets contraints avec un impact minimal sur les utilisateurs classique des réseaux Wi-Fi.
En conclusion, le mécanisme LSA facilite la détection de services disponibles sur les réseaux d'accès et donc la sélection du plus approprié d'entre eux pour satisfaire un besoin donné. Qui plus est, il offre de nombreuses perspectives pour déployer de nouveaux services et améliorer l'utilisation des réseaux actuels. Cependant, notre étude mathématique a montré qu'un compromis devait être trouvé entre la densité de point d'attachement et la fréquence d'annonce du service et ce notamment en fonction du service demandé. Celle-ci permet également de mettre en avant les limitations du modèle de connexion actuel (une connexion complexe pour transporter tous types de flux). Nous proposons donc dans cette thèse d'améliorer ce modèle, en l'individualisant et pour cela d'utiliser des solutions basées sur notre mécanisme. Afin d'aller plus loin dans l'étude de ce mécanisme plusieurs perspectives d'amélioration sont envisageables. Tout d'abord, le modèle mathématique gagnerait à être étendu afin de pouvoir estimer les temps de connexion à un réseau d'accès. Et ensuite, le mécanisme lui-même pourrait être implémenté et expérimenté en situation réelle afin de valider complètement notre modèle basé sur des chaînes de Markov et prouver l'efficacité du mécanisme LSA.

A

B

Publications

IETF Draft

G. Habault, E. Gallet de Santerre, and L. Toutain. "Proposal for Selecting the Default-route according to Source Address". Informational, February 2012. IETF Internet-Draft.

International Conference and Workshop

G. Habault, P. Maille, L. Toutain, A Pelov, N. Montavont, and P. Bertin. "Lightweight service announcement: The case for Wi-Fi M2M service providers". In *Advanced Networks and Telecommuncations Systems (ANTS), 2013 IEEE International Conference on*, pages 1–6, Dec 2013.

G. Habault, L. Toutain, N. Montavont, and P. Bertin. "Service-Based Network Selection Proposal for Complex Heterogeneous Environments". In *IEEE Globecom 2014 TCS Workshop*, Dec 2014.

To Be Published

G. Habault, P. Maillé, X. Lagrange, L. Toutain, N. Montavont, and P. Bertin. "Mathematical Model for re-using Wi-Fi Deployment to Support M2M traffic". 2015.

B

C

Acronyms

6LoWPAN 6 Low Power Wireless Personal Area Network 19
AN Access Network 9
ANQP Access Network Query Protocol 29
AP Access Point 11
ABC Always Best Connected 34
S-ABC Service-based Always Best Connected 36
CI Capability Information 24
CSMA/CA Carrier Sense Multiple Access with Collision Avoidance 18
CO Cellular Operator 30
CN Community Network 37
CHE Complex Heterogeneous Environment 13
CTMC Continuous-Time Markov Chain 82
CER Customer Edge Router 26
DTMC Discrete-Time Markov Chain 86
ECG Electrocardiogram 67
ETSI European Telecommunications Standards Institute 30
GAS Generic Advertisement Service 29
GNSO Generic Network Service Ontology 41
HN Home Network 20
HI Host Identity 56
HIP Host Identity Protocol 55
H2M Human-to-Machine 16
H2H Human-to-Human 16
ISM Industrial Scientific and Medical 18
IE Information Element 24

IoT Internet of Things . . . 22
IP Internet Protocol . . . 9
ISP Internet Service Provider . . . 20
LSA Lightweight Service Announcement . . . 10
LAN Local Area Network . . . 19
LIN6 Location Independent Network Architecture for IPv6 . . . 55
LTE Long Term Evolution . . . 18
LR WPAN Low Rate Wireless Personal Area Network . . . 18
M2M Machine-to-Machine . . . 22
MIH Media Independent Handover . . . 27
MIES Media Independent Event Service . . . 27
MICS Media Independent Command Service . . . 27
MIIS Media Independent Information Service . . . 27
MIP Mobile IP . . . 55
MS Mobile Station . . . 17
MADM Multi-Attribute Decision Making . . . 55
NDP Neighbor Discovery Protocol . . . 25
NSC Network Service Capabilities . . . 31
NSID Network Service Identifier . . . 44
NS2 Network Simulator . . . 67
OWL Web Ontology Language . . . 42
OWL-S Web Ontology Language-Service . . . 42
PoA Point of Attachment . . . 11
PReq Probe Request . . . 24
PRes Probe Response . . . 29
QoE Quality of Experience . . . 16
QoS Quality of Service . . . 16
RSSI Received Signal Strength Information . . . 25
REST Representational State Transfer . . . 31
RDF Resource Description Framework . . . 28
RA Router Advertisement . . . 26
RS Router Solicitation . . . 26
SA Service Announcer . . . 44

SP Service Provider . . . 11
SSID Service Set Identification . . . 24
SU Service User . . . 44
SVAN Service-based Virtual Access Network . . . 51
Shim6 Site Multihoming by IPv6 Intermediation . . . 55
SHOE Simple HTML Ontology Extensions . . . 42
SSWAP Simple Semantic Web Architecture and Protocol . . . 42
STA Station . . . 29
SCTP Stream Control Transmission Protocol . . . 55
TLV Type-Length-Value . . . 28
TCP Transmission Control Protocol . . . 68
UPID Unique Provider Identifier . . . 44
UDP User Datagram Protocol
VW-ISP Virtual Wireless ISP . . . 64
Wi-Fi Wireless Fidelity . . . 11
WLAN Wireless Local Area Network . . . 18
WPAN Wireless Personal Area Network . . . 19
WSN Wireless Sensor Network . . . 19
WWW World Wide Web . . . 16

