Mobile communication & service continuity in a train scenario

Bart Jooris[1], Piet Verhoeve[2], Frederik Vermeulen[3] and Ingrid Moerman[4]

[1]Associate IEEE, Ghent Univ. - IMEC - IBBT, Ghent Belgium, bart.jooris@ugent.be

[2]Senior IEEE, Televic NV, Izegem Belgium, p.verhoeve@televic.com

[3]Member IEEE, Televic NV, Izegem Belgium, f.vermeulen@televic.com

[4]Member IEEE, Ghent Univ. - IMEC - IBBT, Ghent Belgium, ingrid.moerman@ugent.be

IEEE/SCVT Symposium Building Inc., Benelux Chapter,
90 Speakers Corner, 1234 ZZ Enschede, Benelux

October 15, 2005

Abstract. *The fundamental goal of this research is to allow mobile users, in particular train passengers and train crew, to traverse seamlessly across different wireless network technologies while ensuring service continuity and a certain level of QoS in different application domains (data, audio, video, gaming, etc.). Assuming that most of the train passengers use standard 802.11 client adapters inside of their Windows running devices, we present a vendor-independent solution to let the passengers seamlessly enjoy the broadband services while moving in or around the train.*

Keywords: *broadband, wireless, fast moving users, fast handoff, Ethernet*

Introduction to mobility & service continuity scenarios

In future, committers will take it for granted to continue their professional and private activities while travelling, in particular when travelling by train. Recently, some internet services have been introduced like the 21net pilot project on the Thalys [1](route Brussels –Paris) and Icomera [2] (route Copenhagen – Oslo). The issues addressed in this research are: seamless handover, roaming, Quality of Service (QoS) and inter-working between heterogeneous wireless networks, such as the on-board network in the train, the way-side network connecting the train to the outside world and the hotspot network in the railway station.

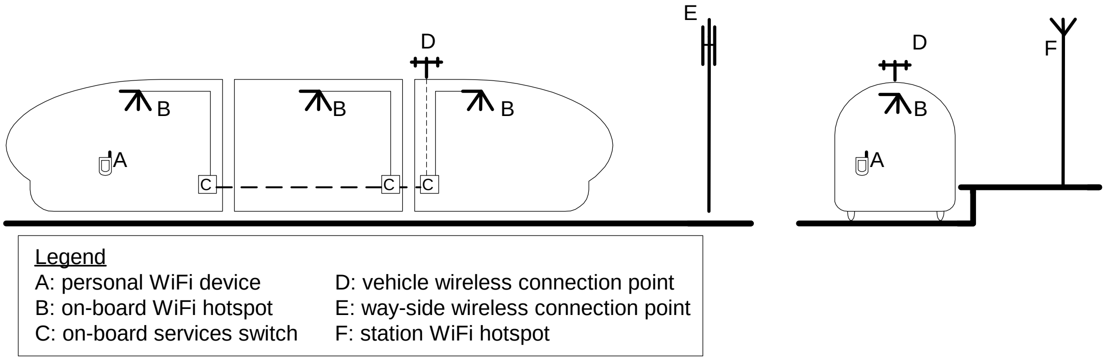
E
D
B
B
B
A
C
C
C
D
F
B
A
Legend
A: personal WiFi device
B: on-board WiFi hotspot
C: on-board services switch
D: vehicle wireless connection point
E: way-side wireless connection point
F: station WiFi hotspot

Figure 1: Schematic overview of a riding train (left) and a train in a station (right)

In particular, we study these issues for the case where both the users and the network are mobile, which is certainly the case for mobile users in the train, where the users are moving with respect to the wireless network in the train and where the train is further moving with respect to the outdoor fixed wireless infrastructure. In order to make the different scenarios clear, a schematic overview (Figure 1) is given in this section.

