Fast Layer-3 handover in Vehicular Networks

Master's Thesis in Computer Systems Engineering

Ahmad Naseem Alvi, Tsovinar Babakhanyan
Fast Layer-3 Handover in Vehicular Networks

Master’s thesis in Computer Systems Engineering

School of Information Science, Computer and Electrical Engineering
Halmstad University
Box 823, S-301 18 Halmstad, Sweden

June 2009
Description of cover page picture: Vehicle entering in new subnet after no coverage area
Preface

This thesis is a concluding part of the master program in computer systems engineering at Halmstad University. This project has been carried out due to the importance of the vehicular communication in terms of safety applications. In this project we analyzed the handover issues in ITS and introduces a solution to reduce the latency of the handover on layer 3. We are very thankful to our supervisor Annette Böhm for her timely help and direction throughout this thesis project.

Ahmad Naseem Alvi & Tsovinar Babakhanyan
Halmstad University, June 2009
Abstract

Wireless communication is of great importance for safety and entertainment purposes in vehicular networks. Vehicles on roads are required to share sensor data, road traffic information or digital maps with other vehicles on the road. To be able to do this, vehicles require to either communicate directly with each other or to be connected to a wireless communication-based access points on the road side. These wireless access points support short to medium range wireless communication through the protocol 802.11p. 802.11p is designed specifically for vehicular communication and it is an amended form of the widely used 802.11 protocol suit for wireless local area networks (WLAN). Vehicles are able to be associated with these wireless access points for exchange of information. While vehicles move along the road infrastructure, they change their point of attachment from one wireless access point to another wireless access point. During this process, connectivity to the access point breaks down until the vehicle is connected to a new access point in its area. This disconnection causes an interruption in the data flow. This interruption increases when vehicle requires a new IP address, i.e. when the vehicle is going to attach to an access point which is part of another network. In this thesis report, we give an overview of standard handover methods and their enhancements and propose a fast handover scheme for layer 3 of the communication stack. Based on the assumption that vehicles know their route in advance, we enhance the handover process and improve seamless connectivity. We also discuss different issues which are the cause of delay and how they can be overcome in our proposed solution.
Contents

PREFACE ...................................................................................................................................................................... I

ABSTRACT ................................................................................................................................................................III

CONTENTS................................................................................................................................................................. V

1 INTRODUCTION ............................................................................................................................................... 1
  1.1 VEHICULAR COMMUNICATION .................................................................................................................... 1
  1.2 FOCUS OF THESIS ......................................................................................................................................... 2

2 VEHICULAR NETWORKS ..................................................................................................................................... 5
  2.1 WAVE ............................................................................................................................................................ 6
  2.2 PARTS OF VEHICULAR NETWORKS ............................................................................................................. 6
  2.3 ITS APPLICATIONS ....................................................................................................................................... 7
  2.4 HANDOVER ............................................................................................................................................... 8

3 HANDOVER TECHNIQUES ............................................................................................................................. 11
  3.1 WHAT IS HANDOVER .................................................................................................................................. 11
  3.2 ROUTING BETWEEN MOBILE NODE AND CORRESPONDING NODE ....................................................... 12
  3.3 MOBILE IPv6 .......................................................................................................................................... 13
  3.4 ADVANTAGES OF MIPv6 OVER MIPv4 ..................................................................................................... 15
  3.5 MOBILE IPv6 TYPES .................................................................................................................................. 16
    3.5.1 Hierarchical Mobile IPv6 (HMIPv6) .................................................................................................... 16
    3.5.2 Fast Handover for Mobile IPv6 (FMIPv6) .......................................................................................... 17
    3.5.3 Fast Handover for Hierarchical Mobile IPv6 (F-HMIPv6): .............................................................. 18
  3.6 NETWORK MOBILITY (NEMO) ................................................................................................................... 19
    3.6.1 NEMO Handover .................................................................................................................................. 20
    3.6.2 Latencies in NEMO Handover ............................................................................................................. 20

4 FASTER HANDOVER ....................................................................................................................................... 23
  4.1 ADVANTAGES ............................................................................................................................................. 28
  4.2 LIMITATION .............................................................................................................................................. 28

5 CONCLUSION .................................................................................................................................................. 31

6 REFERENCES ................................................................................................................................................... 33
1 Introduction

1.1 Vehicular Communication

Vehicular communication is of huge importance in order to increase traffic safety or improve traffic control in the future, as well as provide information and entertainment to the driver. In safety applications, there is a requirement of transferring information relating to e.g. road blocking, accidents and change of lane or path of the vehicles well in time so that accidents can be avoided. Even information about e.g. weather conditions or other factors are exchanged in order to recommend speed limits for safe driving. For transferring this information from or to vehicles, an infrastructure is required which consists of a wireless communication medium and communication devices and internet access. The interconnection of this infrastructure is a challenging task for smooth operation and timely exchange of information. The research field of Intelligent Transport Systems (ITS) has as its goal to develop and support various applications based on vehicular communication networks.

