Helsinki University of Technology Networking Laboratory Report 6/2006
Teknillinen korkeakoulu Tietoverkkolaboratorio Raportti 6/2006
Espoo 2006

BUSINESS MODELS FOR WIRELESS INTERNET ACCESS

Heikki Hämmäinen, Editor
Antero Kivi, Editor

Helsinki University of Technology
Department of Electrical and Communications Engineering
Networking Laboratory

Teknillinen korkeakoulu
Sähkö- ja tietoliikennetekniikan osasto
Tietoverkkolaboratorio

Distributor:
Helsinki University of Technology
Networking Laboratory
P.O. Box 3000
FI-02015 TKK
Tel: +358-9-451 2461
Fax: +358-9-451 2474

ISBN 951-22-8573-8
978-951-22-8573-0
ISSN 1458-0322

Otamedia Oy
Espoo 2006

PREFACE

This report consists of selected student papers presented and evaluated as part of the seminar ”Business Models for Wireless Internet Access” at the Helsinki University of Technology during autumn 2006. As facilitators of the seminar and chief editors of the report we feel that the seminar was successful when looking at the commitment of students and the energy they put into papers.

The seminar topic was chosen because the adoption of wireless local area network (WLAN, IEEE 802.11) technology in mobile handsets is creating space for new value networks and business models. The drivers of this phenomenon are (1) the unlicensed spectrum of WLAN which lowers entry barriers of new players and (2) the indoor focus of WLAN which gives control to building owners. As a consequence some forward-looking municipalities, businesses, and consumers have started providing public Internet access through their own WLAN base stations. It remains to be seen whether the new value networks are able to seriously challenge the central role of traditional fixed and mobile operators.

The first paper by Teemu Rinta-aho provides an introduction to the underlying wireless technology and the problem of network selection in multiradio terminals. Syed Ali Raza extends the technology framework into heterogeneous networks focusing on the Ambient Networks project.

Niklas Tirkkonen studies WLAN regulation and challenges the formal definition of public telecommunications provider.

Real world examples of WLAN business models are grouped in municipality-driven models by Magnus Sippel and Jussi Laukkanen, office-driven models by Joonas Ojala, public facilities driven models by Sampo Hämäläinen, and consumer-driven models by Mathias Tallberg.

The remaining papers focus on specific aspects of WLAN adoption in order to help understand the business dynamics better. Antero Kivi describes the challenge of measuring the user behavior and traffic in a decentralized multiradio environment. Hannu Verkasalo analyzes the role of WLAN in the alternative value networks of mobile voice-over-IP services. Jouni Mäenpää studies the value networks for extending Internet access with ad hoc type of wireless scenarios. Finally Pekka Nurmiranta discusses the question of social optimality of alternative WLAN value networks and business models.

Otaniemi, December 6, 2006

Heikki Hämmäinen	Antero Kivi
Professor	M.Sc.

TABLE OF CONTENTS

I. Dynamic Selection of Optimal Wireless Access Service

TEEMU RINTA-AHO
Helsinki University of Technology
teemu.rinta-aho(a)tkk.fi

Abstract

The number of different wireless access technologies is increasing, as well as the number of players on the market of Internet access. New terminals – both laptops and handsets often come equipped with more than one type of wireless access, like WLAN and 3G. When the number of options increases, the problem of selection becomes more important. This paper describes the problem of dynamic selection of optimal wireless access service, and then some of the current solutions and ongoing research are introduced.

1 Introduction

The number of different radio access technologies (RATs) and operators has been increasing over the past few years. Currently the mobile phone networks provide not only voice service but also packet data service. For example in Finland, GPRS is available practically everywhere and new 3G mobile networks are available in the biggest cities, as well as Wireless LANs, either operated by the same or different operators that run the mobile phone networks. Besides public access networks, more and more homes and enterprises install their own wireless networks.

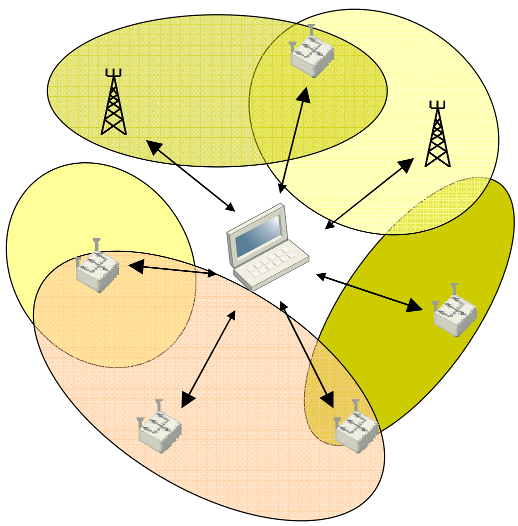

Figure 1: Multiple wireless accesses

The number of network technologies supported by mobile terminals is also increasing. Current portable computers usually have at least LAN and WLAN interfaces, some models may have also Bluetooth and analog modem – if not integrated, they can be added to the mobile system via e.g. USB interface. Mobile phones are going through similar development - besides GSM and UMTS radio they often come with Bluetooth and even WLAN.

The increasing amount of networks available and the increasing support for different networks in mobile terminals provide the mobile users with better network connectivity. However, an immediate question arises: if there are options, which one should be taken? More specifically, which network(s) should be used?

To answer this question we must first understand the different requirements set by the mobile users, operators, applications being used, and system status like battery usage and speed of movement.

This paper introduces the problem of *dynamic access selection*. In section 2 the problem is discussed. In section 3 an overview to current solutions is presented. In section 4 current research done in Ambient Networks and elsewhere is presented, and in section 5 the paper is concluded.

2 Problem

The problem of dynamic access selection is not limited to wireless or mobile devices, but solving the problem efficiently is more crucial for terminals that are moving, and especially for those that run on battery power. For any access network, wireless or cable, the problem is selecting the “best” access at a given time. The best access could be for example the cheapest access that provides the minimum QoS required by the running applications.

In some use cases it may be beneficial to use multiple accesses at the same time to gain e.g. smaller delay [9], but also because some services might be only available via a certain access network. In that case the access selection needs to be done also higher in the protocol stack, either per packet or per connection.

Different accesses may belong to different IP subnets. Selecting an access may result in an IP layer handover and e.g. Mobile IP [7] signaling. This should also be taken into account when doing access selection.

Basically access selection in a wireless environment can be divided to different sub problems:

- Selecting which interface(s) to power on
- Selecting which network to attach, if any

- Selecting which AP to attach, if any
- For application: which interface to use on a multi-RAT terminal

After the access selection a network attachment process may be required to obtain connectivity over the network, but that is out of scope of this paper. Network attachment would include everything required for the node being able to access the Internet, e.g. configuring IP addresses, AAA and mobility updates.

2.1 Current Wireless Access Technologies

Current available public wireless access networks are mostly built on IEEE technology (e.g. 802.11) or ITU/3GPP technology (GSM). These networks have different capabilities regarding bandwidth, delay, support for QoS, security etc. Also both groups create new versions of the standards, which create a situation where dozens of different types of networks may be deployed simultaneously. User may, for example, be in the coverage area of several 802.11a, 802.11b and 802.11g networks as well as 2G (GSM) and 3G (UMTS) networks.

2.2 Access Discovery

Selecting the access requires that the accesses are first discovered. Discovery of the wireless network is usually done by scanning the specified frequencies and listening to broadcast messages. There are two options, the mobile client can either wait for a periodic broadcast message (i.e. beacon) or it may actively request network information by sending a broadcast itself. The details depend on the RAT implementation.

An important question regarding access selection is that what information is available from the discovered networks. Usually the beacons are kept small to not waste the radio resources and they only contain information like the network name and maybe some information regarding the setup (e.g. supported security features with 802.11i [12]). This information might however be inadequate, as it doesn't currently say anything about e.g.

- Network level services
- Network load
- Pricing
- Roaming agreements

Consider the following example: the mobile user has a laptop which has an IPv4-only stack. When the WLAN hardware scans for available access points it makes the decision to associate with the access point to which it has the best signal-to-noise ratio (usual access selection criteria). However, the selected access point is connected to a network that only supports IPv6. The end result is that the applications on the laptop can't make any Internet connections. Similar problem arises when the access point is connected to a network that the user either has no subscription or the subscription cannot be negotiated on-line.

This problem can be solved in several ways. One simple way is to have previously configured information of the networks beforehand. The drawback is that whenever the networks change configuration it is not propagated to the mobile clients.

Another way is to put all possible information in the beacons. Here the drawback is that enlarging the beacon size reduces the available bandwidth for other data traffic, as it is broadcast typically every 100 ms to all mobile nodes (802.11) – even those that are already connected [11].

A better way to help mobile nodes in selecting the access is to make discovery two-stage. Only critical information like the network ID is put into the beacon, and extra information, like available services, is only available on request. This requires that the mobile client requests this second-stage advertisement from the access point and receives it as a unicast reply. With this kind of multi-stage approach it is also possible for a mobile client to send its identity to the access point, and it could then receive a "personalized" second-stage advertisement [5]. This advertisement could then include more private information like network load, if the identity of the mobile client can be authenticated. Typically the networks don't want to send load information to anyone who just anonymously listens to the access points.

It is also possible to send advertisements through other channels than the radio access in question. If the mobile user is already connected to the Internet, other accesses could be searched from a directory in the Internet [5]. The business models for this kind of directory service could be of several types. Either the mobile users themselves keep this kind of directory in a P2P fashion, the co-operating operators themselves or it could be a broker type of business where information of the available accesses are sold, or even bundled to selling of the access itself.

2.3 Access Selection

The most typical real life situation today is when a laptop user sits down and wants to have internet connectivity and he/she is facing the problem of selecting which WLAN network to use (see 2).

The problem is not that severe in the startup phase, as there are typically no applications running yet. But what happens when the user becomes mobile and goes out of the network coverage that he/she has chosen – while having a discussion over an IP phone call? Then the system should automatically select a new access to maintain the connectivity required by the applications.

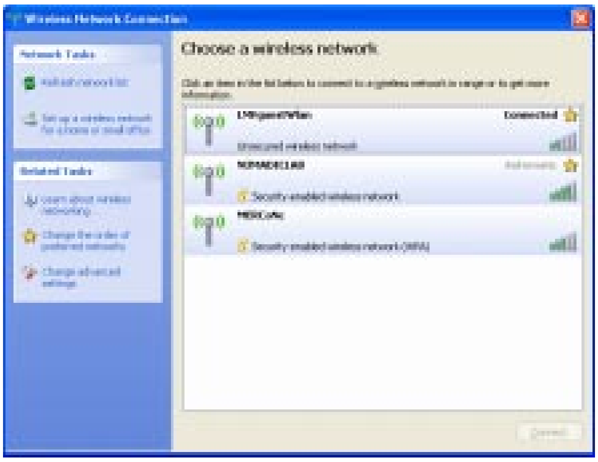

Figure 2: Where do you want to connect today?

First problem is to select which RAT to use, if the terminal has support for multiple different network technologies, like WLAN and 3G. It might not be the best option to have both switched on all the time. This decision depends on the running applications. Currently it could be possible to have a preference to use WLAN for multimedia and 3G for speech, for example, but in the future when the high-speed WCDMA radio accesses are available, the choice might not be that obvious. This is the case especially when both networks belong to the same operator and can be used with the same subscription and with the same rate.

Second step would be to select which network should be used. This requires running the discovery process on the selected RAT. Even if discovered accesses use the same RAT, they may differ in every other aspect:

- They belong to different administrative domains (operators)
- The services they offer may have different
    - IP connectivity
    - QoS
    - Security
- The cost of using the access may differ

After the network has been selected, there is still the selection of the used access point. This is typically a RAT internal process, and might be located in the mobile client, in the network, or they might work in co-operation. Currently in 802.11 based systems it is the mobile client that selects the access point that has the strongest signal quality. In the GSM networks (GPRS, UMTS) it is the network that does the decision.

It is also possible to use multiple accesses at the same time. Then the access selection is done once more higher in the networking stack. One way to do this is to separate different data streams over different accesses based on the application requirements or even split the data stream over different accesses on a per-packet basis [9].

At different stages of access selection some input parameters are required, as well as an algorithm that selects the best option from a given set. These input parameters can be either static or dynamic. Typically the static input is e.g. preferences or policies set by the user, like (“always use the cheapest access” or “always use WLAN if available”). Dynamic input is both the status of the mobile client (running applications, battery status, available protocols) and the network (signal quality, load, price). I have collected some example inputs into a table (see Table 1). These inputs have been grouped into different classes, and further each may have one or more of the following attributes:

- Discoverable before attachment
- Measurable by client
- Possible price effect

Inputs that are discoverable before attachment are information that can affect the selection of the network before attaching to it. Client measurable inputs can be proven correct or wrong by the client. For example the true end-to-end QoS can only be measured this way. The client may then store this data and use the history data in the future when selecting the access network. Some of the inputs may affect the price of using the network.

Depending on the user preferences, the priorities of different inputs can be evaluated. If the user wants to save money, then the price information is the most important input. If he instead prefers the best service, then inputs like signal quality and network load become more important than price. The preferences might be complex and not just “low price” or “good quality”.

3 Current Support for Access Selection

Access selection inside the RAT currently consists of two steps:

- Selection of the network
- Selection of the access point

Selection of the network typically happens based on some pre-configured information. In 802.11 systems the mobile client may have a configuration file that lists the network IDs that are usable, and possibly some keys or certificates that are to be used for security. For example, in wpa_supplicant [13] each network can be given a priority number, so the smallest number wins in the case that several known networks are in sight simultaneously. In the GSM system the terminal contains a SIM card that stores the identity and keys for the user. User is restricted to the subscribed network and networks that have made a roaming contract with the subscribed network. When the terminal is switched on, it searches for available networks and picks the one with the best signal quality among the allowed options. It is, however, possible for the user to list “preferred networks”.

Currently it is not possible to dynamically choose e.g. the cheapest network, but the user needs to obtain this information via e.g. WWW pages of the operators.

The selection of the access point (inside the selected network) is done by signal quality in WLAN. The only major drawback with this simple algorithm is that if there are many access points nearby, load balancing could be done also. This would require a RRM node which controls a set of APs and it is not currently used in WLAN networks

In GSM networks, selection of the access point is based on signal quality between the mobile terminal and the resource usage information. The mobile terminal makes measurements and the network makes the decision which access point the terminal should connect at any given time.

Access selection *between* available RATs in current systems, like laptops, is usually done manually by the user, by switching on and off the network interfaces. For example, in Windows XP, the default interface will be the one that has been switched on last. It is possible for the applications to explicitly select the outgoing network connection, but it is not possible to distribute optimal access selection into every running application. Therefore there needs to be a common function that controls the access selection.

UMTS release 7 will integrate WLAN with 3GPP network [2]. It will not change WLAN AP selection inside the WLAN network, it only defines the selection of the WLAN access, which should belong to the same network as the WCDMA access.

4 Research

There are currently several areas where access selection or multi-access technology are being worked on. In IETF, both Mobile IP and HIP allow the mobile node to do “vertical handovers” between access networks or even use several access networks simultaneously [10].

Another area where research for access selection is being done is the radio access networks. Selecting the optimal input parameters for access selection to gain maximum bitrates have been researched, like in [4]. The simulation studies showed that a terminal with WCDMA and WLAN interfaces could get good results with a simple access selection principle “use WLAN if coverage”. This is valid when the WLAN offers significantly faster bitrates than WCDMA and/or with light traffic loads. However, with higher WCDMA bitrates (like in the coming HSDPA) and with higher loads in hotspots, better results can be achieved when taking the network load into account.

Research is also ongoing in transport area. One of the recent studies [9] show that when optimally combining the use of different access networks, delay and energy consumption per packet can be smaller than with just one single access. This, however, requires that the QoS parameters for each access are known. Also running the selection algorithm on real devices takes CPU cycles away from packet handling and also consume battery.

When looking at all this work done with access selection on different areas raises the question that how will they work together. Thinking of the traditional network architecture – which layer should be responsible for access selection, and should it happen in the network or in the terminal? Ambient Networks is a project that has high ambitions to put different models and networks together.

4.1 Ambient Networks

Ambient Networks (AN) is an integrated project (IP) co-sponsored by the European Commission under the Information Society Technology (IST) priority under the 6th Framework Programme. It has over 35 partners including operators, manufacturers and academia. It aims to provide solutions for mobile and wireless systems beyond 3G [3].

Ambient Networks offer a new vision based on dynamic composition of networks. This goal is realized by introducing the Ambient Control Space, which controls the underlying networks and provides the users with “Ambient Connectivity” and new services.

One of the work items in the project is the Multi-Radio Access (MRA) architecture [8]. One of the key objectives of the MRA architecture is the efficient utilization of multi-radio resources. The main components of the MRA are Generic Link Layer (GLL) and Multi-Radio Resource Manager (MRRM).

The main task of the GLL is the collecting of measurement data from the underlying RATs and abstracting/normalizing it so that MRRM can optimize the combined resource usage of the access networks it controls. GLL can also act as a layer between the *Advertisement and Discovery* function in ACS and in the RATs.

MRRM controls the resource usage by managing *flow sets.* A flow is simply a generic name for a connection between two locators.

The *Detected Set* is formed by accesses that have been discovered. The *Candidate Set* contains accesses that could be used for a flow between the two ANs. The candidate set is filtered from detected set by e.g. applying some static preferences or policies. The *MRRM Active Set* lists the accesses that should be used for connections on MRRM level, and *GLL Active Set* may be a subset, if some accesses map to different GLL entities (see Figure 3). Filtering the active sets from the candidate set is based on measurements done by MRRM.

Both MRRM and GLL are parts of the Ambient Control Space, so they are not handling the actual data traffic. Instead, they control the existing mechanisms in RATs or the functions in RATs have extensions that allow communication with the ACS.

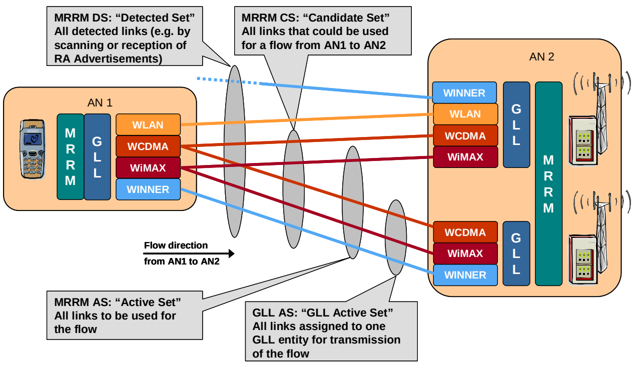

Figure 3: Multi-Radio Resource Management

MRA should enhance the performance for multi-radio mobile clients in areas where coverage areas of different RATs overlap. For example, a hotspot might have both 3G and WLAN access points (of different operators). If all mobile clients in the hotspot follow the simple rule “use WLAN if available” together with the WLAN AP selection logic to use the AP with best signal quality, the result might be that one WLAN access point gets overloaded while other access points have remaining capacity. By combining different sources of information (3G load, WLAN load, user movement, etc.) MRRM can control that the resources of both networks are used optimally, and the users get the best possible service.

Besides GLL, Ambient Networks is also considering other sources of information to base the access selection on, like user input, application requests, context information, dynamic roaming agreements etc.

5 Conclusions

The number of different wireless access technologies is increasing, as well as the number of players on the market of Internet access. New terminals – both laptops and handsets often come with support for more than one type of wireless access, like WLAN and 3G. It is at least the mobile users’ interest to be able to use accesses of different operators with the same terminal, if not for saving money, then for having better coverage for Internet access.

New Internet based applications, like VoIP, are getting more and more popular. A voice call can survive breaks of few hundred milliseconds without disruption in service quality.

Taking all this progress on different fields into account, the problem of dynamic access selection becomes quite important. The problems are with the number of inputs that should be considered together with the limited processing capabilities and battery life of mobile devices. Some example inputs have been collected into a table and categorized to some extent based on different attributes. It can be argued that it is the client that has the ultimate decision which of the input parameters are most important.

Research and standardization are done on many fields: IEEE, IETF and 3GPP have all different ideas and interests of access selection. Different research groups are looking at different parts of the networking system trying to solve the problem or to find optimal algorithms for access selection. New projects, like Ambient Networks, try to take “everything” into account, to be able to provide the users best possible service, any time, anywhere. The following years, and the market, will show which approach was “the best”.

References

[1] 3G Partnership Program, http://www.3gpp.org/

[2] 3GPP system to Wireless Local Area (WLAN) interworking, 3GPP TS 23.234 version 7.0.0, ETSI, 2005

[3] Niebert, Norbert et al: Ambient Networks - Research for Communication Networks Beyond 3G, Proc. IST Mobile Summit, 2004

[4] Yilmaz, Oya et al: Access Selection in WCDMA and WLAN Multi-Access Networks, IEEE VTC Spring 2005

[5] Ho, Lester et al: Business Aspects of Advertising and Discovery concepts in Ambient Networks, PIMRC 2006

[6] Host Identity Protocol (work in progress), IETF HIP WG, 2006, http://www.ietf.org/internet-drafts/draft-ietf-hip-base-06.txt

[7] Mobility Support in IPv6, RFC 3775, IETF, 2004

[8] Koudouridis, G. P. et al: Multi-Radio Access in Ambient Networks, EVEREST workshop “TRENDS IN RADIO RESOURCE MANAGEMENT (2nd Edition)”, 2005

[9] Younis, Mohamed et al: Optimal Dynamic Transport Selection for Wireless Portable Devices, Wireless Communications and Mobile Computing, 2006

[10] Pierrel, Sebastien et al: Simultaneous Multi-Access extension to the Host Identity Protocol (work in progress), IRTF HIP RG, 2006

[11] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE, 1999, ISO/IEC 8802-11: 1999

[12] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications -- Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE, 2004

[13] wpa_supplicant of HostAP project: http://hostap.epitest.fi/wpa_supplicant/

Appendix

Table 1: Example of inputs for access selection

Class	Inputs	Example	D	M	PE
Access network status	Bandwidth	11 Mbps	X	X	X
	Signal quality	78%	X	X	
	Load	25%	(X)		
	Delay	50 ms		X	
	End-to-end QoS	1 Mbps, 75 ms		X	X
	Available services	IPv4	(X)	X	X
Access network attributes	Security	WPA2	X	X	X
	Coverage	1 AP only			X
Terminal status	Running applications	VoIP call	X	X	
	Battery level	2 h left	X	X	
Terminal attributes	Available network interfaces	WLAN, 3G	X	X	
	Available network protocols	IPv4, IPv6	X	X	
Context information	Movement speed	42 km/h	X	X	X
	Movement direction	240º	X	X	
	Geographical location	N 60º 08.532 E 024º 40.034	X	X	X
Business parameters	Price	€ / MB	(X)	X	X
	Available credentials and subscriptions	SIM card	X	X	X
User preferences	Preferences, rules	”Use cheapest”	X	X	X

D = Discoverable before attachment   M = Measurable by client   PE = Possible Price Effect

II. Conceptual Frameworks for Interconnection of Heterogeneous Networks

SYED ALI RAZA
Helsinki University of Technology
sraza(a)cc.hut.fi

Abstract

The paper will present conceptual frameworks for interconnection of heterogeneous networks in techno-business prospective. The framework aims to provide seamless interoperation between heterogeneous networks belonging to different operators or technology domains. Ambient Networks, an EU project, is providing such capabilities for further openness of interfaces that would bring new business opportunities for new players in global market. The concept of network composition and mobility between heterogeneous technologies will bring mass changes in network business. The paper will discuss the interconnection architecture of Ambient Networks, its business model and regulatory aspects.

1 Introduction

Ever since the advancement of telecommunications is taking place, mobile technologies remained the fastest growing in last decade. The advent of new technologies brought new challenges for people in techno-business sector. On one hand the creative destruction horrifies vendors and operators, at the same time it brought new business opportunities. Numerous networks with diverse services are offered to users highlighting the concept of value network. The number of different radio access technologies and operators has been increasing over the past few years. The incompatibilities and inconsistencies between network functionalities [1] limit the potential usefulness of the available networks and infrastructure. End users are increasingly not just owners of a terminal or PC; they own and effectively operate a network of devices at their homes and offices, and around the body.

The Wireless World Initiative (WWI) is a set of 5 coordinated research projects – MobiLife, SPICE, Ambient Networks, WINNER and E2R –spanning the communications stack from future wireless air interfaces, through ambient networking, adaptive radio systems, service provisioning frameworks and distributed application architecture. There are some other projects as well addressing the interconnectivity of heterogeneous networks. The concept of bridging between different heterogeneous networks is introduced to create more business prospects. It aims to provide end-to-end communication that is generally hurdled by seamless bridging between networks and hiding complexities of these networks from each other. **Ambient Network** project [8] is investigating how heterogeneous network configurations and diverse mobile user systems and applications with specific mobility requirements can be integrated into an internetworking architecture, which supports flexible plug & play and easy deployable network services at the same time. The scope of the paper will target ambient network, as one of the method for interconnections of heterogeneous networks.

2 Ambient Network Architecture

An ambient network [6] aims to provide a domain-structured end-to-end view for the network control. In this way, an ambient network is expected to embrace the heterogeneity arising from the different network control technologies such that it appears homogeneous to the potential users of network services. The vision is to allow agreement for cooperation between networks on demand, transparent, and without the need of pre configuration or offline negotiation between network operators. The idea of being operator is drastically changed over the years, as every one can be owner of their own networks at homes and offices.

Figure 1 [6] shows the common distributed control space that encapsulates both legacy and future internetworking infrastructures and shows example functionality such as support for overlay networks or network context. This new common control plane functionality can be integrated as an add-on to existing legacy networks.

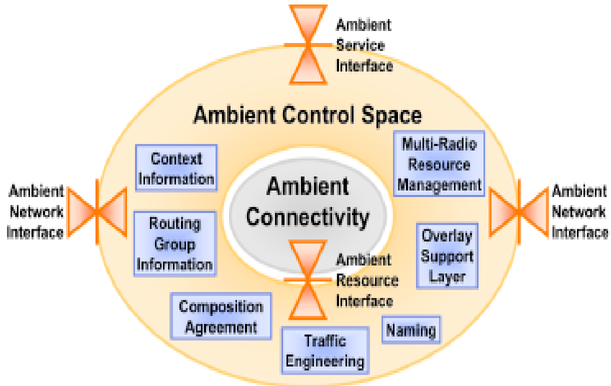

Figure 1: Ambient Network modularization and interface

2.1 Composition

Network composition [5] takes a central part in the Ambient Networks project. It means integration of different networks. Current systems provide this facility only for data plane. However network composition allows dynamic and instantaneous interoperation in control plane. By instantaneous interoperability we mean global availability of user services through different network technologies. Or in other words one user of a particular network service provider can be facilitated seamlessly by any other network technology provider. Composition can result in one single AN comprising of several ANs managing all logical and physical resources contributed by each constituent AN. This main AN has its own ambient control space (Figure 1) controlling all its resources, and communicates to the outside with its own identifier and via its own ambient network interface.

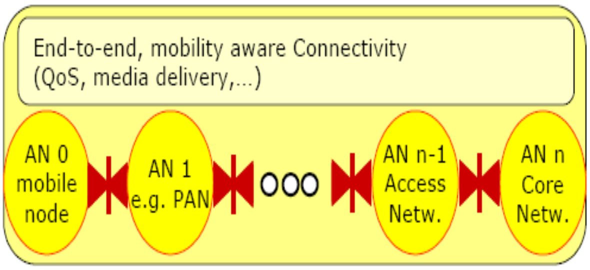

Figure 2: Composition in AN

Composition can result into one or more AN that is influenced by policies and trust aspects between the network operators. Depending on the agreement resources belonging to constituent ANs might stay under the control of each individual AN.

Another new aspect that composition brings to network cooperation is the automation of this process. Automation means automatic and seamless availability of networks. This requires pre-negotiated agreements between different network operators. The network cooperation can be between all kinds of networks, from individual devices (Bluetooth or Zigbee etc) to cellular networks.

2.2 Mobility

AN focuses on integrated mobility [8] concepts. The traditional concept of roaming is extended to a wider framework, i.e., providing roaming between different network technologies. There are four main ideas in AN mobility, handover and locator management, reachability management, moving network support, and triggering.

Handover and locator management takes care of handover procedure in ambient environment. ***Reachability management*** ensures that the corresponding node is always built to locate AN node. ***Moving network support*** handles routing groups along with its formation, maintenance and management. ***Triggering*** is to collect and identify various events from different sources and process them according to the policies. Figure 3 [7] refers to all the above mentioned concepts in AN mobile management. It should be however noted that in order to facilitate these concepts inter-process communication is needed.

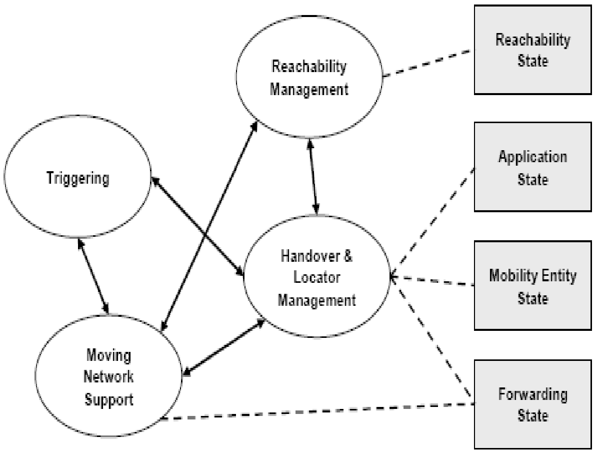

Figure 3: Mobility Management in AN.

2.3 Heterogeneity

AN is an attractive business idea as it supports multiple networks of different operators and technologies, which results in availability of a wide range of services at a low cost to the customer. However realization of such a solution is challenging from technical viewpoint. Heterogeneity addresses the issue of hiding complexities of one network from the other both on application and application developer level by providing the same or interoperable link technologies, IP versions, media formats and user contexts.

