

***Network Provisioning for High Speed Vehicles
Moving along Predictable Routes - Part 1:
Spiderman Handover***

Juan-Carlos Maureira — Diego Dujovne — Olivier Dalle

N° 6850

February 2009

Thème COM



R
**apport
de recherche**

Network Provisioning for High Speed Vehicles Moving along Predictable Routes - Part 1: Spiderman Handover

Juan-Carlos Maureira*, Diego Dujovne†, Olivier Dalle‡

Thème COM — Systèmes communicants
Équipes-Projets Mascotte et Planete

Rapport de recherche n° 6850 — February 2009 — 25 pages

Abstract: This report presents our on-going work on a new system designed to provide a continuous network connectivity to communicating devices located on-board a vehicle moving at "high speed" with a predictable trajectory such as trains, subways or buses. The devices on-board the vehicle form a sub-network called the "in-motion network". This system we propose is composed of two parts. The mobile part, called *Spiderman Device* (SD), installed on the roof of the vehicle, and the fixed part is composed of multiples access points, called *Wireless Switch Access Points* (WS APs), installed along the predictable route of the vehicle. To provide a continuous connectivity, we designed a new handover algorithm that relies on a two IEEE802.11 radio hardware placed in the SD device. This dual-radio architecture allows to minimize or even hide the handover effects, achieving a seamless continuous data-link connection at high speeds, up-to 150 Km/h and possibly more. The link between the SD and the WS AP forms a Layer 2 Ethernet Bridge, supporting any Layer 3 protocol between the infrastructure network and the in-motion network. This concept has been validated by simulations and is currently tested using a real prototype in order to assess the performances and practical feasibility of the system.

Key-words: Wireless Handover, Internet on Rails, Simulation, OMNeT++

* jmaurei@sophia.inria.fr

† diego.dujovne@sophia.inria.fr

‡ olivier.dalle@sophia.inria.fr

Network Provisioning for High Speed Vehicles

Moving along Predictable Routes - Part 1: Spiderman Handover

Résumé : Ce rapport présente nos travaux en cours sur un nouveau système conçu pour fournir une connectivité réseau permanente à des équipements de communication se trouvant à bord d'un véhicule se déplaçant à grande vitesse le long d'une trajectoire prédéterminée, tel qu'un train ou un autobus. Ce système se compose de deux parties. La partie mobile, appelée *Spiderman Device* (SD), est installée sur le toit du véhicule et la partie fixe, composée de multiples points d'accès placés le long du trajet et appelés *Wireless Switch Access Point* (WS APs). Pour fournir une connectivité permanente nous avons conçu un nouvel algorithme de handover qui s'appuie sur deux équipement radio IEEE802.11 présents à la fois dans le SD et les WS APs. Cette architecture à deux radio permet de minimiser, et même cacher les effets du handover, ce qui permet de garantir une connexion continue de niveau data-link layer dans des véhicules en mouvement à des vitesses pouvant atteindre 150km/h. Le couple SD-WS AP fonctionne de façon similaire à un pont Ethernet de niveau deux, ce qui permet d'accomplir un routage multi-protocole transparent au niveau 3, entre le réseau d'infrastructure et le réseau en mouvement. Le concept de ce système a été validé au moyen de simulations et des expérimentations réelles et évaluations de performances sont actuellement en cours sur un prototype réel.

Mots-clés : Réseas sans fil, Handover, Simulation, Connectivité sur la route, OMNeT++

1 Introduction

Full-time network connectivity has become a reality, even in a mobile context, with the advent of 3G telephony. Every day, the market presents new devices, such as smartphones and netbooks, that deliver network connectivity to mobile users. However, the actual solutions for providing the networking service to mobile users are mainly based on telephony networks and related technologies (EDGE/3G/UMTS/...). While being widely available, these telephony networks suffer from their popularity, which results in unpredictable quality of service depending on the level of concurrence in the area of use. Therefore, ensuring a sustained quality of service using such networks in a mobile context is extremely difficult. WiMax and Satellite-based solutions are also worth to mention. Satellite connections happen to be relatively expensive and suffer limited capacity compared to “small range” radio solutions. WiMax is still in early ages and mainly considered for providing a replacement to wired networks in urban areas, but it is not expected to be deployed everywhere. Because of their average to long range wireless connections, systems like satellites or WiMax also fail to ensure connections in covered areas like tunnels (railways or subways).

Paradoxically, despite its wide use in static or low motion context, the WiFi technology (IEEE802.11) has received little attention so far for providing sustained quality connectivity to communicating devices moving along with a high-speed vehicle like a train or bus, over long distances. Indeed, assuming the costs of standard WiFi equipments will continue to drop down, it becomes reasonable to consider the deployment of WiFi Access Points along high traffic roads or railways, even for long distances, during inter-city transits.

In this report we present our on-going work on such a solution, based on a combination of two standard WiFi equipments. Using simulations, we show that the use of such a double-radio configuration is sufficient to provision and sustain a reasonable quality of service between the static and moving parts of the resulting network, despite the fast and continuously occurring handover events. Indeed, at high speed these handover events occur very frequently due to the limited radio coverage range of standard WiFi equipments (roughly every 5s at 150km/h, for a 200m wide coverage). Our study of such a system is divided in two parts: first, the design and study of a solution for ensuring a continuous connection between the in-motion and the fixed parts of the network; and second, the design and study of a static infrastructure network to carry the traffic of the previous solution. In this report we address the first part, leaving the second part for further studies.

The report is organized as follows: in section 2, we present previous related works. In section 3, we give a description of our WiFi-based solution, covering the operational context and the devices that implement the solution. Then, in section 4 we analyze the requirements that make the solution viable. Following, in section 5, we give our firsts evaluation results, based on simulations. Finally, in section 6, we present our conclusions and further directions.

2 Previous Related Work

Several studies have explored the feasibility to use IEEE802.11 devices to provide network connectivity to vehicles [EBM08] and trains [ZSH⁺05] [Tse07]. The common problem they found was the network disruptions caused by the handover between successive hotspots, problem that is increased at higher speeds. The source of this problem is a combination of two common issues that were addressed independently in the literature. The first issue is about the effects of speed on IEEE 802.11 transmissions. For example, Gass et al. [GSD06] and Ott et al. [OK04], have shown experimentally that IEEE 802.11b technology allows the connectivity between the infrastructure network and the in-motion devices up-to 120 Km/h and 180 Km/h, respectively. The second issue is about minimizing or hiding the loss of connectivity during IEEE802.11 handover, such as Ramachandran et al. [RRL06] and Brik et al. [BMB05], that propose the use of two-radio hardware, focusing on how to achieve a steady constant bit rate transmission. These two kinds of issues have never been combined in a single study as we do in this report.