ITS covers a broad range of diverse technologies applied for transportation systems to make them safer and more efficient. The range of technologies comprises sensing, communication and computational technologies. Sensing technology and wireless communication technology are mainly used in vehicular networks for exchange of information. Various wireless communication technologies have been proposed for ITS, IEEE 802.11p is proposed for short to medium range communication whereas WIMAX (802.16), GSM and 3G are used for long range communication systems. IEEE 802.11p-enabled Access Points (AP) are planned to be placed on the road side for vehicle-to-infrastructure (V2I) communication.

These wireless APs are called Road Side Units (RSU). When a vehicle moves along the road, it shares its information with the RSU or receives data from it. These RSUs are linked to back-offices for exchange of information. A group of RSUs which are interlinked with one back-office router creates one subnet. Multiple subnets are present in the vehicular networks. The
connectivity between these RSUs and back office routers may e.g. happen through point to point wireless connections or through fibers.

Vehicles exchange their information through the RSU and are connected to it through an On Board Unit (OBU) present inside the vehicle. There also are multiple Application Units (AU) present in the vehicle, which are used by passengers, like laptops, PDUs etc. These AUs are interlinked with the OBU of the vehicle. All the vehicles are required to be equipped with GPS receivers and navigators with digital map information. The driver of the vehicle can select the destination route plan before starting its journey. This digital route map information is passed on through RSU when vehicle is going to enter on a highway and in response vehicle through OBU receives the information of the RSUs through which vehicle is going to be connected on its way to the destination.

When a vehicle is moving, its point of attachment with the RSU changes as it is breaking its connection with the previous RSU and establishing a new connection with the target RSU. This process of change in point of attachment to the network of the mobile nodes is called handover. These RSUs require to communicate with each other and when the vehicle moves and changes RSU, the handover has strict timing requirement as the time for a vehicle to communicate with a RSU is limited due to its high mobility and the handover should happen without long delays.

1.2 Focus of thesis

Our focus is to study different handover methods developed for mobility and investigate their suitability for the requirements of vehicular networks. We discuss the delays they introduce during layer 3 handover and the limitation in the handover initiation especially when a vehicle is going to attach with the new RSU after an area of no coverage. Our idea includes having information of the RSUs’ placement and the vehicle’s intended route entered into a navigator. Hereby, the intended route can be matched with upcoming RSUs along the road side and the handover procedure between a vehicle and overlapping and non-overlapping RSU can be improved.
In chapter 2, we describe vehicular networks, its infrastructure, requirements and how they work. Chapter 3 is covering different handover techniques and mainly focuses on Mobile IP version 6 (MIPv6). We describe our solution in chapter 4 by introducing a valid prediction, and then conclude our thesis in chapter 5.
Fast Layer-3 Handover in Vehicular Networks
Vehicular Networks

2 Vehicular Networks

Vehicular communication is of the hot topic nowadays. One aspect of ITS is to provide the driver with safety-related data to avoid road accidents. Another aspect is to enhance comfort through e.g. the delivery of entertainment data to the vehicles. Vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) or vehicle to internet server communication is required by many ITS applications. A number of projects are recently going on in Europe like CVIS, car to car communication consortium (http://www.car-to-car.org/) and SafeSpot (http://www.comesafety.org/) All of them are aiming to develop different models and solutions for distinct scenarios like safety applications vs. infotainment, V2V communication vs. V2I etc. Information exchange enables ITS application with other vehicles which are not in its line of the sight, but inside the communication range and inform them about sudden breaking maneuvers, traffic blocking information, weather conditions etc. so that these vehicles may avoid obstacles or dangerous situations ahead. This information can be passed on to other vehicles by RSUs or directly through ad-hoc networks of vehicles. Different protocols are designed for transferring this information.

