Transparent real time service on connected train

Seifddine Bouallegue, Nozha Cherif, Kaouthar Sethom

Transparent Real time Service on Connected Train

Seifddine Bouallegue
INNOV'COM LAB, SUPCOM
University of Carthage, Tunisia

Nozha Cherif
ESPRIT Institute of Engineering
M2M Team, Tunisia

Kaouthar Sethom
INNOV'COM LAB, SUPCOM
University of Carthage, Tunisia

***Abstract*— In order to achieve the everywhere at anytime Internet, connection to the network must be available even inside cars, trains and buses, without disruption of service. In order to reach this objective, intelligent communications are now considered necessary and will play an increasing role in the modern Transportation Systems. As train speeds increase, wireless communications between devices on the train and the outside encounter difficulties, and maintaining communication quality is a major challenge. This paper, propose a new multihomed solution for transparent internet access in trains through secure handoff anticipation.**

I. INTRODUCTION

The growth in wireless communication technologies over the last two decades opens up several opportunities for supporting internet access on trains. While wireless access technologies offer higher data rates and wireless network coverage continuously increases, we are still far from seamless and ubiquitous Internet connectivity. Particularly when users move, wireless conditions change and handovers (potentially to different operators or networks) occur, that may yield significantly different communication characteristics—or connectivity may be lost altogether. Even though Internet protocols and applications are (or should be) designed to adapt to changing network conditions, their capabilities to deal with sudden changes are fairly limited—and disconnections are usually not tolerated at all. The former may and the latter usually do lead to errors and applications break.
Users demand the ability to keep their ongoing communications while changing their point of attachment to the network as they move around.

Currently, NEtwork MObility (NEMO) solutions [1] are being developed by the Internet Engineering Task Force (IETF) and the research community to offer Internet access from vehicles. Special devices (called mobile routers [MRs]), located in the vehicles, handle the communication with the fixed infrastructure and provide access to passengers' devices using a convenient radio technology.

This protocol associates each egress interface of a MR with two distinct addresses, much like what is done in Mobile IP [2]. The permanent home address MR_{HoA} is obtained in the home network and has the same prefix as the home link. The temporary care-of address MR_{CoA} is obtained in the visited network and formed based on the prefix advertised on the visited link.

II. PROPOSED ARCHITECTURE

Large handover latency causes the loss of a large number of MNN packets. Therefore the reduction of handover latency is a very important requirement in enabling mobile networks to support multimedia communications. NEMO, which has large handover delay and high packets loss ratio, cannot meet the requirements for the real-time applications. To address these issues, a secure and faster handover scheme for trains based on multiple antennas cooperation is proposed in this paper.

1. Link layer switching

Mobile networks are more likely to be multihomed than the mobile nodes are. Multihoming refers to a situation where a node can choose between several paths to reach a correspondent.

The multiple choices are due to the train router having several interfaces. Such a configuration is particularly useful in mobility contexts because it ensures mobile entities remain permanently connected to the internet even in the following situations: loss of connectivity (as a result of moving out of a coverage area or because wireless technologies are more subject to interference), lack of connectivity (a given technology cannot cover all geographic areas) or lack of bandwidth (technologies with high bandwidth are generally not available for mobile users).

To take advantage of this technique, we propose a multihoming-based seamless handover scheme using a multihomed MR with dual antennas in NEMO on railway trains [11] (Figure 1). The two antennas are located at the two far ends of the mobile train. One of the two egress interfaces of MR can continuously receive packets while the other is undergoing a handover. Therefore, the proposed scheme has no service disruption or packet losses during handovers.