A: Personal WiFi device. The user in all scenarios is equipped with a personal device that has WiFi capabilities, such as a laptop, a PDA or any other device with a WiFi interface. It should also be noted that the term "user" is not limited to "passenger". Indeed, the train crew can also be equipped with WiFi devices allowing them to access intra-/internet information (e.g. travel information, ticketing, etc.) or communicate with passengers or other crew members (either train attendants or the driver) through the network infrastructure.
B: On-board WiFi hotspots. These on-board hotspots are to be used as the access points for all users and are connected to the wired IP-network in the train. This wired network is used as a backbone network to connect components of the system.
C: On-board services switch. The wired train-LAN is built using special switches specifically designed for train conditions. Besides resistance to the highly electronically unfriendly train environment (EMC, transient bursts, etc.), these switches are designed to provide specific QoS features and have dynamic configuration capabilities to cope with changes in the train configuration.
D: Vehicle wireless connection point. This device has the task to interface the moving vehicle to the fixed world. A Mobile Access Router (MAR) can complete this task. A MAR has one interface for each technology (Wifi, GPRS, satellite, WIMAX…) it supports. The MAR will constantly choose the best link to the fixed world.
E: Way-side wireless connection point. The way-side wireless connection point will depend on the technology that will be used. Satellites and GPRS antennas are the most common at this moment.
F: Station WiFi hotspot. This hotspot will not only be used as a network access infrastructure for the passengers but it will also be used to connect the train to the fixed network

Different mobility scenarios are considered; mobile user inside a train, moving train connected to the outside world, train entering or leaving the station (where train changes connectivity from way-side wireless connection point and station WiFi hotspot and vice versa), user leaving or entering the train. In this paper we will focus on the on-board network in the train. We will discuss solutions to optimize the layer 2 in-LAN (the devices stay in the same LAN) handovers keeping the train conditions into account.

On-board services switch for the train broadband backbone

The on-board services switch (OSS) is a module that provides network connectivity between train vehicles and has been recently developed and implemented by Televic and INTEC. Each vehicle equipped with an OSS, can communicate with its neighbour vehicles, when they also have an OSS installed. Both vehicles communicate with each other using the Ethernet protocol. The physical topology on-board the train looks like Figure 2. The OSS has 5 external interfaces: two to interface to neighbour OSS (Previous Element, Next Element), one to interface with the Public Information System

(PIS) backplane (only for crew), one to interface with third party systems (not shown in figure), and one to interface with the Public Network for example for passenger internet. An internal interface to connect a PIS-public gateway can be foreseen. The OSS does not handle all Ethernet packets the same way as it will assign a priority level to all the traffic. For example; the traffic generated by the PIS backplane has a higher priority than the incoming passenger traffic through the Public Network Interface.

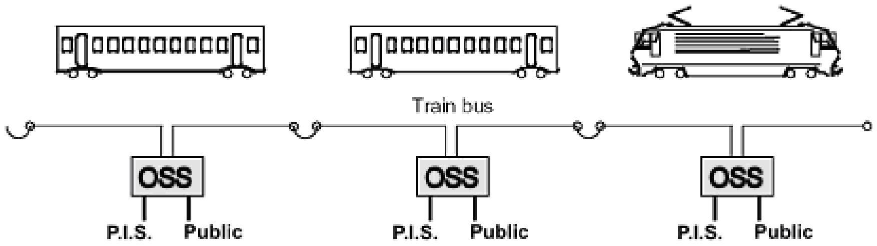

Figure 2 One OSS in each vehicle

Service continuity

Scenarios

In a first step the OSS is extended as shown in Figure 3. All vehicles with an OSS will be equipped with a switch and on-board WLAN base stations (BS). Only a few vehicles (at least one) will be fully equipped with a mobile access router (MAR) and a gateway (GW) which has a link to content servers (not drawn in the figure). A crew member can have a wired connection to the public interface via the switch of the OSS or can connect wirelessly via a BS. If we take a closer look to the scenario “mobile user inside the train” we can derive two types of in-LAN handovers.