For example, consider a media context in which the concern is to accommodate differences between contexts, while still providing an end-to-end service. In order to do so data may have to be manipulated at context borders. This can be done through introduction of the Interstitial Function (IF) [3], whose purpose is to allow data to pass between two adjoining contexts. Contemporary examples of IFs include Network Address Translator (NAT) boxes, signaling gateways, and Border Gateway Protocol BGP routers. IFs may explicitly be used to bridge dissimilar transport networks (e.g. IPv4 onto ATM).

3 Business Model

ANs project focuses on new networking technologies but the strategic goals are very much driven by business considerations, as can be understood by the objectives in the project definition. “The Ambient Networks project aims at an innovative, industrially exploitable mobile network solution, which enables the composition of networks across business and technology boundaries in order to stimulate new business developments and growth in the wireless domain”[4].

We have already mentioned briefly the technical aspects of composition and now our objective is to explore its business side. To give a clear picture we divide this section into two further subsections. In the network composition process, we will elaborate how the composition will come into business reality. Where as, in the market actors, we will further elaborate the key players involved and their possible relationships in value networks.

3.1 Network Composition Process

Network Composition as described earlier can support many different cases, e.g. Cellular network (2G,3G etc) interconnecting to Personal Area Network or residential network connected to sensor network, or a moving network with a cellular network. Users want to pay for “continuous connectivity” that eventually reflects in value networks. The composition process on business level consists of the five phases; Media Sense, Discovery & Advertisement, Security & Internetworking Establishment, Composition Agreement Negotiation and Composition Agreement Realization.

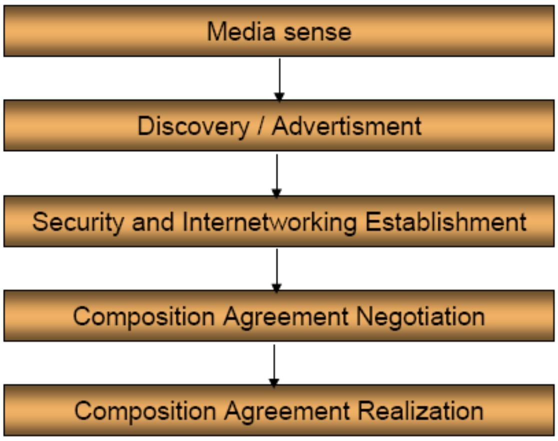

Figure 4: Phases of Composition Process

Figure 4 [7] shows the process of composition in sequence, which can be further described as [7],

Media Sense is to sense a medium that enables communication with a neighboring node, another network or device. The “sensing” also includes the case of discovering a link to a remote AN.

Discovery & Advertisement leads to selection phase; selecting a candidate AN for composition. It also allows discovering other ANs identifiers, resources, capabilities and (networks) services.

Security and Internetworking Connectivity phase is needed after discovery phase as any two ANs need to establish interconnectivity taking care of security aspects through cryptography or third party authentication.

Composition Agreement (CA) Negotiation phase includes negotiations on terms and conditions. Composition Agreement negotiation aims to agree on technology and business. CA template could include the following items; ID, Service description, QoS requirements/guarantees, Legal issues and financial issues, monitoring and performance reporting, problem and failure reporting.

Composition Agreement Realization concludes Network composition. It includes configuration of networks according to Composition Agreement negotiated earlier.

3.2 Market Actors

Business Model Roles will explain the presence of different players, which will be involved to interconnect heterogeneous networks. As the Ambient Network aims to create market opportunities and increase competition and cooperation, several new key players can enter in role with established giants of telecom market.

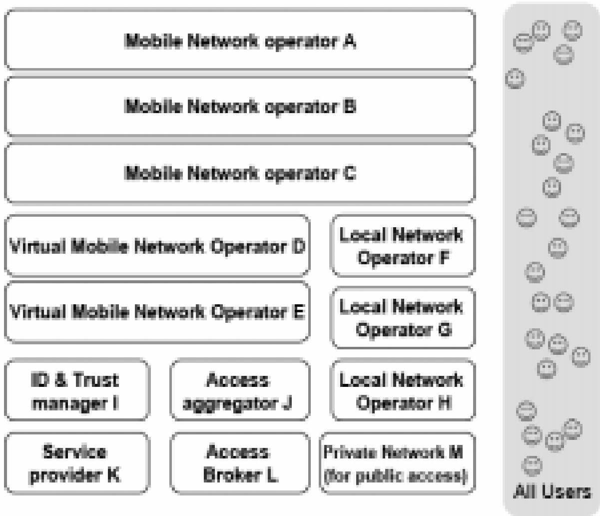

Figure 5: Market Actors in Ambient Networks

Figure 5 [4] shows the key market actors which will play important role in Ambient networks, for the sake of simplicity some business model roles (Clearing House, Compensation service providers) are intentionally avoided. We will briefly look at all these potential “Market Movers”; which includes Local Network operators, Access Aggretator, Access Broker, service provider and ID & Trust Manager.

Local Network Operators- LNO provides local network access and services to local customers. For example, local network can be provided in chain stores which might also be used to provide services.

Access Aggregators will aggregate and bundle lots of LNOs. Access aggregator is justified due to presence of large number of LNOs.

Access broker provides end to end connections between LNOs and access aggregators. It could also have billing relationships with customers, where as its customer ranges from end user to Mobile Network operators.

Service provider works like access aggregator, it bundles services for customers. As ANs will deal with wide range of customers and access networks, it needs to have higher service availability for all the users.

ID & Trust Manager is used to provide common ground for all the parties in need of trust for secure activities that includes authentication, authorization, id management and payment issues.

4 BIG Picture

We have discussed network composition and its market actors. Now it can be summed up through different approaches to make a BIG picture of Ambient Networks that is the concept of value network comes in integration of market actors and composition.

Value Network can be defined as *a web of relationships that generates economic value and other benefits through complex dynamic exchanges between two or more individuals, groups or organizations. Any organization or group of organizations engaged in both tangible and intangible exchanges can be viewed as a value network, whether private industry, government or public sector.*

Market actors as discussed earlier are involved in making complex value networks, aiming to benefit each other through cooperation and competitiveness following rules and regulations imposed by regulatory authorities.

In such a 'value network' each player has different capabilities and resources.

Figure 5 [7] illustrates market actors' interaction in one of the most simplified forms. The presence of thousands of actors around the world makes it **complex** and challenging.

Governance is an important aspect of organizational arrangements in value networks. Value network governance must be distributed in three strong bodies [2]. First the basic rules for participating in the value network have to be set. Secondly, it is necessary to audit performance and check compliance with the set rules. Thirdly, value network participants may be supported in meeting the rules. The question that raises eye brows for small players is who is the **'governor'**? AN keeps Mobile Network Operators (MNO) as heart throbs of network, which creates **insecurity of small players**, as they can be easily swept out depending on goals of MNOs.

As far as users are concerned, all complexities must be hidden from him as he gets only one monthly bill. The actual purpose is to provide lower ***transaction cost*** among market actors in the value network in order to make it work.

The cooperation between small operators (new entrants and local operators) and big players is a must in order to provide a cost-effective solution. The **real trade** between big and small players is that big players can benefit as they do not need to deploy their own infrastructure. On the other hand the small players can take advantage of the larger customer base of the big players. **Market readiness** is one of the most crucial and

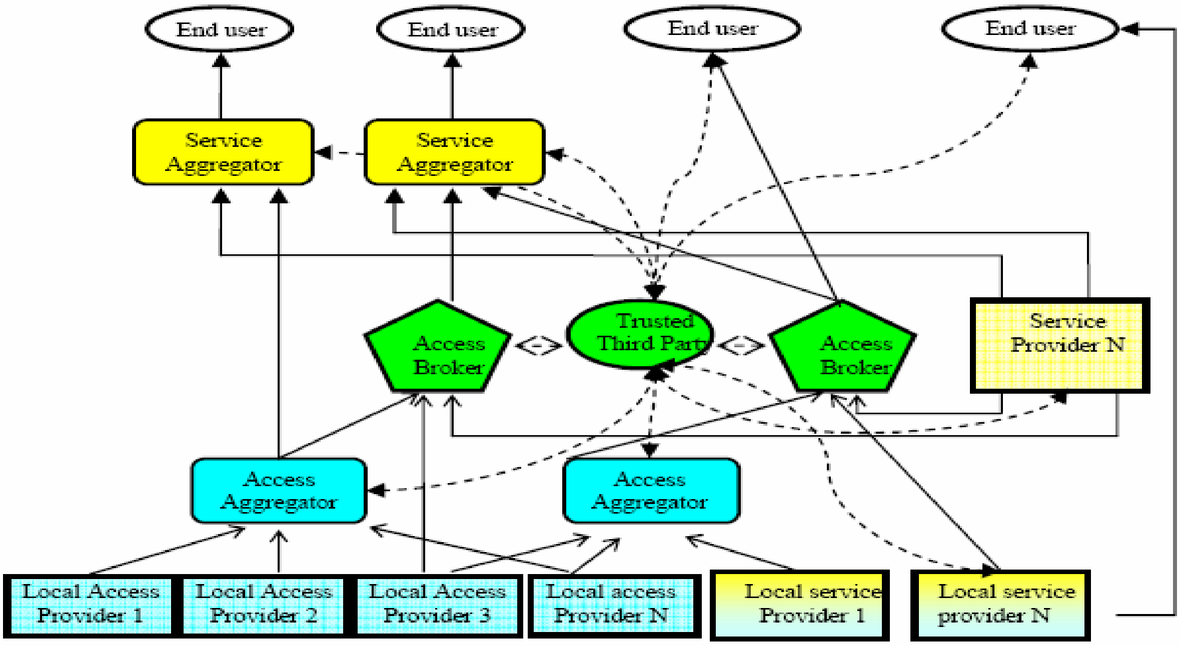

Figure 5: Market Actors in Value Networks [6]

difficult factors when starting a new service based on a new technology [2]. A technology like VoIP for example already existed for years, but was only recently adopted in the marketplace. On of the hurdles for new entrants in value networks could be high **technical sophistication.**

Small players are also affected by the **rate of technological growth**. As the investment on small players' part increases, on the other hand they can also take advantage of saving the **marketing cost** as the big players will marker their network and services anyways. Moreover, providing a new service via local operators involves lesser **investment risks** as cost will be distributed among many market players.

5 Regulatory Aspects

Regulation in telecommunications has proven to result in greater competition in the market, economic growth, increased investment, lower prices, higher penetration, and more rapid technological innovation in the sector. The exponential growth in both the telecommunications customers and devices brought changes in traditional regulatory theories, which are often successful in other sectors rather than telecommunications. Regulations will remain important to take care of new market entrants from havoc of giants with monopoly. Ambient Network brings new regulatory implications as well [3], including

New Market Entrants are awarded with licenses according to demand and supply of particular area. It provides new opportunities for local wireless hotspot operators with local licenses or short term licenses.

Dynamic Roaming must be implemented with AN as it aims to provide interconnection in heterogeneous networks. Here regulation can play part as directives on fair agreement format and procedures [3].

Authentication is also an important aspect of AN regulation. Authentication must be insured by regulation to be non-discriminating.

International presence must also be regulated. Just as the presence of AN at city level, there must be international presence of AN with the same flexibility as for the local presence of operators.

6 Conclusions

The paper briefly discussed **Conceptual Frameworks for Interconnection of Heterogeneous Networks**, with the focus on technical architecture, business model and regulatory aspects. Composition of network, Mobility and Heterogeneity are defined in technical perspective. The paper further explains the complexity of business model, where Technical, financial, organizational, and professional user or consumer's needs and requirements need to be balanced. The big picture discusses some of the important aspects for consideration for making an ambient value network. Regulatory aspects were finally discussed to point out changes required in standardization and government policies for realization of the AN.

It can be concluded that AN is a new, exciting business opportunity which promises a large number of customer services at low cost. However its realization requires removal of insecurities of small players or new entrants, as ambient value network gives high priority to big players (MNOs). Also business complexities, such as, transaction cost, risk minimization, marketing cost and investment risks, should be taken into account.

References

[1] Ahlgren, Bengt and Eggert, Lars and Ohlman, Börje and Schieder, Andreas (2005) *Ambient networks: Bridging heterogeneous network domains.* In: 16th IEEE International Symposium.

[2] B. Kijl, H. Bouwman, T. Haaker, E. Faber: Developing a Dynamic Business Model Framework for Emerging Mobile Service, TU Delft.

[3] Jon Crowcroft, Steven Hand, Richard Mortier, Timothy Roscoe and Andrew Warfield. Plutarch: An Argument for Network Pluralism. Proc.*ACM SIGCOMM Workshop on Future Directions in Network Architecture (FDNA),* Karlsruhe, Germany, August 2003, pp. 258-266.

[4] Martin Johnsson and Jan Markendahl, Ambient networking and related business concepts as support for regulatory initiatives and competition.

[5] M. Johnsson et al, Network Composition, WWRF#15, Wireless World Research Forum Meeting 15, Paris, France

[6] Niebert, Norbert et al: Ambient Networks -Research for Communication Networks Beyond 3G, Proc.IST Mobile Summit, 2004.

[7] Oscar Rietkerk, George Huitema, Jan Markendahl, Business roles enabled by Ambient Networking to provide access for anyone to any network and service.

[8] R. Agüero Calvo, J. Eisl, V. Typpo, S. Uno: Analysis of Mobility Control Functions in Ambient Networks, 3G 2005, The Sixth IEE International Conference

III. Regulation of public WLAN services

NIKLAS TIRKKONEN
Helsinki University of Technology
niklas.tirkkonen@hut.fi

Abstract

The de-regulation of the 90s and the technological convergence of media have changed the telecommunication industry. The role of the regulator is to support competition and to protect the customer. Public WLANs are gaining ground and the regulators are applying existing laws and provisions to them, Finland in the forefront.

Surprisingly the municipalities have found themselves as operators because they have offered wireless access to the Internet in public places. The status of an operator brings obligations.

EU shows corporate driven Americans example of technology neutral regulation. As WLAN is a new technology, case-specific evaluation is often needed on state-level.

1 Introduction

Wireless Local Area Network (WLAN, also referred as Wi-Fi, mostly in the US) is the most prominent unlicensed wireless technology available today. In this paper I am presenting the role of the regulatory authority in case of public WLAN services. The focus is on Finland, how Finnish regulators apply EU laws. EU legislation is compared to American one. I also study authorities as an important stakeholder group and what are their motives and tools to regulate. I have used various papers, memos and theses as my background material in purpose of giving the reader a clear picture of the topic. A list of abbreviations is found in the last page.

WLAN systems are implemented in three main types of venues: enterprise, public places and homes. In all of these places, an upper link, either fixed or wireless, connects the wireless access point to backbone network [9]. In this paper only public usage is considered with its legislative definition.

2 What is regulation?

Regulation can be defined: A written rule made by a government or another authority which is intended to control the way something is made or done [4]. Or: Regulation is the process of making rules which govern behavior [5]. Regulation exists in many forms: economic, health, safety, technologic. In this paper the focus is towards economic regulation.

Regulators have always been interested in the development of the telecommunications industry and infrastructure. In the past, the main role of the telecommunications regulation was in protecting customers from the monopoly power of vertically integrated operators [4]. Deregulation in the 90s changed the industry and the role of the regulators. The technological convergence on the other hand is bringing together the telecom, broadcasting, and information services regulation [3].

The main rationales behind regulation are: effective use of resources, competitive markets, customer rights, preventing abuses like monopolies and cartels, redistribution of wealth.

The regulators have a so called narrow window to guide business models – they can not make any drastic decisions which could affect the industry overnight. New business models may arise either accidentally or deliberately. Regulation may in the worst case seriously hinder business activities, if planned negligently [7].

3 Application of the legislation to public WLAN

Regulators face always challenges when new technologies are introduced. The legislation is always a little bit late. The regulators need to define how they apply the existing laws to new technologies and businesses. Next I present the actions that Finnish Communications Regulatory Authority (FICORA) has taken in Finland. The role of EU is considered and the legislation in the US is presented and compared with the one in EU.

3.1 EU regulatory framework

EU does not impose specific legal provisions on public WLAN. It establishes a regulatory framework, illustrated in figure 2, and defines the tasks of National Regulatory Agencies (NRA). The telecommunications regulatory framework, adopted in March 2002, recognizes that much of telecommunications regulation exists as a means of addressing potential and actual abuses of market power. With that in mind, the EU attempts a comprehensive, technology neutral approach to regulation.

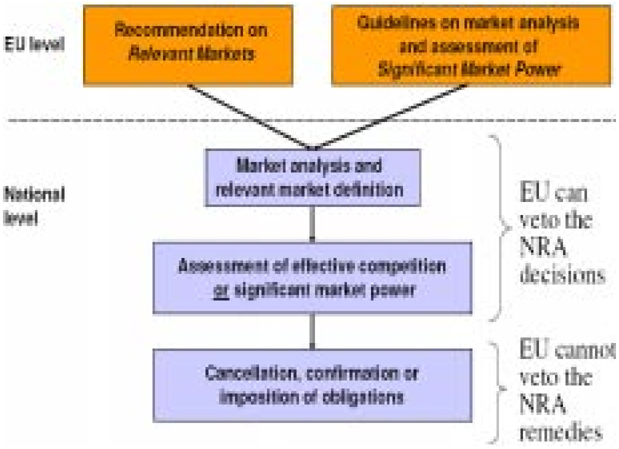

Figure 1 – EU regulatory framework [3]

The European Commission defines a series of relevant telecommunications markets, and provides a set of guidelines for determining the presence or absence of market power. Within each market the NRA determines whether one or more parties possess Significant Market Power (SMP). If SMP exists, the NRA will impose appropriate obligations. Basically EU seeks to move completely away from technology-specific and service-specific legislation [6].

Many countries have not considered the legal status of WLAN Networks because WLAN has not yet become sufficiently common. Some countries have dealt with the matter only from the viewpoint of frequencies and licenses. Most countries that have considered the matter further, share the opinion Finland has taken. For example, Spain, Italy, Switzerland, Turkey, Hungary and Estonia considered that service offered by a café or a hotel to its customers is not public telecommunications. On the other hand, there may be obligations imposed on service providers on the basis of other laws. For example in Italy, service providers must authenticate users on the basis of the anti-terrorism law.

3.2 Status in Finland

Finnish law defines WLAN services as follows: WLAN Network is a communications network. It means a system comprising cables and equipment joined to each other for the purpose of transmitting or distributing messages by wire, radio waves, optically or by other electromagnetic means. Provision of WLAN is thus network service, that is, provision of a communications network that an operator has in its ownership or for other reasons in its possession for the purposes of transmitting, distributing or providing messages. Transmission or provision of messages via a WLAN that a service provider has in its possession or has leased from a network operator is a communications service. Providers of network services and communications services are network operators and service operators, i.e. telecommunications operators.

The Communications Market act is also applicable to a non-profit network or communications service or to a service that is provided without compensation. Therefore, also a municipality or a school can be a telecommunications operator. Provision of the WLAN and the Internet access service via it is regarded as public telecommunications when it is offered to a set of users that is not subject to any prior restriction. The concept of public communications network and public telecommunications are related to technical quality requirements and to obligation to submit a notification on telecommunications [1].

It is not always easy to draw the line between a set of users that is subject to prior restriction and a set of users that is not subject to any prior restriction. Case specific evaluation is often needed. Some typical examples of public telecommunications for wireless broadband networks are: Wireless Internet connections corresponding to fixed ADSL and provided by means of WLAN; WLAN hotspots provided in public outdoor or indoor environments to a set of users that is not subject to prior restriction.

WLANs can also be offered to a set of users that is subject to prior restriction, but in this case the provided services are not public telecommunications. Usually, the restriction is made on the basis of a former customer relationship or membership of an organization. These cases include: WLAN connections offered by a company (e.g. hotel or a café) to its customers directly or after having acquired them trough subcontracting; WLAN connections offered by a school to its students or personnel.

Technically, restriction of users can be done either with relevant coverage area restrictions or through access control methods, which means that only authorized persons have access to the network.

3.2.1 Operators' responsibilities

An operator is regarded to practice public telecommunications when it provides a network service or a communications service to a set of users that is not subject to any prior restriction. Law separates providers of Internet access service, providers of a wireless access network and network layer, and providers of network access management. A wireless broadband service is composed of several logically separate services. The responsibilities are clear when these services are offered by the same provider.

A written notification of the intention to operate public telecommunication must be submitted to FICORA before the operations begin. If the operations are temporary in nature, aimed to a small audience or otherwise of minor significance, the notification duty does not apply.

Public WLAN services are concerned in regard to protection of privacy provisions. An operator must be able to detect traffic that endangers the information security or availability of the communications service. An operator must resolve the events by for example MAC filtering. Information security provisions of telecommunications operators depend on the size and service offered. An operator must provide the user with information related to security issues and combating the threats. A telecommunications operator providing Internet accesses is responsible for monitoring the events in its own network in order to detect malicious traffic, and save and store detailed log information on any processing of identification data.

An operator must take care of physical protection of the network and ensure, for instance, power supply for equipment in a communications network. Basic requirements are needed to place communications network components so that unauthorized access is prevented [1].

3.3 Regulation in the US

In the US the legal and regulatory framework is very different than in EU. The latest revision of the Telecommunications Act of 1934, of 1996, separates telecommunication services from information services. The Act defines an information service as “the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunication system or the management of a telecommunication service.” It underpins the US deregulatory policy toward the Internet. The Internet should be viewed as an enhanced service, and that the Internet consequently should not itself be subject to significant regulation.

In the US regulators seem to lack authority and the people tend to trust the companies more than the government – at least when compared to Europe. The American attitude to large companies has always been somewhat ambivalent – they worry about the power of large corporations wield, and yet at the same time they appreciate the potential benefits associated with the economies of scale and the scope that they command. It is not held to be a problem for a firm to possess market power; rather the abuse of the market power is problematic [6].

FCC has a limited power to collect confidential information and it lacks the ability to protect that information. Although regulation in the U.S. is multilevel with federal, state and municipal bodies, the FCC has taken a position that the Internet is interstate.

There’s a huge interest in WLAN in the US and they are cautious to introduce any laws that might jeopardize the growth of the wireless network infrastructure. On the other hand the Americans are increasingly concerned about cyber-security. They have noticed that the nature of connection is very different from traditional LAN – people can appear and disappear from sight. As they are opening up an additional 255 megahertz of spectrum in the 5-gigahertz band, the biggest concern is whether or not it could affect military radars [2].

Table 1, Regulation comparison the US vs. EU [3]

EU	U.S.
Technology- and service-neutral regulation. Convergence	Detailed silos.
Centralized responsibility for law creation and de-centralized for law enforcement	No separation between them two
Defines the *process* for reaching outcomes	Laws and regulation contain specific regulatory *outcomes*
People trust governments	People trust corporations

Neither the US nor EU has taken public WLAN networks into deeper consideration. In the table 1 there are few major differences that affect the way regulation is applied generally.

4 Conclusions

WLAN networks have just recently become popular and it is evident that the regulators have not yet considered the issue widely. The regulators are on the other hand facing tremendous challenges as the media is converging – it is a tough job to keep up with it. Considering the monopolistic history of telecommunications the task is even more difficult.

In Finland municipalities have just recently started to bear a stamp of an operator. The obligations that being an operator brings, is supposedly keeping the rate of adopting public WLANs low. The concerns of malicious traffic are distinct.

In my opinion the load should be taken off from the shoulders of the operators with small measures to accelerate the growth of public hot-spots. You should make a clear distinction between public and not public telecommunications services and impose differentiated provisions to them. The case is that public WLANs are mostly offered by non-profit organizations and municipalities who do not have the same resources as corporations.

The difference between EU and the U.S. is interesting. The legislative hierarchy seems to be more efficient in EU than in U.S. In EU the adoption of public WLAN is very different from county to another, depending for example on demographics. In this light the separation of law creation and enforcement seems very justified.

It seems that public WLAN networks are more popular in the US, than in the EU region. This on the other hand is clearly linked to the loose control of the US government. Hence, if we in Europe seek to raise the popularity of public WLAN services, should we change the legislation fundamentally?

References

[1] Finnish Communications Regulatory Authority http://www.ficora.fi/englanti/document/wireless_broadband_connection.pdf (Referred 31.10.2006)

[2] Goth, G.: Will the White House Take On Wi-Fi, IEEE Distributed Systems Online, 2006, ISSN: 1541-4922

[3] Hämmäinen, H., S-38.041 Networking Technology lectures, spring 2006.

[4] Koivisto, M: Licentiate’s Thesis: From Control to competition – Changes in Regulator’s Strategic Position in Telecommunication Markets, Networking Laboratory TKK, 9.4.2002.

[5] Review of Industry-Led Regulation, Discussion Paper http://www.consumeraffairs.govt.nz/policylawresearch/industry-led-regulation/discussion/discussion-03.html, (Referred 22.10.2006), July 2005, ISBN 0-478-28445-4.

[6] Scott, M.: OPP Working Paper Series, 36 – The potential Relevance to the United States of the European Newly Adopted Regulatory Framework for Telecommunications, Federal Communications Commission, July 2002

[7] Seminar session on Networking business, Networking laboratory TKK, 12.10.2006

[8] Wi-Fi Alliance, http://www.wi-fi.org/index.php (Referred 31.10.2006)

[9] Xing, J. Master’s Thesis: Economic study on Deployment of Wireless Local area Network in Finland, Networking Laboratory TKK, 4.1.2005

IV. Municipality-driven Business Models for WLAN

MAGNUS SIPPEL
Helsinki University of Technology

Abstract

Although broadband penetration has grown rapidly, there are still many areas that remain under-served. For these communities, municipal controlled WLAN opens up new options and opportunities. Additionally, wireless changes the cost and policy calculus for deploying last-mile infrastructure.

This paper explores two types of questions regarding municipal WLAN networks; Why are cities and municipalities getting involved in deploying these networks and what kind of business models alternatives are there.

Keywords: Municipality, WLAN, Mesh WLAN, municipal, involvement, motivation, business models.

1 Introduction

In the last few years a growing number of municipality deployed WLAN networks has emerged. However, to many people municipal enthusiasm for deploying and operating telecommunication networks comes at a surprise because of the prevailing trend of deregulation and privatization in public utilities. ***[1]***

Increasingly, cities and municipalities are recognizing the power of providing wireless access for their employees, businesses and residents. Motivations range from ensuring Internet access for low income families, to attracting and keeping businesses via affordable access to broadband services, to decreasing costs for municipal networks while increasing city worker productivity.

Wireless broadband technologies such as WLAN is increasing its popularity primarily because of the lower deployment and capital costs and the freedom from cabling. ***[3]***

2 The municipal role in providing Communication infrastructure

The force driving the current wave of municipal WLAN deployment is that e.g. WLAN networks are relatively inexpensive to deploy and operate and also take advantage of available city assets such at street lights and urban furniture which make ideal antenna sites.

Municipal entry into communication services may be justified economically in three basic types of scenarios:

(1) In a response to a market failure
(2) As part of the local municipalities' role in providing basic infrastructure services
(3) In a way to opportunistically take advantage of scale or scope economies afforded by investments or services that were put in place for another reason.

2.1 Market failure

In this case the municipal involvement may be needed because the private alternatives are inadequate. The costs of deploying infrastructure and operating services may be too high relative to the revenue that can be expected so that an insufficient number of private sector providers enter the market. In the most extreme cases, it may be uneconomic for any private carrier to offer the service.

The lack of adequate competitive alternatives may arise for a number of reasons. The market may be too small to sustain more than one facilities-based provider (i.e., a natural monopoly), or even if there are two or three competitors, competition may fail to be sufficiently robust

However, even if a local municipality does decide to invest in local access infrastructure, this does not mean that the municipality needs to provide end-to-end retail services. There are a variety of business models available for how a municipality may offer such services. These include:

(1) Retail Service Model
(2) Franchise Model
(3) Real Estate Model
(4) Coordination Model

3.1.2 Retail Service Model

In the Retail Service model, the municipality offers retail services to consumers over infrastructure that it owns and operates. This form of entry requires the greatest degree of resources and operating involvement in providing communication services,

3.1.3 Franchise Model

At the moment the most common model deployed is the Franchise model wherein the municipality contracts with a private firm to build and operate the facilities. While it is possible that the incumbent telephone or cable company could respond to the municipality's bid, in most cases, the respondents are new carriers. The basic model is similar to the traditional model of municipally franchised cable television service.

Wireless alters the range of players that might be considered and the architectures/services that might be offered.

3.1.4 Real Estate Model

The Real estate model presents a much more limited form of municipal entry. Under this model, the municipality provides access to conduit or public rights-of-way. In the wired-world, this includes access for stringing or burying cables; while in the wireless world, it includes locations for mounting antennas. In this model, the municipality partners with private providers to deliver end-to-end services to consumers. This model requires relatively limited investments in communications specific resources and capabilities, yet offers an opportunity for the local municipal to manage access to an outside plant

3.1.5 Coordination Model:

Another minimalist and common form for municipal entry is the Coordination model. In this case, the municipality provides a nexus for demand aggregation (e.g., buyer groups).

By aggregating demand, the municipality may be able to e.g. reduce the risks (and costs) to private sector entry by demonstrating an assured base of demand for broadband services. Wireless technologies, and especially the potential for edge-based/customer-provided infrastructure through mesh networking, raise new opportunities for municipalities to help coordinate community networking efforts. The municipality can help educate consumers as to new technical options for deploying local wireless hot spots and linking those together to support community-wide coverage networks. ***[2]***

2.2 Basic Infrastructure

According to the "basic infrastructure" rationale, municipal networks may be justified as just another example of community provision of basic infrastructure services. These are services that are

(1) Used by everybody and are perceived as essential services;

(2) May be a natural monopoly or have a public goods aspect (i.e. excluding non-paying users is costly)

(3) Provide important spill-over benefits that are central

Obvious examples include roads and water and sewage systems. While these could be provided via regulated private contractors, such an approach is relatively rare. Other basic infrastructure services include electric power and gas distribution and public transportation.