3 System Description

In this section, we introduce a definition of the proposed system and describe our assumptions on its operational requirements in order to bound the scope of our work. We use the IEEE 802.11b standard as the reference wireless radio technology, but our approach may be further extended to any wireless technology that uses shared access to the medium, such as CSMA/CA. We assume a circular radio propagation model, described by the well known Free-Space Pathloss equation:

$$FSPL = \left(\frac{4\pi d}{\lambda} \right)^\alpha \quad (1)$$

where d is the distance from the transmitter (in meters), λ is the signal wavelength (in meters) and α is the so called path-loss exponent.

Our proposed system is composed of two devices: the *Spiderman Device* (SD), installed on the roof of the bus, train or subway, and a WiFi Access Point that operates at OSI level two, called the *Wireless Switch Access Point* (WS AP). Multiple WS APs are used to access the infrastructure network along the vehicle route. The *Spiderman Device* provides connectivity to the in-motion network; the corresponding link is established within the OSI layer two. This link is kept established nearly full time, using a two-radio hardware and a new hand-over procedure we designed. This procedure alternates the data link associations between the SD and the WS APs found along the path (hence the name, a metaphoric allusion to the way the comics hero Spiderman moves in the air throwing his spider web ropes one after another.) Indeed, the use of two radios, when cruising at high speed, allows to hide the time needed for association and authentication and to maximize the connection time with each WS AP.

The difference between a WS AP and a standard IEEE802.11 AP is the way associations are handled. A standard AP handles each association as a client (STA) and it only store the MAC address of the that client. On the contrary the WS AP handles each association as a wireless bridge link, and its MAC address table contains all the MAC addresses of the clients handled by the SD (instead of the SD itself). This way, The WS AP acts like an OSI layer two switch, having as switched ports the SD associations and the backbone uplink ports.

Before we enter the detailed description of each of the devices previously introduced, we first give a formal description of their operational conditions of use.

3.1 Operational context

Let M be a mobile and P a fixed path of length L , along which M is moving. We note t_0 the time at which the mobile starts from one end of P and t_{max} the time at which it arrives at the other end. For the sake of simplicity, we will use a linear projection of the path P in a one-dimensional space and we note $pos_M : [t_0; t_{max}] \rightarrow [0; L]$ the function that gives the position of M in time. We call N the on-board network attached to M (moving at the same speed).

A set of n wireless Access Points, noted AP_1 to AP_n , each one covering an identical *circular* area of radius r , are installed along the path P . The segment of P that intersects the coverage area of AP_i is noted *coverage*(i). We assume

that AP index are sequentially attributed along the path, such that we have a total order of minimal points of each coverage, and maximal points of each coverage respectively:

$$\begin{aligned} \forall i \in \{1, \dots, n-1\}, \\ \min(\text{coverage}(i)) < \min(\text{coverage}(i+1)) \\ \text{and} \\ \max(\text{coverage}(i)) < \max(\text{coverage}(i+1)). \end{aligned}$$

We note $\mathcal{A}(x) = \{i, \dots, j\}, 1 \leq i, j \leq n$ the set of the index of AP for which M is in the coverage area when arrived at position x of the path.

At any time, we assume the following property is observed (any segment of the path is covered by at least one AP):

$$\begin{aligned} \forall k \in \mathcal{A}(x), x \in \text{coverage}(k) \\ \text{and} \\ \forall k \notin \mathcal{A}(x), x \notin \text{coverage}(k). \end{aligned}$$

All APs are connected to an Infrastructure network I , which links the APs together to the same Ethernet network. Traffic to/from external networks goes through a unique gateway. Notice when we state that M is exchanging traffic with I , we are implicitly stating that in-motion network N is exchanging traffic with I . Fig.1 depicts the described scenario.

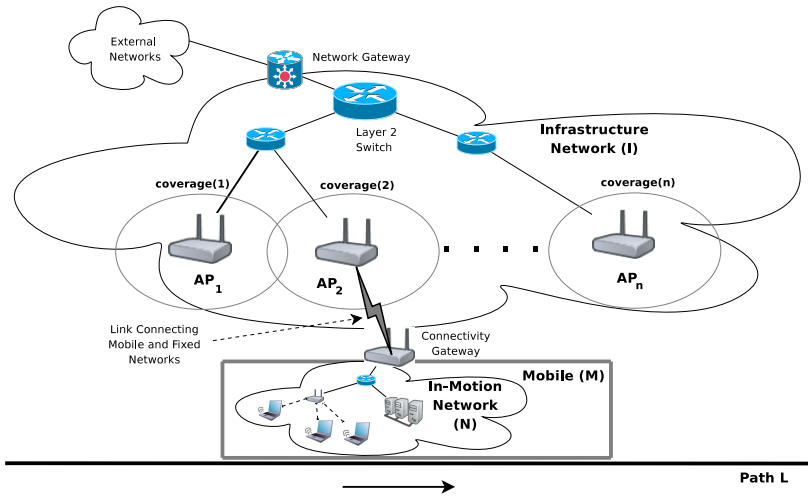


Figure 1: Studied Scenario

Following, we further describe the handover algorithm implemented by the SD. As previously stated in related works, the use of a two-radio hardware was already presented by Brik, Mishra and Banerjee [BMB05] and, after by Ramachandran et al. [RRL06]. They tried to minimize and possibly hide the handover time in order to provide a constant bit rate (CBR) transmission between a single device and an infrastructure network. Our work differs from theirs on two points. First, we aim at providing a continuous connectivity not for a single device, but to an entire network moving at high speed; and second, we consider and evaluate the effects of speed on the proposed handover algorithm, issue that was not addressed by previous works.

3.2 The Spiderman Device

In short, the *Spiderman Device* is an IEEE802.11 two-radio bridge client device with handover capabilities. More precisely, we define the SD as a network bridge that connects on one side, an Ethernet wired port (in-motion network uplink), and on the other side, an Ethernet wireless *virtual* port, provided by the Wireless Switch Access Point to which the SD is associated with.

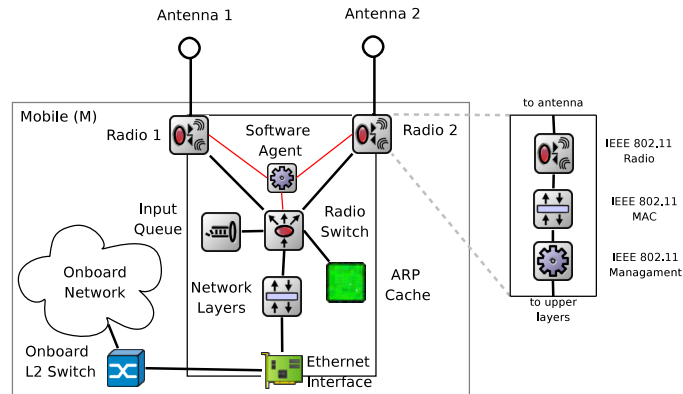


Figure 2: Spiderman Device Block Diagram

Fig.2 describes the device components and their relationships. As shown on the figure, a new *Radio Switch* component is added to dispatch the packets between the two radio devices. This switch also implements an *ARP Cache* table with all the MAC addresses discovered through the wired Ethernet port, and an *Input Queue* used to buffer data packets when changing between radios. The *Software Agent (SA)* controls the handover process, radio scanning and radio switch operations by sending commands to the *IEEE 802.11 Management* and the *Radio Switch* components.