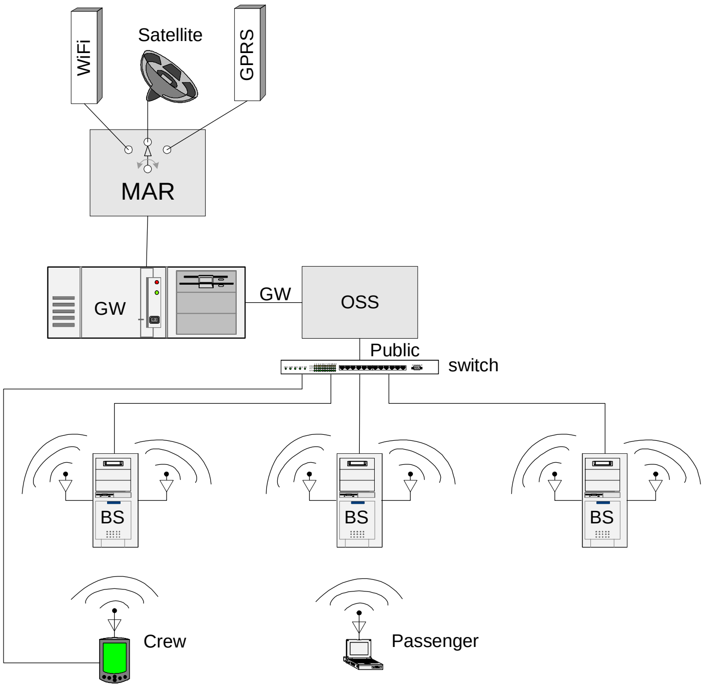

Figure 3 Wireless extensions to the OSS

The first is located when a crew member plugs out (cfr. in) his cable during a session. We must guarantee the continuity of the session over the wireless (cfr. wired) link. In a standard configuration each interface will have its own IP and MAC address. A session is defined as a communication between a client IP address and a server IP address. It is hence impossible to continue the session if we alternate between the two interfaces with two different IP addresses. Even if we succeed to give both interfaces the same IP-address by the way of source Network Address Translation (NAT) the two MAC-addresses will still result in two mutual exclusive entries (couple of IP and MAC address) in the ARP table of the gateway which is connected on the same LAN. A solution to this vertical handover will be discussed as a convergence layer in the next section.

The other handover is located when a mobile user (passenger or crew) moves from one on-board WiFi hotspot to another. A standard station (STA) will handle this as follows; it detects that the AP where it was connected to has a decreasing link quality or is no longer available, it will execute a scan on all the available channels; consequently it will select the best AP to authenticate and to (re-)associate with. When the access network is configured well the session of the mobile user will continue but the session continuity is not really seamless. This “standard” handover process is extensively described by Velayos et al. [11], Mishra et al.[13] and Jon-Olov Vatn[15].. The two most important contributers to the handover latency are the scan phase and the execution phase. The time spent on the scan phase depends heavily on the type of WLAN card and driver is used (typical values can vary from 50 to 400 ms [13]). The time spent on the execution phase depends on the type of security used (typical values can vary from 10 to 1200 ms [19]). Ramani et al. presented a vendor-independent solution: Syncscan [17] which makes it possible to reduce the time spent on the scanning phase by pre-authenticate with all available APs. The TGr [10] discusses fast Basic Service Set (BSS) transitions by optimizing all the different phases. One proposal is to provide the STA with neighbour AP information to reduce the channels to be scanned. In this paper we want to present a solution to eliminate all of these phases by executing the handover in our access network. In the next section we will discuss the “AP follows the STA “-principle to handle this horizontal handover.

It should be noted that although we have limited the scope of this paper to the user inside the train scenario, the other scenarios are also of interest. A MAR can take care of both the scenarios “moving train” and “train entering or leaving the station“. Of course we need to further investigate if a commercial MAR can satisfy our needs. The last defined scenario “user leaving or entering the train” can be solved by installing an on-board WiFi hotspot in the station. In other words we can solve this by implementing the “AP follows the STA “-principle in the station’s hotspot.