As the number of vehicles on the roads will be in the range of millions and every vehicle and the devices inside vehicle might require to access internet services, it means millions of IP addresses are also required. In order to meet these challenges of accessing IPv6 is preferred over IPv4 because of its scalability due to large number of IP addresses range and its flexibility to accommodate any underlying wireless technology. For vehicular communications a special short to medium range communication protocol, 802.11p is designed. In both the US and in Europe, dedicated frequency channels in the 5.9 GHz frequency are planned to be used for V2V and V2I communications. IEEE 802.11p aims to ensure wireless communication in high mobility and is especially designed for vehicular communication as it assumes variable MAC addresses that are changed every time the system starts up and that are meant to protect the driver from being tracked.
2.1 WAVE

IEEE 802.11p is a part of the standard Wireless Access in a Vehicular Environment (WAVE) which supports ITS applications that includes exchange of data between high speed vehicles and also between vehicles and infrastructure (RSU). WAVE mode Basic Secure Set (WBSS) enhances 802.11p MAC functions for rapid changes in the communication environment. Upon start-up, a device monitors the Control Channel (CCH) until a WAVE service advertisement is received that announces a service which utilizes a Service Channel (SCH).

2.2 Parts of Vehicular Networks

Vehicular networks consist of following key components:

Road Side Units (RSU)
In vehicular network, all vehicles are required to exchange their information through RSU which are placed on the road sides. These RSUs are wireless Access Routers (AR) supporting 802.11p. RSUs provide the connectivity with vehicles for transmitting and receiving information. These RSUs are interlinked and also connected with the back office through wired or wireless medium backbones. A group of RSU linked with a back office creates a subnet. There are multiple subnets along the highways. The vehicle attached with the RSU must be a part of that subnet.

Back Office (BO)
A group of RSUs are connected with a back office for the exchange of information. This back office comprising of routers is connected with other back office router for the exchange of information and also with the internet gateways for the internet connectivity.

Internet Gateway
Internet gateways provide the connectivity for the internet access. They are connected to back office at one end and with the internet cloud at the other end to make connectivity through the internet for the vehicular networks.
On-Board Units (OBU)
All the vehicles have an OBU which is a wireless Access Point (AP) supporting 802.11p. This OBU provides the connectivity between vehicle and RSU.

Application Units (AU)
Inside the vehicles multiple application units may be included such as passengers with laptop, PDAs etc which may requires internet connectivity to check their necessary mails. This application units exchange their information through on-board units which are placed in the vehicles.

Figure 2.1. Infrastructure of vehicular network

2.3 ITS Applications
ITS applications are mainly comprising of two parts.
Safety applications
Non-Safety applications

Safety applications require real-time communication including vehicle sensor data for accident avoidance or the positions of broke-down vehicles or construction sites. Real-time information is required to be sent to the vehicle behind the accidental vehicle and the nearby vehicles. This real-time communication is done through the adhoc network directly from vehicle to vehicle and also
through vehicle to RSU to vehicle where as in non safety applications, which provide comfort to
the driver like change of its route plan and direction due to congestion, weather information,
speed limit information etc do not require real-time communication.

We are focusing on comfort applications or those applications which do not require strict timing
requirements as there is no real-time communication involved. However, it is still desirable to
minimize the time and bandwidth used for handover and connection setup even for this kind of
non real-time data exchange.

2.4 HANDOVER

When a vehicle moves along a road, its point of attachment with the RSU changes. This process
of leaving one wireless zone and entering in another wireless zone is known as handover. There
are two types of handover: Horizontal handover and vertical handover. If the change in point of
attachment is between same protocol devices then it is called horizontal handover like if the
vehicle is exchanging its information through 802.16 (WIMAX) and after the handover the new
point of attachment follows 802.16. The handover will be vertical if the change in point of
attachment is between two different protocols like if the first connectivity is through 802.16 and
after connection breaking, the new connectivity is through GPRS.

The multiple RSUs linked with one back-office form a subnet. All the communicating devices
which enter this subnet have to be part of this subnet and an IP address of this subnet is allocated
to each of them for communication. When there are more than one RSU which are part of this
subnet and when the vehicle changes its point of attachment between these RSUs of the same
subnet, then a layer 2 handover is required as shown in figure 2.2 [5].
FIG 2.2 Layer-2 handover

When vehicle is changing its point of attachment between the RSUs of different subnets then it requires a new IP address of that subnet and layer 3 handover is required as shown in figure 2.3
Figure 2.3. Layer 3 handover in vehicular network
3 HANDOVER TECHNIQUES

3.1 What is handover

When a node attached to the internet moves, then a protocol is required to handle the mobility of the user so that its network connection does not break during its movement. In IP, the Mobile IP scheme is the protocol responsible for taking care of all the movement of the MN. When the MN leaves its point of attachment and enters another area, its point of attachment is required to be changed and a handover is required so that the MN keeps its connection with the network and its contact with the corresponding node remains intact. The Mobile IP scheme provides a solution to this problem. Following are the key elements used in Mobile IP: Mobile Node (MN), Home Agent (HA), Foreign Agent (FA) and Corresponding Node (CN).