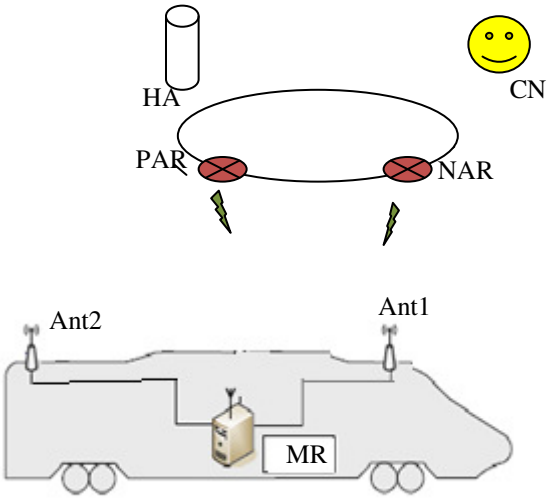

Figure.2 PROPOSED ARCHITECTURE

2. Care of Address pre-configuration

To achieve a low-latency and less-loss handover, the objective of our proposal is to obtain New CoA before handover. To make full use of the train characteristics such as the fixed passenger railway lines and regular movement of trains, we can prepare in advance the list of handover candidate cells and by consequence next ARs. We can thus prepare CoA configurations in advance.

When MR leaves the station home network, it registers its home address to HA. According to the train predefined trajectory, the HA could know the future ARs that the train will meet and can pre-establish with them the list of next CoAs. The HA maintains this list with the right order according to the first crossing AR (CoA n°1), second AR (CoA n°2)…

3. Security issues

A security research group, "The Hacker's Choice" has reverse-engineered the femtocells operated by a British mobile operator and discovered that it could be used to make illegal calls and send text messages [3]. In this paper, we present a secure ITS femtocell scenario and investigate the feasibility of using our solution inside MOBIKE architecture [4] for better security.

The main scenario for MOBIKE is enabling a remote access VPN user to move from one address to another without re-establishing all security associations (SA) with the VPN gateway. MOBIKE updates only the outer (tunnel header) addresses of IPsec SAs, and the addresses and other traffic selectors used inside the tunnel stay unchanged. Thus, mobility can be (mostly) invisible to applications and their connections using the VPN.

III. THE VIRTUAL INTERFACE

Virtual Interface Decision Process

Configuration Phase:
1. Add user specified network devices to the VIP candidate list (or by default all available devices).
2. Select one as the active slave and extract its IP and MAC addresses.
3. Pass these addresses to viMAC0.
4. Enslave devices on the candidate list under the virtual interface (same IP & MAC @).
5. Continue with Normal Phase.

Normal Phase:
While (viMAC0.up=true):
1. Send/receive traffic through the active slave.
2. If (control_interval=true):
Collect information on every slave interface from corresponding Drivers (exp: statistics) and update the slave list if necessary.
3. If (new.event=true):
Add/remove corresponding interface from slave list.
4. If (active.salve=down):
Elect a new active interface from the slave list and Handoff all current transmissions to the new interface.

Figure . 3. VIP INTERFACES MANGEMENT

The principium of multihomed train with dual antennas was proposed in [5]. But the authors consider different IP address for each antenna (*ant*2 and *ant*1). This leads to an additional signaling cost and unnecessary antenna switching: When the Head *ant*1 crosses the boundary of a new cell, it achieves a new handoff with the NAR. When later the trail-ant (*ant*2) crosses the boundary of the NAR (because of train movement), a second handoff is performed to switch traffic to the *ant*2. This implies additional signaling cost and binding updates to the NAR and the HA.

In our point of view, the solution lies on having the same IP and MAC address on the two MR interfaces *ant*1 and *ant*2. By assigning to all the physical devices on the MR the same IP and MAC addresses (with the rule that only one is active in the same subnet at the same time *t*), the mode of communication during handover will be transparent to higher layer transport protocols.

However, the Internet routing model forces routers to have different MAC and IP address for each active physical interface in the MR. This means that in our scenario the MR will have two different IP addresses one for each antenna (IP1 for *ant*1 and IP2 for *ant*2).

