ACCESS 2011

The Second International Conference on Access Networks

June 19-24, 2011

Luxembourg City, Luxembourg

ACCESS 2011 Editors

Alessandro Bogliolo, Università di Urbino, Italy

Eugen Borcoci, University “Politehnica” Bucharest, Romania

ACCESS 2011

Foreword

The Second International Conference on Access Networks [ACCESS 2011], held between June 19 and 24, 2011, in Luxembourg, continued a series of conferences dealing with access networks, services and technologies based on the previous NEUTRAL and HOWAN workshop treating particular access aspects. ACCESS 2011 aimed to provide an international forum by researchers, students, and professionals for presenting recent research results on advances in networking access, including the newest emerging access technologies, broadband access, wireless access, copper access, optical access, mobility aspects, as well as optical/wireless combination and neutrality.

Hybrid Optical and Wireless Access Networks (HOWANs) consists of a multi-hop wireless mesh network (WMN) at the front-end and an optical access network, e.g., a passive optical network (PON) at the back-end. PONs use inexpensive and passive optical splitters to divide a single fiber into separate strands feeding individual subscribers. EPON is based on the Ethernet standard, which comes with the added benefit of the economies-of-scale of Ethernet, and provides simple and easy-to-manage connectivity both at the customer premises and at the central office.

One option is to grant positive externalities to the shared access infrastructure in order to enhance digital inclusion and broadband penetration by triggering a positive feedback loop among users, service providers, network operators, and investors. The access infrastructure can be considered as a network per se, called "neutral access network" (NAN), which provides internal services and possibly exploits its territorial dimension in order to overcome the dichotomy between "on-line" and "off-line" people. While in a traditional access network, people who are not registered with any ISP are left out from the so called "information society", NANs can provide an intermediate area, which is logically placed "before the Internet", where on-line services and applications can be made available to residential and nomadic users who are not yet registered with any ISP.

We take here the opportunity to warmly thank all the members of the ACCESS 2011 Technical Program Committee, as well as the numerous reviewers. The creation of such a broad and high quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and efforts to contribute to ACCESS 2011. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

Also, this event could not have been a reality without the support of many individuals, organizations, and sponsors. We are grateful to the members of the ACCESS 2011 organizing committee for their help in handling the logistics and for their work to make this professional meeting a success.

We hope that ACCESS 2011 was a successful international forum for the exchange of ideas and results between academia and industry and for the promotion of progress in the field of access networks.

We are convinced that the participants found the event useful and communications very open. We also hope the attendees enjoyed the historic charm Luxembourg.

ACCESS 2011 Chairs:

Alessandro Bogliolo, Università di Urbino, Italy
Fabio Chiussi, BZinc, Inc., USA
Georgios Karagiannis, University of Twente, The Netherland
Gyu Myoung Lee, Institut Telecom / Telecom SudParis, France
Guowang Miao, Dallas Telecom Lab / Samsung - Richardson, USA
Mark Perry, University of Western Ontario/Faculty of Law/ Faculty of Science - London, Canada
Sanguthevar Rajasekaran, University of Connecticut - Storrs, USA
Guillaume de la Roche, University of Bedfordshire, UK
Xu Shao, Institute for Infocomm Research, Singapore
Hiromi Ueda, Tokyo University of Technology, Japan
Ljiljana Trajkovic, Simon Fraser University - Burnaby, Canada
Abdulrahman Yarali, Murray State University, USA

ACCESS 2011

Committee

ACCESS Advisory Chairs

Alessandro Bogliolo, Università di Urbino, Italy
Hiromi Ueda, Tokyo University of Technology, Japan
Sanguthevar Rajasekaran, University of Connecticut - Storrs, USA
Mark Perry, University of Western Ontario/Faculty of Law/ Faculty of Science - London, Canada
Abdulrahman Yarali, Murray State University, USA

ACCESS Industry Chairs

Fabio Chiussi, BZinc, Inc., USA
Guowang Miao, Dallas Telecom Lab / Samsung - Richardson, USA

ACCESS Special Area Chairs

Femtocells
Guillaume de la Roche, University of Bedfordshire, UK
Gyu Myoung Lee, Institut Telecom / Telecom SudParis, France

Nextacces
Georgios Karagiannis, University of Twente, The Netherland

Technical/Legal
Mark Perry, University of Western Ontario/Faculty of Law/ Faculty of Science - London, Canada

Wireless
Ljiljana Trajkovic, Simon Fraser University - Burnaby, Canada

Optical
Xu Shao, Institute for Infocomm Research, Singapore

ACCESS 2011 Technical Program Committee

Hojjat Adeli, The Ohio State University, USA
Michael Bahr, Siemens AG - München, Germany
Andrzej Beben, Warsaw University of Technology, Poland
Alessandro Bogliolo, Università di Urbino, Italy
Fernando Boronat Seguí, Polytechnic University of Valencia - Gandia, Spain
Qin Dai, Technische Universität Dresden, Germany
Guillaume de la Roche, University of Bedfordshire, UK
Emiliano Garcia-Palacios, Queens University - Belfast, UK
Vanessa Gardellin, University of Pisa, Italy
Fabio Chiussi, BZinc, Inc., USA
Mounir Hamdi, Hong Kong University of Science and Technology - Kowloon, Hong Kong
Georgios Karagiannis, University of Twente, The Netherland

Gyu Myoung Lee, Institut Telecom / Telecom SudParis, France
David López-Pérez, King's College London, UK
Zoubir Mammeri, IRIT - Paul Sabatier University - Toulouse, France
Elsa María Macías López, University of Las Palmas de Gran Canaria, Spain
Jon Matias, University of the Basque Country (UPV/EHU), Spain
Guowang Miao, Dallas Telecom Lab / Samsung - Richardson, USA
José Mora Almerich, Polytechnic University of Valencia, Spain
Jogesh K. Muppalla, The Hong Kong University of Science and Technology, Hong Kong
Armando Nolasco Pinto, Instituto de Telecomunicações / Universidade de Aveiro, Portugal
George S. Oreku, Tanzania Industrial Research and Development Organization, Tanzania
Mark Perry, University of Western Ontario/Faculty of Law/ Faculty of Science - London, Canada
Sanguthevar Rajasekaran, University of Connecticut - Storrs, USA
Dimitrios Serpanos, ISI / Univ. of Patras, Greece
Xu Shao, Institute for Infocomm Research, Singapore
Álvaro Suárez Sarmiento, University of Las Palmas de Gran Canaria, Spain
Antonio Teixeira, Universidade de Aveiro / Instituto de Telecomunicações, Portugal
Ljiljana Trajkovic, Simon Fraser University - Burnaby, Canada
Hiromi Ueda, Tokyo University of Technology, Japan
Manuel Villen-Altamirano, Technical University of Madrid, Spain
Rong Weifeng, Institute for Infocomm Research, Singapore
Robert Wójcik, AGH University of Science and Technology, Krakow, Poland
Zuqing Zhu, Cisco Systems, Inc., USA

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

Adaptive Resource Allocation Scheme for TETRA Networks with Multi-operators

Salman A. AlQahtani
Information and Communication Technology Department
King Fahd Security College
Riyadh, Saudi Arabia
salman@kfsc.edu.sa

Abstract— **In this paper, we evaluate various aspects of packet data transmission in terrestrial trunked radio (TETRA) networks giving particular emphasis on the performance of applications transmitting data between a number of radio terminals and a fixed server. The utilization of such applications is constantly increasing in public safety networks and so does the need to dimension and configure TETRA networks to meet their reliability, delay and loss requirements. Without an efficient radio resource management (RRM), one operator can exhaust the capacity of others. This study tackles an efficient scheduling to provide maximum system throughput and proportional fairness in accordance with operator capacity share through adaptive resource allocation scheme. We refer to this new scheme as multi-operators time division generalized processor sharing scheme (M-TDGPS). It employs both adaptive rate allocation to maximize the resource utilization and GPS techniques to provide fair services for each operator. The performance analysis of this scheme is derived using the GPS performance model and compared with the normal static rate M-TDGPS scheme. The simulation results show that the proposed adaptive rate M-TDGPS scheduling scheme improves both system utilization (throughput) and average delays.**

Keywords-adaptive rate scheduling; GPS; multi-operator; utilization; TETRA

I. INTRODUCTION

Several IP-based data services are used today in Terrestrial Trunked Radio (TETRA) networks. The traffic of these IP-based applications is characterized by small messages (e.g., in the order of 80–150 bytes) being sent occasionally between a number of TETRA radio terminals and a fixed server. These messages are typically transmitted on a TETRA packet data channel (PDCH), and consequently we term such client-server applications as packet data messaging applications [18].

For current and next TETRA and beyond time division with multiple access (TDMA) networks, sharing the radio access network has become an important issue for TETRA operators. TETRA and beyond network rollout is a very costly and time consuming process. Therefore, sharing of network infrastructure among operators offers an alternative solution to reducing the investment in the coverage phase of TETRA. Another advantage of the deployment of shared networks is the increased coverage, since operators can cooperate on coverage and sites as a more cost-effective way to cover large geographical areas. All together, this will result in reduced time to market and earlier user acceptance for TETRA and its related services. The sharing methods available for similar wireless network operators are proposed in many literatures [1-3]. These sharing methods include, site sharing, radio access network (RAN) sharing, common network sharing, and geographical network. The previous proposals and studies of wireless sharing methods present the problem from an architectural and technical point of view without investigating how the shared radio resources are going to be managed and controlled through radio resource management (RRM) procedures. The RAN based sharing method is of special importance as it reflects the most recent and critical sharing option where more than one operator shares the same RAN. In RAN sharing method, which is the focus in this study, each operator has its own core network and only the RAN is shared as depicted in Fig. 1. This implies that multiple operators fully share the same RAN. Without an efficient RRM, one operator may exhaust the capacity of others. Therefore, there is a critical need for radio resource control between the multiple operators to prevent one operator from exhausting the capacity of others.

Service level agreements (SLA) specify the usage of the radio network capacity for each operator under the RAN based sharing agreement [16]. Each operator receives the agreed upon Quality of Service (QoS) level by following the specified operation rules in the SLA. More about SLA and service management can be found in [16].

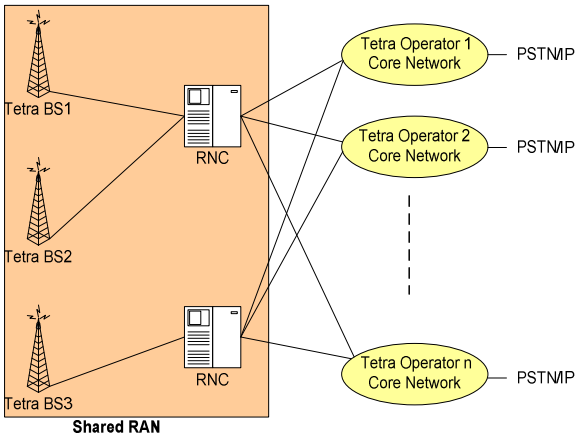

Figure 1. Tetra RAN Sharing

 ISBN: 978-1-61208-142-7

In order to secure the fair access to the network resources and to optimize the usage of the allotted capacity, it is very important to allow the RRM to separately control each operator and guarantee its minimum required capacity. In other words, the RRM procedure should guarantee that the maximum traffic per operator as defined by SLA is not exceeded unless permitted. RRM can allow an operator's traffic to exceed its limit in an adaptive way if there are unused resources related to other unbacklogged operator in order to increase the overall system utilization. Hence, the shared radio resources must be controlled in a fair and efficient way between operators. The Scheduling scheme, as part of RRM, controls the packets transmissions during the connection time. This study proposes the same idea in the case of TETRA networks. It focuses on designing an efficient and fair scheduling scheme for multi-operator TETRA system.

A. *Related Works and Motivation*

An ideal fair scheduling discipline is the well known generalized processor sharing (GPS), and also known as weighted fair queuing (WFQ) [4][5]. The GPS discipline was introduced in [4][5].Several GPS-based fair scheduling schemes have been proposed for wireline packet network [4]-[6]. Also, these GPS-based scheduling algorithms have been adapted to wireless networks. The work in [7]-[9], extend fair scheduling schemes developed for wireline networks to time division multiple access (TDMA)-based and hybrid time-division/code-division multiple access (TD/CDMA) based wireless networks. These schemes are implemented using a conventional time-scheduling approach, requiring high complexity due to the intensive computation for the virtual time of each packet [10].

In order to improve radio resource utilization and achieve fairness with low complexity in such TETRA-based wireless networks, number of recent algorithms for GPS-based uplink scheduling are studied and adapted in [11]-[15]. In [12]-[13], an uplink low-complexity code-division GPS (CDGPS) scheme for dynamic fair scheduling is proposed. The CDGPS scheduler makes use of the adaptability of the mobile wireless physical layer to perform fair scheduling on a time-slot basis by using a dynamic rate-scheduling approach rather than the conventional time scheduling approach as in GPS. At the beginning of each time slot, the scheduler adjusts only the channel rate of each session traffic flow in the system by varying the spreading factor and/or using a multiple of orthogonal code channels, rather than allocating service time to each packet as in GPS to reduce the implementation complexity of GPS [13]. A low-complexity GPS-based bandwidth scheduling scheme similar to the CDGPS is also proposed in [14], where a multi-carrier CDMA system is considered. Based on the minimum power allocation algorithm, a WCDMA GPS scheduling scheme is proposed in [15]. However, all these scheduling schemes are designed for single operator systems without considering how to control and schedule the resources that are shared among more than one operator in an efficient and a unified way.

B. *Research Contribution*

In this study, the CDGPS and GPS discipline idea is adapted and extended in order to design a new high performance GPS-based scheduling scheme which can effectively control the shared resources among TETRA multi-operators in an efficient and fair manner. Efficient means higher system utilization and fair means that each operator guaranteed at least a capacity equals to its capacity share specified in the SLA. Therefore, a multi-operator TDMA based of GPS (M-TDGPS) rate scheduling scheme for the uplink TETRA network is designed and analyzed. The scheme employs both adaptive rate allocation to maximize the resource utilization and M-TDGPS to provide fair services for each operator. The resource allocated to each operator session is proportional to an assigned weight factor as per the SLA specification. After the initial allocation of the allotted capacity, M-TDGPS scheme uses the GPS service discipline to dynamically schedule the assigned channel rates of one operator among the traffic classes within that operator independently.

The rest of this paper is organized as follows. Section II describes the system model and assumptions. Section III explains the proposed scheme in details while Section IV presents the obtained results, as well as the discussion. Finally, the paper is concluded in Section V.

II. SYSTEM MODEL AND ASSUMPTIONS

The original TETRA standard first envisaged in ETSI was known as the TETRA Voice plus Data (V+D) standard [17]. Because of the need to further evolve and enhance TETRA, the original V+D standard is now known as TETRA Release 1. An overview of the network elements covered in the TETRA standard is shown in Fig. 2.

1) Switching and Management Infrastructure (SwMI): The abbreviation SwMI is used to classify all of the equipment and sub-systems that comprise a TETRA network, including base stations.

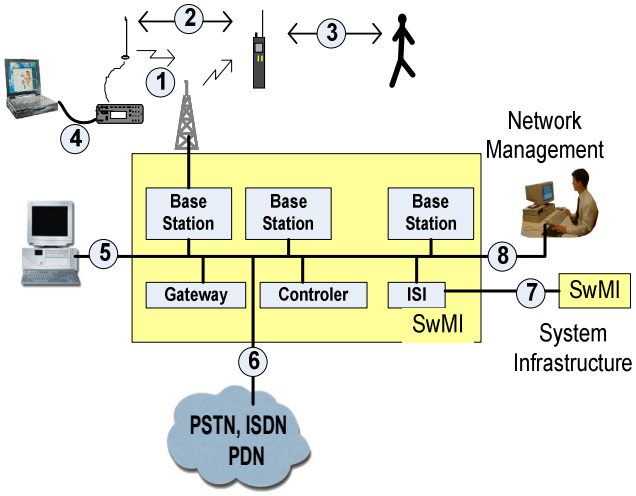

Figure 2. TETRA Standard Interfaces

Even though some ETSI Technical Committee (TC) TETRA members felt that a standard base station interface would be useful (as provided in GSM) it was decided that owing to the way in which different manufacturers configure their networks for optimum performance and design flexibility, it would be impractical to implement.

It was also agreed, for the same reasons as the base station interface, that everything contained inside the SwMI would not be standardized, thereby allowing TETRA infrastructure manufacturers flexibility in design, and the ability to differentiate their portfolio offerings, when in competition with other TETRA manufacturers. This practical approach also meant that new technologies in the areas of transmission and networking could be used without having to go through a long standardization process.

2) Air Interfaces (1 & 2): The most important (and complex) interfaces are considered to be the 'air interfaces' between the base station and radio terminals (1) and the Direct Mode Operation (DMO) interface (2). DMO is a facility that allows terminals to operate in local radio nets independent of the main TETRA network infrastructure.

3) Peripheral Equipment Interface (PEI) (4): This interface standardizes the connection of the radio terminal to an external device, and supports data transmission between applications resident in the device and the connected TETRA radio terminal. The PEI also supports certain elements of control within the radio terminal from the external device and/or application.

4) Remote Dispatcher Interface (5): This interface was originally intended to allow connection to remote wire line dispatcher consoles like those located in major control rooms. Unfortunately, work on this interface was dropped in ETSI TC TETRA as the complexity to provide a universal interface without degrading performance was impractical. This was because the personal mobile radio (PMR) industry had specialist manufacturers of control room equipment, the majority of which differed in the way they interfaced to PMR networks. Similarly, the TETRA network architecture of manufacturers also differed adding to the complexity of providing a universal interface. For these reasons only TETRA manufacturer specific interface specifications are available to support the many voice and data applications requiring access to TETRA infrastructures.

*5) PSTN/ISDN/PABX (6):*This standardized interface enables TETRA to interface with the PSTN, the ISDN and/or a PABX.

*6) Inter-System Interface (7):*This standardized Inter-System Interface (ISI) allows infrastructures supplied by different TETRA manufacturers to inter-operate with each other allowing interoperability between two or more networks. There are two methods of interconnection in the standard, one covering information transfer using circuit mode and the other using packet mode.

7) Network Management Interface (8): Like the local dispatcher interface, it was recognized during standardization activities that a common network management interface was impractical. Fortunately, this early standardization was not wasted as it was later turned into a comprehensive guide to assist users in defining network management requirements.

Besides these network element standards, the many services and facilities available on TETRA are also standardized. The most significant of these being:

- Advanced and fast group call services - clear and encrypted
- Individual calls - clear and encrypted
- Short Data Services - clear and encrypted
- Packet Data Services - clear and encrypted

Each TETRA carrier is spaced at 25 kHz intervals and supports 4 calls. In a typical 400 MHz system there is 10 MHz duplex spacing between the transmit and receive frequencies (45 MHz for 800 MHz systems). Each TETRA carrier is divided into four time slots as shown in Fig. 3. A TETRA call is allocated one of four time slots on a particular downlink carrier frequency for mobile station (MS) reception, and the corresponding time slot on the corresponding uplink carrier frequency for MS transmission. Each time slot can be occupied by a burst which contains traffic in two fields and a number of bits which aid the terminal in synchronizing to the air interface signal.

At the base station the burst signals for four separate calls are assembled into one TDMA frame and these TDMA frames are organized into a structure of multi-frames and hyper-frames. Radio performance testing is concerned with the bursts in the timeslots. Terminals use the timing information from the received signal to judge when they should transmit to the base station in their allotted time slot.

We assume that the channel bit rate is 5Mbps and N operators can share the cell radio resource (channel rate). Each operator has number of MS. The transmission rate of each operator's MS is scheduled on time-slot basis. For each slot, the scheduler allocates adequate service rates to the N operators, using M-TDGPS scheduling procedures, to guarantee the capacity share requirements of all the operators in a fair manner.

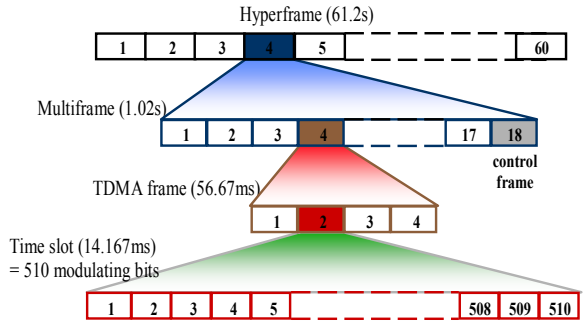

Figure 3. TETRA TDMA

 ISBN: 978-1-61208-142-7

After assigning each operator j its fair service rate, its local scheduler allocates adequate service rates to its flows to guarantee the QoS requirements of all the traffic classes within operator j in a fair manner. The scheduler within each operator can be designed independent of other operator scheduler. Each operator implements its own call admission control, which attempts to control its own arrival traffic.

The new RRM system model is shown in Fig. 4. When a mobile terminal wants to connect, it needs to send a connection requests using the random access channel (RACH). When this request is received at the base station (BS), the multi-operator call admission control (CAC) scheme is first used to check the admission of the connection request of an operator. If the result is positive, the connection request belonging to this operator is accepted and becomes ready for traffic transmission. This is called the admitted connections. When packets for an operator are available for transmission, they need to be scheduled according to their QoS and bit error rate (BER) requirements as a second phase using the uplink scheduler. However, how the packets of this operator's connections are transmitted in each frame is determined by our proposed M-TDGPS scheduling scheme. Therefore, the M-TDGPS scheme employs the dynamic rate allocation among operators in order to increase the overall system utilization and use the GPS model in order to insure the fairness amongst operator when allocating the shared resource. After allocating each operator its resource the TDGPS is then used within each operator to schedule its traffic class.

Two types of services are considered in this study. These two types are: 1) Real-time traffic (RT) such as voice or video, 2) non-real-time traffic (NRT) such as data traffic. The required QoS in terms of delay and BER are different for each of these traffic types. In the next sections, the detail descriptions of the proposed scheme are presented.

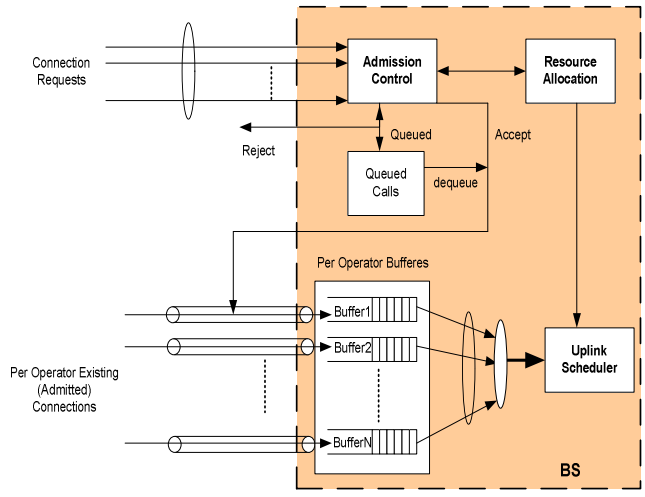

Figure 4. RMM Model for RAN sharing

III. PROPOSED M-TDGPS SCHEMES

The shared resources will be the TETRA channel rate, C, assumed here to be equal to 5 Mbps. We have N operators sharing the same channel. The queuing model of the proposed M-TDGPS scheme is shown in Fig. 5, where the link capacity C is shared by N operators. Each operator has its own assigned soft capacity defined based on the SLA. The assigned weight for operator j is g_j, where $j = 1, 2,\ldots N$. Therefore the total cell capacity in terms of channel rate is divided into N groups. The j^{th} operator maintains two of connections with link rate $C_j(k)$ during the k^{th} medium access control (MAC) slot with capacity $g_j C$.