3.3 The Handover Procedure

In the following, we describe the handover procedure implemented by the Spiderman Device we just described. During the initial synchronization phase, the algorithm starts scanning two frequencies at a time until it detects a first WS AP in the neighborhood, noted AP_1 . Once AP_1 is found, the corresponding radio link, noted RL_1 is used to establish the first association and enter the connected phase. During the connected phase, the SD uses the already associated radio (named *active*) to exchange user traffic packets with the WS AP_i ; it uses the other radio (named *passive*) to scan the neighbourhood and find the next WS AP_{i+1} . This is done as follows: when the algorithm detects that the *active* radio link receives three consecutive beacons with decreasing SNR values, it starts the channel scanning process, using the *passive* radio. This results in an early start of the scanning process, before M arrives to the $coverage(i)$ limit. When the algorithm has found WS AP_{i+1} , it commands the *passive* radio to stop scanning and starts the authentication/association process with WS AP_{i+1} . All these operations must be done before the *active* radio loses connection with the WS AP_i , which is possible if $coverage(i)$ and $coverage(i+1)$ are sufficiently

overlapping. When the *passive* radio is already associated to WS AP_{i+1} , the algorithm activates the *Input Queue* on the *Radio Switch* in order to buffer the incoming packets from the in-motion network. Then, it commands the *active* radio Management module to move all the queued packet to the *passive* radio Management module; then it inserts one Gratuitous ARP packet for each ARP Cache entry in its *ARP Cached Table* into the *Input Queue*, and flushes it into the *passive* associated radio. Then, it waits for these ARP packets to come back via the current *active* radio, generating an ARP loop between the SD radios and the infrastructure network. The arrival of the last ARP packet triggers the radio state swap: passive becomes active and vice verse. The effect of this *Gratuitous ARP "loop"* is to update the layer two route on the backbone network, allowing external traffic to reach the in-motion network through the new association. The delay for updating the route in the fixed network (from WS AP_{i+1} to the network gateway) is evaluated in the section 4. Finally, when the radio states are swapped, the *Input Queue* is deactivated and the packet flow now is directly routed to the new *active* radio. This process is repeated forever until, possibly, both radios lose connectivity. In this case the algorithm is restarted.

Operationally, the described algorithm will alternate the data-link associations between the two radios, using the *coverage(i)* overlapping to minimize, or even to hide, the handover time, and so, to avoid breaking the connection between the in-motion and the infrastructure networks. Fig.3 presents a sequence-chart of the handover procedure. Fig.4 presents the states of each radio, and table 1 shows all the algorithm states.

Table 1: Full decision table of a spiderman Station

Input RC1	Input RC2	Output RC1	Output RC2
Lost1	Lost2	Searching1	Searching2
Lost1	Searching2	Searching1	No change
Lost1	Ready2	Searching1	Active2
Lost1	Active2	Searching1	No change
Searching1	Lost2	No change	Searching2
Searching1	Searching2	Wait1	Wait2
Searching1	Ready2	No change	Active2
Searching1	Active2	Wait1	Wait2
Ready1	Lost2	Active1	Searching2
Ready1	Searching2	Active1	No change
Ready1	Ready2	Active1	No change
Ready1	Active2	Wait1	Wait2
Active1	Lost2	No change	Searching2
Active1	Searching2	Wait1	Wait2
Active1	Ready2	Wait1	Wait2
Active1	Active2	Not valid	Not valid

As M has a fixed predictable route, the WS AP channel assignment can be done by using a predefined sequence, let us say 1,6,11,1,6,11,... This allows the algorithm to reduce the scanning time by avoiding to perform a full scan every time. It is worth noticing that the scanning operation is always an active

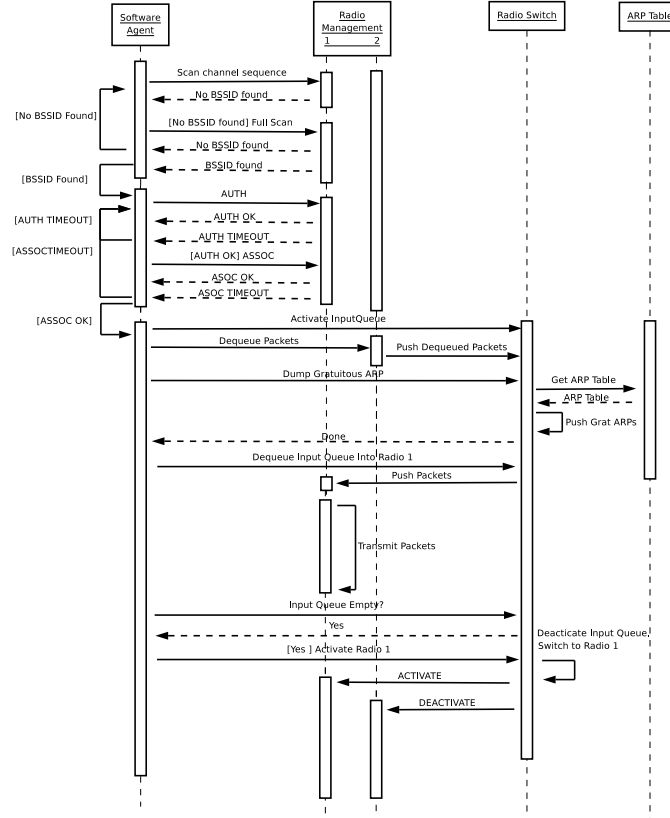


Figure 3: Spiderman Handover procedure

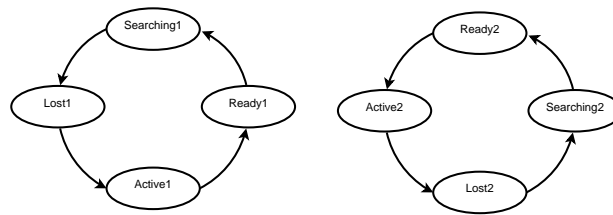


Figure 4: Spiderman link state machine

scanning¹. This reduced scanning is relevant when M is cruising at high speeds, since the time available to find the next WS AP is only the time where M is under mutual coverage between WS AP _{i} and WS AP _{$i+1$} .