Résumé

L'environnement réseau dans lequel évoluent les utilisateurs et leurs appareils a beaucoup changé depuis quelques années. En effet, celui-ci se complexifie à mesure que les appareils, les services et les technologies d'accès évoluent. Il existe deux types d'appareils dans cet environnement : les appareils qui dépendent de la volonté et des besoins de leurs utilisateurs et les objets connectés qui ont des ressources limitées et qui émettent périodiquement des données. Comme les utilisations de ces appareils sont différentes, leurs besoins en terme de bande passante et de délais le sont aussi. Cependant, aucune technologie d'accès ne pouvant répondre à l'ensemble de ces besoins ainsi qu'à la multitude d'appareils en jeu, le nombre de technologies d'accès s'est vu décuplé. Par ailleurs, avec la généralisation du protocole IP au sein de ces différentes technologies, la couverture de l'Internet s'étend continuellement. Par conséquent, dans la majorité du monde, il y a plusieurs manières d'accéder à un réseau.

Les utilisateurs pourraient profiter de cette abondance de réseaux d'accès, et des services associés, en sélectionnant le réseau d'accès le plus adapté à ses besoins. L'objectif de cette thèse est de proposer un mécanisme qui permettrait d'annoncer les différents services disponibles sur chaque technologie d'accès et vers tout type d'appareil. Notre mécanisme, Lightweight Service Announcement (LSA), est simple car se base sur des tags ; réutilise les messages de découverte des réseaux d'accès ; et fonctionne avec une ontologie pour organiser les différents services. Ainsi, il permet de détecter et interpréter automatiquement la disponibilité d'un service sur l'ensemble des réseaux d'accès découvert. Par conséquent, ce mécanisme aide les appareils dans leur choix du réseau d'accès le plus approprié pour un service donné. Qui plus est, ce mécanisme d'annonce de service peut être associé avec d'autres protocoles. Cette association permet aux appareils qui peuvent utiliser plusieurs technologies d'accès, de toujours sélectionner et de se connecter au meilleur des réseaux d'accès et à tout moment. Le résultat de cette association assure la continuité de n'importe quelle session de communication.

Nous avons étudié l'impact de notre mécanisme LSA avec un scénario de récupération de données collectées par des objets mobiles. Ce scénario novateur de réutilisation des points d'accès Wi-Fi domestiques est décrit en détails avant d'en étudier sa faisabilité. Différents environnement Wi-Fi ont été caractérisés à l'aide d'un outil Android. Les données récoltées ont permit d'initialiser une chaine de Markov complexe représentant notre scénario. Cette étude mathématique nous as permit d'évaluer l'impact et la validité de notre mécanisme selon différents paramètres dont : la densité des points d'accès, la fréquence des annonces et le taux de succès de la récupération des données. Nous avons ainsi pu démontrer que notre proposition permet d'améliorer les temps de connexion.

Mots-clés : Environnement réseaux complexe et hétérogène, Internet des objets, Protocoles de réseaux d'ordinateurs, Annonce et découverte de services, Chaînes de Markov

Abstract

The network ecosystem has tremendously changed in the past years and is becoming more complex as devices, available services and access technologies are continuously evolving. Devices currently at stake in this ecosystem can be divided into two categories: user devices, which usage depend on the user willingness and requirements, and constrained self or remote-operated devices, which usually have resource constraints and which usage happen at regular intervals. As usage is different, needs in terms of delay, bandwidth and coverage are also different. None of the existing access technologies manage to fulfill all the needs and requirements of this multitude of different devices. The number of access technologies has then spread to cover these needs and with the generalization of Internet Protocol (IP) over these different technologies, Internet coverage is constantly expanding. As a result, in most parts of the world there are multiple ways to access a given network.

Devices could benefit from this diversity of access technologies, and associated services, to select their accesses based on their needs and service availability. The purpose of this thesis is to propose a mechanism to inform any device from a Complex Heterogeneous Environment on available services within each access technology. Our Lightweight Service Announcement (LSA) mechanism is simple, re-uses existing network discovery messages and is based on an ontology. Therefore, it allows any device to automatically detect and interpret the service availability of each discovered Access Network (AN). As a consequence, LSA mechanism helps devices in their decision and service-based selection of the most appropriate AN. Finally, this service announcement mechanism could be associated with other protocols in order to enable user devices with multiple interfaces to always select and connect to the best possible AN at any given time and in any given location. The resulting framework will ensure session survivability for each application.

We studied the impact of the LSA mechanism in a scenario of M2M data retrieval using existing Wi-Fi deployment. This scenario is fully described before presenting its credibility based on M2M traffic characterization and simulations. Afterward, different Wi-Fi environments are characterized using an Android tool, which also helps us collect empirical data. These data are used to instantiate mathematical models of the studied scenario. Markov chains have been used to model this Wi-Fi M2M scenario and help us evaluate the impact and validity of our proposal depending on different parameters such as the Access Point density, the frequency of service announcement and the success rate of data retrieval. We managed to show that our proposal could enhance the network environment in numerous ways, but it would require additional work.

Keywords : Complex and Heterogeneous network Environment, Internet of Things, Computer Network Protocols, Announcement and Discovery of Services, Markov chain

TELECOM Bretagne

n° d'ordre : 2015telb0328

Télécom Bretagne

Technopôle Brest-Iroise - CS 83818 - 29238 Brest Cedex 3

Tél : + 33(0) 29 00 11 11 - Fax : + 33(0) 29 00 10 00