It is assumed that the traffic characteristic of each input traffic input or stream of the M-TDGPS model is shaped by a Leaky-Bucket regulator [4] in order to achieve a bounded delay and bounded buffer size for traffic queue. Leaky Bucket characterization of a traffic stream is based on specifying two parameters (σ_{ij} , ρ_{ij}) where σ_{ij} and ρ_{ij} are token buffer size and token generate rate, respectively of the leaky bucket. In M-TDGPS scheduling schemes, the allocated resources to an operator $C_j(k)$ during the k^{th} slot can be fixed or adaptive as follows.

A. Fixed rate M-TDGPS

Let c_j is the minimum assigned rate for j^{th} operator such that;

$$c_j = g_j C \quad , j = 1,.., N \tag{1}$$

where g_j is defined based on SLA such that; $\sum_{j=1}^{N} g_j = 1$ and $\sum_{j=1}^{N} c_j \le C$. With this mechanism and at each time slot, an operator j is given $C_j(k) = c_j$ share if there it has a backlogged session. If no packet is ready, then $C_j(k) = 0$ and the unutilized capacity of an operator is not allowed to be used by other backlogged operators. This scheduling called fixed rate (FR) M-TDGPS scheduling and the system can be viewed and multi-independent TDGPS systems. Therefore, the assigned rate for each operator is based on (1).

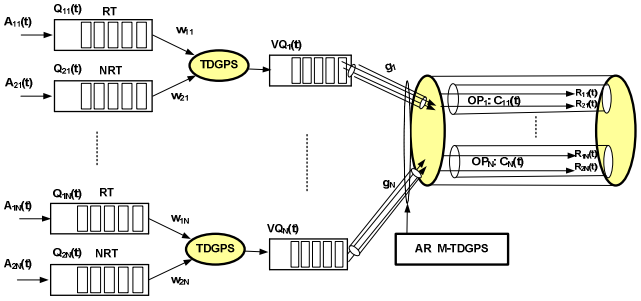

Figure 5. Queuing detail mode for M-TDGPS Scheme

B. Adaptive rate M-TDGPS

In case of an adaptive rate (AR) M-TDGPS scheduling, for each time slot, *T*, first the j^{th} operator is given its minimum c_j as in (1). The unutilized resources, if any, are then specified by;

$$C_r = C - \sum_{j=1}^{N} c_j \geq 0 \quad (2)$$

Then the excess resources are divided amongst the backlogged operator such that

$$c_e = \frac{g_j C_r}{\sum_{\forall i \text{ such that operator}_i \text{ has backlog}} g_i} \quad (3)$$

$$C_j(k) = c_j + c_e \quad (4)$$

The sum of $C_j(k)$ over all the operators should not exceed C in case of adaptive rate and should not exceed $g_j C$ in case of fixed rate allocation. The assigned capacity share to each operator j, $C_j(k)$, is also shared by K traffic classes or flows. Each traffic class i within each operator j has its arrival rate (A_{ij}), queue (Q_{ij}), and maintain a connection with link rate $R_{ij}(k)$ during the k^{th} MAC slot. The sum of $R_{ij}(k)$ over all classes of one operator j should not exceed $C_j(k)$. The procedure used to assign the link rate is explained in the next subsection.

C. The M-TDGPS Procedure

The M-TDGPS procedure is defined as follows. Consider a queuing system of TETRA uplink channel rate with link transmission rate of C. Let $W_j(\tau, t)$ be the amount of operator j traffic served during interval of $(\tau, t]$. Each operator j link is associated with a positive real weight, g_j, j=1,.., N.

Let $S_{ij}(k)$ be the amount of session i traffic of operator j served during the time slot k out of the $W_j(\tau, t)$ that was assigned to its operator. Each traffic i of operator j link is associated with a positive real weight, w_{ij}, i=1,.., K selected based on QoS requirement of this traffic class. Let the scheduling period of M-TDGPS scheme, i.e. the slot length, be T. The M-TDGPS server will allocate each $C_j(k)$ and $R_{ij}(k)$ for each operator j and its individual traffic i, respectively using the following steps.

- Let $OB_j(k)$ be the total amount of backlogged traffic for operator j during the time-slot k, and $B_{ij}(k)$, be the total amount of backlogged traffic of class i of operator j during the time-slot k, such that $OB_j = \sum_{i=1}^{K} B_{ij}(k)$.
- Using $OB_j(k)$, the $W_j(k)$ and $S_{ij}(k)$ are determined as follows. If $OB_j(k)=0$, then $W_j(k)=0$ and $S_{ij}(k)=0$ for all i. If $OB_j(k)> 0$, then $W_j(k)= c_iT$ and $S_{ij}(k)= r_{ij}T$ for all $B_{ij}(k)>0$, where c_i is the minimum capacity share guaranteed to operator j, and r_{ij} is the minimum rate guaranteed to traffic i form the assigned capacity share of its corresponding operator j. c_i and r_{ij} are calculated as follows:

$$c_i = \frac{g_i C}{\sum_{j=1}^{N} g_j} \quad (5)$$

$$r_{ij} = \frac{w_{ij} C_j(k)}{\sum_{i=1}^{K} w_{ij}} \quad (6)$$

The session i with $B_{ij}(k)=0$ will have $S_{ij}(k)= 0$ and $w_{ij}(k)=0$.

- After assigning each operator its $W_j(k)$ then , in case of adaptive rate scheduling if $\sum_j W_j(k) < CT$, then the remaining unused resource is distributed to the operators who need more than their guaranteed service c_iT. The distribution of the remaining unused resource should be in proportion to each operator's weight g_j, according to the M-TDGPS service discipline as shown in (4). When an operator j receives part of the unused capacity, it will be distributed to its traffic who need more than their guaranteed service $r_{ij}T$ in proportion to each traffic's (session) weight w_{ij}.
- Finally the allocated channel rate to each operator j and to each backlogged operator traffic i can be determined by $C_j(k)= W_j(k)/T$ and $R_{ij}(k)= S_{ij}(k)/T$, respectively.

IV. SIMULATION RESULTS

In this section, simulation results are presented to demonstrate the performance of the proposed M-TDGPS scheme in terms of delay and system throughput only due to paper limitation. Throughput is calculated as the average number of served packets per second. C++ is used to build the simulation model. Based on the characteristic of TDMA wireless physical layer, the scheduling period T is 14.167 ms as shown in Fig. 3. In simulation, the M-TDGPS scheme is compared in case of adaptive rate (AR) M-TDGPS and fixed rate (FR) M-TDGPS under heterogeneous traffic environments. The total bandwidth is assumed to be a constant C=5Mbps assuming we have the new generation of TETRA Networks. Three operators are considered (N=3) each operator is assigned different weight based on SLA. We assumed that each operator is given (g_j=1/3) of the bandwidth as a minimum. All operator follows are modeled by a Poisson process with average arrival rate λ and packet length L shaped by a leaky-bucket regulator for providing bounded delay. In this simulation L=512 bits which is the maximum size of data frame, σ_{ij} =100L, ρ_{ij} =C/6, and λ can be varied in order to change the system load.

In the following experiments, the traffic loads of operator 2 (OP2) and operator 3 (OP3) is fixed to 512 Kbps and the traffic loads of operator 1 (OP1) is varied. The system throughputs and the average packet delay versus offered traffic are depicted in Fig. 6 and Fig. 7. The offered traffic is

 ISBN: 978-1-61208-142-7

calculated as the total of all operators' traffics (Packets per second).

Fig. 6 shows the system throughputs comparison in case of fixed rate (FR) and adaptive (AR) rate M-TDGPS. The traffic loads are the sum of average arrival rates of the 6 data follows (two per operator).

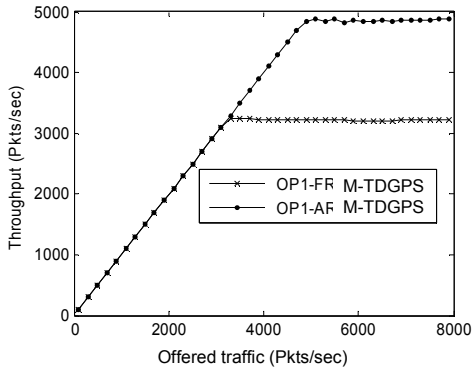

Figure 6. System Throughputs

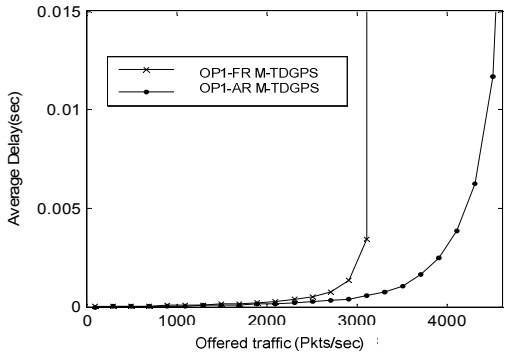

Figure 7. Average packets delay.

As expected the throughputs of adaptive rate M-TDGPS is higher in case of using adaptive rate because of using the concept of utilizing the unused resources of other operators. Hence the system throughputs increase. Fig. 7 shows the average delay with different system loads. In this figure it can be seen that the average delay performance of adaptive M-TDGPS is better than M-TDGPS with a fixed capacity per operator. In adaptive M-TDGPS, the unused resources can be distributed amongst the backlogged flows. Therefore, more packets can be served.

V. CONCLUSION

An efficient adaptive rate M-TDGPS scheme has been proposed for supporting multi-services in the uplink of TETRA networks with multi-operators. The simulation results show that the proposed scheme can improve both system utilization and average delays. The proposed scheme allows for a flexible trade-off between the GPS fairness and efficiency in resource allocation and is an effective way to maximize the radio resource utilization under the fairness and QoS constraints.

REFERENCES

[1] S. AlQahtani and U. Baroudi, “An Uplink Performance Evaluation for Roaming-Based Multi-Operator WCDMA Cellular Networks,” 4th ACS/IEEE International Conference on Computer Systems and Applications, UAE, March 8-11, 2006, pp. 376-380.

[2] Third Generation Partnership Project (3GPP), “Network Sharing; Architecture and functional description (Release 6),” Technical specification TS 23.251, version 2.0.0, June 2004.

[3] Siemens AG, “3G Infrastructure Sharing - The Siemens Perspective,” available at http://www.siemens.com (accessed on 20 Feb. 2011).

[4] A. Parekh and R. Gallager, “A generalized Processor Sharing Approach to Flow Control in Integrated Services Network-The Single Node Case,” IEEE/ACM Transactions on Networking, , vol. 3, No 1,June 1993 ,pp. 344-357.

[5] A. Parekh and R. Gallager, “A generalized Processor Sharing Approach to Flow Control in Integrated Services Network-The Multiple Node Case,” IEEE/ACM Transactions on Networking, vol. 13, No 6, April 1994, pp. 137-150.

[6] Z. Zhang, D. Towsley, and J. Kurose, “Statistical Analysis of the Generalized Processor Sharing Scheduling Discipline,” IEEE J. Select. Areas Commun., vol. 13, No 6, August 1995, pp. 1071-1080.

[7] P. Ramanathan and P. Agrawal, “Adapting Packet Fair Queueing Algorithms to Wireless Networks,” Proc. ACM/IEEE MOBICOM’98, Oct. 1998, pp. 1-9.

[8] M. Arad and A. Leon-Garcia, “A Generalized Processor Sharing Approach to Time Scheduling in Hybrid CDMA/TDMA,” Proc. IEEE INFOCOM ’98, March 1998, pp. 1164-1171.

[9] T. Nandagopal, S. Lu and V. Bharghavan, “A Unified Architecture for the Design and Evaluation of Wireless Fair Scheduling Algorithms,” Wireless Networks, vol. 7, Aug. 2002, pp. 231-247.

[10] D. Stiliadis and A. Varma, “Efficient Fair Queueing Algorithms for Packet-Switched Networks,” IEEE/ACM Trans. Networking, vol. 6, April 1998, pp. 175-185.

[11] A. Varsou and H. Poor, “An Adaptive Rate Processor Sharing Technique,” Proc. IEEE Vehicular Technology Conf., Oct. 2001, pp. 2584-2588.

[12] L. Shen, and J. Mark, “Dynamic Fair Scheduling With QoS Constraints in Multimedia Wideband CDMA Cellular Networks,” IEEE Trans. Wireless Comm., vol. 3, No. 1, Jan. 2004, pp. 60-73.

[13] L. Shen, and J. Mark, “Fair Resource Allocation with Guaranteed Statistical QoS for Multimedia Traffic in WCDMA Cellular Network in Wideband CDMA Cellular Networks,” IEEE Trans. Mobile Computing, vol. 4, No. 2, April 2005, pp. 166-177.

[14] A. Stamoulis and G. Giannakis, “Packet Fair Queueing Scheduling Based on Multirate Multipath-Transparent CDMA for Wireless Networks,” Proc. IEEE INFOCOM, 26-30 March 2000, pp. 1067-1076.

[15] X. Wang, “An FDD Wideband CDMA MAC Protocol for Wireless Multimedia Networks,” Proc. IEEE INFOCOM, 30 March-3 April 2003, pp. 1067-1076.

[16] R. State, K. El-Khazen, G. Martinez, and G. Vivier, “Service management for multi-operator heterogeneous networks". IEEE GLOBECOM, 17-21 Nov. 2002, pp 2069-2073.

[17] http://www.tetramou.com (last accessed on 20 Feb. 2011)

[18] D. Axiotis and A. Salkintzis, “Packet data messaging over TETRA: network performance Analysis,” Wireless networks, vol. 16, No 4, July 2009, pp. 1189-1198.

 ISBN: 978-1-61208-142-7

Towards Neutrality in Access Networks: A NANDO Deployment with OpenFlow

Jon Matias, Eduardo Jacob, Nerea Toledo, Jasone Astorga
University of the Basque Country (UPV/EHU)
Bilbao, Spain
{jon.matias, eduardo.jacob, nerea.toledo, jasone.astorga}@ehu.es

***Abstract*—A next step in the evolution of Access Networks introduces a scenario in which the fair competition among service providers is enabled through the sharing of access infrastructure. CAPEX savings or regulatory aspects are currently promoting such a scenario. By adding neutrality, the positive feedback loop includes customers, service providers and network operators. The NANDO project implements a new layer 2 approach for Neutral Access Networks. This NAN proposal includes a network operator selection mechanism, a secure instantiation of services and a prefix-based forwarding approach (Ethernet-PF). The OpenFlow technology has been selected for its deployment. OpenFlow is a protocol by which an external entity (controller) can control/modify the flow table of a switch, which rules the forwarding process. This paper is focused on describing the NANDO scenario and the most relevant implementation details related to OpenFlow. In addition, a detailed description of the developed controller and its operational model are shown, including some representative examples. Finally, the functional feasibility of NANDO is validated in a scenario where multiple operators share the same physical infrastructure for service delivery.**

Keywords–Neutral Access Networks; OpenFlow; Access Control; Authentication and Authorization; Carrier Ethernet

I. INTRODUCTION

This paper introduces the NANDO project (Neutral Access Network Demonstrator over OpenFlow), which has been accepted for its deployment over Federica [1]. The experiment was proposed by the I2T Research Group from the University of the Basque Country (UPV/EHU, Spain) in collaboration with the TSLab from the Royal Institute of Technology (KTH, Sweden). A new Federica slice was defined and assigned to this project, once it was accepted by the User Policy Board. The Federica facility provides a virtual infrastructure for researchers who want to test their proposals for Future Internet, such as protocols or applications, in a large-scale scenario.

The NANDO project introduces a pure layer 2 (Data Link Layer) approach [2] to get neutrality in next generation access networks. The main idea behind this proposal is that each customer is able to select the network operator when requesting access to a service. The service is anything (video, voice, data) that demands a specific handling in the access/aggregation network. This means that the service provider is able to impose some requirements to the network operator. Therefore, the delivery of certain services, such as video on demand (VoD) or videoconferencing, requires the support from network operators to ensure a certain QoS.

The Neutral Access Network (NAN) approach includes a network operator selection mechanism, a secure instantiation of services and a prefix-based forwarding proposal (Ethernet-PF). Moreover, network virtualization and resource sharing are fundamental issues to overcome in order to achieve neutrality on the access. This means that the same access network is shared simultaneously by multiple network operators.

The main focus of this paper is the implementation of NANDO proposal by using the OpenFlow technology [3]. Due to its commercial support by major vendors (such as Juniper, HP or NEC), this technology enables the NAN approach to be deployed in real scenarios and production environments. OpenFlow has been developed at Stanford University (Clean Slate) and selected by several projects as the enabler for innovation in future networks, such as E-GENI in USA or Ofelia, Change and Sparc in Europe.

OpenFlow is a flow-oriented technology which splits up the control plane from the forwarding process. In this context, an external entity – the controller – is able to control the switching of packets by defining the forwarding table through a standard interface, the OpenFlow protocol. It was originally conceived as a way of supporting research experiments in production networks, but has evolved into network service architectures such as the NOX [4] and Software Defined Networks (SDN) [5].

The rest of the paper is organized as follows. In Section II, several OAN/NAN proposals are analyzed and related to our approach. Then, the NANDO scenario is described and the main contributions are briefly described in Section III. Afterwards, Section IV describes the platform implementation process and how each of the aforementioned contributions has been developed and deployed with OpenFlow. Finally, Section V sums up some final conclusions from this paper.

II. OAN/NAN PROPOSALS

Open Access Network (OAN) has been proposed [6] to bridge the digital divide and enhance the Internet penetration by enabling the fair competition among service providers on a shared access infrastructure (between users and services). The access network is shared with independent edge nodes for all service providers. Neutral Access Network [7] (NAN) is a special type of OAN which grants positive externality to share infrastructure, by making the access network visible to

 ISBN: 978-1-61208-142-7

end users, rather than transparent. Therefore, some services are available to users within the access network before they get access to the service edge node.

In the context of OAN and NAN, there are several technical proposals [8] [9], which try to deal with the requirements imposed by an open or neutral approach. The first proposal [10] is based on DHCP relay, which forwards the DHCP related traffic to the DHCP server associated to the service provider (selected by a captive portal). The same layer 2 network is shared by all the users, which are configured with an IP address from a different subnet depending on the service provider. The second proposal is based on Linux policy routing [9], which makes use of a captive portal for selecting the service provider and source routing for transmitting the packets to the appropriate provider. The third proposal [11] makes use of tunneling to establish a point-to-point connection between the user and the service provider. The available tunnel servers and the service provider associated to each of them should be provided to end users. The forth proposal [8] is only available for WLAN, since it uses multiple SSIDs to distinguish among different service providers. The fifth proposal is based on the CAPWAP protocol (RFC 5415), which allows to assign a different VLAN to the user depending on the 802.11i authentication process. Finally, the sixth proposal [8] is related to the use of IMS in the context of WLAN, which is supported by the 3GPP.

The NAN proposal presented in NANDO is not designed for a wireless scenario. So, the last three proposals are not considered for a further analysis. The first and second proposals make use of a captive portal to select the service provider and then the layer 3 information (e.g., subnet or source IP) is used to distinguish among the target providers. Opposite to these approaches, NANDO is based on layer 2 information, Ethernet services (as described by the Metro Ethernet Forum [12]), to differentiate the target provider. Finally, instead of tunneling all the traffic in point-to-point connections, like in the third proposal, the NANDO approach does not encapsulate the Ethernet frames; thus, reducing the overhead and being more efficient in multipoint scenarios.

Apart from the previous considerations, the main difference is that NANDO enables an environment not only for multiple service providers, but also for multiple network operators providing services over the same access network infrastructure. For this purpose, a new approach for network virtualization is introduced, which is based on the MAC addressing scheme. In this context, the user is able to select the network operator before accessing the services. The selection process is similar to the WLAN association and the use of SSIDs.

If we take a look to the current broadband access architecture (described by the Broadband Forum [13]), the PPPoE is used between the users and the L2TP Network Server (LNS) that is connected to the service providers, and L2TP is used between the L2TP Access Concentrator (LAC) and LNS. The LAC checks the provider, whereas the LNS checks if the user is valid by using a RADIUS server. The architecture supports the introduction of multiple service providers or LNS in the same infrastructure by using multiple point-to-point connections. The main concern is how the services are discovered by users.

On the other hand, the NANDO project introduces a scenario in which no PPP encapsulation is used between users and service providers. The flow definition, introduced by OpenFlow, is used to identify each service and forward traffic from users to the corresponding provider. This approach enables the use of Ethernet frames from end-to-end, reducing the overhead present in tunneling solutions.

Comparing the current broadband proposals and NANDO, there are some key aspects to consider. The former is based on PPP/PVCs for service delivery, which introduces some overhead at data path, whereas the later is based on flows and VLANs. The multicast support is another relevant issue when delivering services, which is not well supported by PPP, since multipoint requires complex mesh networks. On the other hand, multicasting and multipoint capabilities are well supported by Ethernet technology. Furthermore, the authentication capabilities of PPP are quite limited (PAP/CHAP), whereas the IEEE 802.1X introduces an extensible framework for authorization (EAP).

III. THE NANDO PROJECT

The NANDO experiment consists of the deployment of a neutral access network based on OpenFlow switches in which two different network operators are deployed sharing the same physical infrastructure and resources. Each operator provides a set of services to authorized users. At first step, at least one service provider is located in the TSLab at KTH (Sweden), while the customers are located in the I2T Lab at UPV/EHU (Spain). Figure 1 shows the interconnection scenario between both labs, which consists of a not fully meshed group of 5 OpenFlow user space switches (Open vSwitch [14]) along with 2 more machines with the Openflow controllers and the servers (provider selection and AuthN/AuthZ services). At the UPV/EHU premises, NetFPGA [15] devices and IP8800 NEC [16] commercial switches are employed to support experimental traffic in the campus network without disturbing production traffic.

