A TUNNEL-BASED SOLUTION FOR SEAMLESS VERTICAL HANDOVER AND LOAD BALANCING

Iustin Alexandru IVANCIU Andrei Bogdan RUS Virgil DOBROTA
Technical University of Cluj-Napoca, Communications Department, 400027 Cluj-Napoca, Romania,
Phone: +40-264-401226, Fax: +40-264-597083,
Emails: {Iustin.Ivanciu, Bogdan.Rus,Virgil.Dobrota}@com.utcluj.ro

Abstract: This paper proposes a multi-tunnel architecture with a smart mobile router offering uninterrupted services for its wireless customers. It simultaneously uses several wireless/mobile access networks to the Internet in order to reach the service continuity gateway located somewhere in a broadband network. This customer-oriented approach offers seamless connectivity through vertical handover and load balancing.

Keywords: *Handover, load balancing, tunneling.*

I. INTRODUCTION

In intelligent transportation systems a lot of effort is carried out nowadays to investigate whether Wi-Fi access can be used to augment 3G/4G capacity in mobile environments, e.g. from moving vehicles. For instance a system called Wiffler is presented in [2]. It combines multiple interfaces with different costs and degrees of ubiquity in order to reduce costs while meeting application requirements. Wiffler offloads data to Wi-Fi as long as application requirements are met and fast switches to 3G if the packets cannot be transmitted successfully within a small time window. Wiffler was implemented and deployed in a vehicular testbed. Experiments show a significant decrease of 3G usage for a realistic workload. The authors of [3] design and implement Cabernet, a system for delivering data to and from moving vehicles using open Wi-Fi access points encountered opportunistically during travel. Two new components for improving data delivery to moving vehicles are presented. QuickWi-Fi is a client-side process which reduces mean connection time. CTP is a transport protocol that distinguishes congestion on the wired portion of the path from losses occurring on the wireless link and leads to an increased throughput. Experiments show that Cabernet is suitable for a large class of non-interactive vehicular applications. Paper [4] presents PluriBus, a system that enables high-performance Internet access on-board moving vehicles. PluriBus seamlessly bonds multiple wide-area wireless links characterized by high delays and loss rates into a reliable communication channel. PluriBus uses delay-based path selection and packet striping. A new technique called opportunistic erasure coding is introduced. Coded packets are only sent when there is instantaneous spare capacity along the path. Evolution codes, designed for partial recovery, are used. They maximize the number of packets recovered with each coded packet.

None of the existing approaches investigated responded to the need of seamless connectivity in a transportation and/or emergency system involving the mobility of the end users. This paper proposes a multi-tunnel architecture with a mobile router offering uninterrupted services for its wirelessly connected customers. The mobile router simultaneously employs several access networks (IEEE 802.11, 3G, 4G/LTE) to the Internet in order to reach a service continuity gateway located somewhere in a broadband network. The intelligent selection of the tunnels is based on active measurements of the end-to-end Available Transfer Rate between the router and the gateway. This whole process is transparent to the infrastructure operators.

The rest of the paper is organized as follows. Section II describes the background and motivation, followed in Section III by the architecture of a seamless vertical handover and load balancing, considering wireless and mobile access networks. The experimental results in Section IV prove that seamless connectivity without provider intervention is feasible for the proposed solution. Conclusions and future work end the paper.

II. BACKGROUND AND MOTIVATION

This work is partially based on the previous involvement within the FP7-UCONNECT project, which aimed to reach ubiquitous connectivity for public transport. The idea was to implement three connectivity systems: a) a seamless vertical handover one, without cutting the services; b) a seamless roaming system, without depending on which operator is exploiting the access network; c) an interoperability system for efficient transmission and operational costs [5]. However we expanded this previous work and we investigated additional use cases suited for the proposed solution. Thus the emergency service vehicles (ambulances, fire trucks) are clear beneficiaries of it, without needing to overlap the 112 (or 911) systems. We refer to the case of a smart router, running on ambulances for instance, and offering seamless connectivity needed for remote support from hospitals (patient databases, tele-monitoring, tele-diagnosis), or for information about road traffic to the closest premises. This kind of information may/may not be available through the

Manuscript received September 2, 2014; revised September 27, 2014

emergency systems anytime, anywhere, but not all the staff is authorized to use it. Supposing a natural disaster or a major accident occurs, the seamless vertical handover and load balancing architecture could be an alternative to un-efficient use of the public/private networks. Also, a more complex remote monitoring of patients has to be considered, whenever an existing solution of sensors connected through a smartphone to one wireless and/or one mobile operator is not providing enough intelligence.