Since this is not possible with today implementations, we added a new virtual MAC layer between the hardware level and IP level (Figure 3). We assign a unique unicast IP address to this virtual MAC address, consequently, application might think of any flow as dealing with traffic corresponding to a single interface only.

The proposed interface hides the presence of the different router interfaces to the applications layer by providing the illusion of a unique interface and by consequence IP address (Figure 4). All corresponding node's flows are sent to this virtual MAC interface: before the handoff, it will correspond to *ant*1 and after the handoff it will correspond to *ant*2. At any time, the virtual interface must manage the changes in network connection's status (handovers). That's why; it will periodically evaluate interface's status and use this information to select the good interface for communication. The virtual MAC groups all information from the interfaces in a specific table that is dynamically updated [6].

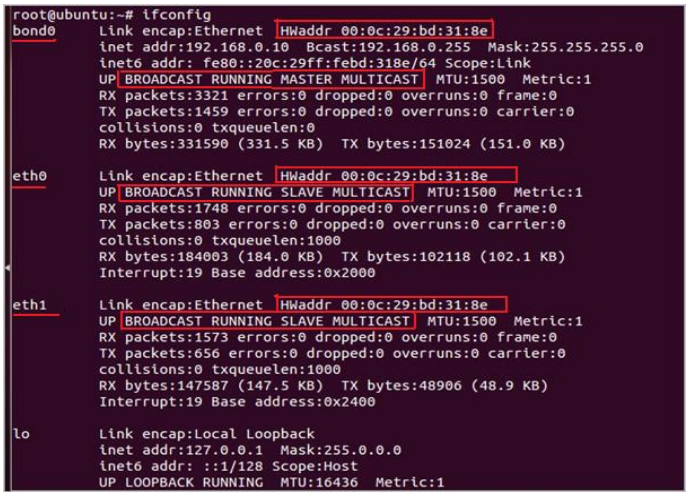

Figure 4. VIP IMPLEMENTATION

After the virtual interface is created, all the network interfaces that have to be attached must be configured as slaves. The MAC address of the virtual interface is taken from its first slave interface. This MAC address is then passed to all following interfaces (Figure 4) and remains persistent (even if the first one is removed). The way the virtual interface is implemented violates this unique MAC address per interface standard, by deliberately making several NICs have the same MAC address.

The two MR antenna *ant*1 and *ant*2 will share the same IP address thanks to VIP implementation. When the ant1 leaves the AR1 coverage, the ant2 will be used by the virtual interface to continue receiving packets to the MR with the same IP address. The network is thus unaware about the change. One the train complete L3 handover with the new AR through *ant*1, it switches to receive traffic through *ant*1 and can use the new CoA.

VI. PERFORMANCE ANALYSIS

In this section, a deep analysis of our solution is proposed based on the handover latency and its impact on packet loss.

1. *Velocity consideration*

The time duration (T_d) during which *ant*2 remains connected to PAR after *ant*1 leaves PAR depends on the distance (d) between *ant*1 and *ant*2, and the speed (v) of the mobile network, i.e:

$$T_d = d/v$$

For a very-low loss handover, *ant*2 should remain connected to PAR for duration greater than or equal to the handover latency (T_h) of *ant*1, i.e., $T_d \geq T_h$. For example, suppose a mobile network on a train where d = 100 meters and v = 100 km/hr. The value of T_d will thus be 3.6 seconds, which is a sufficient time to allow *ant*1 to complete binding updates with its HA before *ant*2 leaves PAR.

.

2. *Signaling cost*

We have analyzed and compared the protocol cost of our VIP-based proposal with basic NEMO [11]. The handover latency is given by:

$$S_h^{NEMO} = S_{L2} + +S_{\mathrm{CoA}} + S_{HA\_BU} \quad (1)$$

$$S_h^{VIP} = S_{L2} + S_{\mathrm{dAd}} + S_{HA-BU} \quad (2)$$

From (1) and (2), it's clear that we have:

$$S_h^{VIP} < S_h^{NEMO}$$

Using VIP has a cost since packets have to go through an additional layer before being sent on the physical medium and

vice-versa. To measure this cost, we studied the impact of VIP on UDP applications and compare the result with that of the standard Linux implementation (section 3).