Because basic infrastructure is perceived as essential to economic activity (i.e., it is used by most businesses), ensuring adequate access to such services is viewed as necessary to promote economic development goals. Additionally, access to communications and media services is often viewed as important for a number of social goals. For example, it can help maintain community cohesion, support democracy and the functioning of the society. While the “basic infrastructure” model appears distinct, it may be subsumed as just another example of a “market failure” ***[2]***

2.3 Opportunistic

The third rationale – "opportunistic entry" – is associated with situations where the municipality is doing something else that makes it relatively low cost for them to expand into offering communication services. The municipality’s entry into communication services may be able to take advantage of scale and scope economies when only an incremental investment is required to expand into communication services. ***[2]***

3 Some arguments against municipal involvement

Even though municipal involvement is increasingly getting more common in the WLAN communication field, the feedback and reception is not always positive.

Opponents of municipality-driven WLAN deployment raise three main objections.

Firstly they claim that the municipal involvement results in an unfair competition for private carriers because the municipality is able to use public assets, regulate the private companies, avoid fees and taxes, obtain low cost finance i.e. allowing them to offer network access at below-cost prices.

Secondly they argue that municipalities have no particular technology expertise and are likely to prove incompetent in selecting technological approaches application and business models

Thirdly they believe that municipal intervention favoring one specific technology creates a distortion by foreclosing competition among alternatives in the market place ***[1]***

Another thing that also is worth considering is that in some countries (e.g. in Finland) the regulator may see WLAN Hotspot services as public telecommunication if the services are offered without prior restrictions (authentication). This means that the municipalities get operator obligations concerning both quality & security of the network – adding additional complexity and costs.

When taking these views into account some consideration is needed when deploying municipal WLAN. When extending municipal activity into rapidly changing markets like those for communication services, it would especially for communities without a municipal utility or a technically sophisticated local resource be worth considering if the desired results and effects are possible to reach without a too direct role in the provisioning of broadband services. With wireless technologies especially, the franchise, real estate, or coordination models seem especially attractive in these cases.

4 Summary

In the last few years a growing number of municipal deployed WLAN networks has emerged. The most common WLAN network models are Standard WLAN Networks and Mesh Networks.

The force driving the current wave of municipal WLAN deployment is that they are relatively inexpensive to deploy and operate and also take advantage of available city assets.

Municipal entry into communication services may be justified economically in three basic types of scenarios: 1) In a response to a market failure 2) As part of the local municipal's role in providing basic infrastructure services 3) In a way to opportunistically take advantage of scale or scope economies afforded by investments or services that were put in place for another reason.

However the municipality does not need to provide end-to-end retail services. There are a variety of business models available for how a municipality may offer such services. These include the Retail Service Model, the Franchise Model, the Real Estate Model and the Coordination Model

Even though municipal involvement in the WLAN area in many cases has been successful, not all of the reception has been positive.

After studying the different reasons for municipal involvement together with the available business models it is worth to notice that municipality without a utility or a technically sophisticated local resource should be careful to assume a too direct a role in rapidly changing markets as the communication market especially as the desired effects often can be reached with surprisingly small contributions and involvement.

References

[1] Bar F. & Park N. , Communications & Strategies no. 61, 1st quarter 2006, p 107, Municipal Wi-Fi Networks: The Goals, Practices and Policy Implication of the US Case.

[2] Lehr William, Sirbu Marvin, Gillett Sharon, Wireless is Changing the Policy Calculus for Municipal Broadband , 2006. http://cfp.mit.edu

[3] Nortel Municipal Wireless Solution. http://www.nortel.com/

V. Municipal WLAN: Case Examples in Finland

JUSSI LAUKKANEN
Helsinki University of Technology
jussi.laukkanen(a)hut.fi

Abstract

Communication industry in Finland is currently going through a rapid development phase with wireless local area network (WLAN) coverage. Within the past two years several WLAN projects have emerged in different parts of the country and, in addition, also completely new business models compared to traditional ones have been introduced. Municipalities have faced new demand by citizens for public internet access points. This paper concentrates on current WLAN cases especially from the viewpoint of different cities and municipalities. Framing of the paper has been made for only the current WLAN cases in Finland.

1 Introduction to municipal involvement in WLAN development

Due to technological development during past years, the Finnish market has seen new devices with capabilities for low-cost WLAN access. However, development of available wireless network coverage has been rather slow since operators have faced financial difficulties. In addition, development of mobile data service market lag some other countries since handset bundling was prohibited by regulations until 2006.

To achieve initial critical mass for larger WLAN networks different types of cooperation models exist between several groups such as cities, municipalities, companies and universities. This has enabled exploitation of existing network structures and investments by sharing bandwidth of individual groups to others thus gaining large shared network coverage.

Another viewpoint to network development has been that all citizens should have access to internet as a public good. Internet access has been compared to basic infrastructure such as road networks, which should be provided by city or municipal funding. Currently several cities and municipalities have provided WLAN access hotspots in their libraries, schools and city offices.

Critique has also emerged towards cities' investments for WLAN purposes and doubts for the effects on operators' revenues if basically the same service is also available for free. [32] However, emerged new WLAN access offerings have been compared to book market in the context of libraries and book stores.[22] Clearly both are offering same goods for their customers in the form of books, but obviously there is demand for both of these offerings.

2 Case examples

This paper presents three leading municipality-driven WLAN cases in Finland: SparkNet, PanOULU and Mastonet. In addition, the paper will introduce other smaller network cases related to municipal WLAN development. Traditional WLAN business models based on Telco-model [10] [27] (currently available by operators such as TeliaSonera and DNA [11]) are excluded from this paper along with foreign cases.

2.1 SparkNet

SparkNet [8] [13] [14], originated from the city of Turku, is currently the largest WLAN network in Finland. During the past three years it has grown to 1577 access points and, according to its owners, serves over 50 000 registered users.

History and development

SparkNet was founded in April of year 2003 and expanded very quickly to cover the campus area of University of Turku, Åbo Akademi University and Turku School of Economics. During the year of 2004, SparkNet was enlarged to offer solutions for companies as well. Four different business solutions were tailored to suite different size of companies' technical demands.

In year 2005, OpenSpark was created to enable individual users to join the community by offering their WLAN access points for shared use. OpenSpark members have also SparkNet access points available thus increasing the amount of total access points in the network. Due to easy scalability and positive network effects, SparkNet and OpenSpark have proven a successful concept with continuous increase of access points. SparkNet has also been able to expand to other cities outside Turku area. Cooperation contracts have been made with cities such as Salo [24], Kaarina, Parainen and Naantali in addition to municipalities such as Lieto, Merimasku and Velkua. Furthermore, SparkNet has been able to capture individual access points from other main cities of Finland along with a few foreign ones as well.

Technical solution

SparkNet is designed to use existing networks of e.g. a member company. It divides current networks' bandwidth to company's internal local area network (LAN) and SparkNet network, Figure 1. The separation of these two networks can be done virtually by virtual local area network (VLAN) or by physical separation with different access cables and access points. Company's private LAN will be protected by its firewall but the SparkNet part will remain as a part of common internet behind authentication gateway. This enables a SparkNet member to access the network with his personal id and password which are managed by a centralized authentication server. This division of bandwidth will enhance security of companies' own LAN's and still enable visitors to use their access points.

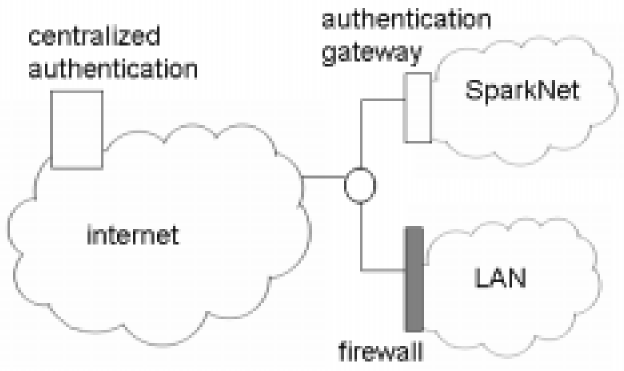

Figure 1 SparkNet's technical solution

Emerged new business opportunities

SparkNet has been able to create value for its customers by offering centralized authentication services. This kind of business model has advantages due to the fact that owners of the network have been able to exploit their customer companies' own investments in network infrastructures. This enables SparkNet owners to leverage from large network effects without having to use large initial investments by themselves.

SparkNet has also created alternative revenue channels by selling time-limited licenses to use their network for visitors who do not belong to SparkNet or OpenSpark community. This business model might provide good opportunities if the community is able to capture dominant position comparing to other networks.

2.2 PanOULU

PanOULU-network [6] is originated from the city of Oulu and has grown to cover 400 access points. The user base has also been enlarged and PanOULU served 4372 unique users in September 2006.

History and development

Development of the PanOULU-network began in October of 2003. The initial cooperation contract was signed by the City of Oulu, University of Oulu, Oulu University of Applied Sciences and Oulu Telecom. After combining their individual networks to share access to other members, PanOULU has been developed to offer also companies or individuals a possibility to participate in network growth by ordering PanOULU subscriptions. This is a very similar business model compared to SparkNet. Initially, PanOULU required its user to have user id and password. However, authentication was removed in June 2005 to decrease the amount of network management and, in addition, to offer easy access for visitors from outside Oulu area. Removing authentication of users has raised questions about network security and possibilities for potential harmful use of network.

Along with development of PanOULU citizens of Oulu have learned about wireless data usage and its opportunities. To promote new potential uses of PanOULU, the city of Oulu even announced a competition for its citizens to create new mobile services which would utilize PanOULU's capabilities. [25]

Technology

PanOULU consists of four different visitor networks which are KampusWLAN, OuluNET, OukaWLAN and RotuaariWLAN, Figure 2. In addition, with the PanOULU subscription companies can offer their guests access to Internet during their visit in company premises.

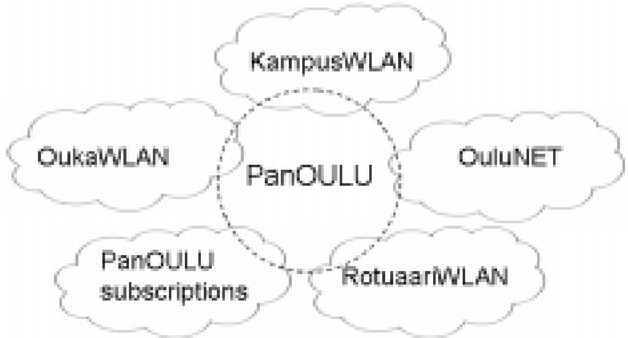

Figure 2 PanOULU visitor networks

Currently, there are three different WLAN standards available: 802.11b, 802.11a and 802.11g. All PanOULU access points are able to use 802.11b-standard and most access points in indoor premises support 802.11a-standard. 802.11g is supported only by new models of access points.

2.3 Mastonet

Development of Mastonet [4] started in 2005. Mastonet is operated by the city of Lahti and is supposed to serve citizens and visitors of Lahti area. Currently the network has grown to cover 85 access points which serve an average of 400 different users per day. According to Mastonet providers, the network coverage is currently 80 % of Lahti citizens. City of Lahti has also realized possibilities for temporary increase of network capacity demand and for example during a large sport event, Lahti Ski Games 2006, Mastonet's resources were temporary enlarged three times to serve city visitors and thus promote city as a technology leader. [31]

Mastonet uses mainly 802.11b-standards with its access points, but also Mastonet's newest access points support the 802.11g-stardard. The City of Lahti has decided that public internet access should be provided to citizens for free and thus no authentication is required when accessing Mastonet. Consequently, user support and security are not provided with as high level compared to telecom operator offerings.

2.4 Other municipal involved WLAN cases

Following good experiences by the leading network providers examples such as cities of Turku, Oulu and Lahti, other cities and municipalities have also began to develop their own WLAN offerings. Cities have realized that offering public WLAN access points they can create value for visitors and enhance business innovations. In addition, offered access points enhance cities credibility as leaders of technology and development. Several cities have began to offer public access points at least to city libraries, city offices, schools and other main public areas. In addition, new potential places have emerged for access points such as city busses in the Helsinki area [29].

Even though initially some cities such as Helsinki were suspicious [19] about city involvement the public pressure has changed their opinions. The City of Helsinki is now developing their WLAN offering and it will cover 60-70 access points in the end of 2006 [20] [30]. Other cities were WLAN access points are being offered are for example Pori [1], Lappeenranta [7], Varkaus [3], Kemiö [5] and Tampere [2]. Some have even taken their offerings one step higher as for example the municipality of Kinnula provides first year college students own laptop computers to use their public WLAN [17].

However, not all cities support this kind of development [17] [26]. For example the city of Espoo does not consider their job to be involved in building WLAN infrastructure [16]. City representatives believe in a market driven development at least in this phase, but few minor projects have been developed by other parties [28]. The same approach has been by city of Tampere were they are also reluctant to use scarce tax funds for developing WLAN coverage. In Tampere there are WLAN access points in city libraries but currently there are no plans to expand their coverage to public city areas. Even though these large cities do not currently play key roles in WLAN development, their actions will definitely be significant to the future development of Finnish WLAN coverage and dominant players

Summary of case examples

The three leading communities have few important differences which might have been significant for their development speed, Table 1. Currently, it seems that authentication and member-only access have created motivation for potential users to join SparkNet/OpenSpark, thus authentication playing a key role in their enlargement success.

Table 1 Summary of three leading networks

Network name	SparkNet	PanOULU	Mastonet
origin city	Turku	Oulu	Lahti
operating since	4 / 2003	10 / 2003	7 / 2005
access points	1577	400	85
authentication	centralized	none	none
free public access	no	yes	yes
community model	yes	yes	no

3 Future issues concerning WLAN development in Finland

This section of the paper concentrates on issues which will be relevant for future development of Finnish WLAN after year 2006. Development examples by three leading actors have revealed some valuable information for other cities to consider. Clearly, SparkNet in Turku has shown fastest enlargement of their network's access point coverage which should be considered as a good growth model for others to follow.

3.1 Development model for building WLAN networks

Clearly most of the different networks share common patterns in their development phases, Figure 3. To achieve critical mass and positive network effects, they must first build initial user base. This is most easily done by cooperation between universities and polytechnics, which already have large potential user bases. In addition, students are a good target group to test new wireless devices. Another separate area where initial development is easily done is city libraries and offices since cities and municipalities want to offer services for their citizen and do not require profits from the users. Cooperation with these kinds of separated networks could be called "early phase" of network development.

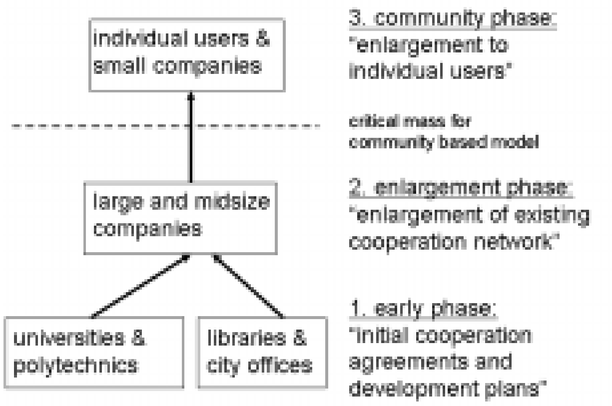

Figure 3 Development model for WLAN networks

After the cooperation between first phase networks has been successfully implemented and tested, a network can enlarge its offerings to corporate customers.

Corporations have also potential user groups already available, but they are not most likely to be willing to join as founding members. Thus second phase is very suitable for them to join the network.

A successful combination of the first phase cooperation networks to second phase company networks can enable a network to achieve critical mass to begin community based network model e.g. OpenSpark. By sharing individually owned access points to other community members an access point owner increases his own value by getting access to other access points as well. Clearly this increases also total value of the network by increasing amount of access points for its members.

3.2 Regulatory challenges concerning public WLAN access offerings

Since new business models have emerged after WLAN development began in 2003, regulators have faced difficulties while trying to adapt the old rules to a new market situation. Main issues concerning these new network models are telecom operators' customers right to share their connection to outsiders in cases like the OpenSpark community. Some operators have seen this as a threat to their business while others have allowed it and seen sharing of connections as a value adding service for their customers. The increasing amount of wireless data usage will thus aid new WLAN service development by enlarging its user base. However, a question has been raised about responsibility issues in case of network violations via shared access points.

Offering of free access points without authentication

Another main issue has been the challenge of defining the term "telecommunication operator", since operators have legal responsibilities on reporting to Ficora about their spectrum usage and service quality. The challenge is who Ficora defines to be an operator. Ficora has published a memo [9] concerning this issue which should help definitions in future cases. From the viewpoint of municipalities, being a telecommunication operator would create additional costs and unavoidable responsibilities [15].

Future development

Development in public WLAN coverage during year 2006 has clearly build a promising foundation for enlargement in near future. Cooperation models and community based access points have proven a successful way to exploit incumbent network infrastructure and individual investments for common benefit. This has enabled WLAN technology to better achieve the required critical mass of users to enhance service development. However, currently most WLAN projects have concentrated on rather small areas. In the future after those developing WLAN projects have matured with their coverage areas, market will probably see more cooperation between different separate networks which would combine their resources for larger network coverage for individual users. In addition, development of terminal equipment will play crucial role in the development and customers' adoption of new services.

There are also possible new entrants to WLAN provider markets which might be able to capture their share of Finnish markets. Fon, originated from Spain, is currently building similar shared access network comparing to SparkNet solution [18]. Currently Fon operates already in various countries worldwide with thousands of access points. Also large foreign WLAN developer The Cloud has been exploring their possibilities towards operations in Finnish markets [21]. The Cloud considers themselves as the largest WLAN operator in Europe thus giving them potential capabilities to enlarge their network to cover Finland.

4 Conclusion

This paper presented the public WLAN situation in Finland in October of 2006 from a viewpoint of city and municipal involvement. Several successful initiatives exist. However, new regulatory issues such as absence of authentication may arise if problems will emerge. This issue will clearly become more important when networks get more users in the future. Furthermore, it is currently not clear what effects will publicly offered WLAN access points have towards operators' revenues.

References

[1] Anon.: Avoin langaton laajakaista avattu Porissa, Prizztech Oy webpage, 18.7.2006, http://www.prizz.fi/sivu.asp?taso=2&id=185

[2] Anon.: City of Tampere webpage – Nettipisteet, 15.10.2006, http://www.tampere.fi/hakemistot/nettipisteet/index.html

[3] Anon.: City of Varkaus webpage, Varkauden kaupungin langattoman verkon (WLAN) palvelut, 15.10.2006, http://www.varkaus.fi/index.asp?language=1

[4] Anon.: Mastonet webpage, 15.10.2006, http://www.mastonet.fi/

[5] Anon.: OpenKimito webpage, 15.10.2006, http://openkimito.fi/infofi.html

[6] Anon.: PanOULU webpage, 15.10.2006, http://www.panoulu.net/

[7] Anon.: Sainet webpage, 15.10.2006, http://www.sainet.fi/?id=index

[8] Anon.: Sparknet webpage, 15.10.2006, http://www.sparknet.fi/fi/

[9] Anon.: Viestintämarkkinalain soveltaminen langattomien laajakaistayhteyksien tarjontaan, Ficora, 5.9.2006, http://www.ficora.fi/suomi/document/Wlan_muistio27062006.pdf

[10] Courcoubetis, C., Weber, R., Wiley, Pricing Communication Networks – Economics, Technology and Modeling, 2003
[11] Heikkilä, Satu: Business models of mobile operators for WLAN: case examples in Finland, Seminar on Networking Business, 2006
[12] Jämsén, Heikki: Kinnulan lukion epuille läppärit ja koululle langaton verkko, Kotiseudun sanomat, 16.8.2006, http://www.kotiseudunsanomat.net/uutiset.php?ID=724
[13] Kuosmanen, Jaakko: New Business Models for Public Wi-Fi Services, Telecommunications Forum lecture in Helsinki University of Technology, 26.9.2006, http://www.netlab.tkk.fi/opetus/s383001/2006/kalvot/TelecomForum-2006.09.26-Kuosmanen-Public_WLAN.pdf
[14] Kuosmanen, Jaakko: SparkNet – Innovative wireless local area network (WLAN), ICT Turku Finland, 2006,
[15] Lehto, Tero: Avoimille verkoille haetaan pelisääntöjä, Tietokone, 6.9.2006, http://www.tietokone.fi/uutta/uutinen.asp?news_id=27947
[16] Lehto, Tero: Espoo ei innostu kaupunkiverkosta, Tietokone, 26.9.2006, http://www.tietokone.fi/uutta/uutinen.asp?news_id=28177&tyyppi=1
[17] Lehto, Tero: Ficom: ”Ilmaiset” WLAN-verkot käyvät veronmaksajien kukkarolle, Tietokone, 30.8.2006, http://www.tietokone.fi/uutta/uutinen.asp?news_id=27864
[18] Lehto, Tero: Fon jakaa Suomen WLAN-verkot, Tietokone, 27.2.2006, http://www.tietokone.fi/uutta/uutinen.asp?news_id=26166
[19] Lehto, Tero: Helsinki ei lämpene julkisille verkoille, Tietokone, 23.2.2006, http://www.tietokone.fi/uutta/uutinen.asp?news_id=26152
[20] Lehto, Tero: Helsinki verkottuu sittenkin langattomasti, Tietokone, 22.9.2006, http://www.tietokone.fi/uutta/uutinen.asp?news_id=28147&tyyppi=1
[21] Lehto, Tero: Julkisten WLAN:ien rakentaja tutkailee Suomea, Tietokone, 25.8.2006, http://www.tietokone.fi/uutta/uutinen.asp?news_id=27818
[22] Lehto, Tero: Kunnan väylä sähköisiin palveluihin – Asiantuntijat uskovat kaupunkiverkkoihin, Tietokone, 4.9.2006, http://www.tietokone.fi/uutta/uutinen.asp?news_id=27915&tyyppi=1
[23] Lehto, Tero: Megabitin laajakaista mökeille ja syrjäseuduille, Tietokone, 9.10.2006, http://www.tietokone.fi/uutta/uutinen.asp?news_id=28338&tyyppi=1
[24] Lehto, Tero: Mukaan Sparknet-yhteisöön - WLAN-kaupunkiverkko suunnitteilla Saloon, Tietokone, 15.8.2006, http://www.tietokone.fi/uutta/uutinen.asp?news_id=27682
[25] Lehto, Tero: Oulussa ideoidaan palveluita avoimeen verkkoon, Tietokone, 6.4.2006, http://www.tietokone.fi/uutta/uutinen.asp?news_id=26618
[26] Leivonniemi, Samuli: Pääkaupunkiseutu verkottuu laiskasti, Helsingin sanomat, 21.7.2006, http://www.hs.fi/kaupunki/artikkeli/P%C3%A4%C3%A4kaupunkiseutu+verkottuu+laiskasti/1135220766407
[27] Nurmiranta, Pekka: Social Optimality of Alternative Business Models, Seminar on Networking Business, 2006
[28] Punkka-Hänninen, Päivi: Tapiolaan ja Otaniemeen tulossa avoin ja ilmainen WLAN-yhteys, Helsingin sanomat, 21.7.2006, http://www.hs.fi/kaupunki/artikkeli/Tapiolaan+ja+Otaniemeen+tulossa+avoin+ja+ilmainen+wlan-yhteys/1135220764757
[29] Salonen, Juha: Helsingin linja-autoihin tulossa ilmainen langaton internetyhteys, Helsingin sanomat, 15.9.2006, http://www.hs.fi/kaupunki/artikkeli/Helsingin+linja-autoihin+tulossa+ilmainen+langaton+internetyhteys/1135221642077
[30] Soininen, Sami: Helsinki avaa 60 langatonta nettiyhteyspaikkaa, Helsingin sanomat, 21.9.2006, http://www.hs.fi/kaupunki/artikkeli/Helsinki+avaa+yli+60+langatonta+nettiyhteyspaikkaa/1135221797527
[31] Summa, Satu: Lahden kaupunkiverkkoa kolminkertaistettiin, Tietokone, 3.3.2006, http://www.tietokone.fi/uutta/uutinen.asp?news_id=26241
[32] Svento, Reijo: Ilmaisia julkisia verkkoja ei ole olemassa, FiCom webpage, 29.8.2006, http://www.ficom.fi/ajankohtaista/ajankohtaista_1_1.html?Id=1156846854.html

VI. Alternative Business Models for Visitors in Office Buildings

JOONAS OJALA
Helsinki University of Technology
joona.ojala(a)hut.fi

Abstract

Much discussion exists about different WLAN (Wireless Local Area Networks) business models. WLAN has been well accepted as a technology and there is a clear user-demand for it, but still many of the current market approaches have failed. WLAN has been typically made available as a complementary service to customers of coffee shops, hotels, airports and many other public places as well, but creating profits from this kind of business model has turned out to be very challenging. New kinds of business models have emerged, and in this paper I will research alternative business models for visitors in office buildings. Nowadays most companies are offering WLAN for their visitors for free, but in this paper I will discuss about the alternative solutions.

1 Introduction

New WLAN hotspots (access points) are introduced all the time. Whether the WLAN service is offered by WISP (Wireless Internet Service Provider) or some other party, like public place owner (airport, café etc.), has clear implications on the business model. Selling WLAN access to consumers has been surprisingly difficult, and WISPs have been forced to develop new kinds of approaches. It has been suggested that WISPs should become more "WOSP-ish" (Wireless Outsourced Service Provider), and start offering more WLAN services for companies instead of creating dense public hotspot network.[7] According to recent studies, 64 percent of businesses intend to increase WLAN deployment during the next 12 months.[4] The question is just – are equipment vendors the only ones who will profit, or can there be something for WISPs as well?

Before evaluating the different business models for visitors in office building in chapter 4, we look at some technical aspects of WLAN. Different standards are shortly introduced, and also the technological challenges are briefly discussed in chapter 2. WLAN is not yet a mature product, and though it can offer seamless wireless connectivity, many problems must be addressed before enterprises are willing to make large-scale investments on WLAN. Normal consumers can more likely tolerate for example some security or network management issues, but companies are expecting mature products. Thus I introduce some technological challenges which must be overcome.

2 Technology Overview

2.1 Standards

802.11b is the most widely used standard nowadays among the 802.11 (the first IEEE's WLAN standard) WLAN standard family. **Wi-Fi** (Wireless Fidelity) is more popular name for the 802.11b standard, which specifies a data rates up to 11 Mbps and uses 2.4-GHz ISM (Industrial, Scientific, and Medical) frequency band and DSSS (Direct Sequence Spread Spectrum) technology.

801.11a specifies data rates up to 54 Mbps and uses 5-GHz UNII (Unlicensed National Information Infrastructure) band and OFDM (Orthogonal Frequency Division Multiplexing) technology for transmission. Though 801.11a offers higher transmission speeds, it has not become very popular – probably for the reason that it is not compatible with most widely used 802.11b standard.

801.11g runs in the 2,4-GHz ISM band (like 801.11b), but it uses the same transmission technology – OFDM – as 801.11a and thus can operate with data rates up to 54 Mbps. 801.11g is backward-compatible with 801.11b, and may potentially become the most popular WLAN standard in the near future.

802.1x concentrates on WLAN security aspects. 802.1x defines port-based network access control, which provides mutual authentication between a network and its client.

802.11i, also known as WPA2, adds more security services to 801.11 WLAN standard family by specifically addressing issues concerning both the media access control (MAC) and physical layers of wireless networks. Authentication schemes in 802.11i are based on 801.1x. WPA2 (and its first version, WPA - Wi-Fi Protected Access) addresses the problems of the original 802.11b security specification, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses.[9]

2.2 Technological challenges

WLAN technology has been widely accepted, but before it can fully break through there are several challenges to overcome. These challenges include authentication, security, coverage, management, location services and interoperability.

Authentication must occur before a user can access the network resources. Authentication must be a very smooth operation, and not require active user participation. One problem with hotspots is that several access methods exist: while one hotspot requires users to login using web-based user interface, another uses client software that must be installed beforehand. This creates problems when users are swapping between hotspots, and probably forces a user to remember multiple username and password combinations. This raises some questions about global user identity databases, which do not currently exist, but could help in case of multiple authentication domains. There could also be a business opportunity for credit card companies which already possess huge customer databases, and could offer authentication and billing services. Finally, authentication mechanisms must be secure from the user's and service provider's point of view.

Wireless-hop security: data privacy must be guaranteed to WLAN users and network must be protected from malicious users. Higher-layer security protocols like SSH, SSL and VPN offer security under all WLAN infrastructures, but are not enough for several reasons: average users do not necessarily understand how they should be used, user authentication is done before any secure tunnels exist, and finally, wireless-hop security allows network service provider to protect against unknown, potentially malicious users. 802.1x and 802.11i standards try to address solutions both to authentication and wireless-hop security challenges. Security questions related to the paper topic will be discussed more in chapter 3.

Coverage can be, especially indoors, poor with WLANs. Radio frequency range and multipath interference limit the user mobility within a hotspot. If network service providers want to offer uninterrupted connectivity to roaming users, they must find ways to increase the density of hotspot coverage.

Network performance and QoS are important issues with WLAN, where the user behavior patterns are different from normal LAN. Network service providers must be able to provide enough capacity and coverage, and to do so, they must understand mobile user behavior. Though traffic pattern studies in enterprises have been implemented ([2]), this issue needs more research.