A MN is registered with its home network called home node network (HNN) and an IP address is allocated to the MN for connectivity with the corresponding node. This home network IP is a permanent IP and is called home address. However, the MN can leave its HNN. At that time it requires new IP address with the help of which it will connect to the internet and CN. The MN in the visitor area sends the messages to the FA for allocating the address of that subnet by giving the information of its address of the home network. The FA sends the packets to its HA for confirming its validity. If HA replies positively then the care-of address (CoA) is allocated to this MN but if the HA denies its validity then the request from the MN is cancelled by breaking the connection. Once the CoA is allocated to the MN, it becomes the member of this new subnet.

After allocating the new CoA, the FA sends the information to the HA of MN by informing that this MN is now part of its network. The new foreign address along with the home address of the MN is entered in the data entry of the foreign network. This is shown in figure 3.1.
3.2 Routing between Mobile Node and Corresponding Node

Delta Routing is the process to exchange the information between MN and CN in which the message is initiated by the CN who has not any information on the MN’s current location. This information is passed on to the FA by the HA. The FA then delivers this packet information to the MN. When the MN is going to reply to the CN, the information is sent directly to the CN through FA by bypassing the HA. This makes a triangle for transferring the information as shown in figure 3.2 [11].

![Diagram of Mobile Node and Corresponding Node](image-url)
Figure 3.2: Exchange of information with CN through Delta Routing

3.3 Mobile IPv6

The mechanism for supporting the mobility of MNs with IPv6 is called mobile IPv6 [2]. IPv6 addresses consists of 128 bits and having a significant space to accommodate large number of IP addresses. The left most bits in IPv6 are called prefix which are of variable length and one can distinguish the network through these bits pattern.

A node attached to a subnet in IPv6 is required to be aware of the subnet prefix of that network. In a most common LAN and other networking environment where nodes having MAC addresses then the IPv6 unicast address will be consisting of 48 bits of MAC address of the node and remaining 80 bits are used for subscriber prefix and subnet ID.

<table>
<thead>
<tr>
<th>N BITS</th>
<th>80-N BITS</th>
<th>48 BITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUBSCRIBES PREFIX</td>
<td>SUBNET ID</td>
<td>INTERFACE ID</td>
</tr>
<tr>
<td>(MAC)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Fast Layer-3 Handover in Vehicular Networks

When a MN enters in a network, it requires a new CoA of that subnet area. The MN is serviced by a HA when it is in its home network area. The attachment with the other subnets is through the router advertisement messages which a router advertises whenever a MN moves into its area. Because of the IPv6 feature of auto configuring of node’s IP addresses in which node fabricates its new care of address comprising of subnet ID advertised by new router through router advertisement messages and its own MAC address. This new care of address is required to be communicated to the HA and CN to let them know of its new location. This is done in the following steps. The MN sends the binding update (BU) message to HA and CN. These messages are sent through its new CoA. The new AR acts as proxy for performing address detection checks. After successfully Duplication Address Detection (DAD) check, a binding acknowledgement is sent to MN which indicates the confirmation of its address. Then the binding acknowledgement BU is sent to CN and HA. In this way the information is transferred to HA and CN, rerouting the traffic to the MN’s new location. The main problem with this approach is to send the binding update to the HA especially when they are geographically far away from the MN’s current location. The MN moves in a small coverage area (micro mobility) and the message exchange transmitting line for transmitting BU will become high and causes delays and disturbance in service. This also increases the load on the core network.

See figure 3.4 and figure 3.5.

![Figure 3.4: Exchange of information with CN in MIPv6](image-url)
3.4 Advantages of MIPv6 Over MIPv4

We preferred MIPv6 over MIPv4 because of its following advantages,

Address auto configuration is a standard part of IPv6 which helps the MN to obtain its COA. This reduces the MN registration time while entering a foreign network, whereas in MIPv4, there is long delay between the communication path between HA and FA for registering the MN.