3.4 The Wireless Switch Access Point

The WS AP is basically an IEEE802.11 Access Point, but it handles the associations as OSI layer 2 bridges and not as wireless stations (STA). It means that the WS AP will consider as stations all the devices *behind* the associated radio

¹Probe-Response method

instead of the radio itself. This modification implies to handle a MAC address table for each bridged association, having as gateway address the association MAC address. This set up is analogous to a Ethernet Layer 2 Switch, since it must implement MAC routing and a sort of spanning tree. Hence its name, since it behaves in the same way as a regular switch, but having as switched port each association and the wired uplink port. The Fig.5 shows a *Wireless Switch Access Point* with two bridges associated, illustrating the MAC look-up tables built after each association.

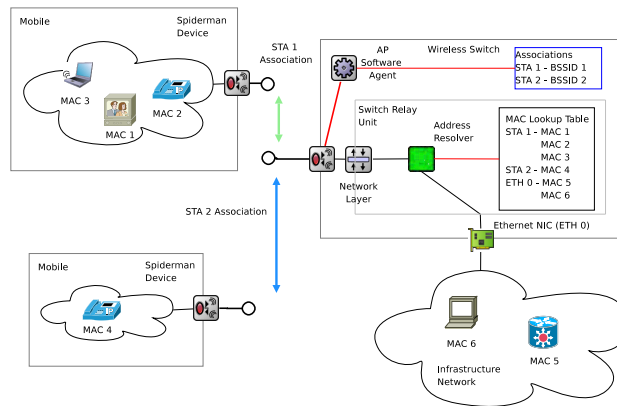


Figure 5: Wireless Switch Access Point and two Mobiles with on-board networks connected to an Infrastructure Network

Notice that the WS AP has an association table, where it handles each associated device, and additionally, it has a MAC address table handling the MAC addresses that are known through each association (and the uplink port). Both tables, association and MAC address have ageing timers associated. A MAC entry is erased from a table after a certain time in case there is no traffic. If one association is removed, all the learned MAC addresses through that association are removed as well.

The consequence of changing from one WS AP to the following is that I must learn all the MAC addresses of the in-motion network inside M to route the packets to the correct destination. This route update is performed by the *Gratuitous ARP loop* defined in the previous section. The route update is transparent to each WS AP.

4 Requirements Analysis

In this section, we analyze the problems affecting the network connectivity between an in-motion network and a fixed infrastructure network when using only IEEE802.11 technology at high speeds. As earlier mentioned in related works, the handover time is critical to ensure a continuous connection. When a single-radio hardware is used, the scanning operation causes a disruption in the data-link layer link, generating packet losses. We analyze the standard handover operation for multiple clients inside a mobile at different speeds by means of simulations, quantifying the handover times and packet losses depending on the mobile speed. Hereafter, we first give a formal description of the handover operation in order to better explain the subsequent results.

4.1 Functional Requirement

An IEEE802.11 wireless station triggers a handover procedure when it needs to move the physical layer connection and state information from one AP to the next. As explained in section 4.2, the handover operation takes a variable amount of time to be accomplished. The time required to perform handover between $AP(i-1)$ and $AP(i)$ is noted as $T_h(i)$, with $T_h(0) = 0$ when entering the $coverage(0)$ area. We divide the handover delay, T_h , in two parts as follows:

$$T_h(i) = T_{scanning}(i) + T_{auth/assoc}(i) \quad (2)$$

where $T_{scanning}(i)$ is the time needed to scan radio channels and discover that $AP(i)$ is the next AP, and $T_{auth/assoc}(i)$ is the time needed to authenticate/associate with $AP(i)$. During $T_h(i)$, no data can be transferred between M and I . Consequently, packets are delayed in queues at both ends of the data link, until the link is re-established. Because queues have finite size, there is a probability of packet drops. Also, notice that $T_h(i)$ depends on the level of SIR/SNR.

Let us note $T_c(i)$ the time that M remains within coverage of $AP(i)$ and $T_d(i)$ the time during which on-board stations can transmit data to/from I . We have:

$$T_d(i) = T_c(i) - T_h(i) \quad (3)$$

In addition, we define $T_u(i)$ as the time taken by the IEEE 802.11 MAC protocol to transmit/receive the minimal number of overhead packets before user data can successfully be sent or received.

Proposition 4.1. *A required condition to have a functional system is :*

$$T_d(i) > T_u(i)$$

In other words, after handover operation, the remaining time until the next handover must be long enough to establish a minimal data exchange.

4.2 Timing Constraints

As previously stated, the handover time T_h depends only on two components: *scanning start time and AP discovery* and *Authentication/Association*. Let us further characterize each of these quantities. First, the *scanning start time* depends only on the appropriate choice of the out of range detection algorithm. Raghavendra et al. [RBPA07] have pointed out that even in static scenarios, the handover rate is surprisingly high. This is consequence of the current mechanisms that trigger the handover under conditions of high medium utilization and packet loss rate. Additionally, the *AP discovery* depends on the number of channels to scan. Mishra et al. [MSA03] have demonstrated that this is the most time consuming operation when handover occurs, even with active scanning². Second, the *Authentication and Association* time, $T_{auth/assoc}$, depends on the complexity of the authentication protocol; this complexity may vary a lot according the security schema to be used. However, $T_{auth/assoc}$ can be well described by the number of exchanged packets between APs and stations when performing the authentication and association process.

We used simulations to evaluate the handover time, T_h according to three variables: Number of Clients, Mobile Speed and packet losses.

4.2.1 Number of Clients

We define a simulation scenario based on the operational context earlier described in 3.1. We consider an in-motion network with a number of wireless clients varying from 1 to 50 (1, 5, 10, 20, 30, 40 and 50), each one establishing connections directly to the infrastructure network. First, we evaluate the handover time for each wireless client using a constant speed. Fig.6 shows the influence of the amount of clients on the handover time T_h .

Multiple Range Tests for T_h by Client

Contrast	Sig.	Difference	+/- Limits
1-5	Yes	-0,472828	0,0158718
1-10	Yes	-0,499724	0,0151961
1-20	Yes	-0,552362	0,0148467
1-30	Yes	-0,605759	0,0147284
1-40	Yes	-0,660888	0,0146689
1-50	Yes	-0,717752	0,0146331
5-10	Yes	-0,0268966	0,0079359
5-20	Yes	-0,0795345	0,00724445
5-30	Yes	-0,132931	0,0069988
5-40	Yes	-0,18806	0,00687269
5-50	Yes	-0,244924	0,0067959
10-20	Yes	-0,0526379	0,00561153
10-30	Yes	-0,106034	0,0052906
10-40	Yes	-0,161164	0,0051226
10-50	Yes	-0,218028	0,0050191
20-30	Yes	-0,0533966	0,00418259
20-40	Yes	-0,108526	0,00396795
20-50	Yes	-0,16539	0,0038334
30-40	Yes	-0,0551293	0,0034994
30-50	Yes	-0,111993	0,00334607
40-50	Yes	-0,0568638	0,00307356

= statistically significant difference.