The key characteristics of the proposed architecture are the following: several simultaneously available wireless/mobile operators, customer-oriented, seamless connectivity. The solution is based on load balancing and vertical handover at flow-level, which is less complex and more feasible to be implemented than at packet-level. Furthermore, tunneling means that encryption is possible for a better security and confidentiality of the exchanged information. *Figure 1* presents the main modules: a) active measurements; b) flow identification; c) algorithm for GAP; d) vertical handover and load balancing. Note that the interoperability system which assures the communication between these modules is not depicted herein.

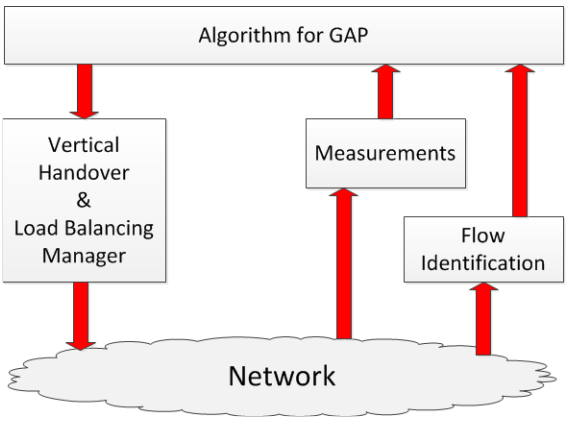

Figure 1. Modules of the tunnel-based solution for seamless vertical handover and load balancing defined in FP7-UCONNECT

The next sections will discuss the vertical handover and load balancing manager only. The novel features obtained by combining in a clever manner the existing support for measurement, flow identification and others are not covered within this paper, but details are in [5].

III. VERTICAL HANDOVER AND LOAD BALANCING

In this paper we refer to VHO (Vertical Handover) as the change of connectivity from one access network carrier to another. Load balancing is defined herein as an aggregated flow-level distribution implemented through VHO. Thus we have a smart router performing flow-level de-multiplexing on multiple access links (i.e. mobile operators). Two specialized modules were designed and implemented for the proposed platform. One software component is custom made for the SMR (Smart Mobile Router) device, while the second one was designed and implemented for the SCG (Service Continuity Gateway) component. As presented in *Figure 2*, the main idea consists of creating a separate tunnel through each mobile carrier between the SMR and SCG entities. Thus, when sending data through a specific tunnel, the traffic will be forwarded using the desired data operator.

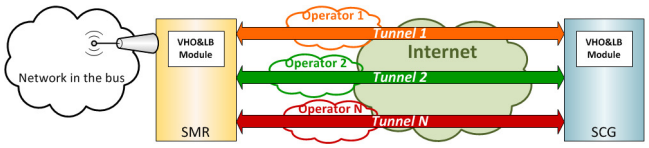

Figure 2. Communications architecture between SMR and SCG entities

The main desiderate is to maintain the VHO and LB operations transparent to the user. As a consequence, it is important to keep all existing communication sessions running, no matter how many times we have to change the utilized operator, for a specific data flow (a flow is identified by the following information: a) source and destination IP address; b) source and destination port; c) transport layer protocol used).

Before presenting the solution, it is important to understand the challenge that must be resolved by the system. Because the IP addresses assigned to the users in the bus are private, NAT (Network Address Translation) must be activated on the Smart Mobile Router. As a consequence, whenever the output interface at SMR side is changed, the source IP address of the forwarded packets is modified. This will break any communication session previously created. To counteract this side effect, the data traffic must be sent through a gateway (i.e. SCG) before being forwarded to the destination. A second NAT mechanism is enabled on the Service Continuity Gateway so that from the destination perspective the source address of the packets will remain unchanged no matter the mobile carrier used between the SMR and SCG devices. VPN (Virtual Private Network) tunnels are created through each available wireless data carrier using the OpenVPN tool available for Linux platforms. Note that a tunnel will be enabled only at the specific request of the SMR entity within the bus.

A. Initializing and Registration

The first two steps presented in *Figure 3* are being performed only once, when the module is first time executed.