In IPv4, there are limited numbers of IP addresses left which are unable to cover millions of vehicles. Due to this limitation in MIPv4, it is not scalable where as in IPv6 there is no such problem and can easily accommodate millions of vehicles. Because of the limited number of IP addresses in IPv4, MIPv4 requires to conserve addresses by using Network Address Translation (NAT) in the FA address but in MIPv6 there are more than enough IP addresses and hence there is no need for the FA but only a co-located COA mode is enough. Delta routing is avoided in MIPv6 due to built in route optimization facility in which MN send Binding Updates (BU) to CN.
for forwarding the packets directly. This overcomes the single point of entry failure at the HA in MIPv4 due to this delta routing. Because of the feature of IPv6 to make source routing possible, the packets are sent directly from CN to MN without need of encapsulation.

3.5 Mobile IPv6 types

Following are the two techniques used for the seamless handover which are widely used in MIPv6 and supported by IETF [6]: Hierarchical Mobile IPv6 (HMIPv6) and Fast Handover Protocol for Mobile IPv6 (FMIPv6).

3.5.1 Hierarchical Mobile IPv6 (HMIPv6)

Hierarchical Mobile IPv6 [12] is a micro mobility management technique in which we divide our network into administrative domains. The concept of Mobility Anchor Point (MAP) is introduced which controls each administrative domain and acts as proxy HA within a local domain. So a separate MAP is required for separate domain. The mobility of the node inside a domain is called micro-mobility where as mobility of node when it enters in new domain is called macro mobility and is managed by MIPv6 that’s why HMIPv6 is also called micro-mobility management scheme as shown in figure 3.6.

When the MN enters in new domain, it acquires two new CoA called Regional CoA (RCoA) and on-Link CoA (LCoA). The LCoA changes whenever the MN changes its AR attachment, but within a domain its RCoA remains same and the RCoA only changes when the MN enters in new domain area. The MN informs its location to its HA and CN by using the RCoA. So they reroute the traffic destined for the MN to its RCoA and packets reached at its current MAP. The MAP encapsulates these packets to the MN with the help of encapsulating them to its LCoA and it is using binding cache. The MN keeps on sending BU messages to the MAP periodically to maintain current mapping [3].

The main drawback of this approach is that it is very complex when the network domain of the MN changes as it is not designed for the layer-3 handover and when the Regional CoA changes then HMIPv6 is not ideal due to increased latencies and delays.
3.5.2 Fast Handover for Mobile IPv6 (FMIPv6)

IETF’s proposed FMIPv6 [1] is an extension of MIPv6 which shows a promising solution for Layer 3 handover by reducing the duration and minimizing the number of packets. The idea of this protocol is to provide all the information of next AR for Layer 3 handover before going to the part of its subnet. It also provides the flexibility to buffer all the packets destined for MN during the handover process.

FMIPv6 handles the handover process as below.

When the MN discovers the neighboring router then it sends the router solicitation messages for proxy advertisement (RtSolPr) to its current AR. The AR then replies with the proxy router advertisement (PrRtAdv) to the MN. Upon receiving these proxy router advertisement messages, the MN send Fast Binding Updates (FBU) to its current AR. These FBUs include the information of MN current subnet address as well as the subnet address of the new AR to which it is going to attach. At this time, the current AR sends the Handover Initiate (HI) messages to new AR which replies with the Handover Acknowledgement (HACK) to the previous AR (PAR). Upon receiving the HACK, the previous AR sends the Fast Binding Acknowledgement (FBACK) to the MN. During all this process, the MN is still connected with PAR. When MN enters in the area of the new AR (NAR) then its link with the previous AR is disconnected and it sends the Router Solicitation messages by Fast Neighbor Advertisement (FNA) messages to the NAR. The purpose of FNA is to inform the NAR to stop buffering the MN’s packets and complete the handover signal. During this handover process previous AR forwards the packets to NAR which are destined for the MN [7]. Figure 7 shows the handover steps in FMIPv6.
FMIPv6 defines how a MN attains the new CoA of a neighboring subnet while connecting with the current AR. However it is worth mentioning that FMIPv6 does not define any specific method for discovering the next candidate AR and this is the major weakness of this protocol. Also during the allocation of the new CoA there is a Duplication Address Detection (DAD) check is performed in which host sends the neighbor solicitation messages to the solicited-node multicast address including the tentative address field to check whether the new CoA is unique or not. This DAD check consumes an extra amount of time and some time it is more than 1sec [7].