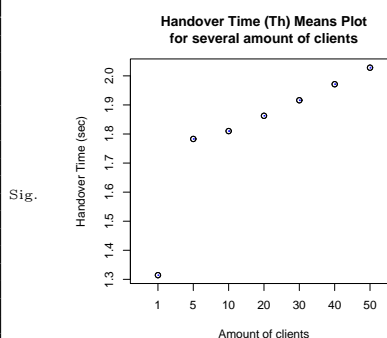


Figure 6: Handover Time versus amount of clients

²Active channel scanning consists in sending packet probes in each channel: the wireless card stabilizes in the new channel, then it sends a probe packet and waits for a response from an eventual AP in the same channel. Probe packets may also collide with other packets in the same channel, thus giving a response timeout.

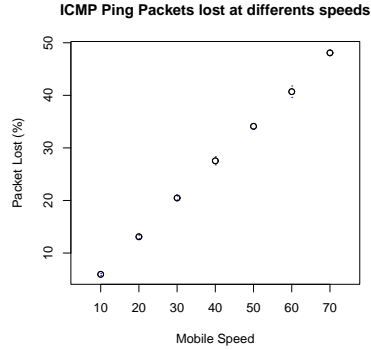


Figure 7: Packet Losses when 40 clients perform Handover at several Speeds

An *ANOVA Multiple Range Test analysis* [Jr.86] of T_h with respect to the number of clients shows significant difference between clients groups (1,5,10,20,30,40,50). This evidences that the number of clients affects significantly the handover time when all the clients compete to perform handover during the same period.

4.2.2 Effects of Speed

Considering now the effects of speed in presence of handover, it is worth noticing that during handover, the client can not exchange packets with the current associated AP. This fact implies a direct correlation between handover time and packet losses. When the mobile speed V increases, the number of traversed AP coverage spots per unit of time increases, as well as the probability of packet loss per unit of time. This effect is observed on Fig.7, where M is traveling several times along P , at various speeds, with a single on-board station. The AP coverage spot traversing time T_c is displayed on Table 2 for different speed ranges within a coverage area of 200 m for a fixed SNR.

Table 2: Time to traverse a 200m cell at various speeds

<i>Mobile Speed</i>	<i>Time to traverse a 200m-wide cell [T_d]</i>
10 km/h - 50 km/h	72.00 sec - 14.40 sec
51 km/h - 100 km/h	14.10 sec - 7.20 sec
101 km/h - 150 km/h	7.12 sec - 4.80 sec
150 km/h - 300 km/h	4.80 sec - 2.40 sec

The on-board client is able to exchange data with I while traversing a coverage spot, for T_d units of time. After the time T_d is up, the on-board client must trigger a handover to connect to the next AP and resume transmission during the next T_d transmission time slot. As T_d depends on the speed of M , there is a speed limit where T_d becomes similar to T_u , turning the system unusable, due the usable time for transmission is smaller than the minimal time required to exchange a minimal amount of data with the AP. This speed limit can be expressed as follow:

$$V_{limit} = \frac{coverage(i)}{(T_u + T_h)} \quad (4)$$

When V approaches to V_{limit} , the time to traverse the coverage area of an AP decreases, while the number of areas traversed per unit of time increases. Hence, the frequency of handover increases, increasing the packet losses. The overall packet losses are increased according to the number of traversed hot-spots per unit of time.

To summarize, the two key factors which influence packet loss are V and the number of in-motion wireless clients inside M .

4.2.3 Packet Losses

When a wireless station (STA) performs a handover, there are two possible sources of packet loss. One is packet buffering on both sides (AP and STA) when the radio is performing the handover operation; the other is during the update of the OSI layer 2 route table in the infrastructure network. It is common practice for each wireless station to broadcast Gratuitous ARP packets to inform the infrastructure network about the new layer 2 route to be used. In simpler words, when a STA is inside the next hotspot, and the infrastructure network is not informed about it yet, it still routes packets to the former AP until the new AP starts sending packets to the infrastructure (and so, update the route). During this transition period, all packets previously routed to the former AP will be lost due to MAC-level retransmission failures. As a consequence, route reconfiguration delays increases the probability of packet loss during the handover.

Summarizing, these three factors are closely related when traveling with a speed such that the radio spot traversing time T_d is comparable to the time taken for handover T_h . In the extreme case, T_d falls to zero. Furthermore, if multiple on-board stations interact directly with the infra-structure network, they compete with each other for the medium during handover, raising the packet loss probability. Moreover, when approaching the coverage limit, all on-board stations will trigger the handover process at the same time, which further increases T_h .

5 System Evaluation

In this section we evaluate the performance of the proposed system by means of simulations. We simulate a train trip with multiple on-board end-user stations, exchanging traffic with peer stations connected to the fixed network, outside the train. Our simulation scenarios are based on the reference scenario described in the section 3.1. The performance metrics we consider are communication delays (Round Trip Time and One Trip Time) and packet losses. These metrics are used to compare the conditions of connectivity between the Spiderman device and the WS AP on one hand, and with normal wireless stations and standard AP on the other hand. We compare these two configurations using two kinds of traffic: ICMP echo-reply loops, and UDP streams. Finally, we discuss the channel availability in both cases.

5.1 Simulation Scenario

We simulate a scenario similar to the one proposed by Zhou et al. [ZSH⁺05] which represents a standard railroad environment and corresponds to our context of reference. The scenario consists of 100 stations, half of which are located in the moving vehicle, and the other half being static, connected to the fixed infrastructure network. The traffic exchanged between the in-motion and the external stations is configured in order to load the network up to the limit at which packets start to get dropped when handover occurs and both devices (AP and client) start buffering the incoming traffic. For the configuration without the Spiderman system, the 50 on-board wireless stations are connected directly to standard IEEE802.11 wireless Access Points placed along the route of the vehicle. For the configuration with the Spiderman system, the on-board stations are connected to an on-board access point, which is linked to the *Spiderman Device*, and *Wireless Switch Access Points* (WS APs) are used in place of standard APs along the route of the vehicle.

For each simulation run, the train, travels with a fixed speed S , chosen in the range of 10-70m/s with 10m/s steps. On the infrastructure side, a 10Km long route is used and covered by 33 access points. The upstream and downstream rates are fixed to 2 Mbps (half duplex). Each AP is connected to an Ethernet Switch using 100 Mbps full-duplex links. Furthermore, all the traffic exchanged with the infrastructure is concentrated in a Layer 3 (IP) gateway. The 50 external stations are beyond this gateway. We initiate two flows for each pair of stations (external station, on-board station): one 10Kbps CBR UDP flow from external to on-board stations, and one ICMP Ping flow at a rate of 1 packet per second. These traffic profiles met the condition of saturation we stated earlier in this section. We also fixed the queue size to 10 packets for all the participating devices inside the train. The simulation time t is configured to 142s, which is the time required time to traverse 33 APs at 70 m/s and produce steady confidence intervals for the measured variables. Additionally, statistical confidence intervals are computed over 30 simulations with different random seeds.