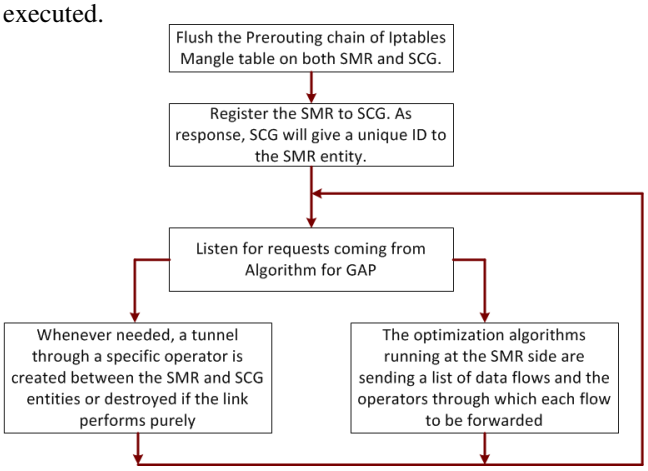

Figure 3. The most important steps performed by the VHO&LB module

The first one consists of cleaning the prerouting chain of the mangle table within iptables, because some “leftovers”

that could interfere with the desired functionality might be present on the device. Furthermore, the SMR must register to the SGC entity because it needs to acquire a unique identifier. Due to the fact that SCG is the only entity that has a global view of the whole SMR fleet, it will be the one assigning these unique IDs.

A detailed description of the interaction between the SMR and SCG when implementing these two steps can be observed in *Figure 4*. The registration process is being made in two phases:

a) SMR sends a register request message
b) SCG responds with a message containing the assigned ID.

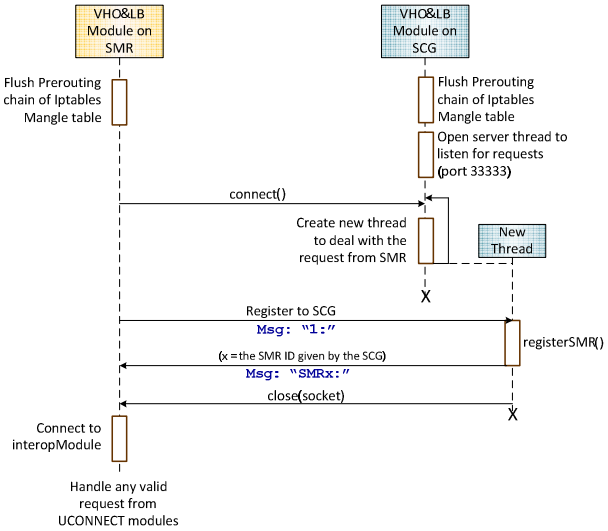

Figure 4. Registration of Smart Mobile Router to the Service Continuity Gateway

B. Creating/ Destroying a Tunnel

Whenever the VHO&LB Module on the SMR receives a tunnel creation message it performs the following set of operations:

1. Send a signaling message to the SCG to create a tunnel with a specific set of data.
2. Waits for a response from the SCG. If at the SCG side the tunnel was created with success, the SMR will perform the needed operations to enable its side of the VPN tunnel. Finally the module will inform the controlling entity (i.e. the one that requested the tunnel creation) regarding the success of the entire operation by sending back the received message and additionally adding the OK or ERROR information. The above steps are depicted into *Figure 5*.

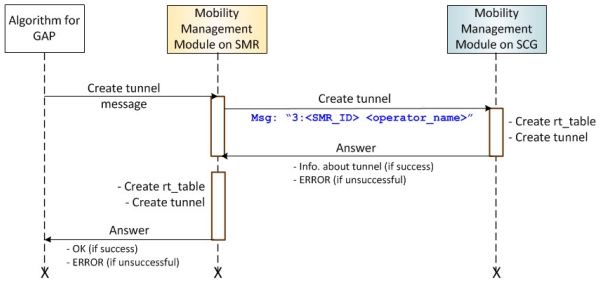

Figure 5. Creating a tunnel

Regarding the process of disabling a tunnel, whenever a destroy message is being received from the algorithm for GAP, the first step will be performed at the SCG side, continuing with the destruction of the tunnel at SMR side.