3.5.3 Fast Handover for Hierarchical Mobile IPv6 (F-HMIPv6):
F-HMIPv6 is developed by combining of both HMIPv6 and FMIPv6. Evaluations [4] show that the combination of both of these techniques reduces the latency and delay during handover and improves the handover performance as well. In this technique, when a MN enters in new subnet area or domain of MAP then it first performs the HMIPv6 registration procedure with the HA and MAP where it follows the local BU procedure of FMIPv6 when it enters from PAR to NAR.
During this handover processing time, the data packets are tunneled by MAP towards NAR through a bi-directional tunnel. This is the same as in FMIPv6, but it is worth mentioning that no bi-directional tunnel is formed between PAR and NAR. Figure 3.8 shows the operation of the F-HMIPv6.

The results shown by different authors indicate that handover performance is increased by the combination of both HMIPv6 and FMIPv6 protocols. Most of the results obtained are by ignoring the DAD factor. Though the probability of address duplication is very low and can not be ignored [5,10] but it can not be ignored. As the handover process initiates when MN receives the beacon transmitted by the next AR and during this stage he requires to be connected with the current AR and this requires a very limited time for completing the handover process and if there is a DAD check consider then there are chances of delay and loss of packets as well.

3.6 Network Mobility (NEMO)

NEMO is a process which is used to manage the mobility of the nodes inside a mobile network. The nodes inside mobile network are called Mobile Network Nodes (MNN). These MNNs are
managed through a Mobile Router (MR) with the help of mobility anchor point, HA. In vehicular networks, the MR is a part of the OBU and MNNs are the devices used inside vehicle to access internet based services.

3.6.1 NEMO Handover

When vehicle with its MR is in its home network then it is attached directly to its HA and all MNNs access internet and other network through a MR. When vehicle moves and it enters in new network then its MR required a new care of address of this network through router solicitation messages and router advertisement messages and obtains the new care of address through auto configuration as in MIPv6. After obtaining a new care of address it sends BU to its HA for binding its new care of address with permanent home address. HA replies with BA message to verify that it has updated its status. A tunnel is established between CoA of MR and the address of HA for transferring of data.[8]

MNN’s are always attached to the MR and are unaware of this mobility as they are fixed to the same network and hence are also called Local Fixed Node (LFN). When another MN capable of mobile routing enters in this network like a passenger with the router capable device enters in a public transport then it requires to be a part of this network. This MNN is called Visiting Mobile Node (VMN). VMN sends the BU to its home agent after attaining the new care of address of this network and a tunnel is created for the transferring of information. This results in two nested level of mobility management as mobile network inside a mobile network. [9]

3.6.2 Latencies in NEMO Handover

The handover process in NEMO comprises of three main parts. We will see the delays during each of the handover stage. In layer 2 handover the MR finds a new AP and it becomes associated with it. The only latency in this process is the delay in finding the new AP and associate with it. When a MR finds the AR as an attachment then this is a layer 3 handover. The network attachment of a MR consists of the router discovery and the CoA configuration. For the router discovery, the MR sends a router solicitation (RS) to the AR and the AR replies with the RA.
There is a delay in sending RA messages from AR. After discovering a new AR, the MR requires a new CoA from this network. This new CoA is attained by following IPv6 stateless address auto-configuration. This new CoA must be unique and in IPv6 this is checked through DAD procedure. This DAD procedure is configuration dependent and causes a delay. The whole delay in the DAD process varies between 1-2 sec. During home registration of the MR, the MR sends the BU to its HA and the HA replies with the BA. This causes the propagation delay and increases the latency. Following figure (fig 3.9) shows the MR along with its attached nodes in Home network and when it moves to the foreign network.

Figure 3.9. NEMO with foreign network
Fast Layer-3 Handover in Vehicular Networks
4 FASTER HANDOVER

In our solution, we focus on Layer 3 fast handover in vehicular networks. We discussed briefly about vehicular network infrastructure in Chapter 2 where we described RSUs which were required to be placed by the road sides. These RSUs communicate with vehicles, transferring data to and from OBUs of the vehicles. These RSUs are also the member of subnet which are connected to a back-office. Each back-office represents one subnet and is also interconnected with other back-offices as well. Our focus is on layer 3 handover, that is when a vehicle enters from one RSU to another RSU of another subnet. These subnets are also connected to the internet through a gateway. Following figure shows the infrastructure of vehicular networks in our scenario. See Figure 4.1.

When a vehicle moves and changes its point of attachment with the RSU within the same subnet, then the handover is on layer 2, whereas it will be on layer 3 when it changes its point of attachments with RSU of other subnet area.
As vehicles are moving, we require to analyze different mobile IP schemes which we discussed in the handover techniques chapter. We foresee some of the problems and limitations in the Mobile IPv4 scenario as it is not scalable due to shortage of IP addresses left in IPv4 and found Mobile IPv6 more suitable as compared to the MIPv4 as it overcomes some of the problems and limitations of MIPv4. In MIPv6 we saw two most commonly used techniques used for handover, HMIPv6 and FMIPv6. In addition to these widely used techniques we also observe some of their complexities and delays during handover. It was also noticeable that during the router solicitation state after L2 handover, OBU request for the router advertisement in order to determine the network identification and this causes extra time consumption.