3. *Test-bed*

We implemented a prototype for performance evaluation. The Femto System Architecture used in our test-bed is shown in Figure 5. It is largely based on the work of 3GPP working group SA3 which is responsible for the overall security of all 3GPP systems. The system architecture is described as having the following features:

• The backhaul link, is connected from the Femto AP (FAP) to the operator's core network via a SeGW (Security Gateway).
• SeGW represents operator's core network to perform mutual authentication with FAP.
• Security tunnel is established between FAP and SeGW (through Mobike) to protect information transmitted in backhaul link.
•An AAA server authenticates the hosting party module, a SIMcard based mechanism that is optionally deployed in the Femto architecture to help the operators effectively managing the FAP.

We choose to install Strongswan software [7] because it's currently the only open source implementing IKEv2 and supporting MOBIKE, and therefore we use it to study the feasibility of using this protocol on femtocell networks. Finally, to simulate the network conditions, we installed Iperf [8], which is an open source software used as a testing network tool that can create UDP and TCP data streams and measure the network performance: bandwidth, delay and packet losses. we used wireshark software [9] for traffic analysis. We conducted experiments on several Linux hosts (Figure 5) whose main features are shown in Table1.

4. *Handoff latency*

We measured handoff latency as the time between the last packet from MN and first received packet after handoff. Two tests were performed according to IKE authentification methods (Figure 6): in the first scenario MOBIKE used public-key cryptography based on RSA algorithm. The second scenario uses certificate x509 to authenticate the two peers of the IPsec tunnel.
The VIP implementation was running during all the tests. Our solution performs with a very low handoff delay of 47 ms in maximum (Figure 6). Compared to previous solutions such as NEMO (where the handoff delay is about 1s [10]), our proposal reduces considerably the handoff latency.

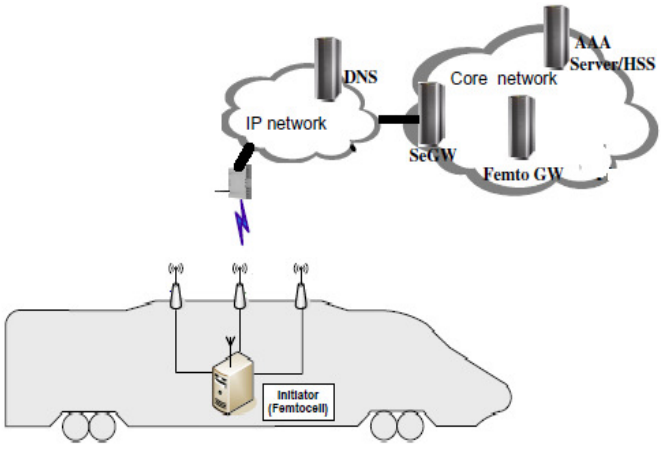

Figure .5 Test-bed scenario

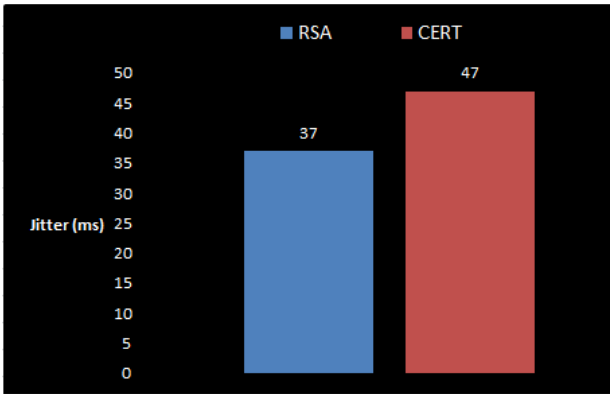

Figure .6 Handoff delay

The performance measurements match our expectations and effectively show the advantages of implementing mobility management at lower layer. As the switching process is very fast, the handoff is performed in a seamless way without long period of interruption.