The simulation software used is Omnet++ (v3.3) with the INET Framework (v20061020) [Var01]. The INET Framework has been modified in order to support the depicted scenario. The most important modifications are the support

of multiple wireless cards in the same host and the support of Gratuitous ARP in the ARP module³.

We have chosen the Pathloss model which is the most appropriate for a short-wireless link without obstacles.

5.2 Delays

We observe on Fig.8 two graphs showing the ICMP ping Round Trip Time (RTT). The graph 8(a) corresponds to the configuration without the SD, and the graph 8(b) to the configuration with the SD and WS APs. The graph 8(a) shows small periodic connectivity drops, that increase with the vehicle speed. These drops are caused by tail drops in queues due to buffering during handover. This contrasts with graph 8(b) in which these drops disappear. This confirms that the Spiderman Device successfully prevents dropping packets during handover disconnections, but it also shows this improvement increases apparently the maximum transmission delay.

Despite the maximum delays are higher in 8(b) than 8(a), in the case of the SD configuration, our statistical analysis of the delay variable in both configurations does not show a significant difference⁴ These peaks are caused by the Gratuitous ARP packets inserted in the *Input Queue* (one sent for each on-board station) when a handover occurs between two hotspots. However, these peaks are not enough to significantly impact the delay mean.

5.3 Packet loss

In the following we compare the packet losses suffered by both our configurations (with and without Spiderman). The comparison is two-fold: first, we study the outbound traffic case (on-board traffic toward Infrastructure); and second, we study the inbound traffic case. In both cases we calculate the packet losses that correspond to MAC drops and queue tail drops in the transmission queues. Fig.9 compares the packet loss observed in our generated UDP flow for a fixed simulation time, in both configurations. In the configuration without Spiderman, we see that the packet loss is growing linearly with the speed of the vehicle, from less than 10% at 10 m/s up to 50% at 70 m/s. This is a direct consequence of the increased number of handover per unit of time and demonstrates the inability of standard handover to operate at high speed.

This strong correlation between speed and packet loss disappears with the second configuration. This is explained by the fact that the Spiderman device is able to queue the packets while handovers are happening. Indeed, the handover time being shorter, the queueing capacity required is limited, which results in a better ability to avoid packet losses at all speeds. Notice in particular that the packet loss variance is uniform for all the simulated speeds we considered.

Packet losses are kept independent of the speed until a critical speed is reached, which depends on the time required for traversing a hotspot (discussed on section 4.2.2). If the usable time, T_d is similar or bigger than T_u ⁵, the

³The complete modified INET framework is available at http://www-sop.inria.fr/members/Juan-Carlos.Maureira_Bravo/download/INET-20061020-JcM.tar.gz

⁴A Student t-test has been used to compare the population means of the delay samples collected during the simulations of both configurations.

⁵In this case, there is no time left to transmit a minimal amount of data to the infrastructure.

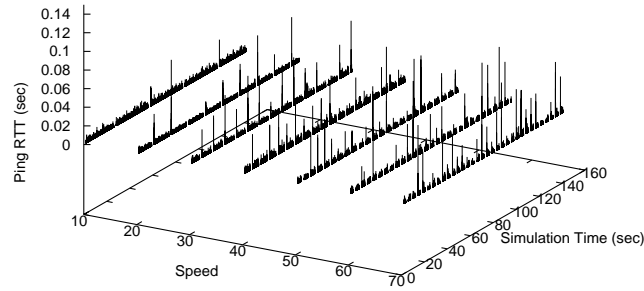
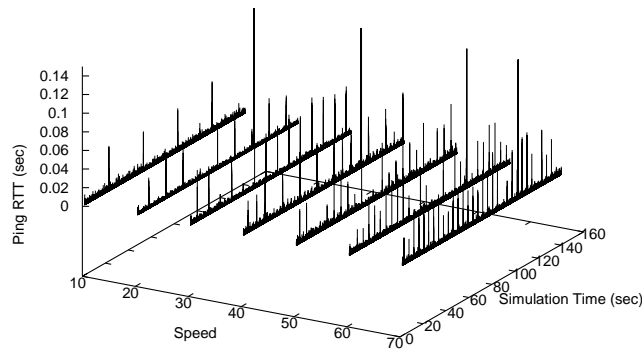
(a) ICMP Ping RTT at different speeds **without** Spiderman(b) ICMP Ping RTT at different speeds **with** Spiderman

Figure 8: ICMP Ping delay without the Spiderman device (a), and with Spiderman device (b)

proposition 4.1 does not hold, and the system becomes unusable. Thus, the larger the coverage area, the higher the speed limit. This is the boundary condition for the speed of M .

In the following, we compare our two configurations in presence of incoming traffic from the Infrastructure AP to the on-board stations. On Fig. 10 we observe the queue length and packet losses during a transition between two APs from the infrastructure point of view. Let us first consider the configuration without the Spiderman device. When the on-board stations exit the current AP coverage and lose connection with the infrastructure network, the AP queue becomes rapidly full since the MAC is hopelessly retransmitting packets. Packets are not received by the on-board stations, and for each ACK timeout there

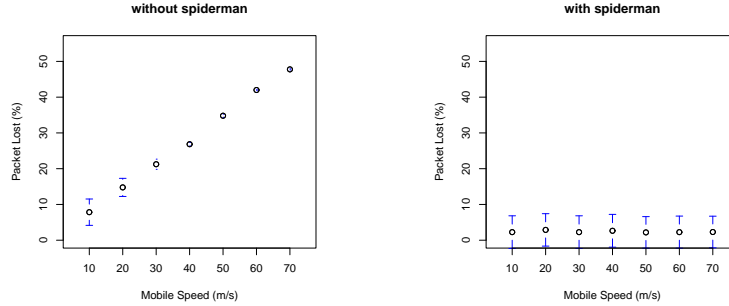


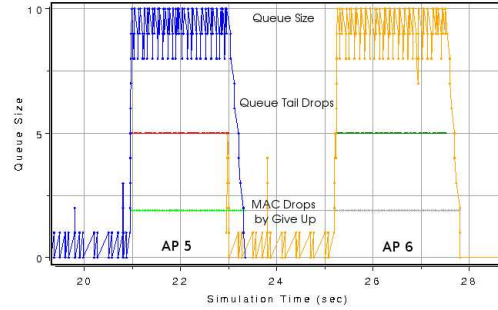
Figure 9: UDP Packet losses at different Speeds

is a retransmission until the retry limit is reached. The time taken by each packet on the queue to arrive to the MAC increases and the queue becomes full. Consequently, packets start to be dropped at the queue level too. During this period, the on-board station starts a full channel scan, finds the next AP, associates and authenticates and finally sends a Gratuitous ARP to announce to the infrastructure switches the route update. The switches stop sending packets to the former AP and start sending packets to the next AP. As a consequence, the queue drop events on the former AP stop and packets are lost only due to failed retransmissions. During this process, all the packets which arrived to the former AP between the start of channel scanning until the switch to the next AP are lost.