For the exchange of e.g. digital map information, sensor information weather data between a vehicle and a RSU, the attachment of the vehicle with the RSU is necessary and the handover time must be as short as possible. As a vehicle is moving fast and due to some fluctuation in signal strength between RSU and vehicle, the handover time must be as short as possible so that the information reaches the vehicle in time before it leaves the transmission range of the RSU again and in order to perform the required actions, like changing the lane or limiting the speed etc.

We observed that in all techniques of MIPv6 the handover process initiates when the MN listens to the beacon messages of new AR. This mechanism has two drawbacks. It is quite possible that when it listens to the new AR then signal strength with the current AR is too weak and it is going to lose its connectivity with the current AR. During this case there are chances that this handover process may not be competed before the MN leaves its connectivity with the current AR. This causes loss of data.

In our case, due to cost and maintenance reasons, it is not possible to place RSU on the road side for perfect coverage. It means that there will be some areas when a vehicle is not connected to any RSU. All the reviewed handover techniques were only designed for continuous coverage of the AR so they fail in the case of non-seamless coverage. When vehicles enter the new RSU’s transmission area, they have no IP address of that subnet. Figure 4.2 shows the scenario of the handover when a vehicle is leaving one subnet and entering in new subnet after no coverage zone.
We come up with the following assumption in order to overcome the above mentioned limitations and drawbacks. The location of the RSU is predefined by following a planning about their placement such that one must also aware of their signal strength at each location and their coverage area is also known in all weather conditions. This assumption is considered by modifying MIPv6 techniques for seamless handover. Navigators are located in each vehicle and through which the driver of the vehicle assigns its route path towards the destination. OBUs inside vehicles have intelligence in selection of AR according to its route map. The OBU is required to transfer this information to its attached AR.
When a vehicle is going to enter on a highway equipped with RSU it requires to register with this network by sending its MAC ID of its OBU interface to the AR and become a part of that network. This first-back office becomes the HA of the vehicle for the rest of the journey until the vehicle stops entirely and get started again then its MAC address changes so it requires to initiate its registration process again and obtains a new HA.

When a vehicle moves and changes its point of attachment with the new AR then a handover is required to take place. As in our case the intelligence of selecting the new AR is inside the vehicle’s OBU with their network prefixes. If the next AR is of same subnet as of the current then there is no need of layer 3 handover and handover process follows local link handover by simply following association process. If the next up-coming AR is of a different subnet the handover is layer 3 as the OBU requires to be a part of new subnet and requires a new care of address of that subnet as shown in figure 4.3.

![Flowchart](image-url)

**Figure 4.3. Decision making of OBU**

When vehicle analyzed that its next RSU is of different subnet as of the current subnet and it requires the new CoA of that subnet to be a part of that subnet then it informs about the next AR’s subnet address along with its own interface ID to the current AR as shown in fig 4.2. This information is sent instantly when the vehicle attached to the current AR. Now, the current AR
creates a new CoA and sends it to the new AR. As in FMIPv6, the current AR will create a new temporary CoA for this OBU and sends this proposed new CoA to the OBU and at the same time to new AR for the verification of this address. The new AR checks this new CoA and if it is valid, then adds it in its cache and sends back the acknowledgement to the current AR. The current AR then informs the vehicle’s OBU about the confirmation of the new CoA. So the vehicle attains the new CoA to which it is going to attach while being connected with the new AR. When the OBU enters the area of a new AR even after no coverage area, as shown in figure 4.2, and receives the beacons generated by the new AR, then the OBU matches these beacon messages whether these are from the same AR with which it is going to connect or not. If the beacons match with its target AR, it responds to these beacon messages of new AR and gets associated. As the OBU does not need to wait for the router’s advertisement as in other handover techniques as in FMIPv6 and no router solicitation messages is sent to the new AR, so the handover time is reduced significantly and the OBU is associated to the new AR in the seamless manner. See figure 4.4. During this handover process, the previous AR forwards the packets to the new AR which are destined for OBU as in FMIPv6.