Figure 7 shows throughputs measurements. As we can see, VIP overhead is very small compared to that of the standard Linux implementation; especially in the case of UDP traffic where it could be equal to zero. This can be explained by the fact that VIP operates at the link layer which does not reduce the volume of data a packet may include. Moreover, as all the physical interfaces share the same MAC address (as the virtual interface), no MAC address translation or swapping is needed; which means no additional packet encapsulation /decapsulation. VIP overhead is only due to the time needed by the virtual interface to consult its local commutation table to decide on which physical interface it could send data.

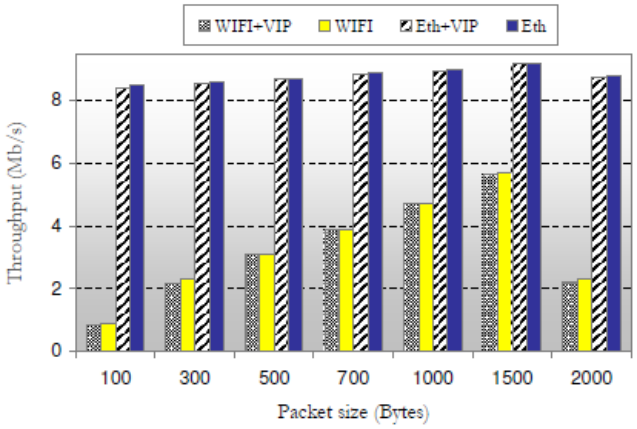

Figure .7 Throughput overhead for UDP traffic

V. CONCLUSION

In recent years, there have been significant interest and progress in the field of intelligent transportation system (ITS) from both industry and academia. Fast handoff in NEMO is very crucial for providing uninterrupted Internet services to the users in quickly moving vehicles. However, the NEMO basic support protocol takes comparatively long time to complete the handoff process resulting in large number of packet drops.

Moreover, the various nodes involved in NEMO are vulnerable as the network is wireless with no security mechanisms. In this paper, we proposed fast NEMO management solution to reduce the handoff latency and packet losses experienced in basic NEMO protocol.

REFERENCES

[1] Devarapalli, V., Wakikawa, R. and Petrescu, A. (2005) 'NEMO basic support protocol', *IETF, RFC 3963*, January 2005.

[2] Banerjee, N., Wu, W. and Das, S. (2003) 'Mobility support in wireless internet', *IEEE Wireless Communication*, Vol. 10, No. 5, pp.54–61

[3] P. Bright. (2011) Insecure vodafone femtocells al-low evesdropping, call fraud http://arstechnica.com/security/news/2011/07/insecure-vodafone-femtocells-allow-eavesdropping-call-fraud.ars

[4] IKEv2 Mobility and Multihoming (*MOBIKE*) www.tools.ietf.org/html/rfc4555

[5] Park, H., Kum, D. and Kwon, Y. (2006) 'IP mobility support with a multi-homed mobile router', *NETWORKING 2006, LNCS 3976*, pp.1144–1149.

[6] K. Sethom,H. Afifi and G. Pujolle. 'VIP*:* Virtual Interface Prototype for Mobile Communication', PIMRC 2005, pp.1591-1595.

[7] MOBIKE open source. www.strongswan.org

[8] www.iperf.fr

[9] Network protocol analyzer. www.wireshark.org

[10] Ng, C., Ernst, T.E. and Paik. (2007) 'Analysis of multi-homing in network mobility support', *Internet-Draft, Draft-ietf-nemomultihoming-issues-07*, February.

[11] K.S. Ben Reguiga, N.Cherif, "Fast handoff management for Internet access on train", Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP , pp1-4.