The idea behind this platform is to test he operational issues related to a neutral scenario under real conditions, in which two different network operators (represented by KTH and UPV/EHU) share the same physical infrastructure (from Federica) to deliver the services provided by a third party. Although for implementation feasibility reasons there are

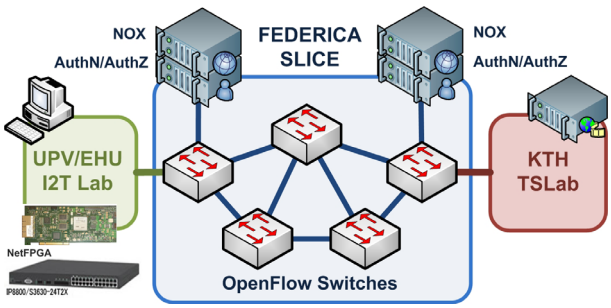

Figure 1. The NANDO Slice

only two entities (KTH and UPV/EHU), the network operator and service provider are supposed to belong to different entities.

Due to space limitation, this section just briefly describes the main contributions of NANDO proposal presented in [2].

A. *Provider Selection Mechanism*

The provider selection mechanism allows customers to freely decide which network operator they want to use before accessing the network and requesting the service. It is a layer 2 service discovery mechanism composed by a scanning phase and a setup phase. First, the customer scans the list of available network operators at its current location. Then, depending on the operator's identity or the services available behind each operator, the customer selects one of them and starts the setup phase. In this step, the customer requests a layer 2 configuration according with the selected network operator. Finally, the end user equipment creates a new virtual interface configured with the leased parameters, such as the MAC address.

B. *Secure Instantiation of Services*

A new procedure for a secure instantiation of services is also implemented as an extension to the Generic AAA Architecture (RFC 2903). The new AAA environment introduces new requirements to deal with. In this context, the service provider must authenticate its customers when requesting the services and impose a set of requirements to the network operator in order to successfully deliver the services. Here, aspects like policy enforcement and obligation handling are addressed.

The basic idea is that after a successful authentication of the customer, the service provider generates a set of profiles which describe the requested service. These profiles are submitted to the network operator to check if all the requirements can be fulfilled. In affirmative case, the operator must establish the path for the service and configure the edge node with the associated access control rules.

C. *Prefix-based Forwarding (Ethernet-PF)*

As a technical solution to overcome the virtualization of the neutral access infrastructure and the distinction (and even isolation) of traffic from one network operator to another, the prefix-based forwarding approach is proposed. By using this approach, the traffic can be easily associated to its operator just by inspecting the prefix (e.g., first byte) of the MAC address. For this, the mechanism described in Section III.A is essential. Once the customer configures the new MAC address leased by one operator, the traffic generated by this interface is handled by the same operator.

If all the MAC addresses leased by a certain edge node have the same prefix (e.g., first 3 bytes), all the traffic to/from users behind this edge node can be identified with a single forwarding rule, thus reducing the flow tables of core nodes. With such a solution, the complete VLAN range is available for each network operator, which eases the network management and inter-operator agreements. The only agreement needed per NAN domain is the very first prefix used to identify each operator.

IV. PLATFORM IMPLEMENTATION

This section is focused on the implementation aspects and OpenFlow related issues concerning NANDO. As previously mentioned, in OpenFlow the flow table is managed by an external entity, the controller. The NOX is the main open-source project which develops an OpenFlow controller, and is used by NANDO. Each and every packet that enters an OpenFlow switch is compared to the flow table, and if no previously defined rule is matched, the packet is encapsulated and transmitted to the controller. Once the packet arrives to the controller, it is analyzed to determine what should be done, and maybe to activate new rules in the flow table in order to handle the packet.

Figure 2 shows a high level view of the platform implementation which represents the main functional blocks and interactions among them. The OpenFlow protocol is used to exchange information between two different entities: the OpenFlow switch and the OpenFlow controller. The OF switch is responsible for forwarding both data and control traffic, which is sent through the downstream interface to/from the users. The upstream interface is used to send the control packets to the appropriate servers (e.g., AuthN/AuthZ or Provider Selection) and the data packets to/from the aggregation network. The NOX controls the behavior of the switch by inserting/removing forwarding rules.

Mainly there are 3 different types of traffic handled by a separate functional block at the NOX. The Provider Selection Traffic Handler receives the selection control packets and inserts the forwarding rules which enable its later exchange between the user and the Provider Selection server. On the other hand, the AAA Process Traffic Handler receives the AAA packets and inserts the forwarding rules which enable the AAA protocol between the user and the AuthN/AuthZ server. This module has also an interface with the AuthZ server to receive the final authorization decisions, which carry the access control rules for inserting/removing new forwarding rules (depending on the AAA process). Finally, the Prefix-based Data Forwarding Decision module

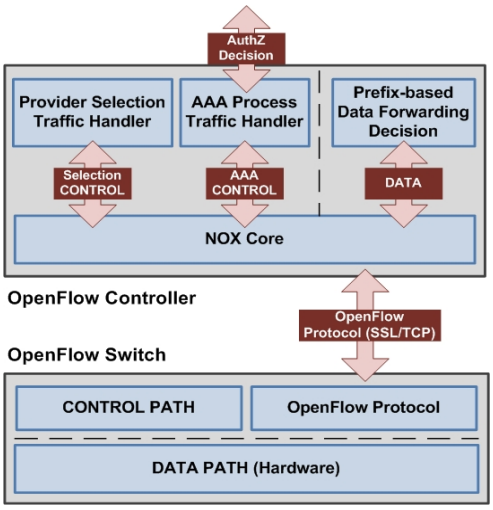

Figure 2. High Level View of the Platform

is the responsible for the data plane. Following the Prefix-based Forwarding approach (Ethernet-PF), the forwarding is based on the first 3 bytes (depending on the prefix length) of the destination MAC address, instead of the whole address. The complete approach relies on the previous controlled distribution of locally administrated MAC addresses provided by the selection mechanism to the end users before accessing the network. Figure 3 introduces a simplified view of the entities and exchanges involved in this process.

A. *Provider Selection Traffic Handler*

As previously introduced in Section III.A, the network operator selection mechanism is based on a client-server protocol. The final outcome is the creation of a new virtual network interface at the client side, with the appropriate configuration for later access to operator. In Linux, this is easily done through the following command:

```
# ip link add link eth0 name veth0 address Leased_MACAddress type macvlan
```

In order to integrate this selection mechanism with OpenFlow, a detailed description of the associated traffic is necessary: a specific ethertype (0x0110) and a multicast address (01:00:5E:90:00:00). First of all, the client sends the scanning request with the aforementioned ethertype to the known multicast address and from its globally administered MAC address (assigned by the NIC's manufacturer). There could be multiple responses to the initial scanning request, with same ethertype, from the server MAC address (unicast) to the client's NIC. After some time (configurable), all the offers from available operators are presented to the client in order to select among them. A unicast setup request/response is sent between the customer's NIC and the selected server.

Regarding OpenFlow, the previously described exchange involves the definition of at least three different flows: the initial multicast flow, both unicast responses (which are exactly the same) and the unicast setup request. The flow registration process is as follows. When a new scanning request comes into the OF switch from the new customer, the packet is redirected to the NOX controller, which checks the ethertype (identified as selection protocol). Then, the NOX enters the learning process and register the physical port associated with the calling station (the NIC address from the customer). At this point, it must be said that all the servers (from network operators) must be previously registered at NOX, which means that their MACs are known.

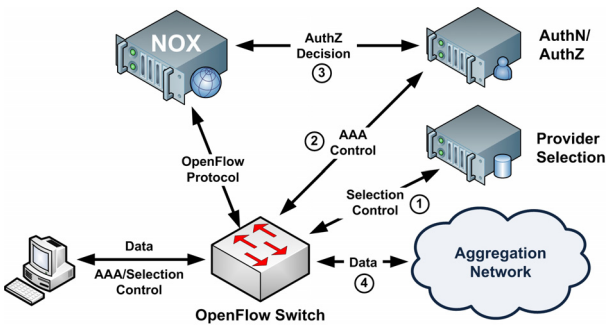

Figure 3. Entities and Exchanges

Due to the temporary nature of the selection process, the rules are charged for a short period of time. In the simplest scenario, the selection process related rules are:

```
DstAddr: 01:00:5E:90:00:00, SrcAddr: NIC_Address, Ethertype: 0x0110, InPort: Learned_Port => Action: Server_Port
DstAddr: NIC_Address, SrcAddr: Server_Address, Ethertype: 0x0110, InPort: Server_Port => Action: Learned_Port
DstAddr: Server_Address, SrcAddr: NIC_Address, Ethertype: 0x0110, InPort: Learned_Port => Action: Server_Port
```

B. *AAA Process Traffic Handler*

This section describes the handling of AAA related traffic with OpenFlow. The secure instantiation of services is based on a modified extension of IEEE 802.1X standard. The standard defines three entities that take part in every AAA process: the supplicant, the authenticator and the authentication server. The traffic relevant to OpenFlow is the exchange of packets between the supplicant and the authenticator, by using the EAPoL protocol. This traffic is completely identified by its ethertype (0x888E) and multicast address (01:80:C2:00:00:03). However, the implemented and deployed solution extends the EAPoL protocol to enable multiple simultaneous AAA processes from the same customer's MAC address. This is essential for requesting multiple services by using the same network operator. Standard and non-standard EAPoL could be distinguished by the version field.

The flow registration process is as follows. Once the client has the new delegated MAC address from the network operator, the authentication process starts on the new virtual interface. Therefore, a new packet with ethertype 0x888E is sent from the new address to the multicast address. Since there is no previously defined rule to handle this traffic, the packet is encapsulated and redirected to the NOX controller. The NOX identifies the ethertype as AAA traffic and checks the multicast address. Then, the learning process takes place and registers the physical port associated with the leased MAC. The authenticator is supposed to be an internal process from the switch, but this is not an option when dealing with an OF switch. Consequently, the authenticator is running on an external machine directly attached to one of the known physical ports of the switch. With this information both rules can be easily defined:

```
DstAddr: 01:80:C2:00:00:03, SrcAddr: Leased_Address, Ethtype: 0x888E, InPort: Learned_Port => Action: Authenticator_Port
DstAddr: Leased_Address, SrcAddr: 01:80:C2:00:00:03, Ethtype: 0x888E, InPort: Authenticator_Port => Action: Learned_Port
```

Up to this point the EAPoL is the only traffic allowed. However, after the AAA process takes place, a predefined traffic from the customer to the provider needs to be enabled.

After a successful authentication (AuthN) process, the authorization (AuthZ) stage takes place. In this step, the AuthZ server determines if the customer is allowed to get access to the requested service and generates a profile describing the service and associated parameters. This profile is needed both for controlling the access and setting up the

 ISBN: 978-1-61208-142-7

connectivity. The former is described in this section, whereas the latter is dealt with in the next Section IV.C.

First of all, a new communication channel with the NOX controller is needed. Opposite to previously described mechanism of sending packets from the OF switch to the NOX, in this case an asynchronous channel from an external entity (the AuthZ server) is required. For that purpose, a web service based on REST is enabled at the NOX controller (Figure 4). Therefore, a new REST client is implemented and launched once the AuthZ generates the profile. For optimization reasons, the profile is transmitted to the NOX controller in JSON format. Once the JSON profile gets into the controller, it is parsed to obtain the needed parameters to activate the new access from the client to the service.

Let us consider a simple example: the client requests a new service to get access to Internet. In this case, the service can be identified at flow level as IP traffic from the client's MAC address to the gateway's MAC address, and vice versa. The rules that should be activated are the following:

DstAddr: Gateway_Address, SrcAddr: Leased_Address, Ethtype: 0x0800, InPort: Learned_Port => Action: Gateway_Port
DstAddr: Leased_Address, SrcAddr: Gateway_Address, Ethtype: 0x0800, InPort: Gateway_Port => Action: Learned_Port

C. *Prefix-based Data Forwarding Decision*

One of the main contributions from this NAN proposal is the prefix-based forwarding mechanism (or Ethernet-PF), built upon the delegation of addresses from network operators to its customers. In this context, only a certain part of the MAC address, defined by a prefix (e.g., first 3 bytes), is enough to determine the physical output port for the packet. That is why in NANDO project, it is only necessary to identify the edge switches for forwarding decisions, which drastically reduces the size of forwarding tables.

Let us consider that the 5 OF switches from the platform are edge switches. This means that only five rules are needed at each OF switch to locate all the possible customers behind those edge switches. Furthermore, each network operator is able to define multiple paths among edge switches by using VLAN tagging. To get the total number of rules those five rules must be multiplied by the number of VLANs. On the other hand, in current switches, the Spanning Tree Protocol is used to get a loop free topology by blocking ports that generate loops. Then, the learning phase takes place to learn all the MAC addresses (one rule per customer) and its associated port. Also, Multiple STP could be enabled to get different topologies associated to different VLAN id's. The learning process is repeated per VLAN. Consequently, Ethernet-PF drastically reduces the forwarding tables and the time, since the MAC's learning process is not further needed.

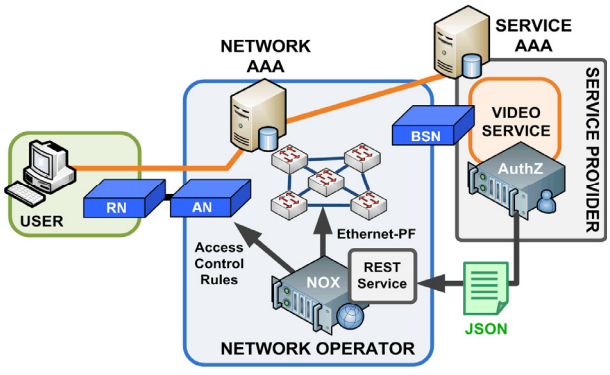

Figure 4. REST Service at NOX (JSON profile)

Regarding the Ethernet-PF implementation, the current OpenFlow version 1.0 does not support MAC-subnetting, but it is to be supported by the next release, version 1.1. So, three options have been considered to get prefix-based forwarding up and running in NANDO. First option is to use the current Ethernet-PF prototype developed with Click tool [17]. Although there is a basic support for OpenFlow in Click (OpenFlowClick) the OFv1.1 is not yet supported. The second option is to hack both NOX controller and OF switch software to add this support. But adding this support to vendor switches (IP8800 NEC) is not possible. The third option is to process all packets by the controller, since at this point the complete packet is available and wildcard matching could be done even at bit level. The problem is the performance of the final platform, since all packets are relayed to the controller. Finally, and mainly due to the mixed infrastructure, with both vendor and software switches, the third alternative is selected.

First of all, a loop free topology is generated with a function developed for NANDO. In this case, the nodes' physical layout is known in advance, so this simplifies the implementation. Then, the controller should register the rules at the OF switches pointing out the defined physical output for each edge switch. Since there is no option for this until version 1.1, the rules are defined and recorded at NOX. A new function has been developed to return the physical output port associated with those records, the idea is to emulate the desired behavior. At this point, each packet that comes into one of those OF switches is relayed to the NOX, and thanks to that function, the output is easily obtained. Then, the packet is forwarded through the predefined port. Of course, the prefix from MAC address (which defines the network operator) and the VLAN id (which defines the topology) are taken into account by this function.

Since network behavior is centralized at NOX, if any failure (link, switch) is detected and reported to the NOX, an alternative topology is computed and reconfigured. There are several proposals to avoid its scalability problems, such as HyperFlow or Maestro.

D. *NANDO validation*

The previously described platform has been validated at functional level. At the beginning, the idea was to validate the proposal over the Federica infrastructure, but due to several unexpected events the original deployment has been very limited. At the end, the main part has been deployed over the I2T Lab (UPV/EHU) and adapted to be extended over a layer 2 platform from the Spanish NREN (RedIRIS).

Figure 5 shows the validation environment that proves the functional viability of NANDO proposal. There are two users (user A and user B), two service providers (service 1 and service 2) and two operators (operator A and operator B)

 ISBN: 978-1-61208-142-7

sharing the same physical infrastructure. Four different setups have been established at the same time. First, user A selects operator A through the provider selection mechanism and creates a new virtual interface with a MAC address delegated from operator A. Then, user A requests a connection to service provider 1 through the AAA process. After a successful authorization the path1 is configured by the NOX and the flow from user A to service 1 is enabled. In a second stage, user A makes use again of the provider selection mechanism to select operator B. At the end, user A has two virtual interfaces, one per operator. By using the new virtual interface, user A launches a new AAA process to request a new connection to service provider 2. Finally, the path2 from the operator B is enabled for this purpose. A similar procedure takes place at user B. At the end, user B has also two virtual interfaces, one from operator A and another one from operator B, which are used to connect to service 2 (path2) and service 1 (path1), respectively.

As previously mentioned, the lack of support for OF v1.1 invalidates the performance evaluation of the proposal, since due to this limitation all the packets must be processed by the NOX, instead of being forwarded at data level.

V. CONCLUSIONS

As the first and main conclusion, the NANDO project has proved the functional viability of the NAN proposal introduced in ACCESS 2010 [2]. Moreover, the OpenFlow technology has been very useful in a mixed scenario such as NANDO, in which vendor switches, NetFPGAs, Open vSwitch and even WiFi devices (OpenWRT) have been integrated under a common controller (NOX), becoming the technological convergence factor. However, the limited set of wildcard options defined in the current OFv1.0 has significantly restricted the fully support for Ethernet-PF. It is not possible until next release (future work) to implement the complete solution over OpenFlow.

Regarding access control, OpenFlow has confirmed to be an ideal technology to unify forwarding and access control rules, since only defined flows are granted, while the rest of the traffic is discarded.

As presented in Section IV.C, the prefix-based forwarding proposal has demonstrated drastic reductions in the number of forwarding rules. For instance, considering a scenario with 20 edge nodes, 35 core nodes and 100 customers behind each edge node, a fully meshed connectivity with Ethernet-PF needs only 20 rules at core nodes. Furthermore, those rules are isolated from customers and the connectivity is enabled just after configuring the rules (since learning process is disabled).

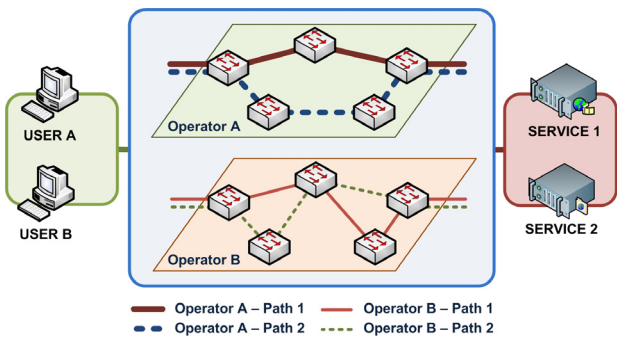

Figure 5. Validation Environment

To conclude, the NANDO project enables a scenario in which customers are able to choose the network operator that they want to use before requesting a service to the provider. Moreover, the same customer is able to select another network operator at the same time to deliver a new service from a different provider. But even more, at the same location (residential or business premises) another customer can select a third network operator to get access to a different service offered by any other provider.

ACKNOWLEDGMENT

This work has been partially funded by the Spanish MICINN project A3RAM-NG (TIN2010-21719-C02-01).

REFERENCES

[1] Federica Project, http://www.fp7-federica.eu, 2010.

[2] J. Matias, E. Jacob, Y. Demchenko, C. de Laat, and L. Gommans, “Extending AAA Operational Model for Profile-based Access Control in Ethernet-based Neutral Access Networks”, The 2nd International Conference on Evolving Internet, pp. 168-173, 2010.

[3] N. McKeown, et. al., “OpenFlow: Enabling Innovation in Campus Networks”, ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69-74, April 2008.

[4] N. Gude, et. al. “NOX: Towards an Operating System for Networks”, ACM SIGCOMM Computer Communication Review, vol. 38, no. 3, pp. 105-110, July 2008.

[5] K.-K. Yap, T.-Y. Huang, B. Dodson, M. S. Lam, and N. McKeown, “Towards Software-Friendly Networks,” in Proceedings of the 1st ACM Asia-Pacific Workshop on Systems (APSys ’10), pp. 49-54, 2010.

[6] R. Battiti, R. Lo Cigno, M. Sabel, F. Orava, and B. Pehrson, “Wireless LANs: From WarChalking to Open Acess Networks,” Mobile Networks & Applications, pp. 275-287, 2005.

[7] A. Bogliolo, “Introducing neutral access networks,” International Conference on Next Generation Internet Networks (NGI 2009), pp. 1-6, 2009.

[8] J. Barceló, A. Sfairopoulou, and B. Bellalta, “Wireless open metropolitan area networks,” SIGMOBILE Mob. Comput. Commun. Rev., vol. 12, no. 3, pp. 34–44, 2008.

[9] A. Seraghiti and A. Bogliolo, “Neutral Access Network Implementation Based on Linux Policy Routing,” The 1st International Conf. on Evolving Internet, pp. 158-162, 2009.

[10] A. Escudero, B. Pehrson, E. Pelleta, J. Vatn, and P. Wiatr, “Wireless access in the flyinglinux.NET infrastructure: MobileIPv4 integration in a IEEE 802.11b,” in 11-th IEEE Workshop on Local and Metropolitan Area Networks, pp.51-53, 2001.

[11] A. Bogliolo, “Urbino wireless campus: A wide-area university wireless network to bridge digital divide,” in Proceedings of AccessNets’07, pp. 1–6, 2007.

[12] Metro Ethernet Forum, http://metroethernetforum.org, 2011.

[13] Broadband Forum, http://www.broadband-forum.org, 2011.

[14] Open vSwitch, http://openvswitch.org, 2011.

[15] NetFPGA devices, http://www.netfpga.org, 2011.

[16] NEC IP8800, http://www.nec.co.jp/ip88n/ip8800_s3630, 2011.

[17] Click tool, http://read.cs.ucla.edu/click, 2010.

 ISBN: 978-1-61208-142-7

A Service-Based Model for the Internet Value Chain

Erika Pigliapoco and Alessandro Bogliolo
University of Urbino
Urbino, Italy 61029
Email: {erika.pigliapoco, alessandro.bogliolo}@uniurb.it

***Abstract*—The exponential growth of Internet traffic is generating revenues which are not fairly distributed among all the actors involved in the value chain. In spite of the increasing returns for over-the-top service providers, application developers, and device producers, network operators and content right owners are not taking advantage of Internet evolution. Analysts forecast that in a few years this imbalance will cause the congestion of the network without any motivation for new investments on it, thus ultimately bringing the Internet to collapse. On the other hand, if properly distributed, the value generated by Internet traffic would be sufficient to sustain innovation and growth. This paper analyses the bottlenecks in the value chain induced by the access-based business models currently adopted by operators. Net neutrality and market law are the pillars which sustain an alternative service-based model granting to the network the degrees of freedom necessary to overcome its own bottlenecks without the need for external enforcement.**

***Keywords*-Internet value chain; Economic equilibrium; Development; Sustainability; Business model**

I. INTRODUCTION

Global mobile data traffic is expected to increase 26 times in 5 years, reaching 6.3 exabytes per month in 2015 [1]. As for fixed Internet traffic, the annual growth in 2014 is expected to be greater than the overall volume in 2009 [2]. These figures are not accidental, but they give evidence of the exponential growth of IP traffic, which is the result of many concomitant causes: the ever increasing pervasiveness of the Internet, users' addiction to network connectivity, the progressive shift of usage patterns towards bandwidth intensive services, the significant improvements in the usability of interfaces, the ubiquitous availability of connected devices, the increasing share of consumer traffic, and the convergence of popular services (voice, TV, video on demand) over IP networks [3].