Figure 4.4. Handover Pattern in new scenario
4.1 Advantages

This handover technique reduces the handover latencies and increases the efficiency in the following ways. The handover is seamless if there is a continuous coverage of the RSU’s and no data loss as the handover process initiates at once as soon as the vehicle is attached with the current AR. This gives enough time for attaining new CoA for vehicle’s next AR while being connected with the previous AR and handover is very fast as OBU of vehicle only need to respond to the beacons of the new AR.

This technique is even suitable for the non-continuous RSU coverage area where as FMIPv6 fails when the coverage is not seamless, as FMIPv6 initiates upon receiving the beacon messages from the router and has to send this information to its currently attached AR. But it is not possible if the vehicle is not connected to any AR whereas our solution overcomes this problem while the handover process will still be as efficient as it is in continuous coverage area because the OBU already attained the IP address of the target AR and only needs to response to the beacon messages and become associated to the new AR.

The communication overheads are overcome by avoiding to send the probe messages everywhere to find out its new router by providing maximum intelligence of attaching to the desired AR inside vehicle’s OBU. The decision of attaching with the new AR is initiated by the AR’s beacon messages.

The chances of loss of data packets during handover processing time are also avoided by sending binding updates to old AR. These binding updates will forward all those packets to vehicle’s new care of address through the new AR which reaches to it during handover process.

4.2 Limitation

Our proposed idea strongly require the information on the RSUs’ placement and if the information of the RSU is not properly communicated then the handover process will not be
ideal. Information of the route plan is required to be fed into the navigator by the driver and if there is any change in the route plan of the vehicle then it must re-define its route plan to get the correct information of the RSU along its way. When a vehicle is not connected to any of the RSU then it requires to exchange its information through vertical handover like WIMAX, GPRS etc. for the connectivity with its corresponding nodes. But as the switching of protocol causes problems and the latencies increases and handover processing time is increased in this case. Because of the changing MAC addresses of the vehicle whenever vehicle restarts then the registration with the new BO causes delay as vehicle has to initiate the registration process to become a member of that network.
Fast Layer-3 Handover in Vehicular Networks
5 CONCLUSION

In vehicular communication, the handover delay issue is of great importance. For fast handover, we preferred MIPv6 over MIPv4 by highlighting some of the limitations of the MIPv4 and discussed some of the advantages of MIPv6. We discussed two widely used MIPv6 methods which reduce the handover delay up to some extent but still they have some drawbacks. We observed that major drawback of these techniques is that handover process requires continuous coverage of AR where as in vehicular environment such scenario is not possible as it is not possible to provide the coverage area throughout roads.

We present our solution by introducing an assumption that the knowledge of the next target router lies within the vehicle’s OBU in which we indicated that the location of the RSUs would be predefined and also the intelligence of the point of attachment with the next AR is inside vehicle. With the help of the predefined location of the AR and by providing intelligence inside vehicle’s OBU, vehicle attains the IP address of the next subnet at the same moment while attaching to the current AR as it already has a knowledge of next AR due to the predefined road path and navigator inside the car. This helps out in reducing the handover time of the vehicle while going to attach with AR of another subnet even after entering from a non coverage area.

Introduction of this assumption will reduce the handover latencies for both continuous wireless signal area as well as non-continuous area. We know that installation of RSU throughout road sides would not be possible in the beginning as a lot of cost is required to implement them and our solution is specifically applicable for such circumstances as it will be ideal for such solution. Right now due to shortage of time we could not investigate the reduction in handover delay through our idea and we would like to work on to prove our assumptions through simulation and numeric analysis and would like to compare how our assumption can really increase the handover timing as compared to the existing scenarios.
Fast Layer-3 Handover in Vehicular Networks
6 References

[4]. R. Hinden: RFC 1884 (rfc1884) - IP Version 6 Addressing Architecture
[5]. M. Emmelmann, T. Langgärtner, M Sonnemann “System design and implementation of seamless handover support enabling real-time telemetry applications for highly mobile users” in proceeding of the 6th ACM international symposium on Mobility management and wireless access, year of publication: 2008, Pages: 1 – 8
[6]. A. Shimizu, Sh. Fukuzawa, T. Osafune, M Hayashi and S. Matsui ”Enhanced functions of 802.11 protocol for adaptation to communication between high speed vehicles and infrastructures”, in proceeding of the 7th International Conference on ITS Telecommunications, 6–8 June 2007, pp: 1 – 3
Fast Layer-3 Handover in Vehicular Networks


[12]. H. Soliman, "Hierarchical Mobile IPv6 Mobility Management HMIPv6)”, RFC 4140, IETF, 2005