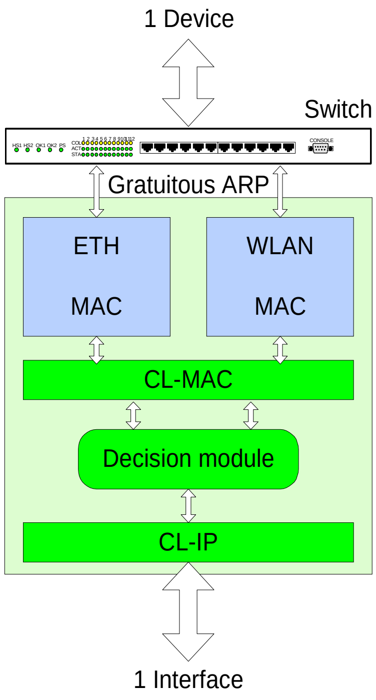

Figure 4 Convergence layer

Operation principle

Convergence layer

As we have “full” control over the crew terminals, we present to install a Convergence Layer (CL). We create such a convergence layer (Figure 4) by the following procedure: hide the Ethernet and wireless LAN interface by not assigning one IP per interface, but creating one virtual interface and assigning a single IP and a single

MAC address to it, keep the desired port of the switch up to date for the terminal. We will manipulate the CAM-table of the switch with ARP-replies (gratuitous ARP). As we will give priority to the wired link the decision module makes use of a robust link detection mechanism on the wired link to make the right routing decision. Every outgoing packet will be encapsulated with the CL-IP and the CL-MAC. The upper layers of the crew node will only see one interface and one IP-address. The other devices that are connected to the train LAN will only see one device and one MAC-address.

Moving access point

The 802.11 standard defines a handover mechanism in an Extended Service Set (ESS), covered by several access points (AP) with the same ESSID. Handover is initiated by the station (STA) based on link quality of the current AP. If this link quality gets too weak, the STA will perform an active scan. After compiling the scan results, the STA will select the “strongest” AP from the ESS to join, authenticate and reassociate. The Inter Access Point Protocol (IAPP) [12] buffers the packets during this handover and it will deliver these buffered packets once the STA is connected to the new AP.

We present an alternative handover mechanism maintained by the access network with standard 802.11 b/g client adapters as they are available today. Our paradigm: the *AP follows the STA* on top of the base stations of our access network. We will implement an AP as a software object that moves from one BS to the other. In our access network we create a unique logic AP for each STA that will be installed on the nearest base station (BS). Every BS will work on its fixed frequency. We will install a one-time vendor-independent software install on each STA that we will use for localisation of the STA (by sending beacons from the STA to the BS of the access network) and to adjust the working frequency of the STA. Handover can be accomplished by installing two interfaces in each BS. The first interface runs an AP for every near STA. The second interface will listen (promiscuous) to the neighbour’s frequencies and measures the signal strength of the broadcast messages of the one-time software install and all the other traffic from every near STA. If the promiscuous interface of BS B detects a stronger signal from a STA than the signal measured by the BS A where the STA is connected to, the AP interface of BS B will take over the AP functionality for this STA. To let the STA know that the AP has changed its frequency we will use the “Current Channel” in the “Direct Sequence Parameter Set” field of the beacon message [3]. Our one time vendor-independent software install will capture all beacons of the AP where it is connected to and once it detects such a frequency hop it will follow the AP to the new frequency. Taking the train environment into account, which is one dimensional, we will use three repetitive frequencies. As a consequence the promiscuous interface of each BS must divide its time to listen to the two neighbours frequencies. When a STA is located outside the range of the train access network, our software will not affect the standard way a handover is handled.