Network management can be difficult once hotspot coverage starts to grow. Installing new access points to various parts of network can require site specific radio frequency measurements and thus consume resources, and also make the network management more challenging.[1] With newest technology network management can be made easier by using central repository for configuration settings and security standards. These properties allow deploying enterprise-grade WLAN more effectively.[10]

Location and context-awareness could be utilized much more effectively than they are now.[1] Location specific information and advertisements could be offered to users, and if WLAN access points would be aware of each other it could be utilized in many ways: failure of one access point would make the nearby access point automatically adjust their power levels to provide coverage in exposed area, the location of wireless device could measured using triangulation, and in enterprise-grade WLANs rogue access points could be identified. Of course all this will require more advanced network management software.[10]

3 WLAN in enterprises

Before alternative business models for visitors in offices are further discussed, we study what kinds of concerns arise when WLAN access is granted for guests. The question is not about just letting the visitors access the Internet, but we must also consider the technology that is used and especially concentrate on the chosen security solution.

Security issues have been the biggest showstopper in enterprise WLAN adoption – studies show that 95 percent of companies consider security to be among the top five concerns in adopting WLANs.[4] Threats like a denial-of-service attack using radio frequency jamming, passive eavesdropping attack, session-hijacking vulnerabilities, rogue access points and – of course – malicious visitors exist, but with good policy control it is possible to produce secure systems. In case of granting the access for visitors, the security aspect is even more emphasized.

Usually unsecured visitor hotspot services run alongside the company's secure internal network. A visitor network is logically tied to a termination point in company's demilitarized zone (DMZ), which resides outside the company's firewall. In this kind of WLAN environments quest users are not any bigger threat to internal systems than normal Internet users.[8]

Another way to run WLANs is one where everyone – whether company's own personnel or visitors – is connected to single wireless network. Especially for larger sites this would be beneficial, because there would be fewer transmitters interfering each others, and less administrative tasks to take care in case of upgrades to access points. Initial configuration would be more time-taking and require special knowledge, but by using VLANs and multiple SSIDs (Service Set Identifier that identifies access point) for different user communities single wireless network can be implemented.[3]This kind of approach is closely related to idea where company's network – either WLAN or LAN – is fully public, and company's personnel must access company servers trough firewalls. Studying this idea further is left for future papers.

4 Business models

WLAN business models are under constant market evaluation. No model has yet proven its superiority, and new models for different types of situations – home, public, office – are continuously developed and studied ([5], [14]).

In the following chapters I have defined four different business models that could be used in case of visitors in offices. Almost no research exists on this field yet, and most of the models are based on some existing service offerings.

Before specifying some alternative business models for visitors in office buildings, I have defined some general success criteria for WLAN business models. Also different stakeholders of value networks are identified.

4.1 General success criteria

A successful WLAN business model must provide value for all stakeholders: end users, network service providers, and building owners.

From the end user's perspective WLAN must be easy to use, economic, and provide fast access in a transparent (device and access technology independent) manner.

Network service providers (WISPs) benefit when they have reliable and robust third-party authentication entity, have established peering agreements with other providers for seamless billing, and are able to adapt varying resource and performance demands of the users.

Building owners can gain profits when they have established business agreements with network service providers for installation, maintenance, monitoring, and support, and they are able to make network access an everyday utility for the end users.[1]

4.2 Free WLAN

Most companies that possess WLAN base stations are offering WLAN for their visitors for free, if the security policies just allow it. WLAN (or normal LAN) connectivity is considered useful for the business – it is a part of client and partner relationship management.

Companies are either renting WLAN service (equipment, installation and maintenance) from network service providers or taking care of all operations by themselves. If a network service provider is renting the service, there is an evident business case for WISPs (we could also use term WOSP that was mentioned in introduction). If the company is taking care of everything by itself, it should be aware of the resources this requires. It is most likely more economic – and also secure – to rent the service from WISP.

From the visitor's perspective this model is clearly the best possible. Especially if user management is implemented in an efficient way, and either visitor's host or someone in the lobby or waiting area is able to grant a temporary access for the user.

4.3 WISP collects profits

Companies might have difficulties in justifying WLAN charge for their visitors, because as stated, in most cases Internet connectivity is offered free for the visitors – and seen as a part of client or partner relationship management. To be better able to justify the costs, the company can outsource the WLAN, and let the WISP setup the WLAN service and gain profits. Most likely also the company would have to participate to setup costs, and if the company wants to use the WLAN for internal purposes it should pay some fees.

For user, this model is not optimal, and most likely decreases user's network usage. On the other hand, if service would be bundled for example to user's normal broadband or WLAN subscription, user would be more likely to use service. This kind of approach would give vantage to dominant WISPs.

4.4 Company generating revenue

Companies can also profit from their visitors, but this will most likely demand some kind of co-operation with WISPs. Network setup and maintenance would be done together with WISP, and also billing would require co-operation. The model would be quite similar to the one that was presented in the previous chapter, but in this case the company and network service provider would share the profits. This kind of model might not happen in case of office buildings, but on the other hand the model would encourage the company to really market their WLAN service.

4.5 Enterprise community

Companies can also form enterprise communities, and let the members use each others WLANs. This model would also require a WISP-like administrative layer that would offer both WLAN setup and maintenance services, and tools for user and network management.

From user's point of view this kind of service would be very beneficial, because it would allow wireless connectivity for free from various sites. Eventually this model is not very different from the model where WISP operates several company sites and allows users to access Internet through all of them. These kinds of models utilize the network effect, and should be interesting from dominant WISPs point of view.

4.6 Comparison of business models

The presented business models are compared from each stakeholder's point of view in table 1.

Table 1 Comparison of business models

	End user (visitor)	Network service provider (WISP)	Premise owner (company)
Free WLAN	service free, encourages usage	outsourcing the service generates opportunities, bundling LAN and WLAN?	costly, must consider co-operating with WISP
WISP collects profits	service charged, decreases usage	expensive set-up (if company not involved), good profits if service widely used	cheap if visitors widely use the service, set-up cheaper
Company generates revenue	service charged, user might not accept	chance to co-operate with company, percentual share for usage	generates profits if service is widely used, set-up more expensive
Enterprise community	service free, multiple sites increase usage	no opportunity, community though requires some kind of administrative layer	probably cheaper than WISP's offering, good option if large community

5 Case examples – Finland

I have identified two alternative business models for visitors in offices in Finland. The concept of offering something else than free access to visitors is very new, and before it can be fully evaluated, more market data is required.

The first case – Sonera HomeRun – is an incumbent telecommunications operator's offering, targeted also for public (airports, cafés etc.) hotspot users. In HomeRun only the network service provider (Sonera) gains profit from visitors.

The second case – SparkNet – is a enterprise community where companies can join. SparkNet generates income from selling business solution packages. SparkNet also sells user accounts for non-members.

5.1 Sonera HomeRun

Sonera is offering its WLAN service as a supplementary service to user's current subscription or as a separate subscription. By purchasing Sonera HomeRun, subscriber is allowed to access Internet through various public hotspots in Finland and abroad. Pricing scheme for Sonera HomeRun is presented in table 2, and hotspot statistics in table 3.

Table 2 Sonera HomeRun price list (19.10.2006)

Sonera HomeRun	
Connection charge, €	6,73
Monthly charge, €/month	3,36
Usage charge in public service area, €/min	0,26
Usage charge in public service area, €/month/subscription (unlimited use)	80
Usage charge in own corporate service area, €/min	-

Table 3 Sonera HomeRun hotspots in Finland and other courties (19.10.2006)

Hotspot type	Sites in Finland	All sites
Hotels and conference centers	149	601
Airports and train stations	25	49
Restaurants and cafés	9	112
Motorway services	9	47
Exhibitions and sport grounds	8	27
Companies	**20**	**93**
Public places	9	115

In addition to Sonera HomeRun, Sonera is offering Sonera HomeRun Corporate Service Area for companies. This solution allows companies to offer WLAN to their visitors without a risk of granting temporary access for visitors to company LAN – WLAN is totally separated from company's LAN. For company's own employees the service is free, but visitors are charged according to used time, unless they are monthly subscribers of Sonera HomeRun. Inside the corporate service area companies are also able to set the startup page of browser – and thus offer some additional information about the company. Additional charges related to Sonera HomeRun Corporate Service Area are presented in table 4.[12]

Table 4 Sonera HomeRun Corporate Service Area price list (19.10.2006)

Sonera HomeRun Corporate Service Area	
Site survey and radio planning, €/service area	588,66
Installation charges, €/base station	126,14
Introduction of portal service, €/service area	462,52
Maintenance/base station, €/month	84,09
ADSL Internet connection, €/month	183,33

Sonera's corporate service area offering is mainly targeted to smaller companies who do not want to operate their own WLAN, but still offer WLAN service for their visitors and own personnel. Companies having corporate service area cannot gain profits from visitors, all subscriber fees go to Sonera. Corporate service area can be also seen as a supplementary service to Sonera HomeRun, which is priced to attract only mobile business users. By getting companies to invest on corporate service area, Sonera is also trying to increase its subscriber base for Sonera HomeRun.

Subscriber value of Sonera HomeRun is clearly affected by the count of hotspots – more hotspots available, more value for the user. On the other hand, the count of hotspots is very closely related to subscriber count – more subscribers allow establishing more hotspots. This is a difficult dilemma for WISPs to solve, and one solution could be roaming agreements.[11] From table 2 it can be seen that only few (20) companies (sites) have so far invested in Sonera HomeRun Corporate Service Area.

5.2 SparkNet

SparkNet is a user community where companies can join by selecting one of SparkNet's business or enterprise solutions. Prices of these solutions are varying according the case, and they include for example tools for web based user management. SparkNet users can also join the OpenSpark community of approximately 2000 private users.

The basic concept of OpenSpark and SparkNet is that once a company has joined the community, it must offer the company's WLAN service to all other SparkNet and OpenSpark users, but it is mutually able to utilize other users' WLANs as well. So far approximately 200 companies have joined SparkNet.[6][13]

6 Conclusions and future work

Alternative business models for visitors in office buildings need further studying and market data. Empirical studies about the current state of visitor WLANs in office buildings would also be beneficial.

In this paper I have suggested few possible business models that could be used. The most promising ones offer value for all stakeholders: user, premise owner (company) and network service provider.

Free of charge model cannot be ignored, because most companies are using it and it is seen as a beneficial part of client or partner relationship management. Whether the visitor pays or not, is clearly an important question, but probably even more should be emphasized how the WLAN service is implemented and sold. Should WLAN be part of company LAN, should the WISPs bundle WLAN and LAN offerings, should it be used also for company' internal purposes, and who should take care of it? If companies are managing their WLANs by themselves, they must be aware of resources and costs it takes. When companies are ready to do large-scale WLAN investments, there should be a market opportunity for WISPs that are able to offer solutions that can handle all security, network and user management issues.

References

[1] Balachandran, A. et al: "Wireless Hotspots: Current Challenges and Future Directions", Mobile Networks and Applications 10, 2005

[2] Balazinska M. et Castro, P.: "Characterizing mobility and network usage in a corporate wireless local-area network", in: Proc. MobiSys'03, May 2003

[3] Betts, B.: "Providing Wi-Fi access for guests", TechWorld, April 25 2005

[4] Gartner Inc.: "Gartner Survey Shows that Corporate Wireless LAN Deployment is Increasing, But Security is a Major Concern", July 5th 2006, www.gartner.com, referred 19.10.2006

[5] Hämäläinen, S.: "Business models based on facilities bundling: success criteria", Seminar on Networking Business, TKK Networking Laboratory, 2006

[6] Kuosmanen, J.: "New Business Models for Public Wi-Fi Services", presentation on Telecommunication Forum 2006, Helsinki University of Technology, September 26 2006

[7] Metrinomics: "New WLAN Report Calls On WISPs To Be More 'WOSP-ish'", July 16th 2003, www.metrinomics.com, referred 19.10.2006

[8] Molta, D.: "Market Analysis: WLAN Security", Network Computing, June 23, 2005

[9] Park, J. S. et Dicoi, D: "WLAN security: Current and Future", IEEE Internet Computing, September 2003

[10] Richards, K.: “Enterprise WLAN is Growing Up”, Software Magazine, August 2005
[11] Smura, T.: “Roaming Considerations for Finnish Public WLAN Market”, Innovation Dynamics in Mobile Communications, Helsinki University of Technology, 2004
[12] Sonera HomeRun, www.sonera.fi, referred 19.10.2006
[13] SparkNet, www.sparknet.fi, referred 19.10.2006
[14] Tallberg, M.: “P2P-based Roaming Between Home WLAN Hotspots”, Seminar on Networking Business, TKK Networking Laboratory, 2006

VII. Business Models Based on Facilities Bundling: Success Criteria

SAMPO HÄMÄLÄINEN
Helsinki University of Technology
Networking Laboratory
sampo.hamalainen(a)hut.fi

Abstract

Wireless access networks have become common in public facilities such as airports, hotels, cafés and restaurants. By providing wireless local area network (WLAN) access the facility owners can attract new customers and create added-value for their core services. These facilities are often called hotspots. A hotspot owner can provide network access free of charge and thus create added-value for its core business, but often the access is provided by a 3rd party wireless Internet service provider (WISP) and bundled with the services or products of the hotspot owner. In this paper I introduce such business cases and related technological challenges.

1 Introduction

IEEE 802.11 has become a widely accepted WLAN standard family. Compared to other wireless access technologies, it provides a relatively high data rate within a short range. Public facilities have found it attractive to provide WLAN access to their customers. Most of today's laptops and personal digital assistants (PDA) are equipped with a WLAN card. Moreover, the trend of mobile phones with WLAN access becoming common makes this business interesting. Technology evolution enables new business roles to emerge. On the other hand, network convergence with variable radio access technologies (RAT) causes new challenges. For example user characterisation and traffic measurement required to understand the network requirements in certain facilities become complicated.

In section 2, I classify the general WLAN business models and value chain. In section 3, I introduce briefly the technologies crucial for the business models and in section 4 business case examples are introduced and analysed. Finally in section 5 I conclude the WLAN business model success criteria and challenges.

2 WLAN Business models

There are several business models for providing WLAN access in public facilities. The facility owner may provide an open WLAN access free of charge, typically with low Quality of Service (QoS), for its customers and thus create added value for its core business. Alternatively, it can buy the service from a 3rd party WISP and provide it bundled with its own services or products. Another option for a WISP is to offer a commercial WLAN access as its own separate service and get all the revenues. The facility owner will then attract new customers, and the WISP gets more customers.

The hybrid operating model for wireless hotspot businesses introduces a model for providing free WLAN access for communities in public facilities [7]. The final business model is based on revenues generated from purchased products and services and localised advertising. However, in this model as proposed by Jamaluddin et al. advertising is implemented over a software application, which the user must install in order to gain access to the network. This decreases remarkably ease-of-use, which is a significant obstacle for the service adoption. Some models use localised advertising by providing only a customised authentication page and forwarding a successfully logged user to a certain web page. Implementing localised advertising at a more detailed level by providing e.g. information from certain parts of mall is an interesting opportunity if always-on WLAN access will get commonly used in mobile phones. However, I do not handle any such cases in this paper.

While defining the business model, one should nderstand that a business model mediates between the technical and economic domains, as discussed in the paper of Mathias Tallberg [16]. Relevant technical issues related to facility bundling are security and authentication: facilities crowded with business users (hotels and airports) must enable a secure connectivity and authentication method. Some 3rd party authentication providers offer customised login pages in order to strengthen the facility owners brand image. The business model consists of market, value proposition, value chain, cost and profit, value network and competitive strategy. Understanding the value creation process is as essential as understanding the real cost structure. In addition to the techno-economic macro environmental factors, social and political factors affect the final WLAN business model. Regulators have so far decelerated the adoption speed of public WLAN services, as is discussed in the paper of Niklas Tirkkonen [18]. On the other hand, limited radio spectrum is not that problematic in indoor facilities as the facility owner has the power to decide who can use it.

2.1 Value chain

Porter (1985) introduced the *value chain* framework as a basic tool for systematically examining all the activities a firm performs and their interactions [12][15].

Figure 1: WLAN Generic Value Chain

Figure 1 illustrates one model, given by Paolini et al. for the generic value chain of WLAN. The hotspot owner negotiates deals with other players to install and maintain the hotspot. In addition, he can develop site-specific content such as localised advertising to users. The added value for hotspot owners is the increased attractiveness of the facility and ability to sell the service to customers. Network provisioning consists of hotspot setup and maintenance, and negotiating with hotspot owners or customer owners. It creates value in terms of hotspot optimization and partnerships with upstream players. Authentication and security provide interoperability and integration with mobile networks, and on the other hand enable business usage and billing. The function of billing and roaming is to establish partnerships between hotspot owners and customer owners, and integrate the WLAN service to the customer owners. Roaming enables larger coverage and customer-base, as will be demonstrated in TeliaSonera's business case. Finally, customer ownership covers customer acquisition, marketing, partnering, and integrating the WLAN service with other mobile services [12]. The value chain described above represents only a simplification of a WLAN service value system. While moving to more complicated business models, the value chains change to multidimensional value networks and should be connected to e.g. hotspot owner's core business. In addition, the technology evolution and new business roles will affect the complexity and dynamics.

3 Technology overview

IEEE 802.11b is currently the most common wireless LAN technology. Albeit it has become a de-facto WLAN standard, there are still several challenges to face until a ubiquitous hotspot infrastructure can be provided. Moreover, it should be mentioned that for example 802.11g standard defines the way wireless LAN gear communicates at up to 54 megabits per second while remaining backward-compatible with 11-Mbps 802.11b. In this chapter I concentrate mainly on the technology and deployment-related challenges related to providing 802.11b access in public facilities, which has a significant impact on the final business models. These challenges include network provisioning, authentication, security, billing and roaming. The generic value chain in section 2.1 illustrated how these challenges link to the final business model.

3.1 Technological challenges

Authentication, billing, security and coverage in public hotspots are problematic because hotspots are administrated by different providers and network accesses are configured differently. Moreover, implementing seamless roaming between variable RATs and service providers will be inevitable. This problem will lead up to new business roles.

Current authentication methods are implemented either through Web-based user interface or through proprietary client software requiring installation and configuration. The easiest option is to use existing user-id's (e.g. email-address or mobile phone number) and passwords, or a well-known 3rd-party authentication provider such as *msn.com* or *aol.com*[2]. Installing software decreases the ease-of-use, but may provide better security (especially if client software for Virtual Private Network (VPN) is included and opportunity for a Hybrid Operating Model [7]. Authentication is commonly based on RADIUS servers, which are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user [14]. Another option is to use SIM-based authentication, provided by GSM-networks. 3G-cards in laptops and WLAN access in mobile handsets enable easy and fast authentication based on user's International Mobile Subscriber Identity (IMSI). Moreover, using SIM-based authentication enables roaming between 3G and WLAN access networks. T-mobile offers access to users through a pre-established account while e.g. TeliaSonera HomeRun offers also one-time login and password to a temporary user.

Authentication provides only user identification, not protection of the transferred data over a wireless connection. The built-in security features of 802.11 include Service Set ID (SSID), Media Access Control (MAC) Address Filtering, Wired Equivalent Privacy (WEP) Encryption and 802.1x/EAP/LEAP [4]. SSID is a weak security method which uses a string of characters to identify a wireless network. Filtering the allowed MAC-addresses is neither a strong method, as the addresses can be figured out and assigned to unauthorized WLAN cards. WEP provides security based on shared keys by allowing only those WLAN cards with a valid key to access the network. However, configuring keys to a large number of users is not scalable and the encryption algorithms are vulnerable to attacks[2]. 802.1x, built on Extensible Authentication Protocol (EAP) and combined with SIM authentication is the emerging security method used by many service providers. According to TeliaSonera, deploying 802.1x and EAP-SIM enables interoperability in wireless LAN networks and easier and seamless access to services[9]. However, further development is still needed as it has been reported about flaws in 802.1x as well[4]. VPN is still the most reliable method in order to secure the connection to closed private networks.

3.2 Deployment challenges

In addition to the technological challenges, providing a sufficient QoS in terms of capacity, coverage, bandwidth, delay etc. is business critical. Network management, dynamic load management and bandwidth provisioning in the wireless network require facility-related information about users' behaviour, data-rate demands and time used in the network. Network should be able to adapt to the changing resource availability or changing traffic characteristics either statistically or dynamically and suggest some form of corrective action to the user. Understanding the deployment challenges related to network management, dimensioning and design, and cost structure incurred from network maintenance is crucial, as will be illustrated in the example case. The network dimensioning process (Figure 2) must be seen as a continuous process. However, although traffic characterisation in different facilities have been studied, it is not clear whether such usage models and network throughput translate to hotspots in public areas[2]. It seems that in order to produce realistic information for the future public network services, measurement should be performed outside the networks.

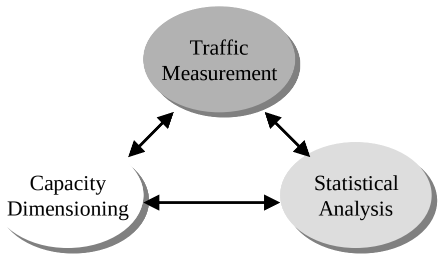

Figure 2: Network Dimensioning Process

3.3 Future vision

Network convergence and dynamics of new technologies, services and business models make the user characterisation and network measurement extremely complicated. Instead of network measurements, multi-radio terminals seem the most promising place to measure usage and traffic in the future [10]. Large operators and WISPs will probably have a major role in providing public WLAN access, as the hotspot owners want to outsource network maintenance, security, complicated billing logics etc. However the technical challenges listed below enable new business roles for providing 3rd party authentication and billing. Internet business players such as Google and Skype already have a large customer base with existing authentication parameters. Moreover, credit cards companies have an opportunity to bundle secure authentication and cost efficient billing, as the existing infrastructure enables lower cost transactions.

4 Business cases

I use Smura's classification of players in the WLAN market based on their background [15].

- Mobile and fixed line operators, providing WLAN services as a complement to their other data service offering
  Examples: TeliaSonera, Elisa, Saunalahti, T-Mobile
- Greenfield operators, providing WLAN services as their main business
  Examples: MobileStar
- Site owners, providing WLAN service in their own premises, both as means to tempt more customers and as a source of additional revenues
  Examples: Starbucks, Hesburger, hotels and cafés in Finland

The first two cases are operator-driven, which needs to be understood in the later examples of service bundling, since it seems that at least in Finland, most hotspot owners want to focus on their core business and bundle their core businesses with outsourced WLAN service. In addition, providing a commonly used service such as TeliaSonera HomeRun is more valuable for the hotspot owners, whose customer's may already be HomeRun subscribers.

4.1 TeliaSonera HomeRun

TeliaSonera is the leading telecommunications company in Nordic and Baltic area. Its product HomeRun offers Internet connectivity in public locations such as hotels, conference centers, cafés, restaurants, train stations and airports. HomeRun aims to enable large coverage of Internet Access Points (AP) for business users. Although the wide infrastructure ties significant resources and the target customers expect high QoS and support, this segmentation is supported by the fact that majority of WLAN service revenues will come from places with a lot of business users[4]. Homerun's large coverage (over 25,000 locations) is achieved through bilateral partnerships and roaming agreements with international WISPs[17]. Pricing is based on usage or time (short time or monthly fee). In addition to regular Internet access, TeliaSonera provides e.g. VPN solutions for secure access to company's intranet and SMS-service for exploring the nearest access point.

Table 1 lists the HomeRun hotspots by location. 58% of the hotspots are located in hotels and conference centers, where business users are present. In some hotels, HomeRun service is included in the hotel room price. Although airports and train stations cover only 5% of the sites, they are crowded with waiting business travellers. Due to roaming agreement with Connexion-by-Boeing, HomeRun service is also available on all airplanes on long haul SAS flights and many flights run by Lufthansa, ANA and Japan Airlines[17]. In addition, the service is provided on some ferry connections between Helsinki and Stockholm.

Table 1: Commercial HomeRun WLAN hotspots (14.10.2006)

Hotspot type	Sites in Finland	All sites
Hotels and conference centers	149	601
Airports and train stations	25	49
Restaurants and cafés	9	112
Motorway services	9	47
Exhibitions and sport grounds	8	27
Companies	20[1]	93
Public places	9	115

When HomeRun was first launched as Swedish Telia's service, it suffered from high price and therefore lack of subscribers [4]. Offering WLAN access to business users where ever they are requires significant investments on infrastructure and QoS. On the other hand, in order to cross the chasm (Figure 3) and get a new technology to the mainstream markets, a number of customer references and hotspots are needed[11]. To get more subscribers for a commercial WLAN service, large coverage is required, which TeliaSonera has later achieved via its wide infrastructure and roaming agreements with other WISPs.

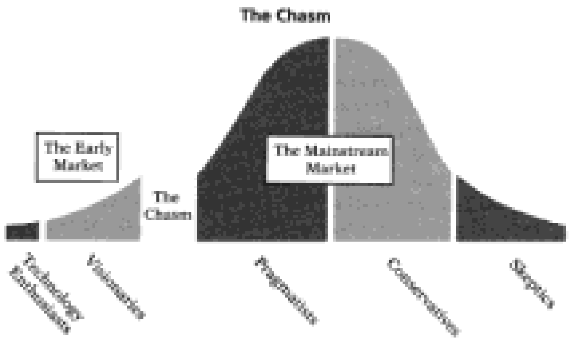

Figure3: Technology adoption curve

What makes HomeRun a successful business?

HomeRun is an attractive option for the service bundlers (facility owners) as it has a large coverage of other hotspots and therefore large base of subscribers who are willing to use HomeRun as their prior WLAN access provider. TeliaSonera's subscribers can combine HomeRun service with TeliaSonera's other offerings. For TeliaSonera, the existing core network infrastructure enables cost efficient operation. In addition, the right market segmentation has been crucial.

4.2 Starbucks, MobileStar and T-Mobile

Starbucks Corporation is a leading retailer, roaster and brand of coffee, located in 37 countries world wide. In January 2001, an American WISP MobileStar announced a strategic deal with Starbucks, Microsoft, IBM and Compaq, of which MobileStar assumed most of the risk and cost. Their vision was to provide broadband access hotspots over all The USA [4]. MobileStar deployed the hotspots in cafés and received all revenues from the service. For Starbucks the model offered more customer potential by enabling Internet usage while enjoying its products. MobileStar did not understand the network dimensioning and the total cost structure caused by scaling the network to a nationwide level. Moreover, additional costs incurred from building and maintaining fixed T1-lines to all the agreed Starbucks facilities. MobileStar lacked from subscribers partly because of poor marketing and early market phase. In October 2001 they failed to receive more funding and went bankrupt [21].

MobileStar was bought by Deutche Telekom and connected with its subsidiary, a multinational mobile phone operator T-Mobile, which has over 90 million subscribers in Europe and the USA and over 7000 hotspots in the USA [22]. WLAN access is still provided in Starbucks cafés, but no bundling is performed so far. T-mobile participates the 3GPP's Unlicensed Mobile Access (UMA)[20]. This combined with large hotspot coverage enable optimal mobile services from the user point of view. As Todd Achilles, director of handset product management at T-Mobile, puts it: "*The device automatically notifies you as you enter a Wi-Fi hot spot and switches to the fastest network available, allowing you to maintain your Internet session as you travel from your home, to Starbucks, to the airport, to a business meeting and to your hotel.*" [23]

4.3 Hesburger

Hesburger is a Finnish fast food chain with about 200 restaurants in Finland and Baltic countries. Its turnover was about 125 MEUR in 2003. According to their Internet page, 100 000 customers patronize daily in their restaurants [6]. The company is known of its well defined concept and uses its brand to bundle services. In addition to fast food restaurants, Hesburger runs a virtual mobile operator, hotel, cafés, car washes, and home product services. With a member card, customers can receive bonus from their shopping and get benefits based on the 'earned' membership level. The level depends on the amount of shopping. Many of the facilities are equipped with WLAN access. Table 2 illustrates how the HeseWLAN service is bundled with other Hese-services.

[1] Major part of the companies represented TeliaSonera's own offices or stores.

Table 2:HeseWLAN prices (14.10.2006)

Membership level	Free WLAN time (min/day)	Price EUR/min
Bonus card	10	0,10
Silver	30	0,10
Gold	60	0,10
Platinum	120	0,10

WLAN access is operated by DNA Finland – a competitor to TeliaSonera and Elisa. HeseWLAN is provided in over 100 facilities owned by Hesburger. In addition, DNA Finland provides the service to non-member customers with a price of 3EUR/30min. Alternatively customers may use the service with their existing DNA WLAN subscription. The partnership between Hesburger and DNA Finland generates a 'win-win-situation' for both parties; DNA Finland gets more subscribers for its existing infrastructure and Hesburger gets added-value for its core business and increased sales via service bundling without significant investments or risks.

The business model success criteria is composed of existing network infrastructure, customer bases, brands and facility network and bundling attractive services for a specified customer segment.

4.4 Hotels in Finland

This section illustrates how WLAN access is provided for the hotel guests in Finland. The analysis is based on interviews with persons responsible for the service offering in three different hotel chains. Hotel Kämp is a five stars hotel located in the centrum of Helsinki. It belongs to the Starwood Hotels & Resorts -chain, which segments to luxury accommodation. Typical guest is a celebrity or a business customer in high position. An open WLAN access is available in the hotels public spaces free of charge and both TeliaSonera's and Elisa's accesses are provided in meeting rooms. Currently HomeRun is available in hotel rooms with price of 50EUR/day. According to the General Manager Timo Tirri, there will be changes in pricing and access provider in hotel rooms. However, Starwood Hotels & Resorts policy defines that no free access will be provided in the hotel rooms[19].

Restel Consolidated runs 43 hotels in Finland with brand names Crown Plaza, Cumulus, Holiday Inn, Hotelli Seurahuone Helsinki, Ramada and Rantasipi. Its target customers vary from families and holiday guests to business customers. They offer the HomeRun service with a price of 15EUR/day for their guests. In addition TeliaSonera has made investments for the WLAN infrastructure in Restel hotels. According to IT Manager Esko Alarvo, a total bundling by providing the service with the hotel room price is under consideration[1].