This trend is only partially sustained by Moore's law, which enables faster switching of data while also improving cost effectiveness of network equipment. Otherwise, continuous investments are required to boost network capacity.

The question is: Does the network generate enough value to sustain its own development? If we limit our observation to the capitalization of user-interface producers and over-the-top service providers, the answer seems to be positive, since they apparently benefit from the exponential trend of Internet traffic. There are, however, other segments in the supply chain, such as content right owners and connectivity providers, which suffer from a lack of incremental revenues which impairs development [4]. Analysts observe that the *capital expenditures* (CapEx) required to fund incremental capacity both in fixed and in mobile networks are much higher that those obtained from the projections based on historical data. CapEx is the amount of money spent by a company to acquire or upgrade its assets in order to increase its capacity or efficiency for more than one accounting period. For a network operator the assets include network infrastructure, equipment, software, sites, and civil assets [5]. The ongoing costs incurred for running the business are called *operating expenditures* (OpEx). Although the revenues of network operators are still sufficient to pay for OpEx, in order for network development to keep pace with the estimated traffic growth, in the next 5 years mobile and fixed infrastructures will ask for a CapEx which is 50% and 30% higher, respectively, than currently planned for the same years [2]. Such additional investments cannot be made as long as the operators do not take advantage from evolution. Hence, the imbalance between costs and revenues and the unfair capitalization of Internet value induced by current business models will end up impairing evolution and bringing the network to a congestion which will affect the whole value chain.

Although governmental measures (such as public funding, antitrust rules, and neutrality enforcement) have been often adopted to mitigate this phenomenon, they cannot be considered as ultimate solutions to guarantee a sustainable growth.

This paper analyses the origins of the bottlenecks in the Internet value chain to propose a new service-based network model (as opposed to the traditional access-based one), which grants to the Internet the capability of overcoming its own bottlenecks without the need for external enforcement and without giving up network neutrality.

II. THE INTERNET VALUE CHAIN

Among the different ways to represent Internet value chain (VC), one of the most detailed and recent representations is provided by A.T. Kearney [4], which splits the Internet market into 5 segments, namely: content rights, online services, enabling technology services, connectivity, and user interface. In order to point out the differences between

 ISBN: 978-1-61208-142-7

access-based and service-based business models, we adopt a 7-stage VC obtained by separating the Internet core from the access network (both of them included into the Connectivity segment in A.T. Kearney's report) and by distinguishing the services provided *over the top* (OTT) from those provided within operators' managed networks (the latter not explicitly mentioned in the above report).

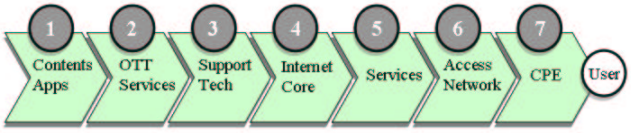

Figure 1. The Internet value chain.

The resulting VC, shown in Figure 1, is composed of the following stages: contents and applications (stage 1), that could be either copy righted or generated by end-users; OTT online services (stage 2), made globally available on the Internet; support technologies (stage 3), which include content delivery overlay networks and hosting services; Internet core (stage 4), made of interchange points and core networks of incumbent operators; online services provided within managed networks (stage 5), which include IPTV services; access networks (stage 6), which include both backhauling and retail access up to the network termination points made available to end-users; user devices (stage 7), which include HW/SW user interfaces and customer premises equipment (CPE) used to connect to network termination points.

It is worth noticing that stage 4 includes both operators' backbones and interchange points, so that Figure 1 does not point out the re-distribution of value within the Internet core, which is governed by peering agreements and managed by international organizations.

According to historical data of market capitalization [2], VC segments have followed very different trends in the recent past: while stages 2, 3, and 7 have known a significant growth from 2004 to 2010 (4x, 2x, and 5x respectively), stages 1, 4, and 6 have not taken any advantage of the fast increase in Internet traffic and their capitalization has slightly decreased in the same period. As for segment 5, mainly represented by IPTV market, the compound annual growth rate is expected to be around 25% until 2014 [6].

The imbalance of Internet market capitalization is schematically represented in Figure 2 in order to provide a qualitative perception of the bottlenecks which risk to impair network development.

A. Access-Based Value Chain

The current functioning of the network is dominated by two main features. The first one is *vertical integration*, which is the absorption into a single organization (namely, the so-called *operator*) of all the aspects required to go from the Internet core to end-users, often including even the provision

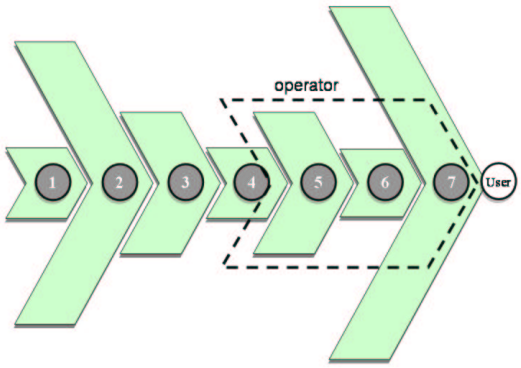

Figure 2. Schematic representation of the unbalanced capitalization of the Internet value chain.

of customer equipment (vertical integration is represented as a dashed macro-stage in Figure 2). The second one is the *all-or-nothing offer* of Internet access, which gives to end-users only the categorical choice between subscribing to full access to the network, or being completely cut off. Internet access is typically sold at a monthly flat fee depending only on the nominal (i.e., maximum) bandwidth at user's disposal.

From operators' stand point this business model was originally motivated by the perspective of: attracting costumers with a simple offer, avoiding the operating costs of complex accounting policies, taking advantage from average individual use well below the nominal bandwidth, and exploiting statistical sharing to over-book the bandwidth available.

From end-users' stand point, the model has induced the misleading perception that: Internet bandwidth is the only good customers pay for (while they also pay for access infrastructures and CPE), the nominal bandwidth is the actual one they are entitled to use all the time (while it represents only a peak value they are not allowed to pass), and the more they use the network the more convenient their contracts become (while the monthly rate was determined assuming they would not have used the Internet all the time).

From OTT service providers' stand point, the access-based business model has created a global market where to offer their services without caring about transport, allowing them to deliver most services for free and to get money from commercial sponsors.

It is a matter of fact that the Internet has become a two-sided market where the apparent gratuitousness of traffic has created a short-circuit between the two sides (namely, service providers and end-users), cutting off from revenues network operators, which lay in the middle.

The ultimate effect of this phenomenon is the so-called *cloud computing*: users feel Internet services to be so close to them and reachable at no additional costs, that they keep on the cloud even their personal files that could fit at no cost in the storage devices embedded in their smart phones.

Although such a short circuit has significantly contributed to the diffusion of the Internet and to the development of advanced online services, the model suffers from many

 ISBN: 978-1-61208-142-7

weaknesses which make it unsuitable to sustain the exponential development.

First, the advent of a huge variety of services with different bandwidth requirements has created a significant spread of usage patterns with a consequent inequality among users who pay the same fee in spite of heterogeneous needs (for instance, 1% of mobile data subscribers generate over 20% of mobile data traffic [7]). If such a monthly fee is higher than the perceived value of the Internet, individuals may be not motivated enough to subscribe.

Second, there are stages in the VC of Figure 2 (such as stage 6) which significantly contribute to the costs incurred by operators without generating any direct value, since they are hidden to end-users. This misalignment between costs and revenues impairs innovation because operators are neither motivated to invest in access infrastructures nor interested in boosting the development of bandwidth-intensive services.

Third, as the average individual use gets close to the nominal bandwidth included in the monthly fee, over-booking causes the congestion of access networks with consequent loss of quality of service (QoS).

To contrast these effects, operators have tried to find scope economies by adopting the so-called *triple-play* market strategy, which consists in providing additional services (namely, IPTV and VoIP) within the walled gardens of their own networks. Moreover, they have been induced to apply *traffic shaping* and *access tiering* techniques in order to delay the congestion of their networks and to mitigate its effects on QoS.

Governments, on the other hand, have come on stage in many ways in order to bridge digital divide, foster competition, and defend end-users' interests. In particular, public funds have been allocated in many countries to finance the development of *next generation networks* (NGNs) and the deployment of access infrastructures in market failure regions, regulations have been enacted to impose incumbent operators to make their infrastructures available to new entrants at controlled wholesale/unbundling conditions, and network neutrality has been enforced by preventing operators from adopting access tiering policies and from establishing commercial relationships with OTT service providers.

If state interventions can play a significant role in triggering development, they cannot guarantee sustainability (if not complemented by private investments and not supported by suitable business models) and they often produce side effects that may even end up thwarting their own original purposes. This is the case of neutrality enforcement and local loop unbundling, which discourage private investments in NGNs by reducing business opportunities, by avoiding bandwidth optimizations, and by making the break-even point unreachable in many scenarios. Moreover, state financial aids, even if targeted only to access networks (stage 6 in the VC), create significant distortions in many other markets (stages 4, 5, and 7 in the VC) because of vertical integration and triple-play market strategies currently adopted by incumbent operators.

B. Service-Based Value Chain

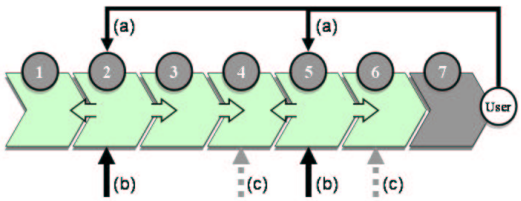

Figure 3. Service-based Internet value chain.

The VC proposed in this section is based on two main features: *vertical separation*, as opposed to vertical integration, and *service orientation*, as opposed to access orientation typical of the current Internet model discussed in the previous subsection.

Technically speaking, separation is an inherent property of the Internet induced by the layered structure of its protocol stack. Network neutrality, which has been one of the main driving forces behind Internet development and innovation, was naturally induced by the layered architecture before becoming a controversial principle. In this context, vertical separation is particularly intended as market segmentation, which enables each segment in the VC to be possibly managed by different actors who interact with all other segments by means of transparent and profitable commercial relationships. Separation also enables each market segment to make business with other industry sectors and public organizations, not represented in the VC, or to be targeted by state financial aids and welfare policies. Vertical separation has been identified by ITU as one of the four technology implications on market structure which prompt for new business models, the other three implications being service innovation, network innovation, and horizontal integration (i.e., network convergence) [8].

Service orientation, which is the second distinguishing feature of the proposed VC, means the opportunity for end-users to directly focus on the services they need, even if they have not yet established commercial relationships with any operator. There are many motivations for focusing on services (delivered both OTT and within managed networks): services/applications are at the top of the TCP/IP stack, they are much more attractive than their enabling technologies (i.e., connection and transport), they provide great opportunities of diversification and innovation, and they have proved capable of taking advantage of traffic growth. Although market capitalization data clearly demonstrate that services are the main driving force of the Internet, current business models do not provide adequate instruments to distribute the revenues along the VC in order to support the development required at all its stages.

 ISBN: 978-1-61208-142-7

An ideal representation of a service-based VC is provided in Figure 3. End-users establish direct relationships with service providers (SPs), who operate both at stage 2 (OTT) and at stage 5 (within managed networks). These interactions, which may or may not involve payments, are represented by black arrows with label (a) in Figure 3, where thick arrows with label (b) represent revenues coming from sponsorships, advertisements, and any other form of business made with stakeholders who take advantage of the Internet without being directly involved in the VC. Both type-a and type-b incomes are collected at stages 2 and 5, even if all stages contribute to the VC. Transparent relations among the actors operating at different stages are then needed to enable a fair redistribution of revenues along the service-based VC. Inter-stage redistributions are represented by horizontal arrows in Figure 3. Finally, dashed arrows with label (c) represent financial aids possibly targeting backbones (stage 4) and access infrastructures (stage 6).

Stage 7 (i.e., CPE) is shadowed in Figure 3 and it is not involved in any inter-stage commercial transaction because it is a thriving market by itself, which is expected to be able to keep following and supporting Internet growth without the need for significant changes in its business model. In other terms, end-users' devices (such as smart phones, net books, PCs, set-top-boxes, ...) can be considered to be already at users' disposal, since customers are highly motivated to pay for them. Hence, they can be neglected in our analysis since they are neither a bottleneck to be overcome, nor a source of revenues suitable to be redistributed along the VC. Notice however that the lack of interactions between stage 7 and the rest of the VC does not mean that CPE cannot be provided by operators (as they usually are in current business models). Rather, it simply means that this kind of scope economies are not considered to be relevant for network development.

Internet bandwidth is nothing but a special kind of service provided at stage 5 by Internet servise providers (ISPs) who manage gateways placed between access networks (stage 6) and Internet core (stage 4). Access infrastructures are assumed to be open to end-users, whose CPE associates for free in order to allow them to gain access to online services (including Internet bandwidth). SPs and ISPs pay a fee to the operators managing the access network in order to be allowed to expose their services to connected end-users. As long as SPs share their revenues with access network operators, the latter are motivated to open their networks to end-users, in that they add to the value of the network by making it more attractive for SPs. This allows operators to take advantage of the development of the two-sided market they enable, and provides the motivation required to invest in access infrastructures.

OTT SPs may keep exposing their services on the Internet without establishing direct relationships with network operators. In this case, they can be reached by end-users who subscribed with some ISP to gain access to the Internet, while they will not be reached by end-users who have connected only to the access infrastructure without buying Internet bandwidth. On the other hand, OTT SPs can decide to enter into a contract with an operator to make their services also reachable, within managed access networks, to end-users who associated for free with the access infrastructure. In the first case the traffic generated within the acces network is paid by end-users (as a share of the fee they pay to ISPs), while in the second case it is paid by SPs. Finally, depending on the nature of the services, OTT SPs may or may not share their revenues with content providers (stage 1) and enabling technology providers (stage 3).

Although many different business models can be conceived and adopted, commercial relationships should be mainly based on IP traffic in order to provide the so-called *price-signal* which acts as a positive feedback in triggering and sustaining development.

In summary, the service-based VC provides a suitable support for development and growth, in that it lowers access barriers for end-users, it reduces information asymmetry by avoiding end-users to be billed unawarely for the traffic generated by the services they use, and it allows operators to establish transparent commercial relationships with SPs without violating network neutrality. In fact, neutrality is preserved as long as the same conditions are applied at each stage to all the actors playing the same role in the VC.

III. A SERVICE-BASED MODEL

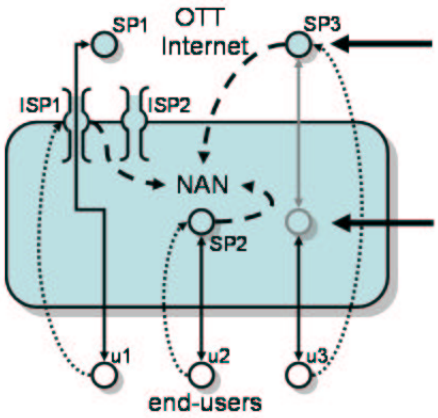

Figure 4. Interactions between end-users and SPs in a service-based neutral access network.

Moving from an access-based to a service-based model implies a paradigm shift in the Internet VC. While at some stages such change can emerge from the natural evolution of current business models, at some others it prompts for innovative architectural and commercial models. The most challenging issue in this context is the re-design of the relationships among end-users, operators, and SPs across access infrastructures. To this purpose, a suitable support can be provided by the so-called *neutral access network* (NAN) model [9].

 ISBN: 978-1-61208-142-7

NANs are a special category of open access networks [10] conceived to make the access infrastructures economically sustainable in market-failure regions by triggering positive externalities and enhancing penetration [11]. A NAN exhibits the features of a full-fledged network by itself, containing a sizeable set of services made available to the users before they register with any ISP. End-users are allowed to associate with the NAN for free without prehemptive registration. Once the users have entered the NAN, they are exposed to all the services made available within the network, including Internet surfing through the gateways managed by ISPs. Registration and authentication are required only to gain access to the Internet or to those internal services which require user identification for accounting, personalization, privacy, or security needs. The entry of a new user into the NAN has a beneficial effect for all other users since it helps reaching the critical mass of users required to incentivize the provisioning of new services. Similarly, the entry of a new SP has a spillover benefit for all other providers since it induces new users to enter the shared marketplace and it contributes to cover the costs of the infrastructure. Service orientation is natural in a NAN. End users have commercial relationships only with SPs (including ISPs), who pay a share of their revenues to the NAN organization. The share is then possibly distributed among multiple stakeholders: real estate owners, investors, and local operators.

Figure 4 represents the possible relations that can be established in a NAN. Vertical solid arrows stay for IP traffic, dotted arrows stay for direct transactions between end-users and SPs, horizontal solid arrows stay for revenues coming from markets outside the VC (including sponsorhips and advertisment), while dashed arrows stay for commercial relationships between SPs and NAN operators. Three paradigmatic cases are depicted, referring to three end-users who are assumed to be connected for free to the NAN by means of their own CPE.

Case 1. End-user u1 wants to gain full access to the Internet. To this purpose, he/she registers with one of the virtual operators (namely, ISP1) offering Internet bandwidth in the NAN. The conditions at which Internet bandwidth is sold by ISP1 include the share he has to pay to the NAN operator for transporting u1's traffic across the NAN. Once on the Internet, u1 takes advantage of the service delivered by an OTT SP (namely, SP1) without taking care of transport. This case reproduces the same user experience of current access-based models, while retaining the benefits of service orientation. Commercial agreements between ISP1 and NAN operators can assume the form of a wholesale contract, but the key novelty is that u1 connected to the NAN before registering with ISP1 and was allowed to choose the ISP as a service.

Case 2. End-user u2 associates to the NAN without buying Internet bandwidth since it is only interested in a specific service (like tourist information, e-government, IPTV, ...) which is supplied by SP2 within the access network. The only relation he/she has to establish is with SP2, who is supposed to pay a fee to the NAN operator for web hosting and transport. Revenues for SP2 can come either from end-users (if they pay for the service), or from sponsors/subsidies (if the service is delivered for free), or from both (if a mixed model is adopted, such as the one of IPTVs providing both free channels and pay-per-view contents).

Case 3. End-user u3 behaves exactly as u2, even if the service he/she wants to use is provided by an OTT SP (namely, SP3). This is made possible by the agreement between SP3 and the NAN operator, signed to expose the online service of SP3 within the NAN. From a technical point of view, this could be done in many different ways, including mirroring, proximity caching, and white listing. The traffic generated across the NAN is then paid by SP3, while the service he/she provides makes the access infrastructure more attractive.

The trade-off between network neutrality, bandwidth optimization, and capitalization is reached thanks to the nature of the commercial relations established at all stages, which are not discriminatory, not exclusive, and inherently regulated by market law.

IV. Conclusions

In spite of the exponential growth of Internet traffic, the unequal distribution of revenues along the Internet VC, together with the imbalance between costs and revenues caused by the business models currently adopted by network operators, risk to impair evolution towards broadband next generation networks.

The VC is like a pipeline the capacity of which is limited by the thinnest pipe, so that a fair distribution of revenues along the VC is essential to trigger and sustain network development.

The Internet VC has been analysed in order to point out the limitations of current access-based models and to propose a paradigm shift towards a new service-based approach. Service orientation, complemented by suitable business models, allows all stages of the VC to take advantage of the attractiveness and diversity of online services and to benefit from the revenues they can generate in terms of sponsorships and advertisement.

It has been shown that neutral access networks provide a suitable support to the adoption of a service-based model, allowing end-users to connect for free to the access infrastructure and then focus only on the services they need, including Internet bandwidth. The systematic application of not exclusive agreements among the actors involved (service providers, content providers, and network operators) provides the basis for a fair redistribution of revenues along the VC, driven by market rather than by policy enforcement.

 ISBN: 978-1-61208-142-7

The urgent need for a paradigm shift in the Internet VC can be viewed in many recent events and market signs.

Amazon's *Kindle 2* has conquered the market of e-book readers by freeing end-users from the burden of connectivity. It integrates a hidden SIM card which allows end-users to be always connected (seemlessly) to the online store. The cost of download is included into the price of e-books thanks to an agreement between Amazon and AT&T, which in its turn has roaming agreements with mobile operators all around the world [12]. This is a neat example of a vertical application built on top of a vertically-separated architecture to provide a service-oriented user experience.

Groupon (www.groupon.com) is a deal-of-the-day website which operates in hundreds of localized markets worldwide. The business model is fairly simple: it offers a deal per market per day. If users who sign up for the offer reach a given threshold, then the deal becomes available to all of them and the retailer shares his/her revenues with Groupon. For retailers, Groupon works as an *assurance contract* which guarantees a critical mass which makes the deal like a *quantity discount* [13]. In 2010, Groupon Inc. refused a 6 billion Dollar offer from Google, clearly demonstrating the value of localized on-line business. It is apparent that Groupon could provide its services within a NAN, making it available to local end-users even if they have not signed with any ISP.

In January 2011, Google Inc. accepted to allow publishers to quit *Google News* without affecting the results returned by its main search engine, and to disclose revenue-sharing arrangements for its *AdSense* partners. This agreement ended an antitrust investigation of the *Italian Competition Authority* (AGCM) triggered by the *Italian Federation of Newspaper Publishers* (FIEG) because most people were content with aggregated summaries found on Google News and bothered to click on the links that led to their newspaper websites, costing the publishers advertising and page views. This story shows that services (e.g., online aggregators and search engines) are much closer to end-users than contents (e.g., news), so that it is much easier for SPs than for content right owners to be paid by end-users and sponsors. The agreement found in Italy also demonstrates that it is worth for both categories to find a suitable revenue sharing mechanism which reduces the imbalance and makes the business sustainable.

Google Inc. has provided free Wi-Fi access in Mountain View (CA) for several years and it has contributed to the development of many other municipal networks. In February 2011 the City Council approved a 5-year extension of the *Google WiFi* deal, with an escape clause for Google. There are two signs that can be found in this piece of news: the first one is that OTT SPs are interested in widening their market by lowering access barriers, the second one is that they do not want to take the place of network operators (the escape clause was wanted by Google).

In December 2010 some of the major European mobile operators, including Orange, Telecom Italia, Telefonica and the Vodafone Group, have demanded that popular OTT services, such as those from Google, Facebook, Skype and Apple, contribute to pay for the traffic they generate on their networks. This request, motivated by the lack of return for operators from the exponential growth of IP traffic, has raised network neutrality issues due to the unsuitability of the business models adopted, which do not allow operators to establish commercial relationships with SPs without impairing the neutrality of the connection they provide.