To implement the access network we will use some principles defined in the CAPWAP and IAPP standards. The CAPWAP [16] defines principles to manage the APs centralized (Split AP), this will be the starting point for our implementation. The IAPP [12] defines methods to set up a connection between APs to exchange packets; we will set up an identical connection between BSs to exchange APs.

Development: implementation in the simulation environment

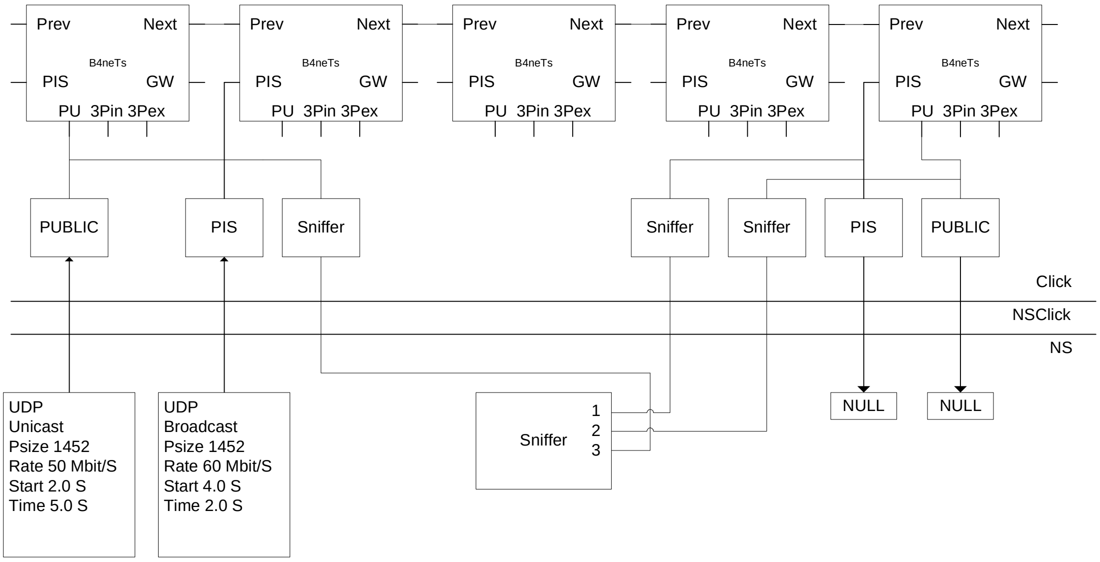

Figure 5 nsclick priority simulation topology

We have implemented the OSS as a click modular software router [6]. To this end we only used standard click elements except for the VLAN functionality (adding and removing VLAN headers).Before validating the OSS on a real test bed some functionality tests in the nsclick [8] environment have been done. This way of working speeds up the implementation and has the great advantage that we are no longer restricted to scalability of our lab or the number of available click routers. By matter of example we present a priority test on the OSS (see Figure 5). We created a linked list of 5 OSS (can easily be extended) and added some public and some PIS nodes. To verify that PIS traffic has more priority than public traffic we generate two streams. A first stream (blue) of 50Mbps is started at second 2 for a period of 5 seconds. A second stream of 60Mbps is started at second 4 for a period of 2 seconds. The resulting streams are represented by the green (cfr. red) line for the public (cfr. PIS) traffic. We can see in Figure 6 that when the PIS traffic is started the public traffic falls back to 22Mbps. The simulations have been confirmed in a smaller scale experimental set-up.