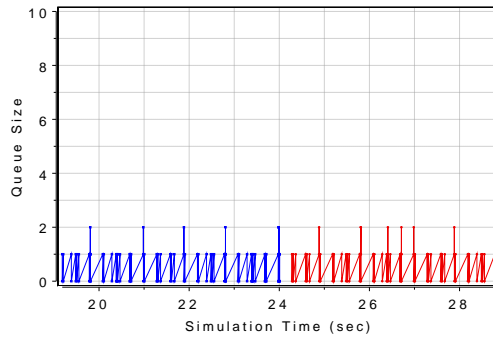
Now, let us consider the configuration with the Spiderman device. We define the time dt as the time interval during which the *Input Queue* is active. As explained in the section 3, the *Input Queue* is active while the Spiderman Device is swapping radios (from the moment that the *passive* radio gets connection, to the moment when the *Input Queue* is completely flushed into the new *active* radio). In this case, when dt starts, the Spiderman device has already done scanning, authentication, association and has already sent the Gratuitous ARP packets to switch the traffic to the next AP. Then, the external traffic coming from the infrastructure switch is transmitted from the next AP smoothly. From the in-motion devices, only dt is observed as the time when the devices are not connected to the infrastructure network.

5.4 Channel availability

Another expected benefit of the *Spiderman Device* and its companion *Wireless Switch AP* is the maximization of the channel availability for user data transmissions. The time-line of the handover process presented in Fig. 11 shows the difference between the two configurations. In the case of Spiderman (overlapping bars in the middle), we see that handover and transmission periods, respectively noted T_h and T_d , are overlapping. This overlap means that T_h does not affect length of T_d , since the device uses the *passive* radio to scan frequencies and find the next AP in parallel with the *active* radio. In the other configuration, without Spiderman, we can see that T_d and T_h periods alternate with each other. And since the sum of both these durations is a constant, the longer we spend



(a) Access Point TX Queue Length, Taildrop events and MAC GiveUp events when on-board stations perform handover between AP 5 and AP 6 **without** Spiderman



(b) Access Point TX Queue Length, Taildrop events and MAC GiveUp events when on-board stations perform handover between AP 5 and AP 6 **with** Spiderman

Figure 10: Access Point queue length and drop behavior (50 on-board stations). Fig.(a) without Spiderman. Fig.(b) with Spiderman.

in T_h for handover, the less time we have left in T_d for user traffic transmission. Notice also that without Spiderman, assuming a configuration in which each on-board is directly connected to the Infrastructure APs, each station has to execute the handover independently, which results in as many full scan being performed in parallel as there are onboard stations, which further increases T_h , and decreases T_d .

This behavior can be observed on Fig.12(a), which shows T_d at 60m/s in such a configuration in which all the on-board stations are competing to access the channel, while in Fig. 12(b) we show the Spiderman device using full scanning and the reduced scanning⁶. The usable transmission time T_d presented in Fig. 12(a) without Spiderman is visibly lower than the one shown on Fig.12(b) with Spiderman, either using quick or full scanning. The channel availability time is increased by 60%, from 3s to 5s per coverage area traversal. The use of a reduced set of channels to scan, or Full scanning does not affect the T_d length. Nevertheless, reduced channel set scanning is more robust than Full scanning because of a shorter repetition cycle, increasing the probability to find the next

⁶scan only channels 1,6,11 as we explained earlier in this report.

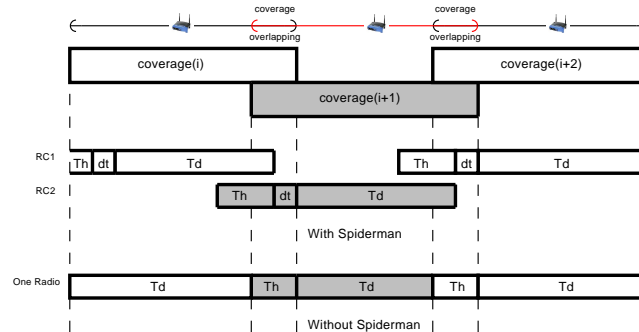
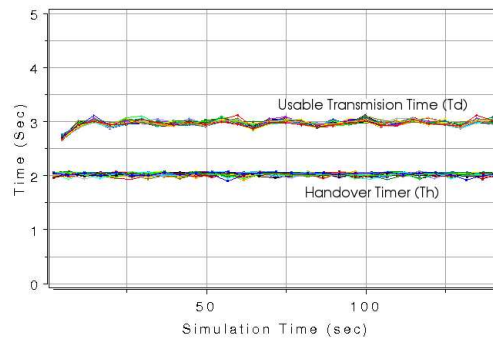


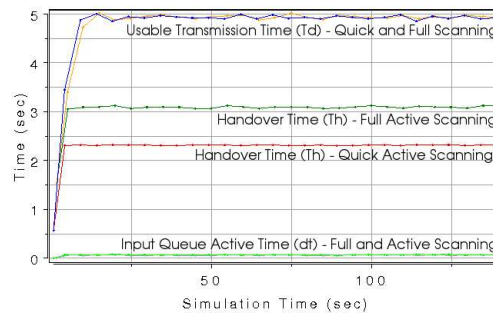
Figure 11: Timing diagram (not to scale)

AP earlier. On Fig.12(b) we see that dt , the radio switch delay (which includes the time to flush ARP packets), is below 0.2s, or less than 4% of the channel availability time.

Regarding the *Gratuitous ARP loop*, the access point proximity (AP coverage diameter) ensures the Gratuitous ARP will return to the spiderman *active* radio in a short time. With wider AP coverage diameter, the process experiments higher dt values.



(a) 50 on-board stations using Full Scanning



(b) 50 on-board stations wired to Spiderman using Full and Quick Scanning

Figure 12: Traveling Time and Handover Time in both scenarios, at 60m/s: (a) without Spiderman, and (b) with Spiderman

Fig.12 gives an empirical illustration, based on simulations, of the timings presented on Fig. 11. This graph shows T_d , which stays constant around 3 seconds, T_h for both handover methods, and dt (the buffering period for the Spiderman device). As we can see, the influence of a full scan is the main cause of the low utilization of the channel even when the stations are within the AP coverage. The Spiderman device reduces unavailability period without significant packet loss, which is 10 times higher in the configuration without Spiderman.