In conclusions, service orientation is proposed in this paper as the key for granting to the Internet the degrees of freedom required to autonomously find the best balance among the segments in the VC, thus overcoming the bottlenecks and creating the preconditions for development.

ACKNOWLEDGEMENT

The research leading to these results has received funding from the EU IST Seventh Framework Programme ([FP7/2007-2013]) under grant agreement n 25741, project ULOOP (User-centric Wireless Local Loop).

REFERENCES

[1] Cisco. Visual Networking Index Global Mobile Data Traffic Forecast. *Cisco White Paper*, 2010.

[2] A. T. Kearney. A Viable Future Model for the Internet. *A.T. Kearney report*, 2010.

[3] Akamai. Q3 2010 - The State of the Internet. *Akamai report*, 2011.

[4] A. T. Kearney. Internet Value Chain Economics. *The Economics of the Internet, Vodafone Policy Paper*, 2010.

[5] S. Verbrugge et al. Methodology and input availability parameters for calculating OpEx and CapEx costs for realistic network scenarios. *OSA Journal of Optical Networking*, 5(6):509–520, 2006.

[6] Multimedia Research Group Inc. *IPTV Global Forecast 2010 to 2014 - Semiannual IPTV Global Forecast Report*. MRG, Inc., June 2010.

[7] Cisco. Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010-2015. *Cisco White Paper*, 2011.

[8] International Telecommunication Union. *ICT regulation toolkit*. http://www.ictregulationtoolkit.org/, last visited on Feb 2011.

[9] A. Bogliolo. Introducing Neutral Access Networks. In *Proceedings of the 5th Conference on Next Generation Internet Networks*, 2009.

[10] J. Barceló, A. Sfairopoulou, and B. Bellalta. Wireless open metropolitan area networks. *SIGMOBILE Mob. Comput. Commun. Rev.*, 12(3):34–44, 2008.

[11] E. Pigliapoco and A. Bogliolo. Enhancing broadband penetration in a competitive market. In *Proc. of the International Conference on Evolving Internet*, pages 159–163. IEEE Computer Society, 2010.

[12] C. Loebbecke et al. Innovating for the mobile end-user market: Amazon's kindle 2 strategy as emerging business model. In *Proc. of the International Conference on Mobile Business*, pages 51–57. IEEE Computer Society, 2010.

[13] A. Mason. *System and Methods for Discount Retailing*. US Patent 2010/0287103 A1 (assigned to Groupon Inc.), 2010.

 ISBN: 978-1-61208-142-7

Digital Complexity in DSL: An Extrapolated Historical Overview

Michael Timmers, Koen Hooghe, Mamoun Guenach, and Jochen Maes
Alcatel-Lucent Bell Labs
Copernicuslaan 50
B-2018 Antwerp, Belgium
Email: {michael.timmers,mamoun.guenach,jochen.maes}@ieee.org,koen.hooghe@alcatel-lucent.com

***Abstract*—Digital subscriber line (DSL) technology for copper twisted pair access networks has been evolving to meet the ever-growing demand for higher data rates. This evolution has gone hand in hand with the roll out of fiber deep in the access network. The most recent technology is vectored VDSL2, able to offer an aggregate data rate of 200 Mb/s on a single copper pair. The next step is to reach 500 to 1000 Mb/s over even shorter copper loops up to a few hundred meters. Such a DSL deployment is an enabler for the cost-effective continuation of the fiber roll-out closer to the end-user. In this paper, a reality check is performed on the digital complexity of a next-generation DSL (ΩDSL) transceiver. By taking into account Moore's law, it is shown that the time is right for this next-generation DSL.**

***Keywords*—Digital Subscriber Line, complexity, analysis**

I. Introduction

After their first introduction in the early 1990s, wireline broadband networks, which includes fiber, coaxial cable and twisted pair, has evolved substantially. Despite the inherent attenuation of copper which limits the capacity, transmission over this medium remains attractive as it is abundantly present throughout the world due to historical telephone deployment. Hence, broadband over copper offers substantial deployment cost savings as compared to fiber-to-the-home (FTTH). Indeed, while FTTH has been technologically viable since 1988 [1], digital subscriber line (DSL) remains the predominant broadband access technology for the residential market [2]. However, as the access network remains the bottleneck in the end-to-end connection and due to the continuing demand for ever higher data rates, copper is being replaced by fiber step-by-step. Due to typical branched topologies, the cost per user of fiber deployment increases substantially when moving closer to the user. This is why different operators have expressed enthusiasm with recent technologies, such as phantom mode and vectoring, which hold the promise of delivering more than 300 Mb/s [3]. The success of vectoring and phantom mode transmission triggered interest in a next-generation broadband DSL, ΩDSL, beyond vectored VDSL2 to deliver 500 Mb/s to 1 Gb/s over relatively short loops, i.e., below 400 m [4]. Standardization of such an ΩDSL has been started in the project G.fast. However, due to the competition from other access technologies, the DSL capacity increase must remain cost-effective and, hence, low-complex. Indeed, as a healthy cost difference between FTTH and Fiber-To-The-Curb (FTTC) needs to stay in place, ΩDSL designs need to carefully evaluate the complexity of the used scheme.

In this paper, we focus on the digital complexity of the underlying scheme. We discuss different generations of DSL technologies based on discrete multi-tone modulation (DMT), using the methodology presented in [5]. We compare the complexity of different DSL flavors by introducing a time scaling based on Moore's Law [6]. Finally, we extrapolate these results to evaluate DMT-based proposals for a ΩDSL. We show that an evolutionary path is in line with previous complexity increases between generations. A DMT-based ΩDSL, which can leverage on proven technology, is, hence, recommended.

This paper is structured as follows. First, we give an overview of discrete multi-tone modulation in Section II. Afterwards, we present challenges and opportunities for the next-generation DSL in Section III. Then, in Section IV, we introduce the reference methodology for complexity analysis. We analyze the digital complexity of the different DSL flavors in Section V and draw conclusions in Section VI.

II. Overview of discrete multi-tone modulation

In this section, we give a short overview of the DMT modulation scheme and discuss its strengths and weaknesses.

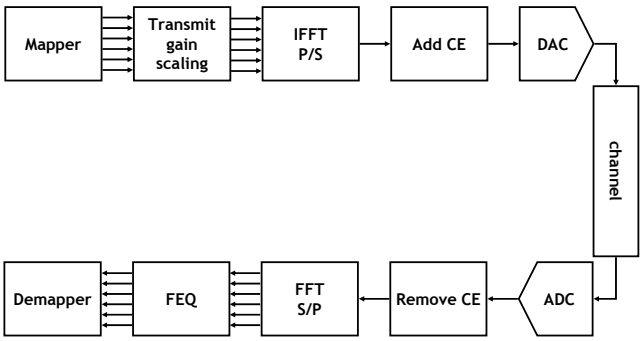

Fig. 1. Discrete multi-tone modulation splits the frequency-selective channel into a number of independent narrowband flat channels, which allows to adapt to the channel in a computationally efficient way.

DSL modems use a particular modulation format referred to as discrete multi-tone modulation (DMT), which splits the frequency-selective channel into a number of independent narrowband flat channels. This allows to cope with severe channel conditions in a flexible and computationally efficient

 ISBN: 978-1-61208-142-7

way. For instance, the frequency-selectivity of the twisted pair channel can be dealt with by means of simple frequency domain equalization techniques. Moreover, narrowband interference can be handled by vacating (notching) the transmission over the corresponding subcarriers, complemented with time-domain windowing. Echo reflection can be tackled by duplexing two-way data transmission in non-overlapping upstream and downstream bands, which is referred to as frequency-division duplexing (FDD). DMT furthermore allows for a spectrally efficient design, as the amount of power and the number of bits transmitted on each subcarrier can be allocated in a flexible and optimal way, using so-called power and bit loading procedures.

In Fig. 1, the general blocks of DMT modulation are shown [5, 7]. In the transmitter, the input data bits are first mapped onto QAM constellations points for each of the n_c carriers. Each carrier has a complex transmit gain to control the carrier power. The frequency domain samples X_k are then converted into a time-domain symbol with an N-point inverse fast Fourier transform (IFFT), where N is twice the number of carriers, n_c:

$$x_n = \sum_{k=0}^{N-1} X_k e^{\frac{-j2\pi kn}{N}} \quad (1)$$

After the IFFT, a cyclic extension (CE) is added with a length ν that is larger than the time delay spread to combat inter-block interference. Windowing is further applied to reduce out-of-band leakage. The resulting signal then passes through a digital-to-analog converter (DAC) and is sent over the channel.

In the receiver, the received signal is digitized with an analog-to-digital converter (ADC). An FFT per DMT block of N samples is applied to switch back to the original frequency-domain symbols. The single-tap frequency domain equalizer inverts the channel on a per-carrier basis, followed by the demapper to recover the transmitted information bits.

III. The next-generation DSL

In this section, we discuss the objectives for ΩDSL. Afterwards, we present a general overview on where the opportunites lie to achieve these objectives.

A. Objectives

To compete with other access network technologies, such as wireless, coax or fiber, ΩDSL should target a data rate of 1Gb/s aggregated over upstream (US) and downstream (DS). Although the residential market demand is still far below this limit, it is expected that the bandwidth consumption will continue its exponential growth and it is expected that the top line data rate demands will exceed 1Gb/s by 2030 [8]. Aside from this data rate, ΩDSL should be very flexible, both in the frequency as in the time domain to adapt to dynamic channel conditions and applications requirements. An important aspect is also energy efficiency: the energy consumption of ΩDSL should scale with the applied load, i.e., the actual throughput. As the DSL environment will become a lot more dynamic, it is also important to be robust by avoiding packet errors, retransmitting and keeping the downtime of the DSL communication as low as possible.

B. Approach

DMT remains one of the prominent candidates for achieving the objectives listed in Section III-A. Indeed, DMT is very flexible in the frequency domain and especially suited for spectral confinement, which is important when moving to higher bandwidths, where additional notching is required.

Furthermore, as any other multicarrier based modulation the frequency selectivity of the channel can easily be addressed by very basic single tap equalizers. It is also robust to near-end crosstalk and echo through frequency division duplexing. Far-end crosstalk can be avoided through precoding, which can be easily implemented in the generic DMT scheme. However, it is not so robust against transient noise. Therefore, we should rely on fast adaptation mechanisms like a fast bit swap and bit loading or adaptive coding techniques, such as FEC or ARQ. Luckily, due to the flexibility of DMT such fast adaptation is possible. However, due to the FFT/IFFT core, DSL is a complex modulation scheme. Hence, in this paper, we want to perform a reality-check and look if ΩDSL is feasible. In this section, we will first describe how the DMT scheme needs to be applied to deliver the high data rates that are required.

We start our analysis from the Shannon-Hartley theorem [9]:

$$C = W \log_2 \left(1 + \mathrm{SNR}\right), \quad (2)$$

where C is the Shannon capacity of the communication channel and W is the analog bandwidth used. The signal-to-noise ratio at the receiver is denoted as SNR. This Shannon capacity is an upper limit on the throughput that can be achieved over a channel with no errors. However, a gap exists between the Shannon capacity and the practical data rate, R, of the channel. For DSL systems the following formula is generally used [12]:

$$R = \eta \Delta_c \sum_{k=0}^{N-1} \min\left(\log_2\left(1+\frac{|H(k)|^2 P_t(k)}{\Gamma(\sigma_0^2(k)+I(k))}\right), b_{\max}\right). \quad (3)$$

Here, η represents the efficiency, which takes into account the coding and CE overhead, Γ is the SNR gap, Δ_c the carrier spacing and $b_{\max}$ the bit cap. The channel attenuation is represented as $|H|^2$ and the transmit power is denoted P_t. A typical value for the transceiver noise power spectral density, σ_0^2, in state-of-the-art DSL designs is -135 to -140 dBm/Hz. The interference power I is the result of radio ingress, alien crosstalk and self-crosstalk.

To increase the capacity of a system, several methods can be applied. The most straightforward is to control the channel attenuation. This is done by pushing fiber deeper in the access network and, thus, shortening the looplengths of the copper channel. ΩDSL will consider looplengths up to 400 m and will be optimized for looplengths from 0 m to 200 m, which is typical for a FTTC or FTTB scenario (see Fig. 2).

Another parameter that can be optimized is the coding efficiency, for which today a typical range of 78% is used [12].

 ISBN: 978-1-61208-142-7

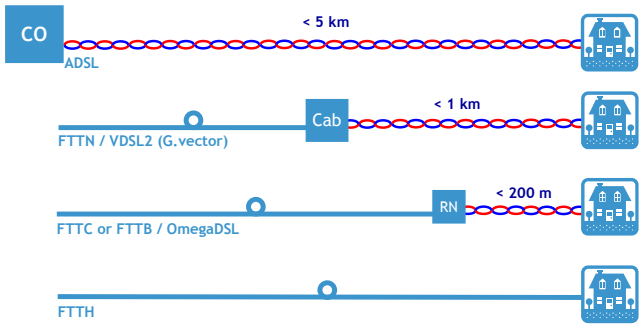

Fig. 2. Fiber is contiuously being deployed closer to the user, starting from an all-copper deployment from the CO (ADSL). An economically interesting next step exist in the combination of FTTB or FTTC with ΩDSL

TABLE I
PARAMETERS USED FOR FIGURES IN SECTION III

	Fig. 3	**Fig. 4**
Looplength	200 m	variable
Twisted pair	24 awg	24 awg
Noise power	-135 dBm/Hz	-135 dBm/Hz
Transmit power	-60 dBm/Hz	-60 dBm/Hz ($f <= 30$ Mhz)
		-76dBm/Hz ($f > 30$ MHz)
Γ	9.45 dB	9.45 dB
b_{max}	15 bits	15 bits
η	78%	78%
Notches	none	none

However, it is clear that the coding will need to provide the desired robustness and resiliency to counter the channel dynamics. Some components of the interference, such as self-crosstalk, can be cancelled today, e.g., in G.vector [10]. Another typical parameter to increase system capacity is the analog bandwidth, W. The widest profile of VDSL2 uses a 30 MHz bandwidth. Today, VDSL2 is limited at lower frequencies by the bit cap, $b_{\max}$, which is set to 15 bits per carrier. Also, here, headroom exist to remove this constraint in low-bandwidth systems, constrained by ADC technology.

In Fig. 3, we show the headroom for these different options for a 24 awg twisted pair with a looplength of 200 m for a transmit power of -60 dBm/Hz and a noise power of -135 dBm/Hz. Each block in the grid of this figure, represents 50 Mb/s (10 MHz multiplied by 5 (b/s)/Hz). Hence, we can immediately see that a 30 MHz bandwidth will not suffice, as it is only able to deliver 750 Mb/s Shannon capacity even on a null-loop (15 blocks in Fig. 3, i.e., 25 (b/s)/Hz over 30MHz). We also see that removing the bit cap, $b_{\max}$, only has limited benefit in the lower frequency range. The efficiency does have a large impact, but, as indicated above, coding overhead is required to deliver the desired robustness and resiliency. An interesting and valuable parameter is the SNR gap, Γ. Traditionally, this is used to cover the channel dynamics. However, when we leverage on the flexibility of the DMT modulation scheme, we can lower this gap. As indicated in Fig. 3, this increases the SNR with 6 dB or, equivalently, about 2 (b/s)/Hz.

In Fig. 4, we show the looplength distribution for three proposals for a DMT-based ΩDSL, using the parameters listed

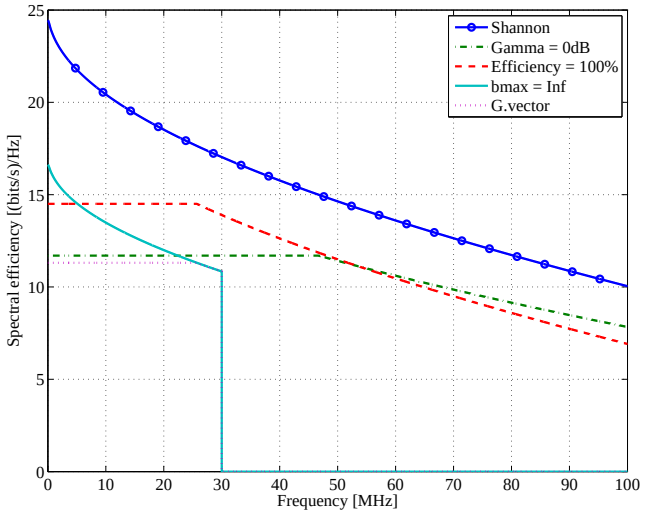

Fig. 3. The headroom of different options shows the relative contributions of each parameter optimization. To reach the 1Gb/s objective, increasing the bandwidth is a must.

in Table I. It shows that a 70 MHz profile cannot reach the desired 1 Gb/s for any looplength. However, a bandwidth of 140 MHz is in line with the objectives for ΩDSL. As a reference, we also included a 280 MHz profile, which is capable to deliver over 2Gb/s for the shortest looplengths.

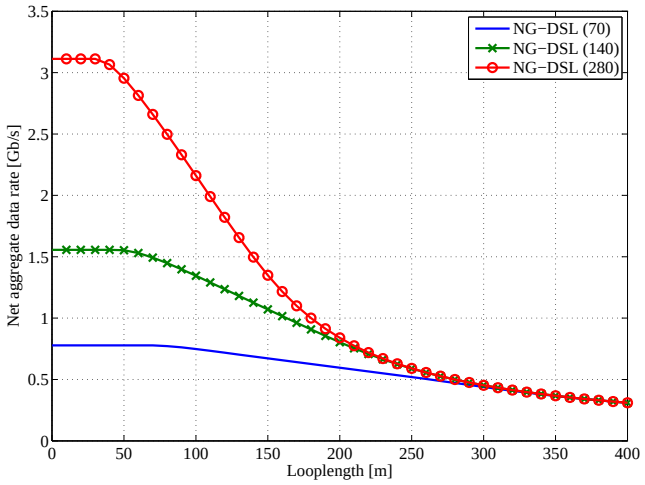

Fig. 4. Using parameters listed in Table I, we show that a 140 MHz profile will reach 1Gb/s for the target looplengths.

IV. METHODOLOGY FOR DMT COMPLEXITY ANALYSIS

In this section, we discuss the methodology for complexity analysis of DMT modulation schemes. We rely on the work, presented in [5], which we summarize below. In this paper, however, we rely on the number of multiply-accumulates per second (R_{MAC}) and the number of memory locations per second (R_{MEM}) for comparison of the different DSL technologies, rather than on the number of multiply-accumulates per bit as done in [5].

 ISBN: 978-1-61208-142-7

TABLE II
COMPLEXITY OF A DMT SYSTEM [5].

Operation Block	$\mathbf{N_{MAC}}$	$\mathbf{N_{MEM}}$
Transmit gain scaling	N	N
IFFT	$0.75N \log_2 N$	$1.5N$
Tx-windowing	2ν	2ν
Rx-windowing	2ν	2ν
FFT	$0.75N \log_2 N$	N
FEQ	$1.5N$	$2N$
Total	$2.5N + 1.5N \log_2 N + 4\nu$	$5.5N + 4\nu$

In Table II, the number of multiply-accumulates per symbol (N_{MAC}) and the number of memory locations per symbol (N_{MEM}) are shown for each block of the DMT modulation scheme. Below, we indicate the number of multiply-accumulates, $N_{\mathrm{MAC,b}}$, in (4) and memory locations, $N_{\mathrm{MEM,b}}$ in (5) to transmit a single bit. We also define the precision-scaled metrics, $NB_{\mathrm{MAC,b}}$ in (6) and $NB_{\mathrm{MEM,b}}$ in (7), respectively [5].

$$N_{\mathrm{MAC,b}} = \frac{N_{\mathrm{MAC}}}{b_{symb}}, \quad (4)$$

$$N_{\mathrm{MEM,b}} = \frac{N_{\mathrm{MEM}}}{b_{symb}}, \quad (5)$$

$$NB_{\mathrm{MAC,b}} = N_{\mathrm{MAC,b}} B_{\mathrm{MAC}}, \quad (6)$$

$$NB_{\mathrm{MEM,b}} = N_{\mathrm{MEM,b}} B_{\mathrm{MEM}}, \quad (7)$$

where B_{MAC} and B_{MEM} are the precisions of the multiply-accumulates (MAC) in bits and the number of bits per word in the memory, respectively. The comparison metrics, R_{MAC} and R_{MEM}, can readily be found as follows:

$$R_{\mathrm{MAC}} = N_{\mathrm{MAC,b}} R, \quad (8)$$

$$R_{\mathrm{MEM}} = N_{\mathrm{MEM,b}} R, \quad (9)$$

where R is the rate (throughput) of the DMT system in b/s. The total complexity of a DMT scheme can be found in Table II. Below, we summarize how the precisions, B_{MAC} and B_{MEM}, can be found. The signal-to-quantization-noise ratio (SQNR) at the ADC output is given by [11]:

$$\mathrm{SQNR} = 6.02 B_{ADC} + 4.77 - \mathrm{PAPR[dB]}, \quad (10)$$

where B_{ADC} is the ADC precision, PAPR is the peak-to-average power ratio in dB of the underlying modulation scheme. The SQNR needs to configured so that the quantization noise only has limited impact on the bit-error-ratio (BER). Typically, the quantization noise should have an impact below 0.25 dB:

$$SQNR > \max_i SNR_i + 12.27[\mathrm{dB}], \quad (11)$$

assuming flat noise. The ADC precision can then be derived as:

$$B_{ADC} = \left\lceil \frac{1}{6.02} \left(\max(\mathrm{SNR}_i) + \mathrm{PAPR} + 7.5 \right) \right\rceil. \quad (12)$$

The most complex blocks in DMT modulation are the FFT and IFFT blocks. The quantization noise, $\mathrm{SQNR_{FFT}}$, on these operations needs to be less than the ADC quantization noise. The $\mathrm{SQNR_{FFT}}$ can be expressed as [11]:

$$\mathrm{SQNR_{FFT}} = 6.02 B_{\mathrm{FFT}} - 12.64 - 10 \log N, \quad (13)$$

which leads to:

$$B_{\mathrm{FFT}} > \lceil B_{\mathrm{ADC}} + 1.67 \log N - 0.17 \mathrm{PAPR} + 2.8 \rceil, \quad (14)$$

where B_{FFT} is the precision of the FFT in bits. Using Table II and equations (3) and (4-14), we can find the complexity metrics as:

$$R_{\mathrm{MAC}} = B_{\mathrm{FFT}}^2 \left((2.5 + 1.5 \log_2 N)(1 - \alpha) + 4\alpha \right) f_s, \quad (15)$$

$$R_{\mathrm{MEM}} = B_{\mathrm{FFT}} \left(5.5 (1 - \alpha) + 4\alpha \right) f_s, \quad (16)$$

where α is the relative overhead due to the CE and f_s the sampling frequency.