C. Vertical Handover and Load Balancing

The Vertical Handover and Load Balancing operations are being made at flow level. Actually, LB operations will be implemented by moving flows to specific tunnels in order to meet a set of requirements (i.e. maximize global transfer rate, minimize cost). When the performance of one connection changes, the flows carried out by the link with problems will be redistributed, using VHO operations, among the available access networks (see *Figure 6*). The distribution of data flows between available tunnels/ operators will be controlled by the algorithm for GAP that has an accurate view regarding available resources on each link towards the Internet, together with the number of flows that need to be forwarded by SMR and their transfer rate.

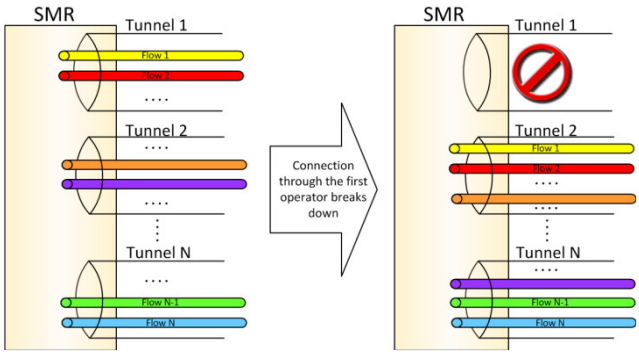

Figure 6. Redistributing flows among available data carriers

Because the KPI (Key Performance Indicators) of access links are varying in time, the algorithm will send updates every second (interval can be adapted if needed), to the VHO&LB Module so that the entire system reacts to any performance change that might occur. The mechanism that performs the VHO and LB tasks is composed of the following steps (see *Figure 7*).

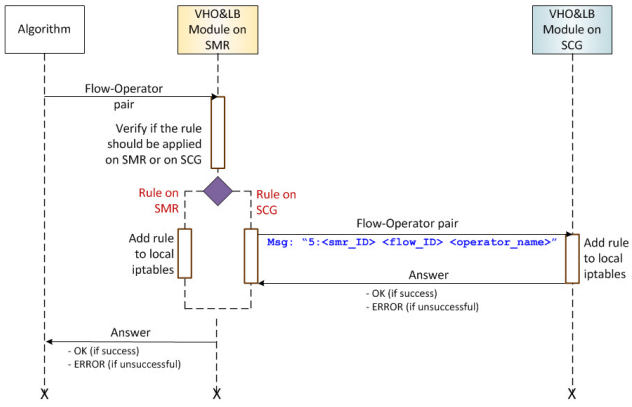

Figure 7. Change the operator through which a flow is being forwarded

A message related to the assignment of a flow to a given tunnel is received from the algorithm for GAP. SMR verifies

if the rule should apply to local *iptables* or to the one on SCG (if the flow ID corresponds to an upload one, the rule will be applied locally otherwise the rule will be sent to SCG). If the rule is applied into the local *iptables*, the marking value will be set according to the operator/ tunnel through which the data flow needs to be forwarded. If the rule must be applied at the SCG side, a control message containing the flow ID and the operator through which the data should be forwarded will be sent back to SMR. At the end, the VHO&LB Module on the SMR will inform the algorithm if setting the *iptables* rule was successful or not.

Note that SCG is able to prevent an unauthorized user to pretend it is the SMR and forward its traffic through the gateway. Thus, whenever SMR registers to the SCG, a VPN tunnel can only be created if the router holds a certain key. Even if a rogue SMR registers to the gateway, no VPN tunnels will be created. Therefore no data will be forwarded through the SCG. This mechanism is running permanently, because the connections between the SMR and SCG come and go depending on access networks availability.

IV. EXPERIMENTAL RESULTS

The testbed previously presented in *Figure 2* provides seamless connectivity which should be transparent to the user. Depending on how fast we move one flow from one tunnel to another, minor freezing of the service may occur. However this does not mean that the service is interrupted. For instance the TCP connections between SCG and the destination are kept, whilst just the access network from SMR to SGC is modified. We considered a realistic scenario, where 3G access is available anytime, anywhere within the testbed, whilst both Wi-Fi1 and Wi-Fi2 may not be available all the time and/or everywhere.