6 Conclusions

In this report we present the Spiderman Device and evaluate its suitability for providing continuous network connection to mobile users located on-board a vehicle cruising at "high speed" along a fixed, predictable route. Using simulations, we have shown that the use of the Spiderman dual-radio used in combination with a custom handover procedure and a custom *Wireless Switch Access Point* is enough to provide a continuous network connectivity to on-board stations inside a Mobile up to at least 150 km/h. Interestingly, these new devices use regular IEEE 802.11 protocols and can easily be built using standard, low-cost, off-the-shelf equipments.

It is also worth to mention that this 150 km/h limit is a worst case conservative estimation based on our limited knowledge of the Doppler effects on 802.11 transmissions at very high speed. Higher speeds up to 250 km/h are envisaged, but this will require further experiments in real conditions. Nevertheless, at higher speeds, the usable transmission time T_d becomes similar or greater than the minimal time required to transmit data to the infrastructure, T_u , which results in a non-functional system once the speed limit is reached. A possible solution to investigate is to use a wider AP coverage area to increase the speed limit (the coverage area used in this study is 200m wide).

We have also shown that the addition of a new input queue to avoid losing packets when switching between the two radios does not affect the overall traffic delay. In addition, we propose to trigger the early sending of Gratuitous ARP packets in order to reduce the handover time and speed up the layer 2 route update.

Another consequence of the use of a single device with two radios is the increase of IEEE 802.11 channel availability time, (+60%) due the aggregation of in-motion clients traffic on a single outgoing interface.

Furthermore, an additional good property is multi-protocol routing ability of the proposed solution, since the proposed device acts as a bridge with handover capabilities. Consequently, any layer 3 protocol can be used. In the special case of IP, there is no need of per client IP address translation, and seamless IP Portability is guaranteed along the path.

7 Further Work

This report leaves issues open for further studies. In particular, the fixed infrastructure design introduces a new challenge that must be investigated: the Infrastructure Network must be cost-effective, self-managed, fault-tolerant, and easy to deploy.

The previous works from Gass, Scott and Diot [GSD06] and Zhou et al. [ZSH⁺05], which have measured packet loss at different Mobile speeds, are good starting points, but a more realistic channel model should be used in simulations in order to provide a better evaluation of the behavior of the proposed handover method under more stressing conditions. Furthermore, implementation and experimentation of the Spiderman device with the Wireless Switch in a real environment would be an important step towards standardization and consolidation as a industry accepted solution to the problem.

Security is another crucial issue to address in current communication systems, and especially in the wireless context. The Spiderman device could benefit from the use of a One Time Password generation function or with the recently standardised 802.11r amendment. Both alternatives will be considered in further studies.

Acknowledgements

The authors would like to thank everyone who helped us write this report. This work was partly founded by the IST-FET AEOLUS project.

References

- [BMB05] Vladimir Brik, Arunesh Mishra, and Suman Banerjee. Eliminating handoff latencies in 802.11 w lans using multiple radios: applications, experience, and evaluation. In *IMC '05: Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*, pages 27–27, Berkeley, CA, USA, 2005. USENIX Association.
- [EBM08] Jakob Eriksson, Hari Balakrishnan, and Samuel Madden. Cabernet: Vehicular Content Delivery Using WiFi. In *14th ACM MOBICOM*, San Francisco, CA, September 2008.
- [GSD06] R. Gass, J. Scott, and C. Diot. Measurements of in-motion 802.11 networking. *Mobile Computing Systems and Applications, 2006. WMCSA '06. Proceedings. 7th IEEE Workshop on*, pages 69–74, Aug. 2006.
- [Jr.86] Rupert G. Miller Jr. *Beyond Anova- Basics of Applied Statistics*. John Wiley and Sons, inc., New York, 11 edition, 1986.
- [MSA03] Arunesh Mishra, Minh Shin, and William Arbaugh. An empirical analysis of the iee 802.11 mac layer handoff process. *SIGCOMM Comput. Commun. Rev.*, 33(2):93–102, 2003.
- [OK04] J. Ott and D. Kutscher. Drive-thru internet: Ieee 802.11b for "automobile" users. *INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*, 1:–373, March 2004.
- [RBPA07] Ramya Raghavendra, Elizabeth M. Belding, Konstantina Papagianaki, and Kevin C. Almeroth. Understanding handoffs in large iee 802.11 wireless networks. In *IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, pages 333–338, New York, NY, USA, 2007. ACM.
- [RRL06] K. Ramachandran, S. Rangarajan, and J.C. Lin. Make-before-break mac layer handoff in 802.11 wireless networks. *Communications, 2006. ICC '06. IEEE International Conference on*, 10:4818–4823, June 2006.

-
- [Tse07] Terry Tse. Study of high-speed wireless data transmissions for railroad operation. Technical Report RR07-10, Federal Railroad Administration - Office of Research and Development, April 2007.
- [Var01] Andras Varga. The omnet++ discrete event simulation system. In *Proceedings of the European Simulation Multiconference*, pages 319–324, Prague, Czech Republic, June 2001. SCS – European Publishing House.
- [ZSH⁺05] Ting Zhou, H. Sharif, M. Hempel, P. Mahasukhon, and Song Ci. Performance of ieee 802.11b in mobile railroad environments. *Vehicle Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd*, 4:2527–2531, Sept., 2005.

Contents

1	Introduction	3
2	Previous Related Work	4
3	System Description	5
3.1	Operational context	5
3.2	The Spiderman Device	7
3.3	The Handover Procedure	7
3.4	The Wireless Switch Access Point	9
4	Requirements Analysis	11
4.1	Functional Requirement	11
4.2	Timing Constraints	12
4.2.1	Number of Clients	12
4.2.2	Effects of Speed	13
4.2.3	Packet Losses	14
5	System Evaluation	15
5.1	Simulation Scenario	15
5.2	Delays	16
5.3	Packet loss	16
5.4	Channel availability	18
6	Conclusions	22
7	Further Work	22



Centre de recherche INRIA Sophia Antipolis – Méditerranée
2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Centre de recherche INRIA Bordeaux – Sud Ouest : Domaine Universitaire - 351, cours de la Libération - 33405 Talence Cedex
Centre de recherche INRIA Grenoble – Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier
Centre de recherche INRIA Lille – Nord Europe : Parc Scientifique de la Haute Borne - 40, avenue Halley - 59650 Villeneuve d'Ascq
Centre de recherche INRIA Nancy – Grand Est : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex
Centre de recherche INRIA Paris – Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex
Centre de recherche INRIA Rennes – Bretagne Atlantique : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex
Centre de recherche INRIA Saclay – Île-de-France : Parc Orsay Université - ZAC des Vignes : 4, rue Jacques Monod - 91893 Orsay Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
<http://www.inria.fr>
ISSN 0249-6399