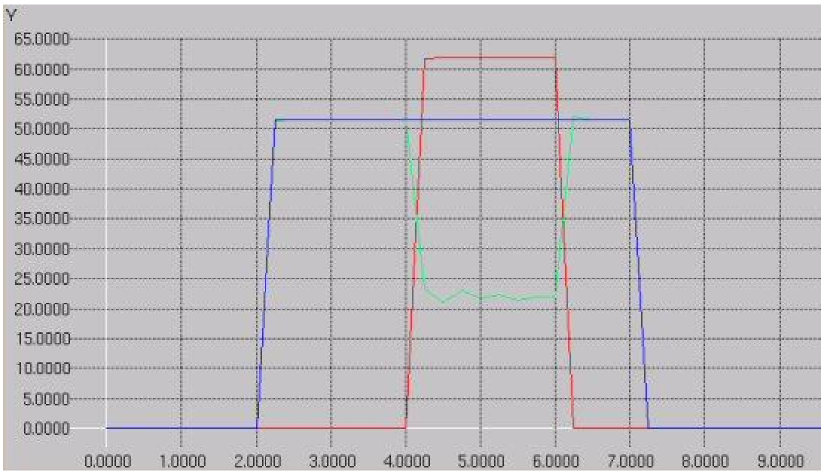

Figure 6 Nsclick priority simulation results

Acknowledgment

This research is partly funded by the ITEA project 'Easy Wireless' (Project No. ITEA ip03008), by The Institute for the Promotion of Innovation by Science and Technology in Flanders (IWT) through the contract No. 050127 and by the Belgian Science Policy through the IAP V/11 contract.

Conclusion and future work

The IEEE 802.11 doesn't define a handover mechanism that guarantees a smooth and seamless change of access points. We presented solutions for both the vertical handover (802.3↔ 802.11) and the horizontal handover (802.11↔ 802.11) to meet our specific in train scenario. The proposed horizontal handover mechanism takes advantage of the linear train topology. In the near future we need to investigate how these methods can be implemented and how they can be further integrated in the other mobility scenarios.

References

[1] 21 Net service, http://www.21net.com/EN/serv-over.htm

[2] GNER, Icomera announce commercial agreement to deliver real-time wireless internet on trains. http://www.icomera.com/news/gner agreement.asp, website, Gothenburg, Sweden, 6 April, 2004.

[3] Matthew Gast, "802.11® Wireless Networks: The Definitive Guide", April 2002, O'Reilly chapters 1-4 and 7.

[4] IEEE, Inc. http://grouper.ieee.org/groups/802/11/

[5] Bruce McMurdo, "Cisco Fast Secure Roaming", Cisco application note, http://www.cisco.com/en/US/products/hw/wireless/ps458/prod_technical_reference09186a00801c5223.html

[6] The click modular router http://pdos.csail.mit.edu/click/

[7] The network simulator NS-2 http://www.isi.edu/nsnam/ns/

[8] The nsclick Simulation Environment http://systems.cs.colorado.edu/Networking/nsclick/

[9] John Bicket, The madwifi.stripped driver http://pdos.csail.mit.edu/~jbicket/madwifi.stripped/

[10] TGr Task group 802.11r : IEEE, Inc. http://grouper.ieee.org/groups/802/11/Reports/tgr_update.htm

[11] Hector Velayos and Gunnar Karlsson, Techniques to reduce IEEE 802.11b MAC Layer Handover Time. April 2003.

[12] TGf Task group 802.11f : IEEE, Inc. http://grouper.ieee.org/groups/802/11/Reports/tgf_update.htm

[13] Arunesh Mishra, Minho Shin and William Arbaugh, An Emperical Analysis of the IEEE 802.11 MAC Layer Handoff process

[14] Arunesh Mishra, Minho Shin and William Arbaugh, Improving the latency of the Probe Phase during 802.11 Handoff, May 2003

[15] Jon-Olov Vatn, An experimental study of IEEE 802.11b handover performance and its effect on voice traffic, July 2003.

[16] IETF's CAPWAP working group, Split AP, http://www.capwap.org/draft-calhoun-capwap-taxonomy-recommendation-00.txt

[17] Ishwar Ramani and Stefan Savage, SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks

[18] Cisco Mobile access router, http://www.cisco.com/univercd/cc/td/doc/product/access/mar_3200/

[19] Alimian and Aboda, Analysis of roaming techniques, March 2004