TABLE III
THE DIFFERENT DSL FLAVORS, CONSIDERED IN THIS ANALYSIS.

DSL flavor	Year of standardization by ITU	b_{max}	n_c	Δ_c[kHz]
ADSL	2001	15	256	4.3125
ADSL2	2002	15	256	4.3125
ADSL2+	2003	15	512	4.3125
VDSL DMT	2004	15	2782	4.3125
VDSL2-8	2006	15	2048	4.3125
VDSL2-12	2006	15	2782	4.3125
VDSL2-17	2008	15	4096	4.3125
VDSL2-30	2008	15	3478	8.625
G.hn	2010	12	2048	48.82
ΩDSL (70)	?	15	4096	17.25
ΩDSL (140)	?	15	8192	17.25
ΩDSL (280)	?	15	16384	17.25

V. RESULTS AND EXTRAPOLATION TO ΩDSL

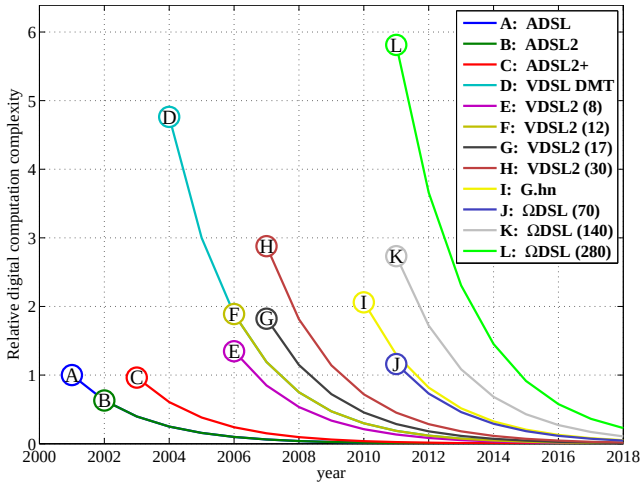

Fig. 5. Relative computational complexity of the different DSL flavors as a function of time.

In Table III, we present an overview on the different DMT-based DSL technologies. For ΩDSL, we include three proposals, all using a carrier spacing of 17.25 kHz, which is deemed appropriate for the looplengths we are considering

 ISBN: 978-1-61208-142-7

for this future technology [12]. However, the results qualitatively hold for other carrier spacing. In Fig. 5, we see the precision-scaled complexity, NB_{MAC}, relative to ADSL in its ITU standardization year of 2001. This relative complexity, $\overline{R_{MAC}(x,y)}$, metric of DSL technology x in year y is based on Moore's law that states that the transistor density on a chip doubles each 18 months [6]. While studies show a flattening of this law, we assume that it holds to facilitate our analysis:

$$\overline{R_{MAC}(x,y)} = \frac{R_{MAC}(x)}{R_{MAC}(ADSL)2^{\frac{2}{3}(y-2001)}}. \qquad (17)$$

A few interesting things can be observed. First, ADSL seems to be a cheap technology. However, the technology for ADSL was already available in 1995, long before the ITU standardization, making it a complex technique at market introduction. The pressure on complexity is mainly related to an increased competitive market.

The innovation from ADSL2 with respect to ADSL were mainly targeted at coding, using the same modulation scheme. This is why they come out equivalently complex in this comparison. The main reason why ADSL2 did not become a commercial success is because it was standardized by ITU almost simultaneously as ADSL2plus and the complexity (cost) of ADSL2plus was acceptable to allow cost-effective and dense line cards and customer premise equipment. Furthermore, we see that all standards, when introduced, have a relative complexity metric in the range $[0.6, 1.6]$. The most prominent outlier is VDSL1 at a relative complexity metric of 4.5. This can indicate why VDSL1 only had moderate commercial success, because of the high complexity cost involved. Furthermore, after two years, the 12 MHz profile of VDSL2 was standardized, which uses the same bandwidth and number of carriers, rendering VDSL1 obsolete.

The other outlier is the 30 MHz profile of VDSL2, which has lower deployment volumes than the 17 MHz profile. This is mainly due to the fact that the 30 MHz profile targets FTTB deployment, which takes a long time to establish. Counter examples are Japan and Korea. More interestingly, the relative complexity metric of the three ΩDSL proposals already fall in 2012 within this appropriate standardization range. This is in line with recent start of actvities at standardization bodies. A similar analysis can be performed for the relative precision-scaled memory complexity metric, $\overline{R_{MEM}(x,y)}$ (see Fig. 6). Given the fact that N is the main contributing factor to both complexity and memory, we draw similar conclusions for the memory complexity.

VI. Conclusions

In this paper, we have discussed the digital complexity of different DSL flavors. We have shown that successful adoption of DMT-based DSL technologies occurs in a certain complexity range, when corrected with Moore's Law. Recently, a next-generation DSL technology is being targeted for very short looplengths and very high data rates. We have shown that the opportunity window for standardization of ΩDSL has come, using an extrapolation of the digital complexity.

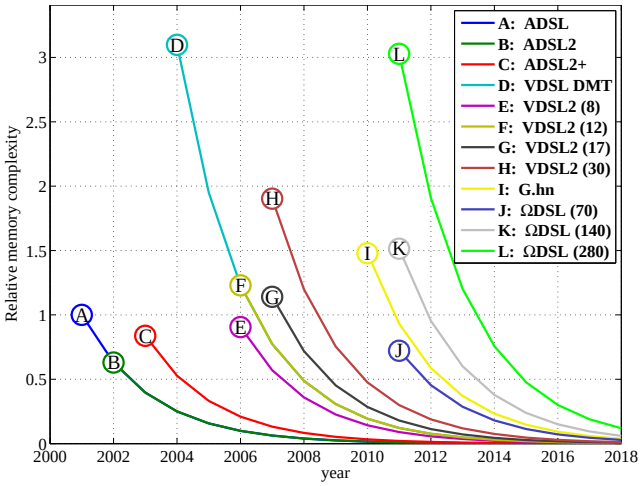

Fig. 6. Relative memory complexity of the different DSL flavors as a function of time.

Acknowledgments

This work was supported by the IWT under contract number 100334, Phanter. The authors would like to thank Paul Spruyt and Adriaan De Lind Van Wijngaarden for their careful review.

References

[1] J. Bourne, "Fiber to the home: practically a reality," in *Proc. of the IEEE International Conference on Communications (ICC)*, 1988, pp. 890–894.
[2] T. Mastrangelo, "Annual Market Outlook Report," *Broadband Trends*, July 2009.
[3] M. Peeters and S. Vanhastel, "The Copper Phantom," *OSP Magazine*, Jan. 2011.
[4] L. Humphrey, "Fibre to the DP," *Broadband Forum*, Dec. 2010.
[5] B. Shim and N. R. Shanbhag, "Complexity analysis of multicarrier and single-carrier systems for very high-speed digital subscriber line," *IEEE Transactions on Signal Processing*, vol. 51, no. 1, Jan. 2003.
[6] G. E. Moore, "Cramming more components onto integrated circuits," *Electronics*, pp. 114–117, Apr. 1965.
[7] J. Bingham, "Multicarrier modulation for data transmission: An idea whose time has come," *IEEE Communications Magazine*, vol. 28, pp. 5–14, 1990.
[8] Zhone, "Choosing the right fttx architecture," Retrieved on January 20 2010 from http://www.zhone.com/solutions/docs/zti-wp-fttx_choices.pdf.
[9] C. E. Shannon, "A Mathematical Theory of Communication," vol. 27, pp. 379–423, July 1948.
[10] V. Oksman, "The ITU-T's new g.vector standard proliferates 100 mb/s dsl," *IEEE Communications Magazine*, vol. 48, no. 10, pp. 140–148, Oct. 2010.
[11] A. V. Oppenheim and R. W. Schafer, "Discrete-time signal processing," *Englewood Cliffs, NJ: Prentice-Hall*, pp. 637–641, 1989.
[12] J. Maes, M. Timmers, and M. Guenach, "Optimized modulation parameters for a next-generation dsl," *Technical Report*, Jan. 2011.

 ISBN: 978-1-61208-142-7

RelaySpot: A Framework for Opportunistic Cooperative Relaying

Tauseef Jamal[1], Paulo Mendes[1], André Zúquete[2]
[1]SITI, R&D Unit of Informatics Systems and Technologies, Universidade Lusofona de Humanidades e Tecnologias (ULHT), COFAC, Campo Grande 376, Lisbon, Portugal
{tauseef.jamal,paulo.mendes}@ulusofona.pt
[2]IEETA / Dep. Electronics, Telecommunications and Informatics University of Aveiro Campus Universitário de Santiago 3810–193 Aveiro, Portugal
andre.zuquete@ua.pt

***Abstract*—Advances in wireless technologies, including more powerful devices and low cost radio technologies, have potential to drive an ubiquitous utilization of Internet services. Nevertheless wireless technologies face performance limitations due to unstable wireless conditions and mobility of devices. In face of multi-path propagation and low data rate stations, cooperative relaying promises gains in performance and reliability. However, cooperation procedures are unstable (rely on current channel conditions) and introduce overhead that can endanger performance especially when nodes are mobile. In this paper we describe a framework, called RelaySpot, to implement cooperative wireless solutions in large mobile networks, based upon the combination of opportunistic and cooperative methods. RelaySpot based solutions are expected to minimize signaling exchange, remove estimation of channel conditions, and improve the utilization of spatial diversity, minimizing outage and increasing reliability.**

***Index Terms*—Cooperative relaying; Opportunistic relaying; Wireless Resource Management; Space-Time Diversity.**

I. INTRODUCTION

Over the past decade, Internet access became essentially wireless, with 802.11 technologies providing a low cost broadband support for a flexible and easy deployment. However, channel conditions in wireless networks are subjected to interference and multi-path propagation, creating fading channels and decreasing the overall network performance. While fast fading can be mitigated by having the source retransmitting packets, slow fading, caused by obstruction of the main signal path, makes retransmission useless, since periods of low signal power lasts the entire duration of the transmission.

Extensive research has been done to mitigate the effect of shadowing in wireless networks, being mostly focused on *Multiple-Input Multiple-Output* (MIMO) systems. Recently, cooperative relaying techniques have been investigated to increase the performance of wireless systems by using diversity created by different single antenna devices, aiming to reach the same level of performance of MIMO systems.

Cooperation occurs when overhearing relays assist the transmission from source to destination by transmitting different copies of the same signal from different locations, allowing the destination to get independently faded versions of the signal that can be combined to obtain an error-free signal [1].

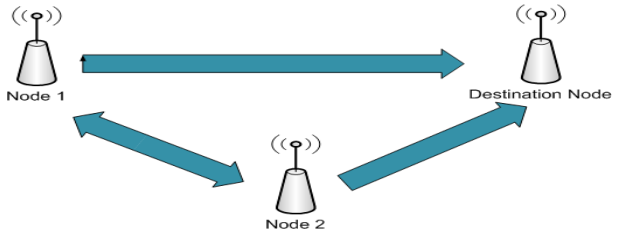

Figure 1. Cooperative Relaying

Figure 1 shows a pair of single antenna devices able to act as relays of each other by forwarding some version of "overheard" packets along with its own data. Because the fading channels of two different devices are statistically independent, this generates spatial diversity. The development of cooperative relaying systems, of which Figure 1 illustrates a simple scenario, raises several research issues including the performance impact on the relay itself, and the interference on the overall network leading to a potential decrease in network capacity and transmission fairness.

At the link layer, IEEE 802.11 uses the CSMA/CA algorithm to control medium access, being the *Distributed Coordination Function* (DCF) the most common operation mode. In scenarios with fading channels and low data rate stations, high throughput, reliability, and coverage may be possible with an efficient cooperative *Medium Access Control* (MAC) layer achieved by modifying the DCF signaling scheme.

The definition of MAC cooperative schemes poses several challenges, specially in the presence of mobile nodes. A major challenge is related to relay selection, which aims to identify the most suitable relay(s) for assisting transmissions between any pair of nodes. Research is ongoing to devise efficient relay selection at MAC layer, being the proposed approaches mostly source or destination based. In the former case, the source maintains a table with *Channel State Information* (CSI) of neighboring devices to support relay selection. In destination-based approaches, the destination decides whether to use relaying or not, based on thresholds and CSI kept on the destination and on potential relays. Both approaches incur in some overhead (specially source-based) and are not efficient

 ISBN: 978-1-61208-142-7

reacting to network changes, mainly in the presence of mobile nodes.

In this paper, we present our arguments in favor of a new type of cooperative relaying scheme based upon local decisions that do not rely on unstable information (e.g., CSI) collected over multiple links. We describe an 802.11 backward compatible cooperative relaying framework, called *RelaySpot*, that aims to ensure accurate and fast relay selection, posing minimum overhead and reducing the dependency upon CSI estimations, which is essential to increase the system performance in scenarios with mobile nodes. The basic characteristic of any RelaySpot-based solution is the capability to perform local relaying decisions at potential relay nodes (can be more than one), based on a combined utilization of opportunistic relay selection and cooperative scheduling. Intermediate nodes take the opportunity to relay in the presence of local favorable conditions (e.g., no concurrent traffic) and absence of relaying attempts by any other nodes. Cooperative scheduling is used to compensate unsuccessful relay transmissions. To the best of our knowledge RelaySpot is the first framework that aims to create the basic conditions to allow relay selection to be done without relying on CSI estimation.

II. State Of The Art

Initial work in cooperative networking was mainly focused on physical layer approaches aiming to achieve higher spatial diversity. Although previous work shows the benefit of cooperation in wireless networks, it does not define medium access methods that would support new cooperative schemes. To take full advantage of physical layer cooperative techniques, new MAC schemes must change the transmitter-receiver communication model to include a transmitter-relay(s)-receiver model. Common examples of cooperative MAC source-based cooperative relaying schemes are that use one relay [2], [3] or two relays in parallel [4]. Source-based relaying approaches require the source to maintain a table of CSI that is updated by potential relays based upon periodic broadcasts. As an example, with CoopMAC [2], the source can use an intermediate node (called helper) that experiences relatively good channel with the source and the destination. Instead of sending packets directly to the destination at a low transmission rate, the source makes use of a two-hop high data rate path to the destination via a helper. In case of CoopMAC, potential helpers overhear ongoing RTS/CTS transmissions for measuring the source-helper and helper-destination CSI. Based on the CSI broadcasted by potential helpers, sources update a local table (cooptable) used to select the best relay for each transmission. Source-based approaches undergo two main problems: channel estimation and periodic broadcasts, which introduce overhead that is problematic in mobile scenarios.

While source-based proposals follow a proactive approach, reactive cooperative methods [5], [6] rely on relays to retransmit on behalf of the source when the direct transmission fails. An example is PRO [5], where relays are selected among a set of overhearing nodes in two phases: First, a local qualification process takes place at potential relays, during which the link quality is compared with some predefined threshold, leading to the identification of qualified relays. In a second phase qualification information is broadcasted, allowing qualified relays to set scheduling priorities. Reactive approaches face the same challenges of source-based methods. CoRe-MAC [7] is another reactive Cooperative MAC protocol. In CoRe-MAC, when a NACK is overheard, candidate relays send an AFR (Apply For Relay) message to the destination within a fixed number of slots. After receiving non colliding AFRs, the destination elects best relay in term of highest received SNR. However the destination does not know which is the suitable number of AFR messages to wait for, in order to reach a good decision. Moreover, the extra handshake messages introduce significant overhead in case of relay failure.

N. Marchenko et al. propose a mechanism [8] where all overhearing nodes estimate the *Signal-to-Noise Ratio* (SNR) for both source-relay and relay-destination channels, based on which they can nominate themselves as potential relays. Potential relays send a nomination message to the destination, by selecting a slot in the contention window, and the destination selects a most suitable relay among all the nominated nodes. This proposal has several drawback: i) geographic position of nodes is assumed to be known; ii) the size of the contention window has great influence in selecting the best relay; iii) the destination node is not aware of the number of nominated relays.

In the case of multi-hop networks the performance gain of cooperative relaying may be exploited by finding a node that assists the transmission for every hop. Although the gain achieved through cooperation diversity increases robustness, it requires retransmissions reducing network capacity. Such a hop base cooperation scheme neglects a crucial evidence: not only the destination of a packet might be in need of help but also the next hop. An alternative approach may be to use two-in-one cooperation [6], in which a single retransmission can improve the success probability of two ordinary transmissions (source to next-hop and next-hop to destination), leading to a better usage of the network capacity. In two-in-one cooperation all potential relays react after detecting a missing *Acknowledgment* (ACK) from the destination. Although two-in-one cooperation can achieve a diversity gain of three, the most suitable relay selection scheme is not investigated.

In what concerns relay selection mechanisms, the basic mechanism defines an opportunistic behavior in which all overhearing nodes estimate the CSI of sender-node and node-destination links based on which they set a timer such that nodes with better channel conditions broadcast first their qualification as relays, or even data to be relayed [9]. Such mechanisms present a high probability of collision, as well as low efficiency in mobile scenarios due to CSI measurements. Nevertheless, opportunistic relaying has been modified aiming to increase its efficiency level [10], [11]. For instance, with relaying on demand [12], the basic relay selection mechanism [9] was modified with the introduction of a receiver threshold aiming to improve energy savings. With on-demand approaches nodes with bad channel conditions do not participate in relay selection. However, such approaches still rely upon RTS/CTS for channel estimation, leading to high overheads.

For better understanding of the different type of relay selec-

 ISBN: 978-1-61208-142-7

tion schemes, Jamal and Mendes [13] devised a comprehensive analysis and taxonomy.

III. RELAYSPOT

Relay selection is a challenging task, since it greatly affects the design and performance of a cooperative network. On the one hand, cooperation is beneficial for the network, but on the other hand it introduces extra overhead (e.g., CSI estimation). The major goal of *RelaySpot* is to minimize overhead introduced by cooperation, with no performance degradation.

Unlike previous work, RelaySpot does not require maintenance of CSI tables, avoiding periodic updates and consequent broadcasts. The reason to avoid CSI metrics is that accurate CSI is even harder to estimate in dynamic networks, and periodic broadcasts would need to be very fast to guarantee accurate reaction to channel conditions. Moreover, relay selection faces several optimization problems that are difficult to solve, which means that the best relay may be difficult to find. Hence, for dynamic scenarios, the solution may be to make use of the best possible relaying opportunity even if not the optimal one (e.g., in terms of CSI). By achieving the best performance over the faced conditions, RelaySpot aims to target a fair balance between relay selection and additional resource blockage.

In summary, RelaySpot aims to select the relay(s) based only on information local to potential relays, with minimum computational effort and overhead. The remaining of this section describes RelaySpot opportunistic relay selection, cooperative relay scheduling, and chain relaying mechanisms.

A. Opportunistic Relay Selection

The relay selection process only takes into account nodes that are able to successfully decode packets sent by a source. This ensures that potential relays are closely bounded with the source, with which they have good channel conditions. The qualification of a node as a relay depends upon local information related to node degree, load, mobility and history of transmissions to the specified destination, and not to CSI.

Node degree, estimated by overhearing the shared wireless medium, gives an indication about the probability of having successful relay transmissions: having information about the number of neighbors allows the minimization of the collision risk as well as blockage of resources. However, it is possible that nodes with low degree are overloaded due to local processing demands, leading to delay.

Equation 1 estimates the interference level that a potential relay is subjected to as a function of node degree and load. Let N be the number of neighbors of a potential relay, T_d and T_i the propagation time of direct and indirect transmissions involving such potential relay, respectively, and N_i and N_d the number of nodes involved in such indirect and direct transmissions (indirect transmissions are the ones overheard by the potential relay, and direct transmissions are the ones ending and starting at the potential relay). Adding to this, T_p is the time required for a potential relay to process the result of a direct transmission. The interference factor (I) affecting a potential relay has a minimum value of zero corresponding to no direct or indirect transmissions.

$$I = \sum_{j=1}^{N_d} (T_{dj} + T_{pj}) + \sum_{k=1}^{N_i} T_{ik}, \quad I \in [0, \infty[\qquad (1)$$

The goal is to select as relay a node that has low interference factor, which means few neighbors (ensuring low blockage probability), short transmissions and few direct transmissions (ensuring low delays).

Figure 2 shows a scenario where node R is selected as a potential relay. Node $N1$ is the direct neighbor of node R, while there are several other indirect neighbors ($N2$,$N3$,$N4$, X). Apart from R, node X also seems to be a relay candidate due to its low interference level. But it may be difficult to select R or X due to the similar interference levels: while R has a short transmission from a neighbor and a long transmission from the source, X is involved in an inverse situation. The selection of R or X as a relay can be done based on two other metrics of the RelaySpot framework: history of successful transmissions towards destination; stability of potential relays.

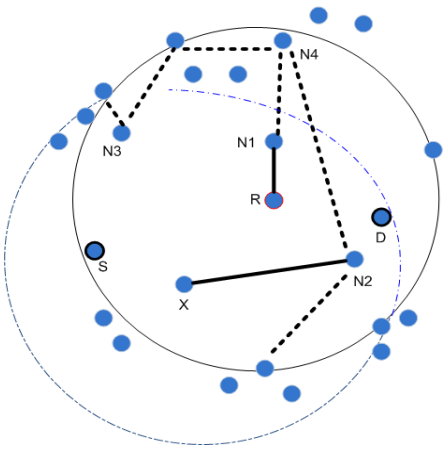

Figure 2. Opportunistic relay selection scenario

Although it is ensured that potential relays have good channel with the source, the quality of the relay-destination channel is unknown. Without performing measurement of CSI for the relay-destination channel, channel conditions can be estimated based on the successful ratio of previous transmissions towards the destination (history factor) and the current stability of a potential relay (mobility factor). The history factor (H), is estimated as a ratio between an exponential moving average of the duration of successful transmissions and the maximum duration of any successful transmission (H_M), variable that is initiated to a time unit. The factor H aims to tell whether the intended relay has probabilistically a good channel with the required destination, without the need to estimate and broadcast channel information.

The mobility factor (M) is estimated as a ratio between an exponential moving average of the pause time of the node and the maximum detected pause time (M_M), which is initiated to a time unit. The factor M aims to select more stable nodes as relays.

 ISBN: 978-1-61208-142-7

Based on the interference factor of a node, as well as its history and mobility factors, the probability of selecting a node as relay for a given destination is given by Equation 2, which shows that the selection factor (S) is proportional to the history of successful transmissions to the destination and the pause time, and inversely proportional to the interference level of the node.

$$S = \frac{H * M}{1 + I}, \quad S \in [0, 1[\tag{2}$$

Lets go back to Figure 2 to illustrate the usage of Equation 2. Lets assume that R is a node that moves frequently around the destination with a good history of successful transmissions. While X is a node with long pause times but that is new near the destination. In this case, Equation 2 may gives preference to node R, although it presents a higher mobility factor than X.