Suppose three controlled flows are sent: *Flow 1*: 1800 kbps, *Flow 2*: 64 kbps, and *Flow 3*: 185 kbps. The ATR measurement process is performed continuously for the two wireless networks using a software tool developed by us, called ATRAM [5]. For the mobile operator, the measurement process is performed once every 15 seconds by means of the *iperf* tool. The algorithm for GAP tried to minimize the cost of sending the data through the tunnels. A key issue is to determine how frequent it should be activated, envisaging from once every second up to once every several seconds.

In order to calibrate the software tools, we first performed *Experiment No.1*. The previously mentioned flows are not actually delivered through the selected tunnels, but the algorithm for GAP is running and decisions are being made every 10 seconds (the optimum value will be determined later on). Based on the minimum measured ATR, we obtained the results in *Table 1*. However trivial, they help us validate the selection.

For the 0…10 seconds interval all the flows could be sent through *Tunnel 1* (1,800+64+185=1,949 kbps < 2,000 kbps) but this would not lead to the minimum cost. Instead, the algorithm decides to send Flow 3 rather than Flow 2 through *Tunnel 2* (free of charge) thus minimizing the total cost. Other allocations are either impossible or provide a greater total cost.

Similarly, the interval 30…40 seconds all the flows could be sent through *Tunnel 3* (1,800+64+185=1,949 kbps < 3,900 kbps) but again this would not lead to the minimum cost. The best allocation is the one given in *Table 1*.

Time interval [s]	Tunnel	Minimum ATR [Mbps]	Decision proposed by the algorithm for GAP
0-10	1	2	Flow 1, Flow 2
	2	0.2	Flow 3
	3	3.8	
10-20	1	3.8	Flow 1, Flow 2
	2	0.2	Flow 3
	3	3.6	
20-30	1	4	Flow 1, Flow 2
	2	0.2	Flow 3
	3	3.8	
30-40	1	1.5	Flow 2
	2	0.2	Flow 3
	3	3.9	Flow 1
40-50	1	1.5	Flow 2
	2	0.2	Flow 3
	3	3.9	Flow 1
50-60	1	2	Flow 1, Flow 2
	2	0.2	Flow 3
	3	3.9	

Table 1. Experiment No.1 for calibrating

Finally, the results confirmed that the tool is properly calibrated. Indeed, the mobile operator, although it is always available, is rarely selected since it has the highest cost. The *Experiments No.2-4* try to answer to the question related to the frequency of applying algorithm for GAP.

Suppose three flows have to be sent through these tunnels:

- *Flow 1*: video stream of 1517 kbps on average
- *Flow 2*: Skype call stream of 41 kbps on average
- *Flow 3*: data stream of 218 kbps on average

We investigated three cases: *a) Experiment No.2:* algorithm used once every second; *b) Experiment No.3:* once every five seconds, and *c) Experiment No.4:* once every ten seconds. All of these 150-second experiments involved that the three flows were actually delivered through the real testbed. The results are summarized in *Table 2* and *Figures 8-12.*

Thus *Figure 8* depicts the rates of the three flows. While the Skype call *(Flow 2*) and the data flow (*Flow 3*) have a rather constant rate, it can easily be observed that the video stream *(Flow 1*) has a rate which varies significantly over time. *Figure 9* illustrates the Available Transfer Rates of the three tunnels opened through the three different carriers. The results were obtained by running ATRAM continuously for the two wireless links. For the 3G carrier, iperf was used every 15 seconds thus providing a total of 10 measurement results. The allocation of the flows on the three tunnels is presented in *Figures 10-12* for *Experiment No. 2* only. For *Experiment No.3* and *No.4* the decision algorithm was executed off-line, using the same data obtained from the measurements in *Experiment No.2*. Whilst the majority of traffic is carried through Tunnel 3, Tunnels 1 and 2 are used whenever the ATR permits it in order to decrease the total cost.

The advantage of performing the algorithm for GAP once every second can easily be observed as the flows may be allocated to a tunnel as soon as the ATR for that specific tunnel becomes large enough. Moreover, the number of

reallocations is not an issue since the process is transparent for the user. A reallocation represents the number of flows that have to be moved from their current tunnel based on the decision made by the algorithm solving GAP. Since there are three flows it means that every time a decision is made, the maximum number of reallocations is three. If the algorithm for GAP is performed once every second, the maximum number of reallocations is equal to 450 (i.e. 150 seconds x 3 reallocations/ second). Performing the algorithm once every 5 seconds leads to a maximum number of 90 reallocations whilst if the algorithm is performed once every 10 seconds there can be no more than 45 reallocations. The number of reallocations obtained by performing the three tests is depicted in *Table 2*.