Radisson SAS Hotels & Resorts chain belongs to Reziror SAS Hospitality, which runs totally 133 hotels. Typical guests are travelling business customers. Radisson SAS aims to provide free Internet access in all their hotels. In Finland, all hotel guests can get HomeRun service while checking in to the hotel. According to the Development Manager Marja-Liisa Järvenpää, the bundling has been a success. Compared to the earlier model of chargeable HomeRun service, total bundling creates much more value for their customers[8]. Moreover, offering access to the service which the guests already subscribe is valuable for both the operator and facility owner.

4.5 Roberts Coffee

Roberts Coffee is the leading coffee shop chain in Nordic countries with nearly 50 cafés in Finland, Sweden, Estonia and Denmark. Its concept Netcup offers Internet access for the café's customers. Six Netcup cafés in Finland offer also free WLAN access. Once a customer buys a product, she gets a one-time username and password for accessing Saunalahti WLAN service. When the customer logs in, she will be forwarded to the Netcup web page. After 15 minutes, the account expires and the customer will be automatically logged out. Customer can then purchase new café products and get new WLAN access with it. According to Beatrice Björklund responsible for Roberts Coffee business sales, the investment has been profitable as the service has a number of users [3].

5 Conclusions

WLAN is a widely accepted network access method, and its importance will grow as the mobile handsets are equipped with 802.11 radio interface. WLAN technology offers an inexpensive investment on facility's attractiveness. However, making successful business by providing WLAN access in public facilities depends on right customer targeting, attractive service bundling and understanding the real value creation process and cost structure. The successful business models are often based on partnerships with existing network infrastructure, brands, facilities and customer bases. Technology evolution enables new business models and roles to emerge. However, there are still a number of challenges in order to manage the end-to-end usability. It is interesting to see, when facilities will bundle new services, such as free VoWLAN calls with a cup of coffee. What are the required actions and business roles for implementing such service bundling?

References

[1] Alarvo, E. IT Manager, Restel Consolidation, phone interview at October 16th 2006

[2] Balachandran, A. Voelker, G.M. Bahl, P. Wireless Hotspots : Current Challenges and Future Directions, Kluwer Academic Publishers, 2005, ISSN: 1383-469X

[3] Björklund, B. Business sales, Roberts Coffee, phone interview October 19th 2006
[4] Efimov, A: Rabbits Return: An Exploration of WiFi Business Models, University of Strathclude, Glasgow, 2002
[5] Hayes, K. Kuchinskas, S. Going Mobile, CMP Books, 2003, ISBN 1-57820-300-7
[6] Hesburger, www.hesburger.fi
[7] Jamaluddin, J. Doherty, M. Edwards, R. Coulton, P: Hybrid Operating Model for Wireless Hotspot Businesses, IEEE, 2004, ISBN: 0-7803-8145-9
[8] Järvenpää, ML. Development Manager, Radisson SAS Hotels & Resorts, phone interview at October 16th 2006
[9] Järviranta JM. Operator View to Multi-access Roaming, Mobile Monday, Helsinki, 2006
[10] Kivi, A. Measuring Mobile Data Service Usage and Traffic in Mobile Multi-Access Networks, Helsinki University of Technology, 2006
[11] Moore, G.A. Crossing the chasm: marketing and selling high-tech products to mainstream customers, revised edition, Harper Perennial, 1999
[12] Paolini, M. Farrar, T. Pow, R. 2002. The WLAN opportunity for wireless service providers, Analysys
[13] Porter, M.E. Competitive advantage, New York: Free Press, 1985
[14] Rigney, C. Willens, S. Rubens, A. Simpson, W. RFC 2865: Remote Authentication Dial In User Service (RADIUS), The Internet Society, 2000
[15] Smura, T: Roaming Considerations for The Finnish Public WLAN market, Innovation Dynamics in Mobile Communications, Helsinki University of Technology, 2004
[16] Tallberg, M. P2P-based Roaming Between Home WLAN hotspots, 2006
[17] TeliaSonera, www.teliasonera.com, www.homerun.telia.com
[18] Tirkkonen, N. Regulation of Public WLAN Services
[19] Tirri, T. Hotel Kämp, General Manager, phone interview at October 16th 2006
[20] UMA Technology, http://www.umatechnology.org
[21] Shosteck Group White Paper. Lessons From Metricom and MobileStar: Success Factors for the Portable Internet Access Market
[22] T-mobile, www.t-mobile.com
[23] Vance, J. When Wi-Fi meets cellular, NetworkWorld.com, March 14th 2005

VIII. P2P-based Roaming Between Home WLAN Hotspots

MATHIAS TALLBERG
mathias.tallberg(a)tkk.fi
Helsinki University of Technology
Networking Laboratory
P.O. Box 3000 FIN-02015, FINLAND

Abstract

The increased amount of broadband Internet connections at home, combined with the low cost of wireless local area network access points, has made it possible for individual end-users to contribute to the wireless landscape by allowing open access to their WLAN access points. Consumers' WLAN access points and emerging handsets equipped with WLAN capability provide an opportunity for peer-to-peer -type of wireless coverage. Current metropolitan areas are already to some extent covered by consumer home WLAN networks and can ideally form one big network which then can be used freely by members of a community. This paper concentrates on describing the current situation in P2P-based roaming between home WLAN hotspots, what are its pros and cons, and why it is being done.

Keywords: WLAN, P2P-based roaming, access point sharing, business model.

1 Introduction

Wireless LAN (WLAN) networks enable end-users to obtain high-speed Internet access at different locations, both indoors and outdoors, through different devices. The coverage of these WLAN networks is constantly increasing and thus enabling the end-users to get better connected to the Internet, at least theoretically. The increased amount of broadband Internet connections at home, combined with the low cost of WLAN access points and other WLAN hardware, has made it possible for individual end-users to contribute to the wireless landscape by allowing open access to their WLAN access points.

The WLAN technology has during the past ten years continuously exceeded expectations. Almost every laptop computer today has WLAN included and the technology is also becoming more common in smaller devices such as mobile handsets. A WLAN access point can be deployed at low cost to offer Internet connectivity practically anywhere where there is a broadband wireline Internet connection.

WLAN, as a technology, is still evolving rapidly and new standards are being created to improve its capabilities. Security for example has been an issue. However, many of the problems related to security have already been solved. Also improvements in quality of service, roaming capability, and improved bandwidth have been considered, i.e. the technology is improving and it will also in the future represent a cost efficient alternative for wireless communications.

WLAN technology can be used in a variety of ways, both as commercial offerings and for free. However, this paper concentrates only on describing the current situation in sharing of home WLAN access points in a peer-to-peer (P2P) manner. The paper starts by defining a business model, and the P2P-based roaming between home WLAN hotspots. Then an analysis and comparison of proposed peering frameworks is given. Next, the P2PWNC framework, and the offerings by OpenSpark, FON, and LinSpot are described. Finally, some regulatory issues are mentioned.

2 Business Models

The term *business model* is known for not being used consistently. Therefore, before going any further a short definition of what is meant by a business model is given.

One definition of a business model, is given by Chesbrough & Rosenbloom [1]. The key ideas of this definition can be seen in Figure 1 below.

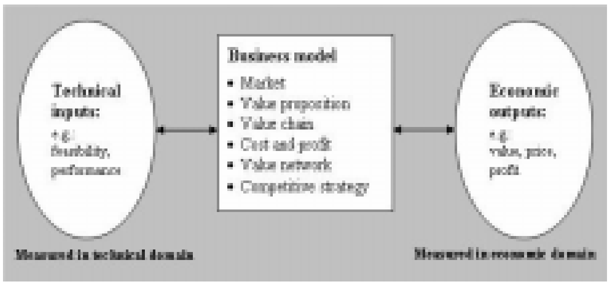

Figure1. Business model mediates between the technical and economic domains. [1]

Here, the functions of a business model are to:

- Articulate the value proposition , i.e. the value created by the offering based on the technology;
- Identify the market segment, i.e. the users to whom the technology is useful and for what purpose, and specify the revenue generating mechanism(s) for the organization;
- Define the structure of the value chain within the firm required to create and distribute the offering, and determine the complementary

assets needed to support the firm's position in this chain;

- Estimate the cost structure and the profit potential of producing the offering, given the value proposition and value chain structure chosen;
- Describe the position of the firm within the value network linking suppliers and customers, including identification of potential complementors and competitors;
- Formulate the competitive strategy by which the innovating firm will gain and hold advantage over rivals.

The six attributes mentioned above also collectively serve additional functions, namely to justify the financial capital needed to realize the model and to define a path to scale up the business.

Timmers [2] provide another relevant definition on how a business model is constructed:

- An architecture for the product, service, and information flows, including a description of various business actors and their roles;
- A description of potential benefits for the various business actors;
- A description of the sources of revenues.

Some work has been done on classifying business models, mostly in the e-commerce and Internet domains. Business models based on trust systems and consumer-driven approach have not been studied deeply though. The problem with these kinds of business models is that it can e.g. be hard to identify the profit potential. The value of these business models can be easy to explain from the end-user perspective. However, making money out of them can be considered much harder.

3 P2P-based Roaming Between Home WLAN Hotspots: Basic Concepts

Consumers' WLAN access points and mobile handsets provide an opportunity for P2P type of wireless coverage, either in fixed hotspots or random locations. Current metropolitan areas are to some extent already covered by consumer WLAN networks and can ideally form one large network which then can be used freely by e.g. neighbors, visitors and mobile users.

WLAN, as a technology, already enables individuals to share their broadband Internet access to their peers. Although this is straightforward technically, two broader issues arise: [3]

1. A scheme for P2P-based sharing of resources must take into account the selfish tendency (i.e. free-riding), which is especially relevant in electronically mediated communities;
2. Any scheme for the P2P-based sharing of resources that is centrally controlled may give birth to mutually inaccessible systems.

To make P2P-based roaming between home WLAN hotspots happen, the first step is to create a community of individuals who share their home WLAN access points between each others. The next step is to get home WLAN access point owners to join the community. By joining a P2P WLAN community, members gain by getting access to other members' WLAN access points. The members of the community are then able to get connected to broadband Internet services more widely without any additional costs and hence, get more value out of their connection. One argument could be that why should someone pay for Internet access on the go when he/she already has paid for it at home?

One proposal for P2P-based roaming between home WLAN hotspots is the P2P wireless network confederation (P2PWNC) scheme explained in detail later on [3]. WLAN by municipalities are currently also being deployed. These networks can offer unified and citywide WLAN access to citizens and visitors alike. [4, 5, 6]. Other related efforts include the various free networks [7] that are being deployed in cities worldwide. The free hotspots are usually set up without centralized coordination. The problem with free networks, however, is that they rely on the altruism of their participants, which can hinder their deployment [3].

Two commercial offerings, LinSpot [8] and Netshare [9], are somewhat similar with the P2PWNC proposal. Users are encouraged to share their residential hotspots with nearby visitors and receive compensation for their contribution. In principle, this model is no different from hotspot aggregation, as it relies on centralized brokers. [3]

Another sharing scheme of WLAN networks is offered by FON [10]. FON is currently the largest WLAN community in the world. The members of the FON community share their wireless Internet access at home and, in return, enjoy free WLAN wherever they find another so called Fonero's access point. Another offering that will be discussed and analyzed in more detail in this paper is OpenSpark [11].

4 Analysis of Selected Peering Frameworks and Offerings

4.1 P2P Wireless Network Confederation

The P2P Wireless Network Confederation framework [3], or shortly P2PWNC, is a design that is fully self-organized and provides collaboration incentives to selfish peers. The goal is to promote cooperation in a resource-sharing community of autonomous peers where the peers can both provide and consume the resource in question.

Briefly, the proposal is this: peers, i.e. owners of home WLAN access points should organize into small groups that are called teams, and start playing a game (in the game-theoretic sense) with three simple rules [3]:

1. Each team must operate and maintain a number of WLAN access points;
2. Members of teams may be freely serviced by WLAN access points belonging to other teams only if they can prove that their team also freely services members from other teams;
3. There is no referee.

The underlying assumption of this game is that the threat of exclusion and the promise of free roaming are good enough reasons to share one's WLAN access points with others.

There is no assumed P2PWNC authority. Hence, P2PWNC peers would be tempted to under-provide. This issue is solved by following a simple protocol that is secured by standard cryptographic primitives that enables contributing peers to detect and exclude such free-riders from the P2PWNC system. This provides incentives for the P2PWNC system to grow as more and more peers join. By eliminating centralized brokers from the P2P sharing scheme a scale-free unified roaming system can emerge.

4.2 OpenSpark

OpenSpark [11] is a community of wireless Internet users administered by MP-MasterPlanet [12]. To become a member of the OpenSpark community one needs to offer his/her WLAN access point to other community members. By doing this the member of the OpenSpark community gets one OpenSpark user-ID. The OpenSpark architecture to the Internet is visible in Figure 2 below.

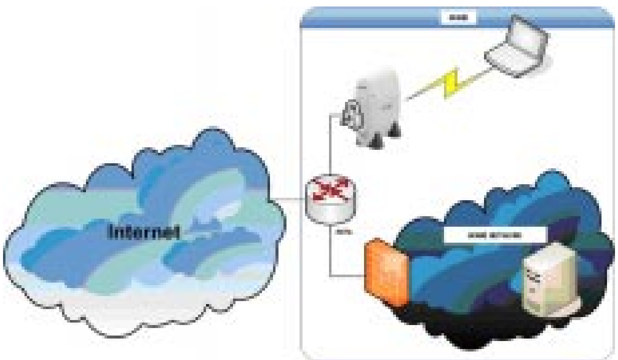

Figure 2. OpenSpark architecture (modified from [11])

With the OpenSpark user-ID the members of the community can use the Internet through all OpenSpark access points. With the OpenSpark access point the user of the wireless network service is prompted with the same look-and-feel to the network regardless of where he/she logs on to the service. The OpenSpark access points are available from an online store.

Other features of the OpenSpark base station include:

- User identification through SSL secured WWW connection;
- Web-based administration;
- Centralized user database;
- Additional user-IDs for visitors and family members.

The OpenSpark access point uses existing broadband connections. Restrictions in the use of broadband connections are as follows:

- A public IP-address is needed, however, the IP-address can be either static or dynamic;
- Traffic on the broadband connection should not be restricted in any way.

A member of the OpenSpark community is offered a secure wireless network at home, a broadband connection that is available also outside of the home, and access to all OpenSpark access points free of charge.

4.3 FON

FON [10] is the largest WLAN community in the world. The members of the FON community are called Foneros. To become a Fonero one needs to buy a La Fonera**,** which is a so called FON Social Router. The router enables a new member of the FON community to share his/her home broadband connection with other Foneros. Then when a Fonero is away from home and he/she needs Internet access, he/she just needs to log on to a FON access point, and use Internet connectivity for free by remembering a login account and a password.

There are three types of Foneros as illustrated below:

Figure 3. Types of Foneros in the FON community [10]

Explanations of the types of Foneros in the FON community:

- Linus: Most of the users are Linuses. A Linus shares his/her WLAN at home and in return gets free WLAN wherever he/she may find another FON access point.

- Alien: Aliens are those that do not share their WLAN. They are charged for the access to the FON community.

- Bills: Bills are in business and want to get additional revenues by charging Aliens for their access to their WLANs. Instead of access, Bills get a share of the money that Aliens pay to access the community through their FON access point.

The charge for access is based on the account status of the "home" router. A Linus has free access to any FON router, regardless of if the owner of the router is a Bill or a Linus. If you are a Bill you have to pay per day regardless of if the router you are connected to belongs to a Linus or another Bill.

The La Fonera offers two wireless network signals (SSIDs), one private and one public. The private signal is encrypted using WPA and the public signal is accessible to Foneros only. The public signal is the one that turns the broadband connection into a FON access point.

4.4 LinSpot

LinSpot [8] is a free software for selling an end-users wireless Internet access. It is based on P2P principles and it uses a combination of different technologies to turn the wireless Internet into a so called "paid-for Internet" access point and let the end-user benefit from it. Hence, LinSpot is not about offering free connection to WLAN access point, but to offer Internet connectivity at a reasonable price, i.e. LinSpot uses the consumer-to-consumer business model to let the end-users earn money.

To start using LinSpot the end-user only needs to download a software, and after that, complete an installation process. The payment transactions for the connectivity charges are handled securely with end-to-end encryption. The features of LinSpot include e.g.:

- A free software with automatic software updates;
- Possibility to earn instant money for shared wireless access;
- Works with all WLAN access points, including NAT and network configurations;
- Free access for an unlimited amount of wireless users which is controlled by the end-user;

Some of the features from a visitor's point of view and what they experience when they connect to a LinSpot network:

- Prices are less than half those of the typical commercial hotspot providers;
- Works on all operating systems;
- No need to download and install any software, as LinSpot works with standard IP protocols;
- Easy 3 steps: configure proxy, select access time and enter payment information;
- Customers get access to other places on the world wide LinSpot network;
- No startup costs or recurring subscription fees;
- No advertisements, no spyware.

LinSpot delivers consumer-to-consumer technology for end users WLAN equipment. A 15% share from the visitors goes to LinSpot to pay for the development of new versions, the LinSpot servers, marketing of the network and profit.

4.5 Comparison

Table 1 shows a comparison of the framework/offerings that have been discussed in this chapter.

	P2PWNC	OpenSpark	FON	LinSpot
Business model	None Free wireless Internet connectivity	Free wireless Internet connectivity Sale of access points	Free wireless Internet connectivity as either: - Linus - Bill - Alien Sale of access points	Free wireless Internet connectivity Possibility to earn from sharing (15% share from visitors)
Administration	No authority	Centralized	Centralized	Centralized
Roaming with other communities	No	Yes	No	No
Framework/ offering	Framework	Offering	Offering	Offering

Table 1. Comparison of proposed peering framework and offerings.

FON and LinSpot are the only offerings that make it possible for WLAN access point owners to earn money. However, these two offerings are centralized in nature (also OpenSpark) which could make it hard for a unified roaming system to emerge. However, OpenSpark community and SparkNet [12] communities can roam between each others access points.

By comparing these frameworks to a subset of the definition of a business model by Chesbrough & Rosenbloom [1], many issues arise. The value proposition is clear in each of the cases. The value that is created goes to consumers, at least in most of the cases, roaming between WLAN access points. The market segment to which the technology is useful is also clear, i.e. home WLAN hotspot owners who also own e.g. a laptop computer or a handheld equipped with WLAN. The revenue generating mechanism(s) for the rameworks are, however, not so clear. This also goes to the profit potential of producing the offering, given the value proposition. Sale of community WLAN access points is one possibility, revenue sharing from paid access is another. However, the gain through only these would require a large community. Other possibilities could for instance include advertisement and possibly also chargeable value added services.

5 Regulatory Issues

Sharing of WLAN access points sounds promising, at least from the consumer's point of view. However, there might be some regulatory obstacles that need to be tackled, e.g. the Internet service provider's Terms of Service (ToS) may not allow sharing of broadband connection with others.

Usually an Internet service provider has the right to offer a service according to its own wishes. This means that the Internet service provider can restrict the service that they offer in some way through the ToS contract. For example some Internet service providers do not allow for the end-user to have an own server, or only if the end-user pays an additional fee. Some providers again explicitly prohibit sharing Internet connectivity with others.

However, many providers have agreed to support cooperation with e.g. OpenSpark and FON. The communities need to actively encourage and drive the Internet service providers to allow WLAN sharing. However, one always needs to remember that regulation is man made and it can always be changed. The question here is, will the regulative framework change so that it will encourage P2P-based roaming between home WLAN hotspots?

6 Conclusions

The large amount of home WLAN access points and the fact that WLAN is becoming more common in smaller devices, such as mobile handsets, provide an opportunity for P2P-type of wireless coverage. Current metropolitan areas are already to some extent covered by consumer WLAN networks and can ideally form one big network which then can be used freely by e.g. neighbors, visitors and mobile users.

This paper introduced the concepts of P2P-based roaming between home WLAN hotspots. The reason why this is of interest is that it makes it possible for individuals to gain substantially by getting access to other individuals' WLAN access points and hence be able to get connected to broadband Internet services widely, which to some extent can be considered self-organized.

This can be done by creating a community of individuals who share their WLAN access points and hence get more value out of their connection. However, any scheme for P2P-based sharing of WLAN access points that is centrally controlled may give birth to mutually inaccessible systems. This can make it hard for this kind of WLAN sharing to become a global phenomenon. Another problem is the actual community building and the network effects associated with it. The actual business model is not clear and many issues are still open. Also the regulation causes some problems.

What will be of interest in the future is how these communities will be able to grow and how much. Also, will there be changes in regulative frameworks that encourage this kind of sharing of home WLAN access points.

References

[1] Chesbrough, H. & Rosenbloom, R. S. (2002) The Role of the Business Model in Capturing Value from Innovation: Evidence from Xerox Corporation's Technology Spin-off Companies, Industrial an Corporate Change, 11, 3, pp. 529-555

[2] Timmers, P. (1998) Business Models for Electronic Markets, URL: http://www.imse.hku.hk/imse2016/Readings/Essential/BusinessModel-Geoffrion/Timmers/98_21_n.html. Referred 01.10.2006

[3] Efstathiou, E. C. & Polyzos, G. C. (2005) Self-organized Peering of Wireless LAN Hotspots, European Transactions on Telecommunications, 16, pp. 471-482

[4] Municipal Wireless, URL: http://www.muniwireless.com. Referred 02.10.2006

[5] Wireless Philadelphia, URL: http://www.phila.gov/wireless. Referred 02.10.2006

[6] PanOulu, URL: http://www.panoulu.net. Referred 02.10.2006

[7] Free Networks Association, URL: http://www.freenetworks.org. Referred 02.10.2006

[8] LinSpot, URL: http://www.linspot.com/. Referred 29.09.2006

[9] NetShare, URL: http://www.speakeasy.net/netshare. Referred 29.09.2006

[10] FON, URL: http://en.fon.com/. Referred 29.09.2006

[11] OpenSpark, URL: https://open.sparknet.fi. Referred 29.09.2006

[12] SpakNet, URL: http://www.sparknet.fi/fi/. Referred 29.09.2006

IX. Measuring Mobile Data Service Usage and Traffic in Mobile Multi-Access Networks

ANTERO KIVI
Helsinki University of Technology, Networking Laboratory
P.O. Box 3000 FI-02015, FINLAND
antero.kivi(a)tkk.fi

Abstract

New wireless access networks, managed by multiple operators, are emerging as alternatives to mobile cellular networks. Thus, having a holistic view on usage and traffic patterns will be increasingly difficult. A range of methods exist for collecting data on mobile data usage and traffic. Surveys and terminal measurements provide very detailed sample based data, whereas mobile network data is less granular but is based on an operator's entire subscriber base. Server measurements give detailed data on usage patterns of a fairly focused user population. In the future of heterogeneous multi-access networks, multi-radio terminals seem the most promising place to measure usage and traffic, while mobile cellular networks are likely to lose most as traffic partly leaks to other networks.

1 Introduction

Accessing the Internet using advanced mobile handsets and mobile usage of laptop computers is increasing rapidly. Reliable and transparent information on true mobile service usage and traffic patterns is of value to many stakeholders, including business development and marketing, product development, network planning and management, as well as academics studying topics such as consumer behavior and usability.

New wireless access technologies, such as WiMAX and Flash-OFDM, are emerging as alternatives to existing mobile cellular network technologies, while the coverage of WLAN hotspots of various providers is ever increasing. The emergence of multi-radio terminals featuring radio interfaces in addition to basic mobile cellular radio is supporting this trend. Meanwhile, the performance of mobile cellular networks is increasing with the HSPA technologies, keeping mobile cellular as a viable alternative for wireless Internet access. In the future, good interoperability between different access technologies will be essential, and terminals should be able to select the best available access network automatically without user input.

In this heterogeneous environment where both licensed and unlicensed radio spectrum is used and the network has no centralized point, understanding the system as a whole becomes hard. Moreover, as traffic will diverge to multiple networks managed by multiple access providers, having a holistic view on usage and traffic patterns will be increasingly difficult.

In this paper, the alternative sources for collecting information on mobile data usage and traffic are presented and compared, after which the effects of the trend towards the use of multiple wireless access network technologies on these methods are considered.

2 Sources of Data on Mobile Data Service Usage

Usage data can be obtained from many alternative sources (see Figure 1). The most straightforward way available to all researchers is to do a survey or a panel study on a sample of real end-users, while actual usage measurements can be conducted directly at (a sample of) terminals, at the mobile network, and at various servers. Moreover, the charging and billing functions in networks and servers can also provide data on service usage.

Some secondary sources can also be used to acquire data on usage. Expert interviews typically provide information either derived from other data sources or just based on the expert's educated guesses, although such interview studies do enable a large scope as specialists and managers from different organizations and functions can be interviewed. Mobile operators and handset manufacturers publish data on usage and sales in their quarterly or annual reports. Background data, albeit with somewhat narrow scope, is published by retail and wholesale organization such as the Finnish Association of Electronics Wholesalers [5] and Kotek [12], and organizations formed due to regulatory requirements, as is the case with number portability and the Finnish NUMPAC organization [16].

2.1 Surveys and Panels

Surveys are the most widely used method of data collection for studying mobile data service usage. Surveys can be implemented using e.g. telephone, postal mail, email, web, and various face-to-face questioning methods, depending on the available resources and the objectives of the research. Thus, the used method also defines the scalability and accuracy of the survey. Time series data can be produced by repeating a certain set of questions. Surveys are an efficient way of collecting

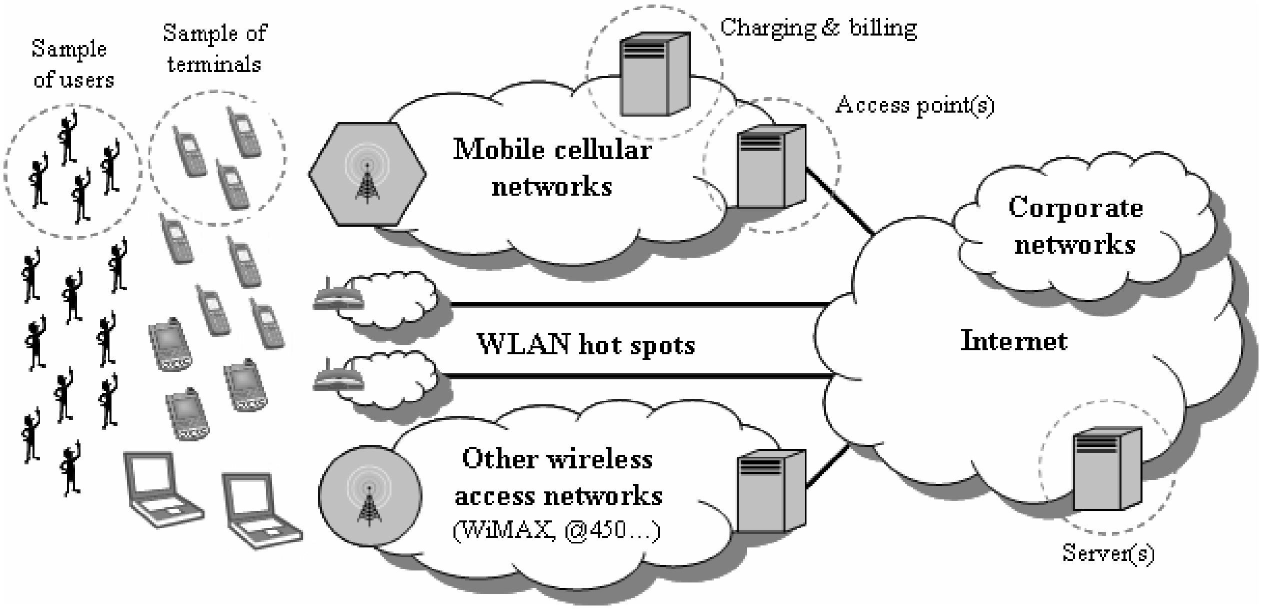

Figure 1 Sources of data on mobile data service usage

information from a large number of respondents, with statistical techniques to determine issues such as statistical significance of the results. Surveys are also flexible as a wide range of information can be collected to study e.g. attitudes, values, beliefs, and past behavior. However, survey responses always depend on the respondents' motivation, honesty, memory, and ability to respond. While a random sample of subjects is often selected for the survey, the actual respondents are usually self-selected, meaning that the characteristics of the whole population cannot be obtained from the sample. Finally, survey question answer-choices could lead to error, as they are often relative only to a personal abstract notion, for both the respondent and the interpreter of the results.

A continuous panel study is a series of measurements on the same sample of test units over an extended period of time. Panel research is used extensively both in Europe and the U.S. to study consumer purchase patterns [1], and it has been used to study mobile service usage as well [10]. Participating panelists use the diary method and register usage events manually to an online or paper "diary", which results in data of high accuracy and granularity. The basic limitations of the panel method are similar to those of surveys, although the continuous nature of panels significantly limits sample sizes.

2.2 Terminal Measurements

Panel studies can also be conducted at the terminal level, where the manual registering of usage events is replaced with the logging functionality of monitoring software or hardware installed in the terminal. Recruiting a representative panel of people is one of the main challenges also in terminal level measurements. Explanatory background variables on the terminal user(s) are also often collected at beginning of the panel, with the reliability issues typical to all survey data. In case of terminals with multiple users (e.g. PC, TV), measures need to be taken to distinguish the usage of each individual.

Terminal level measurements are quite common in the PC world. Commercial analysts, such as Nielsen NetRatings, have panels with hundreds of thousands of monitored participants. The software watches what a user does with the computer and sends that information further. While being otherwise quite similar to benign PC monitoring software, malicious spyware monitors the PC without the consent of the user. Spyware can collect information ranging from tracking the types of visited websites to recording the user's keystrokes to intercept passwords or credit card numbers.