After overhearing data packets or RTS towards a destination, a potential relay uses the estimated selection factor (S) to compute the size of its contention window (CW), between a predefined minimum and maximum values of CW_{min} and CW_{max}, as given by Equation 3.

$$CW = CW_{\text{min}} + (1 - S)\,(CW_{\text{max}} - CW_{\text{min}}) \tag{3}$$

From a group of nodes that present good channel conditions with the source, the opportunistic relay selection mechanism gives preference to nodes that have low degree, low load, good history of previous communication with the destination, as well as low mobility. In scenarios with highly mobile nodes, we expect opportunistic relay selection to behave better than source-based relay selection (e.g., CoopMAC), since with the latter communications can be disrupted with a probability proportional to the mobility of potential relays, and relays may not be available anymore after being selected by the source.

As illustrated in Figure 3 the selection mechanism may leads to the qualification of more than one relay each one with different values of S, depending on current conditions. Selected relays will forward data towards destination based on its cooperative relay scheduling mechanism.

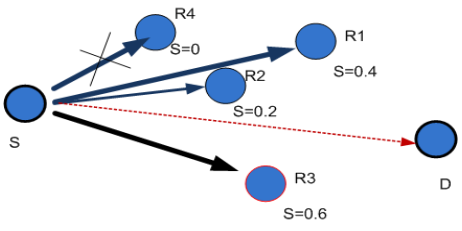

Figure 3. Opportunistic relay selection

B. Cooperative Relay Scheduling

This section describes the functionality proposed to allow self-elected relays to avoid high interference and to guarantee high data rates to a destination while preventing waste of network resources.

The contention window (computed in Eq 3) plays an important role in scheduling relay opportunities. The goal is to increase the probability of successful transmissions from relays to the destination by giving more priority to relays that are more closely bounded to the destination, while not neglecting the help that secondary relays may give. Increasing diversity, by allowing the destination to receive multiple copies of the same packet, aims to construct error free packets while avoiding re-transmissions.

Based on the quality of the packets received from all self-elected relays, the destination estimates which of the involved relays are more suitable to help in further transmissions (to get multiple copies the receiver only process received packets after a predefined time window). By sending a list of priority relays embedded in ACKs the destination allows potential relays to improve the accuracy of the back-off time computation in next transmissions (relay with highest priority sends and the other back-off but keep overhearing the transmission). This functionality leads to a space-time diversity, which leverage the space diversity used by prior art (e.g., CoopMAC). Space-time diversity is achieved by allowing the usage of different relays over time, helping the same source-destination communication.

Cooperation between selected relays, identified by the priority list embeded in ACK message, aims to ensure a high probability of selecting the best set of nodes as relays over time. Decision to switch relays is done as a consequence of a transmission. Figure 4 illustrates the cooperative relay scheduling, in a situation where R1, R2 and R3 are self-elected as relays, with R3 having smaller CW than R1 and R2 (as illustrated in Figure 3). Based on the quality of the received packets, the destination is able to decode the data by combining the packets received from R1 and R2.

In this situation the destination sends an ACK having R1 and R2 as primary relays and R3 as secondary one i.e., ACK(R1, R2; R3). This means that in the next transmission R1 and R2 will transmit (diversity 2) and R3 will back-off and overhear the transmission. Cooperative scheduling allows to keep a source-destination transmission in a good shape even when the primary relay is not useful anymore.

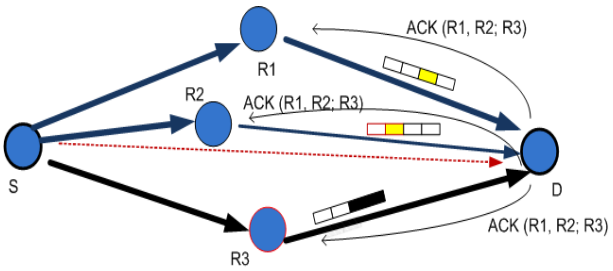

Figure 4. Cooperation relay scheduling

C. Chain relaying

The proposed opportunistic relay selection and cooperative relay scheduling mechanisms aim to increase throughput and reliability, as well as to reduce transmission delay by increasing the diversity adjusting the relaying order. Nevertheless, the presence of mobile nodes, as well as unstable wireless

 ISBN: 978-1-61208-142-7

conditions, may require higher levels of diversity achieved based on nodes that are closed to the destination (higher probability of successful transmissions). Hence, RelaySpot includes the possibility of using recursive relay selection and retransmissions in case of poor performance. This functionality is called chain relaying (c.f. Figure 5).

In a chain relaying, the relaying process is repeated for the relay-destination channel (R1-D and R2-D in Figure 5), by having another relay (R4) or set of relays helping the transmission from each of the previously selected relays to the destination. R4 may not receive correct packets from source, but it is closely bounded to R1 as well as to the destination. R4 can trigger chain relaying when both primary and secondary relays fail, which can be detected after overhearing of two recurring NACK messages (or the absence of ACKs/ NACKs) during a predefined time window. Chain relaying aims to minimize the outage and to increase the overall throughput by complementing the cooperative scheduling functionality.

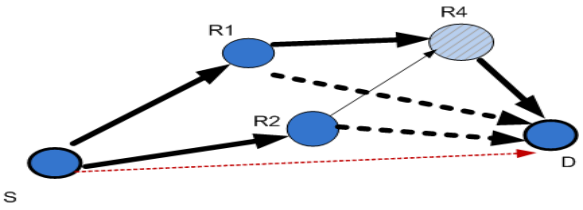

Figure 5. Chain relaying

IV. RelaySpot Algorithm in a Nutshell

The RelaySpot process is triggered by potential relays themselves (the ones with correct copies) if no ACK from the destination is overheard (c.f. Figure 6). RelaySpot operation, for a specific pair source-destination ends when there are no more packets to be send or when the destination informs the relays to stop relaying packets, after detecting that the number of damaged packets received through the direct channel from the source have decreased below a predefined threshold. This action aims to increase network capacity by allowing relays to help other endangered transmissions.

Since the opportunistic relay selection process can lead to several relays being selected, self-elected relays may adjust their priority based on the information collected from the ACK sent by the destination. The goal is to give higher priority to successful relaying operations in future transmissions.

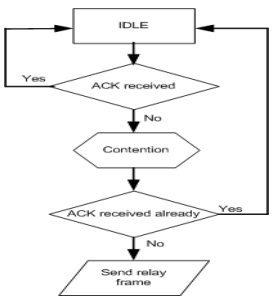

Figure 6. RelaySpot start-up flow

Due to the unpredictable conditions of relay-destination channels, the RelaySpot process can be repeated in a recursive process having relays as sources (Chain Relaying). Nodes that are able to successfully decode packets sent by a relay to a destination may trigger the RelaySpot operation on that relay-destination channel in case the channel conditions are so bad that the node will overhear two consecutive NACK (or the absence of ACKs/ NACKs) during a predefined time window. This means that relays closer to the destination can help the transmission when the destination does not get any (acceptable) packet from any relay in contact with the source.

Figure 7 illustrates the operation of the RelaySpot algorithm in comparison to CoopMAC. Lets consider that we have three potential relays (R1, R2, and R3), where R3 is the best (primary) relay. Figure 7 starts by showing that with CoopMAC at time T0 potential relays do some CSI computation and then broadcast it to source, while at that time RelaySpot potential relays does local computations of I and M factors without any transmission.

At time T1 CoopMAC relays undergoes three way handshake by introduction of “Helper ready To Send” (HTS) message, while RelaySpot potential relays updates local factors I and M without any transmission.

At time T2, CoopMAC sends data via the selected helper i.e., R3. RelaySpot potential relays first computes the selection factor S and CW after the reception of data from source, selecting R3 and R1 as relays, which then transmit data to the destination, achieve higher diversity than CoopMAC. The destination notifies the relays (in ACK message), about priority order for future transmission i.e., ACK(R3; R1). After receiving the ACK, R1 will back-off since R3 seems to be suitable to provide reliable transmissions.

At time T3, R3, the primary relay, moves away. In such case CoopMAC will repeat from start the relay selection procedure after a maximum number of retries. While in RelaySpot, the secondary relay R1 (in this example) will try to help the transmission and will send data to destination on behalf of source after detecting the missing ACK for R3 transmission (or detecting NACK). If this is successful, destination will send ACK(R1).

At time T4 we suppose that R1 is unable to cooperate too. In this situation R4 overhears two consecutive NACKs during a predefined time frame. Thus chain relaying will occur as other nodes (R1, R2, and R3) are not suitable anymore. In case of CoopMAC when there is no suitable relays, poor direct transmission will take place leading to outage.

At time T5 the destination move closer to source and the direct link between source and destination become stronger. In RelaySpot when the destination starts receiving the correct packets from source, it notifies the relays to stop cooperation (i.e., ACK(s)) and continue receiving the direct data, while in CoopMAC the data will be still relayed over the selected relay (R3 in this example).

V. Summary and Future Work

Most of the current cooperative relaying approaches use only one relay, selected based on CSI estimations, without

 ISBN: 978-1-61208-142-7

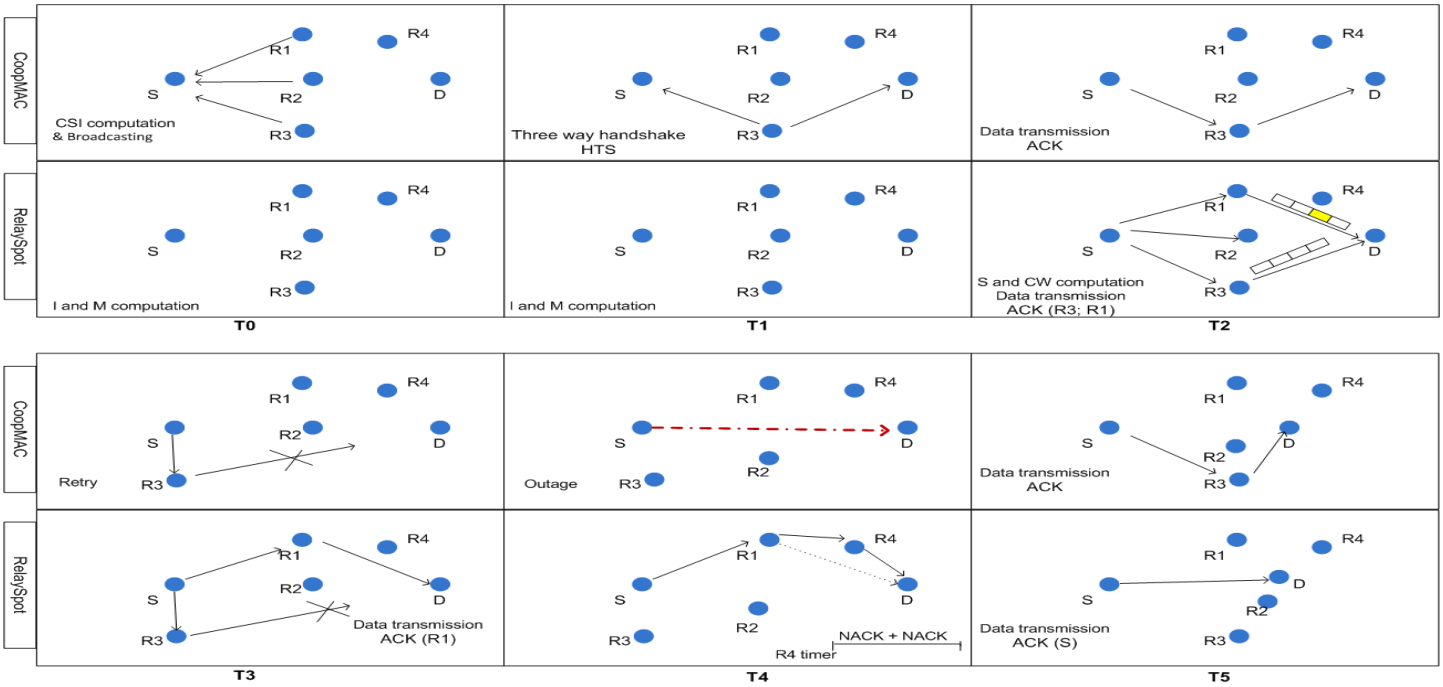

Figure 7. Illustration of the RelaySpot algorithm with chain relaying

exploiting different relays in parallel or in sequence. The proposed *RelaySpot* framework provides a set of functional building blocks aiming to opportunistically exploit the usage of several relays to ensure accurate and fast relay selection, posing minimum overhead and reducing the dependency upon CSI estimations in scenarios with mobile nodes. The proposed building blocks are related to opportunistic relay selection, cooperative relay scheduling, and chain relaying. With very dynamic channel conditions, it is expected that any solution based on the RelaySpot framework will have better performance than previous relaying proposals due to its combination of opportunistic and cooperation operations.

As future work, we aim to implement an instantiation of the RelaySpot framework in a test-bed aiming to prove the efficiency of this new type of cooperative relaying schemes. We expect to prove the potential of the RelaySpot achievements in terms of outage, delay and throughput, as well as to investigate the adjustment for the source retransmission, contention window and chain relaying timers. Finally, the impact of the hidden and expose node problems needs to be addressed, because the RelaySpot framework proposes to avoid RTS/CTS messages since their utilization depends on packet size and increasing overhead.

ACKNOWLEDGEMENT

Thanks are due to FCT for PhD grant number SFRH/BD/60436/2009. The research leading to these results has received funding from the European Commission's Seventh Framework Programme (FP7) under grant agreement n° 257418, project ULOOP (User-centric Wireless Local Loop).

REFERENCES

[1] W. Elmenreich, N. Marchenko, H. Adam, C. Hofbauer, G. Brandner, C. Bettstetter, and M. Huemer, "Building Blocks of Cooperative Relaying in Wireless Systems," *Electrical and Computer Engineering, Springer*, vol. 125, no. 10, pp. 353–359, Oct. 2008.

[2] P. Liu, Z. Tao, S. Narayanan, T. Korakis, and S. Panwar, "CoopMAC: A Cooperative MAC for Wireless LANs," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 2, pp. 340–354, Feb. 2007.

[3] Z. Hao and C. Guohong, "rDCF: A Relay-Enabled Medium Access Control Protocol for Wireless Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 5, Mar. 2006.

[4] K. Tan, Z. Wan, H. Zhu, and J. Andrian, "CODE: Cooperative Medium Access for Multirate Wireless Ad Hoc Network," in *Proc. of IEEE SECON*, California, USA, Jun. 2007.

[5] L. Mei-Hsuan, S. Peter, and C. Tsuhan, "Design, Implementation and Evaluation of an Efficient Opportunistic Retransmission Protocol," in *Proc. Of IEEE MobiCom*, Beijing, China, Apr. 2009.

[6] H. S. Lichte, S. Valentin, H. Karl, I. Aad, L. Loyola, and J. Widmer, "Design and Evaluation of a Routing-Informed Cooperative MAC Protocol for Ad Hoc Networks," in *Proc. of IEEE INFOCOM*, Phoenix, USA, Apr. 2008.

[7] H. Adam, W. Elmenreich, C. Bettstetter, and S. M. Senouci, "CoRe-MAC: A MAC-Protocol for Cooperative Relaying in Wireless Networks," in *Proc. of IEEE GLOBECOM*, Honolulu, Hawaii, Dec. 2009.

[8] N. Marchenko, E. Yanmaz, H. Adam, and C. Bettstetter, "Selecting a Spatially Efficient Cooperative Relay," in *Proc. of IEEE GLOBECOM*, Honolulu, Hawaii, Dec. 2009.

[9] A. Bletsas, A. Khisti, D. Reed, and A. Lippman, "A simple Cooperative Diversity Method Based on Network Path Selection," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 3, pp. 659–672, Mar. 2006.

[10] K.-S. Hwang and Y.-C. Ko, "An Efficient Relay Selection Algorithm for Cooperative Networks," in *Proc. of IEEE VTC*, Baltimore, USA, Oct. 2007.

[11] Y. Chen, G. Yu, P. Qiu, and Z. Zhang, "Power-Aware Cooperative Relay Selection Strategies in Wireless Ad Hoc Networks," in *Proc. of IEEE PIMRC*, Helsinki, Finland, Sep. 2006.

[12] H. Adam, C. Bettstetter, and S. M. Senouci, "Adaptive Relay Selection in Cooperative Wireless Networks," in *Proc. of IEEE PIMRC*, Cannes, France, Sep. 2008.

[13] T. Jamal and P. Mendes, "Relay Selection Approaches for Wireless Cooperative Networks," in *Proc. of IEEE WiMob*, Niagara Falls, Canada, Oct. 2010.

 ISBN: 978-1-61208-142-7

Supporting L3 Femtocell Mobility Using the MOBIKE Protocol

Patricia Noriega-Vivas, Celeste Campo, Carlos Garcia-Rubio, and Estrella Garcia-Lozano
Department of Telematic Engineering
University Carlos III of Madrid
Email: {pnoriega, celeste, cgr, emglozan}@it.uc3m.es

***Abstract*—Femtocells can be used to improve the indoor coverage and bandwidth of 3G cellular networks in homes and buildings. They are designed to be placed in a fixed location. However, their use would also be interesting in mobile environments such as public transportation systems. This paper studies the mobility limitations at the layer 3 and suggests an approach to support mobility on femtocell networks. This solution employs the protocols already defined in the femtocell architecture, minimizing thus the impact on it.**

***Index Terms*—femtocell architecture, mobile femtocell, MOBIKE, IKEv2, IPsec.**

I. Introduction

Femtocells are small, low-cost and low-power cellular base stations, typically designed for use in a home or small business (e.g., a holiday cottage) to improve indoor coverage and bandwidth, and also to off-load traffic from the existing macrocell network [1]. Nowadays, femtocells are usually deployed by the customers, they have a fixed location (i.e., they do not move), and they always connect to the 3G core network using a ciphered IP tunnel through the Internet connection provided by a Digital Subscriber Line (DSL) or cable router. However, femtocells could also be interesting in other scenarios.

Trains, buses or trams could provide faster data speeds and better user experience to theirs passengers setting up femtocells. However, supporting mobility on femtocell networks is a challenge due to their architecture, that was designed to be fixed.

Our work is focused on supporting mobility on femtocell networks by suppressing the original fixed interface and setting a pool of heterogeneous wireless interfaces in its place. Toward this end, it will be necessary to provide mechanisms that perform handovers between technologies, ensuring thus continuity of service to the users. It is expected these handovers will be performed between different technologies (inter-handover) or between interfaces of the same technology (intra-handover). Besides, different Internet service providers could be used in different interfaces obtaining redundant links and thus reliable systems.

In this paper, we investigate what modifications would be necessary at layer 3 (L3) in the femtocell protocol stack to be able to move femtocells through a heterogeneous wireless network scenario. As far as we know this is the first proposal of a change to the femtocecll architecture to support mobility. The idea is to employ the protocols already defined for femtocells and therefore minimize the impact on the existing architecture.

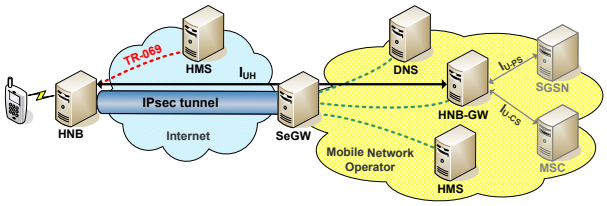

Fig. 1. 3G femtocell network overview

This paper is organized as follows. First, in section II we briefly review the architecture and terminology used in conventional femtocells. Then, Section III explains the L3 requirements and next, in Section IV, we present the IKEv2 Mobility and Multihomming (MOBIKE) protocol, an extension to Internet Key Exchange Protocol Version 2 (IKEv2) able to support mobility. In Section V, we propose a mechanism to integrate MOBIKE into femtocell networks and finally, Section VI presents the conclusions and future work.

II. Femtocell architecture

3GPP describes in [2] an architecture for 3G femtocells that includes new entities and interfaces as Figure 1 shows. This section briefly describes the main entities.

A. Home Node B (HNB)

The HNB is the femtocell. It serves User Equipment (UE) traffic by means of the U_U interface, and sends it to the core network through the I_{UH} interface. It contains part, or all the functionality normally associated to an Radio Network Controller (RNC), and supports HNB and UE registration procedures over the I_{UH} interface.

B. Home Node B Gateway (HNB-GW)

This element terminates the I_{UH} interface and acts as a concentrator to aggregate a large number of HNBs. It is seen as a RNC by the core network which communicates with it using the existing I_{U-CS}, I_{U-PS} interfaces.

C. I_{UH} interface

This interface connects the HNB with the HNB-GW. It defines two new protocols in the control plane to address the differences between HNBs and the original I_U interface:

 ISBN: 978-1-61208-142-7

- Home Node B Application Part (HNBAP) [3]: it provides functions for registering UEs and HNBs into the network, error handling and group management.
- RANAP User Adaptation (RUA) [4]: it provides the signaling service between HNB and HNB-GW in the control plane. It is used to send RANAP messages in a transparent way. It also provides error handling functions.

D. HNB Management System (HMS)

This element facilitates the discovery procedures to the HNB. It is composed of a TR-069 manager [5] and a file server. When a HNB is powered up, it will have to auto-configure using the HMS. The HMS performs location verification and assigns local access information to the HNB. This information is the Serving Security Gateway (S-SeGW), the Serving HMS (S-HMS) and optionally the HNB-GW. It can be accessed using the TR-069 protocol in two ways: through an Intranet (using the established IPsec tunnel) or through the Internet. 3GPP defines two kind of HMS:

- Initial HMS (I-HMS): it may provide location verification and assign the S-HMS, S-SeGW and optionally HNB-GW to the HNB.
- Serving HMS (S-HMS): it has new functions such as performance and fault updates, and assigns the HNB-GW during the HNB registration procedure if the I-HMS did not provide it.

E. Security Gateway (SeGW)

It terminates the IPsec tunnel established with the HNB, provides mutual authentication, encryption, data integrity and access to the S-HMS and the HNB-GW. It is a logically separated entity and it can be implemented as a separate physical element or into others such as the HNB-GW. 3GPP defines two kind of SeGW:

- Initial Security Gateway (I-SeGW): its URL may be factory programmed in the HNB to allow the establishment of the IPsec tunnel with the I-HMS.
- Serving Security Gateway (S-SeGW): it terminates the IPsec tunnel and implements a forwarding function to inject IP packets into the mobile network operator (Intranet) that allows the communication with the HNB-GW, S-HMS and other network elements.

F. Mobility limitations

When an HNB is powered up, a discovery procedure [6] is triggered to provide local access information to the HNB depending on its own location and identity. This information consists on the entities that it needs to provide the service: the S-HMS, S-SeGW and HNB-GW. Then, the HNB establishes a SCTP session with the HNB-GW and registers itself sending a `HNB REGISTER REQUEST` message. This is called the HNB registration procedure.