Time between algorithm decisions [s]	Maximum number of reallocations	Experimental number of reallocations	Real/ maximum number of reallocations [%]
1	450	34	7.55
5	90	17	19.88
10	45	11	24.44

Table 2. Number of reallocations made by the algorithm for GAP No.1 for calibrating

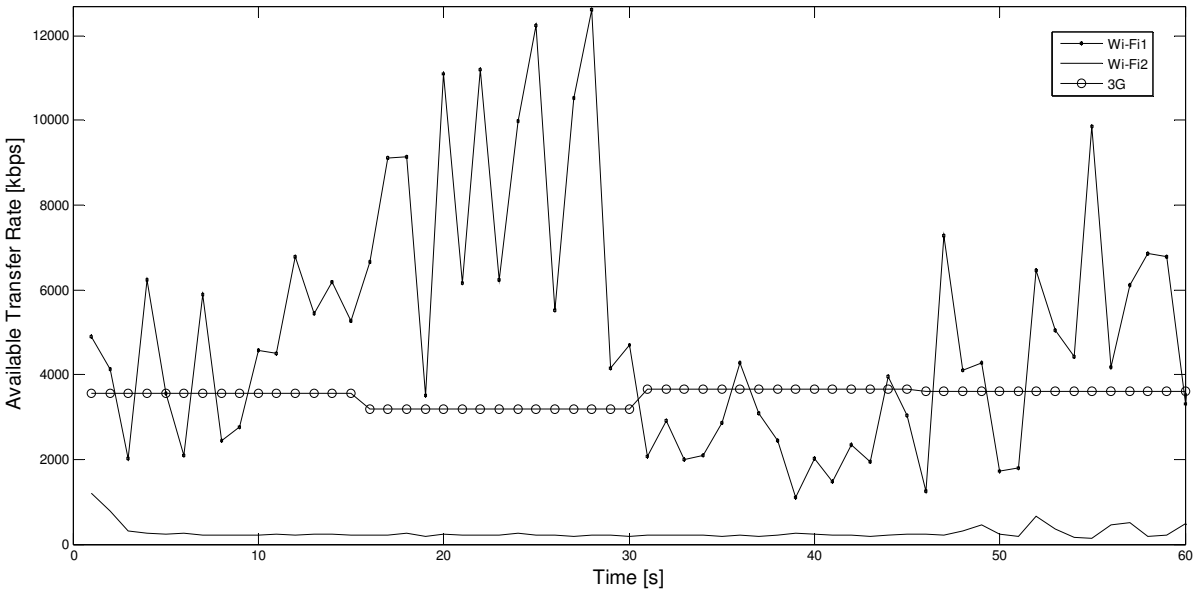

Figure 8. Available Transfer Rates for Experiment No.1