Television viewing can also be measured at the terminal level. In Finland television viewing research is conducted with a continuous measurement of in-home viewing of a panel of 1000 households. The TV sets in panel households are equipped with metering devices to monitor changes in set status and viewer appearance. [6]

The monitoring of advanced mobile handsets has become possible due to recent developments in handset operating systems and processing capability. A handset monitoring software can measure the usage frequencies, durations and volumes of all terminal features and applications. Communication-specific data (e.g. voice calls, SMS, MMS) can be broken down between different callers/senders and recipients, while visited browsing destinations can also be logged. Usage of the handset's different radio interfaces (e.g. GSM/WCDMA, WLAN) for packet data transmission by different applications can be differentiated, and the possible *ad hoc* connections (e.g. Bluetooth, WLAN) with other terminals can also be measured. Usage of the handset's offline features (e.g. camera, multimedia player, games) and broadcast multimedia (e.g. FM radio, DVB-H based TV) is also captured. Moreover, location information (cell identity code) connecting user location and mobility to usage might also be collected, though the actual geographic location of the cell is not known by the terminal. The monitoring software can be further augmented with triggered “real time” pop up questions sent to the panelist after certain pre-specified event (e.g. at 12 o’clock, browsing session ended). While handset monitoring is not yet very common, at least two such software for the Symbian S60 platform with slightly differing functionality have previously been used by the academic community ([11] and [20], [14] and [3]). A major drawback of these studies is that their scope is limited to the users of a certain, albeit widely used, handset operating system (OS) and software platform. As the OS and software platform might also have a large effect on usage behavior, and the results are thus not generalizable to users of significantly differing mobile handsets. Another limitation of such monitoring software is that all non-standardized applications are seen as “black boxes” with no information on the usage “inside” the application. Commercial spyware specifically made for mobile handsets with some of the above functionalities has also emerged recently [7].

Mobile handset and PC monitoring methods have been combined in some rare cases to study the general behavioral patterns related to computer and handset usage of certain focused user populations [8].

2.3 Mobile Cellular Network Measurements

Mobile cellular network is a logical measurement point, as it is a point of convergence of mobile data traffic and covers all subscribers of the mobile operator.

Mobile operator’s charging and billing systems provide a great source of service usage data, as information on all chargeable events generated by the subscriber is registered in them. In principle, the time-stamped GSM/UMTS charging data records (CDRs) identify the mobile subscriber (by IMSI code), the used mobile terminal (by IMEI code), and the volume of packet data traffic to/from different external packet networks (by the used GGSN). The billing system uses aggregated CDR data, and also contains other data on subscribers from the customer register. Subscriptions vary in type (e.g. postpaid / prepaid, consumer / business, fixed-term / continuing) and in tariffs of different services (e.g. voice calls, SMSs, packet data transfer), for instance. Consumer subscriptions are registered to an identity number or social security number and business subscriptions are identified by a business ID, both of which only refer to the bill payer of the subscription and not to the actual end-user. Whether or not the CDR and subscriber data can be combined in detail depends very much on the implementation of the reporting functionalities of the operator’s information systems. Unrestricted access to the CDR databases or customer registers could also enable the use of sophisticated data mining techniques to uncover usage patterns (e.g. [21]).

Mobile network packet data traffic measurements are most easily conducted at the access points to external packet data networks (GGSN Gi interface), such as the Internet, capturing the traffic of all subscribers going via the access point. Capturing TCP/IP packet headers only and thus avoiding sensitive application level user data keeps the amount of measurement data manageable, and enables the analysis of generic traffic patterns. The volume of usage (bytes, flows) can be broken down by application protocol, destination host IP addresses (e.g. for web servers), and by day and time of usage. While individual usage sessions can be separated, they cannot be accounted to individuals as subscriber terminal IP addresses are typically allocated dynamically. Usage of mobile handsets can be distinguished from laptop usage. While browser based identification does necessitate application level header data, the distinct TCP fingerprints of different operating systems enable identification with just the IP and TCP headers. Similar measurements are often used in more technologically-oriented research while studying e.g. network or protocol performance in mobile or fixed networks.

In GSM/UMTS networks, packet data traffic header data could in fact be linked to the charging and billing data, at least in theory. This would necessitate keeping a continuous log of the IP addresses allocated to each subscriber terminal at the SGSN. Thus, a terminal identifier (TAC code) and/or subscriber identifier (IMSI) could be linked to traffic by the used IP address and time of usage. The subscriber identifier in turn could be linked to the data in the customer register. In principle, the network is also aware of the cell identity the mobile is using at all times. Combining location information at to traffic data at this level, however, would be a yet more complicated process. These rather laborious efforts have been done to some extent in [9].

The presented methods apply to GSM/UMTS mobile cellular networks. The extent to which similar measurements can be repeated in other mobile cellular networks or e.g. in WiMAX networks is not clear.

2.4 Server Measurements

Service usage and traffic patterns by mobile terminals can be studied at the server level at various points, including portals and individual web/wap sites/servers, search engines, proxy serves, as well as by with a service provider’s billing data. The scope of server level measurements is naturally limited to the users of the service in question. Background data on the registered users of a service might also be available.

Web portals are a place where usage and traffic converge. Usage of web portals and individual sites can be monitored in a similar manner. A typical method includes placing small pieces of code on all pages of a web site. Each time a page is loaded by a user, the code executes and sends data to another server. New and repeated visitors can be distinguished using browser cookies. At best, the method enables the identification of individual users and their detailed usage patterns. By identifying the used browser version, the use of a mobile device can be identified as well. Another way of obtaining web site usage data is to use server software (e.g. Apache web server) log files. Log file data is typically less detailed, but can cover several sites, as web hotel and hosting services often locate multiple web sites on the same server machine. [18], [2]

Analyst companies (e.g. TNS, Nielsen/NetRatings) providing web site usage analysis services can also combine the data measured on multiple individual web sites. Such data is typically published, if published at all, covering the service providers in one country regardless of the origin of the actual users (see [17]). No mobile-specific data has yet been published, though such data should already be available. The representativeness of these studies is somewhat questionable, as they only cover the clients of the analyst company who also allow the publication of the data of their own site. This means that all web sites are (by far) not included in the data, as analysis services are typically purchased only by well-established service providers. Thus, providers of services such as advertising and adult content, for instance, are typically not covered by the method. Other analytics software (e.g. Google Analytics) could possibly be used similarly to aggregate browsing data.

Search engine companies have another source of usage data at their disposal at the server level, as analysis on the most used search words provides information on service popularity. Mobile usage can be identified from accesses to mobile-adapted search sites as well as from the use of services specifically made for searching the mobile web (e.g. Google Mobile). Moreover, a mobile device accessing standard PC search site can also be identified, again by its browser type, while the searches of individual users can be distinguished with the help of browser cookies. As search companies also offer a range of other Internet services they are able to relate the background data on registered users to search behavior, regardless of which terminal is used as long as browser cookies identify the individual in question. The potential of such data was demonstrated in autumn 2006, when AOL released about 2.2 Gb of search logs to the general public with the seemingly good intention of providing the research community with hard search engine usage data. While the identities of individual people were not revealed by AOL, many of them could be easily deduced from the used search words. [19] In another less controversial case, search engine data has been specifically used to analyze mobile search patterns [3].

Traffic of multiple users converges also at proxy servers. Caching web proxies, for instance, can be used to measure web site popularity. The Opera Mini java browser for mobile devices serves as a specifically mobile related example of proxy based usage measurement. As Opera Mini fetches all requested content through an Opera proxy, detailed statistics on the browsing behavior of all Opera Mini users are available to Opera Software (see e.g. [13]).

Methods comparable to those used in mobile network specific measurements can also be used at server level. The service provider’s billing data gives indications on service usage related to monetary transactions, while traffic measurements with similar methods to identify mobile device usage can also be applied at servers.

2.5 Comparison of Alternative Data Sources

The alternative data collection methods have fundamental differences regarding the typical researcher, research scope, and the nature and granularity of collected data. A summary of the characteristics of each method is presented in table 1.

The selection of a usage data collection method depends very much on its availability, i.e. on the access of the researcher to the data. Surveys are far the most used method as they are available to anybody. Implementing a terminal monitoring panel is harder, as a functioning monitoring client for mobile devices is needed in addition to the capability of recruiting a representative panel. Only mobile operators are able to measure at the mobile network, as direct access to operator reporting systems and the network itself are both required. Server measurements can only be conducted by the service provider in question, or someone on their behalf.

The selected research method dictates the scope and size of the studied sample. While survey sample sizes vary a lot depending on the used survey method (doorstep vs. web surveys), panel studies typically have smaller sample sizes. Mobile network measurements cover a large number of people, as the studied sample can be up to the entire subscriber base of the operator. Server level measurements can have varying sample sizes, at maximum encompassing all users of the measured service.

The main difference between surveys and different measurements is that surveys provide subjective data on usage as perceived by the respondents, whereas measurements generally provide objective data. The accuracy and granularity of the data depend on the method. Survey respondents are likely able to provide information on aggregate usage of different services, whereas diary based panel and actual measurements are able to register even individual usage events and transactions.

The ability to obtain variables potentially explaining usage varies a lot by method. Survey studies can again include any background variable (e.g. gender, handset type, pricing scheme) the respondent is capable of providing. Generic data on the perceived time (e.g. evening) and context (e.g. at home) of usage can also be obtained, while diary based methods might achieve

Table 1 Summary of alternative mobile data usage data collection methods

Methods / Attributes	Surveys and panels	Terminal measurements	Mobile cellular network measurements		Servers measurements
			Charging & billing	**Packet data traffic**	
Researchers with access to data	Anybody (analysts, consulting firms. investment banks, academics…)	Those with a monitoring client and ability to recruit the sample	Mobile operators	Mobile operators	Service providers (mobile operators, 3rd party providers, search engines…)
Research scope and sample size	Survey respondents: $10^1 – 10^5$ Panel participants: $10^1 – 10^3$	Sample of panelists using certain handset OS and software platform: $10^1 – 10^3$	Operator's entire subscriber / terminal base: $10^5 – 10^7$	Operator's entire subscriber / terminal base: $10^5 – 10^7$	All users of the measured service(s): $10^2 – 10^7$
Nature and description of data	Subjective data on perceived aggregate service usage, diary method could sort out individual events	Accurate and objective data on handset application and feature usage	Accurate and objective data on mobile network transactions	Quite accurate and objective profile of mobile uplink / downlink packet data traffic	Objective data on service-specific usage, accuracy depending on the method
Explanatory / independent variables • User • Terminal device • Time • Location	Any background variables on the respondents Perceived time and context of usage Panels using a diary method enable more accuracy in time and location of usage	Many background variables on the panelists Handset model and access network used Time of usage Location of usage (cell ID)	Some background variables on subscription (type, tariff), no data on real end-users Terminal model Time of usage No location data	No data on individual subscribers or terminals, different terminal operating systems identifiable Time of usage No location data	All depends on the used method (identification of individual users, background data on registered users, separation of mobile usage, and time of usage possible) No location data
Usage / dependent variables • Usage volume • Usage frequency • Data granularity	Perceived amount and frequency of service usage	Volume, frequency, and duration of usage per panelist	Volume and frequency of chargeable service usage per terminal or subscriber type	Volume of usage (bytes, flows) per application protocol and traffic destination	Depends on the used method
			Additional measurements could link traffic data to charging and billing data		

higher level of accuracy in this respect. Terminal measurements typically begin with a survey study collecting relevant background data on the panelists. The monitoring software itself is aware of the handset model and features, the used access network, as well as time of each usage event. The location of usage might also be collected (cell ID).

The mobile network charging and billing based data can associate subscription information (type of subscription, tariff scheme) and terminal type to usage, though no data on the actual end-users is typically available. A timestamp of each transaction is also registered, as service pricing might depend on it. Sophisticated data mining techniques might include other variables. In mobile network packet data traffic measurement individual subscribers or terminals cannot be separated from each other. However, additional analysis methods enable the separation of different terminal operating systems, i.e. the separation of mobile handset usage from laptop originated traffic. The exact time of usage is also registered in packet data traffic measurements. While the mobile network is aware of the cell covering terminals with active packet data connections and the operator could actually relate the cell identities to geographical locations, actually combining this data to usage would be very laborious. For server level measurements, it again depends on the type of method used. Individual users might be separated and identified, and previous registration could also provide explanatory background variables for each user. Mobile handset originated usage can also be distinguished from PC usage in some cases, as should if the method is used for measuring mobile data usage. The time of service usage is also often obtainable. The user location cannot be known at the server, though the operator and country of the user could be derived from the user terminal IP address.

The usage volume and frequency of different services can be obtained at different levels of granularity. Surveys and panels provide data on the amount and frequency of service usage, as perceived by the respondent. Terminal measurements register the volume, frequency and duration of usage per application for each panelist. Charging and billing data can produce summary data on usage of different chargeable services, typically aggregated to subscriber or terminal type level. Packet data traffic measurements provide byte and flow counts on the volume of usage, accountable to used application protocols and external network traffic destinations (Internet hosts/servers). As stated before, by conducting additional measurements in the mobile network, traffic data and charging and billing data could be linked. The type of data obtainable on server level usage depends completely on the used measurement method.

The major limitation of any type of usage measurement is the fact that one can only measure what a user has done, not why the user has done something or what he/she actually intended to do. Thus, determining the motivation of usage or the real end-user need is hard based on measurement data only. Surveys are more flexible in this, as data on both perceived usage and motivation of usage can be collected, provided that the survey questions are formulated accordingly to obtain valid data. Terminal measurements facilitating the pop up question mechanism provide a promising new method to uncover the true reasons of usage, as the panelist can be asked triggered questions immediately following a certain type of usage. However, use of the pop up method must be very focused, as only a limited number of questions and only related to unsensitive type of usage can be asked to avoid irritating the panel participants. While mobile network measurements can't basically obtain any data on the motivation of usage, server level measurements have some means to understand it for instance by analyzing the user's site-specific browsing or search patterns.

As each method has its advantages and disadvantages, multiple methods are often used to gain further knowledge on usage. For instance, mobile operators can complement charging data based subscriber segmentation by conducting a survey study to better understand the motivation and usage behavior of each segment. This is also recommendable from the theoretical point of view, as method triangulation can improve both internal and external validity of the data [15].

3 Effect of Mobile Multi-Access to Usage and Traffic Measurements

The use of multiple alternative wireless access methods will diverge traffic to multiple networks. While almost all mobile handset users and many laptop users are currently (2006) still using mobile cellular networks for accessing the Internet, traffic will increasingly leak to alternative access networks in the near future. This will have a profound effect on the methods to measure mobile data usage and traffic.

Survey and panel studies should work quite similarly in collecting data on usage behavior, as perceived by the users. However, if terminals are capable of changing access networks automatically, the users might not be aware of such changes and, thus, of the network they are using at any given time. Relating usage behavior to the performance or other characteristics of a particular network will therefore be hard.

As the same terminal is still used irrespective of the access network used, the mobile terminal is still the point where all usage of an individual user converges. Moreover, if the terminal monitoring software is aware of the changes in network usage, behavior can also be associated with the used network, while the motivation of usage and user experience can also be measured by triggering pop up questions based on the network in use. Thus, the terminal is still a promising place for conducting usage and traffic measurements.

As mobile cellular networks will only represent one of the many alternative wireless access networks, usage and traffic will no longer be holistically measurable in them. While the spreading WLAN hotspots might rapidly take a large share of the total mobile data traffic volume, new HSPA techniques will still be in the scope of the presented mobile cellular network measurements.

Most server level measurements should function in a similar manner regardless of the used access technology. As mobile handsets are converging with PCs in functionality and will be capable of using all the services previously used exclusively by PCs instead of the mobile-specific/adapted versions, distinguishing the two might become more difficult. This also applies to some handset applications (e.g. Opera Mini browser) whose architecture has enabled server level measurements. Some of the methods in identifying mobile clients are still applicable, but the used access method might also be of less interest to service providers in the future when adapting the service to the lesser capabilities of the mobile terminals is no longer necessary.

4 Conclusions

A range of alternative methods for collecting data on mobile data usage and traffic have been presented in this paper. Each of the methods has its advantages and disadvantages, and the applicability of a particular method depends on the research objectives as none of the presented methods is suitable for all purposes. Thus, multiple methods are often used. In general, surveys and terminal measurements provide very detailed sample based data, whereas mobile network data is less granular but is based on the entire subscriber population of an operator. Server level measurements are a compromise between the above, as detailed usage patterns can be uncovered from a fairly focused user population.

In the future of heterogeneous multi-access networks, terminals seems to be the most promising place to measure usage and traffic, while mobile cellular networks are likely to lose most as traffic will partly diverge to other wireless access networks. In addition, the mechanism of pop up questioning in terminal measurements presents a potential research approach.

The usage of money might also provide a centralized view for understanding mobile service usage. While accesses to bank, auction and e-commerce web sites, for instance, already give some indications, authentication in the electronic and mobile environment might be another convergence point of money usage. Although universal authentication is still a thing of the future, authentication is already performed by various actors, including banks, credit card companies, mobile operators, as well as purely Internet based actors such as PayPal. Complementing the time stamp and "location stamp" with a "price stamp" presents an interesting future research prospect for understanding mobile user behavior.

References

[1] Aaker David A., Kumar V., Day George S. (2004). Marketing Research, 8th ed., John Wiley & Sons Inc.

[2] Bluemetrix Inc web site [online]. Bluemetrix – Business intelligence at your fingertips, updated 2006 [accessed September 14, 2006]. Available in www-format: <URL: http://www.bluemetrix.com/engsite/webanalysis/methodology.htm>

[3] Kamvar M., Baluja S. (2006). A Large Scale Study of Wireless Search Behavior: Google Mobile Search, presented at CHI 2006, April 22-27, 2006, Montréal, Québec, Canada.

[4] Eagle N. (2005). Machine Perception and Learning of Complex Social Systems. Doctoral dissertation, Program in Media Arts and Sciences, Massachusetts Institute of Technology, USA.

[5] Elektroniikan Tukkukauppiaat ry web site [online]. Elektroniikan Tukkukauppiaat RY, updated 2006 [accessed September 8, 2006]. Available in www-format: <URL: http://www.etkry.com/>

[6] Finnpanel Oy web site [online]. Finnpanel Oy, updated 2006 [accessed September 14, 2006] Available in www-format: <URL: http://www.finnpanel.fi/>

[7] Vervata Co Ltd web site [online]. FlexiSpy – Spy Software for mobile / cell phones, updated 2006 [accessed September 15, 2006]. Available in www-format: <URL: http://www.flexispy.com/>

[8] Heimo Consulting web site [online]. Heimo Tribe, updated January 2005 [accessed October 5, 2005]. Available in www-format: <URL: http://www.heimotribe.com>

[9] Kalden R. (2004). Mobile internet traffic measurement and modeling based on data from commercial GPRS networks. Doctoral dissertation, University of Twente, The Netherlands.

[10] Kim, J. (2001). Analyzing mobile Internet users: Results from a monitoring study, an experiment, and a survey study. In CHI 2001 Workshop, Mobile Applications: Understanding Users, Adoption & Design.

[11] Kivi A. (2006). Mobile Internet Usage Measurements - Case Finland. Master's Thesis Series. Networking Laboratory. Department of Electrical and Telecommunications Engineering. Helsinki University of Technology, Espoo, Finland, April 2006.

[12] Kotek web site [online]. KOTEK – Kodintekniikka-alan tiedotusfoorumi, updated 2006 [accessed September 8, 2006]. Available in www-format: <URL: http://www.kotek.fi>

[13] Opera Software ASA press release August 8, 2006. Mobile Browsing Bonanza: One billion Web pages viewed with Opera Mini.

[14] Raento, M., Oulasvirta, A., Petit, R., Toivonen, H. ContextPhone – A Prototyping Platform for Context-Aware Mobile Applications. IEEE Pervasive Computing, Vol. 4, No. 2 (April-June 2005), pp. 51-59.

[15] Scandura T., Willians E. (2000). Research Methodology in Management: Current Practices, Trends, and Implications for Future Research. Academy of Management Journal, Vol. 43, No. 6 (Dec. 2000), pp. 1248-1264.

[16] Suomen numerot NUMPAC Oy web site [online]. Suomen numerot NUMPAC Oy, updated 2006 [accessed September 10, 2006]. Available in www-format: <URL: http://www.numpac.fi/>

[17] TNS Gallup web site [online]. TNS Metrix, updated 2006 [accessed April 4, 2006]. Available in www-format: <URL: http://www.gallupweb.com/tnsmetrix.htm>

[18] Tähtinen M. (2006). Tunne web-käyttäjäsi, Tietokone, No. 9, 2006, pp. 55-57.

[19] USATODAY.com [online]. AOL search data release reveals a great deal, updated August 6, 2006 [accessed September 10, 2006]. Available in www-format: <URL: http://usatoday.com/tech/columnist/andrewkantor/2006-08-17-aol-data_x.htm>

[20] Verkasalo, H & Hämmäinen, H. (2006). Handset-Based Monitoring of Mobile Subscribers. Presented at Mobility Roundtable, 1-2 June, 2006, Helsinki, Finland.

[21] Wei, C-P & Chiu I-T (2002). Turning telecommunications call details to churn prediction: a data mining approach, Expert Systems with Applications, Vol. 23 (2002), pp. 103-112.

X. Emerging Trends in the Mobile VoIP Business

HANNU VERKASALO
hannu.verkasalo(a)tkk.fi
Helsinki University of Technology
Networking Laboratory
P.O. Box 3000 FIN-02015, FINLAND

Abstract

This research paper has analyzed the mobile VoIP technology from the business point of view, focusing mostly on the consumer sector. Through the identification of relevant technologies in implementing mobile VoIP services the paper has constructed a classification of major players in the business. First, there are incumbent operators, who might leverage on the combination of cellular and emerging radio technologies in providing mobile VoIP services. Secondly, there are challenger operators emerging, who have a core strategy in mobile VoIP. If they provide standardized interfaces and service-level products without owning any radio access technologies, they are called virtual mobile VoIP operators. There are also Internet companies which might strongly leverage on the modular Internet-like evolution path. These actors might distribute proprietary light-weight clients (e.g. Skype) and approach the mobile VoIP business from the disruptive Internet perspective. It is actually possible that voice connectivity is a simple Internet application in the future, if this path gains momentum. By discussing the technological advancements of the near future and likely evolution of business approaches the paper suggests that in the end of the day it might be a two-way evolution path which emerges on the market. The first path leads to a very vertically integrated operator-driven ecosystem, in which incumbent operators can probably leverage both on their existing cellular infrastructure and on new emerging radio access technologies. Platforms and standards such as UMA and IMS probably drive this path. The alternative evolution path leads to an Internet-like model, in which the ecosystem is layered and highly modular. Bit-pipe operators take care of traffic, whereas on the higher level actors with focused strategies implement mobile VoIP services. In the case of failure of key VoIP standards the major Internet companies with light-weight proprietary clients (e.g. Skype, Google) who prosper, or in the case of wide-scale emergence of SIP-capable WLAN handsets and establishment of open WLAN networks it is virtual mobile VoIP operators who might be better off in future of the mobile VoIP industry.

1 Introduction

Voice has been the key service of the mobile industry. It was voice for which the first analog and digital cellular networks and handsets were developed and built. Though we have seen quite an evolution towards more and more complex mobile services, voice is still there as the most important service category. According to Vesa [1], the non-voice revenue of operators throughout the world is still significantly smaller than voice revenue. No doubt, it is very important to consider the evolution of mobile voice services.

Voice has traditionally built on circuit-switched technologies. As we are now moving towards packet switched networks, in which all kinds of streams and information are easily combined into packets, we have to reconsider the justification for circuit-switched services. It is very expensive to have a separate circuit-switched network to implement voice services, as the integration of all information on a packet-switched network is much more cost-effective and scalable. In addition to the lower investment expenses we see major advantages also in further development of voice services towards e.g. video calls and instant messaging. In the fixed Internet we have already seen quite a number of voice-oriented services, in which voice is essentially coded into streams of packets. These technologies and services are often referred to as voice over IP (VoIP) [15].

In this research paper the focus is on mobile VoIP. Mobile VoIP is here defined as voice-oriented services, in which voice is transmitted over IP networks, and the service is used with a mobile handset. In this paper the foremost focus is on understanding mobile handsets as small smartphone kind of devices, which have at least cellular capability and provide an operating system capable of running add-on applications.

It is important to understand the matrix of technologies which are needed in implementing different kinds of mobile VoIP services. However, the business implications of mobile VoIP might be even more interesting. There are already quite a number of actors somehow running mobile VoIP services, not to talk about the diversity of players currently testing, planning or considering a movement to the mobile VoIP business. In this paper it is argued that the type of technology chosen has major implications on the type of approach to the mobile VoIP business, and different kinds of actors are currently emerging in a certain order because of technical solutions chosen. Through this techno-economical approach the paper then suggests a certain categorization for the business actors taking part in the game, concluding with a timeline kind of analysis of the near future of mobile VoIP.

2 Mobile VoIP technologies

Lots of research is currently pursued in analyzing and categorizing emerging mobile services [2] [3]. The focus is often in disruptive applications. Disruptive applications are generally considered as "…new services that create significant changes in a business model" [4]. Disruptive applications shake dominant business models by introducing new application innovations and at the same time perhaps making older applications obsolete. [21] It is important to understand that mobile VoIP is essentially not understood as a disruptive service in this research paper. Mobile VoIP is not that new a service from the end-customer point of view. Mobile voice connectivity has been there for years, and that is what the customer is seeing when he uses VoIP applications. Although from the technical point of view the implementation is completely different from traditional circuit-switched voice communication services, the end-customer is merely interested in the kind of value-added the new service provides. Of course in the end of day it is possible to better extend basic voice services in IP networks (integrating e.g. video, instant messaging, file sharing and security layers to the basic service), but the core value-added is voice. Therefore we should not call mobile VoIP as a disruptive application, but instead the numerous disruptive technologies around the core service generate the disruptive potential. [4]

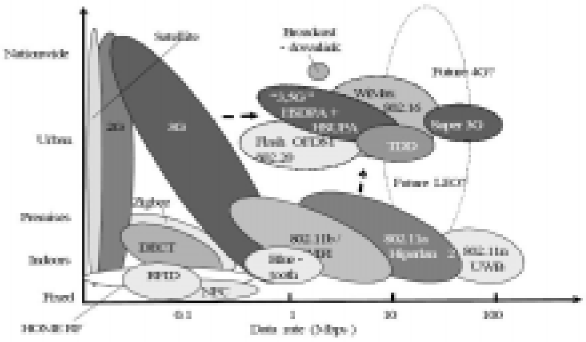

Figure 1 - Emerging radio technologies (adopted from [5])

From the incumbent cellular network operator point of view the greatest threat (i.e. disruptive potential) in the near future is centered on emerging/challenger radio technologies (see Figure 1). In Europe a lot of money and focus has been pushed on the evolution of cellular technologies (1G, 2G, 2.5G, 2.75G, 3G etc.) [5]. In the future we see a continuation of these technologies towards 3.5G, including technologies such as HSDPA and HSUPA. In the UMTS framework we also have to consider the UMTS TDD technology, being an alternative to the WCDMA interface. However, there exist many alternative radio technologies, too. WiMAX is currently considered as a wireless broadband technology for fixed locations. In the future WiMAX will be developed towards more mobile use cases, which will position it as a serious substitute to cellular technologies. FLASH-OFDM is also worth consideration. In addition, with WiFi we refer to a portfolio of standards such as 802.11g and 802.11b. In Europe we generally talk about WLAN technologies. They are already widely deployed and are therefore worth more discussion.

WiFi radio access technologies are considered currently as the most powerful threat to cellular, thanks to a wide deployment of various kinds of WiFi hotspots in public places, enterprise-driven WiFi coverage, municipal WLAN networks etc. Taking WiFi as a case example, it is good to analyze other (middle-layer) technologies which are needed in making VoIP working fluently. In cellular networks we take it for granted that e.g. hand-overs work easily. In WiFi hotspots this is not that easy, and many alternatives are currently considered in implementing seamless hand-overs from a "WiFi cell" to another. Other issues are related to possible roaming arrangements, QoS issues, cellular-to-WiFi-handovers etc. From the network management point of view one also needs various kinds of management tools for WiFi networks. It is quite another thing to get a multiple-WiFi-cell-network to work with handovers etc., than to operate a single WiFi base station mostly meant for flexible but fixed use cases (e.g. WLAN home networks). Currently many of these technologies are under standardization.

By taking a more holistic approach, there any many standards or frameworks on a higher level which basically discuss the evolution of mobile networking from a wider perspective. The concept of 4G is still a bit hasty, but the general idea in the movement towards 4G is the application of various radio access technologies which all together form the ground for IP-based networking. UMA (also known as GAN) deals with largely similar kind of issues, though it is currently being specified whereas 4G is a somewhat future concept. UMA is adopted by 3GPP, and it is considered as a major approach in bringing local and wide area networks closer to each other, solving issues such as roaming and handovers from cellular to e.g. WiFi. It is also developed in parallel with e.g. the IMS (IP multimedia subsystem) platform, which is considered very important in providing IP based services to mobile subscribers in the future. The main idea in IMS is that all the services are provided through a managed IMS platform, in which not only the network operator but also 3rd party content providers can create value to the end-customer. Mobile VoIP is definitely one of the key services thought to benefit from IMS.

Table 1 - Analysis of the concepts/technologies

Layer of interest	Network architectures, switches, mobile subsystems	Radio access technologies	Roaming, handovers, authentication, security (middle layers)	Application layer, software clients	Handset, terminal, network edge
Technologies / Concepts	•UMA •4G •Mesh networking •VoIP PBX •[illegible] •Longboard •SCCAN •IMS •FMC	•GSM •CDMA •CDMA2000 •WCDMA •HSDPA •HSUPA •Bluetooth •WiMax •802.11a •802.11g •802.11b •EVDO rev A	•SIP •uPnP •QoS (IEEE 802.11e) •WPA •WPA2 •WEP	•Call management •Answering machines •Instant messaging •Video calls •CLI	•Battery life •Convergence of radio access technologies •Open software platforms •Processing power •Multimedia capabilities
Companies	•Trapeze Networks •Broadcom •Alcatel •[illegible] Telecom •Cingular •Ericsson •Nokia •Nortel etc.	•Ericsson •Nokia-Siemens •Alcatel •Intel •Nortel etc.	•Kineto Wireless •BridgePort Networks •Longboard Pandora Networks •Intel •Motorola •WLAN •Cisco etc.	•Skype •Vonage •Buzzcall, Jajah •MSN •Yahoo •Google etc.	•Nokia •Motorola •SonyEricsson •Samsung •Windows mobile terminals etc.