Similarly, when an UE connects with a HNB, an UE registration procedure is triggered to perform access control for that UE in the HNB-GW. If the operation is successful, a specific context identifier is assigned to that UE to be used between HNB and HNB-GW.

TABLE I
PROPOSED HNB REGISTER UPDATE MESSAGE

PARAMETER	PRESENCE
Message type	Mandatory
HNB Identity	Mandatory
HNB Location Information	Mandatory
New IP	Mandatory
PLMN-ID	Mandatory
Cell-ID	Mandatory
LAC	Mandatory
RAC	Mandatory
SAC	Mandatory

In the HNB registration procedure, the HNB informs the HNB-GW that it is available at a particular IP address and sends some location and identity information. If the femtocell is moving between different networks, it is expected that its IP changes and connectivity may be lost. To support mobility, the HNB should be able to update its IP address and location information to avoid context identifier losses, which are stored in the HNB-GW.

Toward this end, we propose the addition of a new HNBAP message that updates the HNB location and IP address in the HNB-GW. A possible `HNB REGISTER UPDATE` message with some proposed parameters is presented in Table I. (Consequently, it will be defined the `HBN REGISTER UPDATE ACCEPT` and `HBN REGISTER UPDATE REJECT` to indicate if the operation was successful or not).

The IPsec standardized in RFC 4301 could survive itself to an IP change by indicating how to search a security association (SA) into the Security Association Database (SAD). The SA lookup can be made by three manners:

1) Searching for a match on the combination of Security Parameter Index (SPI), destination and source address.
2) Searching for a match on both SPI and destination address.
3) Searching for a match on only SPI.

This indication must be set either manually or using an SA management protocol as IKEv2. Next section focuses in the last approach.

III. LEVEL 3 REQUIREMENTS

Femtocells were designed to use the IPsec protocol both in user and control planes. IPsec [7] is a protocol suite for securing IP communications by authenticating and encrypting each IP packet of a session. However, IPsec needs a protocol to establish and maintain security associations.

IKEv2 [8] is a component of IPsec. It is used to perform mutual authentication between two parties, to establish and to maintain dynamically SAs for Encapsulating Security Payload (ESP) [9] or Authentication Header (AH) [10] protocols.

There are several scenarios where IKEv2 can be used and this paper is centered in one particular case: when an endpoint is connected to a security gateway using the tunnel mode of

 ISBN: 978-1-61208-142-7

IPsec, since this is the scenario that femtocell networks deploy in the I_{UH} interface.

Figure 1 shows the scenario mentioned above. The HNB (or femtocell) is connected through an IPsec tunnel with the SeGW that is located within the mobile network operator. All traffic generated by the femtocell (user data and control packets) is received by the SeGW and then forwarded through the mobile network operator.

The IKEv2 protocol uses request/response pairs and every pair is called *exchange*. The first exchange in an IKEv2 session is the IKE_SA_INIT in which security parameters for the IKE SA are negotiated. If this exchange is completed, the second exchange, IKE_AUTH, will try to set up a SA for the ESP or AH protocols. These exchanges are known as Phase 1 of IKEv1.

Nonetheless, peers involved in an IKEv2 session may desire to transmit control messages to each other in order to inform about notifications or errors. To reach this behavior, IKEv2 defines an INFORMATIONAL exchange that only can be sent after the initial exchanges. Hence every message sent at this point is cryptographically protected with the negotiated keys.

Messages that belong to the INFORMATIONAL exchange contain zero or more Notify, Delete and Configuration payloads. They have to be confirmed sending some response to the initiator, even with an empty message. Otherwise the sender will assume that the message has been lost in the network and will retransmit it.

The Notify Payload is used to transmit informational data such as state information or error conditions (e.g., specify why a SA could not be established). Every type of message has a concrete value that is specified within the Notify Payload. However, IANA [11] reserves value ranges for future use.

Some reserved values have been used to create extensions to IKEv2 and thus provide new capabilities. For instance, in RFC 5685 [12] it is defined a "Redirect Mechanism for IKEv2" that allows a VPN gateway that is overloaded or it is being shut down for maintenance to redirect a client to attach another gateway. Another interesting extension to IKEv2 using Notify payloads is MOBIKE [13], [14] and it is presented in the next section.

IV. MOBIKE EXTENSION

IKEv2 itself does not provide any mobility support. MOBIKE defines an extension to the existing IKEv2 protocol to provide secure mobility.

MOBIKE can update the IP addresses associated with an IPsec tunnel mode security association using an internal API that provides access to the Security Association and Security Policy (SPD) Databases. Furthermore, it provides multihoming features to allow traffic movement between different network interfaces if for instance, the one that is being used stops working.

MOBIKE allows a peer to have several IP addresses, e.g., a road-warrior with different wireless interfaces such as UMTS or Wi-Fi. However, the decision of which IP address is used for the IPsec SA is made by the initiator peer and it is beyond of the scope of this protocol.

TABLE II
NEW ERROR TYPES DEFINED BY MOBIKE

NOTIFY PAYLOAD	MESSAGE TYPE
UNACEPTABLE_ADDRESS	40
UNEXPECTED_NAT_DETECTED	41

TABLE III
NEW STATUS TYPES DEFINED BY MOBIKE

NOTIFY PAYLOAD	MESSAGE TYPE
MOBIKE_SUPPORTED	16396
ADDITIONAL_IP4_ADDRESS	16397
ADDITIONAL_IP6_ADDRESS	16398
NO_ADDITIONAL_ADDRESSES	16399
UPDATE_SA_ADDRESSES	16400
COOKIE2	16401
NO_NATS_ALLOWED	16402

The standard defines some new IKEv2 notifications whose values are shown in Tables II and III. Although these messages are protected by the keys negotiated in the first exchange of IKEv2 (IKE_SA_INIT), updating an IP address of IPsec SAs has several security considerations. To address them, two new features are included: with "return routability check" one peer can verify if the other party has an available IP address and therefore can receive packets. Conversely with "NAT prohibition" it is assured that IP addresses have not been modified by intermediate agents such as NATs or translation agents.

A. Mobility issues

As in IKEv2, a MOBIKE session is initiated using the normal IKE_INIT exchange. After that, in the IKE_AUTH exchange, every peer informs the other that it supports MOBIKE by means of MOBIKE_SUPPORTED notification.

If the initiator changes its IP address it will send an UPDATE_SA_ADDRESSES notification from the new IP address and thereafter it will be the source address. The responder will save this IP and may perform the "return routability check" of the new address and if it is completed the responder will start to use it as destination address.

The responder does not normally update any IPsec SA unless it receives an explicit UPDATE_SA_ADDRESSES notification from the initiator. However, the update process can be triggered by IKEv2 events. Next events can cause the initiator to re-evaluate its address selection policy, and may trigger an IP address change:

- Several IKEv2 requests have been transmitted and no reply has been received. This suggests that the path is no longer working.
- Receiving an ADDITIONAL_IP4_ADDRESS, ADDITIONAL_IP6_ADDRESS or NO_ADDITIONAL_ADDRESS notification means the addresses may have changed.

 ISBN: 978-1-61208-142-7

- Receiving an UNACCEPTABLE_ADDRESSES notification as a response to an address update means that the update was not carried out.
- Receiving a NAT_DETECTION_DESTINATION_IP [8] notification by the initiator that does not match with the UPDATE_SA_ADDRESSES response. This means that address has changed.

B. Multihoming support

MOBIKE also manages multihoming devices. One peer may inform that it has several IP addresses sending an ADDITIONAL_IP4_ADDRESS (or ADDITIONAL_IP6_ADDRESS) notification in the IKE_AUTH exchange. These messages contain a list of available IP addresses where the peer can receive packets.

Due to the mobility nature of this scenario it is likely that the IP pool changes depending on the peer location. To overcome this issue, MOBIKE uses the same two messages mentioned above to update the list of IP addresses available. Note that it will have to send the whole list and not just IPs that have changed (i.e., there are no separate add/delete operations) replacing the old list.

Both the initiator and responder can send a list of available IP addresses but it is the initiator who uses it as an input to its address selection policy. The initiator may decide to move traffic to an address of the list sending an UPDATE_SA_ADDRESSES.

On the other hand, the responder only uses the initiator (and its own) list when its current address may no longer work and it wants to update the address set. It uses both lists to determine which pair of addresses to use for sending the ADDITIONAL_IP4_ADDRESS (or ADDITIONAL_IP6_ADDRESS) message.

V. Proposed method

MOBIKE protocol defines a mechanism to provide secure mobility but it does no specify how the initiator makes the decision to update an IP address, i.e., when it is initiated, what information is taking into account, how preferences affect the decision... Designing a system that decides when an update IP address procedure has to be triggered may be crucial in real scenarios, moreover when it is moving.

This section presents some design criteria that should be taken into account in order to build a system able to trigger a handoff procedure and thus changing from one wireless interface to another depending on the environment measurement at a given time. Note that we include inter-technology handover, where it is performed between different wireless technologies (e.g., WiMAX to UMTS handoff) and intra-technology handover, that implies, at least, the use of two different interfaces of the same technology (e.g., Wi-Fi to Wi-Fi handoff). Using several wireless interfaces from the same technology we can also build reliable systems due to the redundant links.

We propose the use of MOBIKE on femto-architectures to address the mobility limitations encountered at L3. Specifically, to maintain in a secure way the IPsec tunnel established over the I_{UH} interface.

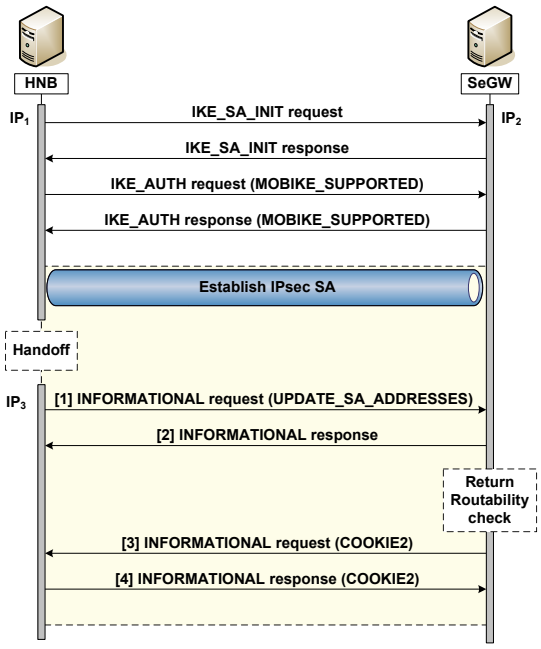

Fig. 2. MOBIKE handoff procedure

We show in Figure 2 how the handoff procedure between a HNB and a SeGW would be if MOBIKE protocol were implemented in both parties.

The first step is the normal IKEv2 IKE_SA_INIT exchange. Then, the HNB and SeGW inform each other that they support MOBIKE sending MOBIKE_SUPPORTED notification (IKE_AUTH exchange). Finally the IPsec SA is established between the addresses taken from the IKE SA, IP_1 and IP_2.

Suppose after a while a new IP address, IP_3, is obtained by other interface and a handover is triggered by decision of the HNB. The HNB should notify that there is a change in its own IP address sending an UPDATE_SA_ADDRESSES notification from the new IP address, i.e., IP_3. When this notification is received by the SeGW, it records the new IP and performs a "return routability check" of that address sending an INFORMATIONAL request with a COOKIE2 notification.

The COOKIE2 notification is added to ensure that the HNB has seen the request after sending a response. If both values do not match, the IKE SA must be closed. Otherwise, if the check is completed, SeGW starts using IP_3 as the destination address for its traffic.

Although both initiator (HNB) and responder (SeGW) could have sent ADDITIONAL_IP4_ADDRESS (or ADDITIONAL_IP6_ADDRESS) notifications in the IKE_AUTH exchange to inform each other that they have a set of available IP addresses, just the initiator uses it as an input to its address selection policy. On the contrary, the responder only uses this list when it needs to update its own list and its current IP is not working.

Therefore, it seems a good idea to use the initiator list by

 ISBN: 978-1-61208-142-7

the responder to recover a connection when the initiator is not responding and an UPDATE_SA_ADDRESSES has not been received. If the responder suspects there is a problem with the current initiator IP, it should check its validity sending some packets. If no response is received after a while, the responder should discard the current IP and it should test the next IP in the initiator list. If a response is received, it should send an UPDATE_SA_ADDRESSES to switch to the new address. To this end, a timer should be configured according with some quality criteria (establishing a minimum delay acceptable, for instance). When the timer expires, the responder should consider the initiator unreachable and it should start checking the next IPs in the list.

A. Delay considerations

In MOBIKE, every time an initiator device performs a handoff procedure, several messages are exchanged. Depending on the throughput of the crossed mediums these messages will reach their destination at a given time. In addition some technologies have different throughput in their uplink and downlink, thus the delay varies according to that fact.

In Figure 2, time required by a handoff process is the time that has passed between message 1 and message 4. Let $T_{tx-update}$, $T_{tx-update-ack}$, $T_{tx-verify}$, $T_{tx-verify-ack}$ denote the transmission time required for the messages 1, 2, 3 and 4 in the handoff procedure, T_{prop} the propagation delay associated with the crossed mediums and T_{proc} the time required for a device to process a request and build a response. The time required to complete a handoff procedure, $T_{handoff}$, is represented by the following expression assuming the propagation and processing delay are negligible:

$$\begin{aligned} T_{handoff} &= T_{tx-update} + T_{tx-update-ack} \\ &+ T_{tx-verify} + T_{tx-verify-ack} \end{aligned} \quad (1)$$

Note that the transmission times depends on the throughput and the packet size. Indeed, if the network is asymmetrical regarding to speed (UMTS, WiMAX, LTE...) messages that are sent through the uplink will take longer than those that are received through the downlink. In our case, $T_{tx-update}$ and $T_{tx-verify-ack}$ are sent through the uplink and $T_{tx-update-ack}$ and $T_{tx-verify}$ through the downlink.

Although the propagation delay is considered negligible compared with the transmission times, in some scenarios this delay should be considered. Propagation delay depends on the medium speed and the distance between both parties. Thus, if the medium speed is very low and the distance high the propagation delay should be considered in the previous expression, furthermore if the device is moving at a high speed and the delay may be critical. Now, the $T_{handoff}$ expression is represented by:

$$\begin{aligned} T_{handoff} &= T_{tx-update} + T_{tx-update-ack} \\ &+ T_{tx-verify} + T_{tx-verify-ack} \\ &+ 2T_{prop-UL} + 2T_{prop-DL} \end{aligned} \quad (2)$$

However, if a handoff is triggered and the "return routability check" is performed, messages that belong to this process can be also sent into the first INFORMATIONAL exchange (messages 1 and 2 in the Figure 2), i.e., including the COOKIE2 payload into it. With this strategy $T_{prop-DL}$ and $T_{prop-DL}$ would be suppressed in (2) but $T_{tx-update}$ and $T_{tx-update-ack}$ would be higher due to the packet size increases.

Delay is an important issue to take into account when systems have been design to ensure continuity of service, moreover when the system is moving through a heterogeneous wireless network, where the throughput can be different in every hop. In addition, it may be critical if the system is moving at high speeds and the size of the following cell is small, since the period of time available to perform handover decreases. Therefore, it is necessary to address the limitations resulting from the delay taking them into account in the design phase of the system.

In the handoff procedure the throughput measured in the uplink should be considered, since it is always the slowest link in every wireless technology (in symmetrical technologies both links have the same speed). Since MOBIKE performs hard-handover (i.e., it does not use both links at the same time) two scenarios can be seen depending on the speed of the mediums crossed:

1) If the femtocell moves from a slow medium to a faster one, it will be more efficient if the handoff is performed as soon as possible, using the fastest link for long time and thus obtaining a better performance.
2) If the femtocell moves from a fast medium to a slower one, it will be more efficient if the handoff waits, as far as feasible, exploiting thus the use of the faster medium.

Next section discusses other issues to perform an efficient handoff procedure regarding to the received power.

B. Power-driven threshold

In this theoretical approach we are assuming that a femtocell can be connected to several wireless network interfaces such as Wi-Fi, UMTS, WiMAX, etc. All these technologies have different features and requirements, and it would be helpful if the femtocell could use the most suitable one at a given time. In mobile environments it is expected that handovers occur frequently, hence the importance to perform them efficiently (to a suitable technology, at a given time).

We propose the *Power-driven threshold* approach, that consists on establishing a quality threshold in terms of received power. Its value will be normalized to be the same in all technologies, since every one has a concrete range of received power required for an acceptable performance. Whenever the system obtains an IP from a given technology, it will be set as available if its received power is above the threshold. Moreover, if there are several available technologies in the pool, the selected one to perform the handover will be decided based on policies such as cost, bandwidth, security...

The handover to other available technology must be triggered when the received power of the used link lowers and reaches the threshold. Then, a rule set will be applied over the available technologies to decide which is the most suitable

 ISBN: 978-1-61208-142-7

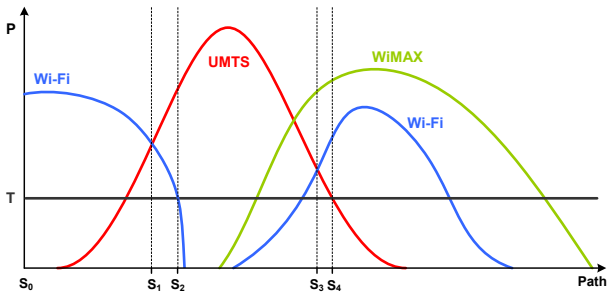

Fig. 3. Power-driven threshold scheme

one. These rules will be defined considering the network performance, cost, bandwidth, security and so on.

In Figure 3 we represent a graph to show the *Power-driven threshold* behavior. The vertical axis depicts the normalized received power in the femtocell and horizontal axis depicts the path that it follows. The threshold has been placed to normalized power T.

Let us assume that in the initial location, S_0, the femtocell is being served by Wi-Fi and its source IP is IP_1. Due to its mobility it may detect some other available technologies along the path. When the femtocell crosses S_1 the UMTS received power is stronger than Wi-Fi. However, the handover will not be perform until S_2 due to the threshold constraint. Then, the femtocell sets IP_2 as a source IP. Some hysteresis will be included in the threshold to avoid bounding between technologies in border areas.

After a while, the femtocell is being served by UMTS. When it reaches S_3, the received power of the WiMAX and Wi-Fi signals are above the threshold (and above the UMTS signal that is being used). At this moment the femtocell would have two alternative IP addresses in the pool, IP_3 and IP_4 obtained respectively by WiMAX and Wi-Fi. When the UMTS power reaches the threshold value at S_4, a decision process will be triggered to decide which of both technologies is the most suitable to perform the handover, by applying the rule set. For instance, a rule could be defined to prefer Wi-Fi over WiMAX because of the cost or to prefer WiMAX over UMTS because of the bandwidth.

Due to the waiting constraint, this technique decreases the number of handoff procedures and thus the messages sent, that seems to be an advantage in mobile environments (especially when the speed is high). However, the efficiency can be reduce when the femtocell is moving from a slow to a faster medium, since it is using the slower one until the threshold is reached.

This approach could be improved by using location prediction algorithms such as the ones shown in [15] if for instance the femtocell path is known a priori as occurs in public transportation scenarios.

VI. Conclusions and Future Work

This paper explained the MOBIKE protocol and presented a novel approach to integrate it into a femtocell scenario to support mobility management in the I_{UH} interface and between the HNB and the SeGW.

We have studied some considerations at L3 to support mobility on femtocell networks. However, some of them may interfere in the behavior of upper layers.

In their control plane, femtocells implements SCTP that is also a multihoming protocol able to support mobility at the transport layer. We are now working on the implications using MOBIKE over SCTP have, and on how to integrate them to work together reusing information, such as the change of IP address in L3.

Similarly, we are studying what implications MOBIKE over GPRS Tunnelling Protocol User Plane (GTP-U) have, since it is used by the femtocells in the user plane at the Packet Switched (PS) domain and tunnels are also used.

Finally, we are simulating and testing some MOBIKE scenarios using strongSWAN [16] to evaluate the $T_{handoff}$ defined theoretically according to different paths and speed. Then, it will be investigated how to relate it with the power threshold and the femtocell speed in order to build an efficient system able to provide continuity of service to its customers.

Acknowledgment

This work has been supported by the Spanish Ministry of Science and Innovation, CONSEQUENCE project (TEC2010-20572-C02-01) and partially supported by the Madrid regional community project CCG10-UC3M/TIC-4992.

References

[1] G. de la Roche and J. Zhang, *Femtocells: Technologies and Deployment*. Wiley, December 2009.
[2] *TS 25.467: UTRAN architecture for 3G Home Node B (HNB); Stage 2 (Release 9)*, 3GPP, June 2010.
[3] *TS 25.469: UTRAN Iuh interface Home Node B (HNB) Application Part (HNBAP) signalling (Release 9)*, 3GPP, September 2010.
[4] *TS 25.468: UTRAN Iuh Interface RANAP User Adaption (RUA) signalling (Release 9)*, 3GPP, September 2010.
[5] *TR-069: CPE WAN Management Protocol v1.1, Version: Issue 1 Amendment 2*, Broadband Forum, December 2007.
[6] *TS 32.583: Telecommunication management; Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Procedure flows for Type 1 interface HNB to HNB Management System (HMS) (Release 9)*, 3GPP, December 2009.
[7] S. Kent, *Security Architecture for the Internet Protocol (RFC 4301)*, December 2005.
[8] C. G. Kaufman and P. Hoffman, *Internet Key Exchange Protocol Version 2 (IKEv2) (RFC 5996)*, September 2010.
[9] S. Kent, *IP Encapsulating Security Payload (ESP) (RFC 4303)*, December 2005.
[10] S. Kent., *IP Authentication Header (AH) (RFC 4302)*, December 2005.
[11] *IANA: Internet Assigned Numbers Authority*, http://www.iana.org, Last Accessed: 28 february, 2011.
[12] V. Devarapalli and K. Weniger, *Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2) (RFC 5685)*, November 2009.
[13] P. Eronen, *IKEv2 Mobility and Multihoming Protocol (MOBIKE) (RFC 4555)*, June 2006.
[14] T. Kivinen and H. Tschofenig, *Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol (RFC 4621)*, August 2006.
[15] A. Rodriguez-Carrion, C. Garcia-Rubio, and C. Campo, "Performance evaluation of LZ-based location prediction algorithms in cellular networks," *Comm. Letters.*, vol. 14, pp. 707–709, August 2010.
[16] *strongSWAN: The OpenSource IPsec-based VPN Solution for Linux*, http://www.strongswan.org, Last Accessed: 28 february, 2011.

 ISBN: 978-1-61208-142-7