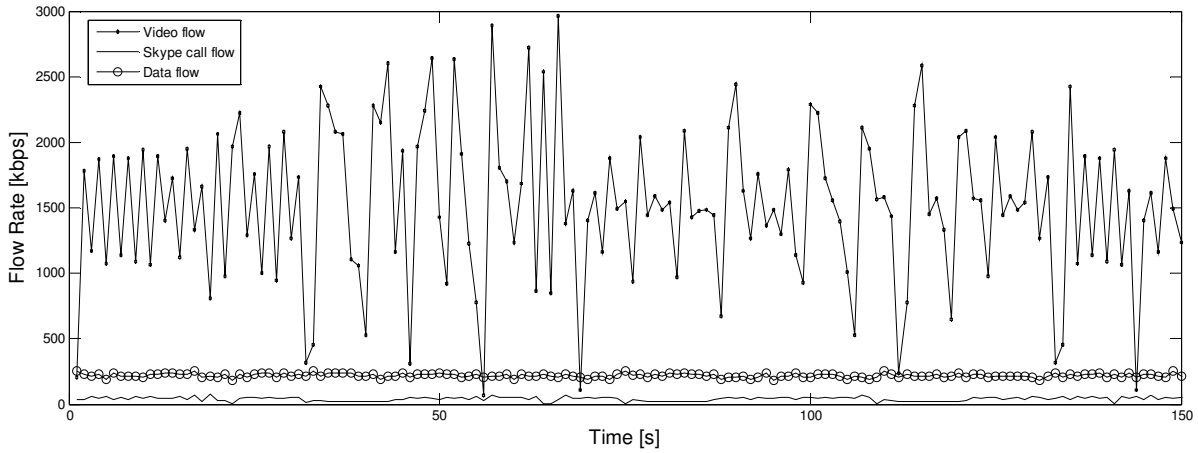

Figure 9. Flow rates for Experiment No.2-4

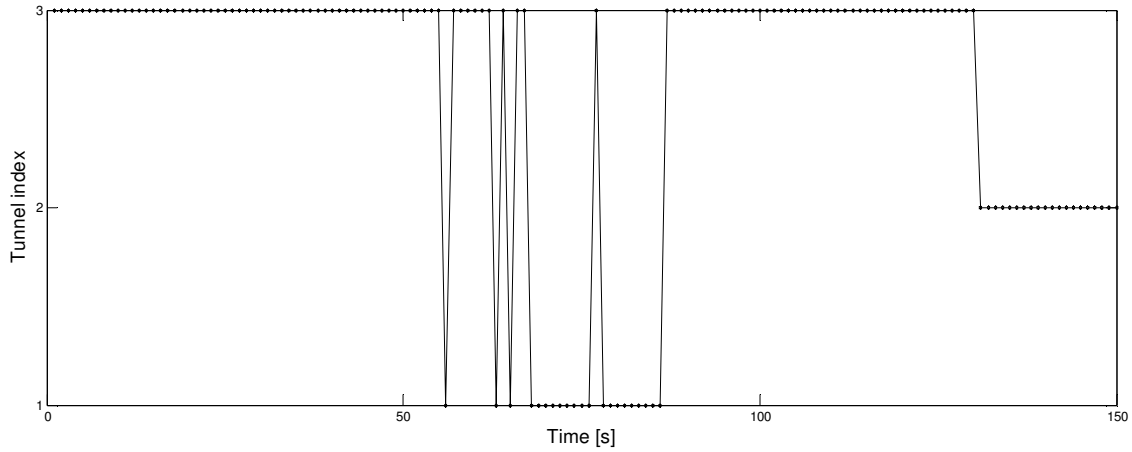

Figure 10. Experiment No.2: video flow (Flow 1) allocation through Tunnels 1, 2 and 3

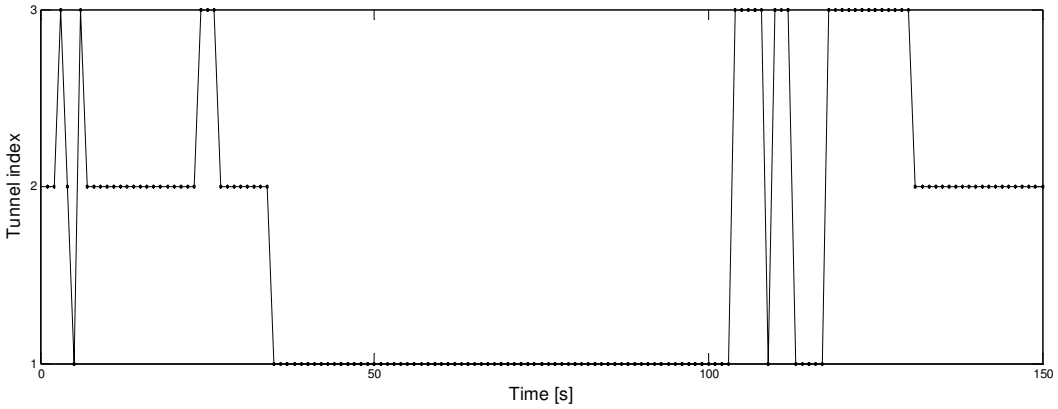

Figure 11. Experiment No.2: Skype call (Flow 2) allocation through Tunnels 1, 2 and 3