Many of the technologies mentioned in this chapter are some sort of standards. However, there exists quite a wide portfolio of technologies and solutions which are not standardized at all. These are referred to as "proprietary" technologies. For example Skype, the widely speculated VoIP service in the fixed Internet, is based on a proprietary technology. For a reverse engineered description of the technology, see [17]. Usually proprietary solutions are considered as a bit hostile, particularly from the open-source kind of perspective. Proprietary solutions typically do not drive e.g. interoperability issues.

The major conclusions of this research paper are related to the possible paths of mobile business evolution, the first of which is based on the dominance of huge cellular operators and standardized interfaces, and another of which can be possibly proprietary based Internet-like service evolution. The technical background is essential in understanding the suggested framework. The relevant concepts and technologies are mentioned in Table 1.

3 Emerging actors and business logic

Now as the technology issues are discussed, we can move to more business-oriented analysis. By taking a holistic look at the mobile VoIP business, we can identify following types of actors in the game (see Figure 2):

- Proprietary 3rd party VoIP service providers
- Virtual VoIP operators
- Incumbent operators

In the categorization above we focused on companies which could actually provide/manage VoIP services, i.e. provide voice connectivity over IP networks to the end-customer/enterprise. There exist a wide number of other actors in the larger value network, too. These include e.g. software/hardware manufacturers, suppliers, consulting companies and ODE type of product developer companies. Some of the distinctions that are emphasized in the categorization of this paper have already been disputed earlier. For example, in [19] the discussion centers on the battle of MNOs against ISPs (which are in this paper referred in many cases as 3rd party client providers because of their high location on the modular Internet business design). On the other hand, in [20] it is described how fixed network operators can take MVNO kind of positions in launching mobile VoIP services. Certainly the concepts have been there also earlier, and they reflect the current typology of actors playing in the mobile VoIP field. However, it might be that in the future we need to reconsider our categorizations based on the evolution of the market. Now it is too early to say what is going to happen.

Incumbent operators - now talking predominantly on incumbent cellular network operators - are currently taking a bit defensive or explorative approach. Sure, major players in the industry are considering the threat or opportunity of mobile VoIP. It is inevitable that voice communication moves to the packet-switched domain. However, cellular operators get their most important and biggest chunk of revenue from mobile circuit-switched voice services, so it would be stupid all of a sudden to leave everything behind. On the other hand, they are also waiting as the technologies evolve. If they are to fluently extend their cellular offerings, people expect them to provide solutions which support seamless roaming and integrate well with all the other services. Incumbent operators have lots of stakes in complementing efficiently the current value offerings together with driving their brand value. Incumbent operators are currently observing the whole technology landscape, putting a lot of trial and development e.g. on the IMS platform. They are also considering how to best combine cellular voice and mobile VoIP, in which UMA player an important role. If the cellular operator also owns e.g. DSL kind of infrastructure and home connections, they might have the incentive to bundle mobile subscription with home WLAN base stations, which then switch calls at home. It also remains to be seen how the possible regulatory agents deal with these kinds of approaches in the future.

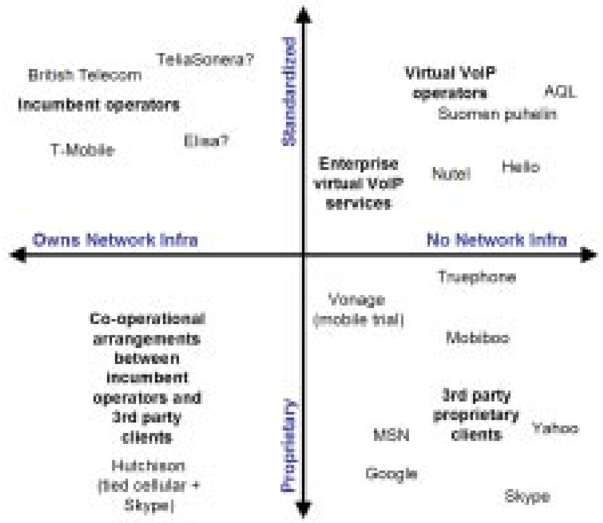

Figure 2 - Classification of actors

Virtual VoIP operators resemble the virtual operators we have already seen in the mobile cellular business, i.e. MVNOs (see e.g. [18]). Virtual operators provide a service, possibly implementing some billing and charging mechanisms, but do not own any network infrastructure. [14] In the VoIP business this kind of actors fit into the value network even better. Currently in many countries it is not the cellular network operators (who might have the possibility to block VoIP kind of traffic) who own the hotspots. On the contrary, there are many WLAN hotspots provided by a municipal actor, there are open networks in which individual households provide WLAN access points, restaurants provide a customer with an incentive to come eat and by providing inhouse WLAN coverage also to access the Internet. If this is the case and very open network access networks emerge and prosper in the future, there is a lot of potential for virtual VoIP operators. They could also partner with companies who drive Internet-like service architectures and in which there is practically no vertical integration. In this Internet model there are separate companies serving as bit-pipe kind of operators, whereas there is room for separate companies providing services, for example mobile voice connectivity through IP networks (i.e. VoIP).

There might emerge many kinds of virtual VoIP operators. Some of them might target the value-added to the enterprise sector, whereas some could focus on consumer customers. Some of them might partner actively with other companies, some might just rely on the fact that the competitive Internet model emerges in which a variety of radio access alternatives are found at least in urban areas. In any case, virtual mobile VoIP operators are likely to have extremely focused strategies on the highest OSI layer. Mobile virtual VoIP operators are likely to build their services on standardized technologies if they are to emerge from scratch and build on other domains, e.g. the base of SIP-capable WLAN handsets.

The third main group of actors in the game is not far from mobile virtual VoIP operators. We call these actors as 3rd party proprietary client providers. Their role can be understood as a bit hostile, as they do not leverage on standards that much. They take advantage of the potential Internet evolution path by only focusing on the highest layer, where they interact (and effectively own) the customer. This can also be understood as a “rupture” scenario [7], as the 3rd party proprietary client providers have quite different business models than the currently well-known incumbent and virtual operators. Their business is based on attracting as big as possible a user domain. We see this kind of actors in the instant messaging world today, as Internet giants such as Microsoft, Yahoo and Google are all trying to maximize the network externalities in their own particular user network. On the VoIP side it is Skype [13], naturally, which best fits in this category. However, the differences of instant messaging and mere VoIP services on the client level are gradually disappearing, as many of the clients already provide both functionalities, not to talk about all the other add-on services such as file sharing or video calls. Business-wise these 3rd party proprietary client providers make money by bundling other services or through advertisement revenue. By keeping clients proprietary they make sure that only they can manage their own customer domain. If there emerges only massive Internet companies who own the customers and provide the core voice communication services, major challenges are of course related to interoperability issues between these actors. Some interoperability/roaming kind of arrangements should be done without doubt, not only to other Internet companies but also older PSTN / cellular networks, which certainly remain complementary in non-urban areas for long. These 3rd party client providers do not work on massive vertical integration projects and/or they do not have to wait for standardization to freeze down, which might takes years. The only thing they are depending on is the very tightly evolved Internet mobile VoIP model, in which all the layers are distinctively separate and competitive.

4 Evolution of the mobile VoIP business in the future

Based on the discussed categorization of VoIP service actors and their respective characteristics, we can draw three SWOT maps reflecting their possibilities in the industry [16]. Maps are illustrated in Figure 3.

Currently it seems that the most light-weight implementations of mobile VoIP are emerging. We are now talking about Skype kind of proprietary solutions. Also virtual VoIP operators, which are using simply SIP-based services through emerging Nokia E-Series handsets, for example, are appearing on the market. These kind of actors emerge quicker, as they are usually quite small and have thus advantages in terms of time-to-market. Furthermore, they do not need to consider issues such as integration to cellular networks (e.g. UMA approach). On the other hand, incumbent cellular/DSL operators are still considering their best movements. They need the interoperability/handover standards, and they also reconsider their business value networks in leveraging on mobile VoIP. Most importantly, they also generate money from the circuit-switched voice, so why hurry? As virtual VoIP operators and 3rd party client providers leverage on the innovative ramp-up, incumbent operators prepare for a defensive mobile VoIP approach more carefully, remembering that they have lots more to risk.

Then, relying on the scenario modeling which tries to identify extreme industry evolution paths, a two-path map is drawn for the future evolution of the VoIP service industry (see Figure 4 for the illustration).

Currently we are moving along the time line towards an expected cross-road. All the different actors emerge, the potential technologies are explored, while the standards and other platforms at the same time evolve and are eventually frozen. Then we face the so-called tipping phase. The business logic / ecosystem will converge to either of the two possible directions.

VIRTUAL VoIP OPERATORS

Strengths	Weaknesses
- Fast ramp-up based on (open/closed) IP networks - Focus on VoIP services	- Lack of vertical integration - Small size and negotiation power
Opportunities	**Threats**
- Innovative business logic - Leveraging on the Internet model and established standards such as SIP and available hardware (e.g. Nokia E-series) - Acquisition by bigger operators?	- Emergence of a strongly operator-centric model - Bigger operators and hostile strategies - Large Internet companies and 3rd party light-weight VoIP clients

INCUMBENT OPERATORS

Strengths	Weaknesses
- Ownership of network infrastructure - Experience in the roaming etc. interoperability arrangements	- Time lag due to standardization and evolution of IMS kind of platforms - Size, slowness
Opportunities	**Threats**
- Bundling of cellular and fixed - Seamless interoperability and combination of cellular and WLAN	- Emergence of an Internet model - Challenger actors (virtual operators and 3rd party client providers)

3RD PARTY PROPRIETARY CLIENTS

Strengths	Weaknesses
- Fast ramp-up - Proprietary solution - Existing user domain in the Internet - Levers on the Internet model	- No network infra - Interoperability issues to other Internet services and PSTN/cellular networks - No vertical integration
Opportunities	**Threats**
- Integration of various other value-added services on the application layer - Innovative potential / challenger benefits	- Emergence of a vertically integrated business model - Value-destroying competition

Figure 3 - SWOT analysis of the main actors

The first path resembles the current mobile cellular business, which is much operator-driven. On this path UMA and IMS play a big role, as incumbent operators need them quite a lot if they are to successfully integrate cellular with alternative radio access technologies and to coherently support the emergence of IP-based services. This path is called a vertically oriented one as operators retain a lot of control, and Internet-type of openness and modularity is absent.

The other possible path leads towards an Internet-like scenario, in which we have strictly layered industry structure. Others provide connectivity, whereas others provide services (e.g. mobile VoIP). On this path operators as we know them today remain as mere bit-pipes, and mobile VoIP becomes a true Internet service. In fact, on this path we might see a major transformation in which voice connectivity all in all moves to a true Internet era!

On this other path we see possibly a strictly dominant category of actors, or alternatively we see both 3rd party proprietary client providers and virtual VoIP operators. The key question remains: What is the role of standards vs. proprietary solutions? It is possible that major virtual service providers emerge who leverage on the established standards implemented in e.g. newer handsets (e.g. Nokia E-Series), or then we see the rise of huge Internet companies like Google, MSN or possibly Skype, who leverage on the user domain and proprietary solutions.

It is impossible to say which is the predominant business logic in the future, the strongly modular Internet-like business ecosystem or more vertically oriented cellular-like operator-driven business ecosystem. It remains to be seen for sure, however, during the next 2-6 years.

5 Conclusion

This research paper has defined the mobile VoIP service and speculated it as a potential disruptive service, not from the service point of view but because of its close linkage to emerging alternative radio technologies which provide IP-access also through other than cellular networks. In this movement towards a holistic network access perspective we see the handset in a central role. Dual-mode handsets (e.g. Nokia E-Series) provide an interesting platform for emerging VoIP services. However, the key uncertainty of the mobile VoIP business relates to the different kinds of implementations of mobile VoIP services.

The key technologies and standards under development were discussed in this paper. Leveraging on this technical assessment the different actors were also introduced who might serve as mobile VoIP services providers. The key idea was that different actors leverage on different kinds of technologies and further on different kinds of business approaches. The tipping phase of the whole industry reveals that towards which of the two main evolution paths the mobile VoIP industry develops. The first main path was an Internet-like scenario with a strongly modular and layered structure. 3rd party proprietary client providers and mobile virtual VoIP operators might benefit from this ecosystem design. The other path leads to a more operator-driven and managed ecosystem, which is not that far from today's cellular business. Vertical bundling and levers on the existing network infrastructure might drive the dominance of this model. While it is too early to say which path is winning, many important parameters exist in addition to business logic and technologies which certainly affect the outcomes. One of these important factors is regulation. Mixed strategies might also emerge. For example Hutchison and Skype have recently launched a trial service together [12].

While this theoretical paper has speculated on the future evolution paths of mobile VoIP, it remains very interesting to follow the scene also in practice. The development of measurement methods in order to follow the market, and analyze the emergence/adoption of mobile VoIP services, remains very important [8] [9].

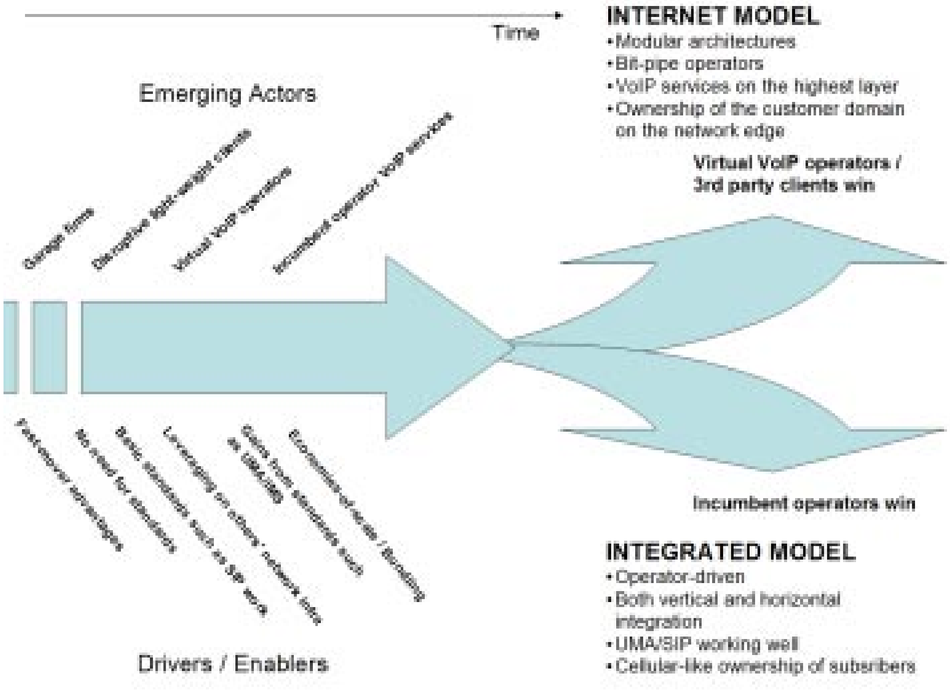

Figure 4 - The evolution path of the mobile VoIP business

References

[1] Vesa, J.: Mobile Services in the Networked Economy. 2005. IRM Press, Hershey, PA, USA.

[2] Verkasalo, H. & Kivi, A. & Smura, T.: Mapping Mobile Applications to End-User Needs. 2006. Working Paper, Networking Laboratory, Helsinki University of Technology.

[3] Verkasalo, H. & Hämmäinen, H.: Handset-Based Monitoring of Mobile Subscribers. 2006. Presented at Mobility Roundtable, 1-2 June, 2006, Helsinki, Finland.

[4] Barsi, T.: Disruptive technology vs. disruptive applications. Telephony Online. 2002. http://telephonyonline.com/news/telecom_disruptive_technology_vs/index.html. Referred 20.9.2006

[5] Lindmark, S. & Ballon, P. & Blackman, C. & Bohlin, E. & Forge, S. & Wehn de Montalv, U.: Alternative Wireless Technologies – Trends, Drivers and European Policy Implication. 2006. ENCIP. i2010: Comments and Contributions. EuroCPR 2006: Selected Papers (edited by Pascal Verhoest), September 2006.

[6] On World: 2005. Mobile VoIP – Competitive Landscape. Executive Summary.

[7] White, P.: Online services and 'transactional space'. Emerging strategies for power and control in the new media. 1997. *Telecommunications Policy, Volume 21, Issue 6, pages 565-573*.

[8] Verkasalo, H.: Handset-Based Monitoring of Mobile Customer Behavior. 2005. Master's Thesis Series. Networking Laboratory. Department of Electrical and Telecommunications Engineering. Helsinki University of Technology, Espoo, Finland, September 2005.

[9] Kivi, A.: Mobile Internet usage measurements - Case Finland. 2006. Master's Thesis, Helsinki University of Technology.

[10] ZTE: IP Multimedia Subsystems – Updating the Telecoms Outlook. 2006. *Telecommunications International; June 2006; 40; 6.*

[11] Stanislaw, S.: Rest assured on IMS? 2005. *Telecommunications International; November 2005; 39; 11*

[12] Leyden, J.: Skype goes 3G. 2006. The Register. http://www.theregister.co.uk/2006/02/15/skype_3/. Referred 27.9.2006.

[13] Red Herring: Skype plans a mobile version. 2006. http://www.redherring.com/Article.aspx?a=17855&hed=Skype+Plans+a+Mobile+Version&sector=Industries&subsector=Communications. Referred 27.9.2006.

[14] Red Herring: VoIP startups go mobile. 2006. http://www.redherring.com/Article.aspx?a=17732&hed=VoIP+Startups+Go+Mobile. Referred 27.9.2006.

[15] VoIP Tutorial: Does the Future Belong to Mobile VoIP? 2006. http://www.voip-revolution-info-site.com/Mobile_VoIP.html. Referred 27.9.2006.

[16] Piercy, N. & Giles, W.: Making SWOT Analysis Work. 1989. *Marketing Intelligence & Planning Vol 7, Issue 5, June 1989.*

[17] Baset, SA. & Schulzrinne, H.: An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. 2006. In Proceedings of the INFOCOM '06 (Barcelona, Spain, Apr. 2006).

[18] Smura, T. & Kiiski, A. & Hämmäinen, H.: Techno-Economic Analysis of Mobile Virtual Network Operators: Strategies, Investments, and Revenues. 2006. 5th Conference on Telecommunication Techno-Economics, 8-9 June 2006, Athens, Greece.
[19] Mobile Communications International: IM in the Spotlight. April 1, 2006. http://www.oz.com/news/2006/IM%20in%20the%20Spotlight.pdf#search=%223rd%20party%20clients%20versus%20incumbent%20operators%22. Referred 22.9.2006.
[20] Nokia: Mobile VoIP: IP Convergence Goes Mobile. Press Backgrounder, Nokia Corporation 2005.
[21] Christensen, CM.: The Innovator's Dilemma - When New Technologies Cause Great Firms to Fail. Harvard Business School Press 1997.

XI. Use of Ad Hoc Networks for Wireless Internet Access

JOUNI MÄENPÄÄ
Helsinki University of Technology
jpmaenpa(a)cc.hut.fi

Abstract

An ad hoc network consists of a collection of mobile wireless nodes that dynamically create a network among themselves without using any infrastructure or administrative support. Therefore, ad hoc networks have the potential to provide a free, non-operator controlled means of mobile communication. On the other hand, they also provide a low cost alternative to extend the reach of current wireless access networks. In this paper, the use of ad hoc networks for wireless Internet access is discussed. An overview of some proposed technical architectures and their challenges is provided. Also business models enabling the use of ad hoc networks and the challenges associated with the models are considered.

1 Introduction

An ad hoc network is a mobile or stationary collection of communication devices (nodes) that dynamically create a network among themselves. The nodes have no fixed infrastructure available, and have no pre-determined organization of available links [19]. Not all nodes in an ad hoc network can directly communicate with each other, meaning that nodes are required to relay packets on behalf of other nodes in order to ensure data delivery across the network. What makes ad hoc networking challenging is that rapid changes in network topology, connectivity and link characteristics are introduced due to node mobility and power control practices.

It has been argued that as applications grow hungrier for bandwidth, wireless architectures are likely to move away from cellular to ad hoc [19]. This is because more capacity requires higher communications bandwidth and thus better spatial spectral reuse. Further, higher bandwidth is found at higher frequencies where communication ranges are shorter. Finally, mobile devices need to minimize power consumption. All these factors support a shift from a single long wireless link to a mesh of short links used in ad hoc networks.

Ad hoc networks can play a disruptive role in the world of wireless communications [8]. First of all, ad hoc networks challenge the traditional ideas of wireless infrastructure and its ownership and control. Secondly, ad hoc networks have the potential to disrupt the existing approach to how wireless networks are used and how wireless applications are designed. Thirdly, ad hoc networks challenge the status quo because they have the potential to provide a free, non-cellular based, non-operator controlled means of mobile communication. Fourthly, ad hoc networks can have an impact on social order and behavior; as the infrastructure is less dependent on the operators, it becomes easier for groups of people to form wireless communities. Finally, ad hoc networks can also be physically disruptive in the wireless spectrum, since they may cause interference with each other and with e.g. Wireless Local Area Networks (WLANs) or Bluetooth networks. Ad hoc networks force a different view on network infrastructure, ownership and resource control. Ad hoc networks also remove the operator linkage and require the creation of alternative business models and applications.

Ad hoc networking is an increasingly important topic and has been regarded as one of the key features in beyond third generation (3G) systems [4]. In these heterogeneous and integrated environments, ad hoc networking is considered to be an important solution to extend the radio coverage of wireless systems and to extend the reach of multimedia Internet services to wireless environments.

The focus of this paper is on the question of how ad hoc networks can be used for wireless Internet access and what impact this has on business models. In Section 2, first the integration of the Internet and mobile ad hoc networks (MANETs), and then personal networking are described. Section 3 presents four business models regarding the use of ad hoc networks for wireless Internet access. In Section 4, some technical and business model related challenges are considered. Section 5 presents a brief overview of how ad hoc networks are used currently. Finally, conclusions are drawn in Section 6.

2 Internet Access through Ad Hoc Networks

In this chapter, technologies and architectures enabling the use of ad hoc networks for wireless Internet access are described.

2.1 Integration of Internet and Ad Hoc Networks

The goal of the integration of the Internet and mobile ad hoc networks (MANETs) is to provide mobile nodes in a MANET with wireless Internet access although they are multiple wireless hops away from the edge of the Internet. The problem of integrating MANETs and the

Internet has been studied e.g. in [2], [5], [6] and [24]. Central to all of these approaches is the use of mobile gateways (MGs), which sit between the MANET and the Internet. Another key feature is the use of Mobile Internet Protocol (IP) [21] for mobility management. The MG has two interfaces: the first interface is connected to the Internet so that normal IP routing mechanisms can be used when packets come in and out of the MANET, while the interface connected to the MANET uses some ad hoc routing protocol to route packets within the MANET. The gateway provides an illusion to the outside world that the MANET is simply a normal IP subnet. The gateways are multihomed, meaning that they can connect simultaneously to multiple access points acting as Mobile IP foreign agents (FAs). The access points can use different wireless access technologies and the gateway can switch between access points of different technology to obtain optimal service [5].

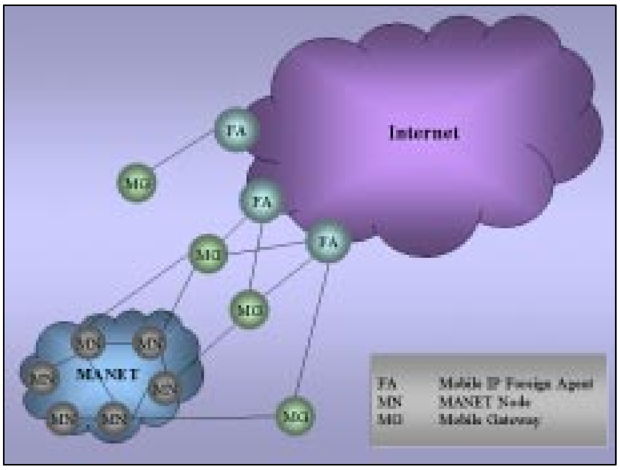

Figure 1 – Integrating MANETs and the Internet

The architecture for integrating MANETs and the global Internet is summarized in Figure 1. Mobile gateways (MGs) are responsible for providing Internet connectivity to MANET nodes (MNs). Mobile IP foreign agents (FAs) act as access points to the Internet and help MGs behave as mobile access points with respect to MANET nodes desiring Internet access. All MNs may not be within the reach of an MG, meaning that other MNs need to relay their traffic towards an MG.

Two principal ways in which ad hoc networks (either stationary or mobile) can be used to extend access networks are presented in [4]. In the first approach, the access network extension is planned. In this approach, which is also known as the cellular ad hoc network, special wireless access routers (WARs) are used for wireless interconnection. The WARs are either stationary or slow-moving and they are operated by legal entities or organizations, like universities or network providers. What makes the planned network extension an ad hoc installation is that the WARs can reach the fixed access points possibly multiple wireless hops away through other WARs. For this, an ad hoc routing protocol is used. Further, no central management is applied; if one WAR drops out, the other WARs will overtake its responsibilities.

The second approach is that of unplanned access network extensions. In this scenario, MGs are used to extend the access network. The MGs are simply normal terminals owned and operated by individual users. A user whose terminal acts as an MG can be seen as an auxiliary network provider, providing an extension of the access service of the access network provider (ANP) to other users. The planned and unplanned access network extension scenarios are depicted in Figure 2.

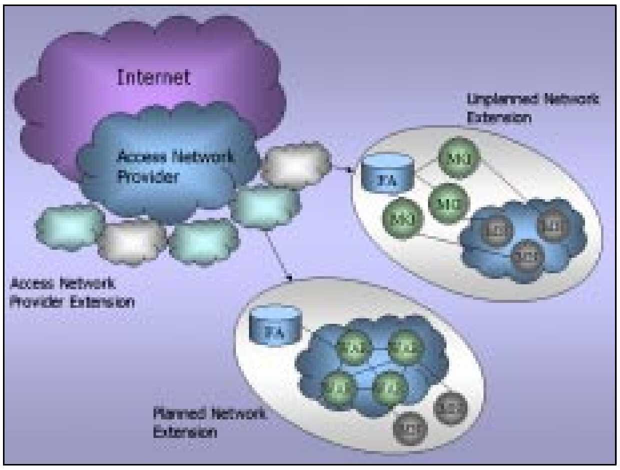

Figure 2 – Planned and Unplanned Extensions

Also a third approach, in which both planned and unplanned network extensions are used, is possible [4]. In this scenario, an MG can connect MNs to WARs when the MNs are out of the range of WARs.

In the most straightforward application of the planned and unplanned access network extension scenarios, the WARs are owned by the ANP and both the MNs and MGs are customers of the ANP. However, one can easily identify situations that are more complicated than this ANP centric scenario. First of all, the WARs and/or FAs could be owned by individual users providing open WLAN hotspots as described in [25]. Secondly, both in the planned and the unplanned access network extension scenarios, the MNs and also MGs might not have a customer relationship with the local ANP, meaning that they would be roaming users in the network of a foreign ANP.

2.2 Personal Networking

Another key concept besides ad hoc networking in beyond 3G networks is personal networking, which can be seen as an evolutionary and revolutionary step towards fourth generation (4G) networks [18]. Personal networks (PNs) introduce a shift from the technology centricity of current second generation (2G) and 3G networks towards greater user centricity. PNs are interesting from the viewpoint of this paper since ad hoc networking is one of their key features.

According to the definition of the European union funded My personal Adaptive Global NET (MAGNET) project, a PN includes a dynamic collection of personal nodes and devices around a user known as the Private Personal Area Network (P-PAN), and remote personal nodes and devices in different clusters, e.g. the home cluster, office cluster and car cluster. The P-PAN is a special cluster consisting of a small-area ad hoc network, and can be thought of as a wireless bubble around the user. The PAN and clusters are connected to each other either through infrastructure networks like cellular networks and Internet, or in an ad hoc hop-by-hop manner. This is illustrated in Figure 3.

Figure 3 – The Layout of a Personal Network

The clusters of the PN are self-organizing. Routes inside a cluster can consist of multiple hops and are built with an ad hoc routing protocol [1]. In fact, the entire PN is dynamic in the sense that it is created, maintained and destructed in an ad hoc manner. For instance, when a user moves around a building, nodes and clusters become a part of the network and leave the network in a dynamic fashion. Within each cluster of a PN, there is a special personal node called the gateway node, which provides to the other personal nodes in the cluster access to devices in remote clusters. If a remote cluster can only be reached through the Internet, the gateway (i.e. an MG) can offer Internet connectivity to other personal nodes e.g. through the nearest WLAN hotspot.

3 Business Models

The following business models regarding the use of ad hoc networks for wireless Internet access are described in this section: (i) network provider centric model, (ii) third party authentication, authorization and accounting (AAA) service provider (SP) centric model, (iii) proxy access network provider (ANP) business model, and (iv) access network repeater business model. These four models were selected because they reflect the different authentication relationships between the MNs and MGs described in [23]. In the network provider business model, it is the home network provider that provides the authentication, while in the 3rd party AAA SP model, this is done by a trusted third party. In the proxy ANP model, the MNs and MGs have a pre-existing trust relationship and are authenticated by each other. Finally, in the access network repeater business model, there is no trust; the nodes are not authenticated.