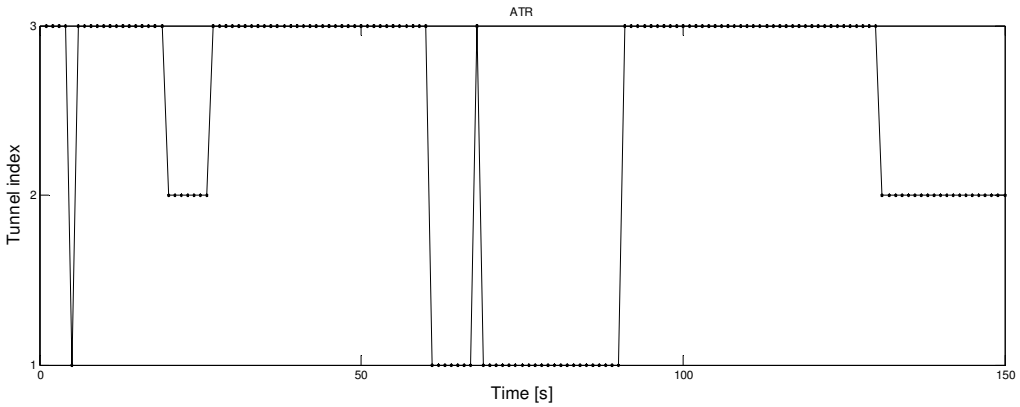

Figure 12. Experiment No.2: Data flow (Flow 3) allocation through Tunnels 1, 2 and 3

Note that the paper covered only the technical aspects of how does the algorithm for GAP minimizes the cost of communication through multi-access networks. Even though tunnels are established and destroyed as new wireless/mobile services become available, the charges of transmitting data through each operator is known. Thus, the algorithm is able to make decisions based on the transmission cost.

V. CONCLUSIONS

There is a tradeoff between seamless connectivity on one hand, fairness allocation of resources and scalability on the other hand. We do not say that our solution is not fair or scalable, but the key feature (i.e. seamless connectivity) explains why the solution is not following the majority of existing approaches (NAT, tunneling at packet-level, operator-oriented, no encryption possible etc.). We compensated by involving smart algorithms for GAP, vertical handover and load balancing. These are minimizing the costs and are making the terminals to switch automatically from one operator to another, without service interruptions. With the proposed solution customers may experience (sometimes) few seconds of data exchange stalling. However it is important that the connections are not released due to the way the smart router interacts with the service continuity gateway. Once we demonstrated that the solution designed fulfills the requirements, we will have to continue our work on optimizing the handover and load balancing in order to minimize the service stalling (not discontinuity). Active measurements of end-to-end delay or energy consumption are needed if sensor networks will be connected to the smart mobile router. There is a work under progress to evaluate also the economic benefits of employing this solution.

ACKNOWLEDGMENT

This paper is supported by the Sectoral Operational Programme Human Resources Development POSDRU/159/1.5/S/137516 financed from the European Social Fund and by the Romanian Government. A previous research leading to the development of the software tools for the demonstrator has partially received funding from the European Union's Seventh Framework Programme managed by REA-Research Executive Agency under grant agreement no. FP7-SME-2012-315161 "UCONNECT-Implementation of Ubiquitous Connectivity for Public Transport". However the views expressed in this paper are solely those of the authors and do not necessarily represent the views of entire FP7-UCONNECT.

REFERENCES

[1] P. Rodriguez, R. Chakravorty, J. Chesterfield, I. Pratt, and S. Banerjee, "Mar: A Commuter Router Infrastructure for the Mobile Internet". *Proceedings of the 2nd International Conference on Mobile Systems, Applications and Services MobiSys 2004*, pp.217-230, 2004.

[2] A. Balasubramanian, R. Mahajan, and A. Venkataramani, "Augmenting Mobile 3G using WiFi". *Proceedings of the 8th International Conference on Mobile Systems, Applications and Services MobiSys 2010*, pp.209-222, 2010.

[3] J. Eriksson, H. Balakrishnan, and S. Madden, "Cabernet: Vehicular Content Delivery Using WiFi". *Proceedings of the 14th Annual International Conference on Mobile Computing and Networking ACM MobiCom 2008*, pp.199-210, 2008.

[4] R. Mahajan, J. Padhye, S. Agarwal, and B. Zill, "E pluribus unum: High Performance Connectivity on Buses". *Microsoft Research*, 2008. [Online]. Available: http://research.microsoft.com/pubs/81326/master.pdf [Accessed: July 15, 2014].

[5] FP7-UCONNECT Project, 2012-2014. [Online]. Available: http://idi.gowex.com/uconnect/ [Accessed: July 15, 2014].