3.1 Network Provider Business Model

In the network provider business model, which is illustrated in Figure 4, all the MNs and MGs have a customer relationship with the network provider. In addition, the infrastructure such as WARs and FAs are owned by the network provider. The end-users always use their home network provider; roaming to the networks of other network providers having overlapping coverage is not possible. Thus, there exists a tight coupling of the user and the network provider and its network. Ad hoc networks are used to extend the coverage of the network provider's wireless access network. The MGs and relay MNs act as auxiliary network providers, and are included as new players in the business model. The network provider business model could be used e.g. in the Unified Cellular and Ad hoc Network architecture (UCAN) [13], in which an operator's 3G network is extended with a WLAN based ad hoc network.

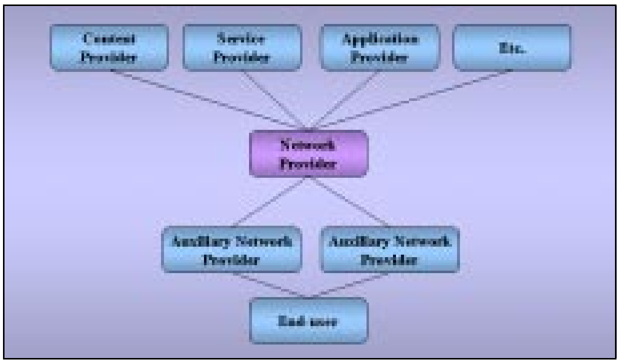

Figure 4 – Network Provider Business Model

Central to this model is that the network provider is in charge of the value network, delivering all different services and applications and controlling the contact to the end-users. Because of this central role, the network provider is dividing the revenue within the value network. The network provider also authenticates the auxiliary network providers and regular MNs and compensates the auxiliary network providers for the use of their resources for relaying the traffic of other users. In general, this model can be seen as a natural continuation of current 2G and 3G network provider business models described in [28] and [16]. However, there is also an aspect of a consumer to consumer business model present, since the auxiliary network providers are compensated for their efforts.

The main issues for the network provider business model include the design of a payment scheme that allows the compensation of the relay nodes, and willingness of users to share and offer infrastructure.

3.2 Third Party AAA Service Provider

In the third party AAA service provider (3P AAA SP) model proposed by the Academic Network on Wireless Internet Research in Europe (ANWIRE) project [4], the end-user is not tied to a single network provider, but can connect to different content providers, service providers and application service providers by using any ANP. Therefore, this model enables much more flexible service provisioning than the network provider centered model. Further, the home network provider is removed from its privileged position. The 3P AAA SP business model is illustrated in Figure 5.

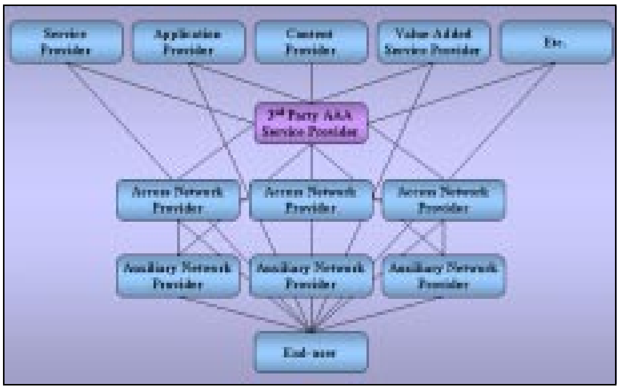

Figure 5 - Third Party AAA SP Business Model

In the 3P AAA SP business model [4], all the players have business agreements with the 3P AAA SP, which is a clearinghouse-like entity providing authentication, authorization and accounting of all the other players in the value network. The 3P AAA SP becomes therefore the central player of the model. All players have business agreements with the 3P AAA SP, whose task is to distribute the revenue within the value network. Also the auxiliary network providers are compensated and authenticated by the 3P AAA SP. Users have agreements with one or more 3P AAA SPs in the same way as they have one or more credit cards, and they receive one itemized bill for all services used through the 3P AAA SP. The 3P AAA SP business model could also include additional players not depicted in Figure 5 such as access brokers and access aggregators, which have been defined by the Ambient Networks project [20].

The main issues with the 3P AAA SP business model include that it is likely to require regulatory and standardization support. Also a payment scheme is needed to compensate the intermediate nodes. Finally, the model is likely to face the resistance of current network providers.

3.3 Proxy Access Network Provider

The proxy access network provider (ANP) business model is based on the idea of a pre-existing trust relationship between the MNs (including the MGs) [23]. The MNs have a trust relationship for instance because they are all devices of a single user or devices of the members of the same family. The MNs can rely entirely on the MG to provide access to the network resources. Because of the special relationship between the nodes, there is no need to provide incentives for the MG to share its Internet connection or for the MNs to relay the traffic of other MNs. The MG can be seen as a proxy ANP, relaying traffic without compensation. As an example of the use of the proxy ANP model, members of a family could establish an ad hoc network between their terminals using Bluetooth and share a single Internet connection. In another, PN related example, the MG might be a gateway node in a PN cluster (e.g. the P-PAN or home cluster) and the MNs the other devices that belong to the same cluster.

In both of the examples above, the ad hoc set-ups do not need a business model, since the relay nodes offer their services for free. However, in the PN scenario, the business opportunity for the network provider lies in the interconnection of the ad hoc clusters constituting the PN. The idea is that although users can set up parts of the network infrastructure and construct and deliver the services themselves, they also need to interconnect and work together with commercial network providers for parts of the network and services [12]. In MAGNET, the remote clusters of the PN are interconnected using dynamic virtual private network (DVPN) tunnels [7]. DVPNs provide users with on-demand QoS, bandwidth, and security. In contrast to traditional VPNs, in MAGNET, DVPN management is placed into the hands of the user. The business opportunity for the network provider lies in the provisioning of the DVPNs. Of course, the success of this business model is tied to the success of the personal networking paradigm.

3.4 Access Network Repeater

When there is no trust relationship between the nodes of the ad hoc network, the intermediate nodes (i.e. MGs and relay MNs) can be seen as mere access network repeaters, as defined in [23]. The MG shares its connection and the relay MNs forward traffic without compensation. The connection can be free (e.g. through an open WLAN hot spot) or non-free (e.g. a 3G connection). The access network repeater scenario could occur e.g. in a campus area where nodes that are strangers to each other create an ad hoc network using a short range wireless technology such as Bluetooth. In addition to these nodes, also nodes that have both a WLAN connection to the Internet and a Bluetooth interface that connects them to the ad hoc network are needed. Such nodes act as MGs, sharing their Internet connections with the MNs of the ad hoc network.

Naturally, if also the ad hoc network is constructed using WLAN links, MG nodes are not needed.

The most significant challenge for the access network repeater business model is the lack of authentication between the nodes and the resulting lack of security. In addition, the model provides no incentives for the intermediate nodes to relay the packets of other nodes or to share their Internet access. Therefore, it can be argued that this model will be very difficult to deploy in real life.

The different business models presented in this Chapter are summarized in Table 1.

Table 1 – Different Business Models Summarized

Model	Auth. done by	Key player	Roaming between ANPs	Relays compensated
Network provider	Network provider	Network provider	no	yes
3rd party AAA SP	3rd party AAA SP	3rd party AAA SP	yes	yes
Proxy ANP	Pre-existing trust relationship	User/ network provider	yes	no
Access network repeater	No auth.	User	yes	no

4 Challenges

In this chapter, the technical and business model related challenges concerning the use of ad hoc networks are discussed.

4.1 Technical Challenges

There are numerous open problems with ad hoc networking [19]. First of all, scalability is an issue; one problem for current ad hoc routing algorithms is that they cannot guarantee an acceptable level of service in the presence of a large number of nodes in the network. Quality of Service (QoS) is another problem, since radio frequency channel characteristics can vary unpredictably and since network partitions can be created because of dynamic topology changes. There are also issues in sharing the channel medium with many neighbors; technologies to enhance spectrum efficiency are required. All in all, end to end QoS is very difficult to achieve since routers may be continuously moving and links may go up and down all the time. Energy efficiency is an important problem, since in the absence of a fixed infrastructure nodes need to rely on the limited power of their batteries. A further problem for mobile ad hoc networks is how to maintain a sufficient density of wireless coverage to prevent the partitioning of the network [27]. If partitions exist, current ad hoc routing protocols will fail to deliver packets. Also node willingness is a problem [11]; due to selfish behavior, nodes may refuse to relay packets of other nodes. The reasons for this might include lack of trust, desire to save battery power, etc. One additional challenge is the interoperation between different ad hoc routing protocols. Finally, one of the most important problems is security [14]. As an example, relay nodes (MNs and MGs) can eavesdrop information, delete messages, inject erroneous messages, or impersonate a node. This violates availability, integrity, authentication and nonrepudiation. Compromised nodes can also launch attacks from within the network.

There are also challenges in the integration of MANETs and the Internet, including the mismatches regarding their infrastructure, topology and mobility management mechanisms [2]. Other problems include gateway discovery, selection of an optimal gateway and providing MANET nodes with globally routable IP addresses [3]. In addition, MGs need to perform dynamic access selection [22] and handle handovers between different access technologies.

4.2 Challenges for Business Models

There are two central issues a business model for ad hoc networks must address [8]. First of all, an alternative means of payment that does not rely on a prearranged trust scheme with the ANP is needed. Secondly, an incentive scheme is necessary for nodes relaying messages on behalf of other nodes. The intermediate nodes may need to be compensated for the use of their resources. One approach that attempts to address both of these issues is the multiparty micropayment scheme introduced in [26].

It should be noted that providing incentives to the intermediate nodes is likely to be necessary even though a pricing scheme such as flat rate was used, since the intermediate nodes participate in the provisioning of end to end QoS, and because relaying the traffic of other nodes consumes limited resources such as battery power, central processing unit time and bandwidth that the intermediate nodes could have otherwise used themselves. An incentive scheme is also needed to prevent the tendency towards selfish behavior; a selfish relay node could temporarily refuse to forward traffic from other nodes to obtain a larger share of the bandwidth for its own traffic.

Other challenges include high costs and limited availability of spectrum, user acceptance and willingness to share infrastructure and resources, and challenges associated with assuring users of the security of ad hoc networks [23]. An important question is also how to price the service offered by the auxiliary network providers. Also the requirement of zero configuration is an important one; ad hoc Internet access should not result in increased complexity for the user. There are also regulatory uncertainties concerning the sharing of network connections and the lack of control over the transmitted content for the relay nodes. Finally, regulatory and standardization support is needed in order to enable more flexible business models like the 3P AAA SP model.

As a summary, there are a number of open problems that need to be addressed before the large-scale deployment of ad hoc networks and their use for wireless Internet access can become a reality. A failure to solve critical technical challenges such as end to end QoS, security and scalability, and business model related challenges like alternative means of payment, regulatory uncertainties and compensation of intermediate nodes can severely hinder the wide-scale deployment of ad hoc networks.

5 Current Use of Ad Hoc Networks

Traditional examples of the use of ad hoc networks are military and emergency situations. In fact, the initial development of ad hoc networks was mainly driven by military applications. However, many companies are starting to realize the commercial potential of ad hoc networks outside their original contexts of use, including companies such as Green Packet [10], PacketHop [17] and Firetide [9]. These companies are targeting e.g. law enforcement agencies, intelligent transport systems, community networking and home networks with their ad hoc networking solutions.

One example of the proxy ANP business model not including the personal networking aspects is when family members use the same General Packet Radio Service (GPRS) enabled handset as an MG for their laptops, utilizing one hop Bluetooth links. Another example is a solution called PacketHop Communication System offered by PacketHop, Inc. [17] to law enforcement agencies and fire fighters. In this solution, law enforcement personnel can create a mobile ad hoc network among themselves. The solution is interoperable with WLAN access points enabling thus also wireless Internet access through ad hoc networks.

The third party AAA service provider business model is not being applied at the moment and the use of the access network repeater business model is limited to few special cases. One such special case is the current opportunistic use of open WLAN hotspots by single terminals, which does not, however, involve the use of ad hoc networks, but rather one-hop wireless links. Finally, a special case of the network provider business model is possible e.g. in companies and universities if the planned access network extension scenario with a mesh network of WARs presented in Section 2.1 is used. In this case, the company operating its own WLAN access network would act as a network provider. The use of this model is possible, since commercial cable-free WLAN-based WARs are already available. One example is the Firetide Instant Mesh Network solution offered by Firetide, Inc. [9].

6 Conclusions

In this paper, the use of ad hoc networks for wireless Internet access was discussed. The proposed architecture for integrating MANETs and the Internet was described and the use of personal networking was discussed. Also four business models for providing wireless Internet access through ad hoc networks were presented. Finally, some challenges were listed and a brief overview of the current use of ad hoc networks was presented.

There are emerging factors supporting the use of ad hoc networks as part of wireless architectures. Further, ad hoc networking can be seen as a potentially disruptive force, since it challenges many current assumptions in the world of wireless communications. Ad hoc networking has also been considered as a key feature in beyond 3G systems. To integrate MANETs and the Internet, the use of mobile gateway nodes acting as a bridge between the MANET and the edge of the Internet has been proposed. Besides ad hoc networking, another key concept in beyond 3G systems is personal networking, in which ad hoc networks have a central role.

Four different business models supporting the use of ad hoc networks for wireless Internet access were considered in this paper. In the network provider centric business model, the network provider is in charge of the value network. To enable a shift from this model towards more flexible business models, regulatory support is likely to be needed. One way to relax the tight coupling of users and network providers is to make a trusted third party responsible for the user account, as is the case in the third party AAA service provider business model. The business opportunity in the proxy access network provider model is that although in personal networking users can setup parts of the network infrastructure themselves, they still need the services of commercial network providers for providing interconnection services. Finally, the access network repeater business model is unlikely to be widely deployable in real life due to its severe security concerns.

Also a number of barriers regarding the use of ad hoc networks for wireless Internet access were identified. In addition to a number of technical concerns, many business model related issues were discussed. The most important of these include the design of an alternative means of payment not relying on the network operator, and the design of an incentive scheme for relay nodes. Although ad hoc networks have the potential to change the wireless landscape, a failure to address the technical and business model related challenges can effectively hinder this potential and the wide-scale deployment of ad hoc networks.

References

[1] Alutoin, M. et al: Towards Self-organising Personal Networks. Proceedings of the ACM DIN'05, September 2, 2005.

[2] Ammari, H. M.: Using Group Mobility and Multihomed Mobile Gateways to Connect Mobile Ad Hoc Networks to the Global IP Internet, International Journal of Communications Systems, John Wiley & Sons, Ltd., 2006.

[3] Andreadis, G.: Providing Internet Access to Mobile Ad Hoc Networks, London Communications Symposium, Sept 2002.

[4] Armuelles, I. et al.: On Ad Hoc Networks in the 4G Integration Process, The Third Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc) 2004.

[5] Aust, S. et al.: Mobile Internet Router for Multihop Ad Hoc Networks, 6th International Symposium on Wireless Personal Multimedia Communications (WPMC 2003), Yokosuka, Kanagawa, Japan, October 2003.

[6] Broch, J. et al.: Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks, Proceedings of the Workshop on Mobile Computing, June 1999.

[7] Calin, D. et al: MAGNET: An Approach for Secure Personal Networking in Beyond 3G Wireless Networks, Bell Labs Technical Journal 11(1), 79-98, 2006.

[8] Doyle, L. et O'Mahony, D.: Ad-Hoc Networking: A Welcome Disruption, IST 2002 Event, Copenhagen, 2002.

[9] Firetide, Inc. http://www.firetide.com (Referred 22.10.2006)

[10] Green Packet, Inc. http://www.greenpacket.com (Referred 22.10.2006)

[11] Harras, K. A. et al.:. Delay Tolerant Mobile Networks (DTMNs): Controlled Flooding in Sparse Mobile Networks, In IFIP Networking, Waterloo, Canada, May 2005.

[12] Henten, A. et Saugstrup, D.: The PN Concept in a Business Modelling Perspective, Center for Tele-Information Working Papers, No. 95, 2004.

[13] Luo, H. et al.: UCAN: A Unified Cellular and Ad-Hoc Network Architecture, Proceedings of the ACM MobiCom'03, September 2003.

[14] Milanovic, N. et al.: Routing and Security in Mobile Ad Hoc Networks. IEEE Computer Society, February 2004.

[15] My personal Adaptive Global NET (MAGNET) http://www.ist-magnet.org/ (Referred 22.10.2006)

[16] Nurmiranta, P.: Social Optimality of Alternative Business Models, Seminar on Networking Business, TKK Networking Laboratory, 2006.

[17] PacketHop, Inc. http://www.packethop.com (Referred 22.10.2006)

[18] Prasad, R. et Olsen, R. L.: The Unpredictable Future: Personal Network Paving Towards 4G, Telektronikk, vol. 1, 2006.

[19] Ramanathan, R. et Redi, J.: A Brief Overview of Ad Hoc Networks: Challenges and Directions, IEEE Communications Magazine 50th Anniversary Commemorative Issue, May 2005.

[20] Raza, S. A.: Conceptual Frameworks for Interconnection of Heterogeneous Networks, Seminar on Networking Business, TKK Networking Laboratory, 2006.

[21] Perkins, C.: IP Mobility Support for IPv4, RFC 3344, August 2002.

[22] Rinta-aho, T.: Dynamic Selection of Optimal Wireless Access Service, Seminar on Networking Business, TKK Networking Laboratory, 2006.

[23] Robles, T. et al.: Usage Scenarios and Business Opportunities for Systems beyond 3G, Proceedings of the IST Mobile and Wireless Telecommunications Summit 2002, Thessaloniki, June 2002.

[24] Sun, Y. et al.: Internet Connectivity for Ad Hoc Mobile Networks, International Journal of Wireless Information Networks, special issue on Mobile Ad Hoc Networks (MANETs): Standards, Research, Applications, 9(2), April 2002

[25] Tallberg, M.: P2P-based Roaming Between Home WLAN Hotspots, Seminar on Networking Business, TKK Networking Laboratory, 2006.

[26] Tewari, H. et O'Mahony, D.: Multiparty Micropayments for Ad Hoc Networks, in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC) 2003, New Orleans, Louisiana, March 2003.

[27] Vahdat, A. et Becker, D.: Epidemic Routing for Partially-Connected Ad Hoc Networks. Technical Report CS-200006, Duke University, April 2000.

[28] Välimäki, J.: Change of Business Models for Wireless Internet Access, Seminar on Networking Business, TKK Networking Laboratory, 2006.

XII. Social Optimality of Alternative Business Models

PEKKA NURMIRANTA
Helsinki University of Technology
pekka.nurmiranta(a)pp1.inet.fi

Abstract

The purpose of this paper is to introduce some basic terminology of consumer theory and methods for analyzing social optimality. These are then applied to study the social optimality of the main business models in wireless LAN (WLAN) hotspot market today.

This paper has the ambitious target to give indication which combination of business models is most likely to produce a socially optimal solution.

1 Introduction

The social welfare research in communication services has its roots in the era of state owned Telco monopolies. In those circumstances the role of the regulator is to ensure that operators set the prices of their services in a socially optimal way. The services need to deliver utility value to consumers and at the same time allow the Telco's to cover their costs and make a profit. The price setting was originally studied in a single service set up – the Telco providing a fixed voice service to its customers in a monopoly environment.

Now the fixed telephony market is decreasing. The GSM, 3G and internet broadband access markets are saturating. The most interesting growing area in the information society is the wireless internet access and the WLAN hotspot services market

The interesting challenge is to try to take the welfare research further and apply it to the fast moving WLAN business where new business models are arising. The dilemma becomes even more complex as multiple radio access is available and the impact should be considered [1].

As new markets are emerging the social planner, regulator, and politician need to follow the development of the market and be ready to take the necessary action to create an environment of healthy competition and welfare creation.

The purpose of this study is to look at the welfare research available, select most interesting business models, and look at the aspect of social optimality.

Some research is already available analyzing the social optimality of WLAN hotspot business models.

2 Terminology

The purpose of this section is to introduce some basic terminology which is used in the social optimality research and literature concerning communication services.

- Consumer's utility = service coverage, bit rate, etc.
- Consumer's surplus = utility – cost
- Producer's surplus = revenue – cost = profit
- Welfare = Consumers' surplus + producer's surplus
- Ramsey pricing – named after English economist Frank Ramsey (1903 – 1960), prices that maximize industry consumer surplus and profits.
- Network externality – value of the network to consumer increases as the number of the users increases
- Monopoly – a single supplier who controls the amount of good produced. The government regulates the monopoly's prices, allowing it to cover costs and make a reasonable profit.
- Perfect competition – many suppliers (and consumers) in the market, every participant is small and so no one can dictate prices
- Oligopoly – a competitive market of a small number of producers

3 Methods for Analyzing Social Optimality of WLAN Business Models

Social welfare (which is also called social surplus) is defined as the sum of all users' net benefits, i.e. the sum of all consumers' and all producers' surpluses. In the research weighted sums of consumer and producer surpluses can be considered, reflecting the reality that a social planner, regulator, or politician may attach more weight to one sector of the economy than to another [2].

The key idea in regulation is that the social welfare can be maximized (and social optimality reached) by setting an appropriate price and then allowing producers and consumers to choose their optimal levels of production and consumption. A supplier sets his level of production knowing only his cost function, not the consumers' utility functions. A consumer set his level of demand knowing only his own utility function, not the producers' cost functions or other customers' utility functions. Individual consumer's utility functions are private information, but the aggregate demand is commonly known [2]. Figure 1 shows an illustration of the social welfare maximization for a single good.

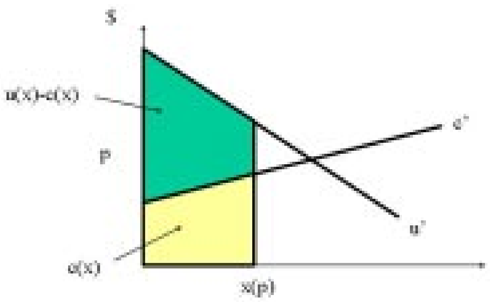

Figure 1. A simple illustration of the social welfare maximization for a single good [2].

The maximum is achieved at the point where the customer's aggregate demand curve u' intersects the marginal cost curve c'.

The approaches for analyzing social optimality are those generally used in analyzing the microeconomic impact, pricing and social welfare of communication services.

The main areas that need to be considered are [2]:

- Demand, supply and market mechanisms
- Maximization of consumer surplus
- The suppliers problem
- Welfare maximization
- Cost Recovery

3.1 Ramsey prices

Ramsey pricing is a pricing theory which is often applied for publicly produced private goods. Ramsey prices are prices that maximize social welfare under the constraint of recovering cost [2].

Here we have a connection between competition and social efficiency. Under potential competition incumbents will be motivated to use prices that maximize social efficiency with no need of regulatory intervention.

3.2 Pricing example

The core of the social optimality is in the price setting. In the case of communication services the price setting can be problematic. Adding a new service to the offering could increase the cost of the infrastructure only marginally – especially in the beginning when this service has only few customers. As usage grows the cost allocation might need to be reconsidered and the marginal cost thinking does not produce the right result. The original mainstream product has become marginal and the originally marginal product has become the main offering.

As an example of the pricing challenge we could consider the following. Let's take Internet broadband access with WLAN as add-on, a multi radio handset and cellular voice – these products and services could be offered separately or packaged as a wireless home offering.

The new multi radio devices enable the operators to commercially package services like cellular voice and Wireless LAN access – with VoIP and eventually with UMA capabilities when these services are introduced to the market

As a packaged service offering 'Wireless Home' this service could be offered with flat fee pricing – maybe 50-100 €/month. The interesting question is – how is the revenue allocated to individual services, how is the cost allocation and profitability of the service calculated and how does the regulator follow that the pricing is socially optimal?

In this literature study it is not possible to go further with this example but it could be analyzed in future research.

4 Business Models

The selection of business models is linked to the market environments described in Chapter 2. The three models selected are [3]:

- Telco model – hotspots owned and managed by Telco (monopoly)
- Free radio – individual users connect to individually owned hotspots (perfect competition)
- Hotspot aggregator – an intermediate between users and individual hotspot providers (oligopoly)

In Figure 2 the models are illustrated on a high level.

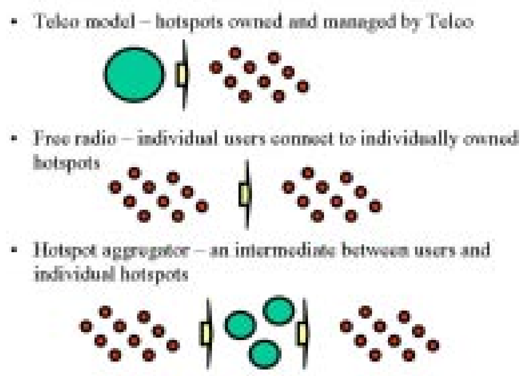

Figure 2. Alternative Business Models [3]

Besides these three selected business models there are also various other models arising in the market today [4]

4.1 Service architectures

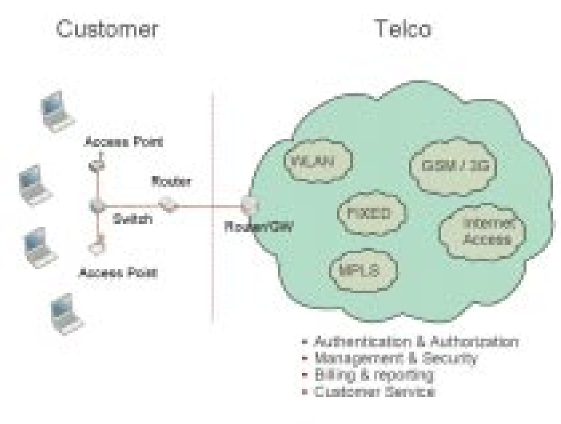

Figure 3: Service architecture of Telco Business Model

To illustrate the wireless LAN service architecture the Telco service architecture is described on a high level in Figure 3. This illustration describes the situation when a Telco provides a wireless LAN hotspot service to a customer. Wireless LAN service is one service in Telco’s service portfolio. In the case illustrated in Figure 3 the customer could be a company who offers wireless access to Internet to its customers visiting the office and wireless Internet and intranet access to its employees. The employees could use a virtual private network (VPN) service to access the corporate network and intranet. The visitors would need to authenticate themselves before accessing the wireless LAN hotspot. The Telco customer could also be a hotel who offers WLAN hotspot services to its customers.

The service package could include the wireless LAN and basic LAN infrastructures, the Internet connection and management and security services for the whole infrastructure.

The service architectures of Free radio and Aggregator business models differ from this in the following main points:

- In Free radio the centralized management of services does not exist as the business model is based on P2P approach
- In Hotspot Aggregator business model the additional services (e.g. authentication server) are produced by the Aggregator as the Internet connection comes from the internet service provider.

4.2 Telco Business Model

In literature [3] the Telco business model is linked with the monopoly position where the Telco has free hands to set price and optimize its profits.

A Telco can include user authentication to the service and reduce security risks and potential misuse of the access.

Telco business model with centrally managed service leads to high bit rate and availability. Focused coverage and high cost reduce the consumer’s surplus.

By definition the monopoly Telco can choose its price for the services. Based on this a Telco makes good profit and as a good taxpayer contributes to the social welfare.

4.3 Free Radio Business Model

Free radio is an application of the P2P approach. Individual hotspot owners open their connections for everybody. A centralized coordination is not required. Instead, the network of hotspots can operate in a fully decentralized way.

The main question of the Free Radio model is - Charge or not – does the individual user charge other users for the service. Free radio assumes that there is not charge. With no charge the business model generates a loss as hotspot setup and management generates a cost.

Consumer’s utility is high when the Free radio business model is widely accepted – coverage is good, high bit rate available with no cost. The service availability and predictability could be a challenge.

Free radio typically leads to a high number of hotspots. The security risks are evident as no user authentication is required.

4.4 Hotspot Aggregator Business Model

A Hotspot Aggregator is a managed Free Radio P2P community with a 3rd Party as an aggregator.

A hotspot aggregator provides a platform for the users and the providers of hotspots. The platform could include authentication service for security reasons.

The Hotspot Aggregator needs to charge a price to cover its costs. Costs are generated from the service platform setup and management. If the number of hotspots is high the cost for users is marginal. The profit optimization happens as a function of the price charged from the user and the fee paid to the hotspot providers.

The business model has potential to be a socially good solution. If widely accepted the coverage is good and the costs are marginal. The presence of an aggregator brings managed service elements to the model and this increases the predictability, security and of the quality of service.

5 Conclusions

Three business models were selected from the research as examples for studying the social optimality of hot spot business models. The business models are called Telco, Free Radio and Hotspot Aggregator. The results are summarized in Table 1.

Business Model	Number of Hotspots	Bit rate	Cost	User surplus	Profit	Welfare
Telco	◐	●	●	◐	●	◐
Free Radio	●	◐	○	◐	○	◐
Hotspot Aggregator	◐	◐	◐	◐	●	◐

● HIGH ◐ MEDIUM ○ LOW

Table 1: Summary of results

The research [3] does not give any easy answers to the regulator and social planner. A mathematical model has been created but the result as such does not give indication which business model would be the most beneficial for the social optimality. Each model has its own strengths and weaknesses.

The analysis needs to be developed further so that the differences in welfare creation between business models can be found.

The effort should then be continued and results applied with possible market development scenarios to find out the impact of regulatory actions to the social optimality of the models.

These scenarios could then be used in real life situations e.g. by the social planner in the decision making concerning regulatory activities.

References

[1] Business Models for Public WLAN, Presentation by Jaakko Kuosmanen in Telecommunications Forum 2006

[2] Courcubetis, Weber: Pricing communication networks – Economics, Technology and Modeling, Wiley 2003

[3] Hotspot Services in the Open Spectrum: Implications of Market Organizations for coverage and welfare, March 10, 2006.

[4] VoIP and WLAN – Changing the rules, Presentation by Klaus Nieminen in Telecommunications Forum 2006